Estudio sobre la Seguridad de la Información y e-Confianza de los hogares españoles

Primera oleada (Diciembre 2006 – Enero 2007)

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Edición: Junio 2007

1 ÍNDICE

PUNTOS CLAVE

I. Hábitos de uso de Internet

- El 78% de los usuarios tienen el hogar como lugar principal de acceso a Internet.
- El 93% de los hogares encuestados acceden a Internet mediante banda ancha.
- El 90% de los usuarios encuestados accede a Internet de manera diaria.
- Los servicios de Internet más utilizados por los hogares son el correo electrónico y la búsqueda de información.
- Los servicios de Internet que son administrados por un mayor número de usuarios son las páginas Web y el blog

II. Hábitos de seguridad en Internet

- Dependiendo del tipo de medidas utilizadas podemos distinguir entre tres tipos de protección de los equipos de los hogares:
    - **Protección Avanzada:** Declaran utilizar tanto protección proactiva como automatizable.
    - **Protección Básica.** Utilizan fundamentalmente medidas automatizables.
    - **Protección Deficiente.** Presentan niveles muy bajos en ambos tipos de protección.
- El 94,5% de los hogares españoles conectados a Internet señalan que disponen de programa antivirus aunque un 8% de estos equipos realmente no lo tienen. El cortafuegos es la segunda medida con mayor penetración, un 76%.
- Las medidas que exigen un comportamiento más activo del usuario (vg: copias de seguridad o partición del disco duro) son menos frecuentes: un 35% de los usuarios hacen copias de seguridad de sus archivos y menos del 10% encriptan documentos.
- Los usuarios pronostican un aumento significativo en el uso de medidas de seguridad no automatizadas.
- Las principales razones para no incorporar las medidas de seguridad son el desconocimiento de la medida o la percepción de que ésta es innecesaria.

- De entre los panelistas que no usan antivirus un 38,1% indican no usarlo porque consideran que entorpece el uso del ordenador y la navegación por Internet.

III. Percepción de seguridad en Internet de los hogares españoles

- Se han detectado tres estilos de navegación referidos a hábitos de seguridad que definen tres segmentos de usuarios:

    - **Uso prudente y no solidario**. Caracterizado por un enfoque individualista de la seguridad, centrándose en la defensa del equipo particular, pero olvidando compartir experiencias con otros usuarios para una defensa solidaria. El 58% de los usuarios pertenecen a este grupo

    - **Uso prudente y solidario**. Añaden a la protección individual, la preocupación por compartir y la mutua ayuda en temas de seguridad. Son un 33% de los usuarios

    - **Uso temerario**. Un 9% de usuarios; no atienden a las normas y hábitos básicos de la prudencia, sufren muchas incidencias y de alta gravedad, y no por ello modifican sus hábitos imprudentes.

- Dado que la manifestación de los efectos del código malicioso no es siempre evidente, los usuarios se muestran generalmente confiados en que sus medidas de seguridad les mantienen protegidos.

- En general, la percepción es que la seguridad es mayor cada año y que las incidencias van disminuyendo en frecuencia y en gravedad.

- Solamente tras incidencias repetidas la percepción de seguridad se ve afectada; esta se recompone ampliando las medidas adoptadas, moderando las conductas de riesgo o ambas a la vez.

- Los hogares españoles señalan como incidencia detectada más habitual en sus equipos, la recepción de correo no deseado (spam). En los últimos tres meses, un 82% de los hogares han recibido correo no deseado.

- Los códigos maliciosos han dado lugar a incidencias reconocidas por los propios usuarios en más de la mitad de los hogares españoles en el último año.

- Tras una incidencia grave detectada por los usuarios, éstos efectúan en su mayoría un cambio en las medidas de seguridad disponibles en sus equipos, pero no así en el comportamiento y uso en Internet.

IV. Situación real de seguridad

- El 32,6% de los equipos analizados mantiene vulnerabilidades en el sistema operativo, frente a 2 de cada 3 que se detectan correctamente actualizados.

- El 72,6% de los ordenadores domésticos con acceso a Internet analizados presentan algún tipo de código malicioso (malware).

- No todos los códigos comportan un riesgo elevado, sin embargo, más del 50% de los ordenadores tiene códigos maliciosos de riesgo alto

- Las mayores amenazas, por su incidencia y gravedad, proceden en la actualidad de los troyanos (50,3% de los equipos). Por el contrario, la amenaza tradicional de los virus se encuentra en el 10,1% de los ordenadores y sólo representan un 1,2% de las variantes de malware encontradas. Esta perdida de importancia se debe a:

    - La eficacia de los sistemas antivirus y las actualizaciones automáticas.

    - El abandono del desarrollo de virus en favor de troyanos y adware

- Por lo general el malware que se produce actualmente (troyanos y adware) está residente en los equipos informáticos de los hogares sin que los usuarios sean conscientes de su existencia. Es un riesgo que pasa desapercibido hasta que acaba manifestándose en forma de daños en el equipo. El 40,4% declaran haber tenido que formatear su disco duro y un 23,6% sufrieron pérdidas de información almacenada. La causa de esta situación es que actualmente los desarrolladores de estos códigos tienen el objetivo de que sus creaciones pasen desapercibidas.

    - **Antes**: Notoriedad.

    - **Ahora**: Robo y explotación de información sensible con fines lucrativos, utilización del ancho banda de terceros con fines espurios, etc.

- El tipo de malware que se distribuye actualmente hace que los antivirus tengan una eficacia relativa. Se constata que la instalación de un antivirus no es suficiente, siendo necesarias otras medidas como buenas prácticas y hábitos de seguridad.

V. Papel de la Administración

- La mayor parte de los usuarios creen que para mejorar la seguridad hay que combinar las medidas preventivas individuales con una acción más decidida por parte de las Administraciones Públicas que ayude a limitar las incidencias de seguridad.

- En concreto, el 66,6% de los usuarios opina que la propagación de amenazas por Internet es el resultado de poca cautela de los usuarios de Internet.
- El 71,8% indican que las Administraciones Públicas deberían encargarse de hacer de Internet un “lugar seguro”.
- Cuando no se consigue recomponer la percepción de seguridad con las medidas habituales aumenta la demanda relativa a la intervención de la Administración.
- Los usuarios piden a la Administración que:
    - Controle y vigile más de cerca lo que está pasando en Internet,
    - Informe y/o alerte a los usuarios
    - Sea más diligente en la persecución de delitos o prácticas abusivas.
- Los problemas de seguridad parecen tener un impacto destacado en el desarrollo de la Sociedad de la Información. Así, un 58,3% indica que utilizaría más servicios online si le enseñaran cómo protegerse mejor.

2 INTRODUCCIÓN Y OBJETIVOS

2.1 Presentación

2.1.1 Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

Su objetivo es doble: por una parte, contribuir a la convergencia de España con Europa en la Sociedad de la Información y, de otra parte, promover el desarrollo regional, enraizando en León un proyecto con vocación global.

La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano. Así, el Instituto tiene la vocación de ser un centro de desarrollo de carácter innovador y de interés público a nivel nacional que constituirá una iniciativa enriquecedora y difusora de las nuevas tecnologías en España en clara sintonía con Europa.

El objeto social de INTECO es la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Innovación en soluciones TIC para la Pyme, e-Salud, e-Democracia.

2.1.2 Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica. El Observatorio nace con el objetivo de describir de manera detallada y sistemática el nivel de seguridad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la Seguridad de la Información y la e-Confianza.

El Observatorio ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad por parte de INTECO, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad en Internet.
- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.
- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.
- Impulso de proyectos de investigación en materia de seguridad TIC.
- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.
- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

2.2 Estudio sobre la Seguridad de la Información y e-Confianza en los hogares españoles.

El presente documento recoge los resultados de la primera oleada del Estudio. En primer lugar se describen los objetivos generales que persigue la investigación, para a continuación pasar a detallar los hallazgos más relevantes de esta primera toma de datos.

2.2.1 Objetivo General

El objetivo general de este Estudio es la evaluación de la seguridad, confianza y nivel de incidencias de seguridad de los hogares españoles usuarios de Internet. Todo ello con el fin de impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la Seguridad de la Información y la e-Confianza.

Esta evaluación se realizará con una perspectiva temporal, de la que este documento es el primer informe, con el fin de servir de apoyo y generar propuestas con el objeto de la toma de decisiones por parte de la Administración para reducir las posibles limitaciones y barreras relacionadas con la seguridad y la confianza de los usuarios de la Red que afectan al desarrollo de la Sociedad de la Información en España.

2.2.2 Objetivos secundarios y objetivos detallados

Este objetivo general se desglosa a su vez en dos objetivos secundarios:

- Analizar hasta qué punto la falta de seguridad de la Red permite explicar los retrasos en la adopción y la extensión del uso de servicios a través de Internet como, por ejemplo, el comercio electrónico, la administración electrónica, la banca online, etc.

  El desarrollo de este objetivo exige tener en cuenta tanto la incidencia y gravedad de los episodios de riesgo como la percepción de este riesgo, es decir, el nivel de confianza que inspira la Sociedad de la Información.

- Orientar iniciativas y políticas públicas, tanto en el área de la mejora individual de la seguridad como en la generación de confianza hacia la sociedad de la información, sustentadas en una percepción realista de los riesgos y los beneficios de la misma.

  El desarrollo de este objetivo precisa de la elaboración de una tipología de usuarios de Internet que combine información procedente tanto de la exposición real a incidencias de seguridad así como la percepción de inseguridad que se percibe en la Red (Matriz Incidencias-Confianza)

2.2.3 Objetivos específicos

Los anteriores objetivos secundarios se desglosan operativamente en los siguientes objetivos específicos que permiten, además, orientar la estructura temática del presente Informe.

Hábitos de Seguridad:

- Conocer las intenciones de adopción en el futuro próximo de los avances relacionados con la seguridad en Internet.

- Estudiar las demandas generales de los usuarios de Internet, hogares y ciudadanos, para el mejor desarrollo de una Sociedad de la Información segura y confiable.

- Conocer las recomendaciones que éstos hacen a terceros sobre seguridad y utilización de las posibilidades de la Sociedad de la Información.

Incidencias de Seguridad y Vulnerabilidad:

- Determinar el nivel de incidencia general de riesgos del código malicioso o malware: virus informáticos, troyanos, gusanos, programas espía, etc.

- Catalogar los tipos de malware más frecuentes, su capacidad de diseminación y la gravedad de los mismos.

- Desglosar la exposición diferencial al riesgo por grupos de edad, nivel de formación, experiencia como usuario de Internet, nivel de ingresos y otras variables relevantes sociológicamente.

Percepción de Seguridad:

- Obtener la percepción general del riesgo ante virus informáticos, amenazas a la privacidad y a la seguridad de los pagos, entre otros, así como su evolución a lo largo del tiempo.

- Determinar el nivel de confianza electrónica desde el punto de vista de los usuarios.

- Detectar los colectivos con percepción de riesgo alto que pueden estar limitando su adopción de soluciones relacionadas con la Sociedad de la Información e impulsar políticas específicas para mejorar la seguridad y confianza de esos grupos de ciudadanos.

- Detectar colectivos con percepción de riesgo bajo que están poniendo en riesgo su seguridad y la de otros usuarios al servir de involuntarios difusores de las amenazas.

3 DISEÑO METODOLÓGICO

De cara a alcanzar los objetivos expuestos, se combinan medidas objetivas de incidencia con medidas subjetivas de percepción de seguridad y confianza en la Red.

Adicionalmente se pretende asentar una base sólida sobre la que se pueda recoger información sobre los cambios del nivel de seguridad y confianza de los hogares españoles. Esto requiere obtener datos robustos sobre una muestra que facilite información de tipo longitudinal. Esto es, se necesita recoger información sobre los mismos hogares y usuarios en diferentes momentos de tiempo. La metodología que mejor cumple con estos criterios es el **Panel online dedicado.**

INTECO ha desarrollado para su Panel de hogares una metodología realmente novedosa. Está integrado por 3.000 hogares, con conexión a Internet, de todo el territorio nacional de los que se extrae información con un origen doble:

- Por una parte, se analiza el nivel de seguridad real con un software que analiza las incidencias de seguridad en los equipos domésticos. Dicho programa informático – desarrollado por INTECO – se entrega a los panelistas con el fin de que estos lo instalen en sus ordenadores. Este software escanea mensualmente los equipos de los panelistas, detectando todo el malware residente en los mismos y recogiendo además datos del sistema operativo y del estado de su actualización. El software envía esta información a INTECO que la trata de manera totalmente anónima y agregada. Los panelistas son informados de que no recibirán información sobre sus incidencias de seguridad, aunque estas sean peligrosas para su equipo, pues prevalece el interés de conocer la situación general de la manera más fidedigna posible frente a las alertas que solucionen problemas individuales. Los panelistas son convenientemente informados de esta situación y aceptan participar bajo las condiciones expuestas.

- De otro lado, la percepción y nivel de confianza de los usuarios domésticos se analizará por medio de encuestas personales. Los panelistas responderán a una encuesta de manera trimestral sobre su percepción de seguridad y sus prácticas y comportamientos en la Red.

Esto permite analizar y contrastar dos fuentes paralelas de información en el ámbito de la seguridad informática, lo que produce una gran ventaja comparativa: se permite conocer las diferencias existentes entre la percepción de seguridad y la situación real de los panelistas. Además esta metodología permite realizar un seguimiento a lo largo del tiempo de:

- El nivel real de seguridad.

- Los cambios en la perspectiva, opiniones y hábitos de seguridad, que experimentan los usuarios.

En general, la recogida de información responde al siguiente plan:

1) Captación del panel dedicado, por medio de invitaciones por correo electrónico.

2) Información del tipo de colaboración requerida, sistema de incentivos y condiciones de confidencialidad.

3) Invitación al escaneo del equipo del panelista con acceso al programa de análisis por identificador personalizado, de forma que permita tanto el control de participación como la fusión de datos de la encuesta.

4) Control de cuotas según diseño muestral que se indica en el "Tamaño y distribución muestral".

La primera oleada del Estudio, cuyos resultados se exponen seguidamente, representa un ciclo mensual completo de escaneo y encuesta y permite un primer análisis de base, tanto de la situación de la seguridad en Internet como de los niveles de participación esperables a lo largo de la vida del panel.

3.1 Ficha técnica

Las características técnicas de la investigación se describen seguidamente:

3.1.1 Universo

Usuarios españoles de Internet, con acceso frecuente a Internet desde el hogar, mayores de 15 años. Para delimitar con mayor precisión el concepto de usuario, se exige una conexión a Internet desde el hogar de al menos una vez al mes.

3.1.2 Tamaño y distribución muestral

Se ha extraído una muestra representativa de 6.357 usuarios de Internet en el hogar con un diseño polietápico:

- Estratificación por Comunidades Autónomas para garantizar un mínimo de sujetos en cada una de estas entidades.

- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[1].

[1] Estas cuotas se han obtenido de datos representativos a nivel nacional de usuarios de Internet mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Comercio y Turismo. ("*Las TIC en los hogares españoles: 11ª Oleada-Octubre 2006")*

Aunque las desviaciones entre la muestra obtenida y la teórica han sido pequeñas, la ***Muestra Total*** (que incluye el total de encuestas recogidas, 6.357 hogares) se ha equilibrado al universo en base a los datos poblacionales por CCAA y a las variables de cuota, para alcanzar un ajuste más perfecto. La ***Muestra Panelizada*** (que incluye sólo a los usuarios que han cumplimentado el cuestionario y han realizado el escaneo, 3.068 hogares) presenta los coeficientes de ponderación asignados como subgrupo de la muestra total.

Las dos muestras representan el grupo de hogares analizados, tanto a nivel de entrevistas como de escaneos. La muestra total incluye el número de hogares escaneados. Dado que la muestra total refleja algo mejor el conjunto del mercado que la muestra panelizada, se ha optado por aprovechar la amplia base disponible de 6.357 entrevistados para analizar los datos de hábitos y opinión, que permite conocer la dinámica de este fenómeno y sirve de contexto para comprender mejor los resultados del escaneo que proceden de la muestra panelizada de 3.068 individuos.

Tabla 1: Distribución muestral por CCAA (%)

CCAA	Muestra obtenida		Muestra teórica
	Panelizada	Encuestada	
Andalucía	14,6	14,2	16,3
Aragón	3,5	3,5	2,9
Asturias	3,8	3,9	3,0
Baleares	2,2	2,1	2,5
Canarias	3,9	3,8	4,8
Cantabria	1,6	1,3	1,5
Castilla-La Mancha	2,8	2,5	3,9
Castilla y León	6,1	6,0	5,6
Cataluña	16,6	16,5	16,8
País Vasco	5,4	5,4	5,6
Extremadura	0,9	1,0	1,7
Galicia	5,4	5,3	5,8
Madrid	19,8	21,0	15,7
Murcia	2,1	2,2	3,0
Navarra	1,0	0,9	1,4
La Rioja	0,7	0,7	0,7
C. Valenciana	9,6	9,7	8,8

n_1 = 3068, Base muestra equipos analizados.
n_2 = 6357, Base total muestra de hogares.

Fuente: INTECO

Tabla 2: Distribución muestral por conceptos (%)

Concepto	Muestra obtenida		Muestra teórica
	Panelizada	Encuestada	
Actividad			
Ocupados	70,2	69,5	63,3
Parado (buscando trabajo)	4,8	4,6	6,2
Estudio	18,2	19,0	22,8
Jubilado	2,9	2,6	2,7
Otros Inactivos	3,9	4,3	5,0
Tamaño del hogar			
1	7,3	7,6	4,9
2	26,1	26,4	15,2
3	26,7	26,2	26,5
4 y mas	39,9	39,8	53,4
Sexo			
Hombre	53,5	52,1	52,2
Mujer	46,5	47,9	47,8
Hábitat			
Hasta 20.000	24,3	24,1	29,5
De 20.001 a 100.000	18,9	17,9	24,5
Más de 100.000 y capitales	56,8	58,0	46,0
Edad			
Hasta 24	23,5	24,7	25,5
25-34	38,8	40,7	29,6
35-49	29,2	26,8	30,5
50 y más años	8,5	7,8	14,4

n_1 = 3068, Base muestra equipos analizados.
n_2 = 6357, Base total muestra de hogares.

Fuente: INTECO

3.1.3 Captura de información

Entrevistas online para el total de muestra (n=6357) y análisis de los equipos informáticos de acceso principal a Internet desde el hogar para un total 3.068 panelistas

3.1.4 Trabajo de campo

Realizado entre diciembre de 2006 y enero de 2007.

3.1.5 Error muestral

De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95,5%, se establecen los siguientes cálculos del error muestral.

Muestra total n=6.357, error muestral ±1,25%

Muestra panelizada n= 3.068, error muestral ±1,81%

Como puede observarse, una muestra mayor redunda en un error muestral inferior. En este caso el diferencial es de 0,56 puntos porcentuales a favor de la muestra total. Por ello, se han utilizado las respuestas de todos los encuestados para analizar la percepción y los hábitos de seguridad de los hogares españoles, minimizando de esta manera el error estadístico sobre los datos presentados

3.2 Consistencia de la muestra

3.2.1 Muestra total (entrevistada) vs. Muestra panelizada (entrevistada y escaneada)

En este epígrafe se realiza un análisis comparativo de la muestra panelizada y de la muestra total, con el fin de contrastar la consistencia de ambas muestras

El único sesgo que podría afectar a la muestra tiene relación, aunque de forma muy moderada como se observa en la Tabla 3, con la mayor presencia de usuarios de Internet solidarios en la muestra de equipos escaneados que en la muestra total. La explicación es simple, se les pide instalar un programa de escaneo que servirá para conocer mejor los problemas de seguridad generales y códigos maliciosos concretos.

Esta situación es más común para los usuarios de Internet que ya están habituados a colaborar de forma desinteresada para la mejora de la seguridad de todos. En todo caso, el sesgo detectado es moderado (2,8 puntos de diferencial entre 66,6 y 63,8) y debe servir para matizar algunas conclusiones.

Tabla 3: Perfil de hábitos de seguridad (%)

Perfiles	Muestra obtenida	
	Panelizada	*Encuestada*
No solidario	66,6	63,8
Solidario	33,4	36,2

n_1 = Base total muestra de hogares.
n_2 = Base muestra equipos analizados.

Fuente: INTECO

Tabla 4: Perfil actitudinal

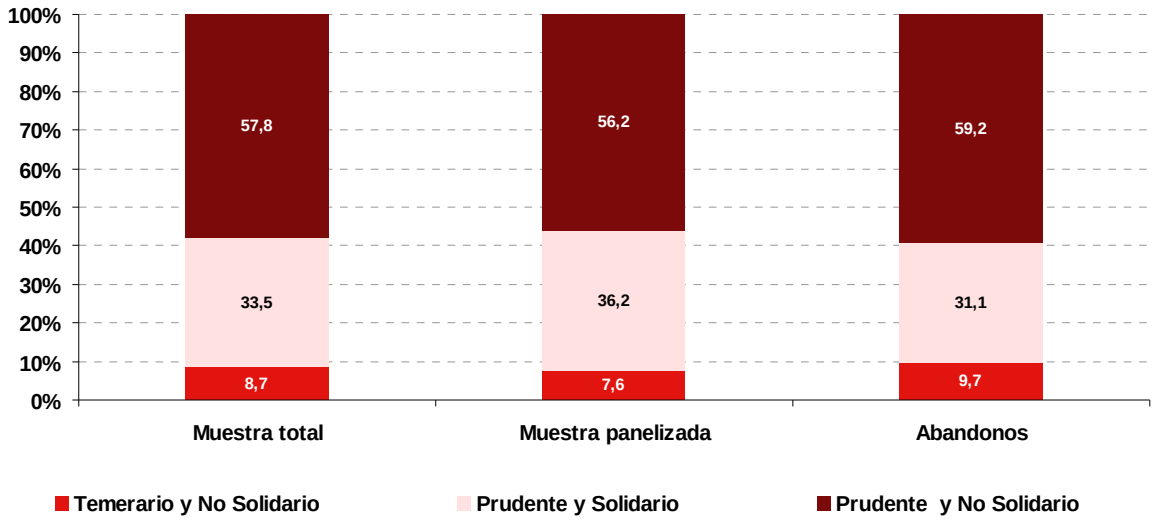
Perfiles	Medias	
	Panelizada	*Encuestada*
Tutelaje	4,14	4,15
Autorregulación	4,13	4,12

n_1 = Base total muestra de hogares.
n_2 = Base muestra equipos analizados.

Fuente: INTECO

De forma gráfica se observa que entre los usuarios que abandonaron la fase de análisis del equipo, se aprecia un 31,1% de solidarios frente a un 36,2% entre los que completaron el escaneo de su ordenador. Es decir, se cuenta con una muestra ligeramente más solidaria en cuanto al análisis del ordenador que la utilizada a efectos de entrevista.

Gráfico 1: Distribución por segmentos de hábitos (%)



Fuente: INTECO

3.2.2 Robustez temporal de la muestra

Para comprobar la robustez del análisis se ha analizado la consistencia de la muestra, contrastando los resultados obtenidos en esta y aquellos extraídos de:

- Datos utilizados para la primera oleada: Análisis de los datos a los que se hace referencia en el resto del documento y que corresponden a la prueba piloto de diciembre y a una parte del mes de enero.

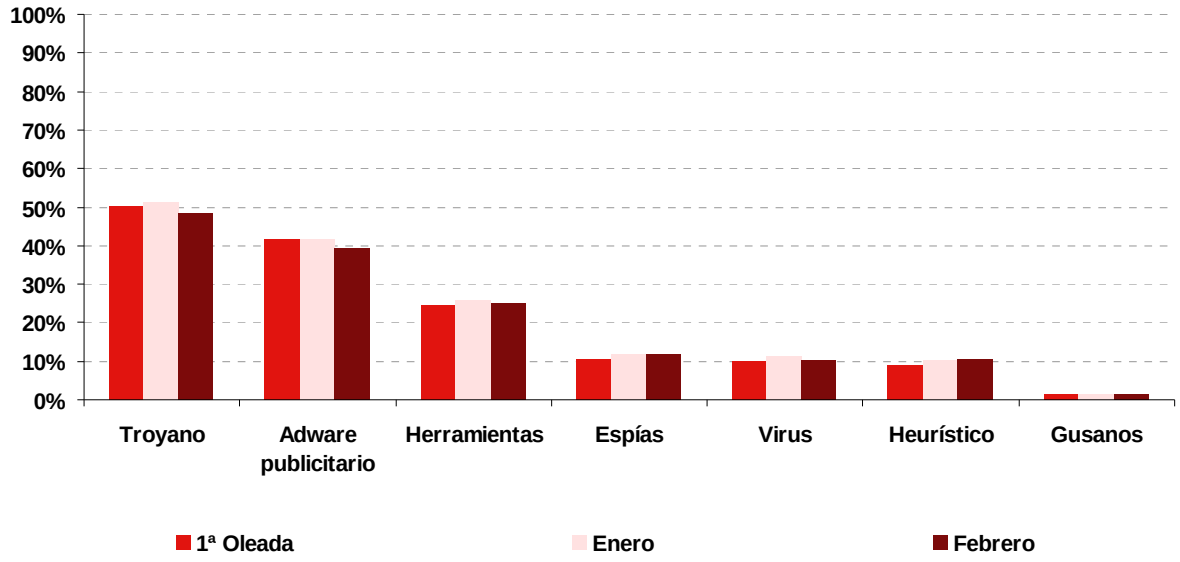
- Los escaneos de los meses completos de enero y febrero, considerándose cada uno de estos escaneos una muestra representativa y válida tal y como se define en la metodología del estudio

Los resultados del malware[2] encontrado en los escaneos anteriormente referenciados se detallan en el Gráfico 2. Los datos que se muestran han de tomarse, no obstante, con cautela, puesto que corresponden a los escaneos realizados con carácter previo a su ponderación y antes de eliminar aquellos registros de usuarios que si bien han escaneado su equipo no han completado adecuadamente los cuestionarios. Por tanto, a pesar de que

[2] Las definiciones del código malicioso que se reflejan en el Gráfico 2 y en el Gráfico 3 pueden encontrarse en el epígrafe 8.2

estos datos no pueden utilizarse para hacer perspectiva, si son ilustrativos del carácter consistente y homogéneo que tiene la muestra.

Gráfico 2: Evolución del código malicioso en los meses de Diciembre a Febrero



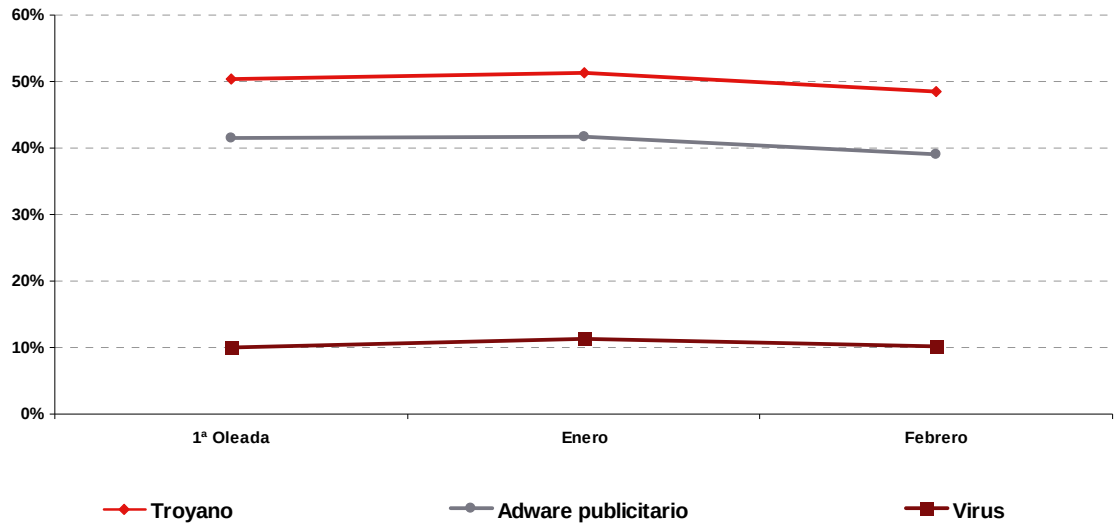
Fuente: INTECO

La muestra está, por tanto, exenta de sesgos y de problemas estructurales. Las variaciones producidas en la muestra a lo largo del tiempo, son fruto del dinamismo del panel, que refleja como están evolucionando las incidencias detectadas en los usuarios. Estos datos se reflejan de manera ilustrativa en el que muestra el porcentaje de detecciones del malware en los meses de diciembre, enero y febrero

En el Gráfico 3 se muestran las variaciones que se producen en la serie respecto de los datos utilizados para la primera oleada, para 3 de los principales tipos de malware.

Por tanto, puesto que las variaciones experimentadas por la muestra están comprendidas en la variación normal establecida por el error muestral y por la evolución lógica y normal de los hábitos de seguridad de usuarios españoles, los resultados obtenidos y expresados en el informe de resultados, pueden considerarse adecuados, y es posible establecerlos como base para un futuro análisis de series temporales que permitirá medir la evolución pasada y predecir posibles situaciones futuras.

Gráfico 3: Evolución del porcentaje del código malicioso más significativo detectado en los equipos durante los meses de Diciembre a Febrero



Fuente: INTECO

4 CARACTERÍSTICAS SOCIODEMOGRÁFICAS Y EQUIPAMIENTO TECNOLÓGICO

4.1 Características sociodemográficas

En la estructura muestral del Estudio ha sido decisiva la participación de los entrevistados en las dos modalidades definidas en el planteamiento metodológico del mismo.

Los resultados de la metodología de doble fuente de información (cuestionario personal y escaneo del equipo) muestran que se deja ligeramente infrarepresentados al grupo de usuarios de Internet más recelosos con estas iniciativas de colaboración, que suponen además instalar programas en su ordenador a petición de un tercero.

Por este motivo, y para calibrar mejor este efecto en la interpretación de los resultados a lo largo de la vida del panel, se procede en esta primera oleada a un análisis comparado, aceptando panelistas con colaboración parcial (solo cuestionario) y con colaboración total (escaneo y cuestionario). En el resto de las variables sociodemográficas relevantes la muestra total es homogénea a la muestra panelizada.

Por tanto, este primer informe tiene a la vez un carácter de estudio de base y de primera ola del panel, permitiendo contextualizar los resultados de esta primera ola del panel en el conjunto de una investigación más general sobre usos y actitudes relacionadas con la seguridad en Internet. En la Tabla 5 se muestra un cuadro comparativo detallado entre la muestra total, la muestra panelizada y el análisis de los posibles sesgos de auto-selección.

Tabla 5: Distribución muestral ajustada (%)

Concepto	Muestra obtenida	
	Panelizada	***Encuestada***
Edad		
Hasta 24	25,5	24,0
25-34	29,5	28,3
35-49	30,6	32,9
50-64	12,1	12,8
65+	2,3	2,0
Hábitat		
Hasta 20.000	29,5	29,7
De 20.001 a 100.000	24,5	25,0
Más de 100.000 y capitales	46,0	45,3
Sexo		
Hombre	52,2	53,3
Mujer	47,8	46,7
Antigüedad en Internet		
Menos de seis meses	0,3	0,3
Entre seis meses y un año	1,4	1,3
Entre uno y dos años	5,0	5,0
Entre dos y cuatro años	14,8	14,8
Entre cuatro y cinco años	13,1	12,7
Más de cinco años	65,4	65,9
Frecuencia de uso		
Menos de 1 hora	5,6	4,5
Entre 1 y 5 horas	34,1	33,8
Entre 5 y 10 horas	20,7	20,5
Entre 10 y 20 horas	18,7	19,7
Entre 20 y 40 horas	13,3	14,2
Más de 40 horas	7,6	7,3

n_1 = 6357, Base total muestra de hogares.
n_2 = 3068, Base muestra equipos analizados.

Fuente: INTECO

4.2 Equipamiento tecnológico

En la Tabla 6, se muestra el perfil de equipamiento tecnológico de los hogares, así como las formas de acceso a Internet más comunes en esos hogares.

Se observa con claridad que se trata de hogares especialmente bien equipados, como corresponde a usuarios intensivos en uso de Internet desde el hogar[3].

[3] Las condiciones técnicas requeridas para la inclusión de un hogar en el panel, disponibilidad de un equipo con conexión a Internet para poder realizar las entrevistas online y los escaneos mensuales, determinan un mayor componente tecnológico en los hogares de la muestra. Los datos presentados en epígrafes como el equipamiento, tipo de conexión, frecuencia de acceso e intensidad de uso, o los servicios utilizados en la red reflejan esta circunstancia.

Es por ello que los hogares disponen de la mayoría de los dispositivos tecnológicos y son, por tanto, hogares que presentan un equipamiento extensivo. Destaca la elevada penetración de dispositivos de relativamente reciente lanzamiento en el mercado como router inalámbricos (WiFi, 46,1%) televisión digital terrestre (TDT, 48,4%), o grabadores de televisión de disco duro (Grabador HD, 22,6%).

Tabla 6: Equipamiento de los hogares (%)

Equipamientos	%
Televisor	99,7
Impresora	92,5
Ordenador de Sobremesa	92,4
Reproductor DVD	92,0
Cámara Fotos Digital	89,0
Grabadora de CD	86,4
Grabadora de DVD	80,0
Video	76,9
Escáner	72,8
Webcam	63,2
Videoconsola	55,5
Cámara de Video	52,7
Ordenador Portátil	52,6
Decodificador TDT	48,4
Router Wireless (WIFI)	46,1
Grabador HD (disco duro)	22,6

Fuente: INTECO

Con respecto a los dispositivos de uso individual, también se aprecia una alta penetración en todos aquellos analizados. Cabe destacar el porcentaje de personas que disponen de PDA/agenda electrónica (20,7%).

Tabla 7: Equipamiento personal (%)

Equipamientos	%
Teléfono móvil	98,9
MP3/Mp4	73,3
PDA/Agenda Electrónica	20,7

Fuente: INTECO

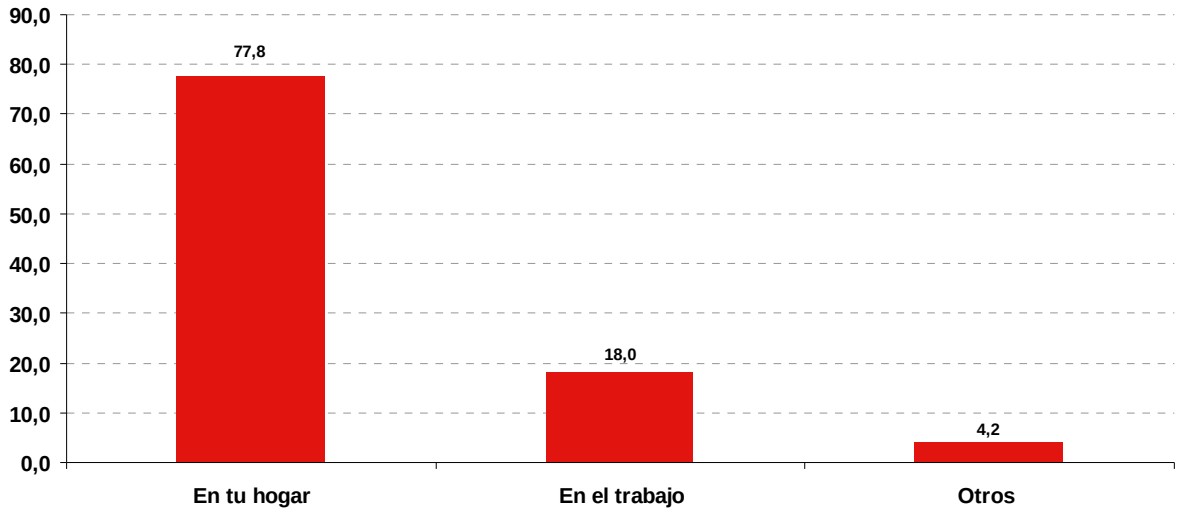
Como síntesis de estos resultados, se puede afirmar los usuarios frecuentes de Internet en el hogar pertenecen en su mayoría a la categoría de 'hogares digitales', característicos de la Sociedad de la Información: un tipo de hogar que sintetiza la tendencia de evolución de

la sofisticación tecnológica. Es decir, se trata de usuarios informados y equipados, que suponen la parte más activa de Internet y del equipamiento tecnológico en general.

4.3 Accesos y conexiones a Internet

En relación al lugar de acceso más habitual a Internet, un 77,8% de los 6.357 hogares analizados acceden a la Red desde el propio hogar y un 18,0% desde el trabajo. El resto de los lugares de acceso principal a Internet (bibliotecas, centros de estudios, telecentros públicos, cibercafés o casas de familiares y amigos) muestran porcentajes muy bajos, representando en su conjunto el 4,2%.

Gráfico 4: Lugar principal de acceso a Internet (%)

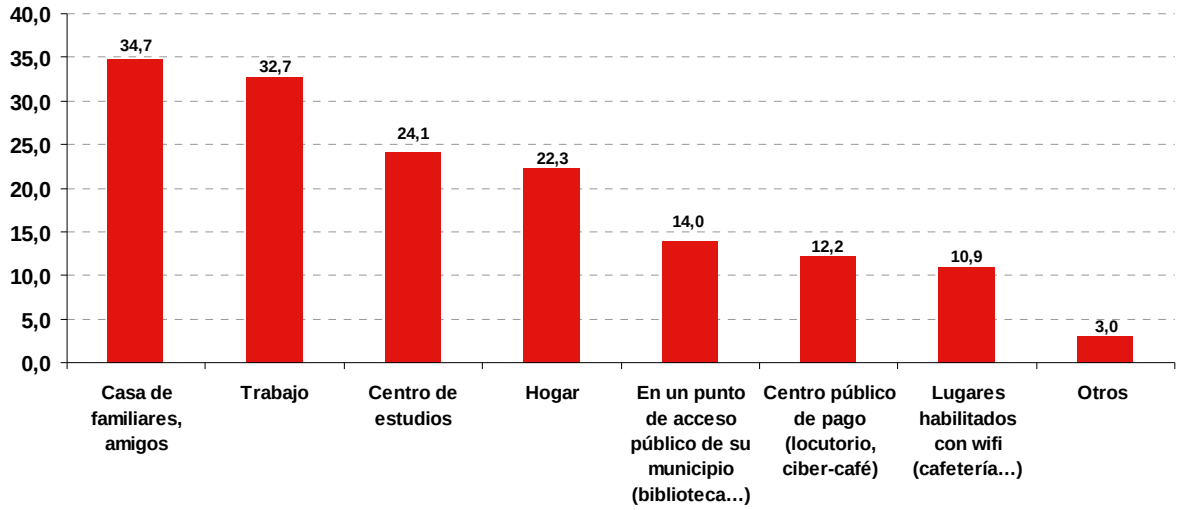


Fuente: INTECO

Como lugar de acceso alternativo (no principal) se observa que los usuarios utilizan principalmente otros hogares de familiares y amigos (34,7%), el trabajo (32,7%) y el centro de estudios (24,1%)[4].

[4] Según los datos facilitados por Red.es, ("*Las TIC en los hogares españoles: 12ª Oleada-Diciembre 2006*") el 57% de los hogares se conecta desde casa y el 35,3% en el trabajo. La obligatoriedad de realizar las entrevistas online y los escaneos mensuales en el ordenador del hogar, determinan un sesgo de los datos del lugar de acceso de la muestra.

Gráfico 5: Otros lugares de acceso a Internet (%)

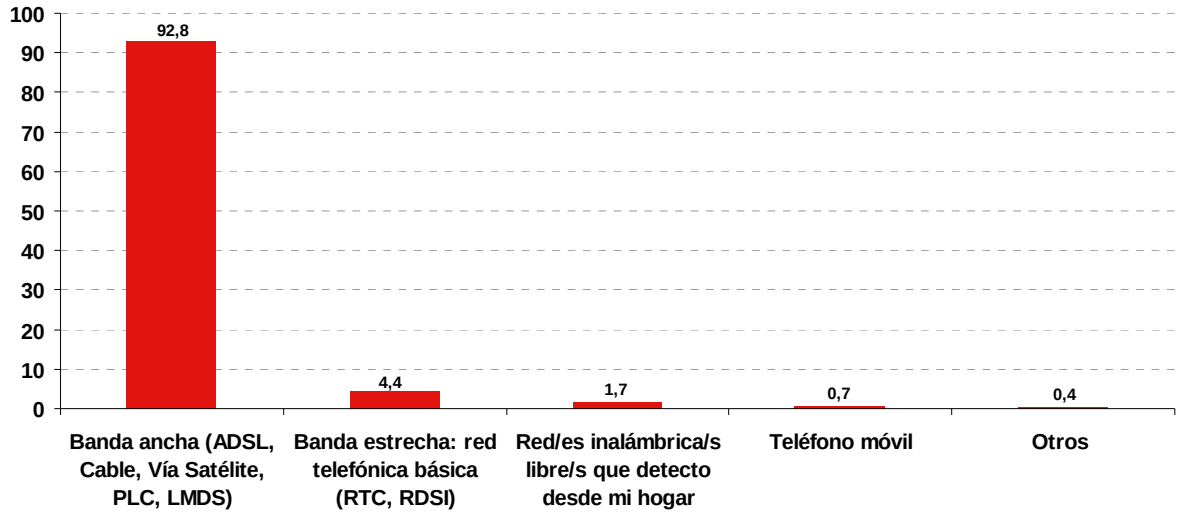


Fuente: INTECO

En cuanto al tipo de acceso (Gráfico 6) la penetración de banda ancha, en la muestra total de más de 6.000 hogares, es prácticamente universal (92,8%), una circunstancia que va a ayudar a explicar la utilización intensiva de algunos servicios de Internet, especialmente las descargas y el intercambio de archivos a través de redes P2P.

La forma de acceso tradicional (banda estrecha) es prácticamente anecdótica (4,4%) y otras formas de acceso, como a través del teléfono móvil, apenas registran penetración.

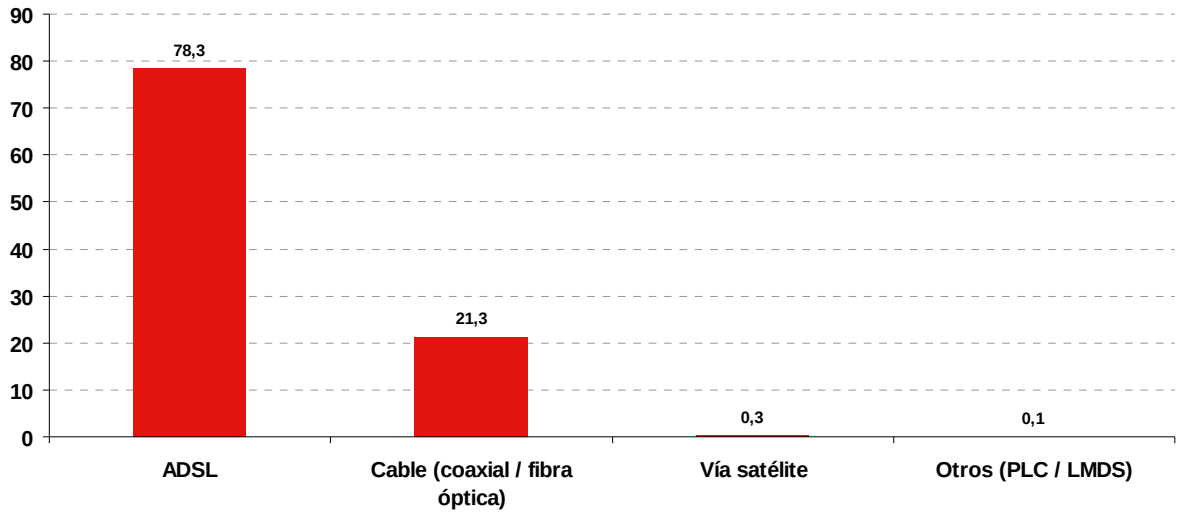
Gráfico 6: Distribución de los sistemas de acceso a Internet (%)



Fuente: INTECO

La modalidad de acceso de banda ancha a través de módem ADSL es mayoritario (78,3%). De cada cuatro usuarios, tres acceden a través de ADSL y uno a través de cable, mientras que otros tipos de acceso de banda ancha apenas registran penetración (Vía Satélite, LMDS, PLC…)

Gráfico 7: Distribución de los sistemas de acceso a Internet por Banda Ancha (%)



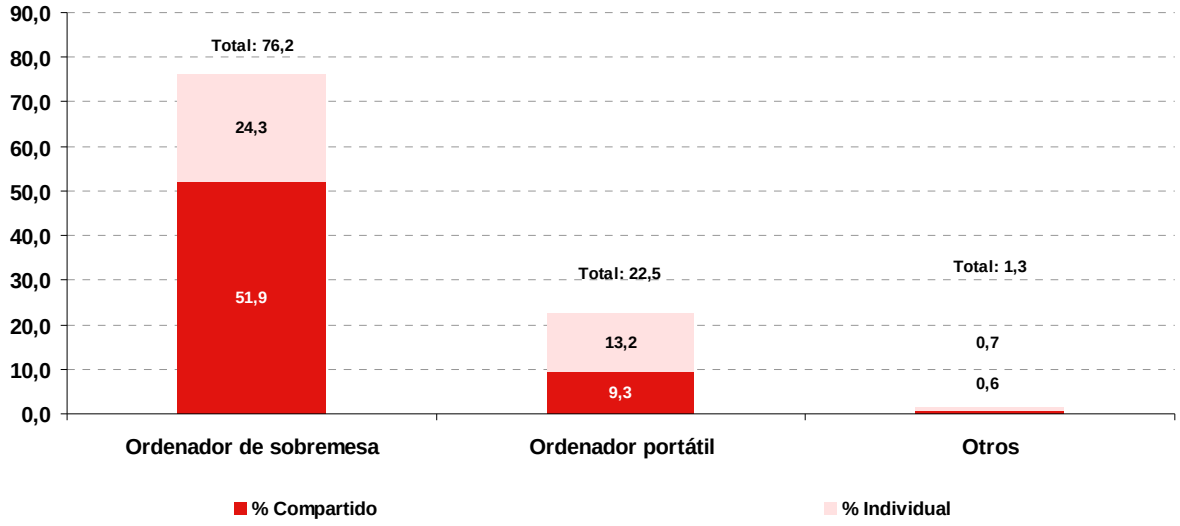
Base acceso Banda ancha *Fuente: INTECO*

Como puede observarse en el Gráfico 8, en lo que respecta a los terminales de acceso a Internet en el hogar más habituales y al tipo de uso que se les da (uso individual o compartido con otros usuarios), se observa que la práctica totalidad de los usuarios (98,7%) utilizan un ordenador: bien de sobremesa bien un ordenador portátil, siendo marginal el acceso a través de otro tipo de terminal [5](PDA, móvil, videoconsola, etc.).

Ambos tipos de terminal (ordenador de sobremesa y portátil) tienden a ser compartidos con otros miembros del hogar, si bien en diferente grado. Algo más de 2 de cada 3 usuarios que acceden principalmente desde un ordenador fijo lo comparten con otros usuarios. El ordenador portátil es compartido en menor grado (menos de la mitad de sus usuarios), si bien este dato confirma que progresivamente va perdiendo su papel de equipamiento individual.

[5] Según los datos facilitados por Red.es, ("*Las TIC en los hogares españoles: 12ª Oleada-Diciembre 2006*") el 79,7% de los hogares se conecta utilizando el ordenador de sobremesa y el 18,4% utilizando el ordenador portátil.
Según los datos del INE: "*Encuesta de Tecnologías de la información en los hogares 2º semestre 2005*" el 88,9% de los hogares se conecta utilizando el ordenador de sobremesa y el 23,1 utilizando el ordenador portátil. Siendo la base en este segundo caso el total de viviendas que disponen de acceso a Internet. No teniendo en cuenta en estos datos ni requiriendo, como así lo hace el Estudio, un uso intensivo de la Red.

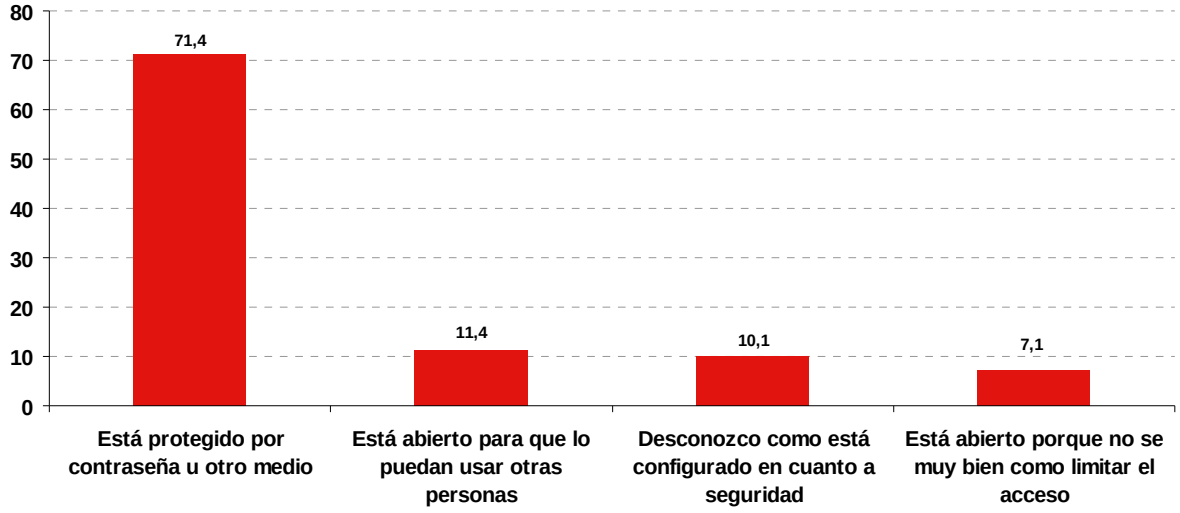
Gráfico 8: Distribución de uso, individual o compartido, del aparato de acceso principal a Internet en el hogar (%)



Fuente: INTECO

La mayoría (71,4%) de los accesos a Internet por medio de redes inalámbricas están protegidos por contraseña. Un porcentaje bastante elevado que indica una razonable orientación hacia la protección. El 11,4% de los usuarios que disponen de WiFi mantienen abiertos sus puntos de acceso con el fin de que otros individuos puedan utilizarlos para conectarse a la Red. El 7,1% tienen abierto el acceso porque ignoran cómo limitarlo. Además uno de cada diez hogares desconoce la configuración de seguridad del mismo.

Gráfico 9: Estado de la protección de accesos inalámbricos a Internet en el hogar (%)



Base acceso inalámbrico WiFi

Fuente: INTECO

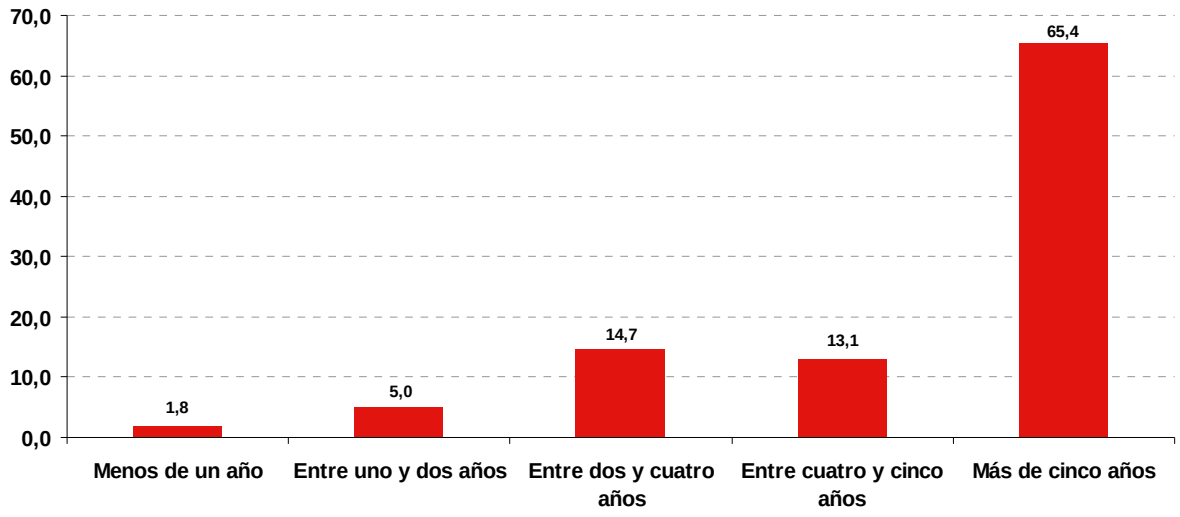
5 HÁBITOS DE USO DE INTERNET

En este bloque se presentan los principales resultados obtenidos sobre los hábitos de los usuarios de Internet desde el hogar, atendiendo a los hábitos generales y a los modos de acceso a Internet.

5.1 Experiencia en el uso de Internet

En el siguiente gráfico (Gráfico 10) se observa que la mayor parte de los usuarios (65,4%) tienen una experiencia mayor a cinco años en el uso de Internet y el 93,2% utilizan Internet, como mínimo, desde hace dos años ó más. Son, por tanto, en su mayoría usuarios familiarizados con Internet.

Gráfico 10: Experiencia como usuario de Internet (%)



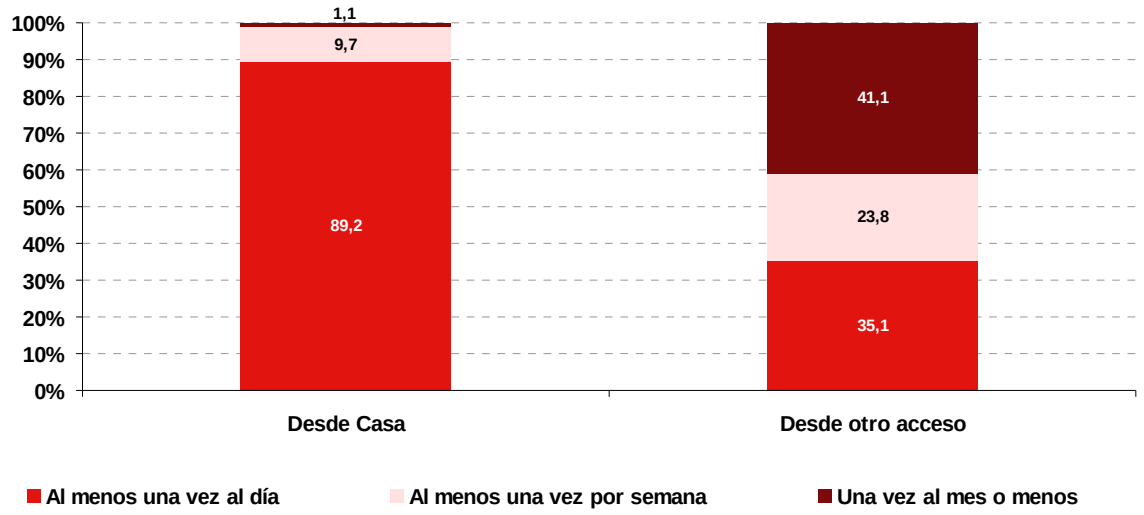
Fuente: INTECO

5.2 Frecuencia de acceso

En cuanto a la frecuencia de acceso a Internet desde el hogar, 9 de cada 10 usuarios lo hacen diariamente y prácticamente la totalidad (98,9%) semanalmente como mínimo. Estos datos sugieren que para los participantes en el Estudio, el uso de Internet en el hogar es continuado y, previsiblemente, ya forma parte de la rutina de la vida en el hogar.

Estos usuarios acceden a Internet desde otros equipos distintos a los usados desde el hogar, si bien en porcentajes sensiblemente menores. Aproximadamente el 60% acceden también a Internet semanalmente desde otros ordenadores distintos al del hogar, aunque sólo el 35,1% lo hacen a diario.

Gráfico 11: Frecuencia del uso de Internet según el punto de acceso (%)

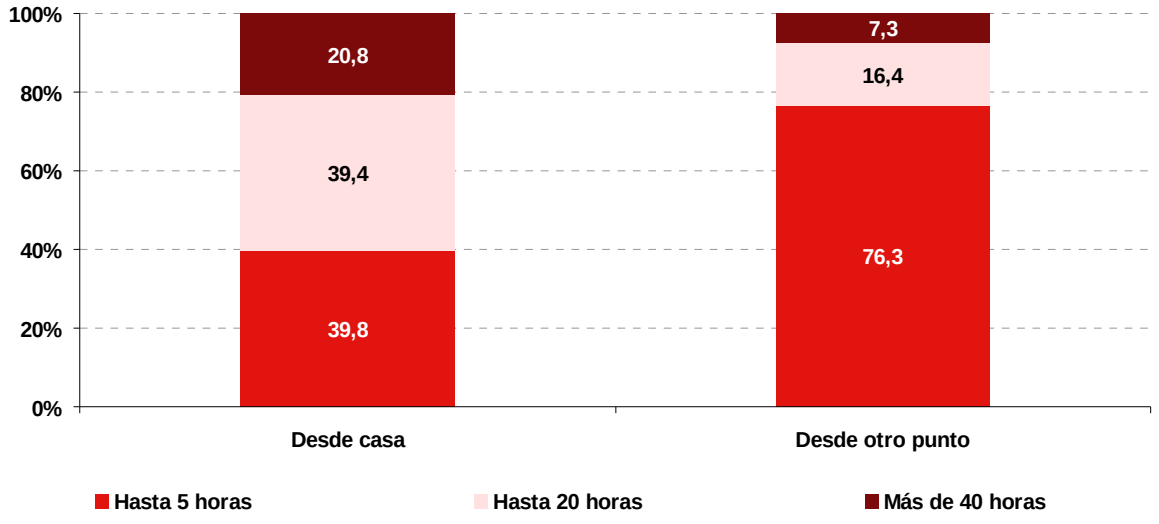


Fuente: INTECO

5.3 Intensidad de uso

Tanto la experiencia en el uso de Internet como la frecuencia de accesos sugieren que el acceso a Internet se ha incorporado en la vida de los hogares como un hábito más. Este comportamiento se ratifica por lo mostrado en el Gráfico 12. Permite contrastar esta idea al reflejar la intensidad en el uso medido por horas a la semana.

Gráfico 12: Intensidad del uso de Internet según el punto de acceso (%)



Fuente: INTECO

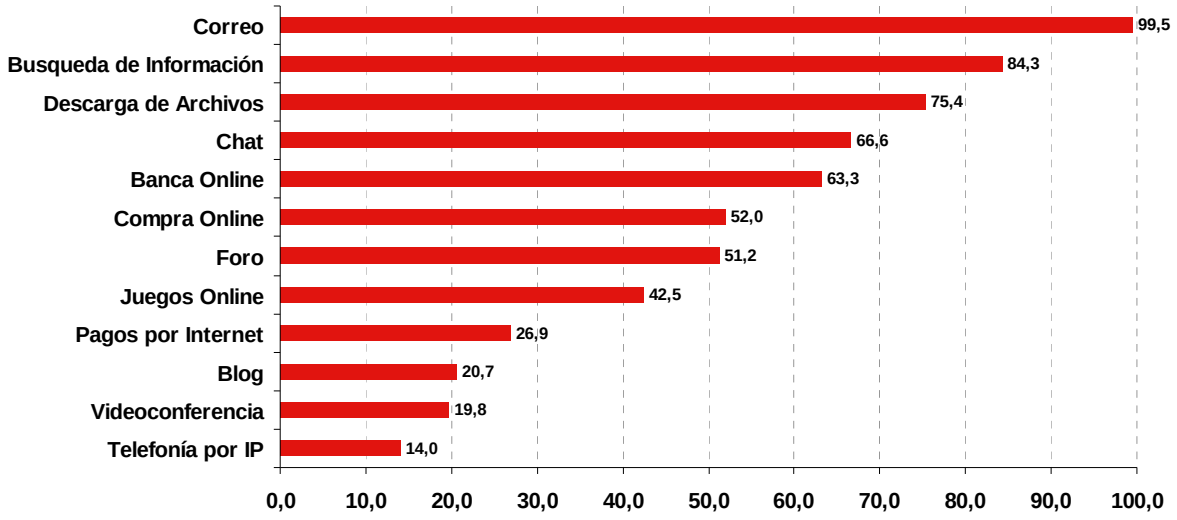
De este modo, el 60,2% dedica más de 5 horas semanales a Internet desde el hogar. Como también se aprecia en el Gráfico 12, el uso intensivo se relaciona con el acceso doméstico, pues fuera del hogar la intensidad tiende a situarse por debajo de las 5 horas semanales. Así, el 76,3% de los individuos se conecta desde otro punto de acceso menos de 5 horas a la semana y sólo el 7,3% se conecta a Internet durante más de 40 horas a la semana desde una ubicación distinta a su domicilio habitual.

Dado que el estudio mide, como se expone en el capítulo correspondiente, la presencia de malware en los ordenadores domésticos, es importante resaltar que estos ordenadores representan el vehículo principal de navegación para los encuestados tanto por frecuencia como por intensidad.

5.4 Servicios utilizados

En el siguiente gráfico se presenta el porcentaje de utilización de los distintos servicios que ofrece Internet ordenados de forma descendente. En dicho Gráfico 13 se observa que la utilización de servicios como el correo electrónico, la búsqueda de información y las descargas de archivos tienen una implantación generalizada: en todos los casos, mayor del 75% y casi el 100% en el caso del correo electrónico. Otros servicios que ofrece Internet como la banca electrónica y las compras online muestran también una considerable penetración (más del 50%).

Gráfico 13: Servicios de Internet utilizados (%)



Fuente: INTECO

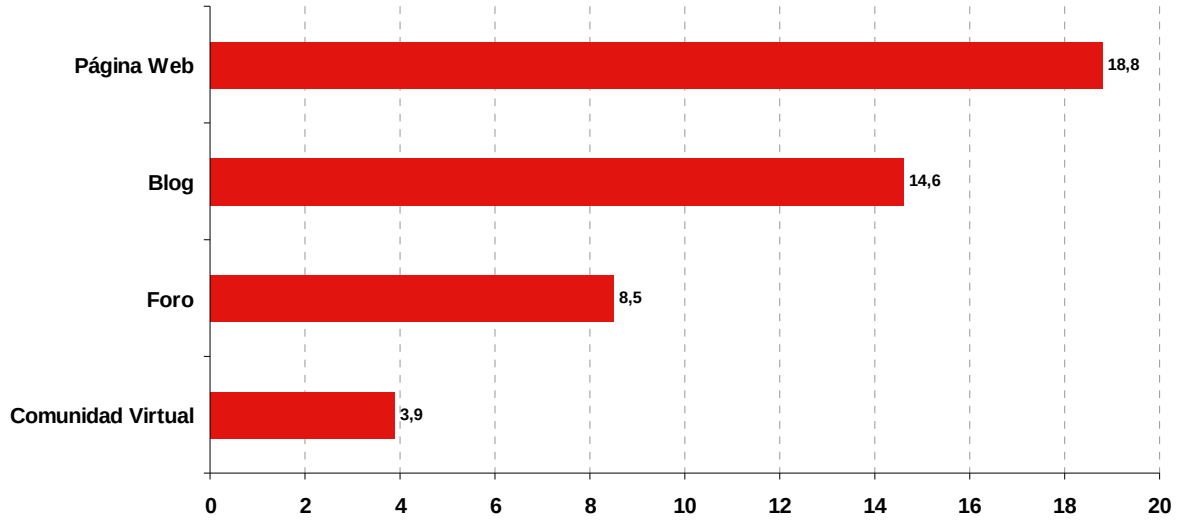
En el otro extremo, como servicios con una menor frecuencia de uso destacan: los pagos por Internet (transferencias realizadas para el pago de subastas, donativos, u otro tipo de

servicios mediante sistemas específicos habilitados al efecto), los blogs o diarios electrónicos y la videoconferencia, que no obstante son utilizados por 1 de cada 5 usuarios.

Es destacable también el uso de servicios de telefonía IP por un 14% de los usuarios.

Con respecto a la administración de servicios online, el 30,8% de los usuarios ya están implicados en labores de administración de algún servicio en Internet. Administrar una web es ya parte de los hábitos de un 18,8% de los panelistas y un blog del 14,6%; foros y comunidades virtuales quedan bastante por detrás.[6] A lo largo de las siguientes oleadas se realizará un seguimiento de estos datos, que permitirán pronosticar las vías de desarrollo de la Red y las posibles consecuencias que esto tendrá en la prestación del servicio por parte de los proveedores de Internet (ISP)

Gráfico 14: Servicios de Internet administrados (%)



Fuente: INTECO

6

Pagina Web: Documento multimedia que puede contener tanto texto como imágenes, sonidos o videos. Es la base de los contenidos publicados en Internet. Su principal característica es la posibilidad de incluir enlaces a otras páginas Web, a otros lugares de la misma página, imágenes, sonidos, etc. conformando con ello la Red (World Wide Web).

Blog: Página Web actualizada periódicamente que recopila -en orden cronológico inverso-, texto, artículos o historias de diversos tipos: tecnológicos, seguridad, personales, económicos, etc. Los blog suelen permitir a los visitantes hacer comentarios al autor, publicándose estos de manera inmediata y así mantener un diálogo.

Foro: Servicio de Internet en el que los usuarios mantienen conversaciones respecto a un tema. Si el foro tiene como base una página Web, permite a los usuarios publicar sus comentarios de manera inmediata, y responder a otros.

Comunidad Virtual: Grupo de personas que comparten información comunicados por medio de Internet. Los participantes tienen un interés en común o afición que sirve de base para la comunidad.

5.5 Uso de Internet desde el hogar

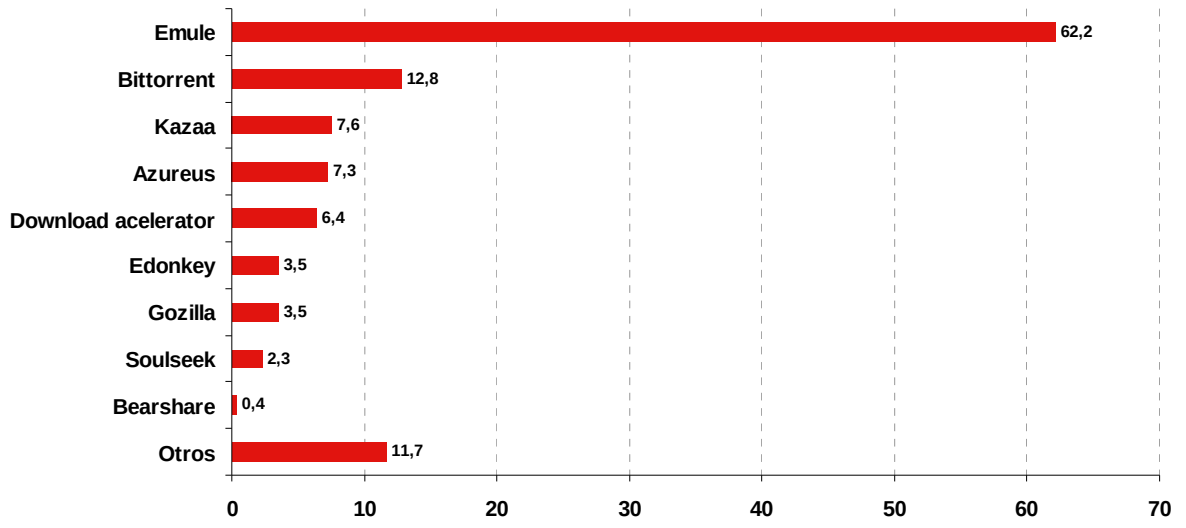
5.5.1 Sistemas operativos

La penetración del sistema operativo Microsoft Windows en sus diferentes versiones y modalidades es prácticamente absoluta (97%) en los ordenadores de acceso a Internet de los usuarios del estudio. Un porcentaje del 2% se reparte equitativamente entre los sistemas basados en Apple Mac OS y GNU/Linux. No obstante, un 1% declara desconocer el sistema operativo instalado en su ordenador.

5.5.2 Programas de descargas

Como se ha visto en el Gráfico 13, un 75,4% de los usuarios utiliza servicios de Internet relacionados con la descarga e intercambio de archivos; eMule destaca como el programa de descarga más utilizado por estos: 6 de cada 10 panelistas indican que lo usan (Gráfico 15). En segundo lugar en términos porcentuales se sitúa Bittorrent (12,8%) que sumados al porcentaje de los que usan Azureus (7,3%), que también utiliza el protocolo[7] de Bittorrent, indica que 1 de cada 5 usuarios (20,1%) utilizan este sistema de intercambio alternativo.

Gráfico 15: Programas utilizados para el intercambio de archivos (%)



Fuente: INTECO

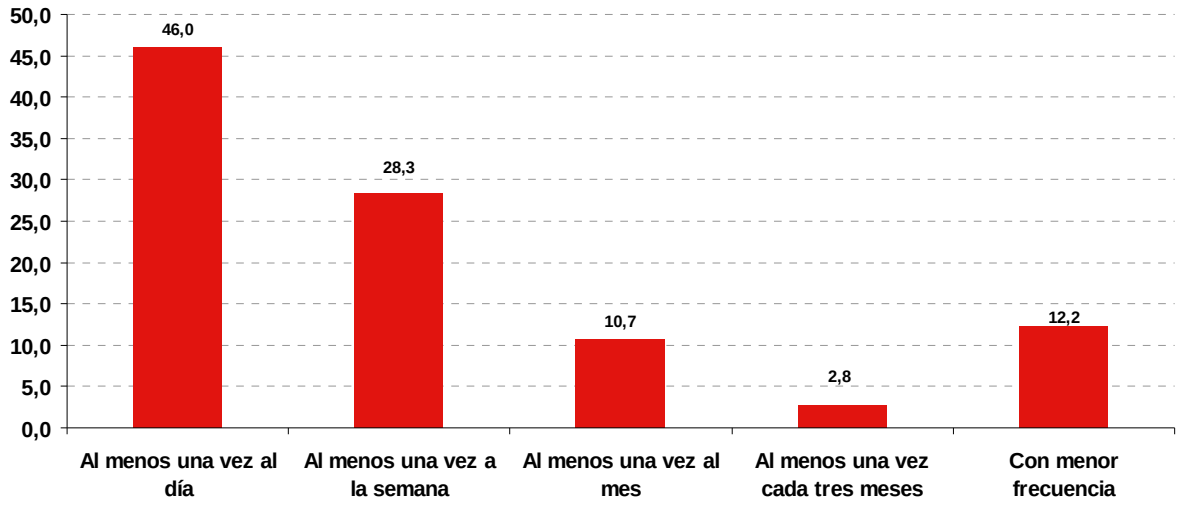
5.5.3 Terminal desatendido y en funcionamiento

La elevada penetración de algunos de estos programas de intercambio de archivos puede explicar el hecho de que el 46,0% de los usuarios dejen desatendido y sin vigilancia su

[7] Conjunto de reglas que determinan las características del intercambio de datos en las comunicaciones entre los actores de la Red.

ordenador principal de acceso a Internet desde casa, al menos una vez al día (Gráfico 16). Esto, sumado a la elevada penetración de la banda ancha, sugiere un ritmo de descargas intenso. Dicha conclusión se corresponde con el perfil de usuarios activos en la red y equipados para servirse de los servicios avanzados de Internet.

Gráfico 16: Usuarios que dejan el ordenador conectado descargando sin vigilancia (%)

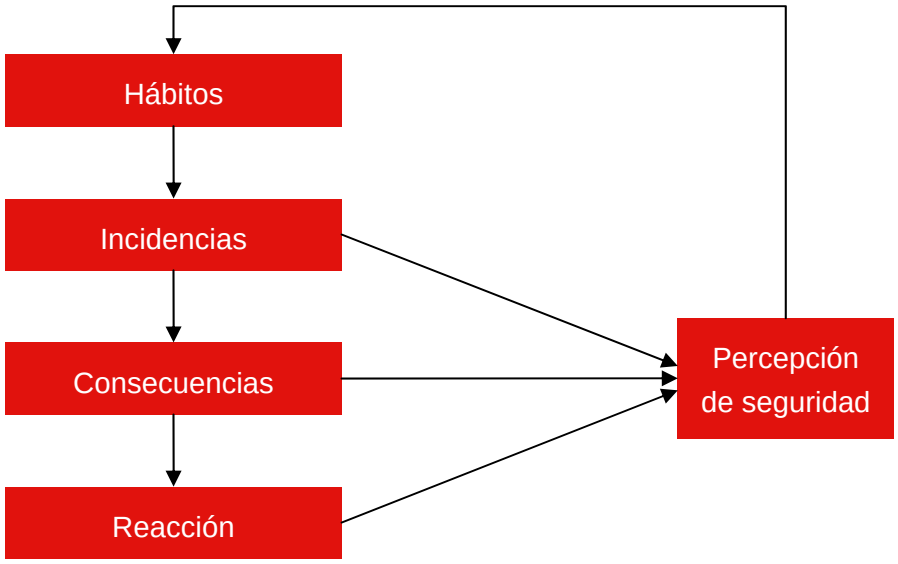


Fuente: INTECO

6 HÁBITOS DE SEGURIDAD EN INTERNET

En este bloque, se estudia la relación entre los hábitos de prevención en el uso de Internet y su efecto en la percepción de seguridad de los usuarios de Internet españoles. Dicha relación se ha analizado conforme al siguiente modelo (Gráfico 17), que ilustra un proceso secuencial con distintas fases, haciendo especial énfasis en la potencial percepción de seguridad hacia Internet.

Gráfico 17: Diagrama relacional de hábitos-percepción de seguridad



Fuente: INTECO

De acuerdo con la secuencia presentada en la figura, los hábitos de prevención en el uso de Internet y la percepción de seguridad que se derivan de ellos están vinculados mediante un proceso de retroalimentación: los hábitos acaban influyendo en los niveles de seguridad percibidos y estos producen modificaciones y correcciones en los hábitos futuros.

El modelo se basa en que la modificación de los hábitos de prevención para mejorar la seguridad está condicionada por dos principios básicos:

- **La existencia de incidencias visibles** que exijan acciones de corrección. En este sentido, potenciales incidencias graves que no sean conocidas por el usuario no producirán ningún tipo de corrección en los hábitos de prevención. Esta circunstancia se explora con mayor detalle más adelante en el epígrafe 8 Incidencias de seguridad: situación real de los equipos de los hogares españoles,

al hablar de la matriz de incidencias-confianza. En este apartado se destaca como una de las tendencias actuales de generación de códigos maliciosos es la ocultación del código a ojos del usuario.

- Las **consecuencias derivadas** de la falta de incorporación de medidas de seguridad. Esto es, cuando el usuario se enfrenta activamente a las consecuencias derivadas de sus hábitos de prevención y tiene que tomar medidas correctoras –en ocasiones drásticas: como formatear el disco duro, afrontar daños en el hardware o reinstalar el sistema operativo– la percepción de seguridad queda notablemente afectada. Esto producirá un mayor reajuste en los hábitos de prevención hacia prácticas más seguras en el uso de Internet.

Además, el efecto de los hábitos de prevención en la percepción de seguridad está condicionado por:

- El tipo de **incidencias** de seguridad que se derivan de los hábitos de prevención;
- Las **consecuencias** que estas incidencias tienen tanto en el software como hardware desde el que se accede a Internet; y
- La **reacción** llevada a cabo por el usuario para corregir o reparar los daños sufridos que retroalimenta el sistema al causar que el usuario aumente nuevamente su percepción de seguridad.

El modelo presentado en la figura anterior implica una secuencia temporal que se analizará mejor cuando, en próximas oleadas del estudio, se disponga de los datos procedentes de nuevas tomas de información longitudinales, a los que se aplicarán técnicas estadísticas que contemplen la temporalidad (modelos causales o modelos de crecimiento).

No obstante, el análisis del modelo con datos procedentes de diseños correlacionales –el caso de este informe– puede permitir explorar algunas hipótesis de interés que posibiliten una delimitación más precisa de las variables más relevantes en cada fase del proceso.

A continuación son presentados los principales indicadores obtenidos sobre los hábitos de prevención, el tipo de incidencias, sus consecuencias en el software y hardware de acceso a Internet, las acciones de respuesta en materia de seguridad derivadas de las incidencias y el nivel de seguridad percibido por el usuario.

6.1 Medidas de seguridad

La Tabla 8 muestra el porcentaje de usuarios de Internet que utiliza cada uno de las medidas de seguridad analizadas, así como la intención de incorporarlas a sus hábitos de

prevención en los próximos tres meses en caso de no utilizarlas en el momento actual. Estas se presentan ordenadas por su penetración de forma descendente.

Ahora bien, dentro del listado total de medidas de seguridad se pueden distinguir dos familias de medidas, según si la intervención del usuario tiene carácter pasivo o activo (medidas automatizables o no automatizables).

Por lo general, los usuarios se decantan por medidas de seguridad de carácter automatizable: son medidas que operan de forma automatizada en los equipos, esto es, no suelen requerir del usuario una atención específica. Son configurables determinadas acciones como, por ejemplo, conseguir la automatización de las actualizaciones de las medidas cada vez que el usuario se conecta a Internet. Esto facilita una gestión automatizada de las medidas que redunda en una mayor comodidad para el usuario y una mayor disponibilidad de tiempo.

Tabla 8: Equipamiento y buenas prácticas de seguridad (%)

Medidas de seguridad	*Dispone*	*Previsión para los próximos 3 meses*
Programas antivirus.	94,5	95,8
Cortafuegos	76,0	79,3
Bloqueo de ventanas emergentes	69,5	73,5
Eliminación de archivos temporales y cookies	62,0	68,6
Anti-spam	56,8	64,3
Antiespías	56,8	64,1
Contraseñas (equipo y documentos)	51,6	57,0
Actualizaciones de seguridad del SO	50,1	62,2
Copia de seguridad de archivos importantes	34,2	52,7
Partición del disco duro	31,3	38,3
Copia de seguridad del disco de arranque	22,8	37,3
Programas de control parental	9,2	12,9
Encriptación de documentos	8,5	13,1
Ninguna medida de seguridad	0,7	-

Fuente: INTECO

6.1.1 Seguridad Pasiva

La lista de **medidas automatizables** incluye: Programas antivirus, cortafuegos o firewalls, programas anti-correo basura, programas anti-espía, programas de bloqueo de ventanas emergentes, actualizaciones de seguridad del sistema operativo y programas de control parental.

La instalación de programas antivirus en los usuarios frecuentes de Internet en el hogar mayores de 15 años es prácticamente universal (94,5%). Además, se prevé que en tres meses el porcentaje de usuarios que disponen de antivirus alcanzará el 95,8% del total.

En segundo lugar, la medida de seguridad más utilizada son los programas cortafuegos (76%). En el tercer lugar del escalafón aparecen otras medidas de seguridad, como bloqueo de ventanas emergentes (69,5%), eliminación de archivos temporales y cookies (62%), programas anti-correo basura y anti-espía (56,8% en ambos casos) y actualizaciones de seguridad del sistema operativo (50,1%).

6.1.2 Seguridad Activa

La lista de **medidas de seguridad no automatizables**, que exigen un comportamiento más activo por parte del usuario, está formada por: Encriptación de documentos, contraseñas, copia de seguridad del disco de arranque, copias de seguridad de archivos importantes, eliminación de archivos temporales o cookies y partición del disco duro. Aunque hoy en día alguna de estas medidas podrían ser automatizadas, la tendencia general, a nivel de usuario doméstico, es realizarlas de modo manual, como por ejemplo sucede en el caso de las copias de seguridad.

Este tipo de medidas de seguridad pasiva son menos frecuentes y, en general, no superan el 50% de penetración. Este dato refleja que una parte de los usuarios busca modos de seguridad que no impliquen su acción constante ni interfieran la navegabilidad.

Finalmente, cabe destacar que solamente hay algo menos de un 1% del total de usuarios que no utilizan ninguna de estas medidas y buenas prácticas de seguridad, ni a nivel activo ni pasivo y que, por ello, a priori están totalmente desprotegidos cuando acceden a Internet.

6.1.3 Previsiones para los próximos tres meses

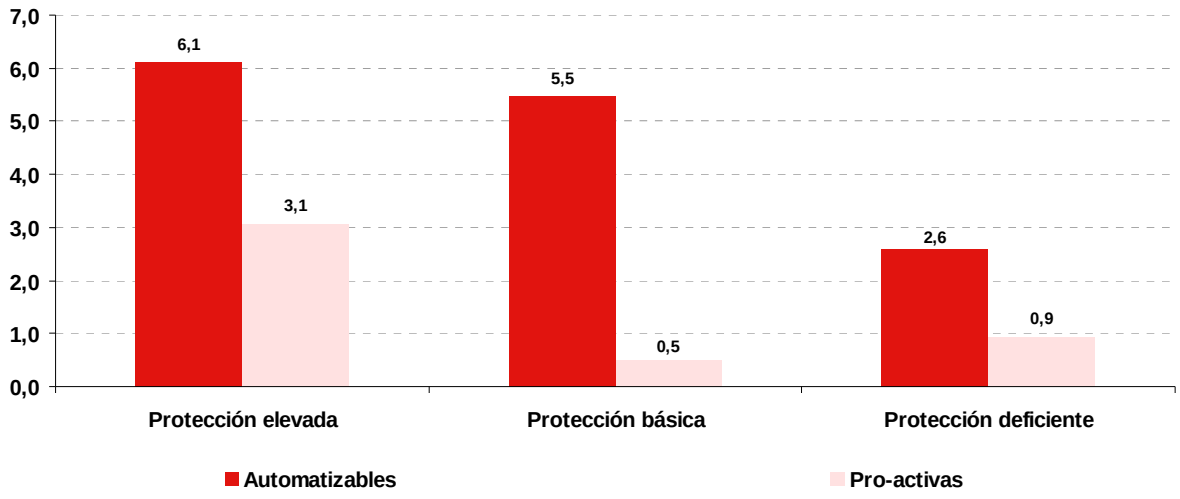
En cuanto a las previsiones de actuación de los usuarios para los próximos 3 meses, las copias de seguridad de los archivos importantes, la copia de seguridad del disco de arranque y la actualización del Sistema Operativo son las medidas que presentan un potencial de crecimiento mayor, con cifras que superan el 10% en el corto plazo. Respectivamente, incrementan sus índices de penetración en un 18,5%, un 14,5% y un 12,1%.

Diferenciales por encima del 5%, y con una previsión media de crecimiento del 7%, también significativos, se prevén para: Eliminación de los archivos temporales y cookies, instalación del programas anti-spam, instalación de programas anti-espías, utilización de contraseñas en el equipo y los documentos y la partición del disco duro.

Esto sugiere futuras acciones que cambien el comportamiento y conducta hacia un uso más seguro y mejoren el estado general de seguridad. En concreto, las acciones con mayor previsión de crecimiento se dirigen dentro del concepto de "seguridad proactiva del usuario". No obstante, en próximas oleadas del panel se contrastará si las previsiones que hacen los usuarios sobre la implementación de medidas de seguridad que conllevan una mayor implicación por el usuario se llevan a término.

Al analizar la distribución conjunta de las medidas automatizables[8] (pasivas) y no automatizables[9] (proactivas) pueden observarse claramente tres tipos de usuarios (Gráfico 18). Un primer grupo, declara utilizar tanto la protección proactiva como la automatizable; un segundo grupo, utiliza preferentemente protección automatizable; y, finalmente, un tercer grupo presenta niveles muy bajos en ambos tipos protección.

Gráfico 18: Número de medidas de seguridad utilizadas según el grado de acción requerido



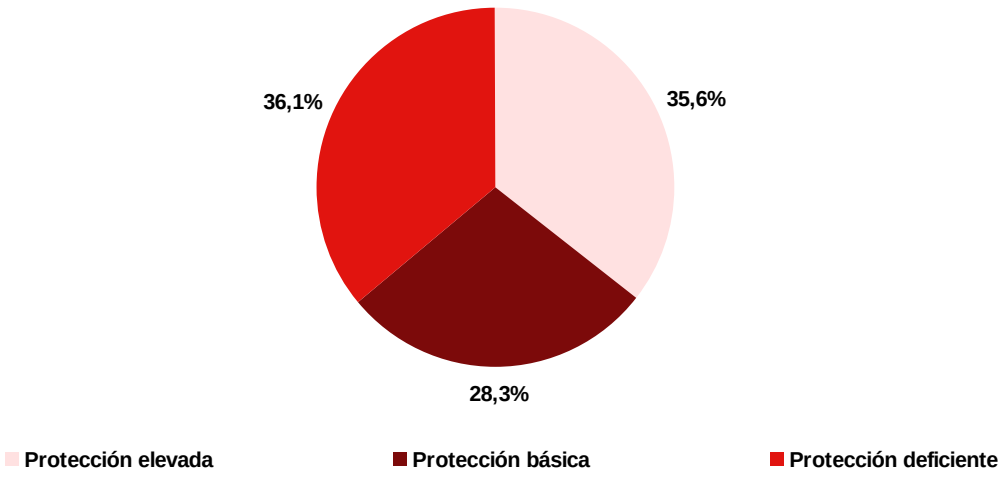
Fuente: INTECO

El Gráfico 19 presenta la distribución de los usuarios dentro de los segmentos asignados según su nivel de seguridad. Es de destacar que un 36,1% de los hogares pertenecen al grupo de usuarios con una utilización muy baja de de ambos tipos de dispositivos.

[8] **Medidas automatizables:** Programas antivirus, cortafuegos o firewalls, programas anti-correo basura, programas anti-espía, programas de bloqueo de ventanas emergentes, actualizaciones de seguridad del sistema operativo y programas de control parental.

[9] **Medidas no automatizables:** Encriptación de documentos, contraseñas, copia de seguridad del disco de arranque, copias de seguridad de archivos importantes, eliminación de archivos temporales o cookies y partición del disco duro

Gráfico 19: Distribución de los usuarios según su nivel de seguridad (%)



Fuente: INTECO

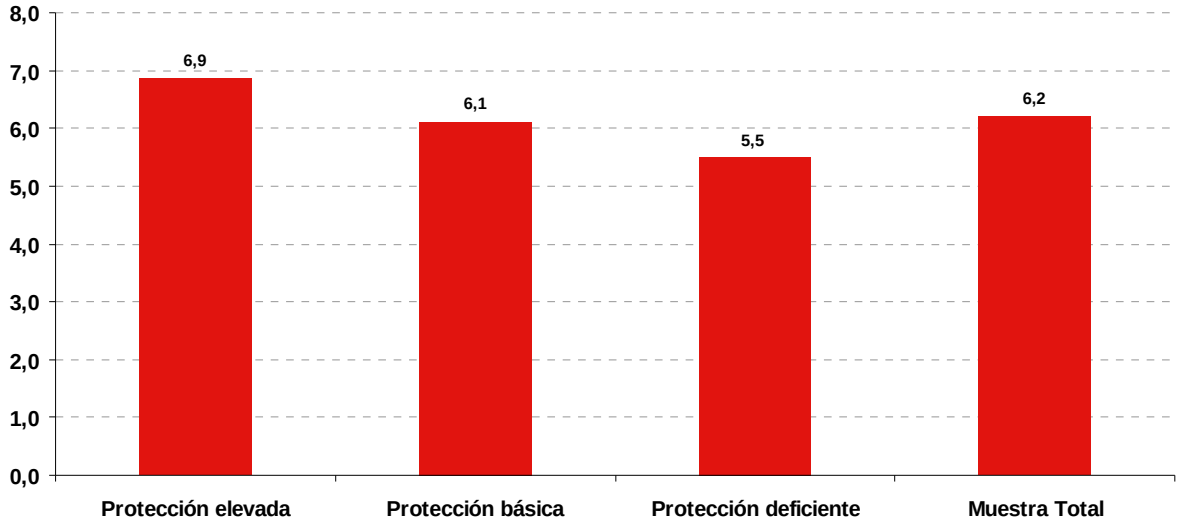
Respecto al uso de los servicios ligados a Internet se observa una clara relación característica entre los usuarios. Aquellos que afirman utilizar un mayor número de dispositivos de seguridad son los usuarios que mayor número de servicios de Internet utilizan (Gráfico 20).

Esta relación entre intensidad de uso de los servicios de Internet y dispositivos de seguridad sugiere una tendencia a incrementar el nivel de seguridad conforme se van incorporando nuevos servicios.

Con respecto a la utilización diferencial de algún tipo de servicio de Internet, no se observan grandes diferencias. En todos los servicios analizados, el porcentaje de usuarios que lo utilizan es mayor en los usuarios con seguridad elevada, algo menor en usuarios con seguridad básica y más bajo aún en usuarios con deficiencias de seguridad.

No obstante, hay que matizar este resultado con el hecho de que un 36% de los usuarios, aquellos con deficiencias de seguridad, utilizan pocos dispositivos de seguridad automatizables y no automatizables Aún así, muestran una utilización media de 5,5 servicios de Internet. Esto indica un riesgo para el sistema, ya que son usuarios de moderada intensidad, con un elevado grado de desprotección en sus equipos de acceso desde el hogar.

Gráfico 20: Número de servicios de Internet utilizados según el nivel de seguridad del usuario



Fuente: INTECO

6.2 Periodicidad de las actualizaciones de las medidas de seguridad

En la Tabla 9 se recogen los hábitos de "puesta al día" de algunos de los programas de prevención, detección y eliminación (antivirus, anticorreo basura, etc.).

De acuerdo con lo declarado en la encuesta, podemos observar que las herramientas de seguridad del sistema se actualizan mensualmente en su mayor parte (83,4%), y destaca un porcentaje residual, en torno al 8,4%, que o bien no se actualiza nunca o tan sólo una vez al año.

Como se ve en la Tabla 9, la gran mayoría de los hogares, un 83,4%, actualiza sus dispositivos de seguridad al menos una vez al mes.

Tabla 9: Actualización de las herramientas de seguridad (%)

Periodicidad	%
Más de una vez al mes	63,7
Una vez al mes	19,7
Una vez cada tres meses	6,1
Una vez cada seis meses	2,1
Una vez al año	2,2
Con menor frecuencia o nunca	6,2

Fuente: INTECO

Por otro lado la siguiente tabla permite completar la información presentada. La mayoría de los equipos desde los cuáles se accede a Internet desde el hogar se analizan en busca de posibles virus en un 71,7% de los casos al menos mensualmente (Tabla 10)

Es decir, a partir de las declaraciones de los entrevistados, puede afirmarse que el seguimiento de las medidas básicas de seguridad individual es razonable para el conjunto, y que las vulnerabilidades se concentran en determinados grupos o segmentos. Así pues, pueden avanzarse dos debilidades del sistema:

- Una procedente de las amenazas "invisibles" para el usuario, como las que detecta el programa de escaneo instalado en los equipos informáticos de los panelistas. Estas son amenazas no detectadas por los usuarios en ningún momento y por tanto no son conscientes de sus consecuencias. Esto se comprueba en el epígrafe 8 Incidencias de seguridad: situación real de los equipos de los hogares españoles, donde se señala que una de las tendencias actuales de creación de códigos maliciosos es la ocultación del código de manera que pueda continuar realizando la tarea asignada durante el máximo tiempo posible.

- Otra con origen en el segmento de usuarios menos prudentes y que terminará por afectar a otras partes de sistema general debido a la naturaleza interactiva y social del fenómeno Internet (correo electrónico, intercambio de archivos y programas, etc.).

Tabla 10: Frecuencia de análisis del ordenador con el programa antivirus (%)

Periodicidad	%
Varias veces al día	5,5
Varias veces a la semana	26,0
Varias veces al mes	40,2
Varias veces al año	17,7
Con menor frecuencia o nunca	5,1
No dispone de antivirus	5,5

Fuente: INTECO

6.3 Motivos alegados para no utilizar las distintas medidas de seguridad

Como se observa en la Tabla 11, las principales razones para no incorporar las medidas de seguridad, según las declaraciones de los panelistas encuestados, son el desconocimiento de la medida o la percepción de que ésta es innecesaria. Ambas respuestas, sin embargo, reflejan que es la inconsciencia respecto a los riesgos y la falta

de información sobre las soluciones pertinentes lo que explicaría una menor protección frente a amenazas a la seguridad de los equipos informáticos.

6.3.1 No son necesarias

Exceptuando los programas antivirus y los cortafuegos, en el resto de las medidas, más del 50% de los usuarios consideran la "no necesidad" como el motivo para no aplicarla. Son muy significativos algunos de los datos que refieren las opiniones de los usuarios: las medidas que consideran menos necesarias son los programas de control parental (77,3%), las contraseñas (70,6%) y las copias de seguridad (67,5%). Curiosamente como se analizó en la Tabla 8, el porcentaje de usuarios que tienen previsto realizar copias de seguridad en los próximos 3 meses crecerá 18 puntos porcentuales en dicho período de tiempo.

Así, las medidas más valoradas según esta clasificación de motivos son los antivirus, cortafuegos y programas anti-espía, siendo las medidas donde el porcentaje de usuarios que creen que son innecesarias es menor. Con todo, un 24,2% de los usuarios que no utilizan programas antivirus, un 25% que no tiene cortafuegos y un 31,7% que no usa programas anti-espía, alegan esta razón.

6.3.2 Desconocimiento

El segundo motivo más frecuente aducido para no aplicar una medida es, en general, que el usuario desconoce la propia medida. Un 35,7% de los usuarios que declaran no utilizar cortafuegos alegan no conocer dichos programas. Un 28,6% refiere de modo similar en cuanto a la encriptación de documentos y se encuentran en porcentajes cercanos al 25% sobre los programas antiespía, programas de bloqueo de ventanas emergentes o particiones del disco duro.

6.3.3 Entorpecimiento del funcionamiento/navegabilidad

Entre los motivos se vislumbra uno que podría enmarcarse entre los más frecuentes y los menos esgrimidos: el factor de entorpecimiento del funcionamiento/navegabilidad. Esta es la razón más frecuente en el caso del 5,5% de los no usuarios de programas antivirus (con un 38,1%) y se encuentra entre las 3 más frecuentes para los no usuarios de programas cortafuegos, programas de bloqueo de ventanas emergentes, programas anti-correo basura y anti-espía o utilización de contraseñas.

6.3.4 Otros Motivos

Otros motivos menos frecuentes aducidos para no aplicar las medidas de seguridad son el precio, que entorpecen el funcionamiento o la desconfianza del usuario en la medida. Algunos usuarios consideran las medidas ineficaces, pero no por ello innecesarias.

Tabla 11: Motivos aducidos para no aplicar medidas de seguridad (%)

Medidas de seguridad	No sé lo que es	Porque es innecesario	Precio	Entorpecen	Desconfío	Ineficaces
Programas antivirus.	4,7	24,2	16,7	38,1	5,9	10,4
Cortafuegos	35,7	25,0	8,1	22,6	3,9	4,7
Bloqueo ventanas emergentes	23,7	34,8	8,7	20,9	5,0	6,9
Eliminación archivos temporales y cookies	18,8	59,4	5,2	7,2	3,6	5,8
Anti-spam	14,8	42,5	11,5	12,7	6,7	11,8
Anti-espía	25,7	31,7	11,6	14,5	9,2	7,3
Actualizaciones seguridad SO	21,7	47,0	10,2	9,7	6,2	5,2
Contraseñas (equipo y documentos)	8,7	70,6	3,9	8,4	3,1	5,3
Copia seguridad archivos importantes	12,9	67,5	5,3	6,2	2,9	5,2
Partición del disco duro	24,5	56,6	3,8	7,2	3,0	4,9
Copia seguridad disco de arranque	18,4	64,0	4,3	5,9	2,9	4,5
Encriptación de documentos	28,6	56,4	4,3	5,5	3,0	2,2
Programas control parental	9,0	77,3	3,4	4,3	2,1	3,9

Fuente: INTECO

6.3.5 Análisis de grupos

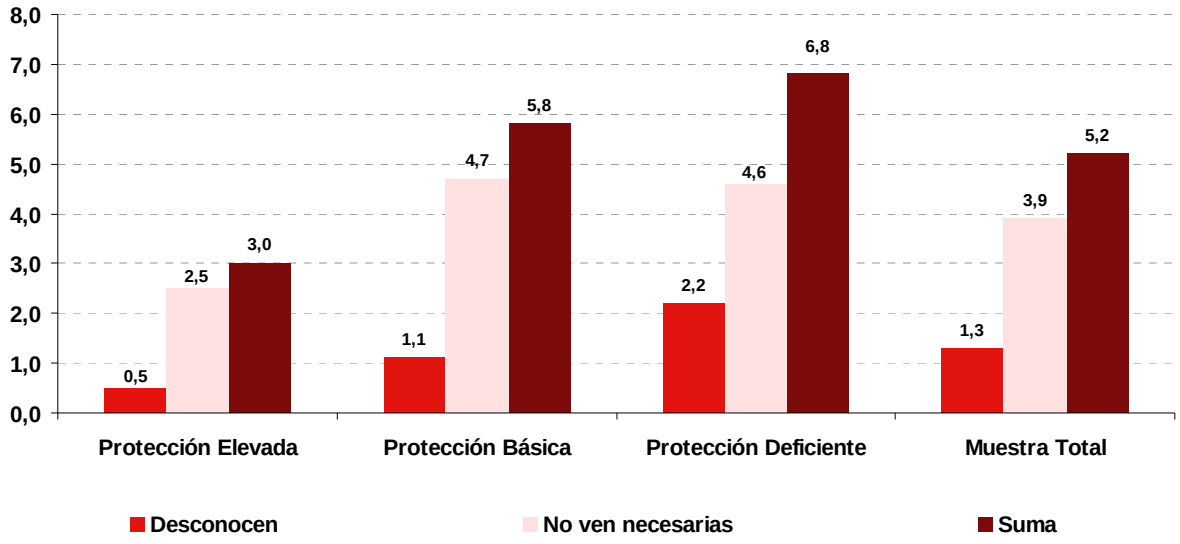
Debido a que estas medidas de protección están relacionadas entre sí (algunos usuarios utilizan preferentemente medidas pasivas pero no medidas activas), es interesante analizar de forma específica las razones por las cuales no se utilizan determinadas medidas de seguridad. Este análisis se configurará según los grupos ya analizados con protección elevada (activa y pasiva), protección básica (solo pasiva), y con protección deficiente.

Específicamente, en relación con las dos respuestas más frecuentes para no utilizarlas (‘no sé lo que es’ y ‘no lo veo necesario’), existen claras diferencias entre los grupos y como muestra el Gráfico 21, se produce un hecho lógico. El grupo de usuarios con protección deficiente contesta en mayor medida, que los grupos de protección básica y elevada, que la principal razón para no utilizar una medida es que no saben lo que es o no la consideran necesaria.

Este desconocimiento acerca de los riesgos y la falta de información sobre soluciones pertinentes es mayor entre los usuarios menos protegidos. Se apunta al papel de la Administración como difusor de una “cultura de seguridad de la información”. En concreto, como transmisora de información pertinente y actualizada sobre las posibilidades de

funcionamiento de herramientas de seguridad y buenas prácticas que no estén extendidas entre los usuarios de Internet en el hogar.

Gráfico 21: Número de medidas de seguridad que los usuarios desconocen o no ven necesarias según grado de protección del equipo.



Fuente: INTECO

6.4 Hábitos de seguridad personales y comportamiento en el uso de Internet

Si bien el sistema, como se ha indicado, presenta algunas carencias en cuanto a la presencia de equipamiento de seguridad, el aspecto que más riesgo comporta para el conjunto de los usuarios se centra en los hábitos de ciertos segmentos, que suponen epidemiológicamente un riesgo general para todos los usuarios de la Red.

El análisis factorial de los comportamientos relacionados con la seguridad ha puesto de manifiesto que existen dos tipos de comportamiento de los usuarios, atendiendo fundamentalmente a dos características que inciden de forma clara en el nivel de riesgo de todo el sistema.

- Por una parte, aquellas prácticas que comportan riesgo para los equipos desde los que se accede, por ejemplo, abrir correos de desconocidos, modificar las medidas de seguridad para acceder a páginas web, etc. Estos comportamientos pueden hacer vulnerables y comprometer la seguridad de los equipos desde los que se realizan estas prácticas. Así, no solo son la puerta de entrada de código malicioso a dichos equipos, sino también al resto del Sistema.

- Por otra parte, los comportamientos solidarios que ayudan a la protección del resto de usuarios, como: por ejemplo, la comprobación de la existencia de virus previa al envío de archivos y documentos, o la notificación de la existencia de un virus tras la recepción por parte de otro usuario. Este comportamiento solidario puede revertir positivamente en el nivel de seguridad global del Sistema.

En principio, ambos comportamientos son independientes entre sí, si bien pueden darse combinados en unas mismas personas. Cada uno de estos factores explicativos del comportamiento se asocia, o viene descrito, por una serie de hábitos característicos: que se recogen en las siguientes tablas: Tabla 12 y Tabla 13.

Como nota general, se observa que los comportamientos responsables son mucho más frecuentes que los comportamientos imprudentes, que son desarrollados con regularidad por un 10% de los usuarios. Es decir, existe una concentración del riesgo para el sistema en estados muy determinados del mismo. Pocos usuarios "imprudentes" realizan las acciones que son causa de la inseguridad existente del Sistema

Tabla 12: Hábitos definitorios del componente "Imprudencia" (%)

Hábitos definitorios del componente "Imprudencia"	Siempre o Muchas veces
Abro correos de remitentes desconocidos si parecen interesantes	9,7
Doy mi dirección de e-mail cuando me lo piden aunque desconozca el destinatario	9,1
Agrego contactos al Messenger aunque no sepa de quién se trata	9,4
Pulso los enlaces que aparecen en las conversaciones del Messenger, sin preguntar de que se trata	6,2
Si es necesario modifico las medidas de seguridad del ordenador para poder acceder a servicios o juegos que me interesan	11,4
Comparto software sin comprobar si está o no infectado (redes p2p)	11,2

Fuente: INTECO

Si bien algunas prácticas de naturaleza solidaria, como la notificación de nuevos virus, puede desembocar en ciertos casos en la difusión de bulos infundados sobre seguridad, en general, corresponde empíricamente, junto con el resto de hábitos, con una tipología de usuario de Internet atento a las necesidades de seguridad tanto propias como ajenas, que acaba dando buenos resultados en cuanto a protección.

Es destacable el hecho de que **casi el 70% de los usuarios de Internet se ponen en contacto con el remitente de correos electrónicos con archivos infectados cuando reciben e-mails con ese contenido.** Este tipo de prácticas contribuye al control de las infecciones y limita los daños causados por el malware.

Tabla 13: Hábitos definitorios del componente "Solidario" (%)

Hábitos definitorios del componente "Solidario"	Siempre o Muchas veces
Alerto sobre aquellas páginas que conozco y hacen un uso fraudulento de los datos del usuario	39,9
Cuando recibo una notificación sobre la existencia de un nuevo virus se lo comunico a la gente que conozco	34,3
Cuando veo que alguien no tiene actualizados sus programas de seguridad le recomiendo que los revise e instale las últimas versiones	50,3
Si envío un archivo por mail compruebo que no contenga ningún virus.	67,1
Cuando recibo un mail de un conocido con un archivo infectado se lo comunico al remitente	69,7

Fuente: INTECO

7 PERCEPCIÓN DE SEGURIDAD, INCIDENCIAS Y VULNERABILIDADES

En este capítulo se detallan los resultados del análisis de incidencias en los hogares. Se analizan las incidencias más comunes de seguridad en el equipamiento de acceso a Internet en el hogar y las consecuencias derivadas. Se propone una tipología de usuarios en función de sus niveles de prudencia y solidaridad, para avanzar hacia la caracterización sociodemográfica, actitudinal, de hábitos de uso y seguridad para cada tipología.

7.1 Tipo de incidencias y tiempo transcurrido

La Tabla 14 presenta la distribución de frecuencias acumuladas en distintos intervalos de tiempo, de las principales incidencias de seguridad detectadas por los usuarios en el ordenador principal con el que acceden a Internet. El análisis se realiza para el momento en que se ha producido la última incidencia de seguridad.

Tabla 14: Incidencias de seguridad detectadas por los usuarios. (En qué momento se produjo la más reciente) (%)

Incidencias	En la última semana	En el último mes	En los últimos tres meses	En el último año	En alguna ocasión	Nunca
Virus Informáticos	7,1	17,4	29,9	52,8	79,4	20,6
Intrusiones en otras cuentas de servicio web distintas del correo electrónico[10]	2,4	5,5	9,1	13,2	18,2	81,8
Fraudes o robos relacionados con cuentas bancarias online[11]	1,0	2,6	4,3	5,8	8,2	91,8
Fraudes o robos relacionados con tarjetas de crédito[12]	1,0	2,5	3,9	5,7	9,1	90,9
Recepción de correos no solicitados / deseados (spam)	66,1	76,7	82,0	86,5	89,1	10,9
Obtención fraudulenta de sus datos personales[13]	5,1	9,4	12,9	16,3	19,9	80,1
Robo de ancho de banda Wifi	2,4	5,3	7,9	10,7	13,8	86,2

Fuente: INTECO

La incidencia más frecuente para todos los intervalos temporales es la recepción de correo no deseado (**spam**). Sólo en la última semana un 66,1% de los hogares declara haber

[10] **Intrusiones en otras cuentas de servicio web distintas del correo electrónico**: el usuario ha sido victima de robo de cuentas de usuario en portales web, foros u otros servicios distintos del correo electrónico.
[11] **Fraudes o robos relacionados con cuentas bancarias online:** la victima ha sido objeto del fraude denominado phishing, en el cual alguien obtiene las claves de las cuentas bancarias del usuario y las utiliza para realizar transferencias monetarias.
[12] **Fraudes o robos relacionados con tarjetas de crédito:** el usuario es victima de robo de los números de sus tarjetas de crédito y estas se utilizan ilícitamente para realizar compras online.
[13] **Obtención fraudulenta de sus datos personales:** el usuario constata que algunos datos personales sensibles están en poder de entidades a las que él no se las ha suministrado.

sufrido la recepción de correo no solicitado/deseado. El porcentaje de hogares que ha sufrido esta misma incidencia es en los últimos tres meses de un 82%, y en el último año un 86,5%. Un 89,1% de los hogares manifiestan haber sufrido en algún momento una incidencia de este tipo. Menos de un 11% de los encuestados declaran no haber recibido nunca ningún mensaje de correo no deseado.

A este tipo de incidencia le siguen otras muy frecuentes. La presencia de **virus** informáticos, que presenta también datos significativos, un 7,1% en la última semana, casi un 30% en los últimos tres meses o un 52,8% de los hogares que señalan haber sufrido un virus en el último año. Es destacable que el 20,6% de los usuarios domésticos señalan no haber sufrido en ningún momento un virus informático.

La **obtención fraudulenta de datos personales** representa el 16,3% en el último año, los fraudes o robos de cuentas bancarias y tarjetas de crédito tienen porcentajes de incidencia menores pero muy representativos (en ambos casos cercanos al 6% en el último año).

7.2 Consecuencias para los equipos

La Tabla 15 presenta las frecuencias de las consecuencias más comunes que se derivan de las incidencias de seguridad en los equipos de acceso a Internet desde el hogar. Se observa que, de entre los usuarios que declaran incidencias, las consecuencias más habituales son el formateo del disco duro (40,4%) y la reinstalación del sistema operativo (32,7%). En conjunto, aproximadamente una tercera parte de los usuarios tuvieron consecuencias graves derivadas de las incidencias de seguridad (formateo de disco duro o reinstalación del sistema operativo) y 1 de cada 10 experimentaron daños en su equipos (hardware). Un 42,7% de los equipos no han experimentado consecuencias de consideración.

Tabla 15: Consecuencias para los equipos derivadas de las incidencias de seguridad (%)

Consecuencias	%
Formateo disco duro	40,4
Perdida de archivos	23,6
Reinstalar sistema operativo	32,7
Aparecen nuevos archivos	16,2
Perdida de privilegios de usuario	2,8
Daños en el equipo (hardware)	12,2
Ninguna consecuencia	42,7

Fuente: INTECO

Es decir, por una parte, la preocupación y el seguimiento de las recomendaciones básicas de seguridad pueden considerarse como una actitud generalizada, salvo excepciones, pero también es cierto que las incidencias graves siguen presentes. Esta doble situación

puede desembocar en un fondo de desconfianza y desorientación entre los usuarios, y es donde el papel de la Administración tiene más recorrido.

Puesto que algunas de estas consecuencias están relacionadas (por ejemplo, el formateo del disco duro y la reinstalación del sistema operativo) se han dicotomizado las consecuencias como 'sin consecuencias' y con alguna 'consecuencia grave'.

Se han considerado consecuencias graves el formateo del disco duro, la reinstalación del sistema operativo y los daños en el equipo (hardware).

El estudio sugiere que es evidente que el aumento de la seguridad en general, tanto a través de acciones sobre las medidas como de una conducta más segura suele ser fruto de incidencias o experiencias graves de seguridad.

7.3 Acciones sobre las medidas de seguridad:

Tras haberse registrado incidencias de seguridad y haber experimentado sus consecuencias, los usuarios adoptan hábitos y acciones de seguridad diversos. En este apartado se analizan las reacciones de los usuarios tras haber registrado incidencias en sus equipos. Estas reacciones se desglosan en tres categorías: cambio de las medidas de seguridad, cambio en la utilización de servicios de Internet y cambio de actitud u opiniones sobre Internet.

7.3.1 Cambios en el equipamiento

En el siguiente gráfico (Gráfico 22) se presentan los cambios efectuados en las medidas de seguridad, entre las que se contemplan los programas antivirus, programas anti-spam, programas anti-espía y programas cortafuegos. La población objetivo son aquellos usuarios que registraron alguna consecuencia grave en su equipo tras las incidencias de seguridad. Los cambios analizados en dichas medidas, como respuestas del usuario ante incidentes de seguridad graves, se centran en 4 cambios:

- Instalación por primera vez del programa.
- Actualización del software.
- Cambio de proveedor del software
- No se aplica ninguna medida

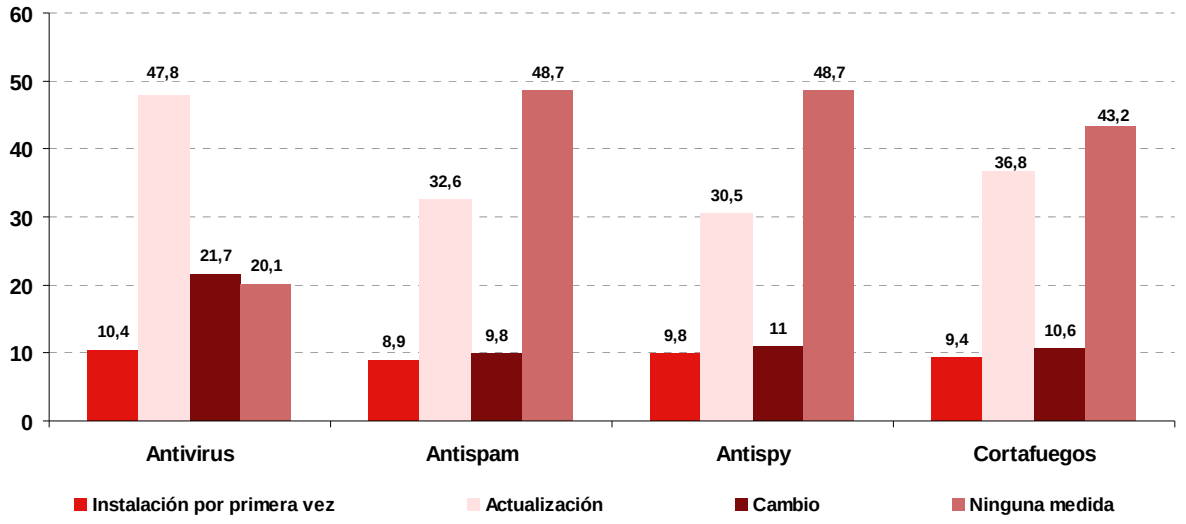
Una vez sufrida una incidencia grave de seguridad, la principal herramienta a la que se recurre y sobre la que se actúa es el antivirus. Este tipo de programas informáticos son la medida de seguridad en la que se registran los mayores cambios, tanto a nivel de actualización manual del usuario (47,8%), de cambio de proveedor de programa antivirus (21,7%) o de instalación por primera vez (10,4%).

Así las cosas, tan sólo el 20,1% dejó el programa antivirus en su estado inicial tras sufrir una incidencia grave.

Como se ha apuntado, si bien las incidencias graves derivan en la mayoría de los casos en una actuación sobre el antivirus, sin embargo el impacto de las experiencias graves es mucho menor respecto del resto de herramientas de protección y detección contempladas. Así, la mayor parte de los usuarios – en torno al 40-50% – no efectuaron acciones de cambio operativo sobre estos programas, una tercera parte los actualizó y en torno al 10% instalaron un antispam, antiespía o cortafuegos por primera vez.

Destaca también el hecho de que los programas antivirus son los que más se reemplazan tras experimentar una consecuencia grave (21,7%), lo que confirma la sospecha de que el usuario deposita en estos programas la confianza para "sentirse seguro" en mayor medida que en sus hábitos de prudencia en la Red.

Gráfico 22: Respuestas del usuario ante incidentes de seguridad graves: actuaciones sobre las herramientas de seguridad instaladas (%)



Fuente: INTECO

7.3.2 Cambios en el uso de Internet

El segundo análisis de reacciones del usuario se centra en el cambio experimentado en la utilización de los servicios de la Red tras sufrir una consecuencia grave de seguridad. Se presenta una comparativa en la distribución de los cambios en el uso de Internet motivados por las incidencias de seguridad según ha experimentado o no alguna consecuencia de gravedad.

En cuanto a los porcentajes de cada uno de los cambios, como se observa en la Tabla 16 entre los usuarios que no han sufrido incidencias graves, **la reacción más frecuente es**

continuar haciendo el mismo uso de los servicios de Internet. Los datos porcentuales, ordenados descendentemente, señalan como cambios específicos más frecuentes: el cambio de contraseña y el abandono de foros, un 23% y un 13,3% respectivamente. El resto de servicios no registran cambios en el uso superiores al 10% de los usuarios.

En relación con aquellos usuarios que sufren incidencias graves, el cambio de conducta, si bien es elevado, es menor al que pudiera pensarse. Así, un 43,4% no modifica sus hábitos y usos de Internet. Un buen ejemplo de esto, es la baja tasa de abandono del servicio – incluso tras haber sufrido algún tipo de fraude, robo o intrusión – en la utilización de la banca y las compras online.

Ambos datos llevan a pensar que para los usuarios de Internet habituales no es tan fácil renunciar a las ventajas de los servicios de Internet o reducir su exposición a los riesgos existentes en la Red, ya que para ellos se ha convertido en algo necesario para su modo de vida.

Tabla 16: Cambios en el uso de Internet derivados de las incidencias de seguridad detectadas por los usuarios (%)

Cambios producidos	Incidencias SIN consecuencias graves	Incidencias CON consecuencias graves
Ningún cambio	65,6	43,4
Cambio de contraseñas	23,0	38,0
Abandono de foros	13,3	24,9
Cambio cuenta de correo	6,6	12,4
Abandono de descargas de archivos(P2P)	4,4	9,1
Abandono de pagos online	3,7	9,3
Abandono de compras online	2,9	8,4
Encriptación de documentos o datos	2,4	6,6
Abandono de banca online	1,8	5,8
Abandono del correo	0,4	1,0

Fuente: INTECO

De nuevo aparece la tensión entre el riesgo y la necesidad de seguir con un estilo de vida en el que Internet tiene un importante papel. Por ello, el posible papel de la Administración como “tercero” intermediario, entre el usuario y la Red, cobra mayor importancia.

El patrón entre usuarios que no han sufrido consecuencias graves es relativamente similar al de los usuarios que experimentaron alguna consecuencia grave en su equipo o software. Si bien, -como era de esperar-, los porcentajes de cambio registrados en el uso para aquellos usuarios que han sufrido consecuencias graves son algo mayores. No obstante, el mayor diferencial, relativo al cambio de contraseña, ni siquiera supera los 15 puntos porcentuales, por lo que estos datos sugieren que la utilización de servicios de

Internet refleja hábitos consolidados que no tienden a ser radicalmente modificados por los posibles riesgos latentes en la Red.

7.3.3 Cambios en la opinión sobre Internet

Finalmente, el tercer grupo de cambios son los relativos a la modificación de la opinión del afectado respecto a Internet derivada de las incidencias de seguridad y del nivel de gravedad de estas.

Se observa con claridad en la Tabla 17 que los principales cambios de opinión sobre Internet tienen que ver con la prevención: uso más cuidadoso y mayor información. Asimismo, la prevención se relaciona también con el papel de la Administración, a la que se pide una mayor implicación en la mejora de la seguridad de Internet.

La tabla también muestra cómo los usuarios que experimentaron alguna consecuencia grave derivada de las incidencias de seguridad han cambiado en general más su opinión sobre todos los ítems, y perciben, tras la incidencia grave, que Internet es más peligroso.

Específicamente, los usuarios que experimentaron alguna consecuencia grave asumen que deberían ser más cuidadosos cuando navegan por Internet (52,8%). Un 49,1%, demandan más información y un 42,1% piden que la Administración se implique más en el control de la seguridad en Internet.

Tabla 17: Porcentaje de usuarios que han cambiado su opinión sobre Internet derivados de las incidencias de seguridad detectadas por los usuarios (%)

Cambios	Incidencias SIN consecuencias graves	Incidencias CON consecuencias graves
No ha cambiado mi opinión	39,2	19,6
Debo estar más informado	38,0	49,1
La Administración debería implicarse más	34,6	42,1
Tengo que ser más cuidadoso	32,3	52,8
Debo alertar de los peligros	15,2	23,5
Es más peligroso	11,3	18,3

Fuente: INTECO

Observando las demandas espontáneas de los usuarios a la Administración en materia de protección en Internet -como se muestra en la Tabla 18-, la petición más frecuente es un mayor control y vigilancia de lo que ocurre en Internet (24,8%). Un 10,3% de los hogares pide más diligencia en la persecución de delitos y prácticas fraudulentas, y un 10,1% pide una mayor contundencia para las infracciones relacionadas con la seguridad en Internet.

Por otro lado se pide que se informe mejor a los usuarios de aquellos peligros que éstos desconocen y sobre la protección de los datos personales, y cómo prevenir las posibles incidencias (8,4%). También se pide una actuación más firme contra el spam (8,5%).

Tabla 18: Demandas espontáneas de los usuarios efectuadas a la Administración (%)

Demandas	%
Controlar y vigilar más de cerca lo que está pasando en Internet	24,8
Ser más diligentes en la persecución de delitos y prácticas	10,3
Ser más contundentes en el castigo a los delitos y prácticas	10,1
Actuar contra el SPAM/protección datos personales	8,5
Informar mejor a los usuarios de los riesgos y como prevenirlos	8,4
Proporcionar antivirus o programas de protección de forma gratuita	7,8
Actualización legislativa para los nuevos delitos por Internet	5,5
Crear un Departamento o una Policía de Seguridad en Internet	3,9
Crear sellos o garantías/seguridad en compras	3,7
Buscar una solución que permita al usuario navegar con tranquilidad	3,2
Avanzar en la identificación digital (DNI electrónico)	1,8
Implicarse/Actualizarse/Poner más medios/Invertir/Investigar	1,1
Otros	3,3
No sabe	7,6

Fuente: INTECO

7.4 Percepción del riesgo por servicio

En este apartado se presenta el análisis de las actitudes de los usuarios hacia la seguridad en Internet así como sus percepciones sobre su nivel de seguridad en la Red, desglosado por tipo de servicio.

En general, los usuarios tienden a atribuir un cierto riesgo a casi todos los servicios de Internet (el 3 de la escala indica “riesgo moderado” y el 4 indica “riesgo alto”). La conclusión es que se utilizan los servicios a sabiendas de la existencia de este riesgo, pero los usuarios están convencidos de que disponen de protección suficiente para efectuar una navegación normal y segura (Tabla 19)

Curiosamente, otorgan un riesgo relativamente bajo al correo electrónico (2,8 puntos), a pesar de ser una considerable puerta de entrada de código malicioso en el equipo y de intentos de fraudes online, como el ejemplo más conocido del phishing.

La explicación podría estar en que los usuarios tienden a pensar que el riesgo asociado al correo electrónico está “bajo control” en mayor medida que otras acciones. La descarga de archivos (3,5 puntos), los pagos y compras por Internet (3,3 y 3,2 puntos respectivamente) y la banca online (3,2) están considerados como los servicios de mayor riesgo percibido

por los usuarios. **Aun así los usuarios perciben que los servicios de Internet considerados más peligrosos tienen un riesgo moderado (valor 3 de la escala 1 a 5).**

Tabla 19: Nivel de riesgo percibido por los usuarios (puntos, escala 1-5)

Acciones	Nivel de riesgo percibido (Media 1-5)
Descarga de archivos (Música, Videos, Programas, etc.)	3,5
Pagos por Internet (Paypal y servicios afines)	3,3
Compra online (libros, discos, dvd, viajes, entradas, etc.)	3,2
Banca online (consulta de saldo, transferencias, etc.)	3,2
Juegos online	3,1
Chat y Mensajería instantánea (Messenger, ICQ, …)	3,0
Correo electrónico	2,8
Foros de opinión,	2,6
Telefonía IP	2,5
Hospedaje de pagina web personal	2,3
Videoconferencia	2,2
Blog (diario electrónico)	2,1
Búsqueda de información	1,9

Fuente: INTECO

7.5 Actitudes de los usuarios hacia la seguridad en Internet

Tras un análisis exploratorio y la posterior depuración de las diferentes variables utilizadas para estudiar las actitudes hacia la seguridad en Internet, se han detectado dos factores actitudinales que podemos denominar como '*tutelaje*' y '*autorregulación*'.

- El **tutelaje** hace referencia a la demanda de los propios usuarios de que, por una parte, la Administración supervise la seguridad en Internet y, por otra parte, de que ejerzan de "educadores", canalizando y proporcionando aquella información que les permita hacer un uso más eficaz de los distintos servicios.

- La **autorregulación** refleja la percepción que tienen los usuarios sobre la necesidad de un uso responsable de Internet y el hecho de que los peligros de Internet derivan de los propios hábitos de los usuarios de Internet y que, por ello deben ser controlados por ellos mismos.

Ambos son indicadores no excluyentes. Esto es, la demanda de una mayor intervención de las Administraciones puede llevar aparejada la autoexigencia de un comportamiento más responsable por parte de los propios usuarios.

A continuación se presentan los ítems que componen cada uno de estos indicadores, así como el porcentaje de usuarios que indican estar de acuerdo o totalmente de acuerdo.

Se ha procedido a un análisis para verificar si los ítems seleccionados definen adecuadamente dos conductas diferentes pero no excluyentes entre sí. Las dos dimensiones representan adecuadamente la estructura de los datos y pueden obtenerse simultáneamente en el mismo usuario[14].

Una vez comprobada la validez del modelo, se han calculado indicadores de tutelaje (Tabla 20) y autorregulación (Tabla 21) a partir de las saturaciones factoriales. Estas puntuaciones se han transformado para que siempre tomen valores positivos y facilitar así la interpretación de los resultados.

Tabla 20: Porcentaje de usuarios favorables a distintas prácticas del Factor Tutelaje (%)

Opiniones	Totalmente de acuerdo + de acuerdo
La seguridad en Internet debe venir determinada por la intervención de los gobiernos.	57,30
La falta de información referente a seguridad en las nuevas tecnologías me hace limitar su uso.	49,10
La Administración Publica debería encargarse de hacer Internet un lugar mas seguro.	71,80
Emplearía más servicios de los que oferta Internet si me enseñasen como proteger mi ordenador.	58,30

Fuente: INTECO

Tabla 21: Porcentaje de usuarios favorables a distintas prácticas del Factor Autorregulación (%)

Opiniones	Totalmente de acuerdo + de acuerdo
Internet seria más seguro si empleásemos correctamente las utilidades de los programas de que disponemos	84,70
La propagación de amenazas a través de Internet es resultado de la poca cautela que sus usuarios manifiestan	66,60
Es culpa nuestra que Internet se haya convertido en un lugar para desarrollar practicas tan poco éticas	53,00

Fuente: INTECO

[14] Existe una correlación moderada entre ambas dimensiones (r = 0,29) lo que confirma empíricamente la idea de que no son actitudes excluyentes sino que pueden coexistir en diferente grado dentro de las opiniones de los usuarios.

7.6 Percepción de la seguridad en Internet

El siguiente punto analizado es la **confianza** que muestran los usuarios respecto de sus conexiones y equipos en el hogar.

En la Tabla 22 se puede observar que la mayor parte de los usuarios perciben que su acceso a Internet desde el hogar es muy seguro. En torno a las ¾ partes confía en la invulnerabilidad de su conexión frente a los intrusos, y un porcentaje aún más elevado, confía en los sistemas de protección del ordenador con el que accede a Internet desde el hogar. Esto da como resultado que el 86% de los usuarios sean de la opinión de que su ordenador está razonablemente protegido.

Tabla 22: Porcentaje de usuarios que opinan que su equipo está seguro (De acuerdo+ Totalmente de acuerdo) (%)

Opiniones	Totalmente de acuerdo + de acuerdo
La conexión que utilizo es bastante segura frente a intrusos que quieran acceder a mi equipo	75,8
Mi ordenador esta razonablemente protegido	86,0
Los dispositivos y sistemas de protección que utilizo están actualizados y son eficaces	83,5

***n* = 6357, Base total muestra de hogares.** *Fuente: INTECO*

A partir de estos elementos se ha calculado un índice de seguridad: **Índice de percepción de seguridad personal** (Tabla 23). En él se contabiliza el grado de acuerdo o desacuerdo en las tres preguntas y se transforma en una escala de valores entre 0 y 100. Cero indica la mínima percepción de seguridad y cien la máxima.

Siguiendo el esquema del modelo explicativo antes expuesto, la siguiente cuestión que se plantea es si la seguridad percibida se relaciona con las experiencias del usuario.

En general se trata de un fenómeno de complejo análisis. A la vista de los datos reflejados en la tabla, la percepción de seguridad es elevada en casi todos los casos, superando en casi todos los niveles de incidencias una puntuación de 75. Solamente la reiteración de incidencias parece tener cierto impacto en la percepción de seguridad, en cuyo caso disminuye la percepción de seguridad de los usuarios, situándose en valores cercanos a los 70 puntos.

A pesar de estos cambios las incidencias persisten, entonces se comienza a ver afectada la percepción de seguridad del usuario de forma permanente.

Tabla 23: Percepción de la seguridad personal según el número de incidencias totales sufridas (puntos, escala 0 - 100)

Número de incidencias	Percepción seguridad personal (0-100)
0	81,1
1	79,1
2	79,0
3	77,4
4	75,3
5	74,1
6	72,6
7	69,8
8	66,5
9	70,4
Total muestra	76,8

Fuente: INTECO

La conclusión que podemos extraer es que los usuarios tienden a mantener constante y elevada la percepción de seguridad pues, de otro modo, su utilización de Internet se volvería muy incómoda. Para mantener alta esta constante modifican sus hábitos, incrementan las medidas de protección o realizan ambas a la vez, de forma que, tras una incidencia, la percepción de seguridad personal vuelva a niveles tolerables. Cuando a pesar de estos cambios las incidencias persisten, entonces se comienza a ver afectada la percepción de seguridad del usuario de forma permanente.

Esta misma relación se aprecia cuando analizamos la gravedad de las incidencias (Tabla 24). Se observa que incluso aunque aumente el número de consecuencias graves padecidas, la percepción de seguridad del usuario es elevada, tomando valores cercanos a los 75 puntos.

Tabla 24: Percepción de la seguridad personal según el número de consecuencias graves experimentadas (puntos, escala 0 - 100)

Número de consecuencias	Percepción seguridad personal (0-100)
Sin consecuencias graves	78,9
Con 1 consecuencia grave	75,5
Con 2 consecuencias graves	74,8
Con 3 consecuencias graves	74,3
Con 4 consecuencias graves	62,8
Total muestra	76,8

Fuente: INTECO

Al relacionar la percepción de seguridad con las actitudes hacia la seguridad de Internet se observan algunos datos de interés (Tabla 25):

- Cuando la seguridad percibida es baja (Índice 0 a 50), los usuarios demandan una mayor intervención por parte de la Administración (factor tutelaje 4,32 sobre 5 y factor autorregulación 4,03), dado que el usuario estima como insuficiente la autorregulación.

- En sentido contrario, cuando la percepción de seguridad es más alta (Índice de 51 a 100), se prefiere que sean los propios usuarios quienes con su comportamiento responsable regulen el sistema (factor autorregulación 4,14 frente a un factor tutelaje de 4,12).

Es decir, parece que se reserva a la Administración un papel de última instancia, cuando la prudencia, los programas de protección y la responsabilidad individual no garanticen una navegación segura. En ese momento es cuando el usuario comienza a experimentar que no mantiene elevados los niveles de percepción de seguridad personal y necesita ayuda. Entonces, se demanda más intervención de la Administración como complemento de la autorregulación.

Tabla 25: Tendencia hacia el tutelaje o la autorregulación dependiendo del índice de percepción de la seguridad personal (puntos, 0 - 100)

Índice	Tutelaje (Media 1-5)	Autorregulación (Media 1-5)
Índice 0-50	4,32	4,03
Índice 51-100	4,12	4,14
Total	4,14	4,13

Fuente: INTECO

7.7 Tendencias de seguridad en el último año

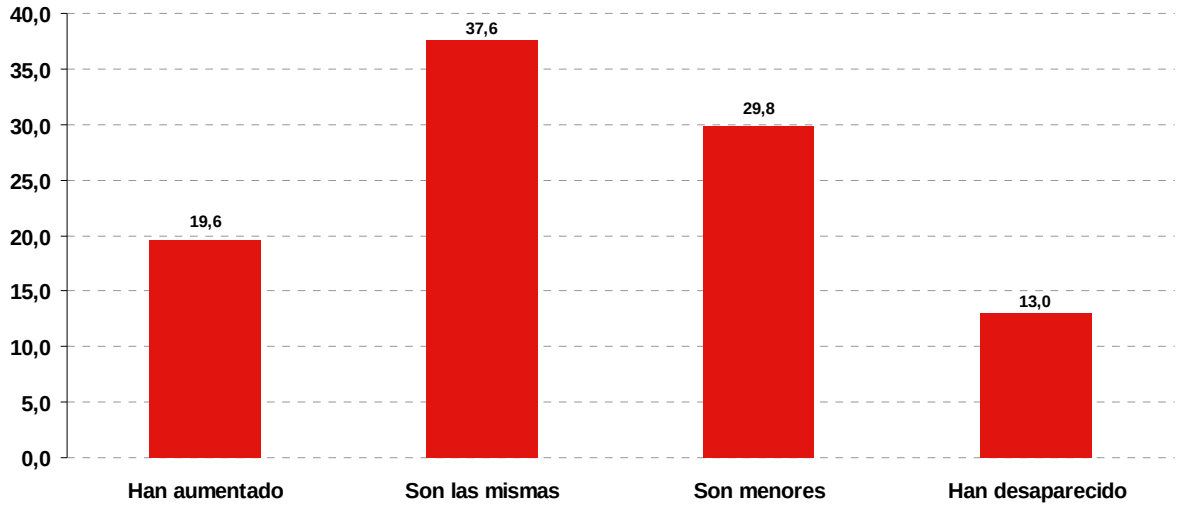
Los resultados presentados hasta el momento reflejan los niveles actuales de incidencias, consecuencias y percepción de seguridad. No obstante, la percepción de seguridad también está correlacionada con la evolución percibida con respecto a las incidencias y consecuencias sufridas en momentos precedentes. En ese sentido, el último año es considerado como el período relevante de reacción frente a una incidencia y su consecuencia.

Así pues, cómo ha evolucionado la percepción del número de incidencias, la gravedad de las consecuencias y el nivel de protección de los equipos de acceso a Internet durante el último año, en opinión de los usuarios.

Respecto a la **percepción del número de incidencias actuales** en comparación con las de hace un año (Gráfico 23), los usuarios piensan que, en términos generales, el número de incidencias se ha reducido.

De este modo, un 42,8% de los usuarios perciben un número menor de incidencias en el momento actual, donde se distingue entre el 29,8% de los hogares que afirma que el número de incidencias es menor y el 13% que indica que ha desaparecido toda incidencia. El porcentaje de usuarios que perciben el mismo número de incidencias en la actualidad que hace un año es de un 37,6%. Por último, sólo un 19,6% refiere la sensación de aumento del número de incidencias en la actualidad respecto al último año.

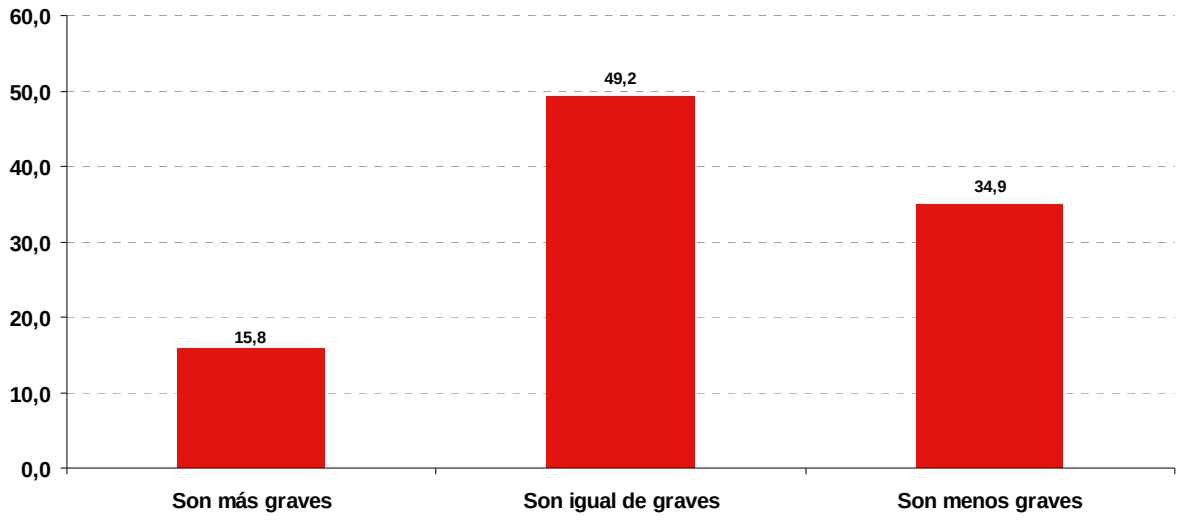
Gráfico 23: Percepción de la evolución del número de incidencias en el último año (%)



Fuente: INTECO

Con respecto a la **percepción de gravedad** de esas incidencias (Gráfico 24) se observa una evolución similar: el porcentaje de usuarios que perciben que las incidencias en la actualidad son menos graves (34,9%) duplica al de usuarios que perciben que estas incidencias son más graves (15,8%). No obstante, para prácticamente la mitad de los usuarios, la gravedad no ha cambiado (49,2%).

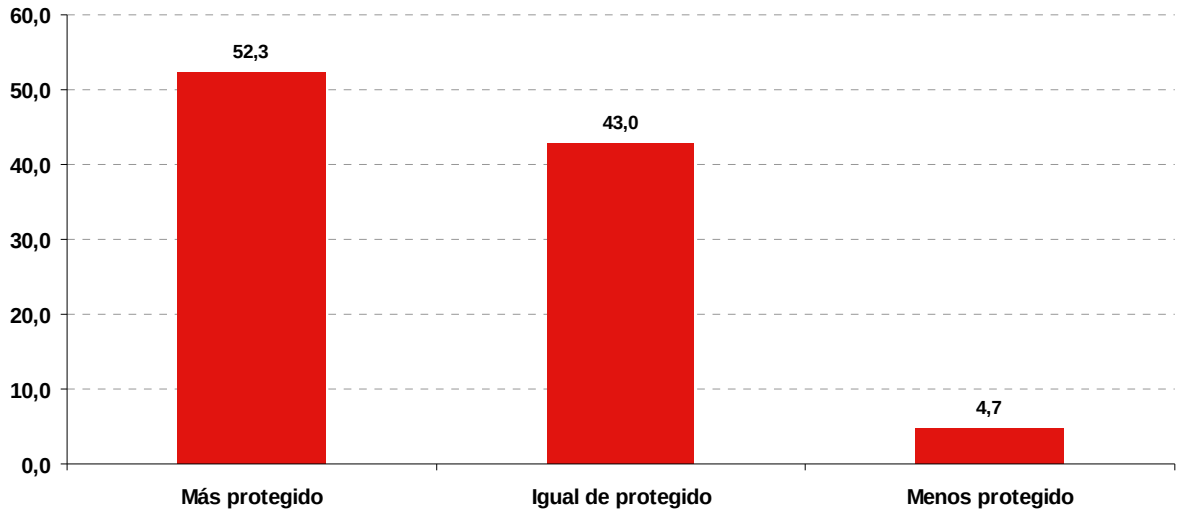
Gráfico 24: Percepción de la evolución de la gravedad de las incidencias en el último año (%)



Fuente: INTECO

Finalmente, el análisis conjunto del número de incidencias y de la percepción de su gravedad en el último año da como resultado una **mayor sensación de seguridad respecto de sus equipos de acceso a Internet desde el hogar en la actualidad, frente a la comparación con hace un año.** La mayor parte de los usuarios tienen la percepción de que sus equipos están mejor protegidos que hace un año (52,3%), y tan sólo el 4,7% se siente menos protegido (Gráfico 25).

Gráfico 25: Percepción de la evolución de la protección de los equipamientos de acceso a Internet (sensación de seguridad)



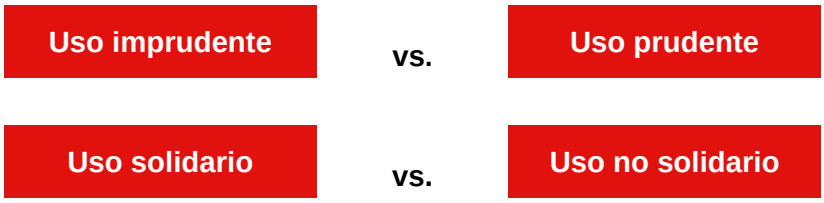
Fuente: INTECO

Estos resultados obtenidos de la percepción de la tendencia evolutiva de la seguridad son consonantes con los elevados niveles de percepción de seguridad obtenidos (Tabla 23). A pesar de haber experimentado, muchos de ellos, consecuencias graves en sus equipos (Tabla 24). En este sentido, la relación entre la percepción de la seguridad y las incidencias y sus consecuencias, aunque directa, está modulada por los niveles previos, tanto de incidencias como de sus consecuencias. Así, usuarios que en el momento actual aún perciben un número considerable de incidencias, o experimentan consecuencias graves, pueden sentirse seguros, si estas incidencias y consecuencias han disminuido considerablemente durante el último año (Gráfico 24).

Esta circunstancia es especialmente relevante al analizar los hábitos de uso de Internet, ya que previsiblemente hábitos temerarios podrían consolidarse si se percibe que el número de incidencias y su gravedad va a menos. En otras palabras, si el usuario se siente "invulnerable" es más probable que actúe de forma menos prudente. Este extremo se analiza con mayor detalle en el siguiente epígrafe.

7.8 Segmentación por hábitos de seguridad

A la luz de los resultados de la investigación, se han identificado dos tipos de comportamiento en el uso de Internet:



Ambos pueden afectar de uno u otro modo a la vulnerabilidad del sistema. El primero compromete principalmente la seguridad de los equipos de acceso y el segundo incide en mayor medida en la diseminación de las incidencias en el sistema.

Existen, por tanto, usuarios con un comportamiento claramente temerario, que además pueden mostrar poca solidaridad con otros usuarios. Este tipo de usuarios no sólo comprometen la seguridad de sus equipos de acceso, sino que favorecen la diseminación de amenazas en el sistema.

Por otra parte, aquellos usuarios que solamente se preocupan de la invulnerabilidad de su equipo, es decir, que son poco solidarios, si bien no suponen un alto riesgo para el sistema, tampoco contribuyen a su mejora.

Un último tipo de usuario, prudente y solidario, facilita y ayuda a mantener blindado el sistema de incidencias de seguridad.

A continuación exploramos la presencia de esta tipología entre los hogares y usuarios españoles de Internet mayores de 15 años.

Aunque en principio es posible reconocer cuatro grupos en la matriz *prudencia x solidaridad*, se ha realizado un agrupamiento en dos fases para comprobar si la estructura de los datos soporta este tipo de clasificación.

Los resultados reflejan que dentro de la matriz debería existir un grupo con unas determinadas características: usuarios con un comportamiento temerario y solidario a la vez. Sin embargo, la especial caracterización de estos usuarios, y la relevancia que dicho comportamiento pudiera poseer, no tiene significación suficiente para que sea analizado independientemente. Es decir, apenas existen usuarios que cumplan dicho perfil en la vida real.

Aunque se puede forzar el agrupamiento para que recoja cuatro grupos, este agrupamiento sería poco realista por lo que se ha optado por respetar la distribución de los grupos atendiendo a su presencia real en los usuarios panelizados. En otras palabras, lo que permite el agrupamiento en dos fases es descubrir la estructura real de los datos:

1. En la primera fase se identifica el número óptimo de grupos: Se puede adelantar que en este análisis son tres los grupos diferenciados que resultan de la segmentación.

2. En una segunda fase se distribuye a los sujetos en cada uno de los grupos en función de sus puntuaciones en las variables de interés. En este análisis en particular la asignación tiene lugar entre comportamiento solidario e imprudente.

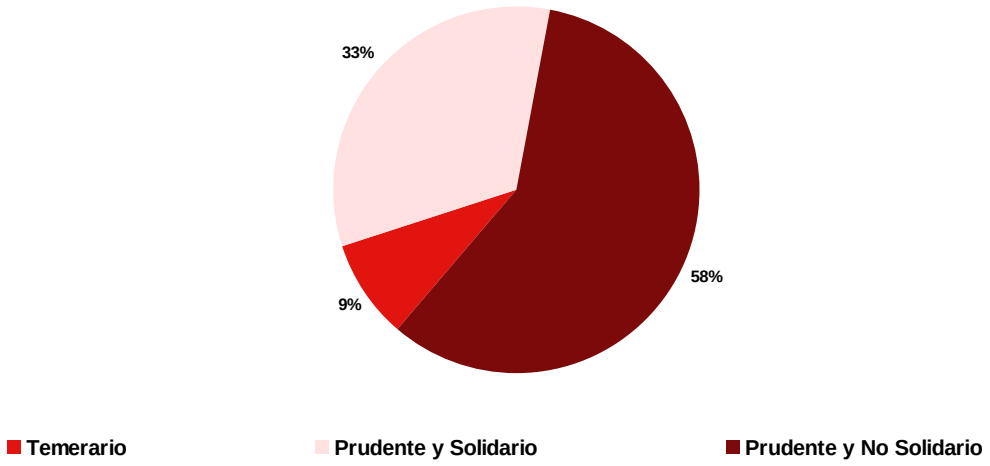
Este procedimiento permite discriminar con mayor eficacia al contrastar en las variables socioeconómicas, actitudinales y de uso, y seguridad en Internet. A continuación, en el Gráfico 26, se presenta la distribución de los tres perfiles característicos en la población.

- La mayor parte de los usuarios (58%) son prudentes en sus prácticas al mismo tiempo son poco solidarios. Dichos usuarios, centran su prudencia en la protección individual, pero sus prácticas con otros usuarios no ayudan a limitar la diseminación de incidencias en el sistema.

- Un 33% de la población de usuarios en el hogar son a la vez prudentes y solidarios: no sólo preservan la integridad de sus equipos sino que con su actitud respecto al resto de integrantes del sistema contribuyen a mejorar la seguridad del mismo.

El tercer grupo – denominado “temerario” – compuesto por un 9% de los hogares constituye un riesgo potencial para el sistema. Las prácticas de estos usuarios comportan no sólo la seguridad de sus propios equipos de acceso, sino que sus actitudes poco solidarias, asimismo comprometen la seguridad del resto de equipos y de la totalidad del sistema.

Gráfico 26: Distribución de los usuarios según hábitos de uso (%)

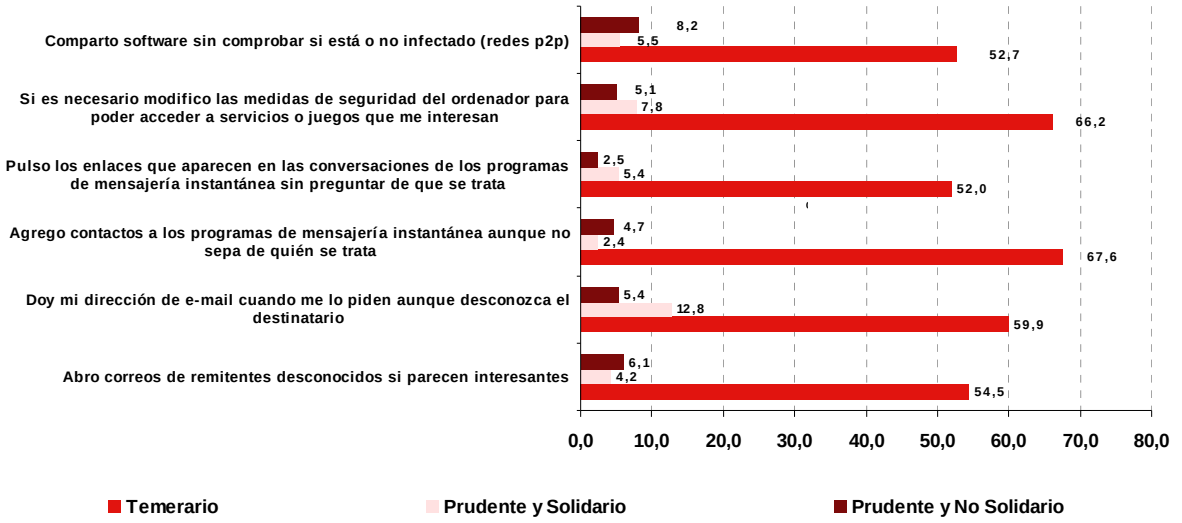


Fuente: INTECO

En el Gráfico 27 se presenta el detalle de los tres grupos de comportamiento, y las actitudes solidarias y temerarias que componen cada uno de los grupos identificados. Se observa que la denominación del grupo *temerario* no es una exageración. Este grupo de usuarios presenta unos hábitos diferenciados del resto de los usuarios de Internet, con serias implicaciones para la seguridad del conjunto.

Entre las prácticas potencialmente peligrosas que caracterizan a los usuarios **temerarios** destacan: la modificación de las medidas de seguridad del ordenador para acceder a determinados contenidos (66,2%), como por ejemplo la desactivación de cortafuegos para acceder a juegos online; compartir y descargar archivos sin comprobar con las herramientas de seguridad adecuadas (antivirus) si están o no infectados antes de ser ejecutados (52,7%); abrir correos de remitentes desconocidos (54,5%); y pulsar enlaces no confiables en conversaciones de mensajería instantánea (52%)

Gráfico 27: Perfil de hábitos de imprudencia por segmentos (%)



Fuente: INTECO

En lo que respecta al comportamiento solidario, en el Gráfico 28, se observa que el grupo de usuarios **prudentes y solidarios** muestra unos hábitos característicos de prudencia y solidaridad muy elevados. Destacan como comportamientos de este grupo la interrelación de la información con otros usuarios para comentar cualquier incidencia de seguridad que haya surgido en el sistema. En concreto, un 97,5% siempre comprueban cualquier archivo que envían adjunto en correo electrónico. Otro dato destacado es que cuando reciben un correo electrónico de un conocido con un archivo infectado, un 97,1% se lo comunica al remitente. También un 91,5% de este tipo de usuario efectúa recomendaciones a aquellos usuarios que no tienen actualizados sus programas de seguridad, para que se instalen las últimas actualizaciones. Destaca también en su comportamiento que alertan sobre la existencia de nuevos virus (85,3%) o páginas que conocen y que hacen uso fraudulento de los datos de los usuarios (76,4%).

El perfil de los usuarios **prudentes pero con menor conciencia solidaria**, se refleja en un tipo de comportamiento más marcado por el individualismo. En general son los menos solidarios de los tres grupos, aunque su riesgo para el sistema es menor debido a que son razonablemente prudentes en todos los hábitos relevantes. Es decir, el comportamiento de este grupo se caracteriza por una mayor prudencia en elementos calificados de imprudencia. La modificación de las medidas de seguridad para poder acceder a servicios o juegos sólo se produce entre el 5,1% de estos usuarios. No pulsan inconscientemente en los enlaces que aparecen en las conversaciones de mensajería instantánea, sólo lo hace un 2,5% de ellos. Es el grupo que en menor porcentaje (5,4%) da su dirección de correo electrónico cuando se la piden. Sin embargo es un grupo en el que determinados hábitos de prudencia son los menos extendidos. Así, sólo la mitad de ellos comprueban

que los archivos adjuntos que envían por correo no contienen virus y sólo algo más de la mitad (55%) avisa al remitente conocido cuando recibe de él un correo con un archivo infectado.

Gráfico 28: Perfil de hábitos de protección por segmentos (%)

Fuente: INTECO

7.9 Caracterización de los segmentos

A continuación se presenta una caracterización sociodemográfica de los tres tipos de usuarios detectados.

7.9.1 Segmentación por edad

En el Gráfico 29 se presenta de forma sintética las características de los tres segmentos de usuarios identificados, distinguiéndolos en función de la variable edad.

Para un universo total del 45% mayor de 35 años y un 55% menor de 35 años la disgregación por tipologías de usuarios ofrece los siguientes resultados:

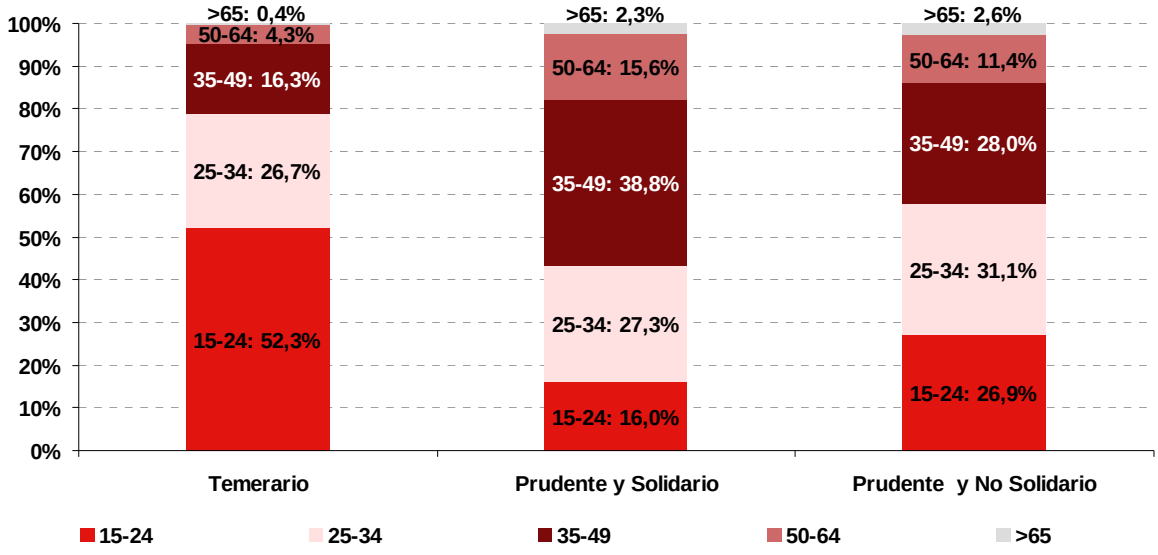
1. Dentro de la segmentación para la tipología de **Temerario** el grupo de edad más frecuente es el de jóvenes entre 15 y 24 años (52,3%). Es decir, el 52,3% de los usuarios temerarios son jóvenes entre 15 y 24 años, seguido de aquel grupo de usuarios con edades comprendidas entre 25 y 34 años (26,7%). Usuarios categorizados como temerarios y mayores de 35 años representan sólo un 21% del total.

2. Dentro de la categoría de usuarios **Prudentes y Solidarios** los porcentajes están más repartidos. El grupo más numeroso dentro de este segmento son usuarios con

edades comprendidas entre los 35 y 49 años (38,8%). Le sigue el grupo de edades entre 25 y 34 años con un 27,3%. En este caso los jóvenes menores de 25 años representan el 16 %, porcentaje similar al de usuarios cuya edad está entre 50 y 64 años (15,6%). tienen un perfil tal que la mayoría son mujeres (53,9%)

3. También se encuentra muy repartida la distribución porcentual para los usuarios **Prudentes y No Solidarios**. Un 31,1% son usuarios con edades comprendidas entre 25 y 34 años. El 28% son usuarios entre 35 y 49 años y el 26,9% corresponde a jóvenes menores de 25 años.

Gráfico 29: Segmentos de hábitos y edad (%)



Fuente: INTECO

7.9.2 Segmentación por sexo

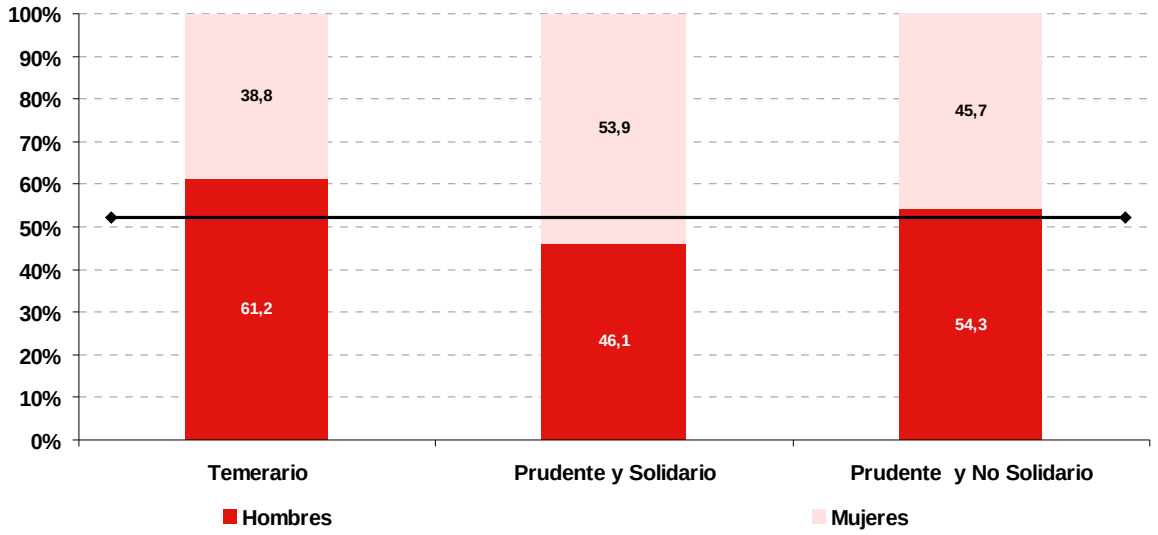
Para un universo total de un 52% de hombres y un 48% de mujeres la disgregación por tipologías de usuarios ofrece los resultados que aparecen en el Gráfico 30

1. El grupo de usuarios **Temerarios** está compuesto mayoritariamente por hombres (61,2%)

2. Los usuarios **Prudentes y Solidarios** tienen un perfil tal que la mayoría son mujeres (53,9%)

3. El grupo de **Prudentes y No Solidarios** está compuesto por un 54,3% de hombres frente a un 45,7% de mujeres.

Gráfico 30: Segmentos de hábitos y sexo

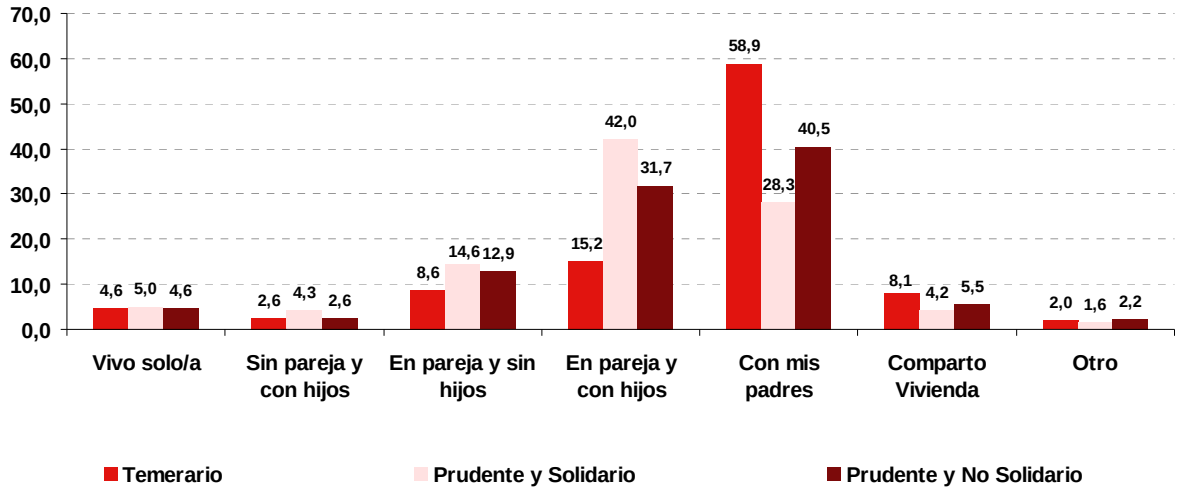


Fuente: INTECO

7.9.3 Segmentación por tamaño del hogar

En cuanto al tipo de hogar en que residen los usuarios (Gráfico 31), se percibe con claridad que el perfil de los usuarios denominados *temerarios* se corresponde con jóvenes que viven con sus padres (58,8%) en una mayor proporción que los restantes usuarios. Los usuarios prudentes y solidarios suelen ser personas que viven en pareja y tienen hijos (42%).

Gráfico 31: Segmentos de hábitos y posición en el hogar (%)



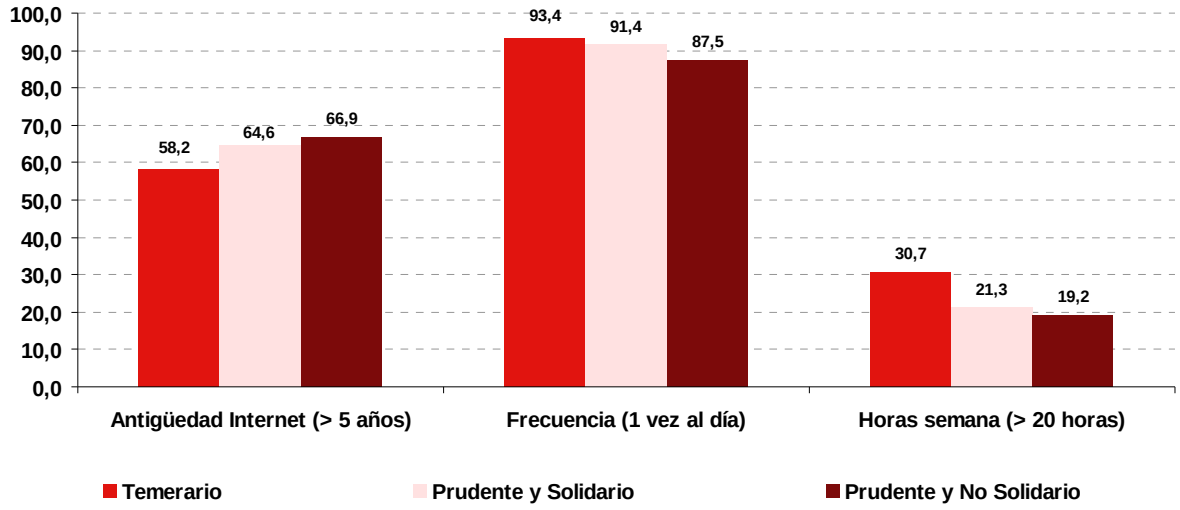
Fuente: INTECO

7.10 Hábitos tecnológicos generales

En cuanto a la experiencia y frecuencia en el uso de Internet se observa que el porcentaje de usuarios temerarios es algo menos antiguo en Internet que el resto (58,2%). La juventud y las ganas de explorar pueden estar en el fondo explicativo de su conducta.

Esta relativa menor experiencia, sin embargo, hay que interpretarla teniendo en cuenta que estos usuarios se conectan con mayor frecuencia (el 93,4% diariamente) y hacen un uso intensivo mayor de Internet, el 30,7% le dedican a Internet 20 ó más horas semanales. Con hábitos opuestos a ellos, en todos los epígrafes del Gráfico 32, se encuentran los usuarios prudentes y no solidarios. Son aquellos que tienen mayor antigüedad en Internet (66,9%) que menores porcentajes presentan para aquellos que se conectan diariamente (87,5%) y un menor número de horas semanales (19,2%).

Gráfico 32: Segmentos de hábitos e intensidad de uso de Internet (%)



Fuente: INTECO

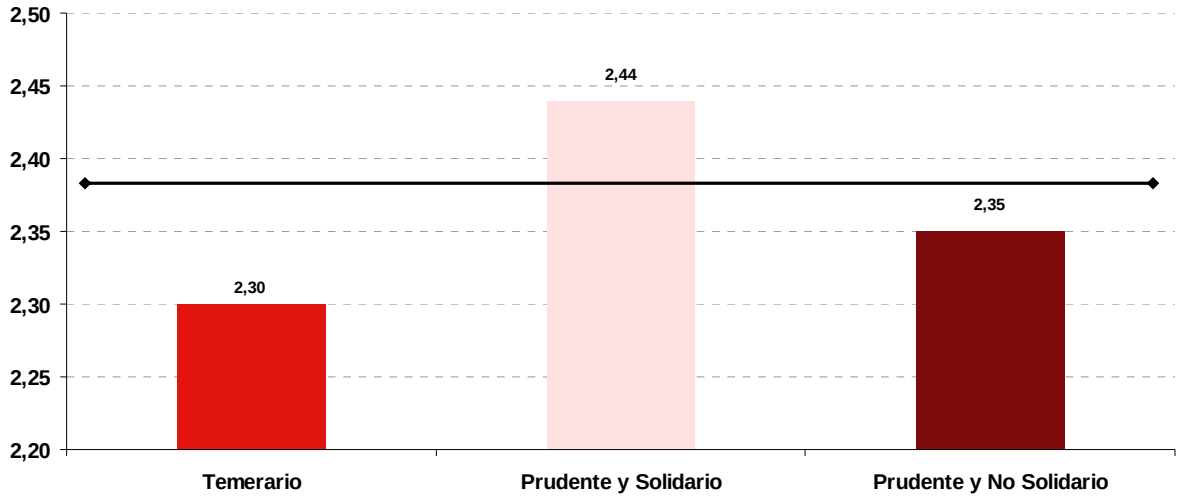
Atendiendo a los datos, **los usuarios temerarios** no sólo comprometen con sus prácticas la seguridad de sus equipos y del sistema sino que, reforzado por un uso intensivo de Internet, se incrementa la posibilidad de que experimenten no sólo incidencias de seguridad, sino que además éstas sean diseminadas en cierta medida en el sistema.

El Gráfico 33 presenta el número de usuarios de Internet del hogar promedio para cada grupo que comparten el mismo terminal de acceso.

Los usuarios prudentes y solidarios suelen acceder a Internet desde terminales cuyo uso es compartido por un mayor número de usuarios, mientras que los usuarios no solidarios

(tanto prudentes como temerarios), suelen acceder a Internet desde terminales individuales en un mayor porcentaje.

Gráfico 33: Media de personas que comparten el terminal para acceder a Internet



Media= 2,38 *Fuente: INTECO*

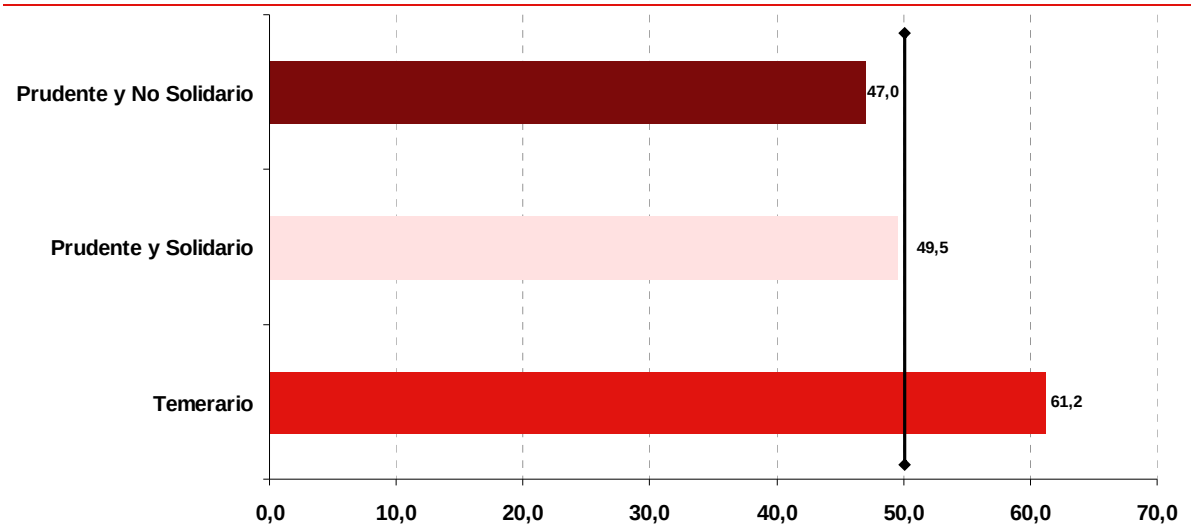
Destaca el hecho de que los usuarios temerarios tienden a utilizar menos equipos de acceso compartidos en el hogar. Como hipótesis explicativa podría considerarse aquí el efecto de la presión social en las prácticas de uso: cuanto mayor es el número de potenciales '*testigos*' menor es el comportamiento de riesgo (*temerario*). **El respeto al resto de usuarios que comparten el terminal en el hogar incluye un componente social relacionado con un comportamiento más prudente.**

7.11 Incidencias de seguridad

En el siguiente apartado se presenta el análisis de las incidencias de seguridad declaradas por cada uno de los tres segmentos. Del resultado del análisis se destaca que el grupo de usuarios temerarios experimentaron un número de incidencias por encima de la media del resto de grupos. Es decir, el comportamiento de este grupo de usuarios eleva por sí solo el número de incidencias.

En este primer análisis temporal el comportamiento observado invita a pensar que **los usuarios denominados temerarios se ven menos influidos por el efecto "aprendizaje".**

Gráfico 34: Porcentaje de usuarios que han sufrido consecuencias graves para su equipo por incidentes de seguridad.

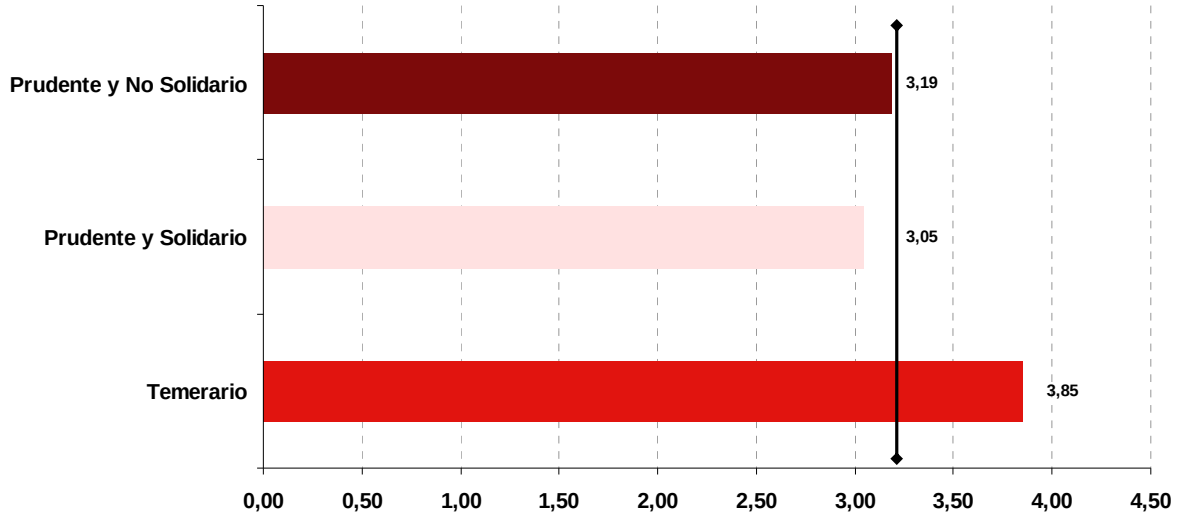


Fuente: INTECO

De hecho, al ser el único grupo que presenta valores por encima de la media podemos decir que es este grupo de usuarios es el que hace subir la media de incidencias de seguridad; casuística paralela con la idea ya avanzada de que son estos usuarios los que en mayor medida comprometen la vulnerabilidad del sistema.

En el Gráfico 34 se presenta el porcentaje de usuarios, en cada uno de los segmentos, que afirman haber experimentado alguna consecuencia grave derivada de las incidencias de seguridad, (bien formateo del disco duro, bien instalación/reinstalación del sistema operativo, o bien daños en el hardware). El porcentaje de usuarios temerarios que experimentan consecuencias graves derivadas de sus incidencias de seguridad (61,2%), es sustancialmente mayor que el de otros segmentos: un 49,5% del los usuarios prudentes y solidarios y 47% de los usuarios prudentes y no solidarios. Además, este porcentaje de usuarios temerarios que han sufrido alguna incidencia de seguridad informática en algún momento, es el único que se encuentra por encima de la media de la población, representada por la línea vertical (50%).

Gráfico 35: Media de incidencias de seguridad declaradas por el usuario



Media= 3,20

Fuente: INTECO

7.12 Percepción de seguridad

En cuanto a la percepción global de seguridad en sus equipos de acceso y sistemas de protección, se observa que solamente el grupo solidario tiene una percepción de seguridad que destaca sobre el resto. Este grupo tiene un índice de percepción de 82,3 puntos, frente a los 74,6 de los usuarios denominados temerarios y los 74,0 puntos de los usuarios prudentes y no solidarios. Sin embargo, es característica común para todos los grupos una percepción elevada de su seguridad, independientemente de las precauciones que tomen, y cercana a 75 puntos en todos los casos.

Tabla 26: Percepción de seguridad personal según la tipología de usuario (puntos, escala 0 - 100)

Segmentos	Percepción de seguridad personal (0-100)
Prudente y No Solidario	74,0
Prudente y Solidario	82,3
Temerario	74,6
Total	76,4

Fuente: INTECO

Por otro lado, llama la atención en los datos el hecho de que los usuarios temerarios no aprecian demasiado la relación entre sus hábitos de riesgo y las incidencias que padecen.

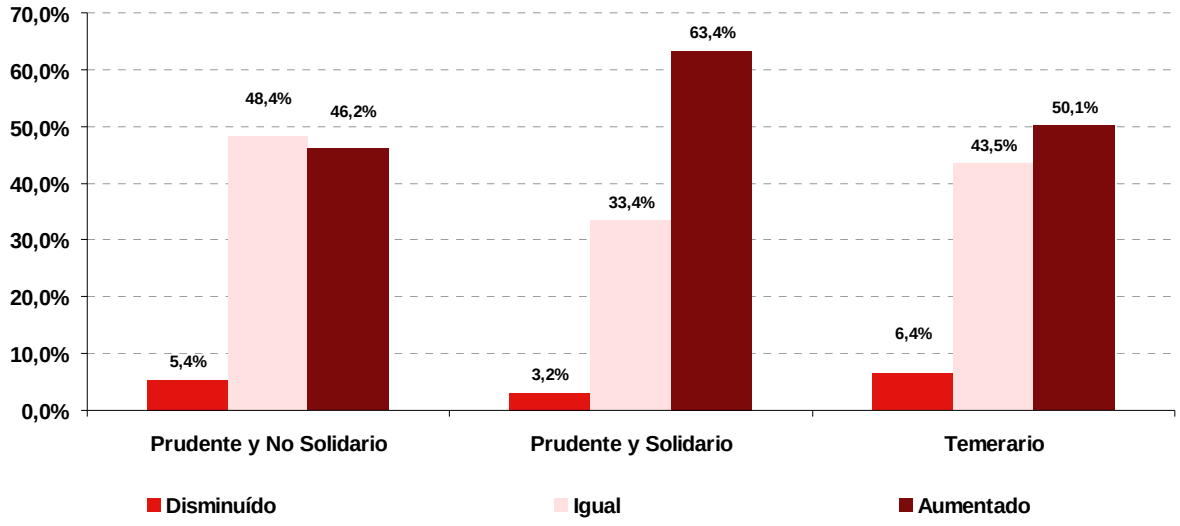
Aunque los datos manejados en este informe son de tipo estático y no permiten todavía analizar la evolución de sus hábitos de seguridad en el tiempo, es interesante analizar cómo cada uno de los grupos recuerda la evolución durante el último año del nivel de seguridad en cuanto al número de incidencias, sus consecuencias y el nivel de protección de sus equipos.

Como se podía observar en el Gráfico 23 existe una percepción generalizada de que durante el último año las incidencias de seguridad son menores y sus consecuencias son iguales o menos graves –84,1%– (Gráfico 24). Evidentemente, la percepción de que disminuyen incidencias y consecuencias hace aumentar la percepción de seguridad. Este dato es coherente con el elevado porcentaje de usuarios que perciben una elevada seguridad en sus conexiones y equipos de acceso.

Finalmente, el Gráfico 36 muestra los niveles percibidos de protección de los equipos en comparación con hace un año.

Como era previsible, -debido, por un lado, a la percepción de la disminución de las incidencias y sus consecuencias y, por otro lado, al aumento de la percepción de seguridad-, los usuarios tienen la sensación de que sus equipos de acceso a Internet están en general más protegidos. Aunque las 3 tipologías de usuarios perciben que la protección de sus ordenadores ha aumentado, es el grupo de los “Prudentes y Solidarios” el que se sitúa por encima de la media en esta sensación. Así, el 63,4% de los “Prudentes y Solidarios” opinan que ahora están más protegidos que hace un año, frente al 50,1% de los “Temerarios“ y el 46,2% de los “Prudentes y no Solidarios”

Gráfico 36: Porcentaje de variación de la sensación de protección en el último año



Fuente: INTECO

7.13 Actitudes hacia la seguridad de Internet

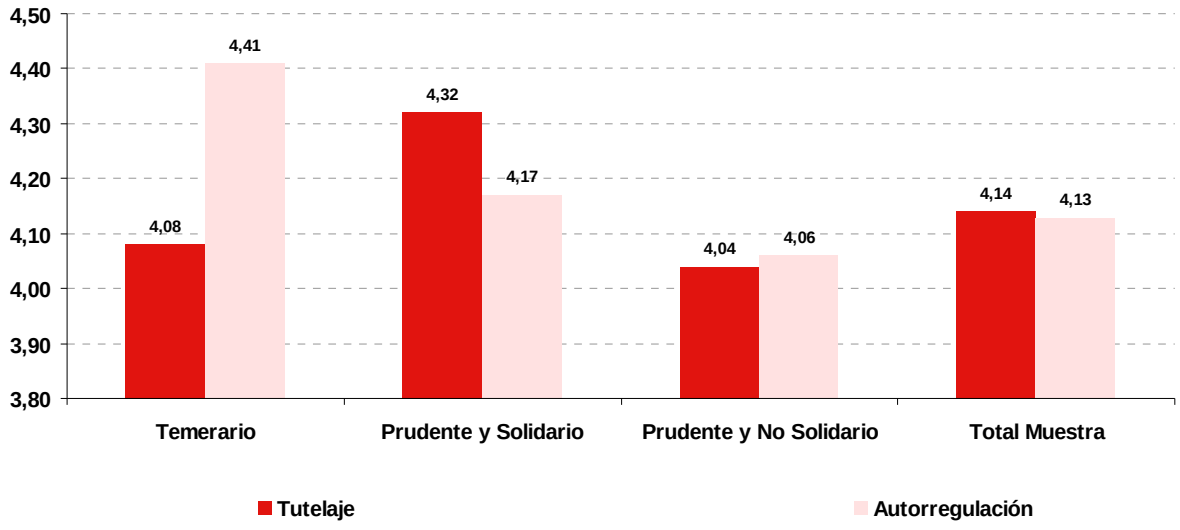
En cuanto a las actitudes hacia la autorregulación o el tutelaje de la seguridad en Internet, en el Gráfico 37 se observa cómo los distintos grupos mantienen distintos patrones en sus componentes actitudinales.

Destacan los valores presentes en el grupo de usuarios temerarios. Estos defienden una actitud fundamentalmente autorreguladora en Internet. Es decir, que sean los propios usuarios los responsables de la seguridad en Internet mediante sus prácticas.

Los usuarios prudentes y solidarios, -conscientes de las consecuencias sociales de sus hábitos-, aunque reconocen en parte la necesidad de unos niveles de autorregulación, son partidarios de una mayor intervención de la Administración (Tutelaje). Ello en interés de canalizar y compartir información relevante y garantizar la seguridad en Internet.

El grupo restante, prudentes/no solidarios mantienen una actitud equidistante respecto a ambas opciones, similar a la media de la muestra.

Gráfico 37: Puntuación media en los componentes actitudinales hacia la protección (Escala 1- 5)



Fuente: INTECO

8 INCIDENCIAS DE SEGURIDAD: SITUACIÓN REAL DE LOS EQUIPOS DE LOS HOGARES ESPAÑOLES

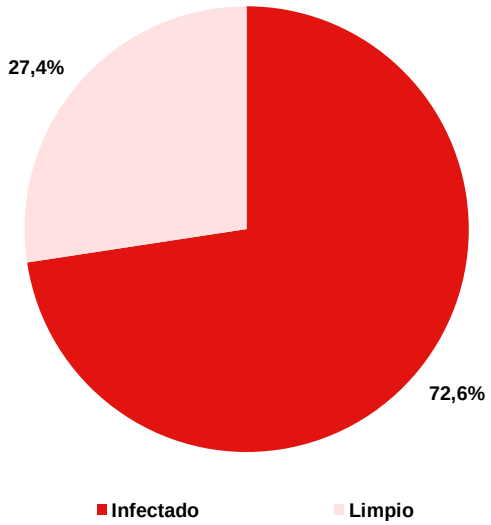
El estudio de incidencias de seguridad y vulnerabilidades, que presentan los equipos de acceso a Internet en los hogares panelizados, se lleva a cabo mediante una aplicación multiplataforma desarrollada por INTECO específicamente para este estudio.

Se trata de una herramienta de análisis de seguridad especializada en la detección de código malicioso (malware). Adicionalmente, y de forma anónima, recoge una serie de parámetros de seguridad íntimamente relacionados con la propagación del malware e infección de sistemas: análisis de vulnerabilidades críticas, detección de soluciones antivirus, y versión del sistema operativo.

8.1 Código Malicioso detectado. Equipos infectados.

El 72,6% de los equipos analizados presenta algún tipo de código malicioso en el sistema.

Gráfico 38: Equipos afectados por código malicioso (%)



Fuente: INTECO

Así pues, 7 de cada 10 equipos mantiene uno o más códigos maliciosos en el sistema. Este dato pone de manifiesto una realidad que pasa desapercibida a gran parte de los usuarios.

En este sentido cabe preguntarse cómo es posible que haya un porcentaje tan elevado de equipos infectados.

En el pasado el *malware* se ha caracterizado por llevar a cabo acciones más o menos dañinas y reconocibles por los usuarios. Así por ejemplo, en los años 90 los virus solían llevar a cabo acciones tras un número determinado de infecciones o en una fecha concreta: desde efectos gráficos hasta el borrado de información. En esos momentos la infección era evidente a los ojos del usuario

Posteriormente, con la llegada de Internet, acaece la era de los gusanos de propagación masiva. También eran reconocibles ya que los sistemas infectados se convertían en distribuidores automáticos del gusano, provocando un aumento del tráfico enviado con el envío del código malicioso.

Sin embargo, en la actualidad los virus y gusanos han dejado paso a otros tipos de *malware*, como los troyanos o el adware, que tienen entre sus objetivos pasar desapercibidos para el usuario y mantenerse ocultos el mayor tiempo posible en los sistemas infectados. Esto explica que haya un elevado número de sistemas infectados sin que los usuarios de los mismos se percaten.

En resumen, existen infecciones pero con una menor percepción de las mismas por parte de los usuarios.

8.2 Definiciones de distintos códigos maliciosos (malware)

Existe una gran cantidad de tipos de *malware* atendiendo a sus características, Para una mejor interpretación de los resultados, INTECO ofrece a continuación las definiciones de cada una de las categorías de código malicioso o malware más significativos, en las que se han clasificado las incidencias de seguridad detectadas:

8.2.1 Adware o programas publicitarios:

Software que muestra publicidad (en ventanas emergentes, banners, etc.) no solicitada. En ocasiones recopilan información sobre los hábitos de navegación de los usuarios para luego redirigirles a la publicidad coincidente con sus intereses. Se suelen instalar junto a otras aplicaciones, y normalmente se avisa de este hecho en extensas especificaciones de las licencias de uso; advertencia que en la mayoría de las ocasiones el usuario acepta sin leer. El peligro es relativo, existen algunas familias orientadas al fraude que emiten publicidad para instar al usuario a que compre productos falsos.

Gráfico 39: Ejemplo de ventana de software publicitario

Fuente: INTECO

8.2.2 Gusanos:

Programas con capacidad para propagarse a otras partes del equipo afectado, a dispositivos extraíbles o a otros equipos. Dependiendo de su código, podría realizar distintas acciones dañinas en los sistemas. A diferencia de los virus, los gusanos son programas que no necesitan otro archivo para replicarse

8.2.3 Spyware o programas espía:

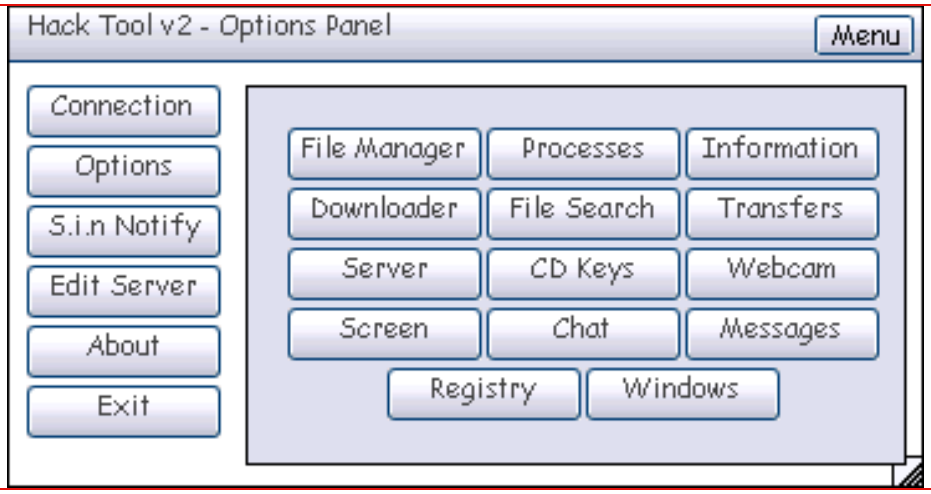
Son programas que recopilan información sobre el usuario sin su consentimiento. Por norma general se instalan como plugins al navegador sin el conocimiento del usuario y envían a un servidor en Internet los hábitos de navegación, como por ejemplo que páginas visita el usuario. Además de la invasión a la privacidad, estos programas transmiten información de forma constante, por lo que consumen ancho de banda de la conexión de sistema a Internet y afecta negativamente a la velocidad del resto de servicios que el usuario esté utilizando.

8.2.4 Tools o herramientas de intrusión:

Herramientas o programas que, sin necesidad de ser malware, pueden ser empleados por un atacante remoto para realizar análisis de seguridad, acceder al sistema afectado, o llevar a cabo otras acciones ilegales (cracking de contraseñas, escáner de puertos, escalado de privilegios, etc).

La peligrosidad o no de la herramienta dependerá de si ha sido instalada con el consentimiento del usuario y se conoce su funcionalidad. Por ejemplo, una herramienta de administración remota puede utilizarse para el mantenimiento del equipo o conexión desde otro ordenador, pero también podría ser instalada por un atacante para acceder sin el consentimiento del usuario, espiar, extraer información sensible, etc.

Gráfico 40: Ejemplo de ventana de herramienta de intrusión y opciones para el atacante



Fuente: INTECO

8.2.5 Troyanos:

Los troyanos no se pueden considerar virus ya que no se replican o no hacen copias de si mismos. En realidad son programas que llegan a un ordenador de forma totalmente normal y no producen efectos realmente visibles o apreciables (por lo menos en ese momento). Pueden llegar acompañados de otros programas y se instalan en el ordenador del usuario. Al activarse pueden dejar huecos en nuestro sistema, a través de los cuales se producen intrusiones.

Existen varios tipos de troyanos dependiendo de lo que hagan en el sistema: puerta trasera o “backdoors” (permite el acceso no autorizado al equipo), downloader (descarga otros códigos en la máquina), dialers, bankers, captadores de pulsaciones etc.…

Bancarios

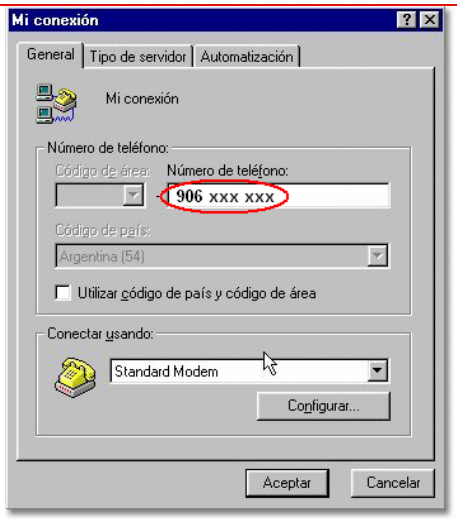
Son una variedad de malware especializada en el robo de credenciales de autenticación utilizadas por usuarios para realizar operaciones bancarias online. La información robada depende de la implementación de seguridad del sitio contra el que actúa y varía desde los simples captadores de formularios de validación hasta los que realizan capturas de vídeo de la actividad realizada por el usuario para realizar dicha validación o los que roban certificados digitales. Este tipo de malware está en alza, y representa el calmen de la tendencia actual del malware a centrarse en el lucro fraudulento y silencioso

Dialers o marcadores telefónicos:

Programas que una vez instalados en el equipo desvían la conexión telefónica original hacia otro número de tarificación especial (806, 807, etc.) con el consecuente perjuicio económico para el afectado. Únicamente pueden afectar a los usuarios que acceden a

Internet a través de banda estrecha mediante RTB (Red Telefónica Básica) o RDSI (Red Digital de Servicios Integrados).

Gráfico 41: Ejemplo de ventana del número de teléfono real por el de tarificación especial

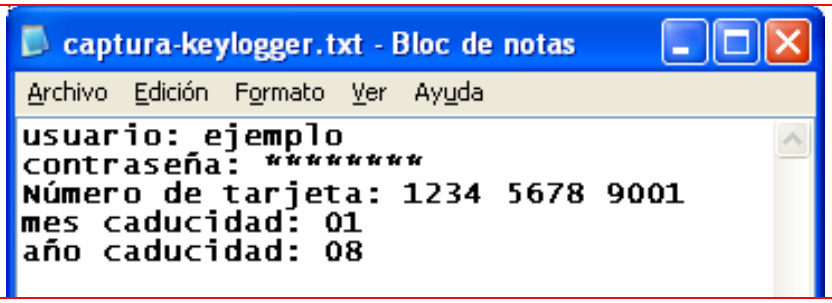


Fuente: INTECO

Keyloggers o capturadores de pulsaciones:

Son un tipo de troyano con capacidad para capturar y almacenar las pulsaciones efectuadas sobre el teclado. Posteriormente esta información (que puede contener contraseñas, datos bancarios, etc.) se envía a un atacante, que las puede utilizar en su propio provecho.

Gráfico 42: Ejemplo de datos recogidos por un capturador de pulsaciones



Fuente: INTECO

Backdoor o puertas traseras:

Troyano que permite a un atacante tomar el control remoto del sistema infectado, pudiendo llevar a cabo diversidad de acciones, como por ejemplo, espiar el escritorio remoto, realizar capturas de pantalla o de la webcam, subir o descargar archivos, altear el funcionamiento normal del sistema, etc.

Gráfico 43: Ejemplo de ventanas cliente/servidor de un troyano puerta trasera

Fuente: INTECO

8.2.6 Virus:

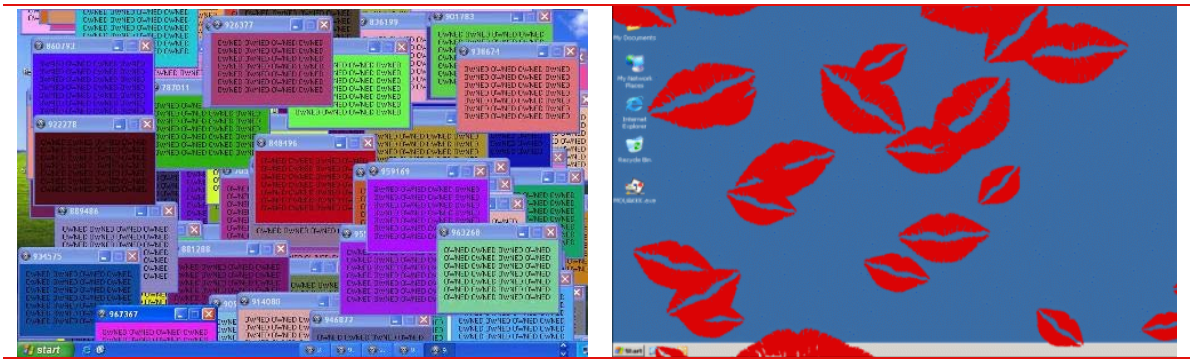
Son programas informáticos que pueden infectar a otros ficheros/programas modificándolos para incluir réplicas de sí mismo en el elemento infectado. Un virus necesita alojarse en otro archivo. Erróneamente se engloba bajo este nombre a todo el software malicioso.

8.2.7 Otras categorías y familias:

Bromas (jokes):

Programas que alteran el normal funcionamiento del equipo con acciones que molestan o distraen al usuario, si bien no causan daño alguno al sistema.

Gráfico 44: Ejemplo de bromas.



Fuente: INTECO

Exploits:

Código malicioso creado con el fin de aprovechar algún fallo o vulnerabilidad de los sistemas. Se suelen utilizar para ejecutar código arbitrario de forma remota, entrar en los equipos vulnerables sin que el usuario legítimo se aperciba de ello y poder actuar con libertad dentro del sistema atacado.

Rootkits o herramientas de ocultación:

Son herramientas que permiten al intruso (persona o código) ocultar su presencia en el sistema de forma que su detección se hace más complicada. Ocultan las pistas que podrían delatar su presencia tales como ficheros, procesos o entradas en el registro de Windows.

Scripts o secuencias de comandos maliciosos:

Son códigos escritos en algún lenguaje de programación con el objetivo de realizar acciones no deseadas en el sistema, normalmente a través del navegador o correo electrónico en formato HTML. Los lenguajes más habituales para este tipo de códigos son Visual Basic Script, JavaScript, etc.

Gráfico 45: Ejemplo de script malicioso. Tiene apariencia similar a uno legítimo

Fuente: INTECO

Archivos sospechosos detectados heurísticamente:

El método heurístico es uno de los métodos utilizados por las aplicaciones antivirus para detectar códigos maliciosos, basándose en la similitud de código, indicios y en comportamientos 'extraños' similares a los de otros virus ya conocidos. No obstante, no existe la certeza de que los códigos detectados como virus por este método sean realmente maliciosos, y puede producir 'falsos positivos'. Para evitar falsos positivos, la herramienta desarrollada por INTECO para el estudio sólo considera un archivo infectado si es, al menos, detectado heurísticamente por 5 de los 30 motores antivirus que utiliza.

Es necesario tener en cuenta que hoy día un mismo espécimen suele tener características de diferentes tipos de malware. Por ejemplo, un mismo código malicioso puede autoenviarse de forma automática como un gusano, presentarse como una aplicación legítima como lo haría un troyano y a la vez actuar como un keylogger que roba claves de acceso en el equipo infectado. Así pues, a la hora de catalogar un código malicioso en uno u otro tipo de malware se hará en función de la característica que se considere más significativa.

A lo largo de este capítulo e desglosarán alguno de estos tipos en varios subtipos, familias o especimenes concretos según necesidades del análisis.

8.3 Equipos infectados según tipología del malware

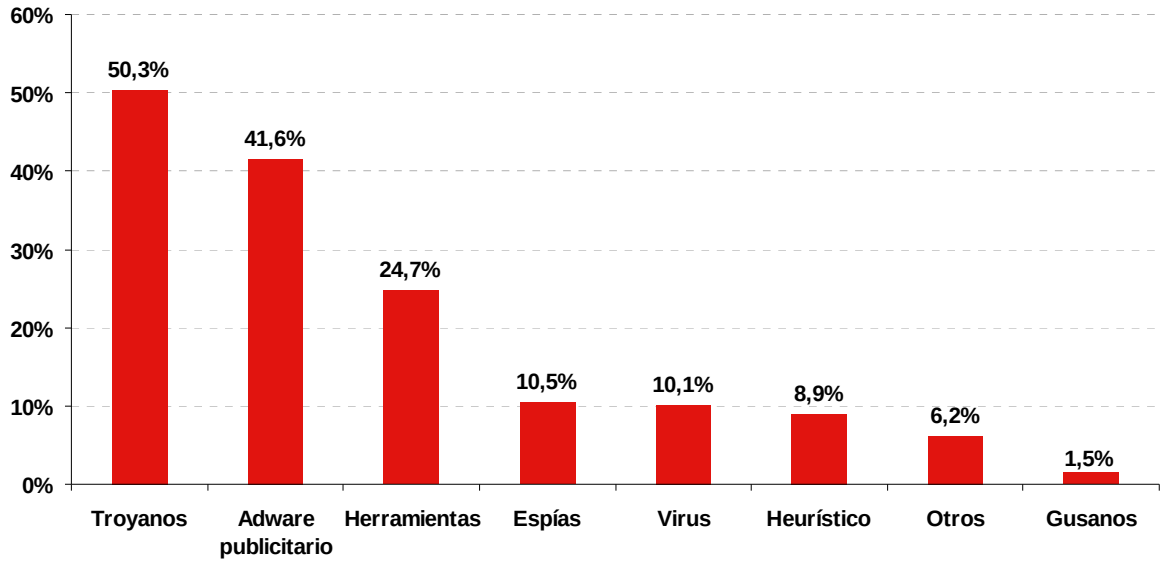
En el Gráfico 46 se presenta el análisis de composición de incidencias de códigos maliciosos hallados en los equipos de los hogares españoles panelizados.

Los tipos de *malware* más frecuentes encontrados en los ordenadores analizados han sido principalmente los *troyanos y el software publicitario*. Más del 40% de los ordenadores muestran presencias de cada uno de estos códigos maliciosos. En concreto un 41,6% de los equipos presentan *adware* y un 50,3% *troyanos*. Hay que destacar el hecho de que dentro de los troyanos se engloban las familias comentadas en el epígrafe 8.2.5 (dialers o marcadores, keyloggers o captadores de pulsaciones, bankers, puertas traseras…). Las *herramientas de intrusión* con un 24,7%, las incidencias de programas espía con un 10,5% y los *virus* con un 10,1%, son los siguientes tipos de malware con mayor porcentaje de incidencia.

Los gusanos tienen actualmente muy poca penetración, y se encuentran en un 1,5% de los equipos analizados. Por otro lado es destacable el hecho de que aun a pesar de utilizar 30 motores de antivirus un 8,9% de los ordenadores tengan malware detectado de manera heurística (es decir que no ha sido posible categorizarlo ni darle un nombre). Este porcentaje podría incrementarse si sólo se utilizara un motor antivirus, ya que el número de firmas que cada solución comercial contiene es limitado.

La categoría “Otros” con un 6,2% muestra los ordenadores que están infectados con malware de alguno de los siguientes tipos: *bromas* (jokes), *exploits*, *scripts maliciosos* o *rootkits.* Todos ellos tienen una presencia marginal cuando se consideran de manera independiente.

Gráfico 46: Presencia de malware por categorías (% sobre el total de ordenadores escaneados)



Fuente: INTECO

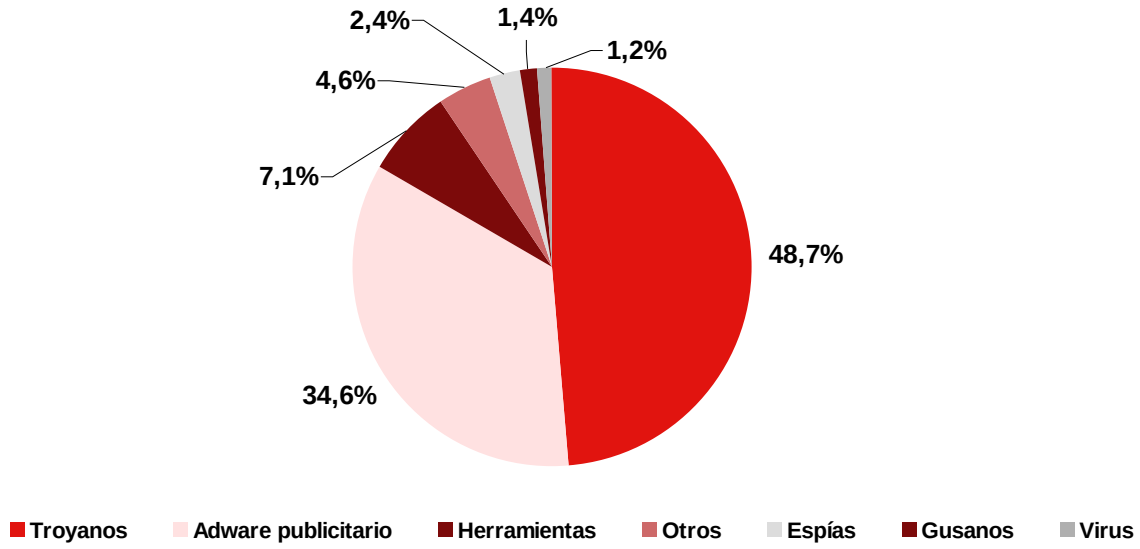
8.4 Variantes por categoría

En este epígrafe se muestra como se reparte el malware identificado durante el estudio atendiendo a variantes únicas detectadas por categoría (cuenta como 1 cada variante detectada con independencia del número de veces que se haya detectado en los equipos analizados).

Como puede observarse en el Gráfico 47, la categoría de los *troyanos* es la que presenta una mayor diversidad de variantes, con un 48,7% sobre el total. Los *troyanos* son el tipo de *malware* que más proliferación tiene en la actualidad. En segundo lugar destaca el *software publicitario* o *adware*, cuyas variantes suponen un 34,6% del *malware* único detectado. Destacan en comparación, por su escasa representatividad, los *virus* (1,2%) y *gusanos* (1,4%), de los que no se están produciendo actualmente muchas nuevas variantes.

Las detecciones heurísticas se han considerado en esta ocasión parte del grupo “Otros” puesto que muchas variantes realmente diferentes pueden ser catalogadas por heurística con el mismo nombre.

Gráfico 47: Diversidad de variantes de código malicioso (%)



Fuente: INTECO

La gran proliferación de *troyanos* y *adware* frente a *virus* y *gusanos* se explica porque actualmente la producción de *malware* está muy relacionada con el fraude, muchos de los nuevos especimenes tienen como objetivo el lucro de sus creadores a costa de los usuarios infectados. En este nuevo escenario los *troyanos* y el *adware* son los códigos maliciosos más productivos para las estafas, por eso se crean mas que otros tipos de *malware*.

Por ejemplo, los *troyanos* especializados en el robo de información confidencial, como los *bankers* dirigidos a clientes de entidades financieras por Internet, permiten suplantar la identidad de los usuarios legítimos infectados y realizar transacciones fraudulentas. Los *adware*, por su parte, se lucran a través de publicidad y anuncios fraudulentos que hacen aparecer en los sistemas infectados. Entre otras estrategias suelen hacer aparecer anuncios de forma indiscriminada, o redirigen a páginas falsas cuando el usuario se interesa por un determinado tema o producto a través de los buscadores de Internet.

Las características de los *virus* y *gusanos* podrían utilizarse para propagar los *troyanos* y el *adware*, pero actualmente este tipo de técnicas no compensa a los creadores de *código malicioso*, ya que tienen una dificultad más elevada, y sus códigos se exponen con más facilidad a ser descubiertos por los laboratorios *antivirus*, los *análisis heurísticos* y las nuevas soluciones basadas en el análisis del comportamiento. De ahí que cada vez existan menos variantes de reciente aparición de los mismos.

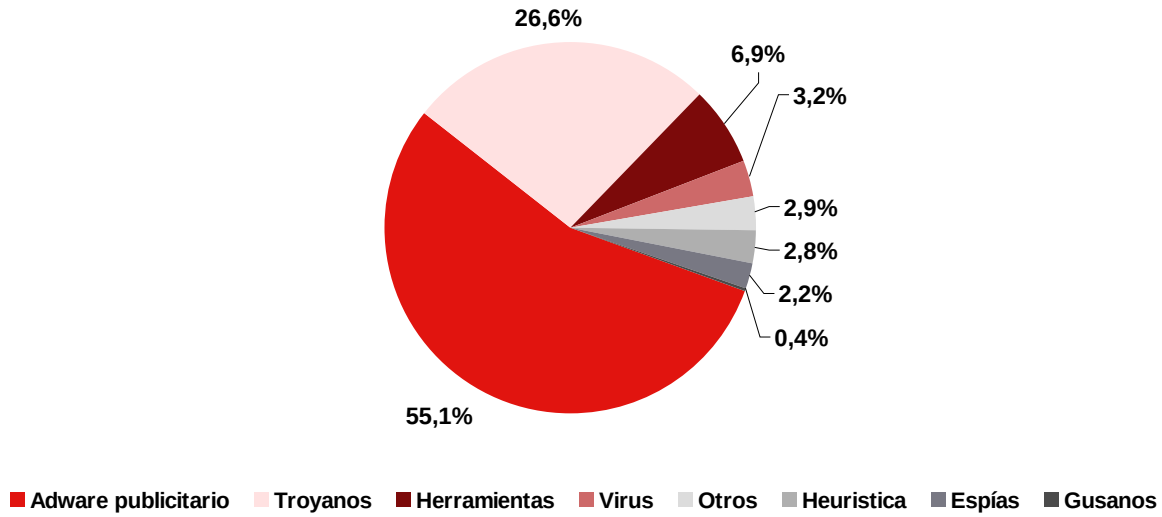
8.5 Total archivos infectados por categoría

En el siguiente indicador, Gráfico 48, se contabiliza el número total de archivos infectados detectados por categoría (se contabiliza cada archivo detectado infectado en el mismo o diferentes equipos sea o no de la misma variante de *malware*).

Cabe señalar que el *adware*, sin ser el *malware* que más variantes tenía según el indicador anterior, infecta el 55,1% del total de archivos infectados que se han detectado en el estudio. Le siguen los *troyanos*, con un 26,6% de infecciones del total de archivos infectados por todo el malware, a pesar de estar presentes como se indica en el Gráfico 46, en el 50,3% de los equipos.

La razón por la cuál habiendo más variantes distintas de *troyanos* se encuentran más archivos infectados por *adware* viene motivada porque la instalación de un *adware* incluye varios archivos y componentes por cada equipo infectado, mientras que la infección de un *troyano* suele ser motivada por un único archivo.

Gráfico 48: Archivos infectados por familia de código malicioso



Fuente: INTECO

Además, la distribución de *troyanos* se realiza de forma más segmentada y discreta. Actualmente un creador de *troyanos* suele crear decenas de variantes al día, con las mismas funcionalidades pero con pequeñas variaciones en su código o tratadas con *empaquetadores*. A continuación distribuye cada variante de forma separada. Esta forma de proceder dificulta que todas las variantes puedan ser detectadas rápidamente por los laboratorios antivirus.

Por norma general el *adware* va adjunto de forma más o menos visible a un programa que se presenta como útil al usuario, que suele instalarlo sin ser consciente de la "funcionalidad" añadida del *adware*. Estos programas que hospedan al *adware* no se actualizan tan frecuentemente, por lo que el *adware* que los acompaña tampoco. En definitiva, los creadores de *adware* no generan tantas variantes diferentes como los creadores de *troyanos*, el *adware* suele ser más estable en el tiempo.

8.6 Riesgo máximo por equipo analizado

Para este indicador, cuyos resultados se expresan en el Gráfico 49, se consideran 4 grados de riesgo en función del tipo de *malware* más peligroso detectado en cada equipo según la siguiente distribución:

- **Riesgo Alto**: *troyanos (de puerta trasera, bancarios,* capturadores de pulsaciones o *keyloggers,* marcadores o *dialers*, *etc.)*, *virus*, *gusanos*, *exploits y rootkits*
- **Riesgo Medio**: programas publicitarios maliciosos (*adware)*, programas espía (*spyware)*, *heurístico*, *scripts*
- **Riesgo Bajo**: *bromas*, *herramientas de intrusión*
- **Sin Riesgo**: equipos donde no se detecta *malware*

No obstante, el *malware* del tipo "herramienta" puede tener un riesgo variable dependiendo de si ha sido instalada conscientemente por el usuario legítimo del equipo o por un tercero sin su conocimiento[15]. Por ello en este indicador se ha aplicado por defecto el nivel de riesgo bajo, aunque en algunas circunstancias un *malware* catalogado como herramienta pueda ser de riesgo alto.

Por otro lado ha de tenerse en cuenta que los *scripts* o el *malware* detectado heurísticamente pueden ser de riesgo alto en algunos casos.

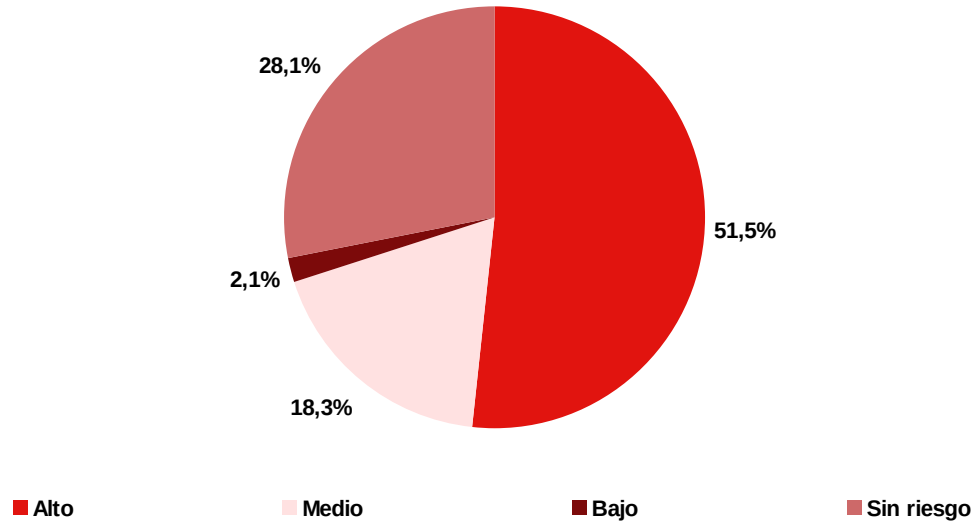
Así, en el caso de los *heurísticos*, al ser una detección genérica y no concreta, no se puede determinar la gravedad del *malware*. Por lo general las soluciones antivirus tienen las heurísticas optimizadas para detectar especimenes como *virus*, *gusanos* o *troyanos*, por lo que en ocasiones serán de riesgo alto. También hay que tener en cuenta que este tipo de detecciones también tienen cierto margen de error. Dada la variabilidad de los tipos de *malware* que pueden ser detectados bajo esta categoría, se ha optado por situarla como de riesgo medio.

[15] Por ejemplo, determinadas herramientas de control remoto, como por ejemplo VNC, puede ser de uso legítimo, pero también podría ser aprovechada por un atacante para espiar o controlar un equipo de forma remota. Igualmente, una utilidad para hacer análisis de red, como un simple analizador de puertos TCP, será detectada por los antivirus como "tool" o herramienta, y sin embargo la mayoría de las ocasiones será un software instalado conscientemente por el usuario.

El caso de los *scripts* es distinto. Por normal general los *scripts* maliciosos están relacionados con la explotación de vulnerabilidades en el navegador o el correo electrónico para instalar *malware* adicional de forma automática. En ese sentido debería considerarse de riesgo alto. Sin embargo la existencia de scripts maliciosos en un equipo no es indicativa de que esa explotación se haya llevado a cabo. Por ejemplo, un usuario con el sistema actualizado (sin vulnerabilidades en el navegador) podría visitar una página con un script malicioso, ese no podría llevar a cabo ninguna acción maliciosa en el sistema, pero quedaría almacenado en la caché del navegador y podría ser detectado por un antivirus o la propia herramienta de escaneo. Por ello finalmente se ha optado por considerar los scripts como riesgo medio.

Así las cosas, el 51,5% de los equipos analizados está infectado por, al menos, un código malicioso considerado de peligrosidad alta. El 18,3% de los equipos está en riesgo medio, en un 2,1% sólo se detecta "*bromas*" o "*herramientas*", y en el 28,1% no se detecta *malware*.

Gráfico 49: Clasificación de los ordenadores en función del riesgo (%)



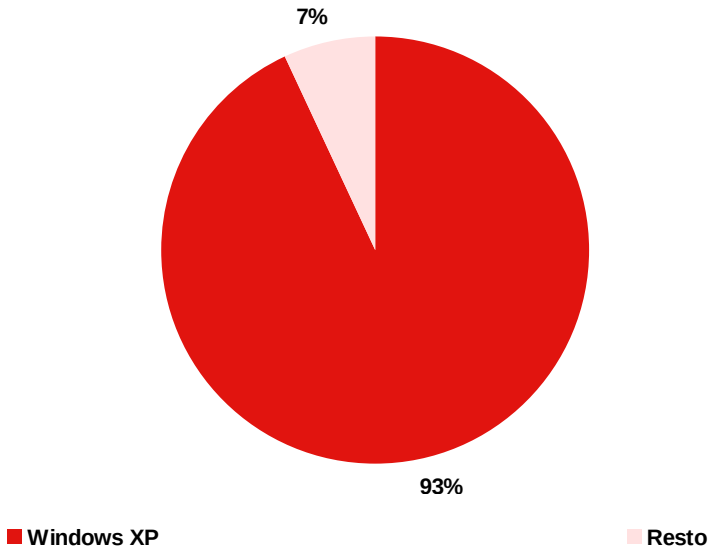
Fuente: INTECO

8.7 Sistemas operativos y malware

Si bien como se recordará en la muestra total (6.357 encuestados) un 97% de los usuarios declaraba tener instalado un sistema operativo Windows, un 2% se repartía entre Apple Mac OS y GNU/Linux y un 1% desconocía el sistema operativo de su equipo. Sin

embargo, en la muestra panelizada (3.068 equipos)[16], Windows es el sistema operativo con mayor representación en los equipos auditados, con un 99% del total. Como se observa en el Gráfico 50 destaca la versión XP de dicho sistema operativo con penetración en el 93% de los sistemas.

Gráfico 50: Distribución de sistemas operativos (%)



Fuente: INTECO

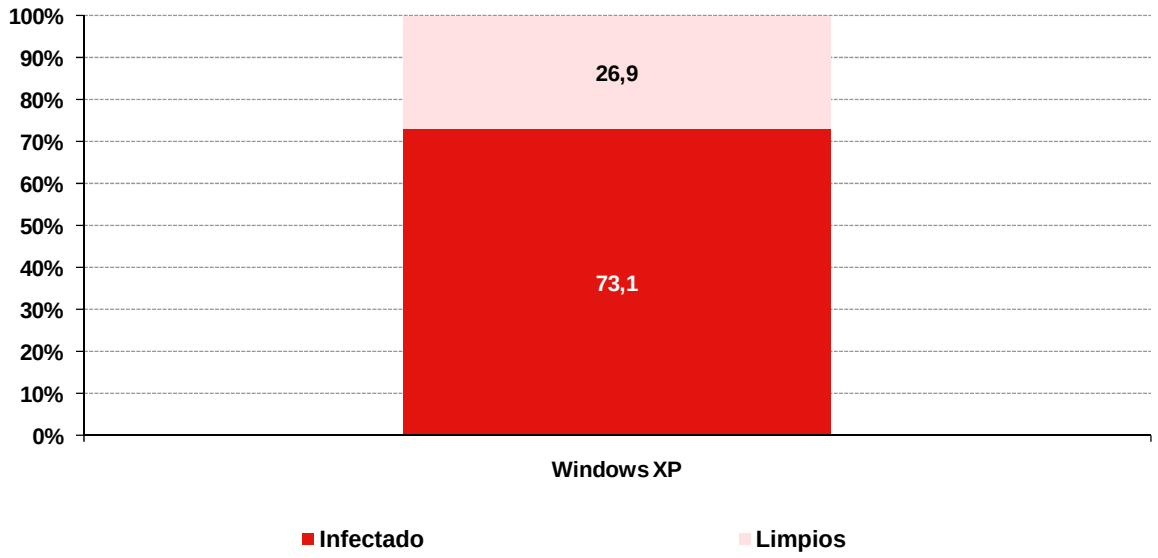
Una posible lectura de esta concentración puede hacerse en base a que Windows es el sistema operativo con mayor representación en el estudio (presente en el 99% de los equipos analizados, destacando Windows XP en el 93% de los sistemas).

8.7.1 Detección de malware en equipos con sistema operativo Windows XP

Como cabría esperar, dada la amplia representación en la muestra del estudio, el porcentaje de infección de los equipos con Windows XP (Gráfico 51) se sitúa en un 73,1%, muy similar al del total de los equipos que se sitúa en un 72,6%.

[16] Como ya se ha comentado en la metodología, la muestra total de 6.357 refleja algo mejor los datos de hábitos y opinión, y su análisis ayuda a comprender mejor los resultados que se arrojan de la muestra panelizada de 3.068 individuos.

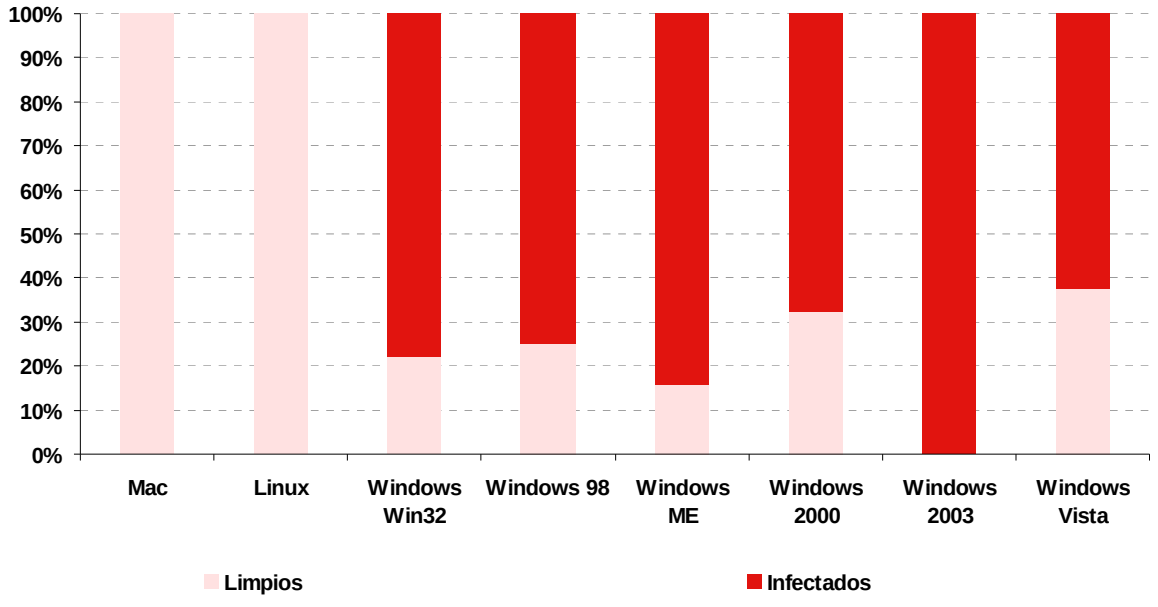
Gráfico 51: Distribución de código malicioso en Windows-XP



Fuente: INTECO

A pesar de que el escaso porcentaje en la muestra de otras versiones de Windows, incluso con menor representación que los S.O. Mac y Linux, no permite realizar estimaciones estadísticas robustas, se pueden correlacionar estas para detectar un patrón común que relaciona las infecciones de malware con el sistema operativo Windows, como muestra el Gráfico 52.

Gráfico 52: Distribución de código malicioso por sistema operativo (%)



Fuente: INTECO

Sin embargo, este hecho no debe llevar a conclusiones equivocadas. Por un lado, estos datos han de tomarse con extrema precaución dada la baja representatividad de la muestra, que no permite extraer conclusiones estadísticas contundentes. Además, es falso que sólo exista *malware* para Windows, y por supuesto, es falso que los ordenadores con sistemas operativos Mac o Linux estén libres de amenazas o ataques.

De hecho las plataformas Linux y Mac tienen *malware* específico conocido, e incluso en algunas ocasiones han protagonizado epidemias de cierta consideración (gusanos para plataformas Unix). También existen virus multiplataforma, como por ejemplo "Winux" capaz de infectar ejecutables Windows (PE) y Linux (ELF), o "Esperanto", un virus multiplataforma y multiprocesador para PC y Mac.

La herramienta que INTECO ha utilizado para los análisis de los equipos, detecta tanto malware de Windows, como Linux, Mac y otras plataformas (incluyendo sistemas operativos de dispositivos móviles como Symbian). Así pues el motivo por el que no se ha detectado malware en Linux y Mac es que el que exista malware conocido no quiere decir que estén propagándose de forma activa. Por ejemplo, la mayoría de los especimenes de malware conocidos para Mac son pruebas de concepto a modo de demostración que no han llegado a propagarse de forma significativa ni han tenido una repercusión directa entre los usuarios finales.

En el caso de Linux el malware más activo ha estado relacionado con gusanos que explotaban servicios relacionados con servidores, y no tanto con estaciones de trabajo o equipos domésticos.

Por último, también se debe ser consciente de que más del 99% de la producción actual de código malicioso está dirigida contra Windows. De manera independiente a consideraciones técnicas, es lógico pensar que los atacantes fijen su objetivo en la plataforma más extendida para conseguir el máximo número de infecciones.

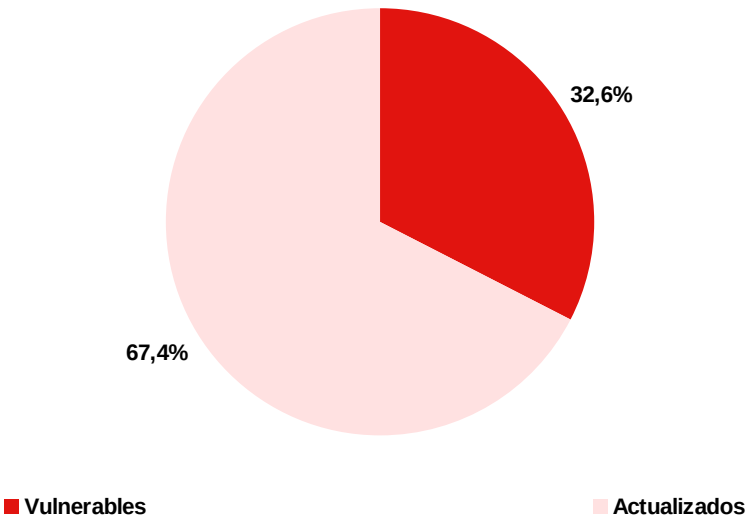
En resumen, si bien en la actualidad la producción de malware está focalizada en Windows, sin embargo, usuarios de otras plataformas deben ser conscientes del riesgo potencial de infectarse y no bajar la guardia.

8.8 Actualizaciones y vulnerabilidades críticas

El Gráfico 53 muestra como el 32,6% de los equipos analizados mantiene vulnerabilidades críticas en el sistema operativo, frente al 67,4% que se detectan correctamente actualizados.[17]

[17] Según la base de datos de vulnerabilidades de INTECO, con fecha junio del 2007, existen registradas 24.600 vulnerabilidades. De todas ellas un 9,6% consisten en vulnerabilidades que afectan a los distintos sistemas operativos. Es por ello que para minimizar los agujeros de seguridad del software no sólo es importante la actualización de los sistemas operativos, sino también del resto de programas instalados en los equipos.

Gráfico 53: Distribución de equipos infectados y vulnerabilidades (%)



Fuente: INTECO

Este indicador se centra en el estudio de la plataforma Windows y en las actualizaciones y parches de seguridad oficiales de Microsoft. Se considera un equipo vulnerable si se detecta una vulnerabilidad considerada por Microsoft en sus boletines de seguridad como de riesgo crítico, normalmente asociadas a la posibilidad de ejecución de código remoto.[18]

A efectos prácticos, los equipos considerados vulnerables en este estudio mantienen problemas de seguridad que permitirían a un atacante lograr el control del equipo de forma remota o a un malware infectarlo de forma automática, sin necesidad de que el usuario ejecute el código malicioso.

8.8.1 Correlación entre vulnerabilidades e infecciones de malware

Mantener el sistema operativo del equipo actualizado no previene la infección por malware de forma absoluta, aunque ayuda.

[18] Con la política actual de Microsoft, de publicar periódicamente actualizaciones el segundo martes de cada mes, este indicador podría leerse como que cerca de 7 de cada 10 usuarios sigue fielmente esa recomendación de seguridad y conscientemente actualiza su equipo.

Otra lectura, tal vez más real, sería la de que una buena parte de esos usuarios con Windows XP Service Pack 2 tienen activada la opción de actualizaciones automáticas, por lo que de forma transparente y desatendida consiguen actualizar sus equipos sin estar pendientes de hacer esta operación de forma manual. Aunque la muestra es pequeña, es un hecho que los equipos vulnerables aumentan de forma considerable en versiones anteriores a Windows XP, bien porque no tienen la funcionalidad de actualizarse de forma automática y desatendida, bien porque ya finalizó el ciclo de soporte y ya no disponen de actualizaciones para las nuevas vulnerabilidades que surgen.

Los datos que arroja el estudio, mostrados en el Gráfico 54, dan un pequeño margen a favor de los equipos actualizados frente a los que presentan vulnerabilidades críticas. En concreto en el 75,0% de los equipos vulnerables se detectó malware, frente al 71,5% de infectados en los equipos actualizados.

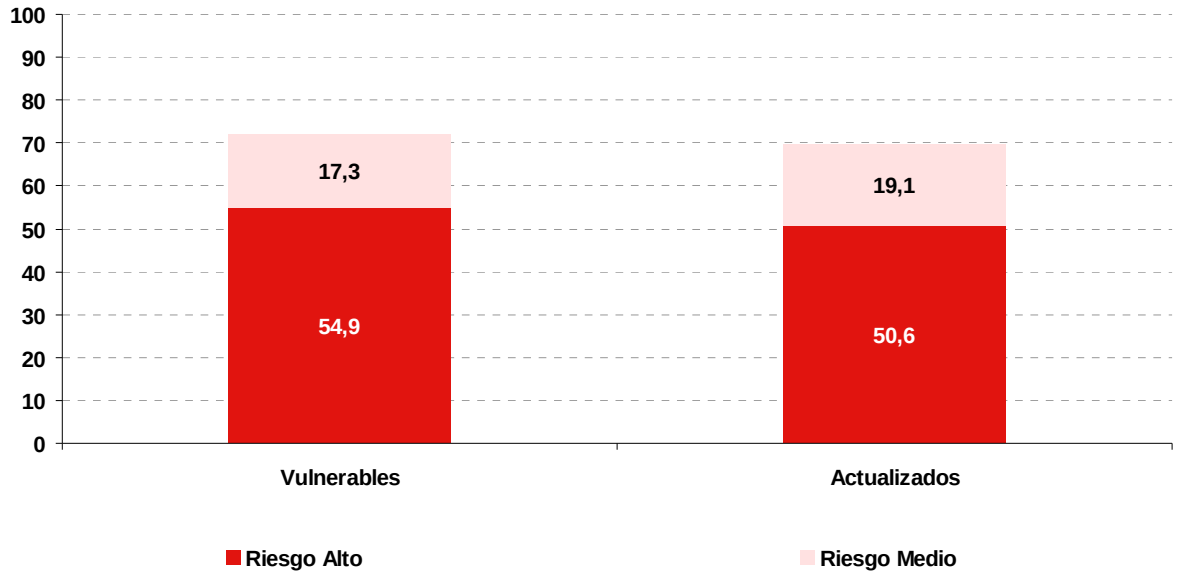
Gráfico 54: Comparativa Infección/Vulnerabilidad (%)

Fuente: INTECO

Si se analiza el riesgo máximo y medio en los equipos infectados se observa también (Gráfico 55) una diferencia similar. En concreto el 54,9% de los equipos vulnerables está infectado con *malware* considerado de riesgo alto, frente al 50,6% en los equipos actualizados.

Este indicador también muestra una mayor infección de riesgo medio en equipos actualizados (19,1%) que vulnerables (17,3%). Aunque en principio pudiera parecer una incongruencia, en realidad se explica por la naturaleza de los tipos de malware que se catalogan como riesgo medio: *software publicitario* (*adware*) y *herramientas de intrusión* o "*tools*". Este tipo de *malware* se caracteriza porque suele ser instalado a demanda por el usuario o por acompañar a software a priori legítimo, no utilizando ninguna vulnerabilidad en su fase de propagación o infección.

Gráfico 55: Comparativa Riesgo/Vulnerabilidad (%)



Fuente: INTECO

En resumen, se observa que **los equipos actualizados mantienen menos infecciones y de menor riesgo, no obstante, la diferencia frente a los equipos vulnerables es relativamente pequeña**. Por tanto, mantener los equipos actualizados es una medida de seguridad muy recomendable frente a intrusiones y al *malware*, pero como se puede comprobar, no es suficiente ni es determinante a la hora de prevenir los diferentes tipos de *malware* y canales de infección actuales.

En este sentido, es posible preguntarse porqué parece poco determinante la actualización de los equipos frente a las incidencias de código malicioso.

La explotación de vulnerabilidades por parte del *malware* destaca en los gusanos de red, como "Blaster" o "Sasser" que protagonizaron epidemias masivas en el año 2004. Estos gusanos conectaban con servicios del sistema operativo Windows a través de las redes TCP/IP e infectaban de forma automática los equipos vulnerables que no estuvieran puntualmente actualizados.

En consecuencia, el descenso en la proliferación de nuevos *gusanos* (que como se ha visto en el indicador de distribución de las incidencias de tipos de malware) tiene una escasa representación, y la popularización de la banda ancha, hacen que este tipo de *gusanos* de red tengan un impacto muy limitado entre los usuarios domésticos.

Este segundo motivo resulta interesante: la banda ancha como protección contra los gusanos de red.

Así, muchas de las configuraciones de banda ancha protegen al equipo doméstico de conexiones directas TCP/IP entrantes desde Internet.[19]

Es por ello que a día de hoy los *gusanos* de red tienen un mayor impacto en las redes corporativas, ya que en este tipo de redes la comunicación suele ser transparente entre sistemas y tampoco se ha popularizado la utilización de firewalls personales. Así, otro aspecto a favor de la ausencia de infecciones por *gusanos* de red la podemos encontrar en la inclusión de la funcionalidad de firewall personal en los sistemas Windows XP.

Finalmente es preciso señalar que actualmente el mayor riesgo para los usuarios domésticos con equipos vulnerables proviene del spam y de la navegación por páginas webs no confiables. Es una práctica habitual de los atacantes aprovechar vulnerabilidades críticas en el navegador para descargar e instalar *troyanos* de forma automática. Este tipo de infecciones es probable que refleje las diferencias entre equipos vulnerables y actualizados en este estudio.

Es decir, si bien las vulnerabilidades del sistema operativo siguen siendo utilizadas por el malware que se produce actualmente, existe una gran proliferación de códigos maliciosos que explotan vulnerabilidades de programas ajenos al sistema operativo

Por ello es muy recomendable mantener el sistema operativo actualizado, así como el navegador, el cliente de correo que se utilice por defecto y en general todo el software que se haya instalado en el equipo. También serán de ayuda herramientas anti-spam, y hacer caso omiso de las direcciones de páginas webs de fuentes no confiables.

8.9 Antivirus y malware

Como resultado del escaneo de los equipos de la muestra panelizada se obtiene el Gráfico 56, que muestra que en el 86,9% de los equipos analizados se detecta una solución antivirus activa, frente al 13,1% de los equipos sin antivirus.

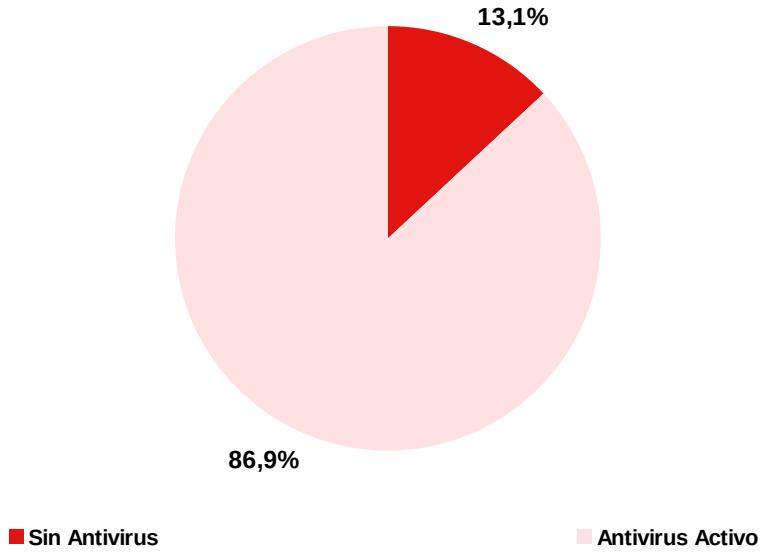
La herramienta de escaneo detecta más de 30 marcas antivirus y varias versiones de cada una de ellas. Para considerar que un equipo tiene un **antivirus activo** es necesario que esté residente en memoria, no basta con que lo tenga instalado en el sistema pero desactivado.

[19] Por ejemplo, en una configuración típica, el usuario de banda ancha dispone de un router ADSL con un interfaz público y otro privado. El interfaz público está configurado en el propio router y es el que posee la IP pública en Internet, mientras que el otro interfaz con una IP privada es el que conecta con el equipo del usuario.

Esta configuración permite al usuario conectarse a Internet utilizando como pasarela el router, pero impide que de forma indiscriminada un atacante o malware pueda interrogar los puertos y servicios del ordenador del usuario desde Internet. Por ejemplo, los gusanos "Sasser" o "Blaster" en Internet sólo tendrían acceso a la IP pública que pertenece al router, y no encontrarían en esa IP los puertos abiertos TCP/IP del equipo del usuario, impidiendo su infección aunque se trate de un sistema vulnerable.

Destaca el alto porcentaje de equipos con antivirus, no en vano es la solución de seguridad informática más conocida y extendida, indicativo de que los usuarios son conscientes de la necesidad de este tipo de protecciones frente al *malware*.

Gráfico 56: Presencia de antivirus en los equipos (%)



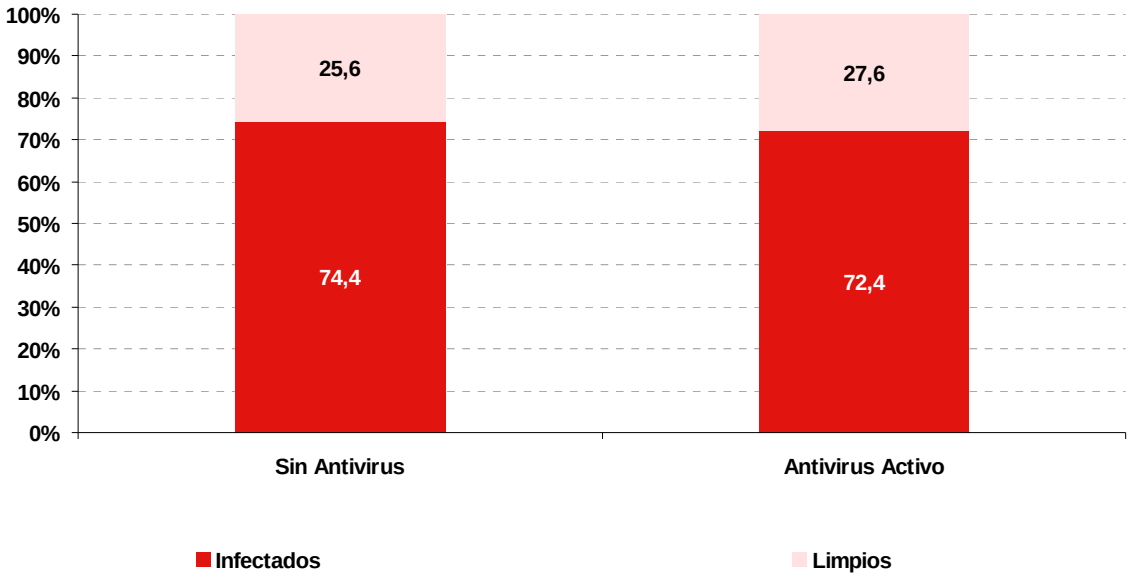
Fuente: INTECO

8.9.1 Correlación entre vulnerabilidades e infecciones de malware

Las soluciones antivirus no garantizan la ausencia de infecciones, aunque ayudan en su prevención como se observa en el Gráfico 57

Atendiendo al número de equipos infectados, los datos que arroja el estudio dan un pequeño margen a favor de los equipos con antivirus activo frente aquellos donde no se detecta un antivirus. Así el 74,4% de los equipos sin antivirus se encuentran infectados, frente al 72,4% de infectados en los equipos con antivirus activo. Estos datos han de ser tomados con cautela ya que el volumen de equipos que no dispone de soluciones antivirus es relativamente pequeño.

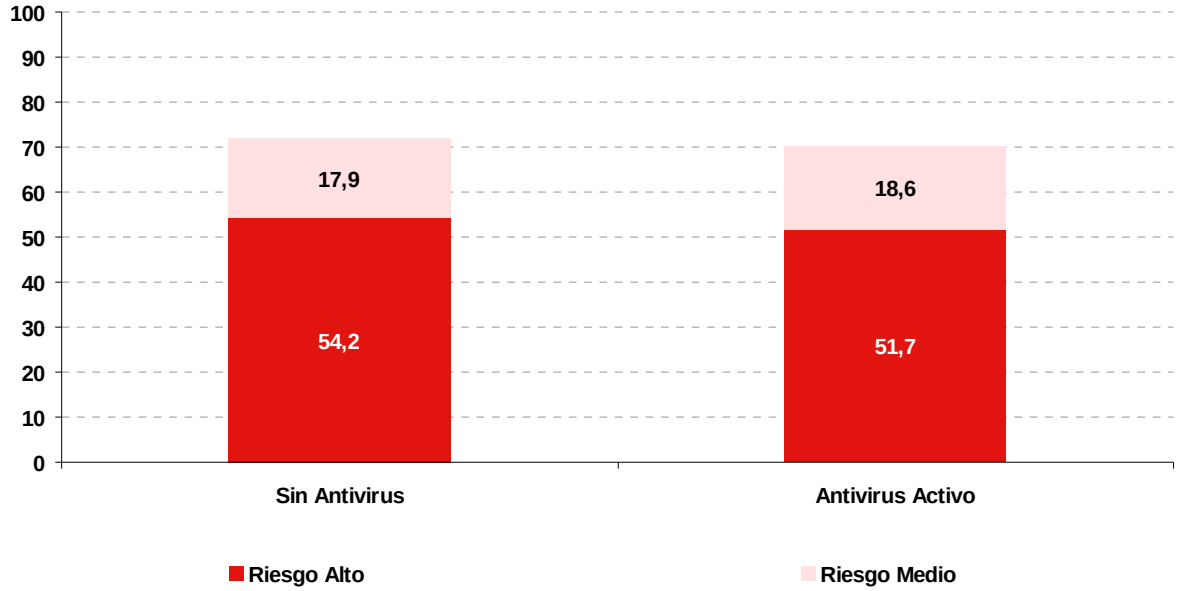
Gráfico 57: Comparativa Infección/Antivirus (%)



Fuente: INTECO

Si atendemos al riesgo máximo y medio en los equipos infectados observamos en el Gráfico 58 una diferencia similar. En concreto el 54,2% de los equipos vulnerables está infectado con malware considerado de riesgo alto, frente al 51,7% en los equipos actualizados.

Gráfico 58: Comparativa Riesgo/Antivirus (%)

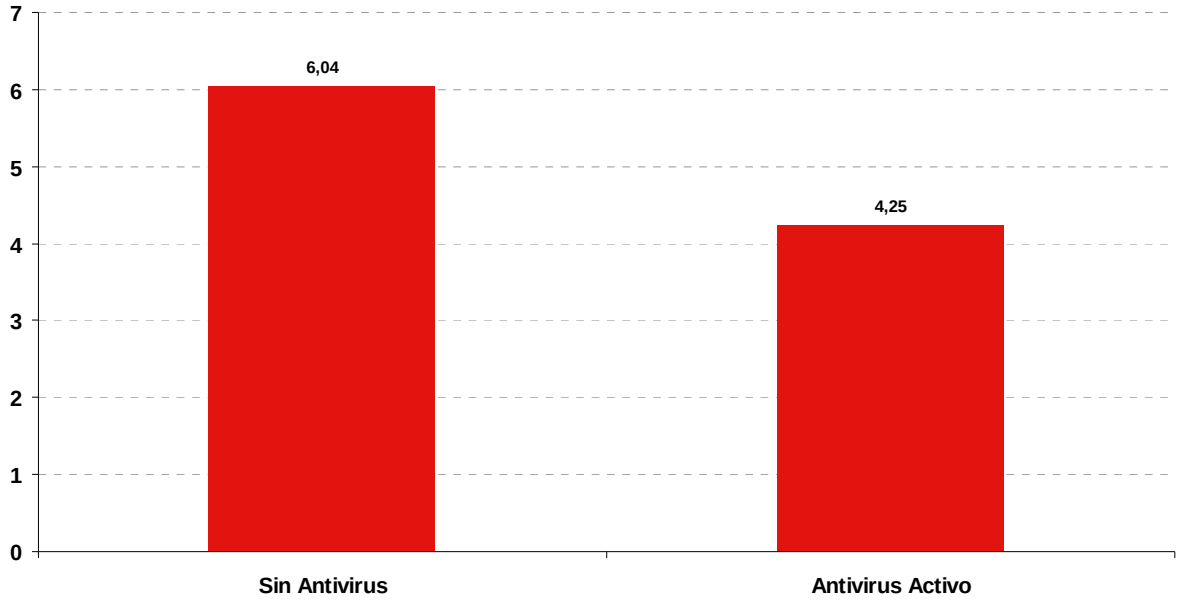


Fuente: INTECO

Como ocurriera en el caso de los equipos actualizados y no actualizados (vulnerables), observamos de nuevo que los equipos con antivirus activo tienen más infecciones de riesgo medio. Hay que recordar que el *malware* catalogado como riesgo medio es el adware y las herramientas ("tools"), que se caracterizan porque suelen ser instaladas a demanda por el usuario o porque acompañan a software a priori legítimo. Este resultado puede leerse como que los usuarios con antivirus son menos precavidos a la hora de instalar software no confiable, tal vez debido a la falsa sensación de seguridad que les supone tener instalado un antivirus.

Por otro lado, calculando el número de archivos con *código malicioso* detectado en los sistemas infectados, encontramos que los equipos con antivirus tienen una media de 4,25 archivos de *malware*, mientras que en los equipos sin antivirus la media asciende a 6,04. (Gráfico 59)

Gráfico 59: Número medio de archivos infectados en función del uso de antivirus



Fuente: INTECO

Aunque todos los indicadores detectan una mayor protección en los equipos con antivirus respecto a los que no lo poseen, puede sorprender que la diferencia sea tan escasa. Es significativo que prácticamente la mitad de los equipos con antivirus, un 51,7%, estén infectados por al menos algún malware considerado de riesgo alto (*troyanos, virus, gusanos, keyloggers, dialers, exploits, bankers, rootkit*).

Los antivirus son una solución recomendable para prevenir la infección por *malware*, al igual que es una medida de seguridad beneficiosa mantener actualizados puntualmente los sistemas. Sin embargo, como hemos podido constatar anteriormente, ni la

actualización del sistema ni la protección que ofrece una solución antivirus es infalible. Por definición, un antivirus no puede detectar el 100% del malware que puede estar siendo distribuido.

Por ello, junto a las medidas de seguridad es imprescindible que el usuario sea consciente de los riesgos y amenazas, y que actúe de forma responsable para prevenir la infección de sus sistemas. Precisamente aquellos usuarios que crean que están muy seguros porque cuentan con un antivirus instalado son los más proclives a realizar acciones de riesgo, como por ejemplo instalar software que proviene de fuentes no confiables, navegar por webs de forma indiscriminada y aceptar la instalación de controles ActiveX, descarga y uso de contenidos de redes P2P que pueden hospedar código malicioso, etc.

Esto viene a constatar que los antivirus, aunque recomendables, son sólo una capa más de seguridad contra el código malicioso, pero que por sí solos no pueden proteger contra todas las amenazas actuales.

Es por ello que hay que insistir en crear una cultura de seguridad. Es necesario que los usuarios sean conscientes de la utilidad de las soluciones como los antivirus, firewalls, antispam, actualizaciones de seguridad, etc., pero también deben conocer sus limitaciones, las amenazas reales, y las recomendaciones adicionales, para que no se cree una falsa sensación de seguridad. Se presenta vital para aumentar la seguridad el proporcionar a los usuarios de una mayor formación de cara a realizar un uso responsable y seguro de las nuevas tecnologías, con hábitos de uso basados en la precaución y la protección.

8.9.2 Explicación del elevado porcentaje de equipos infectados.

En el último año se ha disparado la producción de malware, en especial de troyanos, hasta unos niveles nunca alcanzados.

Los fabricantes de herramientas de protección antivirus reconocen[20] que, si bien nunca un antivirus ha conseguido alcanzar el 100% en la detección y prevención del malware, en los últimos tiempos este porcentaje se ha visto reducido debido a la producción de nuevos tipos de malware. *Los creadores de malware están ganando la batalla por fuerza bruta, distribuyendo cada día cientos de nuevos especimenes, provocando el desbordamiento de la capacidad de análisis de los laboratorios antivirus.*

En la actualidad, como se ha visto, en la tipología y distribución porcentual en los que se desglosa el malware, apenas se produce malware del tipo virus o gusano, que a priori pueden ser los más complicados de programar. Por contra se ha incrementado enormemente la producción de troyanos, que por norma general suelen requerir menores

[20] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010041

conocimientos avanzados de programación ya que no deben preocuparse por la replicación[21].

Además, los atacantes no crean los troyanos desde cero, lo que realizan son pequeñas modificaciones en troyanos ya existentes, con el objetivo principal de cambiar sus firmas de identificación para no ser detectados por los antivirus, lo que reduce mucho el tiempo necesario para obtener una variante y amplía el tiempo preciso para su detección.

Así mismo ha aumentado notablemente el uso de "packers" y compresores de ejecutables. Este tipo de herramientas comprimen un ejecutable y modifican de forma automática la firma superficial del malware, de manera instantánea y con tan sólo pulsar un botón, sin necesidad de tener conocimientos de programación. El resultado es que la generación de variantes que puedan evitar la detección de los antivirus está al alcance de un perfil muy numeroso y heterogéneo de personas. Por tanto, ya no se requiere ser un programador avanzado para crear un *virus* como antaño, ni se requieren tantas horas de desarrollo.

Tampoco se debe olvidar que los creadores de *malware* se han profesionalizado. Si la primera generación de creadores de virus buscaba diseñar *malware* que llamara la atención y/o ocasionara grandes epidemias, en la actualidad asistimos a una generación de creadores de *malware* que prefiere diversificar sus ataques, pasar desapercibidos tanto en los equipos infectados como para los laboratorios antivirus y que tiene como claro objetivo el lucro.

El creador de malware profesional es consciente de que si desarrolla un *código malicioso* autoreplicante con una gran capacidad de distribución (como pudiera ser un *virus* o un *gusano*), aumenta en gran medida la probabilidad de que su creación sea neutralizada por los antivirus. En primer lugar porque las tecnologías heurísticas de análisis de comportamiento y configuraciones de seguridad e IDS en hosts y redes, están más especializadas en detectar los patrones de propagación de un *virus* o un *gusano*. En segundo lugar porque al distribuirse de forma tan rápida es más fácil que la muestra llegue en menos tiempo a los laboratorios antivirus para que sea analizada y desarrollen firmas específicas para su detección.

En cualquier caso, y a pesar de lo anteriormente expuesto, no se debe dudar de la utilidad de la instalación en nuestros equipos de las herramientas antivirus.

Aunque su eficacia, en comparación con épocas pasadas, ha descendido, sigue siendo una medida de seguridad necesaria, ya que protegen contra un gran porcentaje del malware que nos puede afectar. La situación actual es puntual y no deja de estar

[21] Hoy en día existen programas que ayudan a la creación de *malware,* y que en unos pocos pasos y con unas sencillas elecciones de características, son capaces de crear un *malware* personalizado según los requerimientos del atacante.

propiciada por los creadores de malware que están actuando por fuerza bruta, generando tanto código malicioso nuevo que no pueda ser manejado por los laboratorios antivirus.

Los fabricantes de software antivirus están trabajando en nuevas estrategias y tecnologías para afrontar esta nueva etapa, aumentando la celeridad con que se actualizan las firmas antivirus y diseñando nuevos métodos de detección heurísticos más agresivos y sistemas inteligentes que permitan aumentar su capacidad de identificar detectar malware nuevo no catalogado.

8.9.3 Situación real Vs. percepción del usuario

Por otra parte, el análisis de los ordenadores de los hogares españoles, ha puesto de manifiesto que, en la actualidad, el 67,4% de los ordenadores tienen actualizado el sistema operativo. Curiosamente, como podía observarse en la Tabla 8 sólo el 50,1% de los usuarios españoles de Internet declara realizar estas actualizaciones. Esto significa que la automatización de las actualizaciones está ayudando en gran medida a mejorar el nivel de seguridad de los ordenadores conectados a la red. Por el contrario, se ha constatado que el 87% de los equipos tienen un antivirus activo en el momento del análisis, siendo estas cifras algo menores que las declaradas en la entrevista, donde un 95% de los encuestados manifiesta tener instalado un antivirus en la actualidad. Esta diferencia pone de manifiesto que en torno a un 8% de los encuestados desconoce el estado real, en cuanto a programa de seguridad antivirus, de la protección de su equipo.

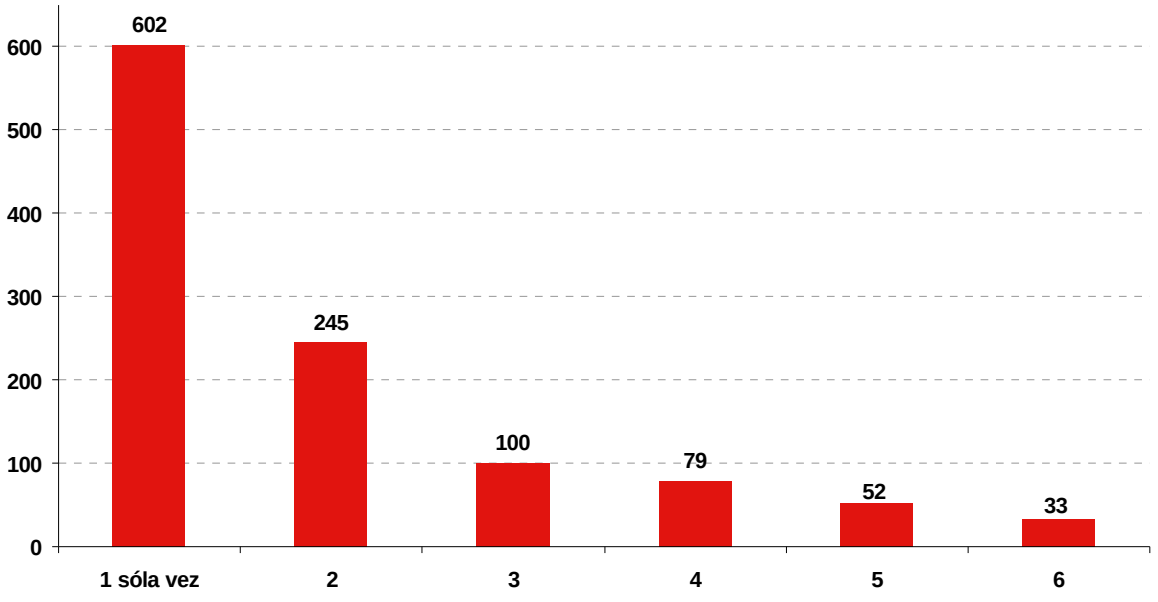
Hay que señalar en este punto, que parte de los terminales de acceso a Internet desde el hogar, son compartidos por dos ó más personas. Ese hecho puede explicar en parte el hecho de que algunos usuarios desconozcan realmente el nivel de protección, si no son ellos quienes se encargan principalmente de su mantenimiento.

8.10 Características del malware detectado

En este apartado se desglosan y analizan algunas de las familias y especimenes de malware más significativos detectados durante el presente estudio.

En total se detectan más de 10.000 archivos infectados con una media de 4,42 códigos maliciosos por equipo infectado. El total de archivos infectados se reparten entre 1.344 códigos maliciosos diferentes, 602 de los cuales se detectan en una sola ocasión como se indica en el Gráfico 60.

Gráfico 60: Número de detecciones de códigos maliciosos



Fuente: INTECO

Este indicador viene a constatar la gran proliferación y heterogeneidad del código malicioso actual, principal obstáculo para que los antivirus puedan llevar a cabo su función de prevención. Hace apenas dos años la mayoría de infecciones se concentraban en una decena de gusanos de distribución masiva que lograban afectar a miles de sistemas. Sin embargo, actualmente el 45% (602 especimenes) de las infecciones están protagonizadas por códigos maliciosos distintos entre sí y que sólo se han encontrado en una única ocasión entre todos los sistemas escaneados de la muestra.

Esta nueva situación también ha puesto en tela de juicio los rankings y los “Top-10” del malware más extendido, ya que en la actualidad el peligro real viene por parte del malware más heterogéneo cuyo reconocimiento y detección plantea una mayor dificultad para las soluciones antivirus, y no tanto por el malware que más difusión tiene y por tanto es más fácilmente detectado por las herramientas de seguridad.

8.11 Especimenes concretos detectados

A continuación se describen brevemente algunos especimenes concretos que, bien por el número de veces que ha sido identificado, bien por sus características, son casos representativos del malware detectado en esta oleada del estudio:

8.11.1 Adware o software publicitario

Adware-Hotbar: Detectado en el 10% de los equipos analizados, es la familia de adware más extendida. Su principal función es mostrar publicidad de forma indiscriminada a través

de banners y ventanas emergentes, o modificar las páginas de inicio y búsquedas del navegador. El autor o autores del Hotbar se lucran vendiendo los anuncios a terceros o con productos propios que publicitan ellos.

La infección se puede producir al instalar los ejecutables de la aplicación que se distribuye como una barra de herramientas con utilidades para el navegador. En otras ocasiones llega al usuario de forma más confusa, a través de controles ActiveX para el navegador Internet Explorer que pueden aparecer de forma espontánea al visitar ciertas páginas webs.

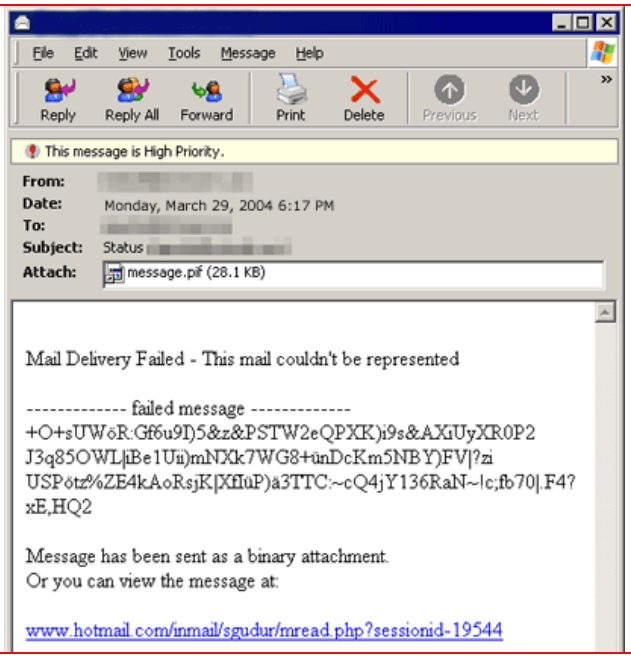
Gráfico 61: Ejemplo de visualización del adware hotbar en el escritorio

Fuente: INTECO

8.11.2 Gusanos

Email-Worm.Win32.NetSky.q: Este gusano de propagación masiva por correo electrónico se ha detectado en el 0,3% de los equipos infectados. Fue uno de los gusanos más representativos y con más capacidad de distribución en el 2004, año del que data este espécimen.

Gráfico 62: Ejemplo de correo utilizado por el gusano NetSky.q para propagarse



Fuente: INTECO

Para propagarse por correo electrónico aprovecha una vulnerabilidad de Internet Explorer que permitía su ejecución de forma automática con tan sólo visualizar el mensaje en Outlook. Su principal objetivo es la autopropagación, además llevaba a cabo un ataque de Denegación de Servicio (DoS) desde los sistemas infectados contra diversos sitios webs en determinadas fechas.

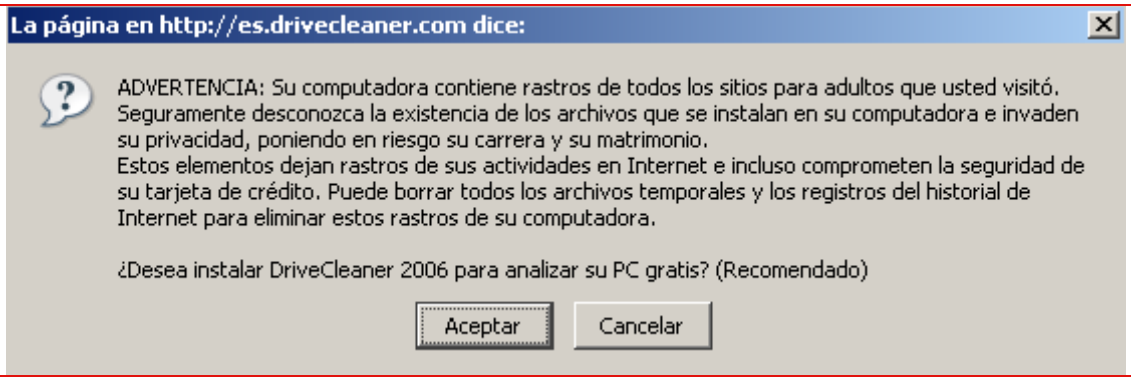
8.11.3 Troyanos

Winfixer: Detectado en el 7,9% de los equipos analizados, se incluye en su familia las variantes detectadas como "ErrorSafe", "WinAntiVirus" o "DriveCleaner". Dependiendo del motor antivirus puede ser catalogado como Adware o Programa no deseado, si bien por sus características encuadraría mejor en la denominación clásica de troyano.

Se caracteriza por intentar engañar al usuario creyendo que su ordenador tiene errores o virus a través de banners o ventajas emergentes, como la del Gráfico 63 al visitar páginas webs, ofreciendo al usuario una herramienta gratuita para corregir los problemas, que en realidad es el troyano.

Una vez instalado, el programa sigue detectando problemas en el sistema de forma ficticia y solicita al usuario que registre el programa, previo pago, para solucionarlo. El autor o autores de esta familia se lucran por la venta directa del programa engañando a los usuarios con errores y virus falsos. El daño puede ser mayor que el puramente económico, ya que también puede crear una falsa sensación de seguridad al usuario creyendo que ha adquirido un antivirus que le protegerá contra el malware.

Gráfico 63: Ejemplo de ataque del troyano Winfixer



Fuente: INTECO

Marcadores automáticos o dialers

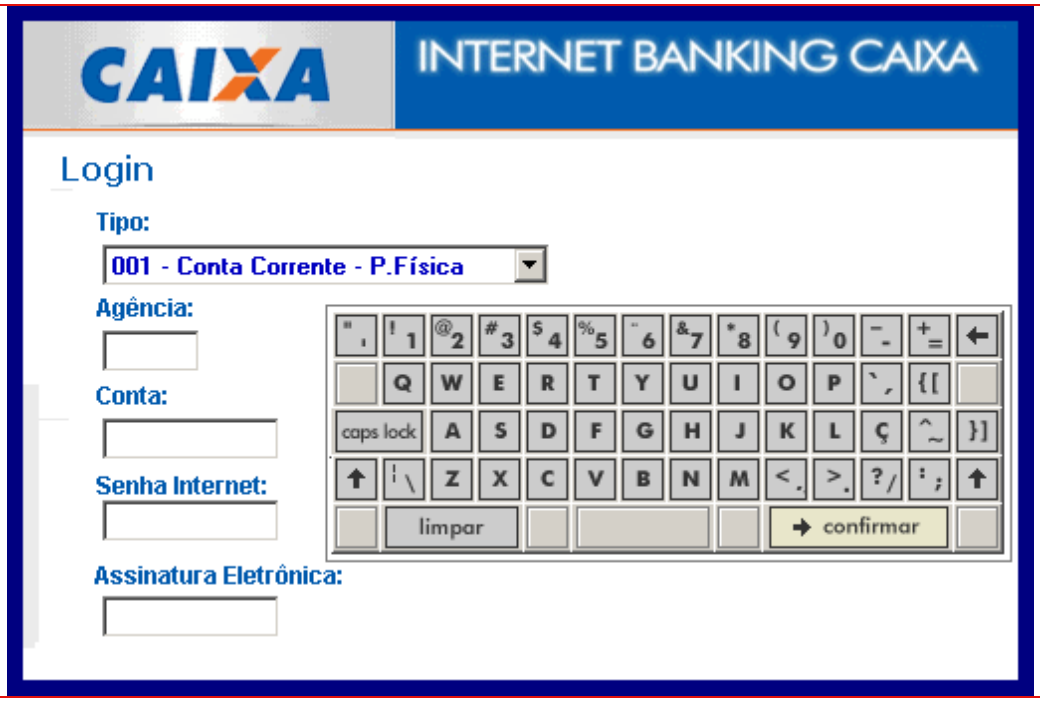
Porn-Dialer.Win32.Bienvenido" Es el espécimen más difundido siendo detectado en el 0,3% de los equipos analizados, propagado a través de páginas web de contenido erótico. Los creadores obtienen beneficio económico de la facturación de las líneas de tarificación especial.

Los marcadores están presentes en el 2,7% de los sistemas analizados, se caracteriza por desviar la conexión telefónica a redes original hacia otro número de tarificación especial (806, 807, etc.) con el consecuente perjuicio económico para el afectado. Su impacto es cada vez menor gracias a la banda ancha, ya que los dialers afectan a las conexiones que realizan marcación, como las llevadas a cabo por módem a través de la red telefónica básica (RTB) y RDSI.

Troyanos bancarios o bankers

Trojan-Spy.Win32.Bancos.KC: Pertenece a la familia Trojan.Bank que está bastante diversificada, siendo este el espécimen concreto más detectado (ha sido detectado en el 1% de los equipos analizados) Está especializado en el robo de credenciales de diversas entidades financieras españolas. Las vías de infección pueden ser variadas, aunque destacan el correo electrónico y la explotación de vulnerabilidades a través de páginas webs.

Gráfico 64: Visualización de una ventana creada por el troyano bancario que emula la ventana de acceso original del banco para engañar al usuario



Fuente: INTECO

Este malware se inserta dentro de la categoría de los troyanos bancarios. Los Trojan.Bank se detectan en el 9,8% de los equipos analizados, esta subcategoría de los troyanos es una de las más peligrosas, ya que está especializada en el robo de credenciales de acceso a la banca electrónica y servicios sensibles a través de Internet. Los creadores de

este tipo de troyanos obtienen un beneficio económico directo al suplantar la identidad de los afectados y realizando transacciones económicas en su nombre.

Puertas traseras o backdoors

Trojan.Backdoor.CMI: Es el espécimen concreto más extendido de la categoría de troyanos de puerta trasera. Está presente en el 0,3% de los equipos analizados, un indicador de lo diversificada que está la subcategoría. Por lo general se trata de ataques individuales y personalizados, donde los creadores intentan lograr el control remoto del sistema de la víctima con el fin de espiar sus acciones y sustraer información sensible.

Este malware se inserta dentro de la categoría de los troyanos de puerta trasera. Es una subcategoría de los troyanos que se detecta en el 4,4% de los sistemas analizados, y es uno de los tipos de malware más diversificados y peligrosos, ya que permiten al atacante obtener control remoto sobre el sistema.

Gráfico 65: Ejemplo de ventanas cliente/servidor de la puerta trasera "Backdoor.CMI"

Fuente: INTECO

8.11.4 Virus

Virus Parite-B: Este virus se ha detectado en el 0,8% de los equipos analizados. Aunque su tasa de incidencia no es especialmente elevada, sobre todo al compararla con algunos especimenes de adware o troyanos, si es una muestra representativa de un virus tradicional que sigue en activo.

Data del año 2001, y se caracteriza por ser un virus polimórfico (capaz de mutarse en cada infección y cambiar su aspecto más externo) que infecta archivos EXE y SCR. Además de infectar el sistema local, puede propagarse infectando otros archivos a través de las unidades compartidas de las redes locales. Este virus no muestra ningún síntoma visible

en los equipos infectados ni el autor obtiene beneficio alguno con ello, el único objetivo del espécimen es reproducirse.

8.11.5 Otros especímenes

Exploits

Exploit.Java.ByteVerify: Se trata de un applet de Java que aprovecha una vulnerabilidad en la Máquina Virtual de Microsoft, que data del año 2003, para ejecutar código arbitrario de forma remota.

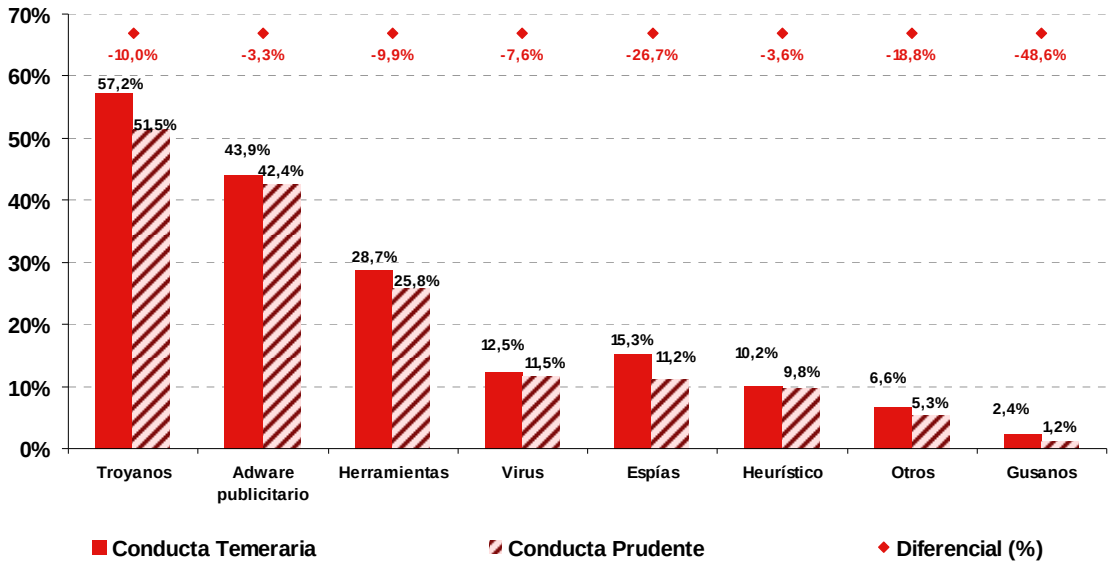
Para propagarse los atacantes incrustan el applet malicioso en una página web que se ejecuta de forma automática cuando un usuario con un sistema vulnerable la visualiza. Las firmas antivirus detectan el intento de explotar la vulnerabilidad, pero cada ataque en concreto puede tener fines diferentes, desde la propagación de malware hasta ataques más personalizados.

8.12 Efecto de los hábitos y buenas prácticas de seguridad sobre las incidencias.

La combinación, por una lado, de los datos recogidos en las encuestas y, por otro lado, del análisis de los equipos por medio del programa de escaneo proporcionado por INTECO, revelan datos significativos.

En el Gráfico 66 se aprecia como la conducta prudente tiene un efecto reductor en el número de incidencias detectadas en los equipos de los panelistas. Esta reducción, aunque moderada, se produce para todas las categorías de malware, entre las que destaca la reducción experimentada en el porcentaje de *programas espía*, que se sitúa en el 26,7%. Es destacable el hecho de que la familia de los *troyanos*, la de mayor difusión, reduce su porcentaje de incidencias en un 10,0% ante un comportamiento prudente. Esto viene a confirmar la idea de que los hábitos contribuyen de manera decisiva a controlar las infecciones por código malicioso.

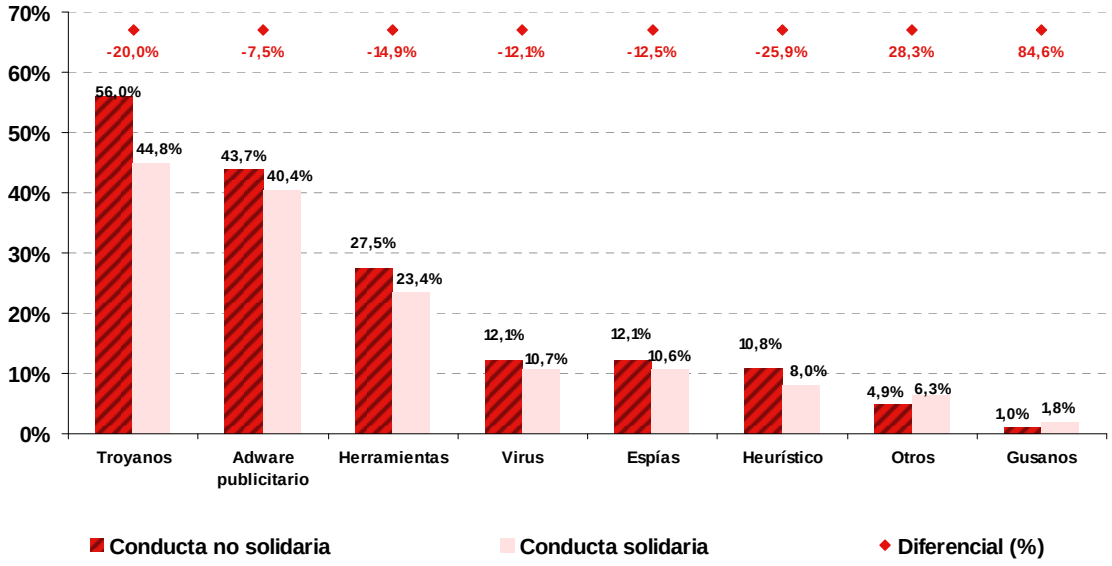
Gráfico 66: Impacto de la conducta prudente sobre la presencia de malware (%)



Fuente: INTECO

En el Gráfico 67 se observa que los usuarios con los hábitos que se han denominado "solidarios", acaban teniendo un efecto considerablemente benévolo en la reducción de los *troyanos* y bastante intenso en los *virus*. Así, un usuario con hábitos de comportamiento solidario tiene un nivel de incidencias de *troyanos* un 20,0% inferior a un usuario con un comportamiento no solidario (prudente no solidario y temerario), a causa de la mayor preocupación por la seguridad del Sistema y las medidas que toman al respecto.

Gráfico 67: Impacto de la conducta solidaria sobre la presencia de malware (%)

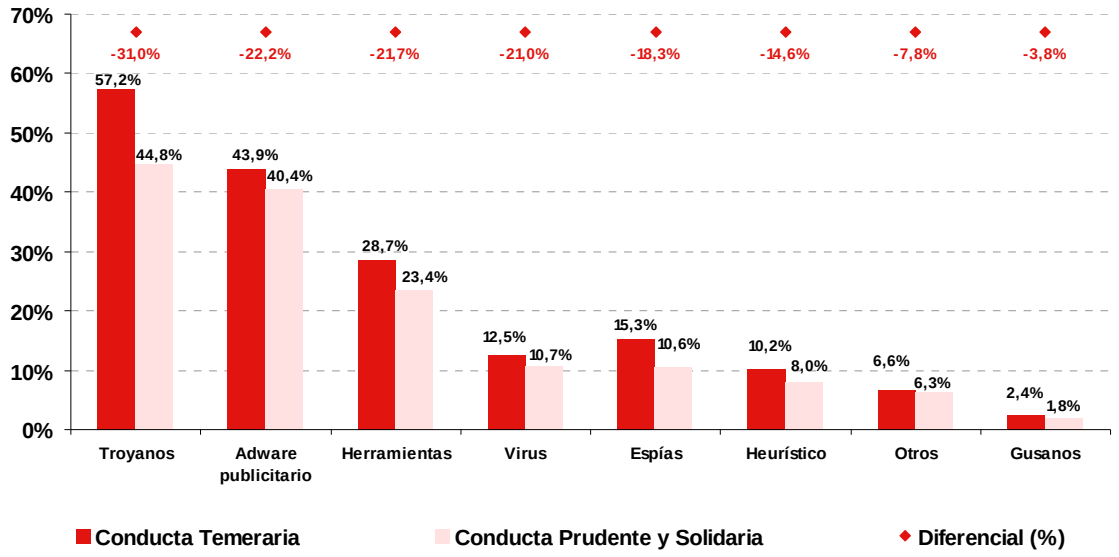


Fuente: INTECO

Se aprecia, sin embargo, un aumento en el número de *gusanos*. Este crecimiento que si bien es poco significativo, los *gusanos* representan menos del 2% del malware detectado, puede explicarse por el método de propagación que tienen los *gusanos* (principalmente vía correo electrónico) y alguno de los comportamientos de los individuos solidarios (reenvían alertas y correos electrónicos sobre posible malware) que pueden hacer que en el caso de encontrarse el individuo infectado, contribuyan a extender el malware.

El Gráfico 68 muestra el efecto combinado de los hábitos prudentes y solidarios frente a los hábitos directamente temerarios. Esto es, la diferencia en los niveles de incidencias para los distintos tipos de códigos maliciosos para los dos extremos de la segmentación. Es considerable la reducción en los porcentajes de incidencias de *troyanos (3*1,0%), *virus* (21,0%) y *herramientas de intrusión* (-21,7%). Incluso se aprecia el efecto en los *programas espía* (18,3%).

Gráfico 68: Impacto combinado de las conductas prudente y solidaria sobre la presencia de malware (%)



Fuente: INTECO

Estos resultados ponen de manifiesto la correlación entre la presencia real de incidencias de seguridad y los hábitos de uso, y son, a su vez, concordantes con los resultados obtenidos a través de la encuesta. Como se verá más adelante, gran parte de los hallazgos encontrados en la caracterización de los grupos solidario/imprudente sirven también para explicar los niveles reales de seguridad debido a que hábitos e incidencias reales están estrechamente vinculados.

9 SISTEMA DE INDICADORES DE SEGURIDAD Y E-CONFIANZA

Todo el análisis e información sobre incidencias de seguridad y confianza de los usuarios en Internet se puede dirigir hacia el cálculo de una serie de indicadores que sinteticen todo lo expuesto de manera sistemática. Para ello se construye un conjunto de indicadores generales que, tras el análisis previo, se espera sirvan para hacer un seguimiento de la evolución y las tendencias de la seguridad en Internet y la confianza de los hogares. Ello desde la combinación de la perspectiva sociológica y tecnológica que anima toda la investigación.

El sistema de indicadores diseñado por INTECO tiene las siguientes ventajas:

- Es integral, pues abarca tanto los hábitos de uso como el equipamiento en seguridad o las incidencias reales de malware.
- Es sintético, pues condensa en un conjunto de 7 indicadores todos los aspectos relevantes de la seguridad.
- Es sensible, pues ha demostrado detectar variaciones pequeñas de la seguridad y ser relevante para detectar situaciones de riesgo en segmentos concretos de la población.
- Es estable, pues permite tener una visión de conjunto de la situación de seguridad de cualquier mercado segmento o sub-segmento referido a puntuaciones cuya referencia es siempre el 100 de la escala. Incluso en el caso de que se variasen el número de preguntas que componen un indicador el sistema de indicadores conservaría su estabilidad y su comparabilidad histórica.
- Es operativo, pues permite de forma muy sencilla detectar las debilidades del sistema e inspirar medidas para reducir estas debilidades.
- Es estratégico, pues ayuda a entender las consecuencias para el conjunto del sistema de las situaciones individuales de falta de protección, al tiempo que permite introducir la conexión en entre política de seguridad de la Administración y comportamiento individual de los usuarios.

IS.1 Indicador de equipamiento en seguridad

Mide el equipamiento y adopción de medidas de seguridad.

Se calcula en función de determinadas medidas del equipamiento de seguridad disponible, comparando los datos con una situación óptima de seguridad, la cual se establece en un equipamiento completo. El equipamiento incluido para el cálculo del indicador incluye las medidas con mayor penetración entre las definidas en la Tabla 8: programas antivirus, cortafuegos, bloqueo de ventanas emergentes, eliminación de archivos temporales y cookies, programas anti-correo basura, antiespías, contraseñas (equipo y documentos), actualizaciones de seguridad del sistema operativo, copia de seguridad de los archivos importantes y encriptación de documentos. El cálculo del indicador no sólo se centra el la propia seguridad del sistema, sino que también incluye medidas que favorecen la seguridad de la información.

IS.2 Indicador de conducta temeraria

Mide la intensidad de los hábitos de riesgo en el uso de Internet.

Puntuación obtenida en los comportamientos temerarios respecto de la puntuación máxima posible tal y como se definen en la Tabla 12: abro correos de remitentes desconocidos si parecen interesantes, doy mi dirección de e-mail cuando me lo piden aunque desconozca el destinatario, agrego contactos al Messenger aunque no sepa de quién se trata, pulso los enlaces que aparecen en las conversaciones del Messenger, sin preguntar de que se trata, si es necesario modifico las medidas de seguridad del ordenador para poder acceder a servicios o juegos que me interesan, comparto software sin comprobar si está o no infectado (redes P2P).

IS.3 Indicador de percepción de seguridad personal

Mide la percepción subjetiva de seguridad cuando se usa Internet.

Puntuación obtenida en los criterios de percepción de seguridad respecto de la puntuación máxima posible, tal y como se definen en la Tabla 22 (la conexión que utilizo es bastante segura frente a intrusos que quieran acceder a mi equipo, mi ordenador esta razonablemente protegido, los dispositivos y sistemas de protección que utilizo están actualizados y son eficaces).

IS.4 Indicador de conducta solidaria

Mide la intensidad de los hábitos de solidaridad con otros usuarios referidos a la seguridad en Internet.

Puntuación obtenida en los comportamientos solidarios respecto de la puntuación máxima posible, tal y como se define en la Tabla 13 (Alerto sobre aquellas páginas que conozco y hacen un uso fraudulento de los datos del usuario, cuando recibo una notificación sobre la existencia de un nuevo virus se lo comunico a la gente que conozco, cuando veo que alguien no tiene actualizados sus programas de seguridad le recomiendo que los revise e instale las últimas versiones, si envío un archivo por mail compruebo que no contenga ningún virus, cuando recibo un mail de un conocido con un archivo infectado se lo comunico al remitente).

IS.5 Indicador de ordenadores con alguna incidencia de malware

Indica el porcentaje de ordenadores con alguna incidencia de malware detectada en el escaneo.

Porcentaje de ordenadores con al menos una incidencia de código malicioso en el escaneo.

IS.6 Indicador de ordenadores con riesgo potencialmente alto

Indica el porcentaje de ordenadores con alguna incidencia de malware con riesgo alto detectada en el escaneo

El malware considerado de riesgo alto se compone de las siguiente familias: troyanos, virus, gusanos, marcadores automáticos (dialers), capturadores de pulsaciones (keyloggers), exploits, rootkit.

IS.7 Indicador de ordenadores con riesgo de diseminación potencialmente alto

El cálculo de este indicador incluye conceptos que implican, en mayor o menor medida, un potencial riesgo de diseminación entre el resto de los usuarios: estado real de las actualizaciones de seguridad del sistema operativo, ordenadores con presencia de alguna incidencia de malware de tipo gusano o script, utilización de servicios de mensajería instantánea, descarga de archivos, frecuencia e intensidad de la navegación por la red, compartir software sin comprobar si está o no infectado o enviar correos electrónicos comprobando que no contenga ningún virus.

9.1 Indicadores

En la Tabla 27 se muestran los resultados de los 7 indicadores definidos que ofrecen una visión de conjunto sacando el máximo partido de toda la riqueza de información disponible.

Tabla 27: Indicadores de Seguridad

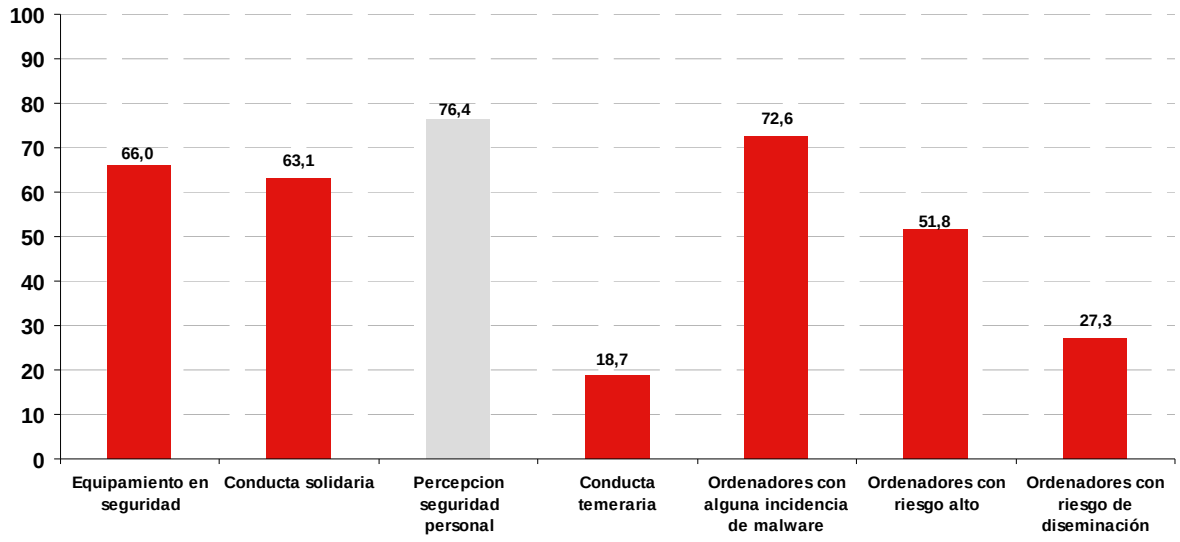
	Indicador	Puntuación
IS.1	Indicador de equipamiento en seguridad	66,0
IS.2	Indicador de conducta solidaria	63,1
IS.3	Indicador de percepción de seguridad personal	76,4
IS.4	Indicador de conducta temeraria	18,7
IS.5	Indicador de ordenadores con alguna incidencia de malware	72,6
IS.6	Indicador de ordenadores con riesgo potencialmente alto	51,8
IS.7	Indicador de ordenadores con riesgo de diseminación potencialmente alto	27,3

Escala de variación de 0 a 100 *Fuente: INTECO*

Las posibilidades de análisis que brinda este conjunto sintético de dimensiones, puede verse a continuación.

Se muestra en primer lugar el perfil medio de la muestra panelizada en cuanto a las 7 dimensiones básicas en el siguiente gráfico:

Gráfico 69: Perfil de indicadores de seguridad Muestra Panel (0-100)



Fuente: INTECO

Se puede entender el Gráfico 69 a modo de balanza. En el centro, el fiel de la balanza --representado en gris-- es la **percepción de seguridad personal**. Esta variable tiende a mantenerse por encima del valor 75 (Tabla 22), para lo cual, el usuario modifica los valores de los indicadores en los flancos:

- A la izquierda: los **indicadores relacionados con la protección**: el *índice de equipamiento en seguridad* y el *índice de conducta solidaria*.

- A la derecha, los **indicadores relacionados con el riesgo**: El *índice de conducta temeraria*, el *índice de ordenadores con alguna incidencia de malware*, el *índice de ordenadores con riesgo* alto y el *índice de ordenadores con riesgo de diseminación.*

Como se indica, el sistema del conjunto de indicadores se contrapesa: un aumento de las incidencias tiende a compensarse con un mayor equipamiento en seguridad y hábitos más prudentes para restablecer el equilibrio que viene marcado por una e-confianza elevada.

En general, la balanza se mantiene con una conducta prudente y con un equipamiento en barreras de protección considerable, pero no excesivo. Esto se refleja en los indicadores de *Índice de equipamiento de seguridad* (66,0 puntos) y el *Índice de Conducta Solidaria* (63,1 puntos). Como resultado se obtiene una alta incidencia en ordenadores con códigos

maliciosos (72,6 puntos), pero muchos menos con riesgo alto (51,8 puntos) y, de forma muy especial, una cifra relativamente baja de ordenadores con potencial diseminador de riesgos serios (27,3 puntos).

9.2 Segmentación del sistema de indicadores

Es un sistema en equilibrio inestable, cuyo eje es una sensación de seguridad que tiene origen y es dependiente de que los riesgos potenciales no se conviertan en consecuencias serias detectadas por los usuarios.

Este análisis en las dimensiones de seguridad puede hacerse para cualquier grupo o segmento de usuarios, poniendo de relieve las diferentes configuraciones que puede adoptar el marco general de seguridad dependiendo de los hábitos u otras características aunque los riesgos asumidos por cada segmento son bien distintos. Por otra parte no aparecen grandes variaciones en equipamiento de barreras de protección aunque los riesgos asumidos por cada segmento son bien distintos

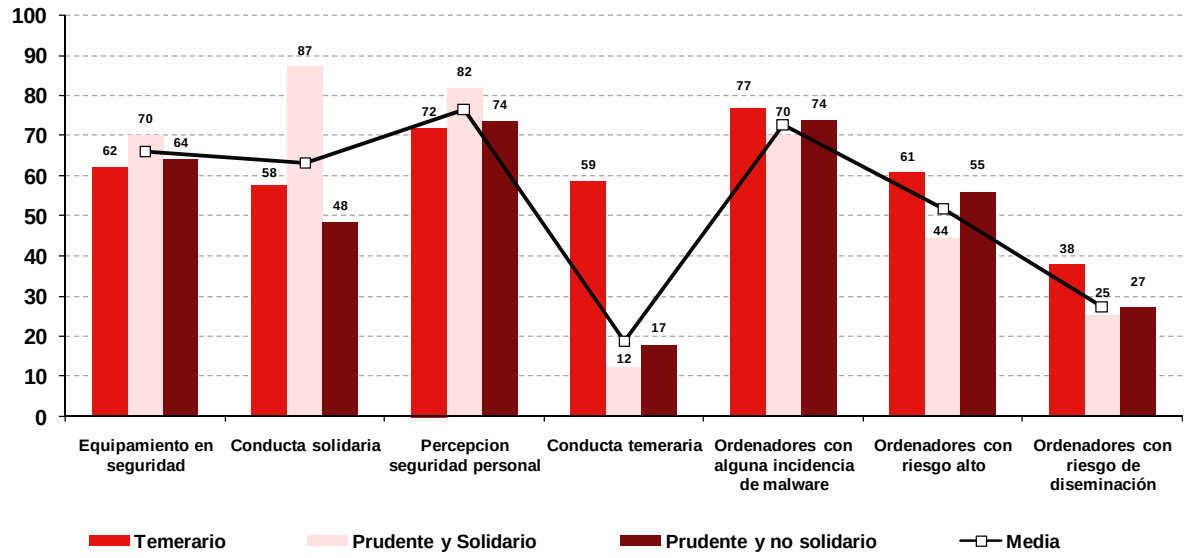
9.2.1 Segmentación por hábitos de uso

En el Gráfico 70 y en el Gráfico 71 se aprecia como los indicadores del nivel protección, los dos del lado izquierdo del gráfico (equipamiento en seguridad y conducta solidaria), son significativamente superiores para el grupo de usuarios prudente y solidario. Ocurre todo lo contrario para los otros dos tipos de usuarios (los denominados temerarios y aquellos prudentes y no solidarios). Los índices de incidencia, los cuatro de la derecha del gráfico, toman valores menores para los usuarios prudentes y solidarios.

Es para el segmento de los usuarios temerarios donde los indicadores de incidencia se disparan en valor. Por ejemplo, para el Índice de conducta temeraria toma un valor significativo de 59 puntos, un 213% superior al valor medio del indicador que se sitúa en 19 puntos. Este valor se encuentra también muy por encima del los 17 puntos del segmento prudente y no solidario, o de los 12 del segmento de los usuarios prudentes y solidarios.

Por su parte, la presencia de malware es más acusada en los usuarios denominados temerarios, que también presentan cifras relativamente mayores de ordenadores con riesgo alto, siendo el indicador correspondiente un 17% superior al valor medio y concentran una parte importante de los casos detectados de ordenadores con riesgo de dispersión de amenazas, un 38% superior a la media. Es decir, se confirma que el riesgo total del sistema se encuentra bastante concentrado en esta fracción minoritaria de usuarios. Que por su parte se sienten bastante protegidos y seguros.

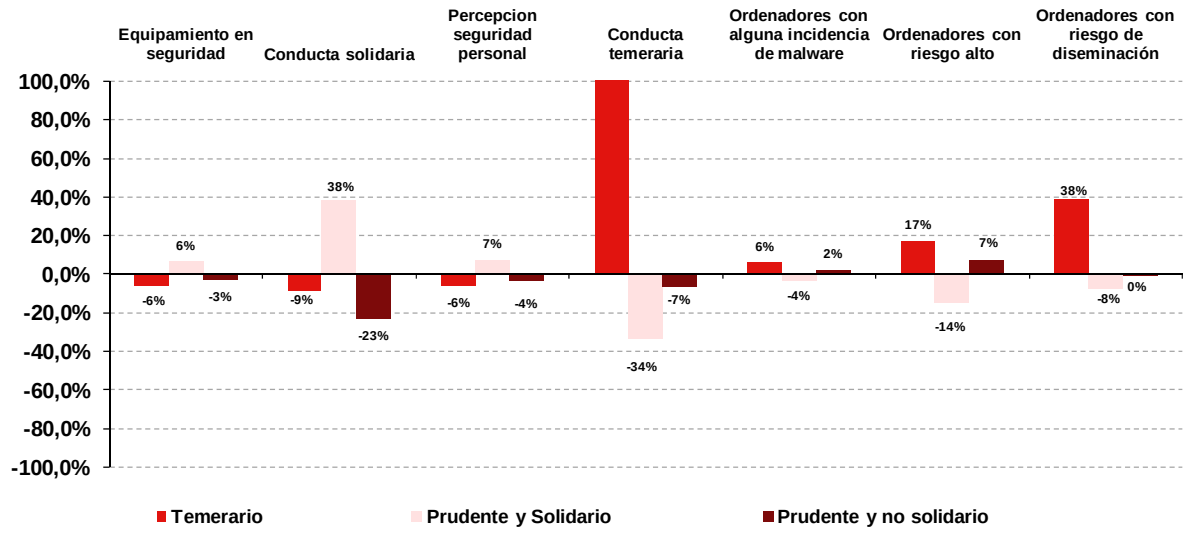
Gráfico 70: Perfil de indicadores de seguridad: Segmentos de hábitos vs Muestra panel



Fuente: INTECO

Estos datos recuerdan que las incidencias reales de seguridad detectadas en el escaneo parecen tener su solución en dos factores relativamente independientes: la presencia real de dispositivos de seguridad y los hábitos de uso preventivos y solidarios. Ambos factores constituyen los pilares de la seguridad del sistema y su complementariedad debería ser potenciada en la medida de lo posible: no hay seguridad sin la presencia de ambos.

Gráfico 71: Perfil de indicadores de seguridad: Segmentos de hábitos vs Muestra panel (diferencias porcentuales)



Fuente: INTECO

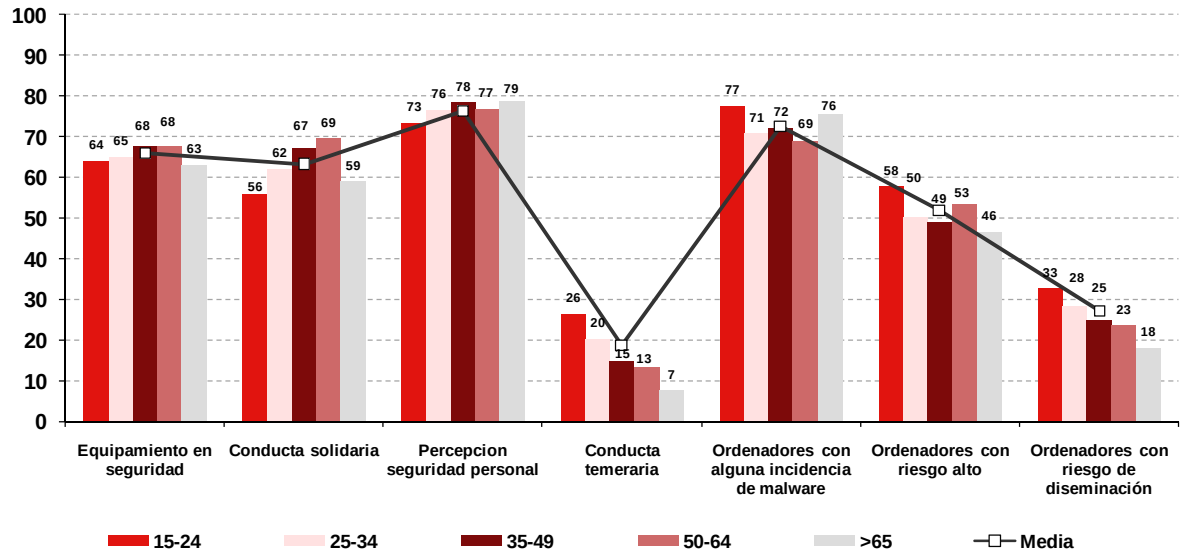
Por tanto se hace necesario un esfuerzo en dos frentes: por un lado, potenciar el uso de dispositivos de seguridad y, por otro lado, remarcar la necesidad de un uso responsable de los equipos, para que esos dispositivos sean realmente eficaces. Esto permitiría evitar el efecto paradójico ya comentado de que el equipamiento en seguridad lleve a un comportamiento demasiado imprudente que potencie la vulnerabilidad del sistema.

9.2.2 Segmentación por edad

Se obtiene del cruce entre la edad y la configuración de seguridad basada en los siete indicadores.

La imagen del fiel de la balanza ayuda a entender que las diferencias de percepción de seguridad por edades son pequeñas, aunque los hábitos y los equipamientos sean dispares. En el Gráfico 72 se aprecia como para los grupos con menores edades, hasta 35 años, los dos indicadores de seguridad toman valores menores: 64 y 65 puntos en el caso del *Índice de equipamiento en seguridad*. Para el *Índice de conducta solidaria* dentro del nivel de protección, se toman valores de 56 y 62 puntos para el grupo de menores de 24 años y el grupo entre 25 y 34 años respectivamente. En el lado contrario se encuentran los usuarios mayores de 35 años que presentan unos índices superiores dentro del nivel de protección, obteniendo valores superiores en un 10% a la media para el caso de los individuos con edades de 50 a 64 años en el Índice de conducta solidaria. Evidentemente, y según el nivel del *Índice de seguridad personal*, las diferencias porcentuales son negativas o cercanas a cero para los jóvenes, y positivas para los usuarios mayores de 35 años.

Gráfico 72: Perfil de indicadores de seguridad: Grupos de edad



Fuente: INTECO

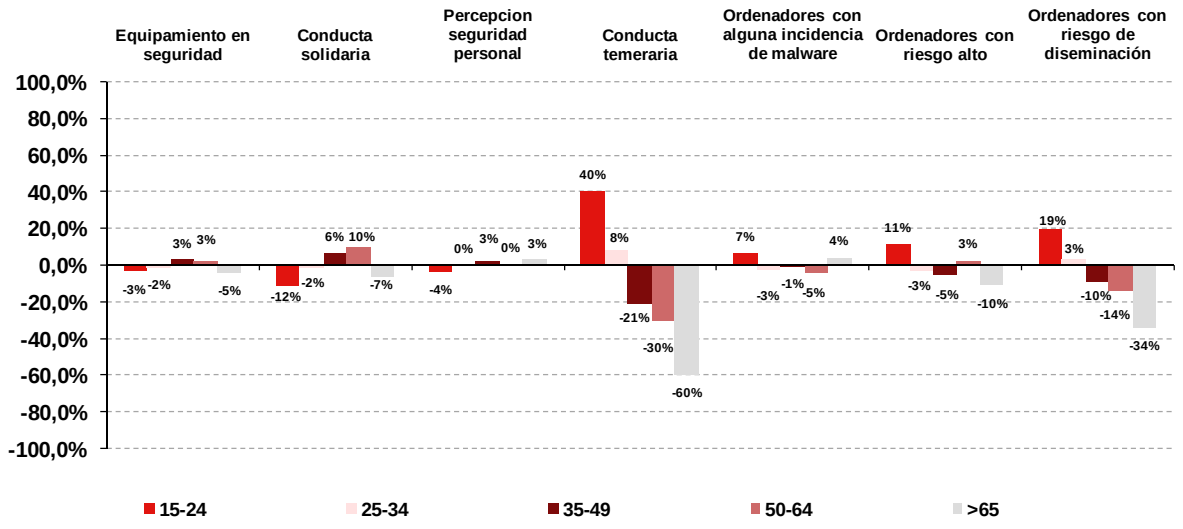
Dentro del nivel de Incidencia, para los cuatro índices de la derecha del Gráfico 73, las diferencias porcentuales respecto a la media son positivas para los jóvenes con edades hasta los 24 años. Para jóvenes entre 25 y 34 años estas diferencias toman valores que rondan el nivel cero. Para usuarios de más de 35 años los indicadores del nivel incidencia presentan por lo general valores inferiores a la media. Existe por tanto, según la edad, un comportamiento diferenciado respecto a los niveles de incidencia y protección. Siendo los usuarios mayores de 35 años aquellos que muestran un comportamiento más *seguro* y *confiado* en la red.

El comportamiento principal reflejado entre indicadores y grupos de edad señala diferencias. Los mayores tienen un comportamiento más seguro y unos hábitos más saludables. Los jóvenes, según los indicadores, reflejan comportamientos más temerarios.

El comportamiento principal reflejado entre indicadores y grupos de edad señala diferencias. Los mayores tienen un comportamiento más seguro y unos hábitos más saludables. Los jóvenes, según los indicadores, reflejan comportamientos más temerarios.

También pueden verse datos característicos en los ordenadores implicados. Los jóvenes y los mayores de 65 años tienen en sus equipos mayor presencia de *malware*, pero solamente los jóvenes tienen más códigos realmente maliciosos, con valores un 11% superiores a la media. Los mayores destacan por tener menor riesgo de dispersión en sus ordenadores.

Gráfico 73: Perfil de indicadores de seguridad: Grupos de edad vs Muestra panel (diferencias porcentuales)



Fuente: INTECO

En general, las principales diferencias en el análisis de los indicadores se observan en lo concerniente a la conducta prudente y temeraria. Los usuarios menos solidarios suelen ser

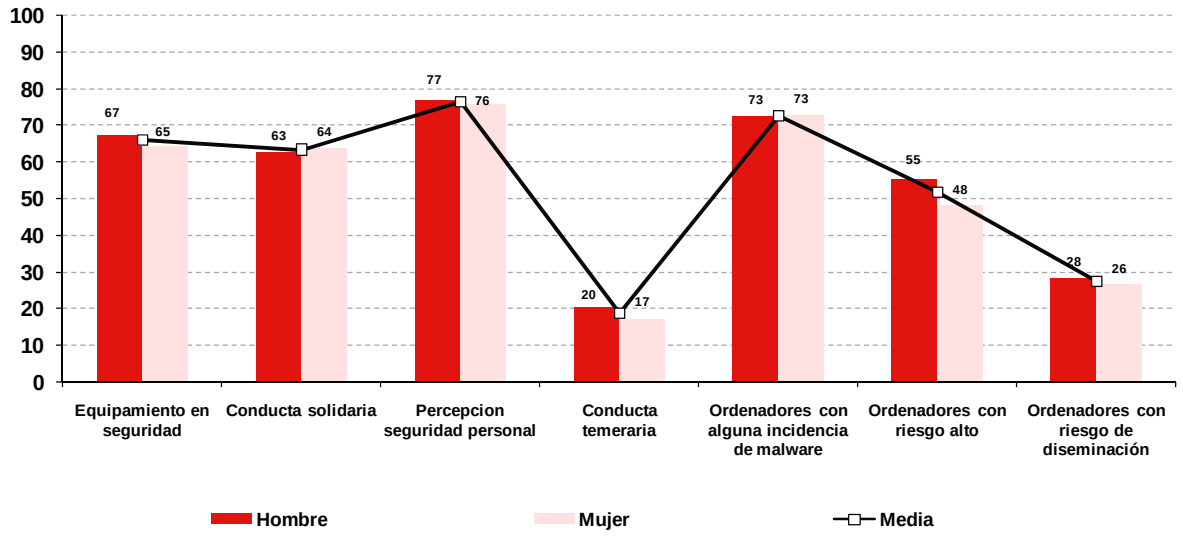
los usuarios jóvenes y los mayores de 65 años. Posiblemente por razones distintas, los jóvenes porque gustan de asumir más riesgo, y los mayores aunque destacan por sus comportamientos prudentes, no son excesivamente solidarios. Esta explicación se consolida al prestar atención a la conducta temeraria: máxima en los jóvenes y mínima en los mayores.

9.2.3 Segmentación por género

Como puede verse en el Gráfico 74 y en el Gráfico 75, los indicadores muestran que, por lo general, las mujeres tienden a equiparse menos en seguridad. Sin embargo, tienden a ser más prudentes en el uso de Internet que los varones. El resultado es que ambos sexos tienen niveles similares de *malware*, según se observa en las diferencias porcentuales, pero las mujeres tienen menos ordenadores con riesgo elevado (7% inferior a la media).

Ambos sexos se encuentran confortablemente seguros con lo que hacen, unos confiando más en las barreras tecnológicas, los hombres, y otros en los hábitos razonables de uso de Internet, las mujeres. Los resultados favorecen la actitud de las segundas frente a los primeros.

Gráfico 74: Perfil de indicadores de seguridad: Sexo vs Muestra panel

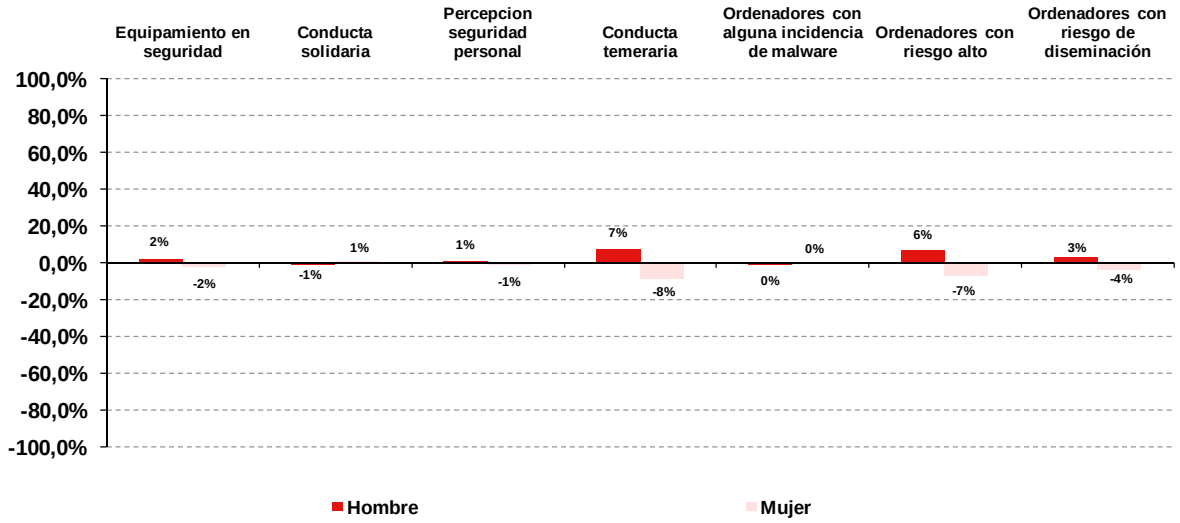


Fuente: INTECO

El reparto por sexos de la distribución de indicadores señala como característica general que el comportamiento generalizado en los hombres tiene una ligera mayor conducta temeraria, en cuanto al indicador de ordenadores de riesgo alto y el de ordenadores de riesgo de diseminación. Para la mujer los indicadores reflejan conductas y equipamientos ligeramente más seguros. Señal de que las diferencias son mínimas entre ambos sexos, es que no se detectan diferencias significativas en la presencia de malware entre hombre y

mujeres, ni en las actitudes solidarias y percepción de seguridad de cada uno de los grupos.

Gráfico 75: Perfil de indicadores de seguridad: Sexo vs Muestra panel (diferencias porcentuales)

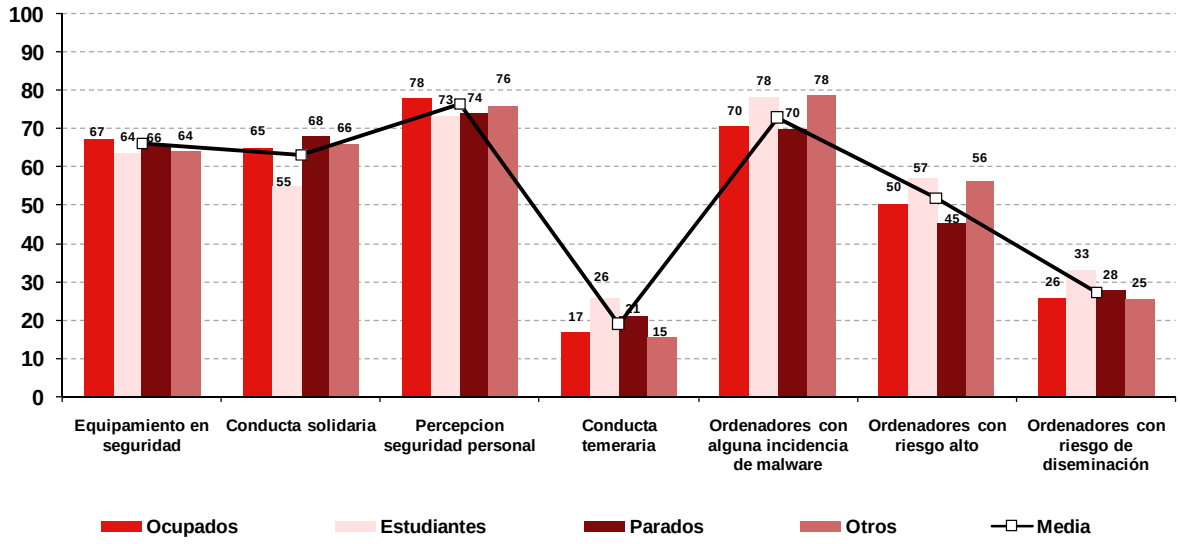


Fuente: INTECO

9.2.4 Segmentación por tipo de actividad económica

La actividad económica también ha mostrado relación con las incidencias de seguridad, vía hábitos distintivos de uso de Internet (Gráfico 76 y Gráfico 77).

Gráfico 76: Perfil de indicadores de seguridad: Tipo de Actividad vs Muestra panel

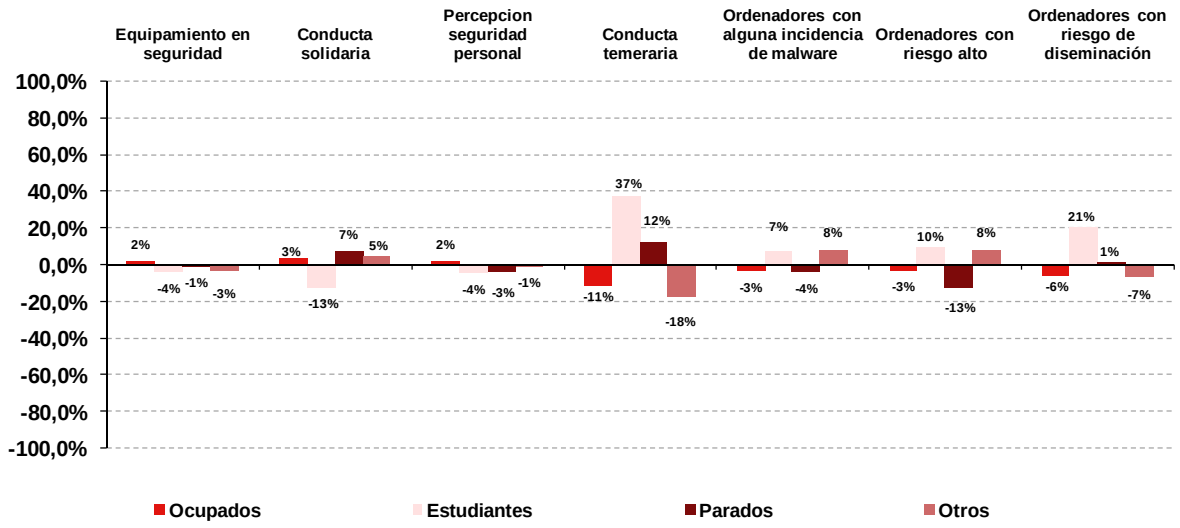


Fuente: INTECO

Los estudiantes son quienes menos usan las barreras de seguridad en sus equipos, (64 puntos, -4% respecto a la media del *Índice de equipamiento en seguridad*). A esto se añade que los estudiantes se adhieren más frecuentemente a un comportamiento temerario (con una puntuación un 37% superior a la media del indicador).

En este caso, esta diferencia de prudencia no puede compensar el menor equipamiento. Tampoco destacan los grupos de estudiantes por los hábitos solidarios, y acaban siendo los que acumulan mayor riesgo en sus equipos.

Gráfico 77: Perfil de indicadores de seguridad: Tipo de Actividad vs Muestra panel (diferencias porcentuales)



Fuente: INTECO

Los estudiantes se engloban en comportamientos más peligrosos, con menor conducta solidaria y mucha mayor conducta temeraria y ordenadores con riesgo alto de diseminación. Son el grupo de perfil de actividad con un comportamiento más específico. Los ocupados, por cuenta ajena o por cuenta propia, destacan por una conducta menos temeraria (-11% inferior a la media), al igual que el grupo de otros[22]. Los parados, aún teniendo una conducta más solidaria, 7% superior a la media, tienen también un índice de conducta temerario con una diferencia positiva (12% superior al índice medio de conducta temeraria).

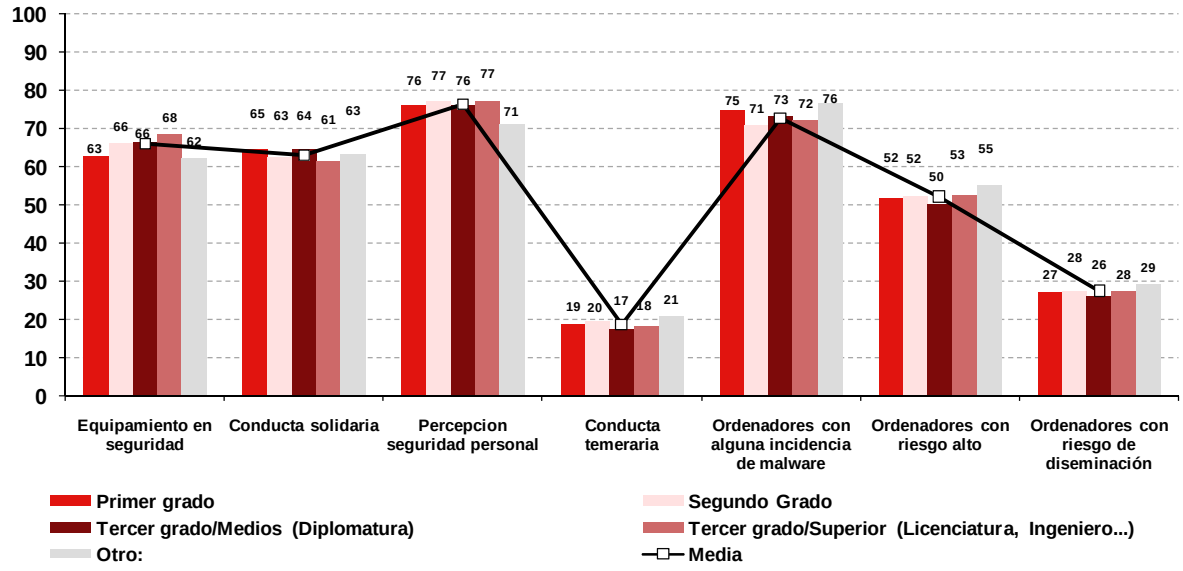
9.2.5 Segmentación por nivel de estudios

Las diferencias de valor entre los distintos indicadores según el nivel de estudios del encuestado son ligeramente significativas. El grupo donde se aprecia cierta relevancia es

[22] El grupo de "Otros" engloba jubilados, amas de casa o aquellos encuestados que no se encuentran en ninguna de las categorías mencionadas. La menor muestra de este grupo incrementa la variabilidad de los datos del indicador.

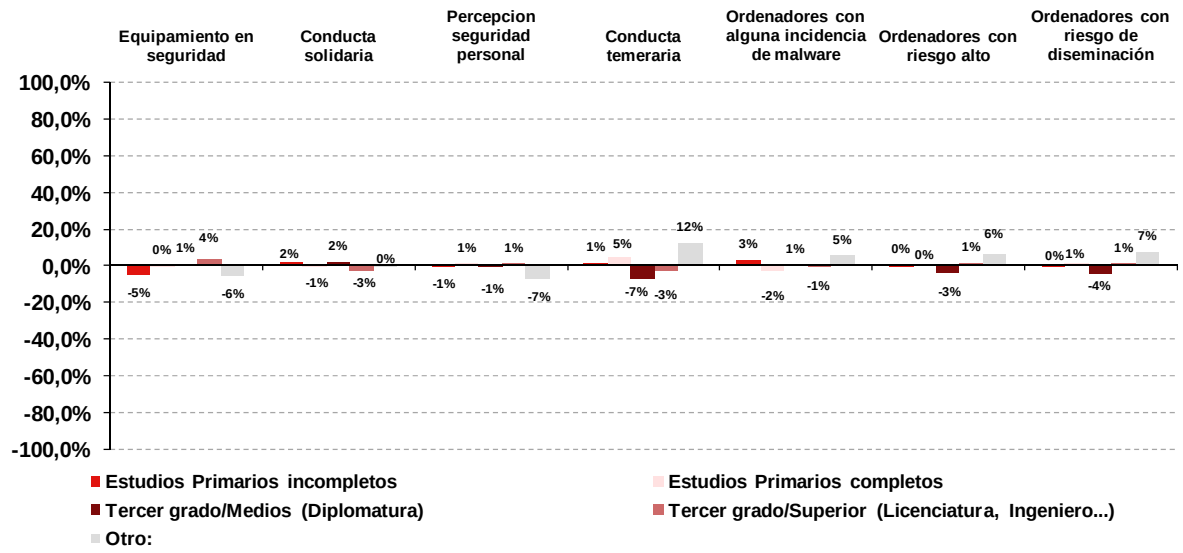
el grupo de otros, donde, como ocurre en el tipo de actividad, una menor muestra, diferencia los valores de dicho grupo, y donde la menor homogeneidad de los perfiles que componen dicho grupo provocan comportamientos diferenciados.

Gráfico 78: Perfil de indicadores de seguridad: Nivel de estudios vs Muestra panel



Fuente: INTECO

Gráfico 79: Perfil de indicadores de seguridad: Nivel de estudios vs Muestra panel (diferencias porcentuales)



Fuente: INTECO

El equipamiento de seguridad está más extendido entre aquellos sujetos con nivel de estudios de tercer grado/superior, aunque éstos mismos son los que muestran menor conducta solidaria. Aquellos sujetos que se incluyen dentro de los grupos de nivel de

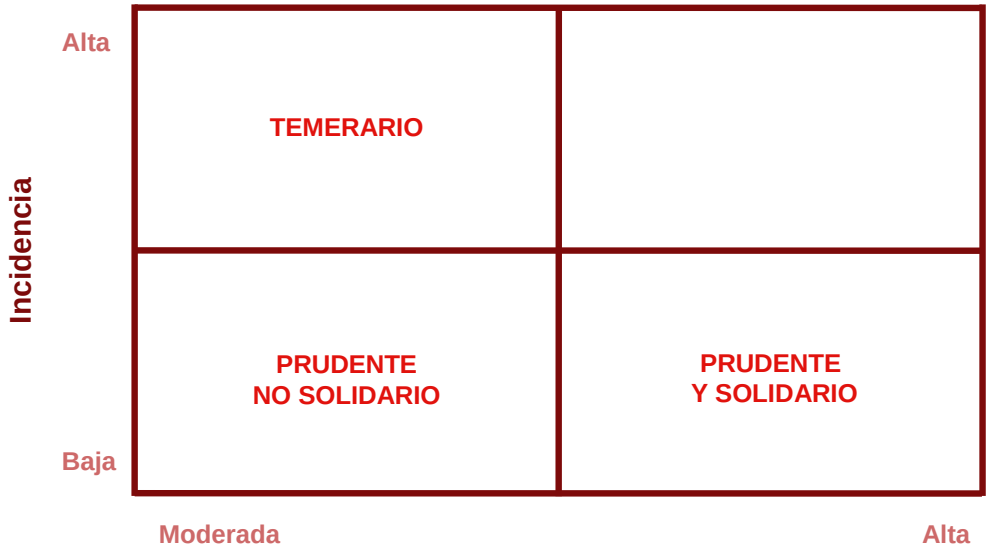
estudios primarios y de otros son los que están por debajo de la media en cuanto a equipamiento. El grupo de otros también es el que tiene un menor valor de su percepción de seguridad, a lo que hay que añadir que son aquellos con mayor conducta temeraria, con ordenadores con alguna incidencia de malware y de riesgo alto y con riesgo de diseminación alto.

9.2.6 Matriz Incidencia-Confianza

Los hábitos prudentes son una buena protección, no obstante es necesario contar con herramientas y medidas de seguridad adecuadas para lograr el efecto completo deseado.

De lo anteriormente expuesto puede inferirse que para una visión de conjunto se ha ubicado a los distintos tipos de usuarios en un mapa o matriz de incidencia-confianza, que se muestra a continuación en el Gráfico 80:

Gráfico 80: Mapa de la tipología de usuarios en la Matriz "Incidencia-Confianza"



Fuente: INTECO

El cuadrante superior izquierdo relaciona un nivel moderado de confianza y con un nivel alto de incidencias. En este cuadrante se sitúan los **usuarios que someten a un riesgo considerable sus equipos**. Las características de este son el **comportamiento temerario** en todos los aspectos, como en la utilización de los equipos y percepción de confianza, déficits en seguridad al tiempo que son los que más relatan haber padecido incidencias y consecuencias graves. Es previsible que, con el tiempo, se corrijan determinados hábitos y se mejore el equipamiento en seguridad, salvo los más extremos, clasificados como temerarios que son algo más tardos en adoptar conductas prudentes.

El cuadrante inferior izquierdo recoge, en general, **individuos desconfiados y poco implicados con el uso de Internet.** En este grupo predominan las mujeres. Su uso de Internet además es esporádico (menos de 1 hora al día).

El cuadrante inferior derecho viene definido por **usuarios mejor equipados en seguridad, prudentes y solidarios en su uso de Internet**. Son usuarios en un rango de edad alto, que suponen el mayor capital de seguridad para el conjunto del sistema.

Las tendencias previsibles de comportamiento prevén que:

- Los **usuarios con niveles altos de incidencias** a los que través de información sobre seguridad y hábitos de conducta, se espera que puedan disminuir su nivel de incidencias aunque, del mismo modo, se minore ligeramente su nivel de confianza.

- A los **usuarios con niveles bajos de incidencia** no se les prevé cambio de tendencia en el comportamiento, dado que no se esperan cambios en las medidas habituales que aplican de actualización de los sistemas de protección y en sus hábitos seguros.

- Los **usuarios que muestran desconfianza hacia Internet**, aunque no hayan experimentado incidencias, son usuarios que tampoco muestran un comportamiento que parezca vaya a cambiar en el futuro.

- Sin embargo, los **usuarios desprevenidos**, con medidas bajas de protección y uso intensivo de Internet, pueden dirigir su comportamiento hacia el componente autoregulatorio de la seguridad.

En general se ha observado que la tendencia se dirige hacia un estado de mayor seguridad con el paso del tiempo. Los usuarios van a aprendiendo a protegerse, sobre todo después de incidencias graves que les causan pérdidas de información y daños en los equipos.

La tendencia descendente del número de incidencias y de la gravedad de las mismas, se ha puesto de manifiesto por casi todos los tipos de usuarios.

- El componente de **necesidad de protección individual** parece bien asentado en la mayor parte de los usuarios. Si bien hay algunos grupos que requieren todavía formación e información sobre como protegerse adecuadamente.

- La asignatura pendiente parece residir en la **dimensión social de la seguridad**, sobre todo a la vista de los buenos resultados que obtienen los actuales usuarios “solidarios”.

- El tercer nivel de la seguridad se refiere a la **intervención de la Administración**. Aunque desde el momento de su origen el fenómeno Internet ha favorecido la autorregulación, la extensión de su horizonte hacia todo tipo de usuarios abre la puerta hacia una mayor presencia de los poderes públicos. Dado que en algunos casos los usuarios muestran signos de desorientación en seguridad, para garantizar lo que empieza a verse como el "derecho de utilizar Internet sin sobresaltos". Junto a esto, la Administración puede responsabilizarse de la formación de los usuarios, de la creación de una cultura de seguridad, y de la persecución de delitos, que como se ha demostrado son medidas fundamentales para contribuir a la seguridad de los usuarios en Internet.

10 CONCLUSIONES Y RECOMENDACIONES

El principal interrogante que ha motivado la realización de este Estudio es determinar el nivel de seguridad de los hogares/usuarios españoles de Internet y la confianza que tienen en general respecto a la Sociedad de la Información, y, en particular con relación a Internet. La vía para alcanzar dicho objetivo ha sido doble: por una parte evaluando la confianza y percepción de seguridad de los usuarios y, por otro lado, realizando un análisis del nivel real de incidencias de seguridad en los equipos de los hogares españoles usuarios de Internet. El resultado del contraste de ambas variables es una serie de segmentos y perfiles de usuarios en función de la seguridad de la información.

Se han detectado tres estilos de hábitos de seguridad que delimitan tres segmentos de usuarios:

- **Uso Prudente y no solidario**. Caracterizado por un enfoque individualista de la seguridad, centrándose en la defensa particular y olvidando compartir experiencias para la defensa solidaria. El 58% de los usuarios pertenecen a este tipo.

- **Uso prudente y solidario**. Añaden a la protección individual, la preocupación por compartir y la mutua ayuda en temas de seguridad. Son un 33% de los usuarios.

- **Uso temerario**. Son un 9% de usuarios que no atienden a las normas y hábitos básicos de la prudencia, sufren muchas incidencias y de mayor gravedad, pero no por ello modifican sus hábitos imprudentes.

Visto en su conjunto (social y tecnológicamente), el sistema de seguridad en Internet viene definido empíricamente por las siguientes características:

En primer lugar, la mayor parte de los usuarios utilizan el equipamiento básico de protección al conectarse a Internet. Antivirus y cortafuegos se utilizan por más del 75% de los usuarios. Otras protecciones como anti-correo no deseado, anti-espías, utilización de contraseñas y actualizaciones de seguridad del sistema operativo, las ponen en práctica en torno al 50% de los usuarios.

Otras medidas de seguridad que exigen un comportamiento más activo por parte del usuario como copias de seguridad, partición del disco duro o encriptación, son bastante minoritarias. Ahora bien, estas mismas medidas encuadradas dentro del concepto de “seguridad proactiva del usuario” son las que presentan una mayor previsión de crecimiento en los próximos meses según las opiniones de los propios usuarios.

En general, los usuarios parecen buscar modos de seguridad que no exijan una atención constante, ni interfieran con la sensación de uso libre de Internet.

El nivel de incidencias declaradas por los usuarios es considerable, aunque la frecuencia de incidencias serias es menos elevada. Cabe destacar, entre las consecuencias más frecuentes declaradas por los usuarios, el 40,4% de los hogares que tuvieron que formatear el disco duro y el 23,6% perdieron archivos, al menos en una ocasión, desde que están conectados a Internet en el hogar, por culpa de las incidencias de seguridad.

Entre las incidencias de seguridad, la más frecuente es la recepción de correo no deseado (spam). Sólo en la última semana un 66,1% de los hogares ha sufrido este tipo de incidencia. En el último año un 52,8% declaran haber sufrido virus informáticos, pero otras amenazas serias como fraudes o robos en cuentas o tarjetas del crédito, no alcanzan el 5%.

Se aprecia, por lo general, en el comportamiento de los usuarios, una actitud de seguimiento de las recomendaciones básicas de seguridad, aunque todavía se producen incidencias graves.

Por su parte, el escaneo de los equipos ha revelado que el 72,6% de los usuarios tienen algún tipo de código malicioso en su ordenador, aunque la mayor parte de estos códigos tienen una peligrosidad moderada o baja. Un 51,8% de los ordenadores escaneados presenta algún código de riesgo alto. Son en la actualidad más frecuentes las incidencias de códigos maliciosos de troyanos o software publicitario, entre cuyos objetivos tienen principalmente el pasar desapercibidos en el sistema infectado. Esto es posible por el aumento de las técnicas de ocultación como *rootkits*. Por lo que hoy en día pasan más desapercibidas las infecciones para los usuarios. El cambio de tendencia de producción de códigos maliciosos de gusanos y virus, que provocaban grandes epidemias, a troyanos y software publicitario, es fiel reflejo de la tendencia actual de que la producción de *malware* está enfocada hacia el fraude y el lucro económico de los creadores de dichos códigos. A lo que se añade la gran variedad de códigos maliciosos existentes y la aparición diaria de multitud de variantes.

El efecto de las incidencias sobre el comportamiento de los usuarios se desarrolla en dos vertientes:

- Actualizando, renovando o instalando nuevas barreras de protección. La medida sobre la que más frecuentemente se actúa es el programa antivirus, tanto a nivel de actualización, como de cambio de proveedor o de primera instalación.

- Modificando sus opiniones y hábitos en la red. En este caso se aprecia la concienciación sobre estar más informados, extremar las precauciones, aumentar la solidaridad con otros usuarios y exigir en mayor medida la actuación de la Administración.

El análisis señala en general que las incidencias no están impulsando que los usuarios abandonen servicios o dejen de utilizar Internet. El usuario tiene una percepción elevada de la seguridad, indicando la gran mayoría de los usuarios, un 86%, que su ordenador está razonablemente protegido. Sólo ante un aumento destacable del número de incidencias en el equipo del hogar, se modifican los comportamientos o medidas de seguridad para mantener alta la percepción de seguridad. Sin embargo, entre los usuarios que no han sufrido incidencias graves de seguridad, la reacción ante una incidencia es la de continuar utilizando los mismos servicios de Internet que venían utilizando anteriormente. Aunque casi la mitad de los hogares indican que utilizarían más servicios si supieran reducir su riesgo. Existe un efecto de retraso sobre el desarrollo de la Sociedad de la Información, y debe buscarse este efecto entre los no usuarios, aquellos que no se sienten suficientemente protegidos como para desarrollarse plenamente en Internet.

De forma general, los usuarios habituales de Internet han englobado de tal forma los servicios online en su estilo de vida que se les hace muy difícil prescindir de los mismos. El motivo puede ser de operatividad, dado que sean condiciones de servicio único las que rijan con dicha prestación. Puede tratarse también de una serie de condiciones que obliguen al usuario a no poder realizar su actividad más que de ese único modo. En este contexto, las incidencias sufridas se interpretan como avisos para aumentar su equipamiento de protección y/o para mostrarse más prudentes en sus hábitos, pero no se interpretan como razones para abandonar o reducir el uso del medio. Simplemente, para muchos usuarios, la segunda alternativa no parece posible.

En estos casos, se pide una mayor atención sobre lo que sucede en Internet, complementado con una mayor diligencia en la persecución de los infractores y mayor contundencia con los mismos.

A pesar de las incidencias declaradas, y del conocimiento del riesgo bastante realista que manifiestan los usuarios, la sensación general es de confortable seguridad en el uso de Internet. La gran mayoría considera que su conexión y su equipo les garantizan una navegación segura. Es por ello que los usuarios, aún para los servicios que estos perciben como peligrosos, consideran que su nivel de riesgo es moderado. Los usuarios perciben que la seguridad en Internet ha evolucionado de manera positiva en el último año. Igualmente, los usuarios piensan que sus equipos están más protegidos ahora que hace un año, esto puede hacer que los usuarios actúen de modo menos prudente.

Los análisis realizados ponen de manifiesto que la e-confianza está en los 76,4 puntos de media en una escala de 0 a 100. Esta e-confianza es elevada en todos los grupos de usuarios, sin distinción de sus hábitos de riesgo o del nivel de equipamiento en seguridad. Solamente se sitúa por debajo de los 70 puntos entre quienes han sufrido con mucha reiteración incidencias de seguridad destacables (más de 3 consecuencias graves).

La conclusión que se puede extraer es que la confianza elevada es un prerrequisito para el uso gratificante de Internet. Los usuarios tienden a mantener esta e-confianza por encima de los 75 puntos.

Cuando se rompe la sensación de seguridad por una incidencia inesperada, el usuario intenta recomponer el equilibrio aumentando su equipamiento en seguridad, aumentando su prudencia o ambas a la vez.

Generalmente, estos cambios sirven para recomponer un nivel confortable de e-confianza. Pero si no resulta como se espera (incidencias reiteradas), comienza a cobrar fuerza la necesidad de apoyo de un tercero. Este tercero al que se demanda ayuda es la Administración.

En concreto, el papel que los usuarios asignan a la Administración en materia de seguridad parece consistir en ser una última instancia. El resultado debe garantizar la seguridad cuando las medidas al alcance del usuario y los hábitos prudentes de navegación se revelan insuficientes. En general, esta intervención es aceptada y reclamada por más del 70% de los usuarios.

El resultado global de este proceso de reequilibrio en el tiempo es que los usuarios opinan que se ha reducido en el último año tanto el número como la gravedad de incidencias que padecen en sus equipos. Lo que refuerza su idea de que el reequilibrio es la estrategia adecuada.

Dado que nivel de equipamiento básico es similar en la mayor parte de los usuarios, la prudencia en los hábitos de uso se ha revelado como un importante factor de protección adicional. De hecho, los resultados del escaneo de los ordenadores muestran cómo los hábitos de seguridad marcan generalmente las diferencias en incidencias entre los usuarios con antivirus y sistemas operativos actualizados.

En materia de seguridad se puede hablar de una e-paradoja: algunos usuarios se sienten seguros por sus sistemas actualizados de protección. Pero su número de incidencias reales es mayor debido a que sus prácticas se vuelven imprudentes. Los usuarios con hábitos prudentes y sistemas de protección actualizados son quienes presentan un menor número de incidencias reales. Como se ha señalado, los sistemas de protección, por sí solos, son insuficientes para garantizar la seguridad del sistema.

El papel de la Administración es clave: se debe canalizar información atendiendo tanto a los sistemas de protección como a las prácticas seguras.

Se ha podido comprobar empíricamente gracias al escaneo de los ordenadores el impacto de los “hábitos saludables” de seguridad en Internet (prudencia y solidaridad con otros usuarios). Es reseñable, por ejemplo, que una mayoría de los usuarios de Internet, un

70%, se ponen en contacto con el remitente de correos electrónicos cuando éstos contienen archivos infectados. Este tipo de prácticas contribuye al control de las infecciones y limita los daños causados por el malware. Estos hábitos se relacionan con una reducción de los *troyanos* de un 31,0% y de un casi 21,0% en el caso de los *virus*.

Si se comparan estos resultados con el impacto aislado de los programas antivirus en la reducción de los códigos maliciosos, la diferencia entre tener antivirus o no tenerlo sólo es de dos puntos porcentuales en cuanto al porcentaje de equipos infectados. Estos datos se explican debido a la especial situación que vive el sector en estos momentos. Por otro lado, se demuestra que actualizar el sistema operativo es importante para mejorar el estado de las infecciones pero, dado que existen vulnerabilidades que afectan a programas que no son propiamente el sistema operativo, no es suficiente la actualización únicamente del propio sistema operativo. Es por ello que tanto la actualización de todo el software del equipo, como el factor sociológico son muy importantes para mejorar la seguridad.

Los datos indican que las incidencias reales de seguridad detectadas en el escaneo parecen tener su solución en dos factores relativamente independientes: la presencia real de dispositivos de seguridad y los hábitos de uso preventivos y solidarios. Ambos factores constituyen los pilares de la seguridad del Sistema y su complementariedad debería ser potenciada en la medida de lo posible: no hay seguridad sin la presencia simultánea de ambos.

Con el Estudio se han identificado tres debilidades del Sistema:

- Posiblemente la principal vulnerabilidad empírica, la conducta temeraria, se incrementa firmemente a medida que se reduce la edad. Es propia de jóvenes, principalmente varones que viven en el hogar paterno y no comparten su equipo con otras personas. Esta conducta terminará por afectar a otras partes de sistema general debido a la naturaleza interactiva y social del fenómeno Internet y de los servicios y medios de comunicación entre usuarios: correo electrónico, intercambio de archivos y programas, etc. También se ha detectado que el uso compartido del terminal es un factor positivo de reducción de las incidencias, dado que aquellos usuarios que comparten el uso del mismo equipo son más precavidos en su navegación.

- Un segundo punto frágil del Sistema, de menor intensidad, proviene de los usuarios de Internet con menor experiencia y déficit de equipamiento en seguridad, que no consiguen reducir su riesgo real a pesar de mostrar unos hábitos prudentes de navegación.

- La tercera debilidad del Sistema, que afecta a la mayoría de los usuarios, consiste en que estos tienden a hacer residir la e-confianza en el equipamiento y en las soluciones individuales, quizá influidos por la comunicación y el marketing de estos productos, despreocupándose de los hábitos de seguridad, que se han demostrado fundamentales para mantener la seguridad de los equipos. A esto hay que añadir la significación de las amenazas "invisibles" para el usuario, como las que detecta el programa de escaneo instalado en los hogares. Estas amenazas no son detectadas por los usuarios en ningún momento y por tanto no son conscientes de sus consecuencias.

Por tanto se hace necesario un esfuerzo en dos frentes: por un lado, potenciar el uso de dispositivos de seguridad y, por otro lado, remarcar la necesidad de un uso responsable de los equipos, para que esos dispositivos sean realmente eficaces. Esto permitiría evitar el efecto paradójico ya comentado de que el equipamiento en seguridad lleve a un comportamiento demasiado imprudente que potencie la vulnerabilidad del sistema.

Es por ello que hay que incidir en crear una cultura de seguridad. Es necesario que los usuarios sean conscientes de la utilidad de las soluciones como los antivirus, cortafuegos, anti correo basura, actualizaciones de seguridad, etc., pero también deben conocer sus limitaciones, las amenazas reales, y las recomendaciones adicionales, para que no se cree una falsa sensación de seguridad. Es imprescindible, para aumentar la seguridad, el proporcionar a los usuarios de una mayor formación de cara a realizar un uso responsable y seguro de las nuevas tecnologías, con hábitos de uso basados en la precaución y la protección.

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

Instituto Nacional
de Tecnologías
de la Comunicación

www.inteco.es