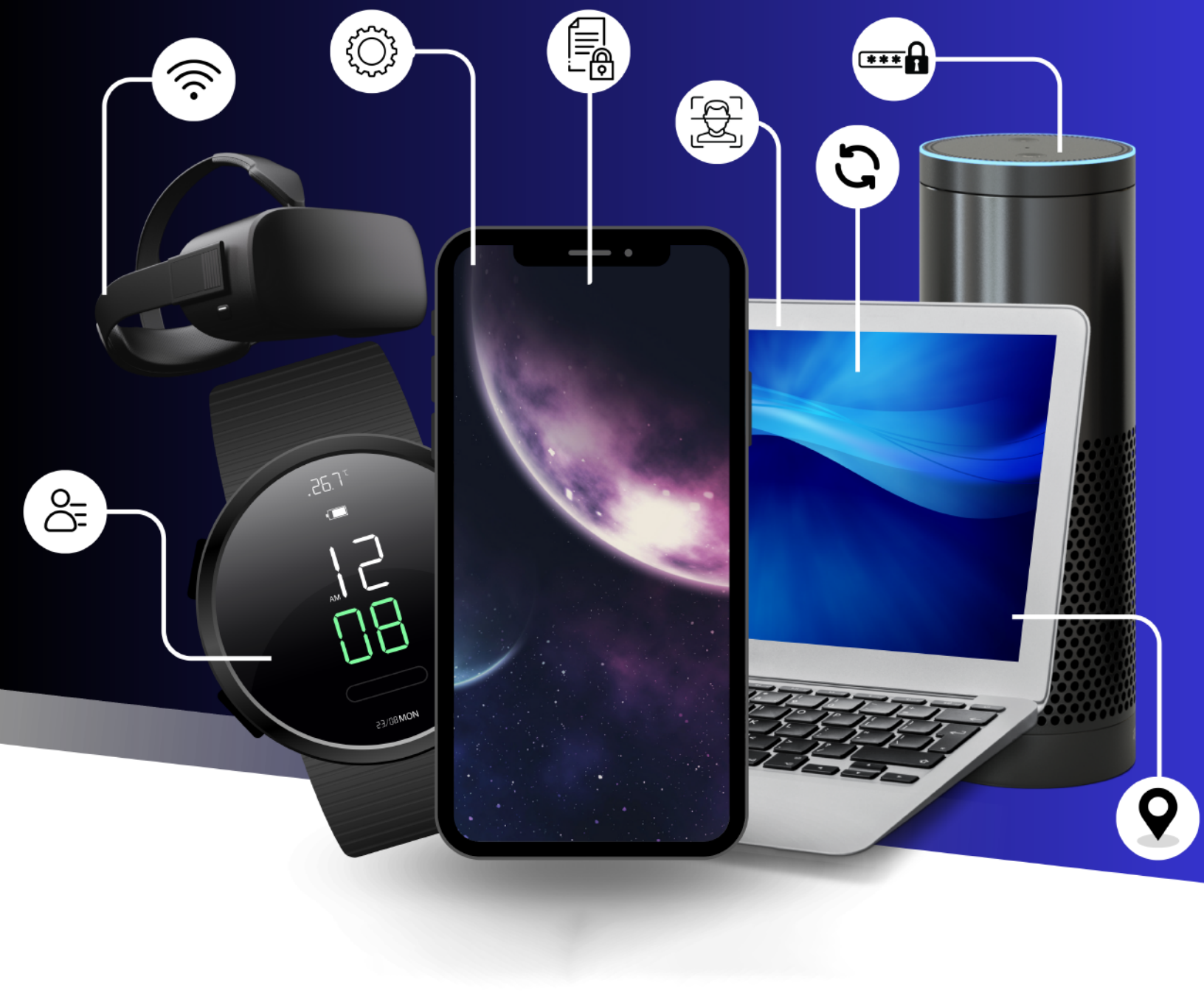
ift INSTITUTO FEDERAL DE TELECOMUNICACIONES



CIBERSEGURIDAD EN LOS DISPOSITIVOS DE INTERNET DE LAS COSAS (IoT)

INTRODUCCIÓN.

Como parte del avance tecnológico y la inclusión de nuevas oportunidades de comunicación, en la actualidad aquellos productos y aparatos que tradicionalmente no se conectaban a Internet, hoy lo hacen y ofrecen a los usuarios una variedad de opciones para hacer más fáciles algunas actividades.

Actualmente, las personas comparten su información a través de un número creciente de Dispositivos IoT y servicios asociados en línea que permanentemente están recolectando y procesando dichos datos. Lo anterior, permite que terceros puedan conocer los gustos, preferencias, horarios, direcciones, entre otra información de las personas, por lo que es importante tomar conciencia acerca de los datos que se comparten en la red y los riesgos que esto conlleva.

Por ello, resulta importante que los dispositivos sean diseñados para resistir amenazas en la seguridad, ya que los riesgos vinculados a una falla o falta de seguridad en estos dispositivos conectados a Internet afecta la confianza de los usuarios que los usan, y puede existir una afectación en su privacidad y economía.

En 2023, el Instituto Federal de Telecomunicaciones publicó el "*Código de mejores prácticas para la ciberseguridad del Internet de las Cosas*", documento que tiene como finalidad coadyuvar a una evolución tecnológica segura y confiable mediante la promoción de la responsabilidad social en el ecosistema digital.

Asimismo, en el año 2022, el Instituto publicó el Catálogo de Dispositivos Internet de las Cosas, mismo que tiene como finalidad ofrecer información sobre las principales características de los dispositivos IoT que se comercializan en México y que han sido homologados. Consultable en: Catálogo de Dispositivos IoT

Podemos entender que un Dispositivo de Internet de las Cosas, se trata de una pieza o componente de un equipo que pueda hacer uso del espectro radioeléctrico o ser conectado a redes de telecomunicaciones, los cuales se pueden emplear típicamente en el hogar o en dispositivos electrónicos portátiles, con capacidades opcionales de teledetección, accionamiento, captura, almacenamiento y/o procesamiento de datos y que guarda relación con un servicio asociado a este.

Por lo anterior y con la finalidad de incentivar la adopción de estas nuevas tecnologías e informar a los usuarios sobre la información que comparten y otros aspectos importantes relacionados con la ciberseguridad, el Instituto publica el documento Ciberseguridad en los dispositivos de internet de las cosas (IoT), en el cual se plasman los resultados del análisis de 348 fabricantes o marcas, que tienen dispositivos homologados ante este Instituto, los cuales se pueden consultar en: Catálogo de Dispositivos IoT

OBJETIVO:

La publicación del presente informe tiene como objetivo transparentar la información que los fabricantes o marcas difunden en sus portales de internet y que se encuentra asociada a las características que se establecen en el Código de mejores prácticas para la ciberseguridad del Internet de las Cosas.

Lo anterior, también permitirá que las personas usuarias conozcan algunos de los elementos de ciberseguridad que el IFT recomienda para el diseño y fabricación de dispositivos IoT.

METODOLOGÍA.

Para la integración del presente documento, se llevó a cabo una clasificación de los controles técnicos y políticas organizativas que se sugiere observen los fabricantes de los Dispositivos IoT en el Código de mejores prácticas para la ciberseguridad del Internet de las Cosas publicado por el IFT.

Posteriormente, se clasificó la información y se plasmó en las fichas organizativas conforme a los siguientes apartados:

- Contraseñas.
- Actualizaciones al Software.
- Sobre el Uso de Comunicaciones Seguras.
- Integridad del Software.
- Sobre los Datos de Telemetría.
- Sobre la eliminación de los datos personales.
- Sobre las credenciales y los parámetros de seguridad sensible.
- Sobre la eliminación de los datos personales.

Es importante destacar que la información plasmada en el documento se recolectó en los sitios de internet de los fabricantes o marcas y el análisis de la información no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales o marcas ya que su única finalidad es informativa.

Para pronta referencia, se agrega al final de cada tabla la o las fuentes de los 348 fabricantes o marcas analizadas, a fin de que, en caso de tener mayor interés, se pueda consultar más información.

Finalmente, es importante destacar que los fabricantes o marcas comercializan un gran número de equipos con diversas características y funcionalidades, por lo que la información que se establece en las páginas analizadas pudiera variar y atender algunas las variables consideradas en la integración de las tablas que se muestran en el presente informe.

PRINCIPALES HALLAZGOS.

1. La información sobre especificaciones de ciberseguridad en los productos de algunas de las marcas revisadas no fue de fácil ubicación, ya que en sus páginas web es necesario realizar una búsqueda exhaustiva.
2. De las marcas revisadas, algunas no cuentan con una página web donde se puedan consultar sus productos, así como los términos, condiciones y avisos de privacidad.
3. En algunos casos, las páginas web de las marcas revisadas redirigen a otros sitios web para consultar términos, condiciones y avisos de privacidad.
4. Algunas de las marcas revisadas en sus términos, condiciones y avisos de privacidad no incluyen información respecto a los incidentes de seguridad relacionados con la información y datos personales de los usuarios.
5. En algunas ocasiones, no existe información ni página web para consultar información de seguridad en los dispositivos.
6. Del ejercicio realizado, se destaca que, en algunos casos, los términos, condiciones y avisos de privacidad de las marcas revisadas, se encuentran en idiomas distintos al español.
7. De las marcas analizadas incluidas en el Catálogo de Dispositivos IoT, únicamente el 8% no cuenta con ningún tipo de información relacionada con las características de ciberseguridad de sus dispositivos.
8. Del ejercicio que esta CGPU llevó a cabo para la búsqueda de información relacionada con la ciberseguridad de equipos IoT en las marcas analizadas, se puede desprender que esta información es de difícil acceso para los usuarios, por lo que resulta importante que se promueva la transparencia de esta para la generación de confianza y el uso seguro de estas nuevas tecnologías.

RECOMENDACIONES.

Con la finalidad de promover la confianza y el uso seguro de estas nuevas tecnologías resulta importante tomar en cuenta las siguientes recomendaciones:

1. Verifica si las actualizaciones de software de tu dispositivo se realizan de manera automática o no, y procura mantenerlo actualizado.
2. Personaliza el nombre de usuario y contraseña del dispositivo y/o la cuenta asociada.
3. Utiliza contraseñas seguras para acceder a tu dispositivo y la cuenta asociada.
4. Si es posible, además de las contraseñas seguras, utiliza un método de doble autenticación para acceder a tu dispositivo y la cuenta asociada.
5. Revisa el tratamiento que le darán a tu información y datos personales.
6. Cuando no estés haciendo uso del dispositivo, desactívalo.
7. Si ya no utilizarás el dispositivo, elimina tu información y datos personales almacenados en este, así como la cuenta asociada.
8. Identifica la información que tus equipos recolectan y los mecanismos que tienen habilitados para configurar la privacidad. Utiliza los mecanismos de configuración de privacidad con la finalidad de que solo sea visible la información que desees.

DIRECTORIO DE MARCAS

ÍNDICE

ÍNDICE

ÍNDICE

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

360

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://smart360.mx/

https://smart360.mx/policies/privacy-policy

https://smart360.mx/pages/servicio-tecnico-oficial

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ABODE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://support.goabode.com/docs/contacting-abode-support

https://support.goabode.com/docs/abode-terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ACTIA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

http://actia.com.mx/

https://www.actia.com/en/legals

https://www.actia.com/en/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ACTIONTEC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.actiontec.com/

https://www.actiontec.com/terms-of-use/

https://www.actiontec.com/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ADVANCED HOME

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://lloydscorp.com/

https://lloydscorp.com/contactanos/

https://lloydscorp.com/privacy-agreement-advancedhome/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AIRLINK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.airlinkambulance.com/

https://www.airlinkambulance.com/terms-conditions-site/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AIWA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://aiwalatinoamerica.com/

https://globalinternet.com.pa/politica-de-privacidad/

https://globalinternet.com.pa/terminos-de-servicio/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AJAX

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://ajax.systems/es/

https://ajax.systems/es/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AKASO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.akasotech.com/

https://www.akasotech.com/terms

https://www.akasotech.com/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ALARM.COM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://alarm.com/

https://www.alarm.com/terms_conditions.aspx

https://www.alarm.com/legal/privacy?culture=es

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ALCATEL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.alcatelmobile.com/mx/

https://www.alcatelmobile.com/mx/privacy/

https://www.alcatelmobile.com/mx/terms-conditions/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ALCATEL-LUCENT (ALE INTERNACIONAL)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.al-enterprise.com/en/

https://www.al-enterprise.com/en/legal/privacy

https://www.al-enterprise.com/en/legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ALTAI (ALTAI TECHNOLOGIES, SIN MARCA)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	si
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://supportsystem.com/privacy/

https://www.altaitechnologies.com/contact-us/

https://supportsystem.com/terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AMAZFIT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://mx.amazfit.com/

https://mx.amazfit.com/pages/aviso-de-privacidad

https://mx.amazfit.com/policies/terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AMAZON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.amazon.com.mx/gp/help/customer/display.html?nodeId=468496&ref_=footer_privacy

https://www.amazon.com.mx/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GA75EXWGGZPEFSQS

https://www.amazon.com.mx/gp/help/customer/display.html?ref_=hp_left_v4_sib&nodeId=GLSBYFE9MGKKQXXM

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AMPLIFI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://ampli.ca/

https://ampli.ca/terms-and-conditions

https://www.rbc.com/privacysecurity/ca/index.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ANGEL CARE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://angelcarebaby.com/pages/privacy-policy

https://angelcarebaby.com/pages/terms-conditions

https://angelcarebaby.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

APPLE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.apple.com/mx/

https://www.apple.com/mx/legal/sales-support/terms/repair/

https://www.apple.com/mx/legal/privacy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ARISTA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.arista.com/en/

https://www.arista.com/en/privacy-policy

https://www.arista.com/en/terms-of-use

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ARLO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.arlo.com/en-us/

https://www.arlo.com/en-us/privacy-policy.html

https://www.arlo.com/en-us/terms-and-conditions.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ARRI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.arri.com/en/privacy

https://www.arri.com/en/terms-conditions

https://www.arri.com/en

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ARRIS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://arrisbuilt.com/privacy-policy/

https://arrisbuilt.com/privacy-policy/#contact

https://arrisbuilt.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ARUBA / HEWLETT PACKARD ENTERPRISE / HPE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hpe.com/us/en/legal/privacy.html#

https://www.hpe.com/us/en/about/legal/terms-of-use.html

https://www.hpe.com/us/en/home.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ARUBA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hpe.com/us/en/legal/privacy.html#

https://www.hpe.com/us/en/about/legal/terms-of-use.html

https://www.hpe.com/us/en/home.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ATTOP

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ATVIO

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AUDIO PRO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.audiopro.com/en/

https://www.audiopro.com/en/new-terms-and-conditions/

https://audiopro.zendesk.com/hc/en-us

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AVA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.avasoluciones.com/politica-de-privacidad/

https://www.avasoluciones.com/reembolso_devoluciones/

https://www.avasoluciones.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AVERA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://avera.mx/pages/aviso-de-privacidad

https://avera.mx/pages/terminos-y-condiciones

https://avera.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AVIA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://avia.com.es/politica-de-privacidad/

https://avia.com.es/condiciones-legales-app/

https://avia.com.es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AXIS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.axis.com/es-es/privacy/privacy-policy

https://www.axis.com/professional-services-gtc

https://www.axis.com/en-us

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

AXON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.axon.com/politica-de-privacidad/

https://es.axon.com/condiciones-de-uso/

https://es.axon.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BANG& OLUFSEN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bang-olufsen.com/es/mx/legal/privacy-policy

https://www.bang-olufsen.com/es/mx/legal/terms-of-use

https://support.bang-olufsen.com/hc/es

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BARCO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.barco.com/es/about/trust-center/privacy-policy

https://www.barco.com/es/about/terms-conditions

https://www.barco.com/es

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BAXTER

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.baxter.mx/es/aviso-de-privacidad-baxter-sa-de-cv

https://www.baxter.mx/es/terminos-de-uso

https://www.baxter.mx/es

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BDCOM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bdcom.com/pages/view/privacy-policy

https://www.bdcom.com/pages/view/terms-and-conditions

https://www.bdcom.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BELKINI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.belkin.com/us/privacypolicy/

https://www.belkin.com/general-terms.html

https://www.belkin.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BENQ

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.benq.com/es-mx/policy/privacy-policy.html

https://www.benq.com/es-mx/policy/user-terms.html

https://www.benq.com/es-mx/index.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BINTEC ELMEG

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bintec-elmeg.com/en/company/terms-and-conditions/privacy-policy/

https://www.teldat.com/legal-notice/

https://www.teldat.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BLACKVUE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://blackvue.com/warranty-terms-conditions/

https://helpcenter.blackvue.com/hc/en-us

https://blackvue.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BLUEBIRD

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bluebirdcorp.com/about/privacy

https://www.bluebirdcorp.com/about/resource-library

https://www.bluebirdcorp.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BLUESOUND

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bluesound.com/privacy-policy/

https://www.bluesound.com/legal/

https://www.bluesound.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BMW

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bmw.com.mx/es/footer/footer-section/privacy-policy.html

https://www.bmw.com.mx/content/dam/bmw/marketMX/bmw_com_mx/Descargas/Aviso-de-Privacidad/2023/BMW_CD_TC_MX-ES_2023.07

https://www.bmw.com.mx/es/index.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BOSE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bose.mx/es_mx/legal/privacy_policy.html

https://www.bose.mx/es_mx/legal/terms_of_use.html

https://www.bose.mx/es_mx/index.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BOWERS& WILKINS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.bowerswilkins.com/es-es/privacy-policy.html

https://www.bowerswilkins.com/es-es/terms-and-conditions-of-supply.html

https://www.bowerswilkins.com/es-es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BROTHER

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.brother.com.mx/politica-privacidad

https://www.brother.com.mx/terminos-de-uso

https://www.brother.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

BTICINO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://bticino.com.mx/aviso-de-privacidad

https://bticino.com.mx/ayuda

https://bticino.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CAFÉ

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://cafeappliances.lat/Privacidad.aspx

https://cafeappliances.lat/Terminos.aspx

https://cafeappliances.lat/Index.aspx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CAMBIUM NETWORKS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.cambiumnetworks.com/privacy-policy/

https://www.cambiumnetworks.com/legal-terms/

https://www.cambiumnetworks.com/support/

https://www.cambiumnetworks.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CANON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.canon.com.mx/aviso-de-privacidad

https://www.canon.com.mx/terminos-condiciones

https://www.canon.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CASIO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.casio.com/mx/terminos-y-condiciones/

https://www.casio.com/mx/privacy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CHAFON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

http://www.chafon.com/cpzx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CHAMBERLAIN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.chamberlain.com/social-terms

https://www.chamberlain.com/privacy-notice

https://support.chamberlaingroup.com/s/?_gl=1*134hya1*_gcl_au*NzE1MDAwOTk5LjE3MDE2NjgwNjc.*_ga*OTY4ODY1NDE3LjE3MDE2NjgwNjc.*_ga_LTGW1ESFYC*MTcwNTQ0MzUyNi4yLjEuMTcwNTQ0Mzc0OC4wLjAuMA..*_ga_1DRKQPY8MG*MTcwNTQ0Mzc0My4yLjAuMTcwNTQ0Mzc0My4wLjAuMA..&_ga=2.73116182.486324060.1705443527-968865417.1701668067

https://www.chamberlain.com/about-chamberlain/legal-disclaimer

https://www.chamberlain.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CIRCLE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.circle.com/en/legal

https://www.circle.com/en/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CISCO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.cisco.com/c/es_mx/about/legal/privacy-full.html

https://www.cisco.com/c/en/us/about/legal/terms-conditions.html

https://www.cisco.com/c/en/us/about/legal/privacy-full.html#cookies

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CITAQ

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.citaqpos.com/index.php/technical_support/technical_support.html

https://www.citaqpos.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CITIZEN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.citizenwatch.com/mx/es/terminos-condiciones.html

https://www.citizenwatch.com/mx/es/home/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CLARION

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.clarion.com/xl/es/usage/

https://www.faurecia-clarion.com/legal-notice

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

COLORLIGHT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://en.colorlightinside.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

COMERCIAL ELECTRIC

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CONCOX (SIN MARCA)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.iconcox.com/about/privacy.html

https://www.iconcox.com/about/cookiess.html

https://www.iconcox.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CRADLEPOINT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://cradlepoint.com/

https://cradlepoint.com/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CTEK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://cdn.shopify.com/s/files/1/0117/5237/4372/files/CTEK-Privacy-Policy-01.25.2019.pdf?14599092788908898462

https://cdn.shopify.com/s/files/1/0117/5237/4372/files/CTEK_Terms_of_Service.pdf?4453098566109398991

https://www.ctek.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

CURRENT

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DACE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.daceap.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DAHUA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.dhmex.com/marketplace/homes/Default.aspx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DATALOGIC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.datalogic.com/eng/index.html

https://www.datalogic.com/eng/legal-notice-pa-92.html

https://www.datalogic.com/eng/privacy-policy-pa-112.html

https://www.datalogic.com/eng/terms-and-conditions-pa-93.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DEFINITIVE TECHNOLOGY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.definitivetechnology.com/en-us/support/terms-and-conditions

https://www.definitivetechnology.com/en-us/support/privacy-policy

https://www.definitivetechnology.com/en-us/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DELL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.dell.com/es-mx/dt/services/index.htm

https://www.dell.com/learn/mx/es/mxcorp1/policies-privacy

https://www.dell.com/learn/mx/es/mxcorp1/terms-of-sale

https://www.dell.com/learn/mx/es/mxcorp1/policies-cookies-ads-emails

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DENON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.denon.com/es-es/our-vision/denon-privacy-policy

https://www.denon.com/es-es

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DENSAY SV

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://en.desaysv.com/index.php?id=law

https://en.desaysv.com/index.php

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DIESEL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.diesel.com/es/help-show?content=termsSale

https://es.diesel.com/es/help-show?content=terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DIGI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.digi.com/legal/privacy

https://es.digi.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DIGITAL SECURITY

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DJI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.dji.com/mx/policy?site=brandsite&from=footer

https://www.dji.com/mx/terms?site=brandsite&from=footer

https://www.dji.com/mx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DOJO SAN 990

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DOTS (OUI FI)

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DRAGON TOUCH

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DRAY TEK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.draytek.com/policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DREAMTECH

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DS18

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:
https://ds18.com/policies/privacy-policy

https://ds18.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DSC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.dsc.com/

https://www.johnsoncontrols.com/privacy-center

https://www.johnsoncontrols.com/legal/terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DSDEVICES

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://dsdevices.com/privacy-policy/

https://dsdevices.com/terms-of-use/

https://dsdevices.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DSPREAD

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://dsdevices.com/privacy-policy/

https://dsdevices.com/terms-of-use/

https://dsdevices.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DTRESEARCH

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.dtresearch.com/index.html

https://www.dtresearch.com/en/Support/legal.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DYSON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://privacy.dyson.com/es-xl/politica-global-de-privacidad.aspx

https://www.dyson.com.mx/footer-secondary-links/terms-and-conditions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

DZEES

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://dzees.com/policies/privacy-policy

https://dzees.com/pages/terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ECOM

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EDIMAX

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.edimax.com/edimax/post/post/data/edimax/global/privacy_policy/

https://www.edimax.com/edimax/global/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EERO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://eero.com/legal/privacy

https://eero.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ENGENIUS (TECH INC.)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.engeniustech.com/privacy-policy.html#

https://www.engeniustech.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ENGENIUS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:
https://www.engeniustech.com/privacy-policy.html#
https://www.engeniustech.com/

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EPCOM

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EPSON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://epson.com.mx/politica-de-privacidad

https://epson.com.mx/aviso-de-privacidad-m%C3%A9xico

https://epson.com.mx/terminos-de-uso

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EVELAB INSIGHT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://evelabinsight.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EVL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.evl.mx/

https://www.evl.mx/evl-aviso-de-privacidad

https://www.evl.mx/terminos-y-condiciones

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EVL PRO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.evl.mx/

https://www.evl.mx/evl-aviso-de-privacidad

https://www.evl.mx/terminos-y-condiciones

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EXPLORE ONE

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EXTREME NETWORKS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.extremenetworks.com/about-extreme-networks/company/legal/privacy-and-cookies-policy

https://www.extremenetworks.com/#sortCriteria=%40computedpublisheddate%20descending&aq=%40contenttypetitle%3D%22(Press%20Release)%22

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

EZVIZ

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:
https://www.ezviz.com/la/legal/privacy-policy

https://www.ezviz.com/la/legal/terms-of-service

https://www.ezviz.com/la/legal

https://www.ezviz.com/la

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FANVIL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://fanvil.com/partners/mappolicy.html

https://fanvil.com/service/doc/index.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FEIT ELECTRIC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.feit.com/pages/privacy-policy

https://www.feit.com/pages/terms_and_conditions

https://help.feit.com/hc/en-us

https://help.feit.com/hc/en-us/articles/18441583923479-How-to-Reset-the-Account-Password-for-the-Feit-Electric-App

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FENDER

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FIBERHOME

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FINDER

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.findernet.com/es/mexico/soporte/

https://www.findernet.com/es/mexico/soporte/software-y-app/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FITBIT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://storage.googleapis.com/support-kms-prod/rMYHmnx8YY7iOsOy4gClinqNnvPxY8joobW8

https://storage.googleapis.com/support-kms-prod/ns01NgUvlsLYfZtsKLipHdLd2hqspIf1OVGv

https://help.fitbit.com

https://support.google.com/product-documentation/answer/13511576?hl=es-419&ref_topic=13510581&sjid=6894539592402939496-NC

https://www.fitbit.com/global/es/legal/supplierterms/vendor-security-measures

https://help.fitbit.com/articles/es/Help_article/1392.htm

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FLUKE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.fluke.com/es-mx/fluke/politica-de-privacidad

https://www.flukeprocessinstruments.com/es/search/node/telemetria

https://www.fluke.com/es-mx/soporte/descargas-de-software

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FORTINET

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.fortinet.com/lat/corporate/about-us/privacy

https://www.fortinet.com/lat/corporate/about-us/legal

https://www.fortinet.com/lat/solutions/enterprise-midsize-business/application-security

https://www.fortinet.com/lat/resources/cyberglossary/network-security

https://www.fortinet.com/lat/products/endpoint-security/forticlient

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FOSSIL

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FUJIFILM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.fujifilm.com/mx/es/privacy

https://www.fujifilm.com/mx/es/term

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FUJITSU

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.fujitsu.com/global/about/resources/privacy/

https://www.fujitsu.com/global/about/resources/terms/

https://www.fujitsu.com/ru/imagesgig5/c120-0065-02es.pdf

https://support.ts.fujitsu.com/IndexDownload.asp?lng=ES

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FURBO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://furbo.com/mx/pages/privacy-policy

https://furbo.com/mx/pages/terms-conditions

https://help.furbo.com/hc/en-us/articles/17472804287641-How-to-Update-Furbo-Firmware

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

FUSION

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.garmin.com/es-MX/c/marine/fusion-audio-entertainment/

https://www.garmin.com/es-MX/privacy/global/policy/#retenci%C3%B3NDeDatosPersonales

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GARMIN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.garmin.com/es-MX/privacy/global/policy/#retenci%C3%B3NDeDatosPersonales

https://www.garmin.com/es-MX/privacy/global/policy/#retenci%C3%B3NDeDatosPersonales

https://www.garmin.com/es-MX/legal/security/

https://support.garmin.com/es-MX/?faq=uGHS8ZqOIhA0usBzBMdJu7

https://www.garmin.com/es-CL/legal/security/

https://www.garmin.com/es-MX/software/express/windows/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GELCSMART

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GENIUSPY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.geniuspycam.com/policies/privacy-policy

https://www.geniuspycam.com/policies/terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GETAC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.getac.com/latam/

https://www.getac.com/latam/privacy-policy/

https://www.getac.com/latam/terms-of-use/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GHIA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ghia.com.mx/soporte-tecnico/

https://www.grupocva.com/aviso-privacidad.php

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GL INET

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.gl-inet.com/privacy-policy/

https://www.gl-inet.com/terms-of-service/

https://www.gl-inet.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GOOGLE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://policies.google.com/privacy?hl=es

https://policies.google.com/terms?hl=es

https://safety.google/intl/es/principles/

https://safety.google/intl/es/cybersecurity-advancements/

https://cloud.google.com/learn/what-is-opentelemetry?hl=es-419

https://safety.google/intl/es-419/authentication/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GOPRO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://gopro.mx/pages/politicas-de-privacidad

https://community.gopro.com/s/?language=en_US

https://gopro.mx/policies/terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GRANDSTREAM (SUBMARCA: SIN MARCA)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.grandstream.com/privacy-statement

https://www.grandstream.com/support

https://www.grandstream.com/products/networking-solutions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GRANDSTREAM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.grandstream.com/privacy-statement

https://www.grandstream.com/support

https://www.grandstream.com/products/networking-solutions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GUEST INTERNET HOTSPOT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.guest-internet.com/ES/index_es.php

https://www.guest-internet.com/guest_internet_hotspot_privacy_policy.php

https://www.guest-internet.com/guest_internet_hotspot_terms_and_conditions.php

https://www.guest-internet.com/index.php

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

GUEST INTERNET SOLUTIONS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.guest-internet.com/ES/index_es.php

https://www.guest-internet.com/guest_internet_hotspot_privacy_policy.php

https://www.guest-internet.com/guest_internet_hotspot_terms_and_conditions.php

https://www.guest-internet.com/index.php

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HARMAN KARDON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.harman.com/privacy-policy-statement-es-mx

https://www.harmankardon.com.mx/terms-of-use.html

https://support.harmankardon.com/mx/es/#support-products?basketContents=&basketUrl=https://www.harmankardon.com.mx/cart

https://www.harmankardon.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HIKIVISIÓN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hikvision.com/es-la/

https://www.hikvision.com/es-la/policies/privacy-policy/

https://www.hikvision.com/es-la/policies/general-terms-of-use/

https://www.hikvision.com/es-la/about-us/cybersecurity/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HILOOK (HIKVISION)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hikvision.com/es-la/

https://www.hikvision.com/es-la/policies/privacy-policy/

https://www.hikvision.com/es-la/policies/general-terms-of-use/

https://www.hikvision.com/es-la/about-us/cybersecurity/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HILOOK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hikvision.com/es-la/

https://www.hikvision.com/es-la/policies/privacy-policy/

https://www.hikvision.com/es-la/policies/general-terms-of-use/

https://www.hikvision.com/es-la/about-us/cybersecurity/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HISENSE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://hisense.com.mx/terminos

https://hisense.com.mx/privacidad

https://hisense.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HITRON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hitrontech.com/

https://www.hitrontech.com/legal/privacy-policy/

https://www.hitrontech.com/legal/terms-of-use/

https://www.hitrontech.com/service/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HKPRO

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HOMESYS

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HONEYWELL HOME

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.honeywell.com/mx/es

https://www.honeywell.com/us/en/privacy-statement#spanish

https://www.honeywell.com/us/en/terms-and-conditions

https://www.honeywell.com/us/en/contact/support

https://www.honeywellhome.com/us/en

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HONEYWELL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.honeywell.com/mx/es

https://www.honeywell.com/us/en/privacy-statement#spanish

https://www.honeywell.com/us/en/terms-and-conditions

https://www.honeywell.com/us/en/contact/support

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HP

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://support.hp.com/mx-es

https://www.hp.com/mx-es/privacy/privacy-central.html

https://www.hp.com/mx-es/terms-of-use.html

https://www.hp.com/mx-es/home.html

https://www.hppstelemetry.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HUAWEI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://support.huawei.com/enterprise/mx/doc/EDOC1000173015/3ea8d77c/telemetry-configuration

https://e.huawei.com/mx/

https://www.huawei.com/mx/privacy-policy

https://www.huawei.com/mx/legal

https://www.huawei.com/mx/contact-us

https://consumer.huawei.com/mx/

https://consumer.huawei.com/mx/support/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HUBBLE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://hubblenetwork.com/privacy-policy

https://hubblenetwork.com/terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HUBITAT ELEVATION

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://hubitat.com/

https://docs2.hubitat.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HUBLOT

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HYTERA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hytera.com/la/product-new/radio-de-comunicacion.html?utm_term=hytera&utm_campaign=MX+_GA+_RADIOS&utm_source=adwords&utm_medium=ppc&hsa_acc=6331949623&hsa_cam=12912825736&hsa_grp=122042138575&hsa_ad=518327665129&hsa_src=g&hsa_tgt=kwd-24925498139&hsa_kw=hytera&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAiAkp6tBhB5EiwANTCx1KyBfksM9k646NTMz1CB13mpJHqXJPuDXaRhbqhgwyX5oXqIXCexVhoCNj0QAvD_BwE

https://www.hytera.com/la/privacy.html

https://www.hytera.com/la/about-hytera/contact-us.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

HYUNDAI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hyundaielectronics.com.mx/es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ICOM AMERICA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.icomamerica.com/

https://www.icomamerica.com/company/privacy_policy/

https://www.icomamerica.com/company/terms/

https://www.icomamerica.com/support/

https://www.icomamerica.com/support/firmware_driver/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

IMOU

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.imoulife.com/na

https://www.imoulife.com/na/policy#privacy-policy

https://www.imoulife.com/na/policy#terms-of-use

https://www.imoulife.com/na/imou-protect

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

INBODY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.inbodymexico.com/preguntas-frecuentes/#descargas

https://www.inbodymexico.com/preguntas-frecuentes/#soporteinb

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

INGENICO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://ingenico.com/es/notas-legales

https://ingenico.com/es/necesita-ayuda

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

INSTA360

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.insta360.com/es/support/supportcourse?post_id=20166&_gl=1*13b3wgk*_ga*NDg3MTM4NDI5LjE3MDU5NDMxMzc.*_ga_46QD011RHK*MTcwNTk0MzEzNy4xLjEuMTcwNTk0MzE1MS40Ni4wLjA.&_ga=2.111856647.280578307.1705943137-487138429.1705943137

https://www.insta360.com/es/support/supportcourse?post_id=9146&_gl=1*u2xq2m*_ga*NDg3MTM4NDI5LjE3MDU5NDMxMzc.*_ga_46QD011RHK*MTcwNTk0MzEzNy4xLjEuMTcwNTk0MzE2OC4yOS4wLjA.&_ga=2.23766329.280578307.1705943137-487138429.1705943137

https://store.insta360.com/?utm_term=INRBZDI

https://www.insta360.com/es/support/workorder?_ga=2.23766329.280578307.1705943137-487138429.1705943137&_gl=1%2A2ex958%2A_ga%2ANDg3MTM4NDI5LjE3MDU5NDMxMzc.%2A_ga_46QD011RHK%2AMTcwNTk0MzEzNy4xLjEuMTcwNTk0MzE4OC45LjAuMA.

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

INTEL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.intel.la/content/www/xl/es/homepage.html

https://www.intel.la/content/www/xl/es/privacy/intel-privacy-notice.html

https://www.intel.la/content/www/xl/es/legal/terms-of-use.html

https://www.intel.la/content/www/xl/es/support/detect.html

https://www.intel.la/content/www/xl/es/collections/services/platform-telemetry-and-insights.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

IO MABE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.iomabe.com.mx/

https://www.iomabe.com.mx/preguntas-seguridad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

IONVAC

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

IROBOT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.irobotshop.mx/terminos-y-condiciones

https://www.irobot.lat/irobot-home-app

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ITALKPTT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.italkpttlatam.com/politica-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

IVIEW

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

FUENTE:

https://iviewus.com/pages/support

https://www.informatec.com/en/legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

JABRA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.jabra.lat/footerpages/disclaimer#:~:text=Jabra%20no%20recopila%20intencionadamente%20datos,o%20sorteos%20patrocinados%20por%20Jabra.

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

JANAM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	NO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.janam.com/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

JBL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.jbl.com.mx/privacy_policy.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

JIMI IOT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.jimilab.com/about/privacy.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

JVC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.jvc.com/compania/privacidad/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

KOBO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://authorize.kobo.com/terms/privacypolicy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

KOCOM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.syscom.mx/principal/aviso-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

KODAK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://kodakmoments.kodakalaris.com/mob/privacy.aspx?language=es

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

KONFTEL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.konftel.com/es/privacy-statement

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

KYOCERA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.kyoceradocumentsolutions.mx/es/footer/privacy-and-cookies/online-privacy-statement.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LANIX

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://store.lanix.com/pages/aviso-de-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LAXIHUB

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	NO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://laxihub.com/pages/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LEICA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://leica-camera.com/es-MX/data-protection

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LENOVO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.lenovo.com/mx/es/privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LEVITON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.leviton.com/es/politica-de-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LEXMARK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.lexmark.com/es_mx/aviso-de-privacidad.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LG ELECTRONICS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.lg.com/mx/privacy

www.lg.com/mx/soporte/email

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LIGOWAVE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ligowave.com/terms-and-conditions#privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LINKSYS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.linksys.com/mx/documentation.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LLOYD'S

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	NO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://lloydscorp.com/politica-de-privacidad/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LOGITECH

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.logitech.com/es-mx/legal/product-privacy-policy.html#controlling-and-accessing-information

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LOREX

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://mx.lorex.com/policies/privacy-policy

https://mx.lorex.com/pages/compromiso-de-privacidad

https://mx.lorex.com/pages/compromiso-de-seguridad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

LOUIS VUITTON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATOS
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATOS
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATOS
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATOS
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATOS
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATOS
IV. Integridad del software. Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATOS
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATOS
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATOS

FUENTE:

https://la.louisvuitton.com/esp-mx/avisos-legales

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MAKENA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	NO
Permite el uso de medios de autenticación de múltiples factores.	NO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	NO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	NO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	NO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	NO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	NO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	NO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	NO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	NO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	NO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	NO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	NO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	NO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	NO

FUENTE:

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MAKITA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATOS
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATOS
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATOS
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATOS
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATOS
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATOS
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATOS

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATOS
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.makita.com.mx/aviso-de-privacidad-makita-mexico/

https://www.makita.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MARANTZ

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATOS
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATOS
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATOS
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATOS
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATOS

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATOS
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.marantz.com/es-es/support/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MARSHALL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATOS
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATOS
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATOS
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATOS
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATOS
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATOS
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATOS

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATOS
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.marantz.com/es-es/support/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MARVELL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.marvell.com/privacy-statement.html

https://www.marvell.com/terms-of-use.html

https://www.marvell.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MASTERBUILT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.masterbuilt.com/pages/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MATTERPORT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://matterport.com/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MERAKI (CISCO, CISCO SYSTEMS, INC.)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.cisco.com/c/es_es/about/legal/privacy-full.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MERAKI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.cisco.com/c/es_es/about/legal/privacy-full.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MERCADO PAGO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.mercadopago.com.mx/privacidad#start

https://www.mercadopago.com.mx/privacidad/declaracion-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MERCUSYS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	NO
Permite el uso de medios de autenticación de múltiples factores.	NO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	NO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	NO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	NO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	NO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	NO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	NO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	NO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	NO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	NO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	NO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	NO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	NO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	NO

FUENTE:

https://www.mercusys.com.mx/about-us

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MERIK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.merik.com/terminos-y-condiciones

https://www.merik.com/aviso-de-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MI (XIAOMI)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.mi.com/mx/support/terms/terms-of-use/

https://www.mi.com/mx/about/privacy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MICHAEL KORS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.michaelkors.com/info/privacy-notice.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MICROSOFT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://privacy.microsoft.com/es-mx/privacystatement

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MIKROTIK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://mikrotik.com/privacy

https://mikrotik.com/support

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MIRATI HOME

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	NO
Permite el uso de medios de autenticación de múltiples factores.	NO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	NO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	NO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	NO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	NO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	NO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	NO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	NO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	NO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	NO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	NO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	NO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	NO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	NO

FUENTE:

https://miratihome.com/#

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MIURA (MIURA SYSTEMS)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATOS
Permite el uso de medios de autenticación de múltiples factores.	SIN DATOS
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATOS
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATOS
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATOS
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATOS
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATOS
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATOS

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATOS
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://miuraboiler.mx/aviso-privacidad.pdf

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ML(XIAOMI)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATOS
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATOS
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATOS
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.mi.com/mx/about/privacy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MONOGRAM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATOS
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATOS
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATOS

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATOS
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://monogram.com.mx/Privacidad.aspx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MONTBLANC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATOS
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATOS
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATOS
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.montblanc.com.mx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MOTOROLA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.motorola.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

MULTITECH

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATOS
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.multitech.com/legal/legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NANOLEAF

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://nanoleaf.me/es-MX/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NESPRESSO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.nespresso.com/mx/es/legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NETALLY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.netally.com/privacy/

https://www.netally.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NETATMO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	NO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://legals.netatmo.com/?gsc=true&goto=legal-mentions

https://legals.netatmo.com/?gsc=true&goto=legal-mentions#element2

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NETGEAR

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.netgear.com/es/about/ad-cookie-policy/

https://www.netgear.com/es/about/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NETIO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.netio.com.ar/index.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NETZHOME

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://netzhome.com.mx/aviso-de-privacidad/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NEWLAND

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.newland-id.com/es/privacy-policy

https://www.newland-id.com/es/terms-and-conditions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NEXXT SOLUTIONS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.nexxtsolutions.com/es/infraestructura/soporte/privacidad/

https://www.nexxtsolutions.com/es/conectividad/soporte/privacidad/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NEXXT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.nexxtsolutions.com/es/infraestructura/soporte/privacidad/

https://www.nexxtsolutions.com/es/conectividad/soporte/privacidad/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NIKON

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.nikon.com.mx/about-nikon/privacy-policy.page

https://www.nikon.com.mx/about-nikon/terms-of-use.page

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NILE GLOBAL Inc

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://nilesecure.com/company/privacy-policy/

https://nilesecure.com/company/security-and-compliance/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NINTENDO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es-americas-support.nintendo.com/app/products/detail/p/989?fbclid=IwAR09his7iKwIpWetu_8rUrXZb4pdiMzeXr0Rra_QZ6O1q0w3dn9Qcj3OPKE

https://es-americas-support.nintendo.com/app/answers/detail/a_id/50798/?_gl=1*1ypnwve*_ga*MTc3Mzg0OTI4Ny4xNzA2MDM3MTEw*_ga_F6ERC4HMNZ*MTcwNjAzNzExMC4xLjEuMTcwNjAzODE5Ny4wLjAuMA&fbclid=IwAR2HQUkyOeilNJ-htNCiOawS3qZozuvURim8s3IePPgEVsjqMl9kbd5L4e4

https://www.nintendo.com/es-mx/privacy-policy/?_gl=1*2rtbl3*_ga*MTc3Mzg0OTI4Ny4xNzA2MDM3MTEw*_ga_F6ERC4HMNZ*MTcwNjAzNzExMC4xLjEuMTcwNjAzODIwNy4wLjAuMA&fbclid=IwAR1_nIetIwPk9LVzTfNV4z0tmle-vBoZQMOSI_O_fC7kOtF1w8N374MVXmU

https://www.nintendo.com/es-mx/?fbclid=IwAR2-bTuqBnpQ4RuPZ8tDKulSbmIT6qQ4IGsaV9JJXo6Qdnv23bTcqO4_ETY

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NLT DIGITAL SOLUTIONS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	NO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.nltdigital.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

NOKIA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	NO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.nokia.com/privacy/

https://www.nokia.com/notices/terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

OCULUS

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

OLYMPUS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	NO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.olympus-global.com/privacy/

https://www.olympus-global.com/products/terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

OMNITRACS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.omnitracs.com/es/node/906

https://www.omnitracs.com/es/node/921

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ONN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	NO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://onntvsupport.com/privacy-policy

https://onntvsupport.com/terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

OPPO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.oppo.com/mx/privacy/

https://www.oppo.com/mx/terms/

https://www.oppo.com/en/legal/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

OPSWAT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.opswat.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ORBIT B-HYVE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.orbitonline.com/policies/privacy-policy

https://www.orbitonline.com/pages/terms-of-use

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

OWL LABS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://owllabs.com/security

https://owllabs.com/privacy-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PACKARD BELL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://packard-bell.co.za/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PANASONIC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.panasonic.com/mx/privacy-policy.html

https://www.panasonic.com/mx/terms-of-use.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PANDUIT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.panduit.com/latam/es/legal-information/panduit-privacy-policy.html

https://www.panduit.com/latam/es/legal-information.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PENTIUM (INTEL PENTIUM)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.intel.la/content/www/xl/es/privacy/intel-privacy-notice.html

https://www.intel.la/content/www/xl/es/legal/terms-of-use.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PHILIPS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.philips.com.mx/a-w/aviso-de-privacidad.html

https://www.philips.com.mx/a-w/condiciones-de-uso.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PHOENIX CONTACT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.phoenixcontact.com/es-mx/terminos-y-condiciones/data-privacy

https://www.phoenixcontact.com/es-mx/terminos-y-condiciones

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PIONEER

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.pioneer-mexico.com.mx/aviso-de-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

POLAR

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.polar.com/mx-es/legal/privacy-notice

https://www.polar.com/mx-es/legal/terms-of-use

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

POLK AUDIO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.polkaudio.com/privacy-policy

https://es.polkaudio.com/terms-conditions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

POLK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.polkaudio.com/privacy-policy

https://es.polkaudio.com/terms-conditions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

POLY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hp.com/mx-es/privacy/privacy-central.html?_gl=1*14g22gj*_gcl_au*MTM1ODY3Nzg0Ny4xNzAyNTY0ODY2

https://www.poly.com/mx/es/legal/terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

POLYCOM (POLY)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hp.com/mx-es/privacy/privacy-central.html?_gl=1*1p38jm5*_gcl_au*MTI1NjUwOTc5OC4xNzAzNzI2NzQ4

https://www.hp.com/mx-es/terms-of-use.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

POLYCOM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.hp.com/mx-es/privacy/privacy-central.html?_gl=1*1p38jm5*_gcl_au*MTI1NjUwOTc5OC4xNzAzNzI2NzQ4

https://www.hp.com/mx-es/terms-of-use.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PROFORM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.proform.com/privacy

https://www.proform.com/terms-of-use

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

PROSOFT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://mx.prosoft-technology.com/ProSoft-Technology-Legal-Terms-and-Conditions#privacypolicy

https://mx.prosoft-technology.com/ProSoft-Technology-Legal-Terms-and-Conditions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

QOLSYS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.johnsoncontrols.com/privacy-center

https://www.johnsoncontrols.com/legal/terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

QUAMTUM CONNECTIVITY DE MÉXICO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	NO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://quamtumconnectivity.com/politicas-de-privacidad/

https://quamtumconnectivity.com/politica-de-uso/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

QUANTUM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.quantum.com/es/quantum-corporation-privacy-policy/

https://www.quantum.com/es/terms-of-use/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

QUARONI (CVA)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	NO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.grupocva.com/aviso-privacidad.php

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RADIOSHACK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.radioshack.com.mx/store/radioshack/en/PoliticasDePrivacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RAKUTEN KOBO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://authorize.kobo.com/terms/privacypolicy

https://authorize.kobo.com/terms/termsofuse

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RALEJ

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RCA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://rca-mex.com/pages/aviso-de-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

REALME

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.realme.com/mx/legal/privacy-policy

https://www.realme.com/mx/legal/user-agreement

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

REALTEK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	NO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	NO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.realtek.com/en/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RED DIGITAL CINEMA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.red.com/legal

https://www.red.com/contact-us

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RED

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SIN DATO
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://es.red.org/privacy-policy

https://es.red.org/terms-privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

REMARKABLE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://support.remarkable.com/s/legal

https://support.remarkable.com/s/article/Vulnerability-Disclosure-Policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RICOH

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ricoh-americalatina.com/es/productos/pd/software/control-y-recuperaci%C3%B3n-de-costos/ricoh-streamline-nx-v3

https://www.ricoh-americalatina.com/es/productos/pd/software/configuraci%C3%B3n-y-administraci%C3%B3n-del-equipo/ricoh-device-manager-nx-lite

https://www.ricoh-americalatina.com/es/acerca-de-ricoh/politica-de-privacidad

https://www.ricoh-americalatina.com/es/acerca-de-ricoh/t%C3%A9rminos-de-uso

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RING

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es-es.ring.com/pages/terms

https://es-es.ring.com/pages/privacy-notice

https://support.ring.com/hc/es/articles/360022109431-Upgrading-Changing-or-Canceling-your-Ring-Protect-Plan

https://support.ring.com/hc/es/articles/14856637902868

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ROCKET HOUSE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://rockethouse.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ROKU

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://docs.roku.com/published/deviceplayereula/es/mx

https://docs.roku.com/published/therokuchannel-userstermsandconditions/en/us

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RUCKUS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://support.ruckuswireless.com/TOS

https://es.commscope.com/about-us/terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RUGGEAR

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.ruggear.com/es/terms-and-conditions.html

https://www.ruggear.com/es/privacy-policy.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

RUIJIE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://latam.ruijienetworks.com/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SAMSUNG

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.samsung.com/mx/info/terms-and-conditions/

https://www.samsung.com/mx/info/privacy/

https://www.samsung.com/mx/sustainability/security-and-privacy/security/

https://securityreport.samsung.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SANYO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	NO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sanyo-av.mx/support/privacy.php

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SATO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.satoeurope.com/es/pdf/sato-privacy-policy.pdf

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SAWGRASS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	NO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	NO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://sawgrassexchange.sawgrassink.com/legal/privacy-policy

https://sawgrassexchange.sawgrassink.com/legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SCREENBEAM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.screenbeam.com/es/about/terms-of-use/

https://www.screenbeam.com/es/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SEEED

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.seeedstudio.com/privacy_policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SEMEQ

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://semeq.com/en/home-en/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SENNHEISER

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	NO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es-mx.sennheiser.com/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SHARP

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sharp.com.mx/assets/aviso_de_privacidad.pdf

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SIEMENS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.siemens.com/global/en/company/about/compliance/reporting-channels.html

https://www.siemens.com/global/en/general/privacy-notice.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SIERRA WIRELESS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.semtech.com/legal

https://www.sierrawireless.com/privacy/

https://www.sierrawireless.com/legal/terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SKF

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.skf.com/mx/footer/privacy-policy

https://www.skf.com/mx/footer/terms-and-conditions

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SKYBELL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://skybell.com/pages/skybell-privacy-policy

https://skybell.com/pages/skybell-terms-of-service

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SMART TOYS & CANDY CO.

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.smarttoysandcandy.com/aviso-privacidad-smart-toys.pdf

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SOMFY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.somfy.mx/asistencia/terminos-y-condiciones

https://www.somfy.mx/privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SONICWALL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sonicwall.com/legal/privacy-statement/

https://www.sonicwall.com/legal/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SONOS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sonos.com/es-mx/legal

https://www.sonos.com/es-mx/legal/privacy

https://www.sonos.com/es-mx/security

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SONY

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sony.com.mx/corporate/MX/legal/avisodeprivacidad.html

https://www.sony.com.mx/corporate/MX/legal/derechosreservados.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SOPHOS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sophos.com/es-es/legal/sophos-group-privacy-notice

https://www.sophos.com/es-es/legal/sophos-end-user-terms-of-use

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SPECTRA

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SPORTLINE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.sportline.mx/sl-terminos-y-condiciones

https://www.sportline.mx/sl-aviso-de-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SQUARE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://squareup.com/us/en/sales/contact?page=/us/en/security

https://squareup.com/us/en/legal/general/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

STEAM DECK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.steamdeck.com/es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

STEELSERIES

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://mx.steelseries.com/policies/privacy

https://mx.steelseries.com/policies/terms

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

STEREN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.steren.com.mx/aviso-privacidad

https://www.steren.com.mx/politica-de-privacidad-steren-app

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

STF

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.stf.tech/pages/aviso-de-privacidad

https://www.stf.tech/pages/terminos-y-condiciones

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SUNGROW

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://mx.sungrowpower.com/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SUNMI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.sunmi.com/es/data-privacy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SUPREMA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.supremainc.com/es/util/privacy-policy.asp

https://www.supremainc.com/es/util/legal-notice.asp

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SURFSIGHT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://surfsight.com/privacy

https://surfsight.com/eula

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SUUNTO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.suunto.com/Privacy-Policy/

https://www.suunto.com/Terms-of-use/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SWANN

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://us.swann.com/privacy-policy/

https://us.swann.com/company/terms-of-use/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

SYSTEM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://tdsystems.es/politica-de-privacidad

https://tdsystems.es/aviso-legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

T2GO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://train2go.com/legal/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TAG HEUER

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.tagheuer.com/mx/es/legal/privacy-policy.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TAPO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.tp-link.com/mx/support/replacement-warranty/

https://www.tp-link.com/mx/about-us/privacy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TCL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.tcl.com/mx/es/legal/privacy-notice

https://www.tcl.com/mx/es/security

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TEAMVOX

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://redbooth.com/security

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TECHZONE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://techzone.com.mx/pages/politicas-privacidad

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TECNOLITE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://tecnolite.mx/aviso-de-privacidad

https://tecnolite.mx/terminos-y-condiciones

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TEKA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SI

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SI
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.teka.com/es-mx/aviso-legal/

https://www.teka.com/es-mx/aviso-de-privacidad/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TELOSYSTEMS

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TELTONIKA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://teltonika-networks.com/es/about-us/policies-certificates/privacy-policy

teltonika-networks.com

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TENDA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.tendacn.com/mx/service/page/Privacy.html

https://www.tendacn.com/mx/default.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

THE SINGING MACHINE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://singingmachine.com/pages/privacy-policy

https://singingmachine.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TIVO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://tivo.pactsafe.io/legal.html#privacy-policy

https://www.tivo.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TJD

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.tjdlatam.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TOPFLYtech

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.topflytech.com/home-page

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TOSHIBA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.toshiba.com.mx/contact.html

https://www.global.toshiba/ww/privacy/corporate.html

https://www.global.toshiba/ww/terms/corporate.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TOUS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.tous.com/mx-es/policies/privacy-policy

https://www.tous.com/mx-es/policies/terms-and-conditions

https://www.tous.com/mx-es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TOYOTA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.toyota.mx/politica-de-privacidad

https://www.toyota.mx/

https://www.toyota.mx/terminos-y-condiciones

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TP-LINK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.tp-link.com/mx/about-us/privacy/

https://www.tp-link.com/mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TRENDNET

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.trendnet.com/langsp/company/?company=privacy_policy

https://www.trendnet.com/langsp/home

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TRIMBLE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center/privacy-notice

https://www.trimble.com/en

https://www.trimble.com/en/legal

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TSC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://latam.tscprinters.com/es/declaracion-de-privacidad

https://latam.tscprinters.com/es

https://latam.tscprinters.com/es/terminos-y-condiciones-del-servicio

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

TXPRO

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UBIQUITI INC. (UNIFI)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ui.com/legal/privacypolicy/

https://www.ui.com/introduction

https://www.ui.com/legal/services-terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UBIQUITI NETWORKS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://u-networks.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UBIQUITI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ui.com/legal/privacypolicy/

https://www.ui.com/introduction

https://www.ui.com/legal/services-terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UBITIQUI INC. (UI.COM, UNIFI)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SI
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ui.com/legal/privacypolicy/

https://www.ui.com/introduction

https://www.ui.com/legal/services-terms/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UNITECH

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ute.com/en

https://www.ute.com/en/terms

https://www.ute.com/en/privacy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UROVO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://es.urovo.com/Index/privacy.html

https://es.urovo.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

UTEPO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SIN DATO
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.utepo.net/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VERIFONE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SI
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SI
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.verifone.com/en/global/legal/privacy-policy

https://verifone.cloud/terms-of-use

https://www.verifone.com/es/mx

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VERKADA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.verkada.com/es/privacy/

https://www.verkada.com/es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

INSTITUTO FEDERAL DE TELECOMUNICACIONES

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VIASAT

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones al Software Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el Uso de Comunicaciones Seguras Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del Software Se menciona que:	

Utiliza un módulo de seguridad en el "hardware".	SI
En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SI
V. Sobre los Datos de Telemetría	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SI
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI

Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI
III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.viasat.com/es-mx/privacidad/

https://www.viasat.com/es-mx/

https://www.viasat.com/content/dam/mx-site/documents/TandCS_MyViasat_11102021.pdf

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VIEW SONIC

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.viewsonic.com/terms-of-use

https://www.viewsonic.com/us/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VIMAR

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.vimar.com/es/int/smart-home-automatizacion-aparatos-electricos-vimar-energia-posi-9904122.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VIOS

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VIVITAR

Nota: No se encontró información relacionada con las características de ciberseguridad de esta marca.

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VOLTEDGE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SIN DATO
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SIN DATO
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SIN DATO
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SIN DATO
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SIN DATO
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SIN DATO
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SIN DATO

FUENTE:

https://www.voltedge.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

VORWERK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SIN DATO
Permite revocar el consentimiento para el uso de los datos personales.	SIN DATO
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SIN DATO

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.vorwerk.com/es/es/c/home/general/politica-privacidad

https://www.vorwerk.com/es/es/c/home

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WATCHWARD

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.watchguard.com/es/wgrd-trust-center/terms-of-use

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WEMO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.belkin.com/products/wemo-smart-home/

https://www.belkin.com/legal/privacy-policy/

https://www.belkin.com/legal/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WESTINGHOUSE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://whouse.com.mx/pages/aviso-de-privacidad

https://whouse.com.mx/pages/terminos-y-condiciones

https://whouse.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WINIX

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://winixes.es/politica-de-privacidad.html

https://winixes.es/terminos-y-condiciones-de-uso.html

https://winixes.es/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WINMATE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.winmate.com/Corporate/AboutPrivacyPolicy

https://www.winmate.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WITHINGS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SI
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.withings.com/us/es/data-security

https://www.withings.com/us/es/legal/legal-notice

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WYZE CAM

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.wyze.com/policies/privacy-policy

https://www.wyze.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

WYZE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SIN DATO
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SIN DATO

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.wyze.com/policies/privacy-policy

https://www.wyze.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

XIAOMI

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SI
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SI
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SI
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.mi.com/mx/about/privacy/

https://www.mi.com/mx/support/terms/terms-of-use

https://www.mi.com/mx/support/policy/cookie-policy

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

XIRRUS (XIRRUS WIFI NETWORKS)

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.cambiumnetworks.com/support/security/

https://www.cambiumnetworks.com/eol/

https://www.cambiumnetworks.com/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

XIRRUS

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.cambiumnetworks.com/support/security/

https://www.cambiumnetworks.com/eol/

https://www.cambiumnetworks.com/privacy-policy/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

YALE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.yalehome.com.mx/es/aviso-de-privacidad

https://www.yalehome.com.mx/es/aviso-de-privacidad/legal

https://www.yalehome.com.mx/es/contacto

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

YAMAHA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.yamaha.com/en/privacy_policy/

https://www.yamaha.com/en/terms_of_use/

https://www.yamaha.com/en/?header

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

YEAHLINK

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.yealink.com/en/onepage/privacy-statement

https://www.yealink.com/en

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ZEBRA

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://hackerone.com/zebra_vdp?type=team

https://www.zebra.com/la/es/about-zebra/company-information/legal.html

https://www.zebra.com/la/es/about-zebra/company-information/legal/privacy-statement.html

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ZKTECO

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://docs.zktecolatinoamerica.com/compania/Politica-de-Privacidad-ZKTeco-LATAM.pdf

https://docs.zktecolatinoamerica.com/legal/avisos-legales-zkteco.pdf

https://zktecolatinoamerica.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ZMARTECH

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.zmartech.com.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ZTE

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.ztedevices.mx/aviso-de-privacidad-2/

https://www.ztedevices.mx/soporte/

https://www.ztedevices.mx/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

CÓDIGO DE MEJORES PRÁCTICAS PARA LA CIBERSEGURIDAD DE LOS DISPOSITIVOS DEL INTERNET DE LAS COSAS (IOT)

Aquí podrás conocer algunas características de ciberseguridad de la marca:

ZUMIMALL

Nota: Es importante mencionar que la información que se refleja en el documento fue recolectada en los sitios de internet del fabricante y no deberá tomarse como una valoración, juicio de valor o recomendación de los equipos terminales, y que su finalidad es informativa.

Información General	
I. Contraseñas. Se menciona que:	
Permite el uso de contraseñas únicas preinstaladas y/o que requieran que el usuario elija una contraseña.	SIN DATO
Permite el uso de medios de autenticación de múltiples factores.	SIN DATO
Proporciona al usuario o al administrador un mecanismo simple para cambiar las contraseñas o mecanismos de autenticación.	SIN DATO
II. Actualizaciones del software. Se menciona que:	
El fabricante notifica al usuario cuando se aplicará una actualización de "software" que interrumpa de forma temporal el funcionamiento básico de éste.	SIN DATO
Los mecanismos son configurables a efecto de que los usuarios puedan activar, desactivar y/o posponer la instalación de dichas actualizaciones.	SIN DATO
Los dispositivos son identificables a través del etiquetado en éste o mediante su interfaz física.	SI
III. Sobre el uso de comunicaciones seguras. Se menciona que:	
Se emplean prácticas en materia de cifrado para comunicaciones seguras.	SIN DATO
IV. Integridad del software. Se menciona que:	
Utiliza un módulo de seguridad en el "hardware".	SIN DATO

En caso de cambios no autorizados en el "software", estos alertan al usuario y al administrador de la red sobre el incidente detectado.	SIN DATO
V. Sobre los datos de telemetría.	
Se menciona que permite examinar los datos de telemetría, como datos de uso, registro y medición de estos.	SIN DATO
VI. Sobre la eliminación de los datos personales.	
Permite la eliminación de los datos personales por parte del usuario.	SI
Permite la eliminación de los datos personales en el caso de una transferencia de la propiedad a otro usuario del dispositivo o de los servicios asociados.	SI
Permite la eliminación de los datos personales cuando el usuario elimine un servicio asociado del dispositivo.	SI
Permite la eliminación de los datos personales cuando el dispositivo llegue al fin de su vida útil.	SI

SOBRE LA INFORMACIÓN QUE PROPORCIONAN LOS PROVEEDORES Y FABRICANTES

I. Ponen a disposición de los usuarios al menos lo siguiente:	
Información de contacto para la notificación de vulnerabilidades.	SI
Información sobre los plazos para el acuse de notificación inicial de vulnerabilidades.	SIN DATO
Información sobre la actualización del estatus de la vulnerabilidad notificada hasta la resolución de ésta.	SIN DATO
II. Sobre las credenciales y los parámetros de seguridad sensible.	
Proporciona a los usuarios información sobre cómo se utilizarán sus datos personales, quién los utilizará y con qué fines.	SI
Permite revocar el consentimiento para el uso de los datos personales.	SI
Si se pretende dar un uso distinto de los datos personales, se recabará nuevamente el consentimiento.	SI

III. Sobre la eliminación de los datos personales.	
Le proporciona instrucciones al usuario sobre cómo eliminar los datos personales registrados.	SI
Les proporcionan a los usuarios la confirmación clara de que sus datos personales han sido eliminados de los dispositivos o los servicios asociados.	SI
Implementan mecanismos que permitan eliminar los datos personales o los dispositivos o servicios asociados.	SI
El fabricante o el proveedor realiza copias de respaldo de los datos personales de los usuarios.	SI

FUENTE:

https://www.zumimall.com/pages/privacy-policy

https://www.zumimall.com/pages/terms-conditions

https://www.zumimall.com/

https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf