GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza2

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles

3er trimestre de 2010 (14ª oleada)

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Enero 2011

El informe de la 14ª oleada del "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles" ha sido elaborado por el siguiente equipo de trabajo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (dirección)

Susana de la Fuente Rodríguez (coordinación)

Laura García Pérez

Cristina Gutiérrez Borge

Eduardo Álvarez Alonso

Correo electrónico del Observatorio de la Seguridad de la Información: ***observatorio@inteco.es***

INTECO quiere señalar la participación en la realización del trabajo de campo e investigación de este estudio de:

ÍNDICE

PUNTOS CLAVE

El presente informe constituye una nueva entrega trimestral del *Estudio sobre la seguridad de la información y e-confianza en los hogares españoles*. Gracias a la realización de encuestas periódicas y al análisis online de los equipos que componen la muestra, el informe permite realizar, con una perspectiva evolutiva, un diagnóstico de la situación de los hogares españoles conectados a Internet en lo que respecta a la seguridad de la información y e-confianza.

El período analizado en este documento abarca los meses de julio a septiembre de 2010. Durante este tiempo se han realizado 3.538 encuestas y 8.836 análisis online a los 7.351 equipos que componen el panel.

Se exponen a continuación los puntos clave del análisis.

I Medidas y hábitos de seguridad

Los primeros puestos en el ranking de utilización declarada de medidas de seguridad están ocupados, una vez más, por medidas automatizables: programas antivirus (92,5%), cortafuegos o firewall (81,3%) y actualizaciones del sistema operativo (80,7%). Por detrás de ellas, se encuentran dos medidas no automatizables, como son el uso de contraseñas (79,3%) y la eliminación de archivos temporales y cookies (79,2%).

Como ya ocurriera en trimestres anteriores, destaca la predisposición positiva de los usuarios por incorporar el DNI electrónico a corto plazo: un 33% de los encuestados manifiesta tener intención de utilizar el DNIe en los tres meses siguientes a la realización de la encuesta.

Los usuarios confían en las medidas cuya configuración permite una puesta en marcha automática: el 80,8%, declara que su sistema operativo gestiona las actualizaciones de forma automática.

Los usuarios de redes sociales cada vez son más cuidadosos con su privacidad, y en este sentido el 66,2% declara que su perfil puede ser visto únicamente por sus amigos o contactos, lo que supone un incremento de 6,5 puntos porcentuales en los últimos 18 meses.

Con respecto a los hábitos de seguridad observados en hogares donde viven menores que se conectan a Internet, el 47,8% de los padres reconocen haber creado una cuenta de usuario limitado para el acceso del menor a Internet. Este dato resulta muy positivo puesto que limita el impacto en el equipo de una potencial conducta peligrosa por parte del menor.

II Incidencias de seguridad

El incidente más común es de nuevo la recepción de correos electrónicos no deseados o spam. En los últimos tres meses ha afectado al 66,9% de los encuestados, según sus propias declaraciones. De acuerdo con los datos empíricos facilitados por las redes de sensores de INTECO, en septiembre de 2010 se detectó que el 77,4% de los correos circulantes era basura.

El 53,6% de los equipos auditados alojan malware en septiembre de 2010, un dato que se mantiene estable en los últimos meses.

Este trimestre vuelve a dominar el troyano como tipo de código más detectado en septiembre, con un 38,7% de equipos que albergan programas de esta categoría. Por detrás del tipo troyano se encontraría, una vez más, el adware (27,1%).

En septiembre de 2010, un 38,1% de los equipos son considerados de riesgo alto, frente a un 10,3% de riesgo medio y un 5,2% de riesgo bajo. Se confirma la progresiva reducción de los niveles de riesgo de los equipos a lo largo del último año, sobre todo, en el caso de riesgo medio.

III Consecuencias de las incidencias de seguridad y reacción de los usuarios ante ellas

El 60,6% de los usuarios no ha realizado ningún cambio en sus hábitos de navegación por Internet como resultado de una incidencia vivida, frente a un 39,4% que sí ha adoptado algunas medidas de precaución.

Los cambios que llevan a cabo los usuarios en sus hábitos de seguridad tras haber experimentado una incidencia son de carácter preventivo, como el refuerzo o la instalación de determinadas medidas de seguridad, mientras que con una frecuencia muy baja se producen abandonos en el uso de servicios.

Entre las reacciones dirigidas al refuerzo o la instalación de medidas de seguridad, las acciones más habituales de los usuarios son actualizar los programas de seguridad (que sube tres puntos desde el trimestre pasado, desde el 52,1% al 55%) y cambiar las contraseñas (que ha descendido del 48, 7% al 45,9% en esta oleada).

En cuanto a la forma de resolver los problemas de seguridad que afectan a los ordenadores, buena parte de los encuestados declara que lo hacen de manera autónoma. Casi la mitad de los usuarios (44,6%) afirma que se ocupa él mismo sin la ayuda de nadie y un 19% lo hace con la orientación de alguien más experto para solucionarlos.

IV e-Confianza de los hogares españoles

La mayoría de los internautas españoles confían en Internet (89,9%). De ellos, un 40,4% reconocen tener bastante confianza en la Red, frente a un 6,4% que admiten depositar mucha y un 43,1% adicional que muestra un nivel de confianza suficiente.

Además, un 81,5% de los ciudadanos encuestados considera que su ordenador está razonablemente protegido, y un 45,2% está de acuerdo en afirmar que Internet es cada día más seguro.

A pesar de estos datos, que suponen un indicio del adecuado nivel de e-Confianza existente en los hogares españoles, los usuarios siguen mostrando mayor confianza en las operaciones físicas que en sus homólogas en el mundo virtual. Así, un 72,9% confía mucho o bastante en la realización de transacciones bancarias en una sucursal, frente a un 50,8% que reconoce confiar cuando se llevan a cabo a través de la Red.

Ante la afirmación *La Administración tiene que implicarse más en mejorar la seguridad en Internet*, un 79,3% de los encuestados se muestra de acuerdo o totalmente de acuerdo, mientras que a un 17,3% le es indiferente.

A la Administración, los usuarios le piden principalmente vigilar más de cerca lo que está pasando en Internet (28%) y desarrollar y ofrecer herramientas de seguridad gratuitas (26,4%)

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

1.1.1 Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las PYMES, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

- **Seguridad Tecnológica:** INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y por supuesto que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT) con su Centro Demostrador de Tecnologías de Seguridad, y la Oficina de Seguridad del Internauta, de los que se benefician ciudadanos, PYMES, Administraciones Públicas y el sector tecnológico.

- **Accesibilidad:** INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus

usuarios. Y que faciliten la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. Asimismo desarrolla proyectos en el ámbito de la accesibilidad orientados a garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las AA.PP.

- **Calidad TIC**: INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software.

- **Formación**: la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

1.1.2 Observatorio de la Seguridad de la Información

OBSERVATORIO INTECO

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica. 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.

1.2 Estudio sobre la seguridad de la información y e-confianza en los hogares españoles

El *Estudio sobre la seguridad de la información y e-confianza en los hogares españoles* es el referente nacional, en términos de diagnóstico, del estado de adopción de medidas de seguridad y del nivel de incidencia de situaciones que pueden constituir riesgos de seguridad, así como del grado de confianza que los hogares españoles depositan en la Sociedad de la Información. El presente informe constituye la decimotercera entrega del mismo.

El estudio cuenta con dos particularidades, que lo convierten en material de referencia en seguridad de la información a nivel nacional e internacional:

- En primer lugar, la investigación se realiza con una perspectiva evolutiva, realizándose lecturas periódicas de los indicadores de seguridad y e-confianza que permiten llevar a cabo un análisis histórico y definir tendencias y pronósticos.

- En segundo lugar, los resultados del estudio proceden de una doble fuente, poniendo en contraste la percepción del usuario y la situación de seguridad real.

1.2.1 Objetivo general

El objetivo general de este estudio es el análisis, basado en las percepciones de los usuarios, de la evolución de la situación de seguridad de la información y confianza entre

los usuarios de Internet españoles, al mismo tiempo que el contraste con el nivel real de seguridad e incidencias que mantienen sus equipos.

Se pretende, en última instancia, impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe tiene como finalidad servir de apoyo en la adopción de medidas por parte de la Administración.

Este objetivo general se desglosa a su vez en dos:

- Analizar hasta qué punto la falta de seguridad de la Red puede suponer un freno para el desarrollo de 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 en la Sociedad de la Información, sustentada en una percepción realista de los riesgos y los beneficios de la misma.

1.2.2 Objetivos específicos

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

Medidas y hábitos de seguridad

- Conocer el nivel de implantación actual de las medidas de seguridad automatizables y no automatizables y analizar su evolución temporal.

- Analizar la frecuencia con la que los usuarios de Internet aplican y actualizan las herramientas de seguridad de sus equipos.

- Conocer los motivos que los ciudadanos argumentan para no utilizar medidas de seguridad.

- Establecer pronósticos sobre la implantación futura de herramientas de seguridad.

- Identificar hábitos seguros de comportamiento seguidos por los usuarios españoles de Internet y el grado de adopción de los mismos.

Incidencias de seguridad

- Conocer la frecuencia con la que los usuarios declaran padecer incidencias de seguridad en sus equipos.

- Determinar la evolución del nivel de incidencia general del código malicioso o malware y definir sus diferentes categorías: virus informáticos, troyanos, gusanos, programas espía, etc.

- Analizar la diversificación del código malicioso actual, a partir de la existencia de variantes únicas y del número de detecciones en los equipos.

- Catalogar los tipos de malware más frecuentes y la gravedad de los mismos.

- Conocer la reacción de los usuarios ante una incidencia de seguridad.

Percepción de seguridad y e-confianza de los hogares españoles

- Determinar el nivel de confianza electrónica desde el punto de vista de los usuarios, así como su tendencia de evolución.

- Analizar en qué medida la seguridad afecta a la utilización de nuevos servicios.

- Señalar los principales agentes responsables de la seguridad en Internet y colaborar con ellos para ayudar a garantizar el estado de protección de los usuarios.

- 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.

Sistema de indicadores

- Establecer un sistema de indicadores que permita monitorizar la evolución de la seguridad en el acceso a Internet desde los hogares.

2 DISEÑO METODOLÓGICO

El *Estudio sobre la seguridad de la Información y la e-confianza de los hogares españoles* se realiza a partir de una metodología basada en el panel online dedicado.

En la definición de la metodología del estudio, se ha considerado una fórmula que permita obtener información, con una perspectiva evolutiva, relativa al nivel de seguridad y e-confianza de los hogares españoles. La necesidad de unos datos robustos sobre los mismos hogares y usuarios en diferentes momentos del tiempo hace que el panel online dedicado resulte la metodología idónea para satisfacer los objetivos del proyecto.

El presente informe constituye la decimotercera entrega del estudio, cuya primera lectura data de diciembre de 2006.

En la actualidad el panel está compuesto por 7.351 hogares con conexión a Internet repartidos por todo el territorio nacional. Sobre los miembros del panel se aplican dos técnicas diferenciadas, que permiten obtener dos tipos diferentes de información:

- Encuestas online a usuarios españoles de Internet mayores de 15 años con acceso frecuente desde el hogar, llevadas a cabo con una periodicidad trimestral. Los datos extraídos de las encuestas permiten obtener la percepción sobre la situación de la seguridad en Internet y nivel de e-confianza de los usuarios domésticos. En el período analizado en la presente entrega (3er trimestre de 2010), 3.538 usuarios han respondido a la encuesta. 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%, el error muestral para n=3.538 es de ±1,68%.

- Auditoría remota online del nivel de seguridad real de los equipos informáticos existentes en los hogares, realizados mensualmente. Para ello, se utiliza el software iScan[1], desarrollado por INTECO, que analiza los sistemas y las incidencias de seguridad en los equipos gracias a la utilización conjunta de 46 motores antivirus. Este software se instala en los equipos y los analiza, detectando todo el malware residente en los mismos y recogiendo además datos del sistema operativo, de su estado de actualización y de las herramientas de seguridad instaladas. El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada. La muestra en este tercer trimestre de 2010 se compone de 3.846 hogares que escanearon online su ordenador entre julio y septiembre de 2010. El número total de análisis remotos de seguridad o escaneos realizados en el período ha sido 8.836.

[1] En el Anexo I se incluye un apunte metodológico completo donde se explica de forma detallada el funcionamiento de iScan.

La fortaleza de la metodología empleada se basa en dos pilares:

- Las lecturas periódicas (trimestrales en el caso de las encuestas y mensuales en el caso de los análisis online) permiten comparaciones evolutivas que identifican variaciones y tendencias.

- La combinación de medidas objetivas de incidencia con medidas subjetivas de percepción de seguridad y confianza en la Red garantiza el contraste entre la percepción sobre la seguridad que tienen los encuestados y la situación real de los equipos de los panelistas.

El lector puede hallar una caracterización más detallada de la muestra y del software iScan en el anexo titulado *Diseño metodológico detallado*.

3 MEDIDAS Y HÁBITOS DE SEGURIDAD

El uso de las nuevas tecnologías ya no se concibe sin la seguridad asociada y activada desde su diseño. Los líderes del mercado de los nuevos dispositivos, sistemas operativos y programas, han tomado la seguridad como una prioridad, y no como algo accesorio (algo que, sorprendentemente, ocurría hace pocos años). Este esfuerzo de los fabricantes y programadores, aunque positivo, no es suficiente: los usuarios deben mantener unas medidas y hábitos de seguridad saludables para que las medidas técnicas surtan realmente efecto.

En este epígrafe se analizan las medidas y hábitos de seguridad que siguen los internautas españoles.

3.1 Medidas de seguridad

En el análisis de las medidas de seguridad, se ofrece el contraste entre la opinión del usuario acerca de las que cree tener instaladas en su equipo y los resultados ofrecidos por iScan[2], que ofrece una visión de las herramientas realmente implantadas. Esta información permite identificar el grado de familiarización de los panelistas con el equipamiento de su máquina.

3.1.1 Medidas automatizables y no automatizables: nivel de implantación y evolución

En función del nivel de participación del usuario, las medidas de seguridad se clasifican en automatizables y no automatizables.

- Las medidas automatizables o de carácter pasivo son aquellas que, por lo general, no requieren una actuación específica por parte del usuario, o cuya configuración permite una puesta en marcha automática. En general, se podrían considerar herramientas de seguridad en sentido estricto.

- Las medidas no automatizables o de carácter activo requieren la participación del usuario para su funcionamiento. Más que de herramientas, se trata de acciones llevadas a cabo por el usuario que redundan en una mayor seguridad (por ejemplo: utilización de contraseñas, realización de copias de seguridad, partición de disco duro, etc.).

En la Tabla 1 se muestra el porcentaje de usuarios que declara utilizar cada medida y se contrasta, en los casos en los que es posible, con el dato real obtenido a través del

[2] Op. cit 1

programa iScan[3]. Se encuentran ordenadas de forma descendente por porcentaje de uso declarado y se distingue entre automatizables (sombreadas) y no automatizables.

En el conjunto de medidas, aquellas en las que la implicación del usuario es pasiva muestran una mejor penetración frente a las medidas que requieren proactividad.

Los primeros puestos coinciden con medidas automatizables: programas antivirus (92,5%), cortafuegos o firewall (81,3%) y actualizaciones del sistema operativo (80,7%). Por detrás de ellas, se encuentran dos medidas no automatizables, como son el uso de contraseñas (79,3%) y la eliminación de archivos temporales y cookies (79,2%).

La zona media de la tabla se reparte entre medidas automatizables y no automatizables. En el primer caso, destacan los programas de bloqueo de ventanas emergentes (72,5%), programas anti-spam (68,9%) y programas anti-espía (63,9%). En relación a las no automatizables, los usuarios declaran la realización de medidas de tratamiento y recuperación de información, como la realización de copias de seguridad de archivos (61,7%), las copias de discos de restauración del sistema (60,3%) y partición del disco duro (46,8%).

Las medidas cuyo uso declarado es inferior son el cifrado de documentos o datos (21,1%), el DNI electrónico (21,7%) y los certificados digitales de firma electrónica (30,7%).

¿Qué beneficios aportan los certificados digitales de firma electrónica?

Los certificados son documentos electrónicos que garantizan la identidad del usuario que los utiliza. Aunque se utilizan comúnmente en los servidores web con conexiones cifradas para autenticar la página a la que el usuario se conecta, también pueden ser utilizados desde el lado del cliente. Así, este también se autentica ante el servidor. Son como una especie de DNI para los sistemas informáticos. Asocian una firma electrónica a un usuario. Muchos sistemas de autenticación online se basan en certificados y no solo en contraseñas para permitir acceso a los recursos. El acceso al certificado, a su vez, puede estar protegido por contraseña. Esto eleva la seguridad general del acceso puesto que en este caso el factor de autenticación es doble: algo que se posee (el certificado) y algo que se conoce (la contraseña que lo protege). Los certificados se almacenan en un lugar determinado del sistema operativo, y son utilizados por el navegador cuando la página lo solicita. El único inconveniente para el usuario es que no podría acceder a los recursos en todos los sistemas operativos, sino solo en los equipos en los que haya instalado personalmente su certificado digital.

[3] Op. cit. 1

Tabla 1: Utilización declarada y real de medidas de seguridad automatizables y no automatizables 3T 2010 (%)

Medidas de seguridad[4]	Declarado 3T 10	Real Sep. 10
Programas antivirus	92,5%	81,4%
Cortafuegos o firewall	81,3%	
Actualizaciones del SO y programas	80,7%	47,3%
Contraseñas (equipos y documentos)	79,3%	
Eliminación de archivos temporales y cookies	79,2%	
Programas de bloqueo de ventanas emergentes	72,5%	
Programas anti-spam	68,9%	
Programas anti-espía	63,9%	
Copias de seguridad de archivos	61,7%	
Copia discos de restauración del sistema	60,3%	
Partición del disco duro	46,8%	
Búsqueda información sobre seguridad informática	45,9%	
Programas de control parental[5]	41,4%	
Utilización habitual con permisos reducidos	37,7%	21,9%
Programas anti-fraude	37,4%	
Certificados digitales de firma electrónica	30,7%	
DNI electrónico	21,7%	
Cifrado de documentos o datos	21,1%	

Base: Total usuarios (n=3.538) *Fuente: INTECO*

En relación al contraste entre las herramientas que el usuario declara y el uso real que lleva a cabo, se señalan los aspectos más importantes a continuación:

- Programas antivirus: este software se ha identificado en el 81,4% de los equipos auditados, frente al 92,5% declarado por los usuarios encuestados. La diferencia entre los dos valores (11,1 puntos porcentuales) es ligeramente superior con respecto a trimestres anteriores.

- Actualizaciones del SO y programas: el sistema operativo está efectivamente actualizado en un 47,3% de los ordenadores; según declaraciones de los usuarios, en un 80,7%. La brecha entre ambos valores ha crecido hasta los 33,4 puntos, lo que puede significar una errónea percepción por parte de los usuarios en relación a la automatización de las actualizaciones de los equipos y programas. En la página web de INTECO-CERT (http://cert.inteco.es/) se proporcionan servicios gratuitos que ayudan a realizar esta tarea.

[4] Las medidas automatizables aparecen sombreadas.

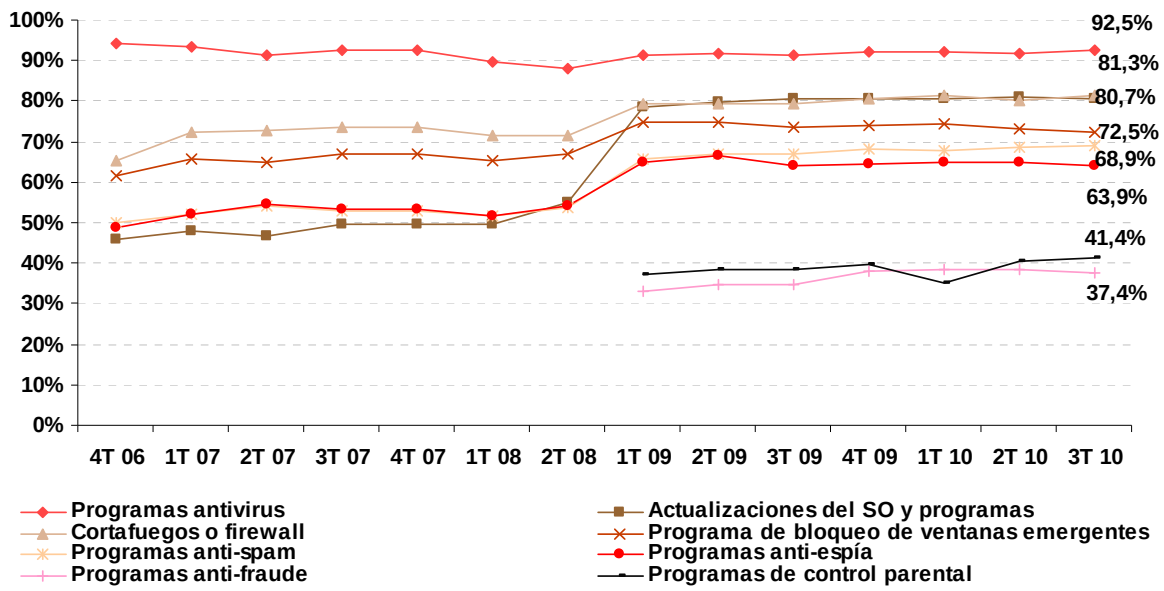
[5] Los datos referentes a los programas de filtro de contenidos (control parental para menores) se presentan sobre la submuestra de usuarios con hijos menores que se conectan a Internet (20,1%).

- Utilización con permisos reducidos: frente a un 37,7% de usuarios que declaran la utilización de cuentas con permisos reducidos, la herramienta de escaneo confirma un 21,9% real. En este caso, la diferencia entre los dos valores es de 15,8 puntos porcentuales, inferior a trimestres anteriores. Todavía cabe un amplio margen de mejora: los usuarios deben entender que el uso sin privilegios del sistema operativo es una de las medidas más eficaces contra el malware en general.

El Gráfico 1 muestra la evolución en el uso declarado de medidas automatizables. En el último trimestre, las oscilaciones de los distintos valores han sido mínimas con respecto al período anterior, con ligeras subidas en la utilización declarada de cortafuegos o firewall (1,3 puntos porcentuales), programas de control parental (1 punto porcentual), programas antivirus (0,9 puntos porcentuales) y programas anti-spam (0,5 puntos porcentuales).

Tomando como referencia el periodo comprendido entre el primer trimestre de 2009 y la actualidad, destaca la recuperación experimentada en el uso declarado de programas de control parental. Tras la caída experimentada en el primer trimestre de 2010, en la que registró su mínimo (35,1%), en los últimos dos trimestres ha confirmado su recuperación hasta alcanzar en el último periodo analizado su valor histórico más alto (41,4%).

Gráfico 1: Evolución de la utilización declarada de medidas de seguridad automatizables[6] (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

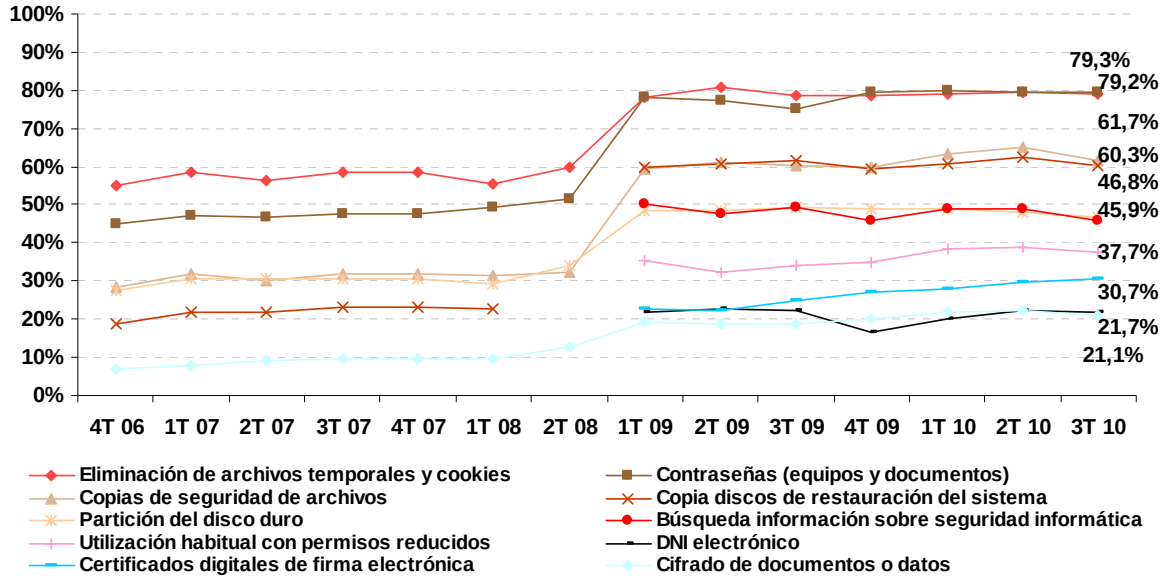
[6] Op. cit. 5

El Gráfico 2 presenta la evolución de las medidas de seguridad no automatizables. En este caso, el último trimestre muestra un ligero descenso en la mayoría de las herramientas analizadas, salvo en el caso de la utilización de certificados de firma electrónica, que experimenta una subida de 0,8 puntos porcentuales con respecto al trimestre anterior, hasta alcanzar el 30,7%.

Desde comienzos de 2009, las series han mostrado bastante estabilidad, con niveles de uso declarado en torno al 80% en utilización de contraseñas y eliminación de cookies (79,3% y 79,2%, respectivamente). En torno al 60% de seguimiento se encuentran la realización de copias de seguridad de archivos (61,7%) y copia de los discos de restauración del sistema (60,3 %). Por detrás de estas medidas, la partición del disco duro y la búsqueda de información de seguridad informática también presentan una evolución con valores cercanos al 50%, situándose en el 46,8% y el 45,9% respectivamente, datos que muestran un ligero descenso en el último trimestre.

Por último, las medidas con menor uso declarado también revelan una evolución positiva desde comienzos de 2009, con valores entre el 20 y el 40%. Destaca el caso del DNI electrónico, que confirma el repunte experimentado durante 2010 hasta alcanzar el 21,7%, por delante del cifrado de documentos o datos (21,1%).

Gráfico 2: Evolución de la utilización declarada de medidas de seguridad no automatizables (%)



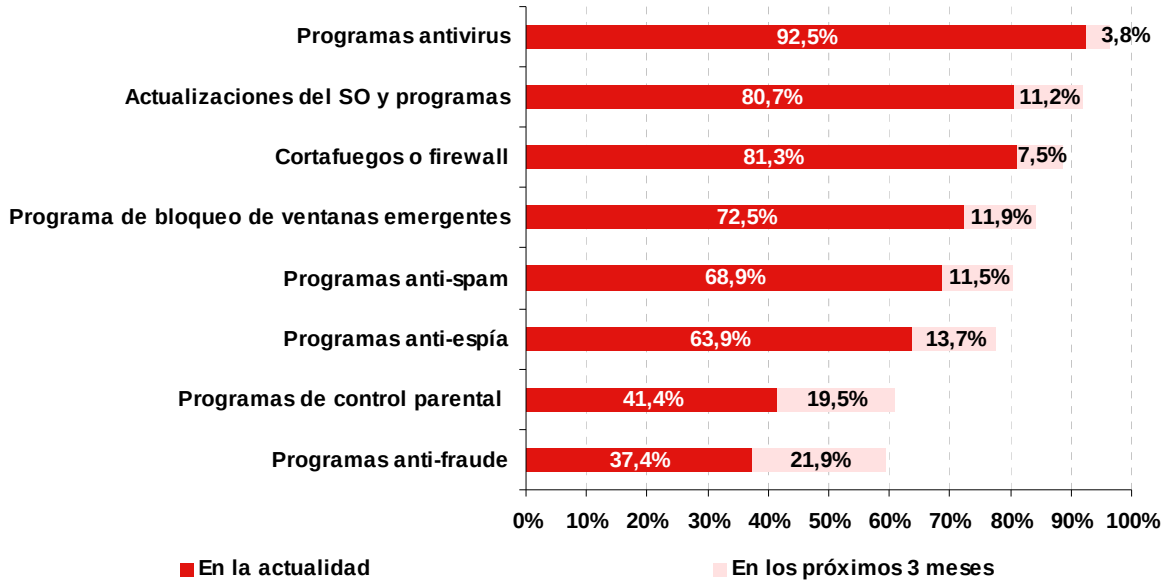
Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

3.1.2 Estimaciones a futuro

El Gráfico 3 muestra la intención que declaran los usuarios de utilizar las medidas de seguridad automatizables en los tres meses siguientes a la realización de la encuesta.

Las medidas menos instaladas actualmente son las que presentan mayor intención de uso en el futuro inmediato. Así, los usuarios pretenden incorporar en mayor medida programas anti-fraude (21,9%), programas de control parental (19,5%) y programas anti-espía (13,7%).

Gráfico 3: Intención declarada de uso de medidas de seguridad automatizables en los próximos 3 meses (datos del 3T 2010)[7] (%)



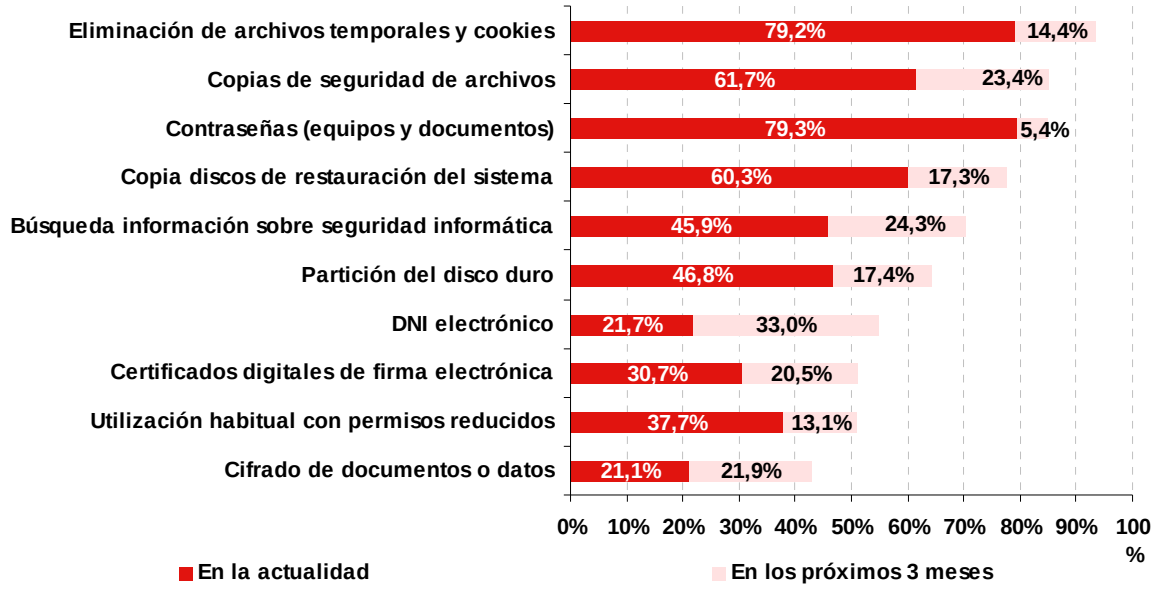
Base: Total usuarios (n=3.538) *Fuente: INTECO*

El mismo análisis para las medidas no automatizables se muestra en el Gráfico 4, si bien en este caso no siempre se cumple que las medidas con menor implantación tengan mayor intención de uso en los próximos tres meses.

Como ya ocurriera en trimestres anteriores, destaca la predisposición de los usuarios por incorporar el DNI electrónico a corto plazo (33%), la búsqueda de información sobre seguridad informática (24,3%) y la realización de copias de seguridad de archivos (23,4%).

[7] Op. cit. 5

Gráfico 4: Intención declarada de uso de medidas de seguridad no automatizables en los próximos 3 meses (datos del 3T 2010) (%)



Base: Total usuarios (n=3.538) *Fuente: INTECO*

3.1.3 Motivos alegados para no utilizar medidas de seguridad

En la Tabla 2 se muestran los motivos que los usuarios declaran para no utilizar las medidas automatizables analizadas en la actualidad ni tener intención de incorporarlas en los próximos tres meses.

Los dos motivos más alegados para no utilizar cada una de las medidas expuestas son la falta de necesidad y el desconocimiento.

El primer motivo, la falta de necesidad, es el más alegado para no utilizar programas de control parental. Casi la mitad (el 44,9%) de individuos que ni utilizan ni tienen intención de incorporar esta medida alegan que no la necesitan. En el caso de los antivirus, destaca que el 26,7% de los encuestados que no tienen intención de utilizar esta medida declaren no necesitarlo, siendo este programa una capa de seguridad necesaria en cualquier equipo.

El segundo motivo alegado es el desconocimiento, con especial relevancia entre aquellos que no tienen intención de utilizar los programas anti-fraude (40,6%), los programas anti-espía (32,8%) o programas de bloqueo de ventanas emergentes (32%), entre otros. Esta situación puede ser debida, en parte, a la tendencia de la industria antivirus a comercializar paquetes únicos que incorporan varias de estas funcionalidades (módulos anti-fraude, anti-espía, anti-spam, etc.).

Realmente, hoy en día, debido al uso masivo por parte de spammers y atacantes del correo como vehículo para difundir malware y correo basura, no es posible realizar un uso eficaz de ninguna cuenta de correo si previamente no ha sido filtrada por algún sistema anti-spam. Aunque el usuario final no lo perciba, su correo puede haber sido filtrado (es muy probable) por parte del servidor en una etapa anterior que el usuario no controla. Incluso, muchos clientes actuales de correo cuentan con algún sistema anti-spam que, de forma transparente para el usuario, elimina el correo basura de la bandeja de entrada.

Tabla 2: Motivos para no aplicar medidas de seguridad automatizables 3T 2010 (%)

Medidas	% hogares que no tienen intención de utilizar	Motivos						
		No conoce	No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros
Programas antivirus	3,7%	3,1	**26,7**	16,1	22,2	0,0	10,7	21,2
Actualizaciones del SO y programas	8,1%	**23,9**	5,1	16,7	21,2	2,1	8,9	22,1
Cortafuegos o firewall	11,3%	**31,2**	12,1	12,8	21,5	1,0	7,1	14,3
Programas de bloqueo de ventanas emergentes	15,7%	**32,0**	12,3	10,5	22,0	0,5	7,5	15,3
Programas anti-spam	19,6%	**20,5**	**20,5**	9,4	17,8	1,4	14,4	16,0
Programas anti-espía	22,4%	**32,8**	15,7	11,6	15,6	1,3	9,2	13,9
Programas de control parental[8]	39,0%	10,7	**44,9**	3,6	17,6	0,6	8,8	13,8
Programas anti-fraude	40,7%	**40,6**	17,5	10,5	9,8	1,5	8,6	11,5

Base: Usuarios que no tienen intención de utilizar cada medida *Fuente: INTECO*

En cuanto a los motivos declarados para no utilizar las medidas no automatizables en el presente o futuro cercano, igualmente destacan la falta de necesidad y el desconocimiento.

El 57,9% de los usuarios que no tienen intención de utilizar contraseñas declaran que es porque no las necesitan. Lo mismo ocurre en el caso de la utilización habitual con permisos reducidos (40,4%) y de las copias de seguridad de archivos (26,9%). Sin embargo, es importante recordar la importancia que tiene la información hoy en día en los diferentes ámbitos del individuo (personal, profesional, etc.) por lo que, para asegurar la integridad, la disponibilidad y la confidencialidad de la información es recomendable utilizar estas herramientas de protección.

Los usuarios declaran que el desconocimiento de la medida es el argumento para no utilizar certificados digitales de firma electrónica (42,8%), realizar partición del disco duro

[8] Op. cit. 5

(41%), cifrado de documentos o datos (40,9%) e incorporar medidas para la eliminación de archivos temporales y cookies (40,7%).

Por último, la categoría "Otros motivos" es alegada mayoritariamente por los encuestados que no tienen intención de utilizar el DNI electrónico (44,5%), hacer copias de restauración de discos del sistema (34,5%) ni realizar búsquedas de información sobre seguridad de la información (32,9%).

Tabla 3: Motivos para no aplicar medidas de seguridad no automatizables en 3T 2010 (%)

Medidas	% hogares que no tienen intención de utilizar	Motivos						
		No conoce	No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros
Eliminación archivos temporales y cookies	6,5%	**40,7**	10,6	3,6	13,6	0,0	12,0	19,6
Copia de seguridad de archivos	14,9%	26,5	**26,9**	4,8	8,7	0,2	8,3	24,6
Contraseñas (equipos y documentos)	15,3%	7,0	**57,9**	0,6	8,8	0,2	7,8	17,7
Copia discos de restauración del sistema	22,5%	30,6	15,2	5,2	7,2	0,6	6,7	**34,5**
Búsqueda información sobre seguridad informática	29,8%	23,2	23,5	4,6	6,0	1,6	8,1	**32,9**
Partición del disco duro	35,7%	**41,0**	14,7	2,1	10,1	0,6	6,6	24,9
DNI electrónico	45,3%	15,2	21,6	4,4	2,7	5,5	6,2	**44,5**
Certificados digitales de firma electrónica	48,8%	**42,8**	16,1	3,4	3,0	2,1	6,2	26,3
Utilización habitual con permisos reducidos	49,3%	22,5	**40,4**	1,7	12,1	0,2	4,2	18,7
Cifrado de documentos o datos	57,0%	**40,9**	22,7	2,4	6,6	0,7	4,8	21,9

Base: Usuarios que no tienen intención de utilizar cada medida *Fuente: INTECO*

3.1.4 Frecuencia de actualización y aplicación

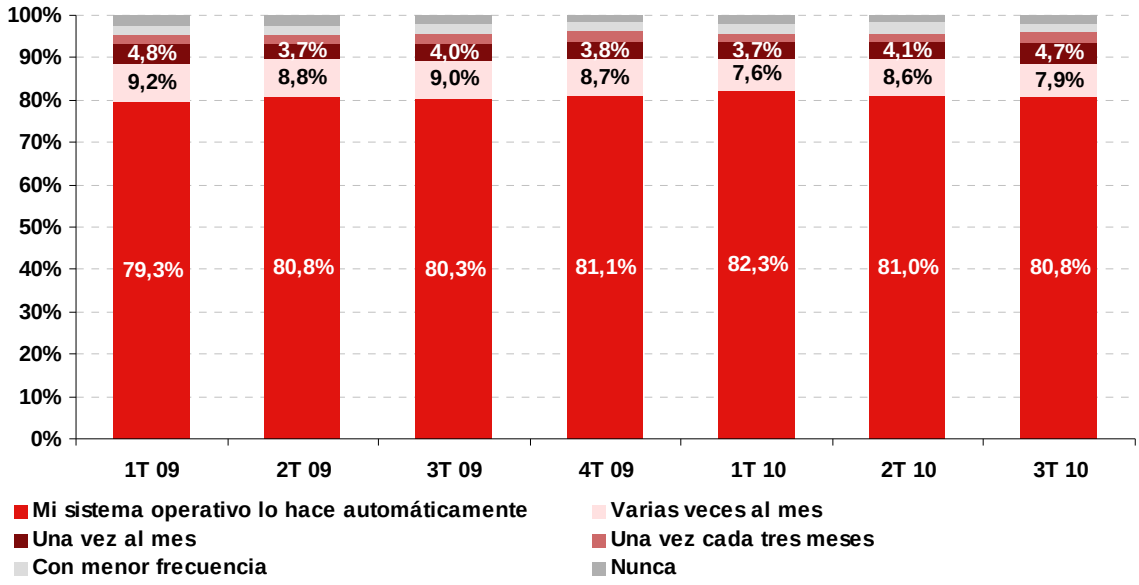
En el caso de las herramientas de seguridad, las actualizaciones no solo están destinadas a mejorar el producto, corregir errores o proporcionar nuevas funcionalidades, sino que también constituyen una fuente de protección frente a nuevas amenazas.

Hace algunos años, los propios antivirus recomendaban una actualización semanal de sus bases de datos para mantener la protección. Hoy en día, todas las casas de antivirus actualizan diariamente (y muchas de ellas en varias ocasiones) sus firmas. Incluso así, tienen problemas para abarcar todo el malware que se genera. Por tanto, la actualización de las herramientas de seguridad supone un paso fundamental para que sean realmente eficaces.

Tanto los programas de seguridad como los sistemas operativos no actualizados suponen un peligro mayor del que en un principio se pudiese considerar, no solo para el usuario sino para cualquier sistema que se relacione con él o al que se encuentre conectado. Estos equipos son muy vulnerables a todo tipo de ataques, y por tanto, la probabilidad de que se infecten con malware o acaben controlados por terceros es muy alta. Estos sistemas suponen un riesgo por ellos mimos y suponen un importante foco de infección por ser usados por los atacantes como plataformas anónimas desde donde realizar nuevos ataques e infecciones.

El Gráfico 5 presenta la evolución de la actualización de herramientas de seguridad, en términos de frecuencia declarada. La mayoría de usuarios, el 80,8%, declara que su sistema operativo gestiona las actualizaciones de forma automática. La evolución observada en los últimos 7 trimestres corrobora esta afirmación y la constancia en la tendencia.

Gráfico 5: Evolución de la frecuencia declarada de comprobación de la actualización de herramientas de seguridad (%)

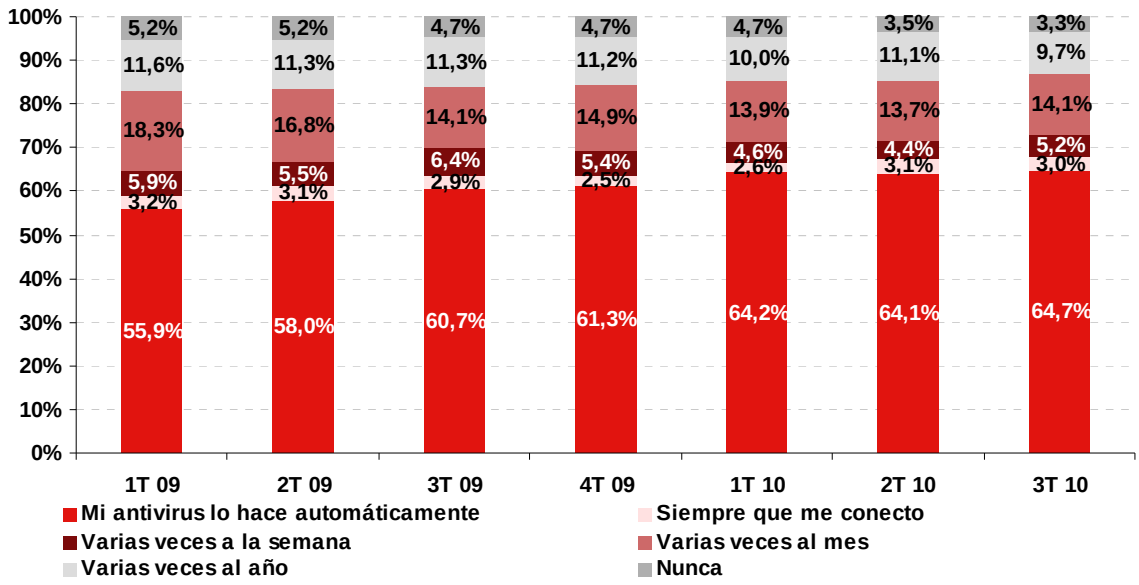


Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

Para mantener estándares adecuados de protección, es necesario realizar un análisis del sistema operativo cada cierto tiempo, con el objetivo de buscar nuevas amenazas. Los ficheros que en principio no son detectados como malware durante su uso, podrían serlo con un análisis completo del disco duro realizado por un programa antivirus, ya que estos programas actualizan frecuentemente sus bases de datos de malware.

En este sentido, el Gráfico 6 presenta la frecuencia de escaneo del ordenador con el programa antivirus con datos de los últimos siete trimestres. El 64,7% de los usuarios confía en el antivirus el escaneo del equipo, delegando en la herramienta la frecuencia con la que se realice este análisis. Se observa una línea ascendente, lenta pero constante, en cuanto a la proporción de usuarios que confían en el análisis automático de los antivirus.

Gráfico 6: Evolución de la frecuencia declarada de escaneo del ordenador con el programa antivirus (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

3.2 Hábitos seguros de comportamiento en Internet

A continuación se ofrece una visión del nivel de adopción de hábitos seguros en la utilización de Internet, agrupándose en 6 categorías: 1) navegación por Internet; 2) correo electrónico; 3) chats y mensajería instantánea; 4) banca en línea y comercio electrónico; 5) redes P2P y 6) redes sociales.

Para cada una de estas categorías se han evaluado tanto los comportamientos que pueden suponer un riesgo, como los que pueden ayudar a prevenir incidentes de seguridad. Se han presentado a los panelistas una serie de actitudes en este sentido y se les ha pedido que respondan si se muestran de acuerdo o en desacuerdo con la afirmación.

3.2.1 Navegación por Internet

El navegador ha pasado en apenas unos años de ser una herramienta opcional en un sistema operativo, a convertirse en centro de operaciones de los equipos actuales. Con el avance de los lenguajes de programación adicionales al HTML que lo potencian y

dinamizan, la web 2.0 y el traslado de las aplicaciones a la Web (y a la nube), la navegación se ha convertido en el centro neurálgico del Internet actual y, consecuentemente, en un punto objetivo para atacantes.

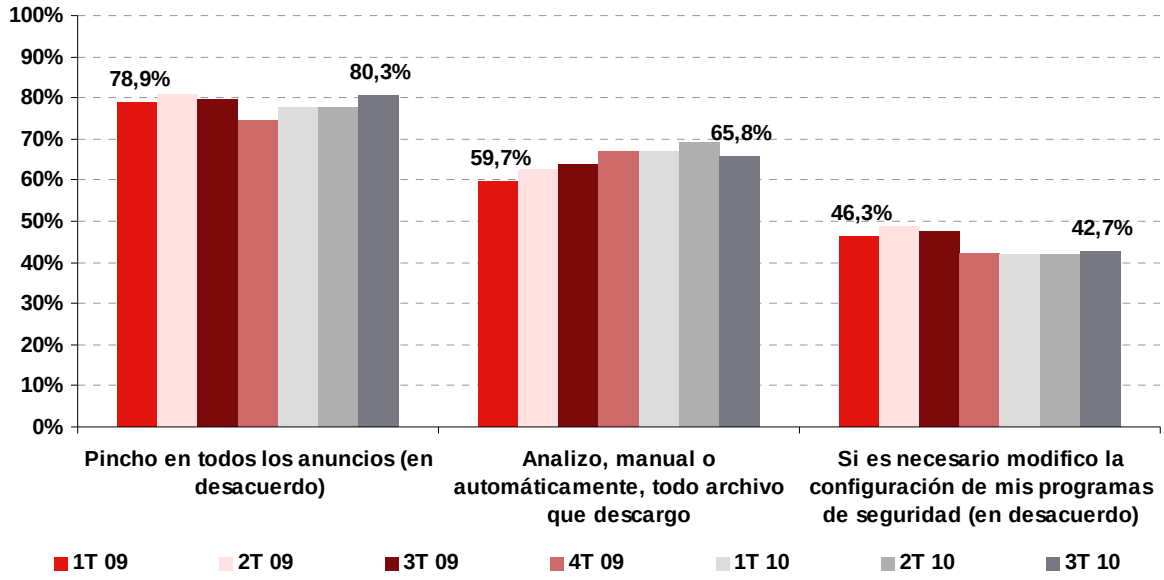
Con respecto a la navegación por Internet, se analizan tres comportamientos prudentes. La apreciación "en desacuerdo" implica que el porcentaje de usuarios indicado no realizan esas prácticas en su navegación en Internet, evitando así comportamientos que podrían derivar en situaciones peligrosas para su sistema y datos.

- *Pincho en todos los anuncios interesantes o atractivos, aunque no conozca al anunciante (en desacuerdo)*. Remonta ligeramente, con respecto a datos del los últimos tres trimestres, el porcentaje de usuarios que se muestra en desacuerdo con pinchar en todos los anuncios (80,3%).

- *Analizo, manual o automáticamente, con un antivirus todo archivo que descargo de Internet antes de abrirlo / ejecutarlo.* Este dato disminuye ligeramente con respecto al porcentaje del trimestre anterior y se sitúa en el 65,8% de los encuestados. No obstante, la evolución experimentada desde comienzos de 2009 es de signo positivo, con un incremento de 6,1 puntos porcentuales desde el inicio de la serie.

- *Si es necesario, modifico la configuración de mis programas de seguridad o del sistema operativo de mi ordenador para poder acceder a servicios web o juegos que me interesan (en desacuerdo).* Se mantiene la tendencia constante del último año, con un 42,7% de los encuestados. La evolución desde comienzos de 2009 es de signo ligeramente negativo, lo que podría indicar cierta tendencia a asumir el comportamiento imprudente de modificar la configuración de sus programas.

Gráfico 7: Evolución de los hábitos prudentes relacionados con la navegación por Internet (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

3.2.2 Correo electrónico

Se analizan cuatro comportamientos prudentes que tienen que ver con el uso del correo electrónico:

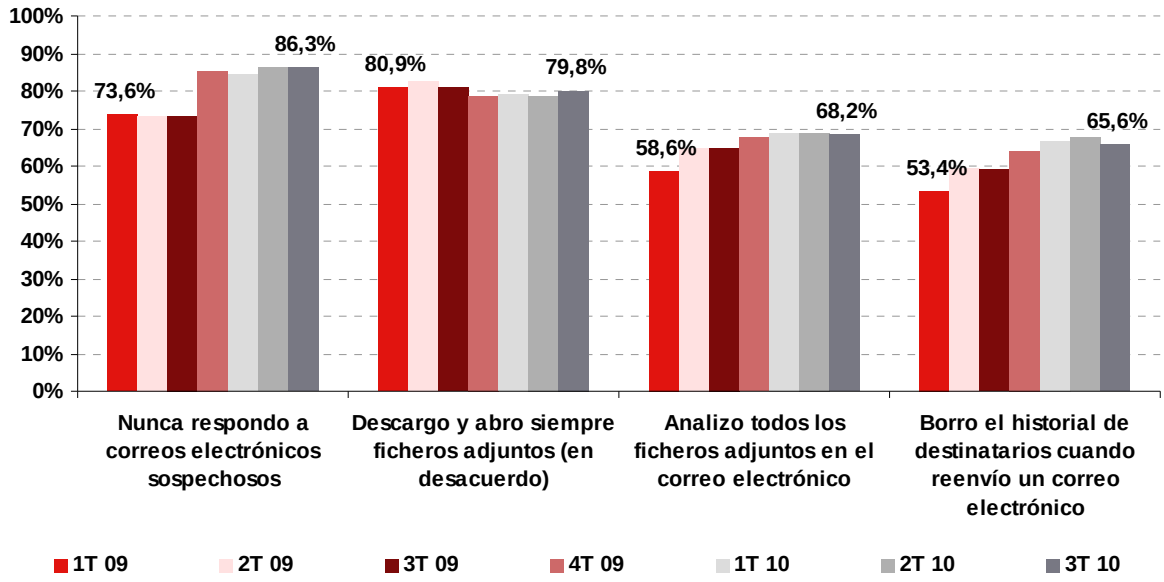
- *Nunca respondo a correos electrónicos sospechosos de ser falsos ni a cadenas de correo.* El 86,3% de los usuarios de Internet españoles corroboran esta afirmación, la más seguida de las cuatro analizadas. Desde el inicio de la serie (primer trimestre de 2009), se consolida la adopción de esta medida, con un ascenso de 12,7 puntos porcentuales.

- *Descargo y abro ficheros adjuntos a correos electrónicos procedentes de desconocidos, o que yo no haya solicitado, si me parecen interesantes (en desacuerdo).* De nuevo una gran mayoría de usuarios está en desacuerdo con esta afirmación, el 79,8%, siendo la evolución de este valor bastante estable a lo largo de la serie.

- *Analizo todos los ficheros adjuntos en el correo electrónico con un antivirus antes de abrirlos.* La evolución de esta práctica de seguridad muestra signo positivo, pasando de un 58,6% declarado en el primer trimestre de 2009 a un 68,2% en el tercer trimestre de 2010. Este último dato es muy similar a los trimestres anteriores.

- *Borro el historial de destinatarios cuando reenvío un correo electrónico a múltiples direcciones.* La evolución de los usuarios que declaran borrar el historial de destinatarios al reenviar un correo electrónico mantiene su línea ascendente, con el 65,6 % de usuarios, frente al 53,4% de principios de 2009.

Gráfico 8: Evolución de los hábitos prudentes relacionados con el correo electrónico (%)



Base: Usuarios que utilizan el correo electrónico (n=3.538 en 3T10) *Fuente: INTECO*

3.2.3 Chats y mensajería instantánea

En el Gráfico 9 se analizan cinco comportamientos prudentes que tienen que ver con la utilización de chats y mensajería instantánea:

- *Nunca facilito datos confidenciales (contraseñas, nombre de usuario).* Los usuarios son conscientes de la importancia de mantener su privacidad en los servicios de chats y mensajería instantánea. Este es el hábito con mayor tasa de seguimiento, con un 88,8% en este trimestre y una subida de 15,6 puntos porcentuales desde el primer trimestre de 2009.

- *Evito pinchar en invitaciones a visitar sitios web que proceden de desconocidos*. La segunda afirmación con mayor tasa de seguimiento, un 87,6%, muestra su máximo histórico en este trimestre.

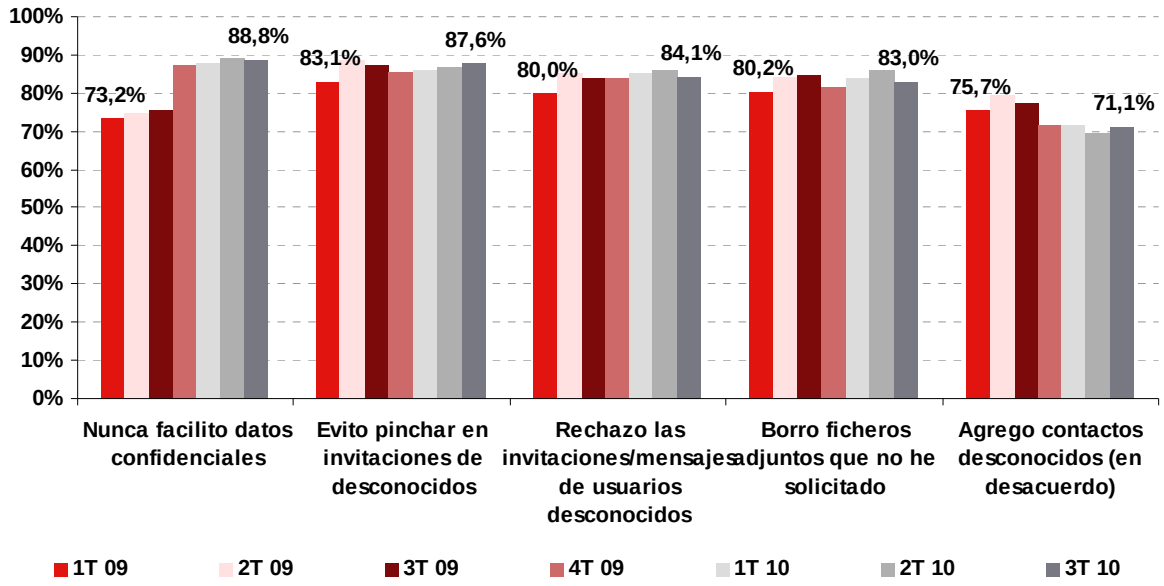
- *Rechazo las invitaciones / mensajes de usuarios que no conozco o de los que no quiero recibir mensajes*. El valor que alcanza este hábito es el 84,1%, lo que indica un amplio seguimiento por parte de los internautas españoles y una estabilidad en su evolución desde comienzos de 2009.

- *Borro los ficheros adjuntos que no he solicitado y que recibo por mensajería instantánea*. Este hábito prudente también demuestra estabilidad en su evolución, con un 83% de tasa de seguimiento en el último trimestre analizado.

- Agrego contactos de terceros desconocidos al programa de mensajería (Messenger, ICQ) *(en desacuerdo).* Este es el comportamiento menos corroborado de los cinco, si bien un mayoritario 71,1% de los ciudadanos usuarios de Internet lo siguen. Su evolución muestra una ligera tendencia a la baja en relación a valores de principios de 2009 (75,7%), pero con una mayor estabilidad en el último año.

De forma general, se mantiene el elevado nivel de cumplimiento de comportamientos seguros en estos servicios que tienen que ver con los chats y mensajería instantánea: cuatro de los cinco comportamientos presentan una tasa de seguimiento superior al 80%.

Gráfico 9: Evolución de los hábitos prudentes relacionados con chats y mensajería instantánea (%)



Base: Usuarios que utilizan mensajería instantánea y/o chats (n=2.906 en 3T10) *Fuente: INTECO*

3.2.4 Banca en línea y comercio electrónico

En el Gráfico 10 se analizan seis comportamientos que tienen que ver con la seguridad en la realización de transacciones de banca en línea y comercio electrónico.

- *Cierro la sesión al terminar de realizar operaciones online con mi banco*. El 87% de usuarios de banca online declara realizar este hábito prudente, con datos ligeramente superiores a los de trimestres anteriores, en moderada tendencia al alza.

- *Evito usar equipos públicos o compartidos (cibercafés, estaciones o aeropuertos)*. El segundo hábito con mayor tasa de seguimiento (83,2%) muestra una tendencia bastante estable desde comienzos de 2009, cuando alcazaba un valor de 82,1%

- *Vigilo periódicamente los movimientos de la cuenta bancaria en línea*. Cada vez son más los usuarios (79,1%) que observan los movimientos de su cuenta, con un signo positivo en su evolución. Este hábito constituye una alerta temprana ante un intento de fraude.

> Se deben vigilar periódicamente los movimientos de la cuenta bancaria no sólo desde el mismo equipo desde el que habitualmente se realizan las transacciones, sino desde un canal diferente como pueden ser los cajeros automáticos o los extractos físicos que el banco envía a sus clientes. Se han detectado familias de troyanos que además de todas las técnicas habituales que usa el malware para pasar desapercibido, falsea el balance del usuario víctima una vez ha sido robado. Así, el afectado no puede detectar la falta de dinero en su cuenta a menos que analice un extracto por algún otro medio.[9]

- *Cuando mi banco me pide mis datos personales o contraseñas por correo electrónico o por teléfono se los facilito (en desacuerdo)*. El 76,9% de los ciudadanos se muestra en desacuerdo con esta afirmación, confirmando el repunte del trimestre anterior.

> Con la popularización de la Voz sobre Protocolo de Internet (VoIP) y el consiguiente abaratamiento de las conferencias, además de la posibilidad de sistematizar los procesos de llamadas automáticas se ha extendido lo que se conoce como "vishing" (phishing a través del VoIP). Esta técnica consiste en llamar indiscriminadamente a números de teléfono donde una grabación invita a las potenciales víctimas a entregar sus números secretos de banca online. Se trata de una técnica similar al phishing a través de llamadas telefónicas. Para evitar este tipo de estafas, se recomienda que sea el usuario el que inicie la llamada y marque explícitamente el número oficial del banco con el que desea ponerse en contacto.

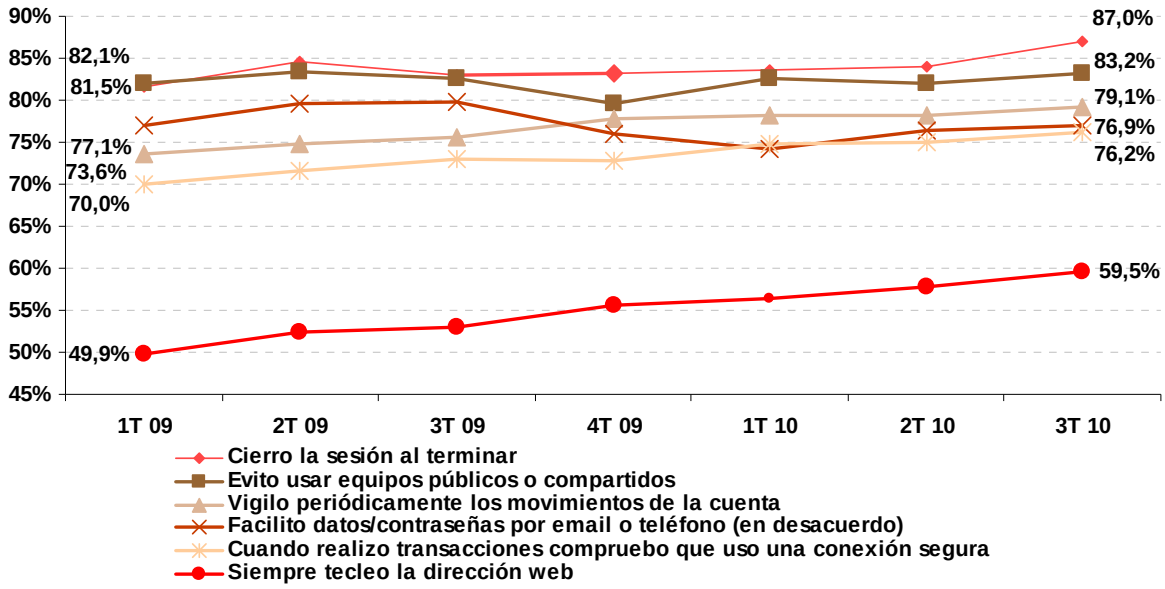
- *Cuando realizo transacciones en línea (pagos, compras, transferencias) compruebo que uso una conexión segura (protocolo https, validez y vigencia del certificado)*. Este hábito muestra un comportamiento ascendente, lento pero continuado, pasando del 70% de comienzos de 2009 al 76,2% actual.

- *Siempre tecleo la dirección web de mi banco en la barra de direcciones*. El hábito menos seguido de los seis analizados es teclear directamente la dirección web del banco en la barra del navegador, con un 59,5%. Sin embargo, es el que mayor

[9] Fuente: http://www.hispasec.com/unaaldia/3994

crecimiento ha experimentado en los últimos 7 trimestres, con casi 10 puntos porcentuales más que en el primer trimestre de 2009 (49,9%).

Gráfico 10: Evolución de los hábitos prudentes relacionados con banca en línea y comercio electrónico (%)



Base: Usuarios que utilizan banca en línea y/o comercio electrónico (n=3.248 en 3T10) *Fuente: INTECO*

3.2.5 Redes P2P

Las redes P2P están dando paso a otro tipo de sistemas de intercambio de archivos centralizados. Estos son los llamados de "Descarga Directa" y tienen la ventaja de contar con un servicio gratuito que permite la descarga a gran velocidad de un número limitado de archivos, y servicios de pago donde tanto la descarga como el ancho de banda para el usuario son ilimitados. Compañías como RapidShare y Megaupload son el mayor exponente en este sentido, y están desplazando a sistemas P2P tradicionales como Bittorrent, Emule, etc.

En este epígrafe se analizan tres comportamientos que tienen que ver con la seguridad en la utilización de redes *peer to peer* o P2P. Los resultados se plasman en Gráfico 11.

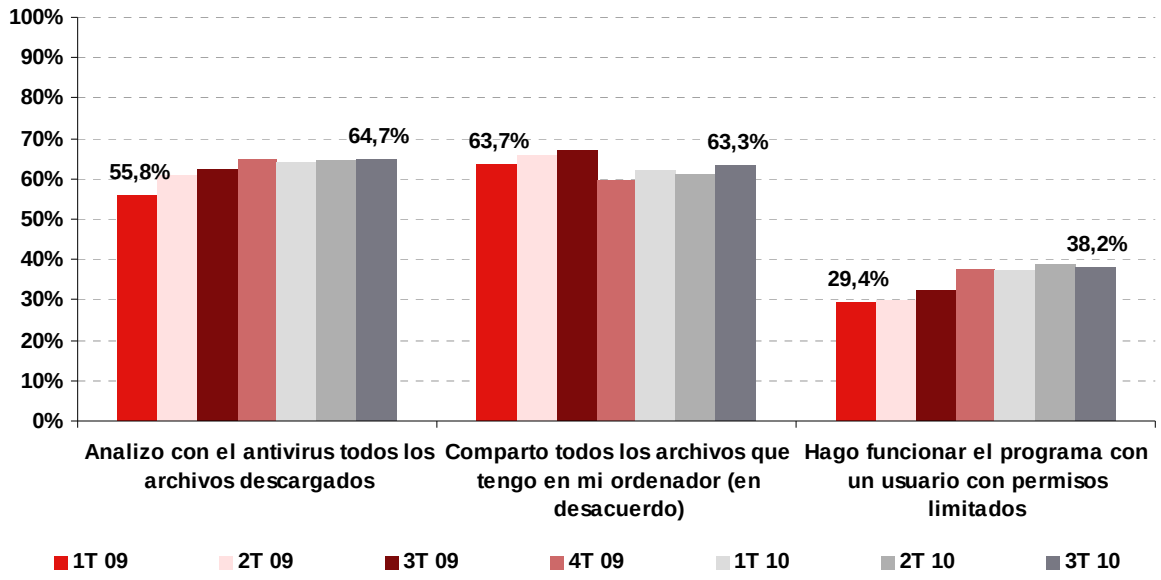
- *Analizo con el programa antivirus todos los archivos descargados a través de redes P2P*. El 64,7% de los usuarios P2P españoles observa este hábito prudente, lo que consolida la tendencia creciente iniciada en el 1er trimestre de 2009

- *Comparto todos los archivos que tengo en mi ordenador con el resto de usuarios P2P (en desacuerdo).* Este indicador muestra valores muy similares (63,3%) a los de comienzo de serie (63,7%), lo que significa que estos usuarios son conscientes

de la importancia de proteger su intimidad y la seguridad de su equipo, evitando que terceros tengan acceso a la información almacenada en su equipo: fotografías, documentos, vídeos, etc.

- *Hago funcionar el programa de P2P con un usuario con permisos limitados*. Este hábito, a pesar de su evolución positiva (se ha pasado de un 29,4% a principios de 2009 a un 38,2% en esta última lectura), indica que los usuarios P2P no siguen de manera mayoritaria un comportamiento prudente a la hora de gestionar los privilegios de acceso.

Gráfico 11: Evolución de los hábitos prudentes relacionados con las redes P2P (%)

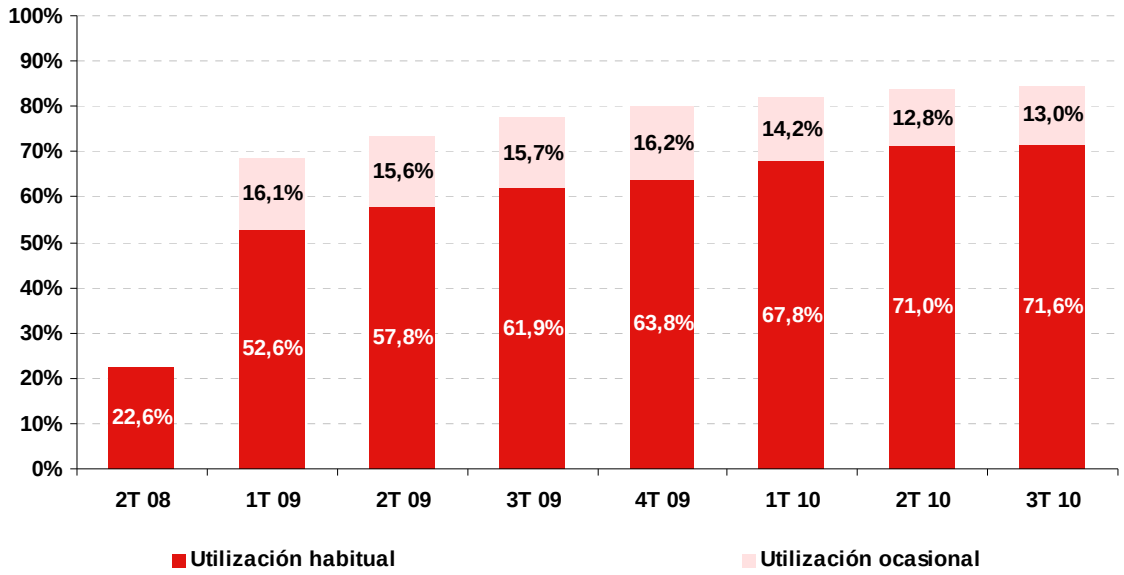


Base: Usuarios que utilizan redes P2P (n=2.463 en 3T10) *Fuente: INTECO*

3.2.6 Redes sociales

Durante 2010 las cifras sobre el uso de las redes sociales en España demuestran que se están haciendo imprescindibles para los internautas españoles. En el 3er trimestre de 2010, un 71,6% afirma utilizar habitualmente las redes sociales, y un 13% dice hacerlo esporádicamente.

Gráfico 12: Evolución de la utilización declarada de redes sociales (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

En el Gráfico 13 se analizan los usos que hacen los ciudadanos de las redes sociales.

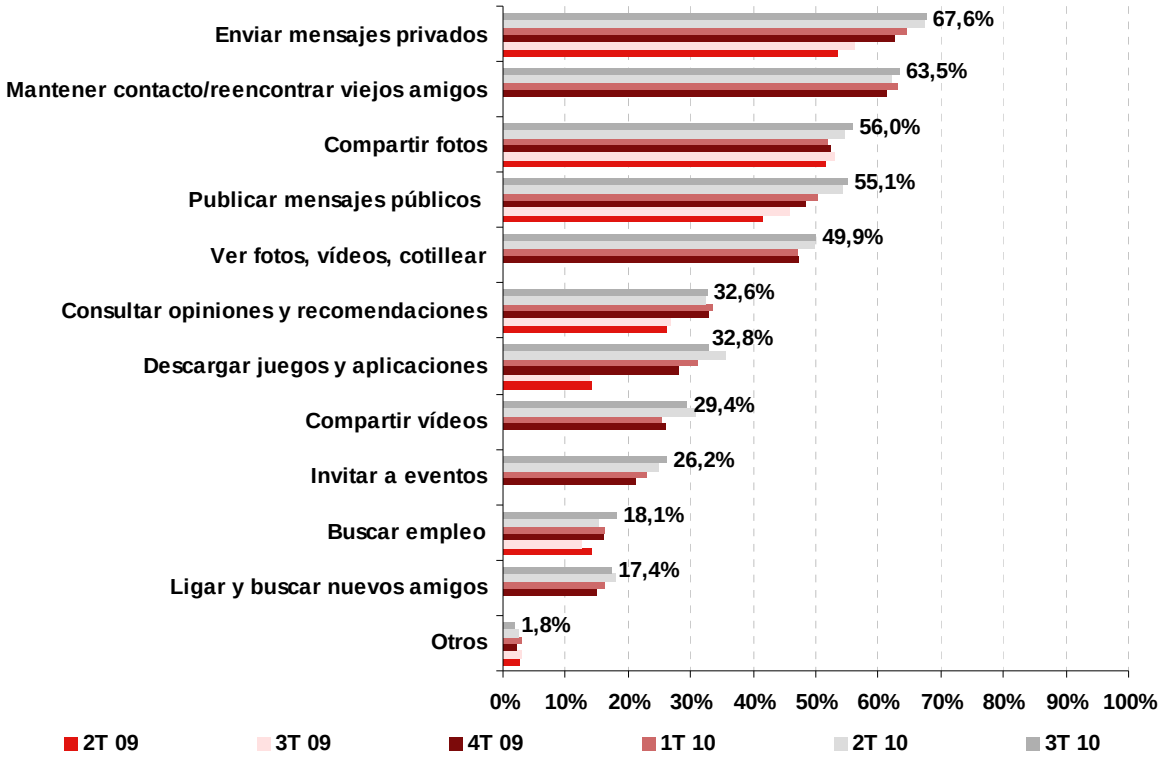
Las actividades preferidas por los usuarios de redes sociales siguen siendo el envío de mensajes y comentarios privados (declarado por un 67,6%), mantener el contacto y reencontrar a viejos amigos (63,5%) y compartir fotos (56%).

Por detrás estarían actividades como publicar mensajes públicos (55,1%) y ver contenido multimedia y cotillear (49,9%).

Los últimos lugares los ocupan actividades con carácter más esporádico para los usuarios, como invitar a eventos (26,2%), buscar empleo (18,1%) o buscar nuevos amigos y ligues (17,4%).

De forma general, la evolución muestra una mayor intensidad de uso en todos los servicios, con valores actuales superiores a los de principios de la serie.

Gráfico 13: Evolución de los usos declarados de las redes sociales (posibilidad de respuesta múltiple) (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

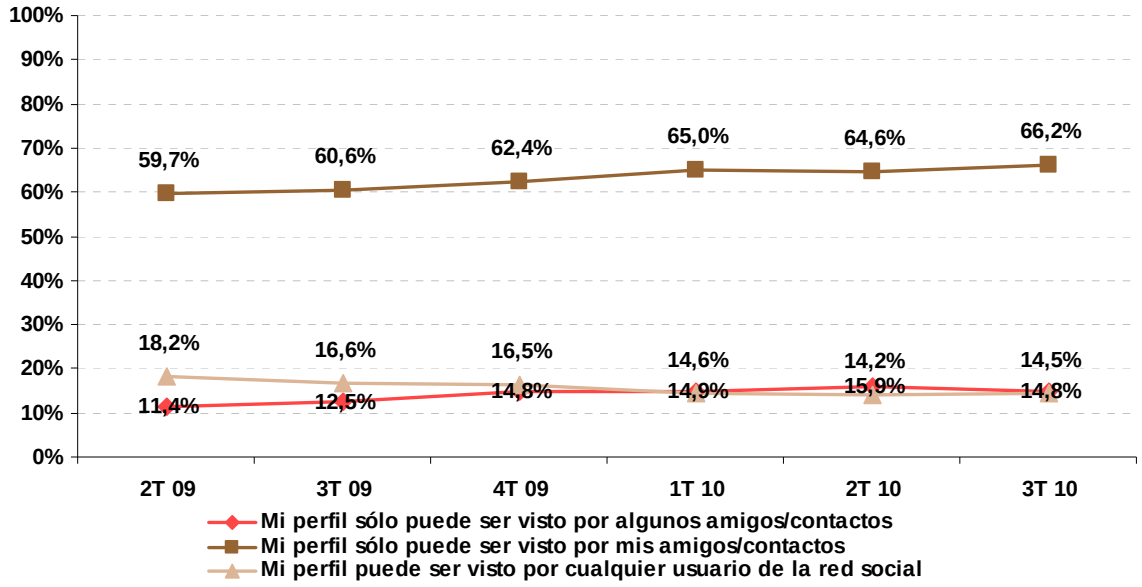
Se realiza a continuación un análisis del nivel de privacidad que cada usuario asigna a sus perfiles de redes sociales:

- Los usuarios de redes sociales cada vez son más cuidadosos con su privacidad, y en este sentido el 66,2% declara que su perfil puede ser visto únicamente por sus amigos o contactos, lo que supone un incremento de 6,5 puntos porcentuales en los últimos 18 meses.

- Un 14,8% muestra todavía mayor prudencia al permitir el acceso al perfil únicamente a algunos amigos o y contactos, dato que también muestra una evolución positiva, desde el 11,4% del 2º trimestre de 2009.

- Por último, una buena noticia es que continúa el descenso en la proporción de usuarios que muestran una actitud imprudente al tener su perfil abierto a cualquier usuario de la red social, aunque con una bajada paulatina, desde el 18,2% en el comienzo de la serie al 14,5% actual.

Gráfico 14: Evolución del nivel de privacidad del perfil del usuario de redes sociales (%)



Base: Usuarios que utilizan redes sociales (n=2.836 en 3T10) *Fuente: INTECO*

3.3 Hábitos de seguridad en hogares con menores

Para analizar la categoría de hábitos de seguridad en hogares con menores se han evaluado una serie de comportamientos que tienen que ver con el fomento de un uso seguro de Internet por parte de los menores. Los datos de este epígrafe se han construido exclusivamente sobre la submuestras de 859 hogares donde vive al menos un menor que accede a Internet.

Se han considerado un total de 11 comportamientos, que se han sistematizado en tres grupos, en función del carácter de la medida:

- Medidas coercitivas y de control.
- Medidas de comunicación, diálogo y educación.
- Implicación del padre en la navegación del hijo.

En general, los hogares con menores que se conectan a Internet presentan un alto compromiso con el cumplimiento de buenos hábitos de seguridad, y los adultos suelen ser conscientes de los peligros de Internet para sus hijos. En los siguientes subepígrafes se profundiza en cada tipo de medida, y se analiza la evolución experimentada desde el primer trimestre de 2009.

3.3.1 Medidas coercitivas y de control

En esta categoría se analizan los siguientes comportamientos:

- *No le dejo que haga una compra en Internet o proporcione datos de cuentas o tarjetas sin un adulto delante*. Esta norma es la más adoptada por los hogares participantes en el estudio, un 91,5%, con un incremento de 13,9 puntos desde el primer trimestre de 2009.

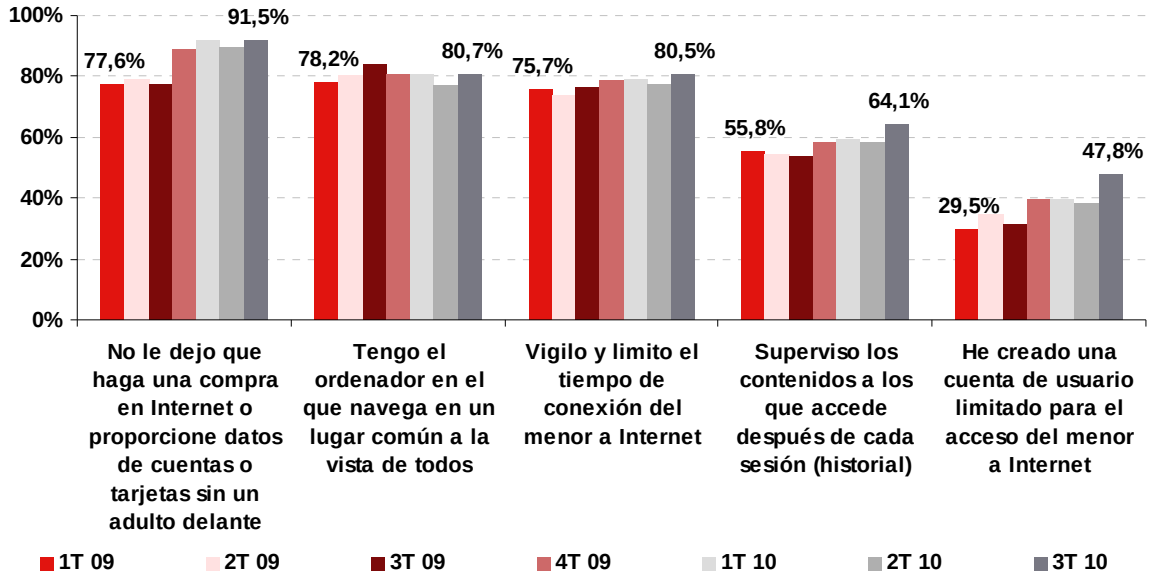
- *Tengo el ordenador en el que navega en un lugar común a la vista de todos*. Esta norma alcanza el 80,7% de adopción declarada en este periodo.

- V*igilo y limito el tiempo de conexión del menor a Internet*. Los padres con hijos menores usuarios de Internet establecen limitaciones a la actividad de sus hijos en la Red cada vez en mayor medida: desde el 75,7% del primer trimestre del 2009 hasta el 80,5% del tercer trimestre de 2010.

- *Superviso los contenidos a los que accede después de cada sesión (historial).* El 64,1% de los adultos realiza esta supervisión sobre los contenidos a los que los menores acceden en la Red. El recelo de los padres a invadir la intimidad de los hijos parece haber descendido, ya que en el primer trimestre de 2009 el nivel de seguimiento de esta medida de control se situaba en el 55,8%.

- *He creado una cuenta de usuario limitado para el acceso del menor a Internet.* Esta medida también ha experimentado un incremento importante en el último trimestre, hasta alcanzar el 47,8%. Se impulsa así la tendencia alcista manifestada desde el inicio del periodo analizado, comienzos de 2009 (29,5%). Este dato resulta muy positivo, puesto que limita el impacto en el equipo de una potencial conducta peligrosa por parte del menor.

Gráfico 15: Evolución de los hábitos relacionados la supervisión de los menores en el uso de Internet manifestados (medidas coercitivas y de control) (%)



Base: Usuarios que viven con hijos menores que se conectan a Internet (n=859 en 3T10) *Fuente: INTECO*

3.3.2 Medidas de comunicación, diálogo y educación

En esta categoría se analizan los siguientes comportamientos:

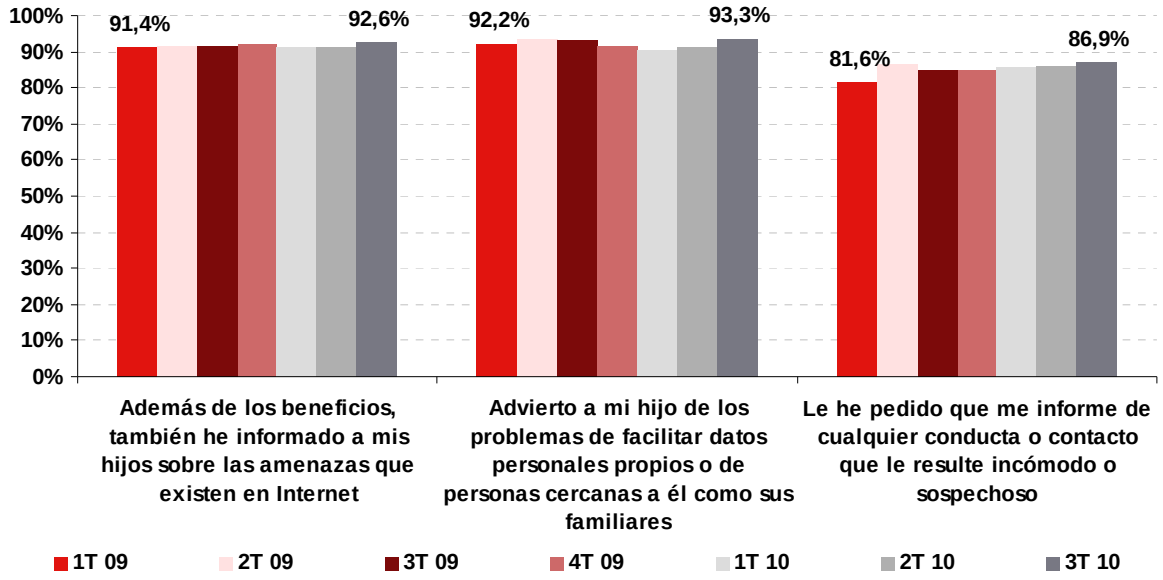
- *Además de los beneficios, también he informado a mis hijos sobre las amenazas que existen en Internet*. El 92,6% de los menores reciben esta advertencia en sus hogares, comportamiento mayoritario y constante a lo largo del tiempo.

- *Advierto a mi hijo de los problemas de facilitar datos personales propios o de personas cercanas a él como sus familiares*. Casi la totalidad de los hogares españoles con menores internautas les aconsejan sobre la importancia de mantener su privacidad en la Red (un 93,3%).

- *Le he pedido que me informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.* Cada vez son más los hogares (86,9%) en los que se pide a los menores que comuniquen al adulto cualquier comportamiento sospechoso que detecten en la Red.

Los hogares españoles con menores que utilizan a Internet se muestran favorables a adoptar medidas de carácter educativo. Como muestra el Gráfico 16, el nivel de adopción de los tres comportamientos analizados es muy elevado (superior al 85% en todos los casos) y se mantiene constante a lo largo del tiempo. Esto da una idea del nivel de diálogo positivo que se establece en los hogares con respecto a la Red y su uso responsable.

Gráfico 16: Evolución de los hábitos relacionados la supervisión de los menores en el uso de Internet manifestados (medidas de comunicación, diálogo y educación) (%)



Base: Usuarios que viven con hijos menores que se conectan a Internet (n=859 en 3T10) *Fuente: INTECO*

3.3.3 Medidas de implicación del padre en la navegación del hijo

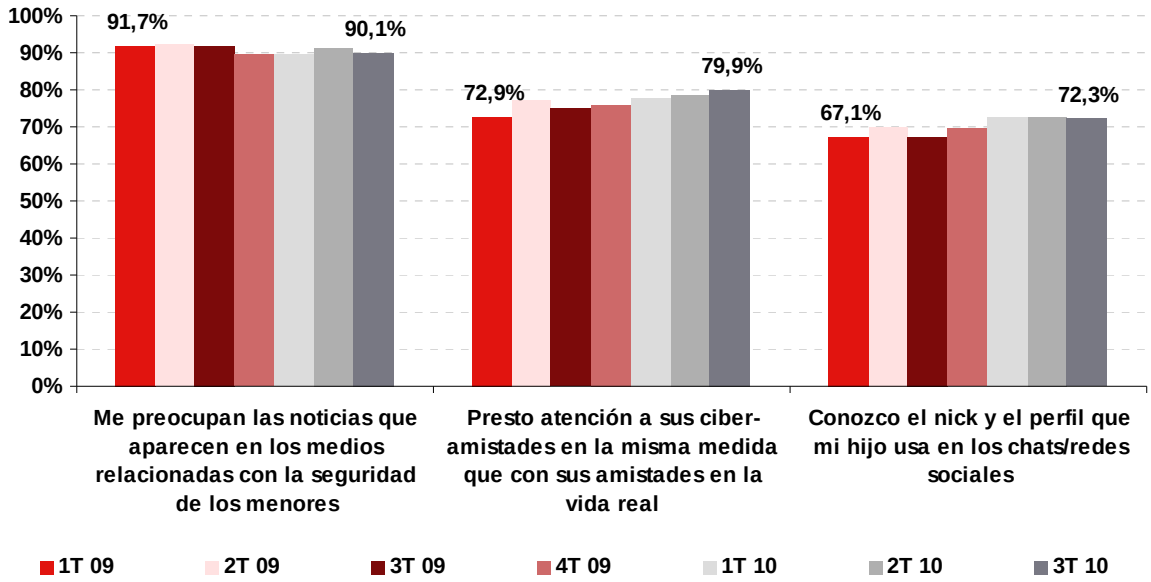
Por último, el Gráfico 17 analiza el nivel de acuerdo del adulto con una serie de afirmaciones, que constituyen indicios de la implicación de los padres en el uso que los hijos hacen de la Red. En concreto:

- *Me preocupan las noticias que aparecen en los medios relacionadas con la seguridad de los menores*. Con el 90,1% de seguimiento, no cabe duda de que a los padres les preocupa el uso que sus hijos hacen de la Red, y están implicados de manera activa en su navegación.

- *Presto atención a sus ciber-amistades en la misma medida que con sus amistades en la vida real*. Esta afirmación alcanza en este trimestre el 79,9%, lo que indica que los padres tratan de conocer las relaciones que sus hijos mantienen en la Red. Esta supervisión puede evitar riesgos relacionados con el contacto con desconocidos.

- *Conozco el nick y el perfil que mi hijo usa en los chats/redes sociales*. Este trimestre, el 72,3% de los padres corroboran este enunciado. Relacionado con el punto anterior, se confirma que los padres son cada vez más proactivos en la supervisión efectiva de los chavales.

Gráfico 17: Evolución de los hábitos relacionados la supervisión de los menores en el uso de Internet manifestados (medidas de implicación del padre en la navegación del hijo) (%)



Base: Usuarios que viven con hijos menores que se conectan a Internet (n=859 en 3T10) *Fuente: INTECO*

En general, los padres adoptan en mayor medida los hábitos relacionados con el diálogo y la educación que los que tienen que ver con las medias restrictivas o de control, intentando respetar la intimidad del menor. Destaca la relevancia que están tomando las amistades en redes sociales y chats, de forma que los adultos cada vez entienden más que este tipo de amistades deben ser supervisadas de la misma forma que lo harían con las amistades en la vida real.

4 INCIDENCIAS DE SEGURIDAD

En la Tabla 4 se muestra el porcentaje de usuarios que han sufrido alguno de los incidentes de seguridad más comunes, en función del momento de su detección.

El incidente más común es, de nuevo, la recepción de correos electrónicos no deseados o spam. En los últimos tres meses ha afectado al 66,9% de los encuestados, según sus propias declaraciones. De acuerdo con los datos empíricos facilitados por las redes de sensores de INTECO, en septiembre de 2010 se detectó que el 77,4% de los correos circulantes era basura. Este dato supone un importante descenso con respecto a trimestres anteriores, en los que el volumen de correos basura facilitados por las redes de sensores de INTECO se movía en valores superiores al 90%. ¿Qué ha provocado este descenso? En este caso, parece existir un origen claro. A mediados de septiembre, las operaciones de spamit.com fueron cerradas. Spamit.com era un grupo conocido que trabajaba con spammers y botnets para proporcionar las infraestructuras y recursos necesarios para gestionar las ganancias de los negocios publicitados. Por tanto, se trataba de un sistema *underground* que, asociado con los spammers, conseguía gestionar los negocios anunciados en correos basura. En concreto spamit.com era responsable de gran parte de los conocidos anuncios de "*Canadian Pharmacy*", esto es, farmacias que venden sin receta y a precios bajos productos como Viagra, Xanax, etc. La desaparición de spamit.com ha hecho que los valores generales de spam durante la segunda mitad de septiembre, descendieran con respecto a los niveles habituales, mientras los atacantes se reabastecían con nuevas infraestructuras.

Los internautas apenas han sufrido la suplantación de identidad (78,7% nunca la ha sufrido) y el robo de ancho de banda en la conexión a Internet (83,0% de usuarios afirma no haber sido víctima).

Sobre la incidencia de malware y otros códigos maliciosos, un 24,1% de los encuestados declara haber alojado malware en el sistema en los últimos 3 meses, mientras que los datos recopilados por iScan elevan al 53,6% el porcentaje de usuarios que efectivamente alojan código malicioso en su equipo en septiembre de 2010. Se profundizará en estos datos en el apartado 4.2.

Tabla 4: Incidencias de seguridad declaradas por los usuarios en función del momento de detección 3T 2010 (%)

Incidencia	DECLARADO				REAL
	Nunca	Alguna vez	Alguna vez (último año)	Alguna vez (últimos 3 meses)	Sep. 10
Recepción de correos electrónicos no deseados	13,1%	6,9%	13,2%	66,9%	77,4%[10]
Virus u otros códigos maliciosos	24,2%	29,5%	22,2%	24,1%	53,6%
Víctima de suplantación de identidad	78,7%	8,5%	6,4%	6,3%	
Robo de ancho de banda en la conexión a Internet (intrusión Wi-Fi)	83,0%	7,0%	6,1%	4,0%	

Base: Total usuarios (n=3.538) *Fuente: INTECO*

4.1 Incidencias de seguridad por malware o código malicioso: conceptos previos

El término malware procede del inglés *malicious software*, y es cualquier software que tiene como objetivo infiltrarse o dañar un ordenador sin el conocimiento de su dueño y con finalidades diversas. A los efectos del estudio, se emplean los términos malware y código o programa malicioso de forma indistinta. En el lenguaje cotidiano se utiliza la expresión genérica "virus informático" para describir todos los tipos de malware, si bien en realidad los virus son una de las múltiples tipologías del malware.

Se describe a continuación la categorización empleada para agrupar las manifestaciones de código malicioso que se analizarán en este epígrafe:

- **Troyanos o caballos de Troya**: se trata de software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador y contaminar a los equipos por medio del engaño. No producen efectos realmente visibles o apreciables en el momento de llegar al equipo. Dentro de los troyanos, a su vez, existen diferentes tipos, en función de los efectos sobre el sistema. En general presentan un nivel de peligrosidad alta. Ejemplos de clases de troyanos:
    - Bankers o troyanos bancarios: realizan 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 captadores de formularios de

[10] Este dato procede de la red de sensores de INTECO, y refleja el porcentaje de spam detectado entre el 1 y el 30 de septiembre de 2010. Datos disponibles en: https://ersi.inteco.es/index.php?option=com_sanetajax&Itemid=55&lang=es

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 su objetivo se centra en el fraude.

- Backdoors o puertas traseras: permite al atacante tomar el control remoto del sistema infectado, pudiendo llevar a cabo diversas acciones (espiar el escritorio remoto, realizar capturas de pantalla o de la webcam, subir o descargar archivos, alterar el funcionamiento normal del sistema, etc.).

- Keyloggers o capturadores de pulsaciones: tienen 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. En definitiva, se trata de una variedad que también se centra en el fraude.

- 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), por eso se trata de una categoría infrecuente.

- Rogueware: el Rogueware o rogue software es un tipo de malware cuya principal finalidad es hacer creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto del pago suele ser la compra de un falso antivirus, que resulta en realidad el malware en sí. En los últimos tiempos, este tipo de malware está siendo muy difundido y se están detectando gran cantidad de variantes.

- **Adware o software publicitario**: muestra anuncios publicitarios que aparecen inesperadamente en el equipo cuando se está utilizando la conexión a una página web o después de que se ha instalado en la memoria de la computadora. En ocasiones recopilan información sobre los hábitos de navegación de los usuarios para luego redirigirles a la publicidad coincidente con sus intereses.

- **Herramientas de intrusión**: 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.

- **Gusano o worm**: 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 no necesitan otro archivo para replicarse. Pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar.

- **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 qué 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 del sistema a Internet y afecta negativamente a la velocidad del resto de servicios que el usuario esté utilizando.

- **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.

- **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 puedan producir falsos positivos.

- **Otros**: se incluyen dentro de esta categoría las siguientes:

    - **Exploit**: 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 perciba de ello y actuar con libertad dentro del sistema atacado.

- **Rootkits**: son programas insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante.

- **Scripts**: 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.

- **Jokes o bromas:** alteran el normal funcionamiento del equipo con acciones que molestan o distraen al usuario, si bien no causan daño alguno al sistema.

4.2 Incidencias detectadas

Este apartado está construido íntegramente a partir de los datos reales obtenidos del escaneo de los equipos de los panelistas gracias a la herramienta iScan desarrollada por INTECO. Una explicación más detallada de la herramienta se encuentra disponible en el *Anexo I: Diseño metodológico detallado*.

4.2.1 Evolución de las incidencias de malware

El Gráfico 18 muestra conjuntamente los datos procedentes de los escaneos de los equipos con iScan (línea roja) con la información procedente de las encuestas trimestrales (columnas rosas).

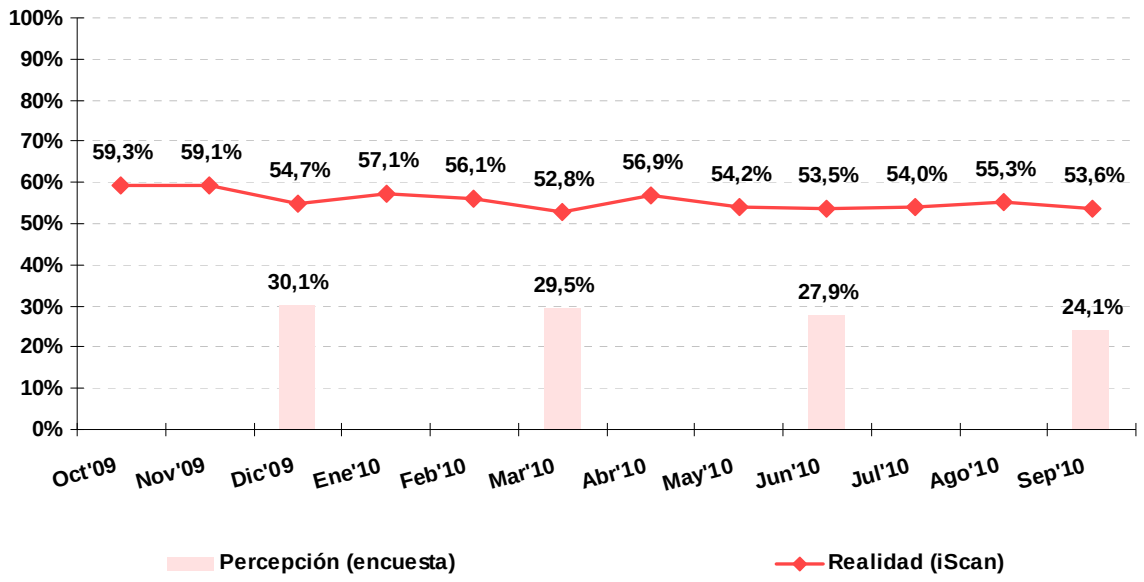
En septiembre de 2010, un 24,1% de los usuarios declaran haber sufrido malware en los últimos tres meses, un valor que encuentra su mínimo histórico con respecto a datos de trimestres anteriores. El dato real recopilado por la herramienta iScan, sin embargo, no refleja este descenso. El 53,6% de los equipos auditados alojan malware en septiembre de 2010, un dato que se mantiene estable en los últimos meses.

¿A qué puede deberse ese descenso de la percepción de los usuarios con respecto a las incidencias de malware? Una de las formas más claras por las que un usuario puede percibir que ha sido infectado por algún tipo de código malicioso es la detección por parte de su antivirus de este código, y el envío de una alerta. Cuando el antivirus reconoce el malware, alerta al usuario y este percibe la infección. Si la percepción del usuario ha descendido, es posible que la razón se deba a que no han sido alertados por su antivirus. Sin embargo, la realidad indica que sí que existe infección: un análisis real y mucho más exhaustivo (realizado con más motores) sobre el sistema indica que los niveles de infección siguen en unos niveles similares a trimestres anteriores. Entonces, la conclusión no es que se hayan producido menos infecciones, sino que la brecha entre percepción y realidad se ha abierto aun más (en torno a 30 puntos porcentuales). El problema, por

tanto, puede ser achacable a una pobre detección por parte de los antivirus, que no han alertado al usuario y, por tanto, no han percibido una infección que se ha demostrado real.

También es posible que el usuario aloje malware no activo en su sistema. De esta forma no sería alertado por su antivirus, pero sí por iScan.

Gráfico 18: Evolución de equipos que alojan malware (%)

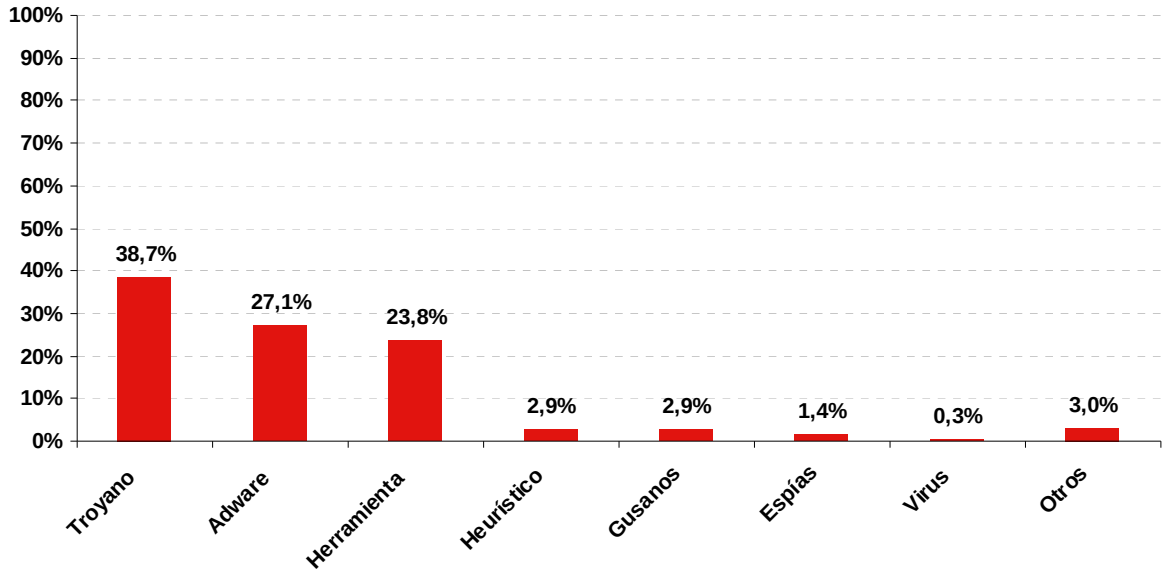


Percepción = declaran haber sufrido malware en los últimos 3 meses *Fuente: INTECO*

4.2.2 Tipología del código malicioso detectado

Este trimestre vuelve a dominar el troyano como tipo de código más detectado en septiembre, con un 38,7% de equipos que alojaban malware de esta categoría. Por detrás del tipo troyano se encontraría, una vez más, el adware (27,1%).

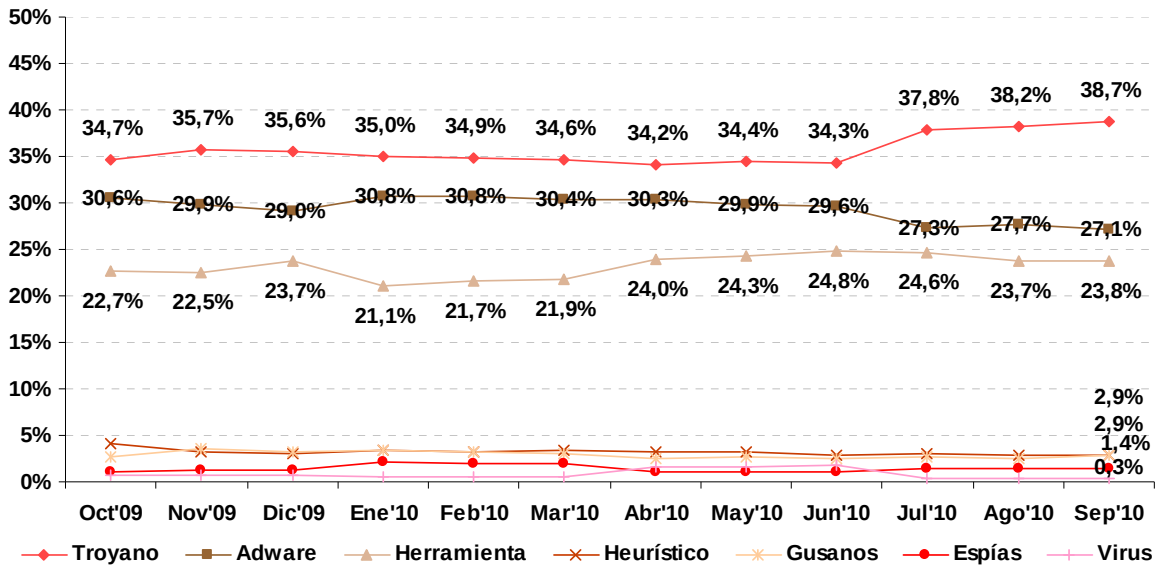
Gráfico 19: Equipos que alojan malware según tipología de código malicioso en sep. 10 (%)



Fuente: INTECO

En el Gráfico 20 se muestra la evolución de estos valores. El tipo troyano continúa indiscutiblemente al alza como el tipo de malware más detectado. El adware publicitario, aunque muy presente (27,1% en septiembre) va perdiendo fuerza con respecto a lecturas de principios de 2010. El resto de tipos de malware (virus, gusanos, espías y otros) continúan con valores residuales y estables inferiores al 3%.

Gráfico 20: Evolución de equipos que alojan malware según tipología (%)

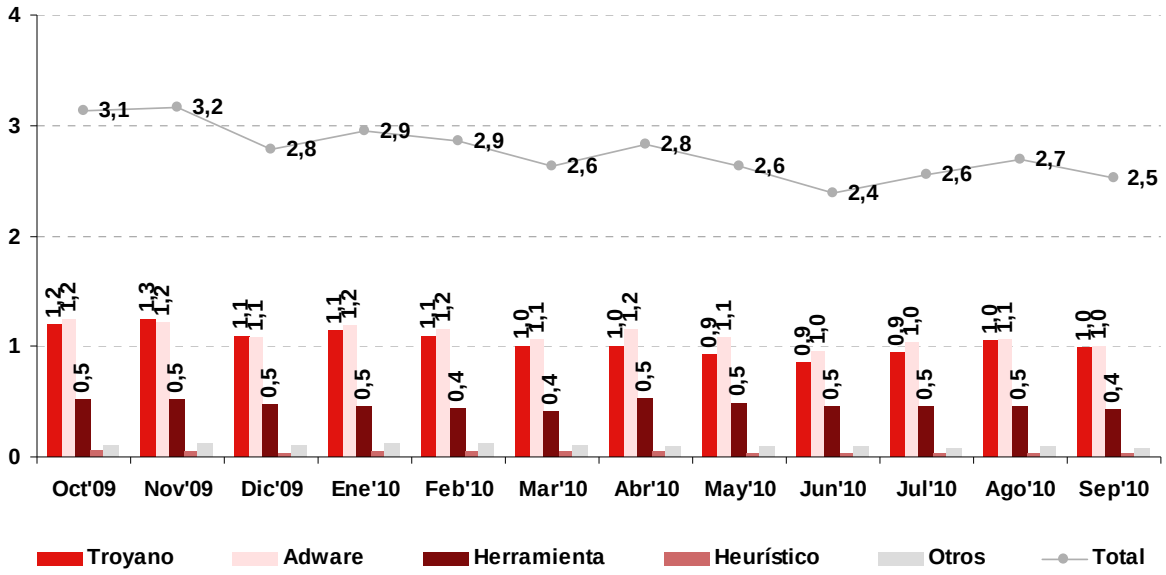


Fuente: INTECO

En el siguiente gráfico se analiza la media de archivos infectados por equipo, clasificados por tipología. En total, en el mes de septiembre se detectan 2,5 archivos maliciosos por equipo.

En los meses de agosto y septiembre, se vuelve a alcanzar la media de 1 troyano por ordenador, tras el descenso ocurrido en mayo, junio y julio, donde por primera vez se detectaron menos de 1 troyanos por máquina (0,9 de media).

Gráfico 21: Evolución del número medio de archivos maliciosos por equipo



Fuente: INTECO

4.2.3 Diversificación del código malicioso detectado

Para los atacantes, es importante diversificar su código. Con ello pretenden pasar desapercibidos no solo para los antivirus, sino para los detectores de intrusos y otras herramientas de seguridad.

Variantes únicas de malware

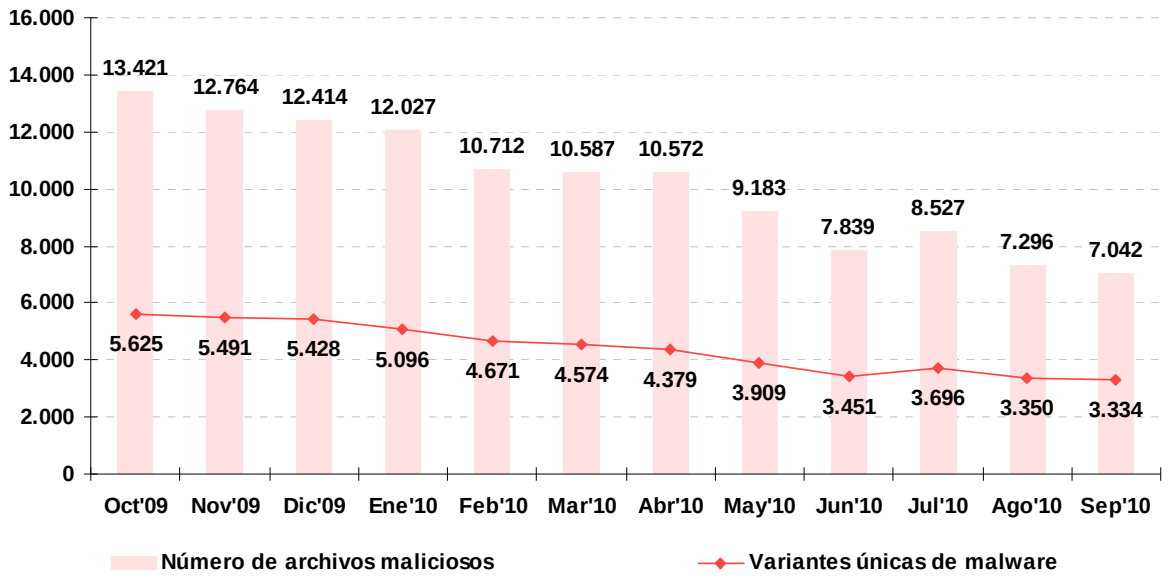
En el siguiente gráfico se analiza este comportamiento. Las barras rosas analizan la evolución mensual, en números absolutos, de archivos infectados. La línea roja representa el total de variantes diferentes que representan.

En junio se observa un descenso del número total de de archivos infectados, mientras que en julio vuelve a remontar sustancialmente hasta los 8.527. En agosto y septiembre retrocede de nuevo el volumen de archivos comprometidos, alcanzando valores ciertamente bajos. Este comportamiento puede estar explicado parcialmente por el menor número de máquinas analizadazas. En este tercer trimestre, se han escaneado 3.337 equipos en julio, pero solo 2.716 en septiembre y 2.783 en septiembre (ver

Tabla 9), lo que significa una muestra ligeramente menor a lo que viene siendo habitual en períodos anteriores.

Se observa, sin embargo, cierta estabilidad en el número de variantes únicas de malware encontradas cada mes, en torno a los 3.500 desde junio de 2010. Esto significa que el nivel de diversificación del código malicioso es elevado. Así, poniendo en relación ambos datos (7.042 archivos maliciosos entre 3.334 variantes únicas), cada variante única detectada se avistaría sólo 2 veces de media en septiembre de 2010.

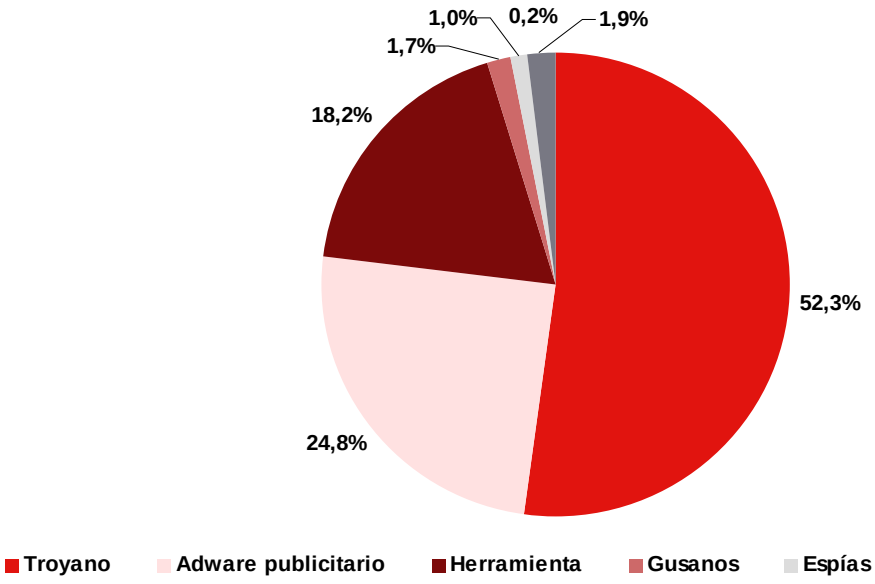
Gráfico 22: Evolución del número total de archivos maliciosos y variantes únicas de malware



Fuente: INTECO

La diversificación se observa sobre todo, como indica el Gráfico 23, en la categoría de troyanos, categoría donde se encuadran el 52,3% de las variantes únicas encontradas en septiembre de 2010. Los troyanos (en su mayoría destinados al robo de información, principalmente de carácter bancario) siguen siendo el tipo preferido para los atacantes por el lucro que les podría llegar a proporcionar.

Gráfico 23: Categorías de código malicioso de las variantes únicas, septiembre 2010 (%)

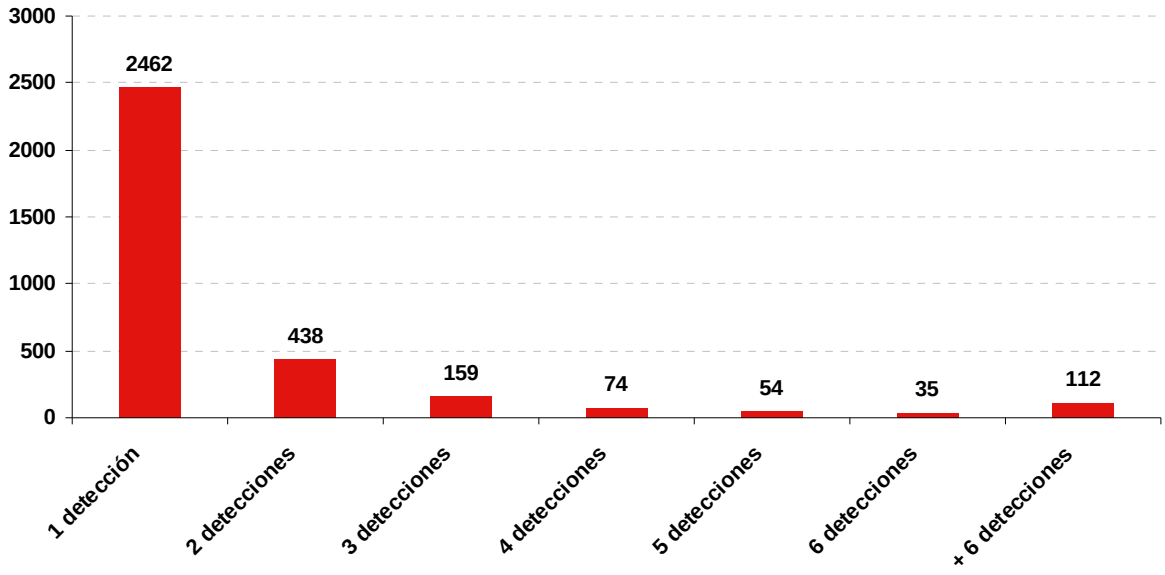


Fuente: INTECO

Número de detecciones de las variantes únicas

En septiembre de 2010, de las 3.334 variantes únicas detectadas, 2.462 se manifestaron solo una vez. Se sigue confirmando la tendencia a que, en cada equipo, convivan variantes únicas que no son muy avistadas dentro de otros sistemas.

Gráfico 24: Número de detecciones de cada variante única de malware, septiembre 2010



Fuente: INTECO

4.2.4 Peligrosidad del código malicioso y riesgo del equipo

Definición del nivel de peligrosidad del código malicioso

Se han definido tres categorías de riesgo de las variantes de malware detectadas: alto, medio y bajo. En la asignación de cada variante a uno u otro grupo se ha seguido el siguiente criterio:

- **Riesgo alto**: se incluyen en esta categoría los especímenes que, potencialmente, permiten el acceso remoto por parte de un atacante al sistema víctima; pueden suponer un perjuicio económico para el usuario; facilitan la captura de información confidencial o sensible de la víctima; se emplean como pasarelas para atacar otros equipos (pudiendo acarrear consecuencias legales para la víctima) y minan el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.

  En base a este criterio, se asimilan a variantes de malware de riesgo alto los troyanos, dialers (marcadores telefónicos), keyloggers (registradores de pulsaciones de teclado), virus, gusanos, rootkits y exploits.

- **Riesgo medio**: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema, no perjudican de forma notoria su rendimiento: abren ventanas no deseadas al navegar; incrustan publicidad en páginas web legítimas que realmente no contienen publicidad; facilitan la captura de información no sensible de la víctima (por ejemplo, patrones de navegación para crear perfiles de publicidad dirigida, etc.).

  Las categorías consideradas son: adware (software publicitario no deseado), spyware (programas espía), scripts[11], así como las detecciones heurísticas.

- **Riesgo bajo**: aquí se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, etc.). En la mayoría de los casos son herramientas instaladas por el usuario de forma intencionada, para listar y matar procesos, o conectarse remotamente a su equipo, etc. Por otra parte, también se consideran especímenes de riesgo bajo los típicos programas broma (por ejemplo aquellos que despliegan una ventana que se va moviendo y resulta imposible cerrarla con el ratón) y los virus exclusivos para plataformas móviles pues estos no son capaces de ejecutarse sobre los equipos de los usuarios.

[11] Las secuencias de comandos maliciosos (scripts) pueden representar riesgo alto en determinados casos.

A los efectos del estudio, se consideran como malware de bajo nivel de riesgo las herramientas de intrusión[12], bromas y malware alojado en los ordenadores pero orientado a otros dispositivos (móviles, PDA's).

Se trata de una clasificación genérica y, por tanto, sujeta a un margen de error[13]. El sesgo puede proceder no sólo de la necesaria generalización en categorías, sino también del entorno en donde se encuentre el archivo malicioso. Por ejemplo, un dialer o marcador telefónico será en realidad de riesgo nulo para un equipo que no posee un modem convencional para red telefónica básica ya que por regla general los routers ADSL no tienen la posibilidad de hacer llamadas; sin embargo, en la clasificación empleada en el estudio se está considerando a los dialers como de riesgo alto, por su potencial impacto económico sobre la víctima.

Nivel de riesgo de los equipos

El análisis que aquí se presenta se efectúa sobre los equipos, y no sobre el código malicioso en sí mismo. Se intenta clasificar aquí lo arriesgado de usar un equipo infectado por las clasificaciones anteriormente expuestas. Las categorías de malware más sofisticadas suponen un riesgo mayor.

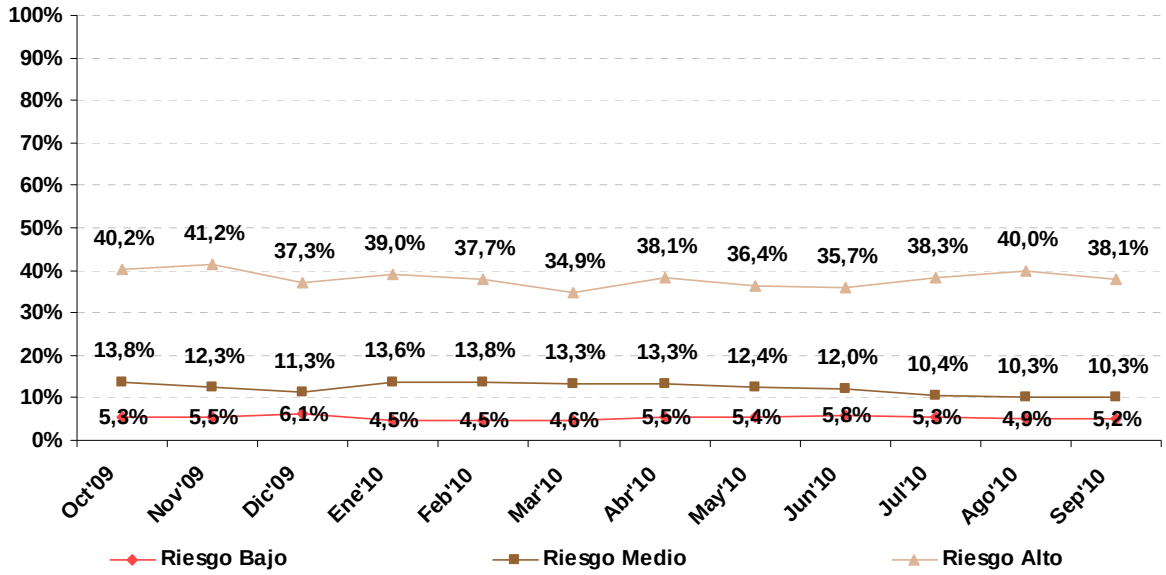
Un equipo infectado con troyano y adware estará incluido en el grupo de riesgo alto (troyano), y no en el medio (adware).

En septiembre de 2010, un 38,1% de los equipos son considerados de riesgo alto, frente a un 10,3% de riesgo medio y un 5,2% de riesgo bajo. Se confirma la progresiva reducción de los niveles de riesgo de los equipos a lo largo del último año, sobre todo, en el caso de riesgo medio. En concreto en el mes de septiembre, quizás motivado por el menor número de análisis realizados, se observa también un ligero descenso del porcentaje de equipos con riesgo alto.

[12] 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. 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.

[13] La determinación del riesgo de las muestras mediante análisis manual de las variantes, si bien más rigurosa, sería en exceso lenta y costosa. Considerando que las propiedades de las distintas categorías del malware estudiado siguen una distribución gaussiana, la desviación global de la adopción de un enfoque genérico es despreciable en términos estadísticos.

Gráfico 25: Evolución del nivel de riesgo de los equipos (%)



Fuente: INTECO

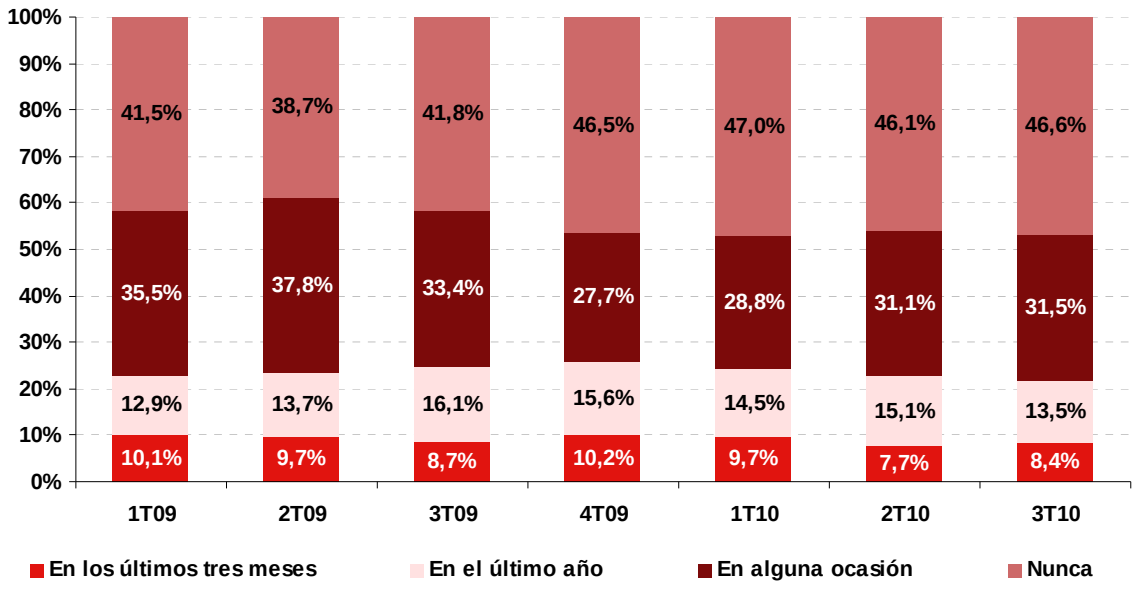
5 CONSECUENCIAS DE LAS INCIDENCIAS DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS ANTE ELLAS

5.1 Consecuencias de las incidencias de seguridad

En este epígrafe se analizan las consecuencias materiales que sufren los usuarios, como consecuencia de las incidencias de seguridad sufridas.

En primer lugar, el Gráfico 26 muestra la evolución de la pérdida de información como consecuencia de alguna incidencia de seguridad. Los valores se mantienen relativamente estables con respecto a trimestres anteriores. El 46,6% de los encuestados afirma que nunca ha sufrido una pérdida de datos, frente al 53,4% que sí ha experimentado una situación así en algún momento; de éstos, un 8,4% lo ha hecho en los últimos tres meses.

Gráfico 26: Evolución de las consecuencias de las incidencias de seguridad: pérdida de datos (%)

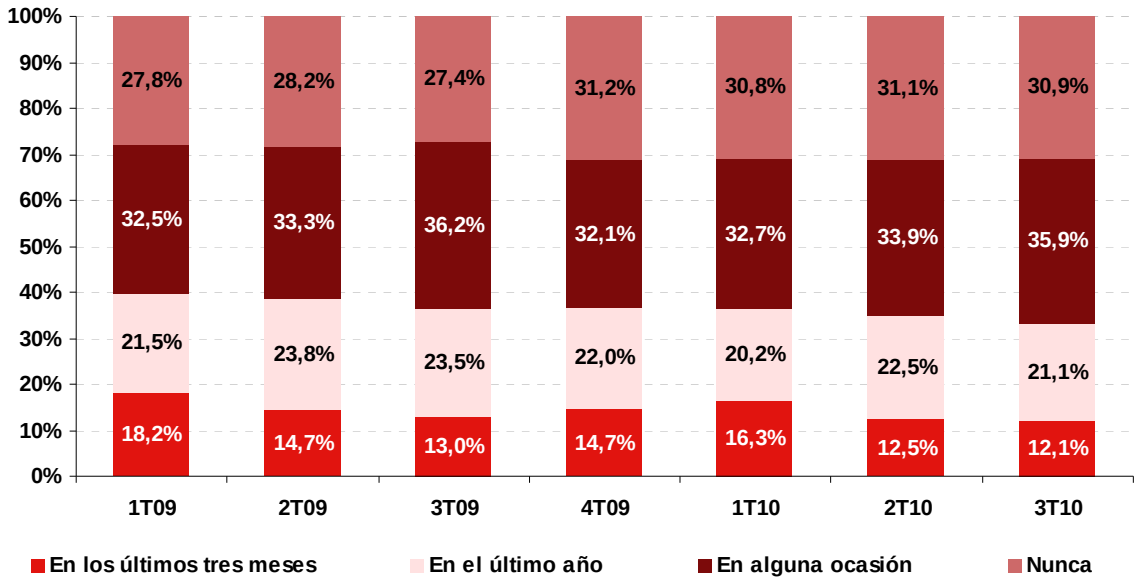


Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

El siguiente gráfico muestra la evolución de la reinstalación del sistema operativo como consecuencia de alguna incidencia de seguridad. De las tres consecuencias de las incidencias analizadas, ésta es la que se da con mayor frecuencia. Un 69,1% afirma haber sufrido esta experiencia en alguna ocasión. Concretamente un 12,1% de estos lo ha tenido que hacer en el último trimestre, un 21,1% en el último año y un 35,9% en alguna ocasión.

Hay que tener en cuenta que la reinstalación del sistema operativo no siempre puede solucionar los problemas ocasionados por el malware. Algunos tipos de rootkits consiguen manipular el Master Boot Record (MBR). Esta es la primera zona del disco duro que lee el ordenador para encontrar el sistema operativo y comenzar el arranque. En esa zona, ciertos malware consiguen introducir código que modificará por completo (troyanizará) el comportamiento del sistema operativo, de forma que podría pasar desapercibido. Si durante el formateo no se elimina además el MBR con las herramientas adecuadas (por ejemplo si se reparticiona el disco duro), el malware podría sobrevivir en el equipo.

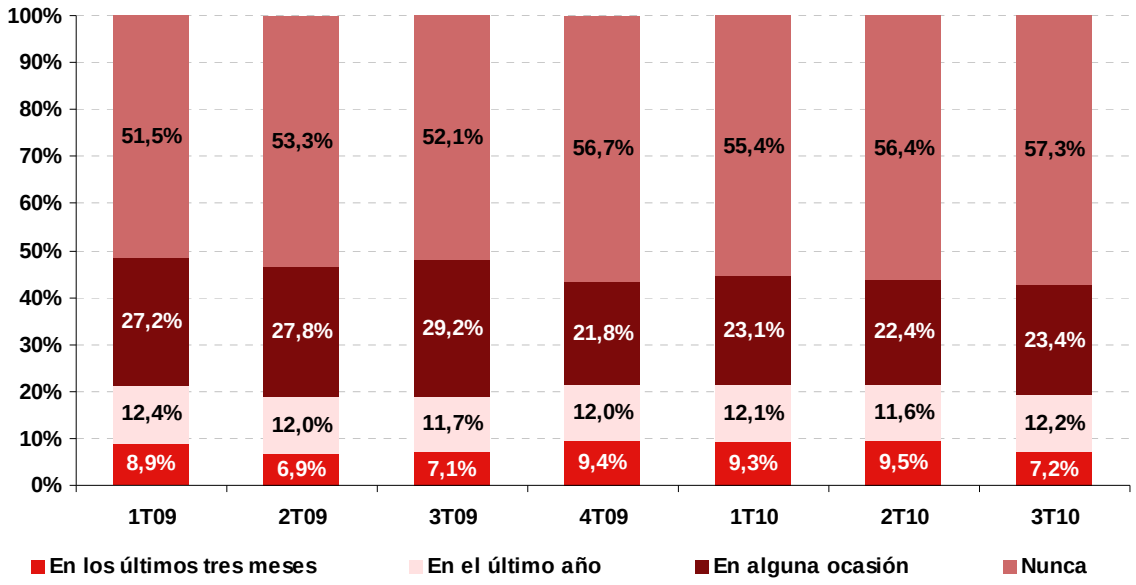
Gráfico 27: Evolución de las consecuencias de las incidencias de seguridad: formateo y reinstalación del SO (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

Sufrir daños en el hardware es la consecuencia que, globalmente, se da con menor frecuencia, tal y como confirma el Gráfico 28. Un 57,3% admite no haberlo sufrido nunca.

Gráfico 28: Evolución de las consecuencias de las incidencias de seguridad: daños en el hardware (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

5.2 Cambios adoptados tras una incidencia de seguridad

El 60,6% de los usuarios no ha realizado ningún cambio en sus hábitos de navegación por Internet como resultado de una incidencia vivida, frente a un 39,4% que sí ha adoptado algunas medidas de precaución.

En el siguiente epígrafe centramos la atención sobre este segundo grupo. En concreto se analiza cómo afecta esta experiencia al usuario en cuanto a cambios en sus hábitos y medidas de seguridad y en cuanto a cambios en el uso de los servicios de Internet.

5.2.1 Cambios en las medidas o herramientas de seguridad

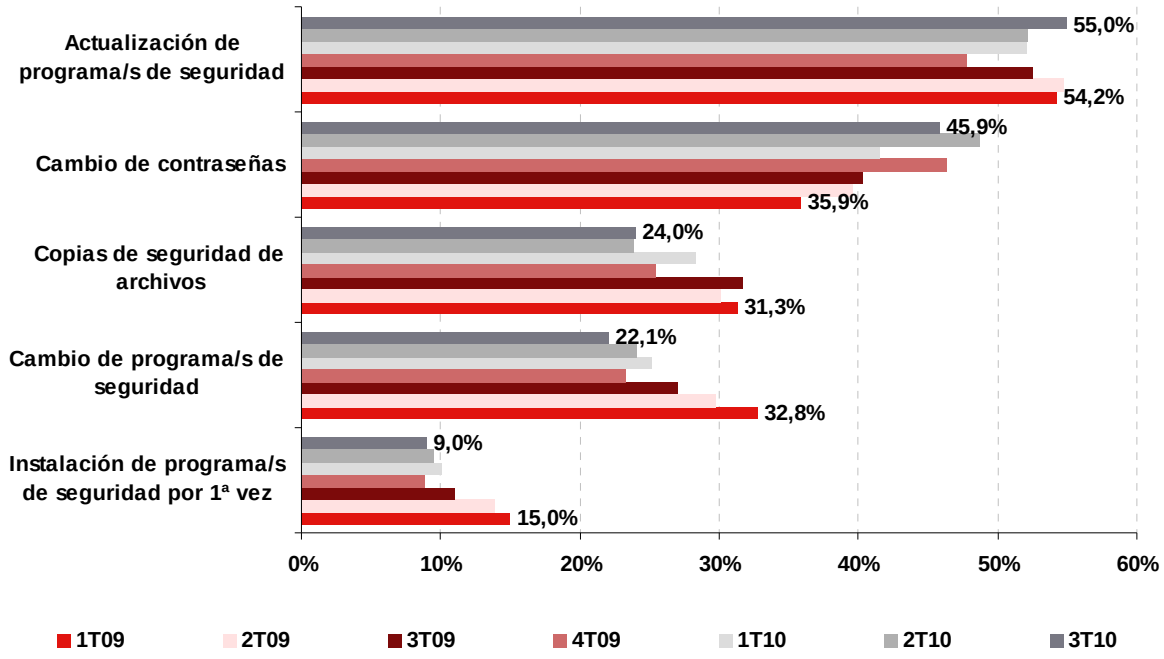
Los cambios que llevan a cabo los usuarios en sus hábitos de seguridad tras haber experimentado una incidencia son de carácter preventivo, como el refuerzo o la instalación de determinadas medidas de seguridad, mientras que con una frecuencia muy baja se producen abandonos en el uso de servicios.

Entre las reacciones dirigidas al refuerzo o la instalación de medidas de seguridad, las acciones más habituales de los usuarios son actualizar los programas de seguridad (que sube tres puntos desde el trimestre pasado, desde el 52,1% al 55%) y cambiar las contraseñas (que ha descendido del 48,7% al 45,9% en esta oleada).

En un segundo plano, otras medidas también adoptadas para aumentar la protección son el cambio de las herramientas de seguridad (22,1%), la realización de copias de

seguridad de los archivos (24%) y la instalación por primera vez de programas de seguridad (9%).

Gráfico 29: Evolución de las reacciones adoptadas tras sufrir un incidente de seguridad: cambio en las medidas y herramientas de seguridad (%)



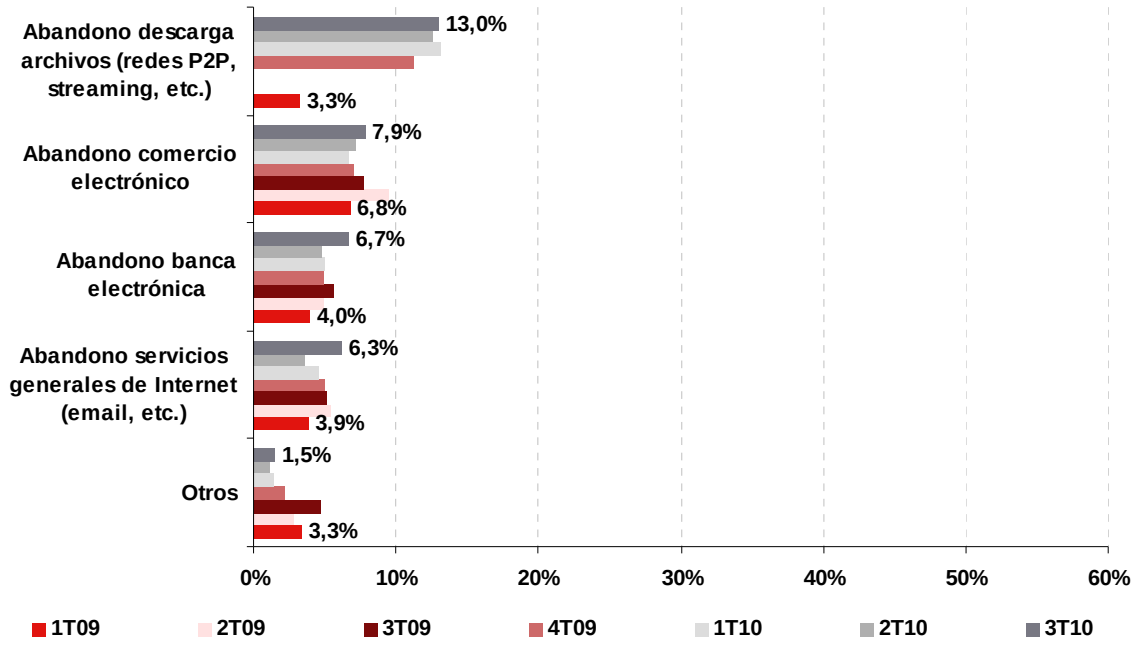
Base: Usuarios que adoptan cambio tras un incidente de seguridad (n=1.350 en 3T10) *Fuente: INTECO*

5.2.2 Cambios en el uso de servicios de Internet

En el Gráfico 30 se analizan las reacciones relacionadas con el uso de servicios online. Los cambios que implican un abandono de la utilización de servicios de Internet no son frecuentes, tomando esta decisión un porcentaje muy reducido de la población.

El servicio en el que más bajas de uso se producen, según declaran los usuarios, es la descarga de archivos mediante redes P2P, con una incidencia del 13%. En el resto de servicios la tasa de abandono es aún bastante menor, aunque en este tercer trimestre se ha incrementado en 3 puntos el porcentaje de usuarios que han abandonado el uso de servicios generales de Internet como email, mensajería instantánea, redes sociales... pasando del 3,6% que declaró ese abandono en el trimestre anterior al 6,3% de esta ocasión.

Gráfico 30: Evolución de las reacciones adoptadas tras sufrir un incidente de seguridad: cambio en el uso de los servicios de Internet (%)



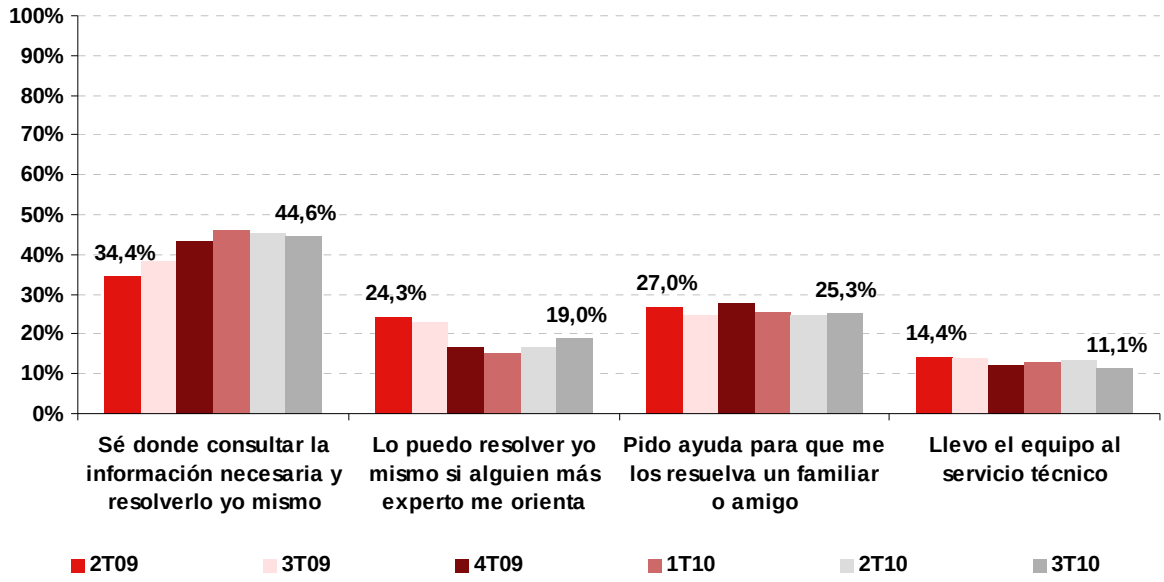
Base: Usuarios que adoptan cambio tras un incidente de seguridad (n=1.350 en 3T10) *Fuente: INTECO*

5.3 Resolución de incidentes de seguridad

En cuanto a la forma de resolver los problemas de seguridad que afectan a los ordenadores, buena parte de los encuestados declara que lo hacen de manera autónoma. Casi la mitad de los usuarios (44,6%) afirma que se ocupa él mismo sin la ayuda de nadie y un 19% lo hace con la orientación de alguien más experto para solucionarlos.

El otro tercio restante depende de alguien para solventar estos problemas; un 25,3% acude a personas de su entorno y un 11,1% recurre directamente a un servicio técnico.

Gráfico 31: Evolución de la forma de resolución de las incidencias de seguridad (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

6 e-CONFIANZA DE LOS HOGARES ESPAÑOLES

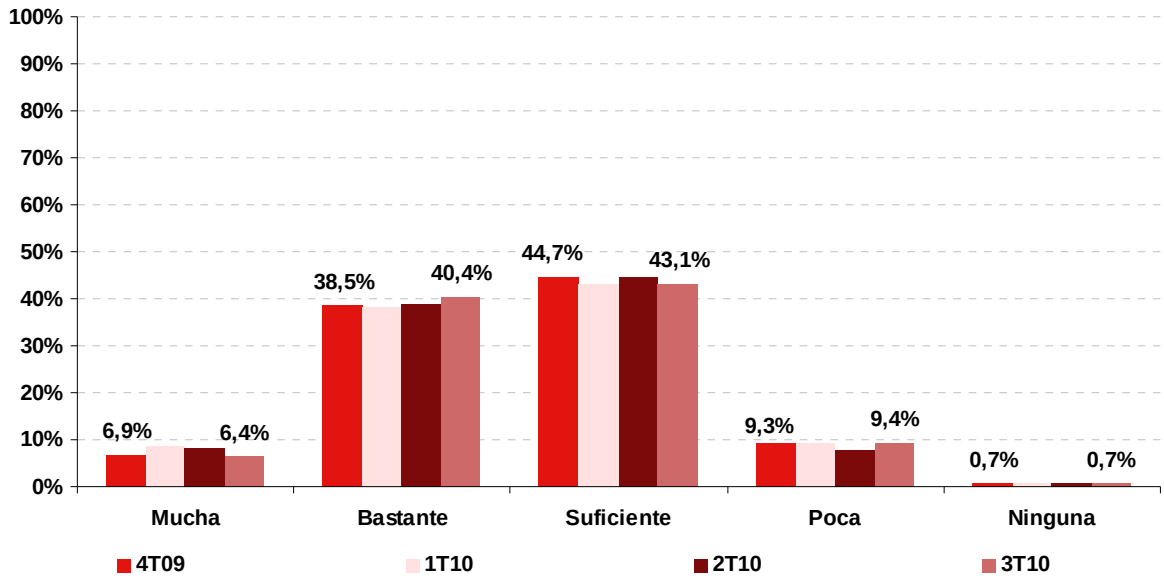
La confianza es un elemento clave para el desarrollo la Sociedad de la Información. Este capítulo analiza, desde distintas perspectivas, la confianza que les proporciona a los usuarios españoles el uso de Internet.

Para ello, además de contar con la valoración de la confianza en la realización de determinadas actividades a través de este medio, se analiza la percepción de los usuarios respecto a la situación de seguridad en Internet y su opinión sobre quiénes deben asumir principalmente esta responsabilidad. Además, se identifican las actuaciones que se consideran prioritarias para mejorar la situación de seguridad, y los riesgos percibidos como consecuencia del uso de Internet.

6.1 e-Confianza en la Sociedad de la Información

La mayoría de los internautas españoles confían en Internet (89,9%). De ellos, un 40,4% reconocen tener bastante confianza en la Red, frente a un 6,4% que admiten depositar mucha y un 43,1% adicional que muestra un nivel de confianza suficiente.

Gráfico 32: En general, ¿cuánta confianza le genera Internet? (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

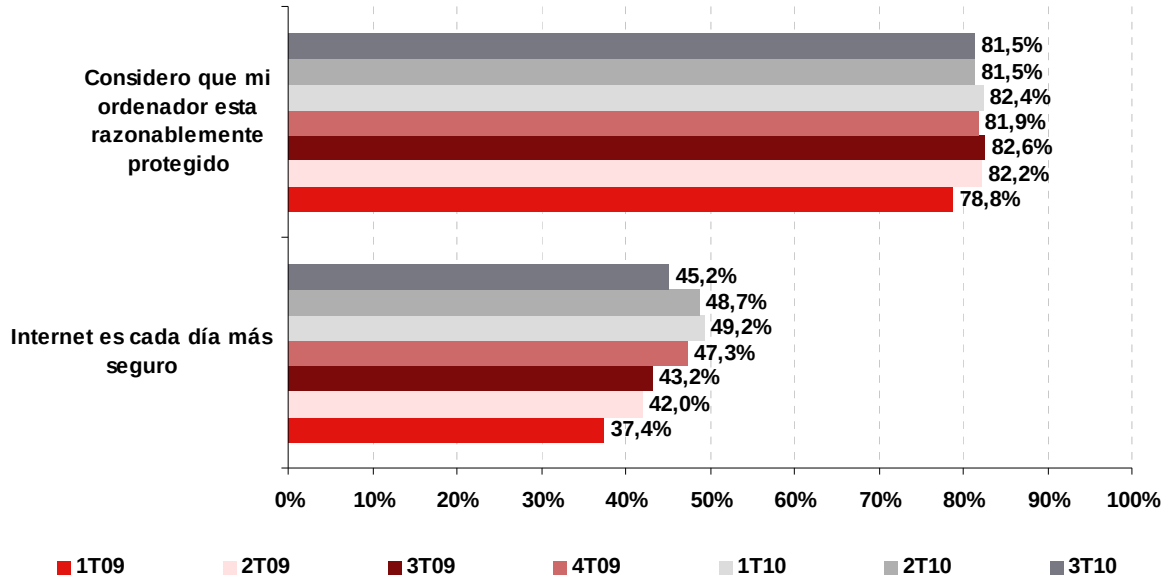
Se ha planteado al encuestado que muestre su grado de acuerdo o desacuerdo con las siguientes dos afirmaciones (los resultados se reflejan en el Gráfico 33):

- *Considero que mi ordenador está razonablemente protegido*. Un 81,5% de los ciudadanos encuestados se muestran de acuerdo con esta afirmación.

- *Internet es cada día más seguro*. En este caso, el 45,2% lo declaran.

En ambos casos, los datos del último año indican una evolución estable.

Gráfico 33: Evolución del porcentaje de usuarios que se muestran totalmente de acuerdo y de acuerdo con... (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

Se analiza a continuación la confianza que los usuarios de Internet españoles tienen depositada en la realización de actividades online, en comparación con la que les genera la misma actividad en el entorno físico.

En concreto, se ofrece un diagnóstico de la confianza en la realización de operaciones bancarias (Gráfico 34), pagos y transacciones de compraventa (Gráfico 35) y actividades que implican el intercambio de datos de carácter personal (Gráfico 36).

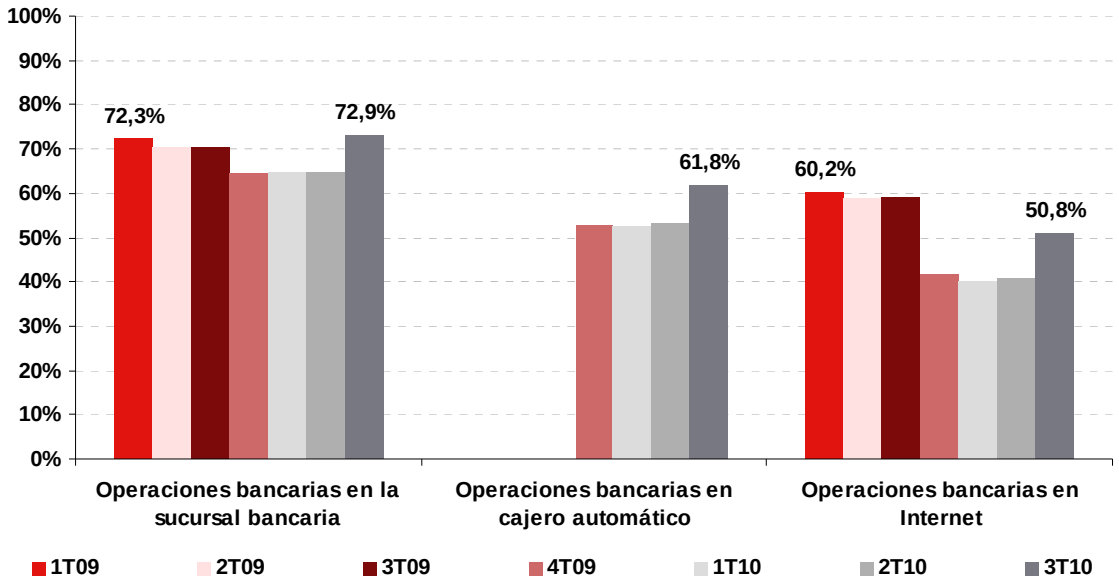
Realizar operaciones bancarias genera cada vez más confianza en los usuarios españoles. Una vez más, las operaciones realizadas en sucursales físicas despiertan mayor tranquilidad que aquellas llevadas a cabo en cajero automático y a través de Internet:

- La realización de operaciones en la sucursal bancaria genera mucha y bastante confianza a un 72,9% de los encuestados.

- A un 61,8% las operaciones efectuadas en cajero automático le ofrecen mucha y bastante confianza.

- Las operaciones bancarias por Internet, aunque con un menor porcentaje, ofrecen mucha y bastante confianza a un importante 50,8% de los encuestados.

Gráfico 34: Evolución del porcentaje de usuarios que confían mucho y bastante en la realización de actividades físicas / online relacionadas con operaciones bancarias (%)



Base: Total usuarios (n=3.538) *Fuente: INTECO*

Con respecto a la realización de compraventas o transacciones de carácter económico, en el siguiente gráfico se puede comprobar el contraste entre la confianza que el ciudadano deposita en llevar a cabo estas actividades en el mundo físico o hacerlo en el entorno virtual.

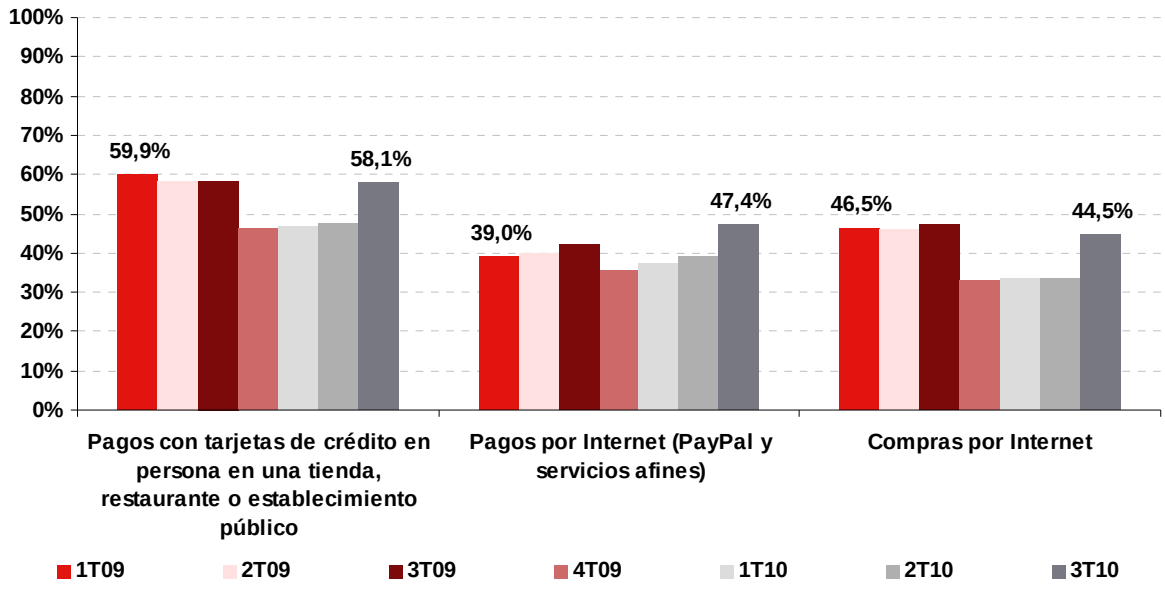
También en este caso el pago con tarjeta en un establecimiento físico ofrece mayor seguridad y confianza a los encuestados que si el pago se realiza en la Red.

- Los pagos con tarjeta de crédito en persona en el punto de venta generan mucha y bastante confianza al 58,1% de los encuestados.

- Este porcentaje es algo menor (47,4%) en el caso de realizar el abono a través de servicios de pago seguros en Internet (como por ejemplo, PayPal).

- El 44,5% de los usuarios se sienten muy confiados a la hora de realizar compras en Internet. En los últimos años, ventajas como la mayor diversidad de artículos o la no limitación de horarios han contribuido a la preferencia por las compras online.

Gráfico 35: Evolución del porcentaje de usuarios que confían mucho y bastante en la realización de actividades físicas / online relacionadas con pagos y transacciones de compraventa (%)



Base: Total usuarios (n=3.538) *Fuente: INTECO*

El contexto físico también genera mayor confianza en el usuario en el caso de la realización de operaciones que impliquen el intercambio de datos personales:

- Proporcionar información personal en un organismo físico de carácter público es la operación que más confianza genera en los usuarios (mucha y bastante), con un 68,4% de encuestados que así lo declaran.

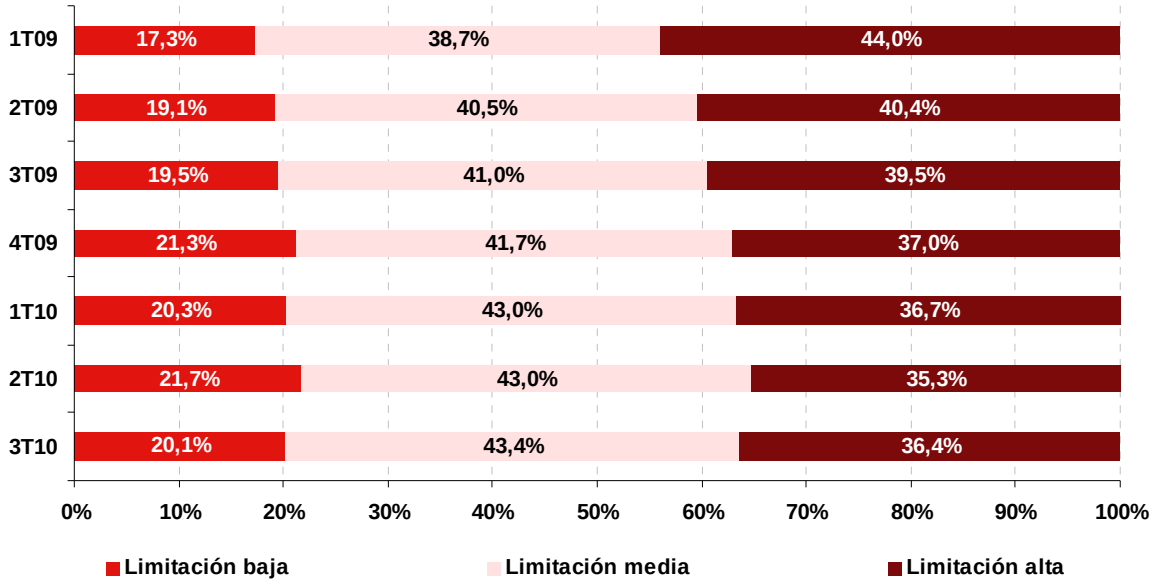
- Este intercambio de datos personales en un establecimiento también físico, pero de carácter privado (tienda, banco, etc.), genera mucha y bastante confianza al 54,2%.

- En servicios online, proporcionar datos de carácter personal genera menos confianza que en los casos anteriores: el 43,1% se siente muy confiado.

- Por último, dar información personal a través de correos o mensajería instantánea (servicios como la red Msn de Microsoft o ICQ) es lo que menos confianza ofrece a los usuarios: en concreto, declaran que poca o ninguna un 43,1%, dato positivo en cuanto a que los usuarios son conscientes de la importancia de proteger la privacidad de sus datos personales en Internet, sobre todo en este tipo de servicios.

Si bien los datos obtenidos en lo que va del año 2010 son muy similares, la evolución muestra un incremento lento pero paulatino hacia posturas que consideran a la seguridad como limitación baja o media.

Gráfico 37: Evolución de la seguridad como factor que limita la utilización de nuevos servicios (%)



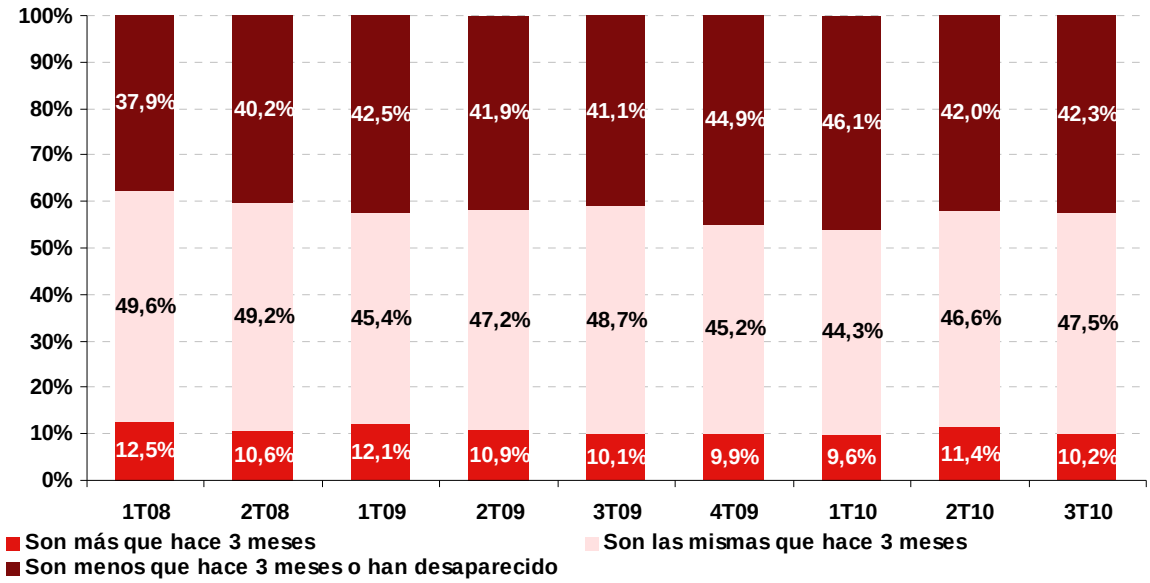
Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

6.2 Evolución de la percepción de la seguridad en Internet por parte de los usuarios

En el tercer trimestre de 2010, el 47,5% de los usuarios de Internet creen que las incidencias de seguridad son las mismas (en número) que hace 3 meses, si bien son casi los mismos (42,3%) los que opinan que son menos frecuentes que en los meses anteriores. Un 10,2% declara que han aumentado estas incidencias.

Si se observa la evolución histórica, los usuarios tienden a considerar que el número de incidencias se reduce: un 42,3% de los usuarios así lo afirman en el tercer trimestre de 2010, frente a un 37,9% que lo declaraba en el primer trimestre de 2008.

Gráfico 38: Evolución de la percepción del número de las incidencias de seguridad con respecto a hace 3 meses (%)



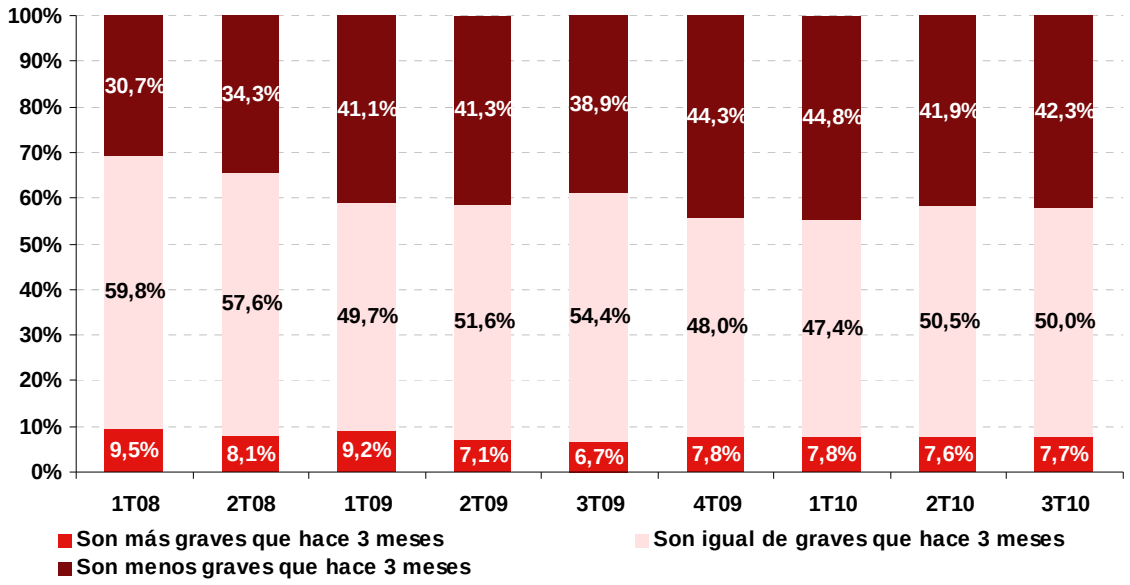
Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

A continuación se analiza la evolución de la gravedad de las incidencias de seguridad percibida por los usuarios.

En el tercer trimestre de 2010, la mitad de los encuestados no ven diferencias sustanciales con respecto a la gravedad de las incidencias de los meses anteriores. Para el 42,3% estas son menos graves y únicamente para un 7,7% lo son más que hace tres meses. Los usuarios que perciben menor gravedad han aumentado desde un 30,7% a principios de 2008 hasta un 42,3% en el último periodo estudiado.

Por tanto, el análisis evolutivo desde el primer trimestre de 2008 indica que los usuarios españoles perciben cada vez menos incidencias en su navegación en Internet y menor gravedad en las mismas.

Gráfico 39: Evolución de la percepción de la gravedad de las incidencias de seguridad con respecto a hace 3 meses (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

6.3 Autorregulación vs. Tutelaje

Existen dos orientaciones principales en cuanto a la actitud de los usuarios en lo referente a la seguridad de la información:

- El tutelaje hace referencia a la demanda de los propios usuarios para que la Administración supervise la seguridad en Internet y ejerza de "educador", canalizando y proporcionando aquella información que 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. Se entiende que los peligros que entraña derivan, en buena medida, de los hábitos de los usuarios. Según esta perspectiva, son los usuarios mismos quienes deben controlar la actualización de su información y adoptar conductas cautelosas.

Se trata de posiciones no excluyentes. Esto es, la demanda de una mayor intervención de las Administraciones puede llevar aparejada la exigencia de un comportamiento más responsable por parte de los usuarios.

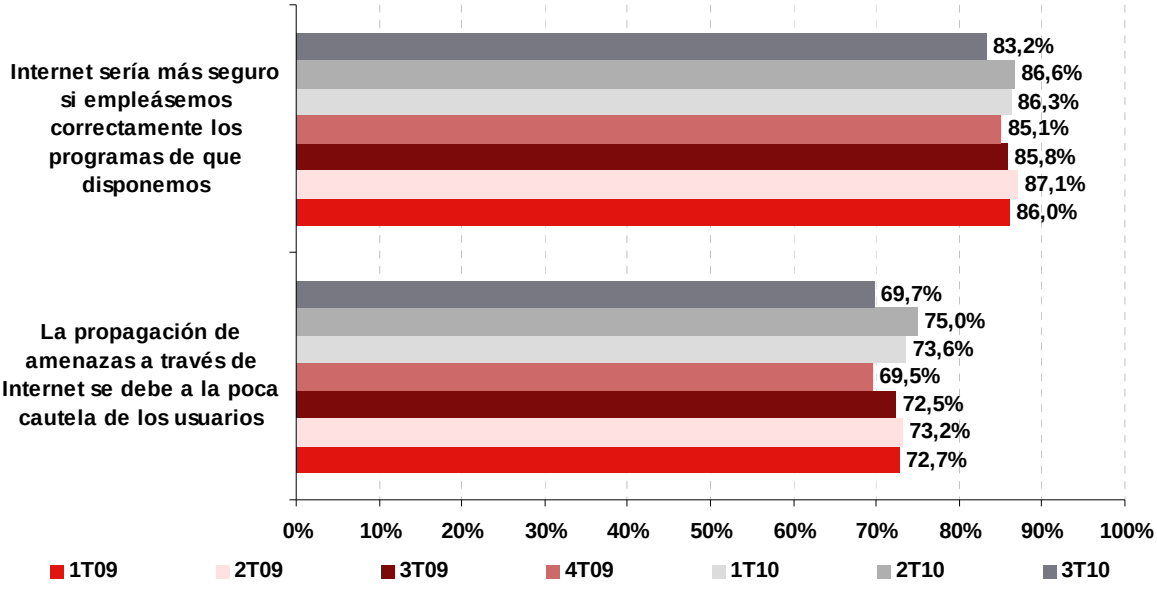
6.3.1 Usuarios

A continuación se profundiza en la autorregulación, analizando el nivel de acuerdo de los ciudadanos españoles con dos afirmaciones que implican cierta responsabilidad de los usuarios a la hora de garantizar la seguridad en Internet.

- *Internet sería más seguro si empleásemos correctamente los programas de que disponemos*: una gran mayoría de los usuarios, el 83,2%, están de acuerdo con esta afirmación, en línea con la tendencia observada en los trimestres anteriores.

- *La propagación de amenazas a través de Internet se debe a la poca cautela de los usuarios*: el 69,7% de los usuarios encuestados han declarado estar de acuerdo con esta afirmación, porcentaje muy similar al registrado en el último trimestre de 2009.

Gráfico 40: Evolución del porcentaje de usuarios que se muestran *totalmente de acuerdo* y *de acuerdo* con... (%)



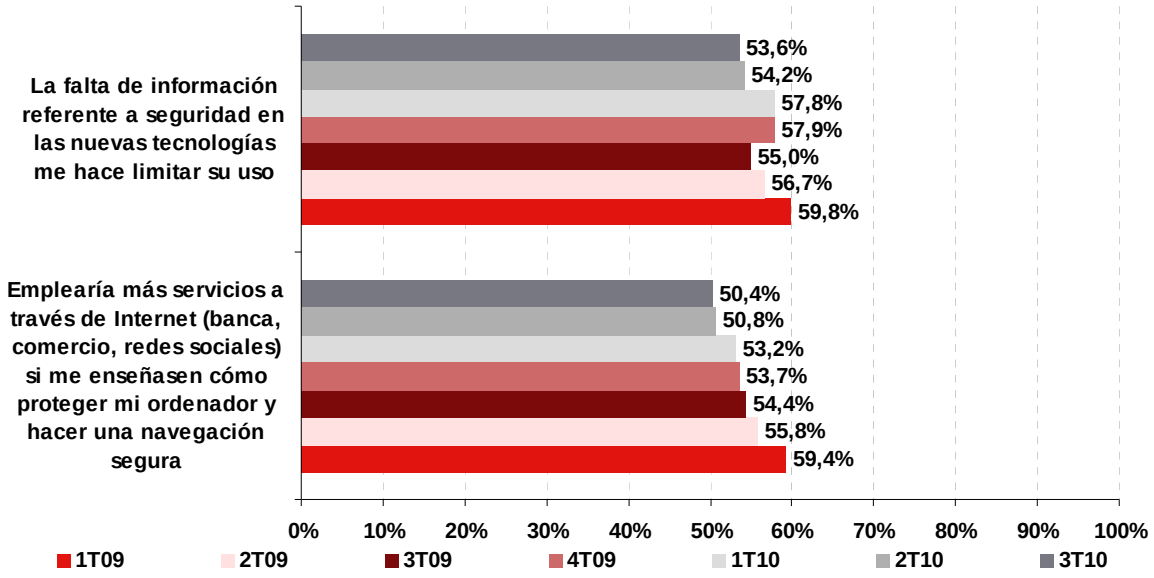
Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

Las afirmaciones que se analizan a continuación van dirigidas a conocer de qué manera la falta de información sobre seguridad representa un freno para el avance de la Sociedad de la Información. Dichas afirmaciones están planteadas desde una perspectiva personal de cada usuario.

- *La falta de información referente a seguridad en las nuevas tecnologías me hace limitar su uso*: un 53,6% de la población ve una relación entre falta de información y menor uso. Los valores son estables en los últimos trimestres.

- *Emplearía más servicios a través de Internet de los que emplea actualmente si me enseñasen cómo proteger mi ordenador y hacer una navegación segura*: un 50,4% de los usuarios incrementaría su uso si recibiese información específica. La tendencia muestra un descenso leve y paulatino en la proporción de usuarios que requieren esta información.

Gráfico 41: Evolución del porcentaje de usuarios que se muestran *totalmente de acuerdo* y *de acuerdo* con... (%)



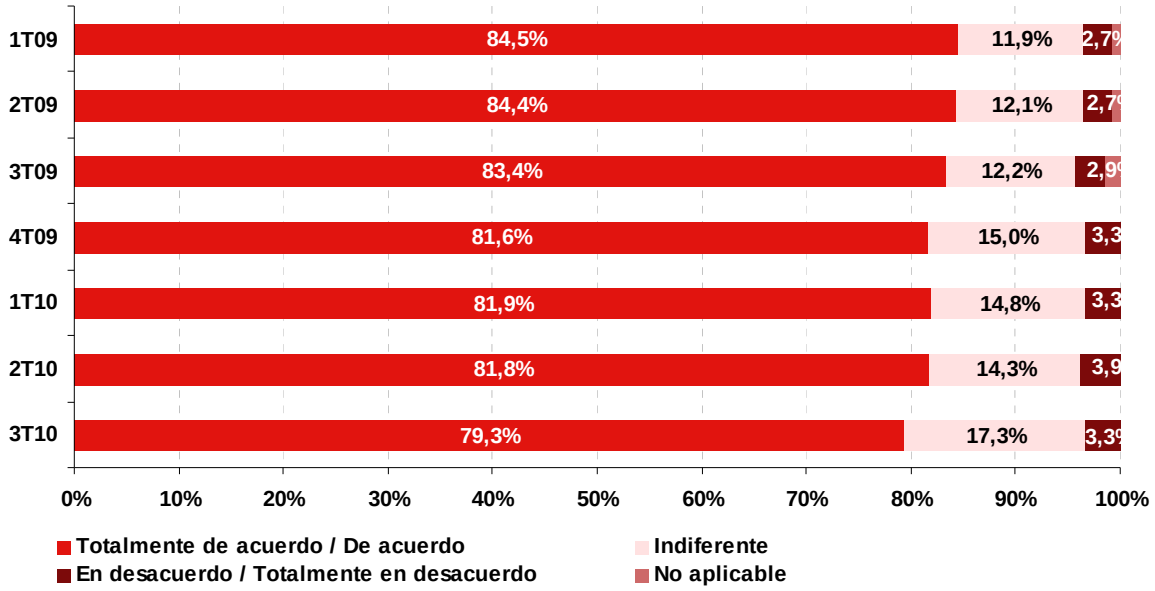
Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

6.3.2 Papel de la Administración en la garantía de la seguridad de la información

Ante la afirmación *La Administración tiene que implicarse más en mejorar la seguridad en Internet*, un 79,3% de los encuestados se muestra de acuerdo o totalmente de acuerdo, mientras que a un 17,3% le es indiferente.

El porcentaje de usuarios que se muestran totalmente o de acuerdo con esta afirmación ha descendido ligeramente en los últimos trimestres. Aunque los valores siguen evidenciando que los ciudadanos reclaman más implicación de la Administración para mejorar la seguridad de las redes, parece que cada vez es mayor la proporción de usuarios a los que les resulta indiferente esta participación.

Gráfico 42: Evolución del nivel de acuerdo con la opinión *La Administración tiene que implicarse más en mejorar la seguridad en Internet* (%)



Base: Total usuarios (n=3.538 en 3T10) *Fuente: INTECO*

Puesto que los ciudadanos tienen claro que la Administración debe involucrarse, en la Tabla 5 se recogen las medidas concretas que los usuarios le piden.

Se han agrupado las medidas en cuatro categorías:

- Vigilancia, que incluye vigilar de cerca lo que ocurre en la Red y velar por el uso adecuado de los datos personales.
- Respuesta técnica, que implica dar soporte a los usuarios y desarrollar herramientas gratuitas.
- Sensibilización, que tiene que ver con hacer campañas de información y ofrecer cursos y talleres.
- Respuesta institucional y legislativa.

Los usuarios demandan en su mayoría medidas incluidas en las dos primeras categorías. Así, vigilar más de cerca lo que está pasando en Internet es la medida prioritaria para el 28% de los encuestados, mientras que desarrollar y ofrecer herramientas de seguridad gratuitas, lo es para el 26,4%.

La actualización y reforma legislativa para los nuevos delitos por Internet, dentro de las medidas de carácter institucional y legislativo, es preferente para el 12% de los usuarios. En este sentido el 23 de junio de 2010 se publicó en el BOE la Ley Orgánica 5/2010, de

22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Ha entrado en vigor el 23 de diciembre de 2010 y endurece y tipifica varios delitos informáticos. Hasta ahora, el código penal no había previsto el uso de las tecnologías de la información para invadir la intimidad de las personas o para violar, acceder o descubrir sus secretos. Con esta reforma, se castiga a quien acceda a un sistema informático sin consentimiento, independientemente de si lleva a cabo algún tipo de daño en el sistema o algún perjuicio al propietario del equipo[15].

Tabla 5: Medidas demandadas a la Administración 3T 2010 (%)

Carácter de la medida	Medida	Medida prioritaria
Vigilancia	Vigilar más de cerca lo que está pasando en Internet	**28,0**%
	Velar por el uso adecuado de los datos personales en Internet	7,3%
Respuesta técnica	Dar respuesta/soporte técnico a los problemas de seguridad de los ordenadores de los ciudadanos	6,3%
	Desarrollar y ofrecer herramientas de seguridad gratuitas	**26,4**%
Sensibilización	Hacer campañas de información y sensibilización sobre los riesgos y cómo prevenirlos	**6,5**%
	Ofrecer cursos y talleres formativos sobre servicios de Internet y seguridad	3,4%
Respuesta institucional y legislativa	Una mayor coordinación (legislación, persecución, información) entre los organismos de la administración implicados (policías, jueces, …) en la solución de los problemas de seguridad	9,8%
	Actualización y reforma legislativa para los nuevos delitos por Internet	**12,0**%
TOTAL		***99,7***

Base: Usuarios que se muestran totalmente de acuerdo y de acuerdo con la afirmación La Administración tiene que implicarse más en mejorar la seguridad en Internet (n=2.933) *Fuente: INTECO*

Se estudia ahora la evolución de cada una de las medidas demandadas a la Administración, agrupadas por las categorías mencionadas.

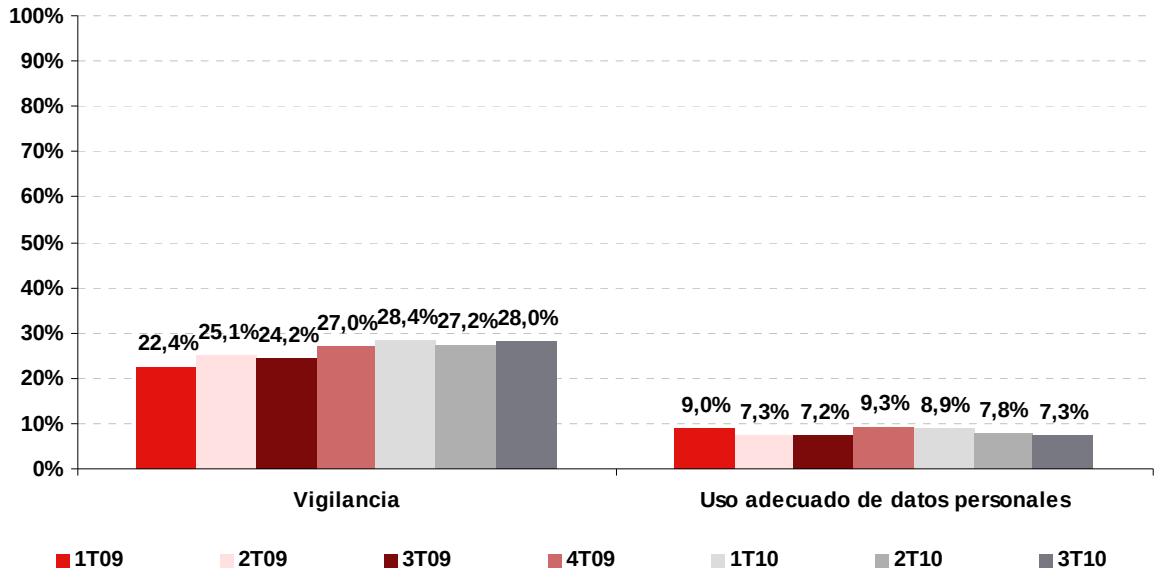
Medidas de vigilancia

- *Vigilar más de cerca lo que está pasando en Internet* es la medida prioritaria para los usuarios encuestados (28,0%), al igual que en los últimos trimestres, mostrando una tendencia ligeramente al alza en el número de usuarios que demandan esta medida.

- En cuanto a *Velar por el uso adecuado de los datos personales en Internet,* esta medida es demandada por el 7,3% de los usuarios, en línea con los valores registrados en trimestres anteriores.

[15] Disponible en: http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf

Gráfico 43: Evolución de las medidas de vigilancia demandadas a la Administración (%)



Base: Usuarios que se muestran totalmente de acuerdo y de acuerdo con la afirmación La Administración tiene que implicarse más en mejorar la seguridad en Internet (n=2.933) *Fuente: INTECO*

Se destacan a continuación algunas iniciativas de la Administración que tienen que ver con la vigilancia:

- El Observatorio de la Seguridad de la Información de INTECO (http://observatorio.inteco.es) tiene como objetivo vigilar, estudiar y describir la situación general de seguridad en Internet. Así, los informes periódicos del Observatorio (de los que este documento forma parte) son el registro escrito de una labor continuada de observación y diagnóstico.

- La red de sensores de correo (https://ersi.inteco.es/) de INTECO vigilan la evolución de amenazas como el spam, recopilando información sobre el correo no deseado.

Medidas de respuesta técnica

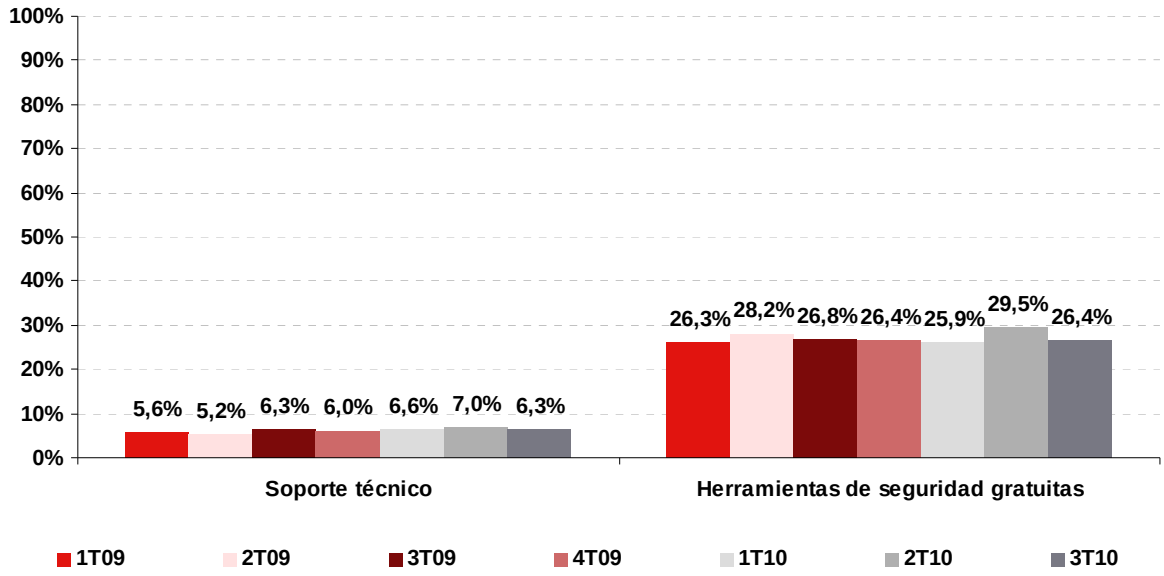
Las dos medidas de respuesta técnica analizadas son:

- *Dar respuesta/soporte técnico a los problemas de seguridad de los ordenadores de los ciudadanos*: un 6,3% de los ciudadanos consideran esta medida como prioritaria, valor muy similar al de los últimos trimestres.

- *Desarrollar y ofrecer herramientas de seguridad gratuitas*: es la segunda medida preferente para los encuestados, con un 26,4% de usuarios que así lo declaran.

La tendencia observada es estable, con valores similares a los del primer trimestre de 2009.

Gráfico 44: Evolución de las medidas de respuesta técnica demandadas a la Administración (%)



Base: Usuarios que se muestran totalmente de acuerdo y de acuerdo con la afirmación La Administración tiene que implicarse más en mejorar la seguridad en Internet (n=2.933) *Fuente: INTECO*

Se destacan a continuación algunas iniciativas de la Administración que tienen que ver con respuesta técnica:

- INTECO pone a disposición de los usuarios a través la Oficina de Seguridad del Internauta (www.osi.es) una serie de herramientas y útiles de seguridad gratuitos, que tienen como finalidad la prevención de ataques e infecciones en los equipos.

- Igualmente, el INTECO-CERT (Centro de Respuesta a Incidentes de Seguridad) ofrece, de manera gratuita para el ciudadano, herramientas antimalware, de bloqueo, de análisis y de recuperación: http://cert.inteco.es/Proteccion/Utiles_Gratuitos/ .

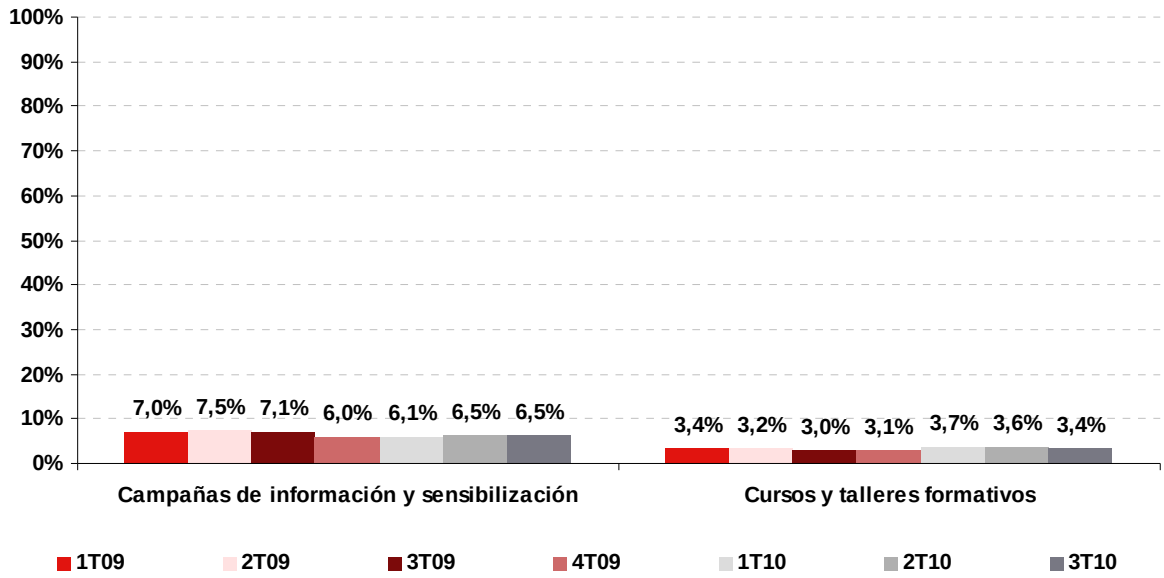
Medidas de sensibilización

Las medidas de sensibilización son las menos prioritarias para los ciudadanos.

- *Hacer campañas de información y sensibilización sobre los riesgos y cómo prevenirlos*: en el tercer trimestre de 2010, el 6,5% de los usuarios priorizan esta medida. La evolución histórica apenas muestra cambios en los valores.

- *Ofrecer cursos y talleres formativos sobre servicios de Internet y seguridad*: el 3,4% de los encuestados está de acuerdo con la prioridad de esta medida. La evolución de los valores es muy estable.

Gráfico 45: Evolución de las medidas de sensibilización demandadas a la Administración (%)



Base: Usuarios que se muestran totalmente de acuerdo y de acuerdo con la afirmación La Administración tiene que implicarse más en mejorar la seguridad en Internet (n=2.933) *Fuente: INTECO*

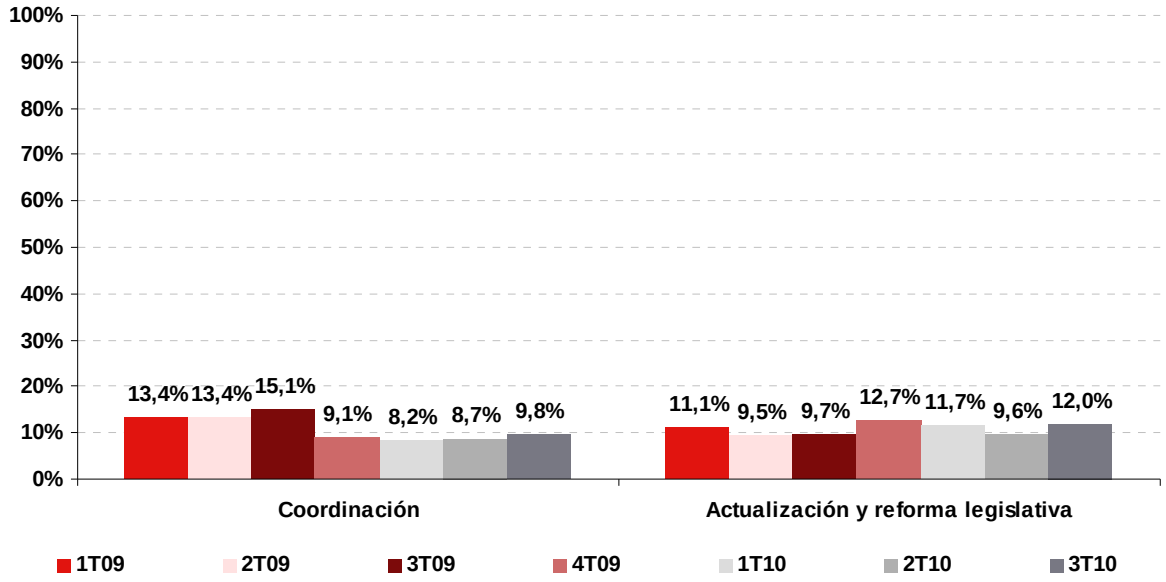
Medidas de respuesta institucional y legislativa

Las medidas de respuesta institucional y legislativa que los ciudadanos piden a la Administración son las siguientes:

- *Una mayor coordinación (legislación, persecución, información) entre los organismos de la Administración implicados en la solución de los problemas de seguridad*. Esta medida es prioritaria para un 9,8%, valor muy similar a los registrados durante el último año.

- *Actualización y reforma legislativa para los nuevos delitos por Internet*. Esta medida crece hasta el 12% de usuarios que la respaldan, recuperando niveles cercanos al del último trimestre de 2009.

Gráfico 46: Evolución de las medidas de respuesta institucional y legislativa demandadas a la Administración (%)



Base: Usuarios que se muestran totalmente de acuerdo y de acuerdo con la afirmación La Administración tiene que implicarse más en mejorar la seguridad en Internet (n=2.933) *Fuente: INTECO*

Las acciones de coordinación son prioritarias en el ámbito nacional e internacional. El Consejo de Europa aprobaba en junio de 2001 el Convenio sobre Ciberdelincuencia con el objetivo de eliminar las barreras jurisdiccionales entre los países de la Unión Europea en delitos relacionados con la informática.

También en el contexto europeo, la UE ha provisto fondos para proyectos del Séptimo Programa Marco que reciben el nombre de "acciones coordinadas". Una de estas acciones es ICT-Forward (http://www.ict-forward.eu/), que busca poner en contacto a distintos actores de la seguridad informática (cuerpos de seguridad, órganos legislativos, compañías de seguridad, operadores de telefonía, proveedores de Internet, etc.) para promover la colaboración y anticiparse a amenazas futuras.

En los últimos años han aparecido más agentes relacionados con el tratamiento y resolución de problemas de seguridad, lo que justifica la necesidad de una adecuada coordinación entre ellos a fin de garantizar la agilidad necesaria.

Como medidas de actualización y reforma legislativa, se mencionaba anteriormente (páginas 70 y siguientes) la reciente entrada en vigor de la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal[16].

[16] Disponible en: http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf

6.3.3 Papel de otros actores en la garantía de la seguridad de la información

Usuarios y Administraciones son responsables indiscutibles de mejorar la seguridad en la Red. En el informe de la Organización para el Desarrollo Económico y la Cooperación (OECD) titulado *Malicious Software (Malware): A Security Threat to the Internet Economy*[17], se destacan otros actores que tienen influencia a la hora de garantizar la seguridad de la información:

- Desarrolladores de software, que deberían programar aplicaciones fiables, seguras y exentas de vulnerabilidades.
- Empresas antivirus y desarrolladores de software de seguridad, encargados de suministrar soluciones de seguridad a los usuarios finales.
- Proveedores de Internet, responsables de administrar las redes que los usuarios emplean para conectarse a Internet.
- Entidades de registro de dominios y reguladoras de nombres, que tienen el poder de desactivar dominios maliciosos.
- CERTs o CSIRTs (Equipos de respuesta ante incidentes de seguridad informática), que en muchas ocasiones juegan un papel importante a la hora de detectar, contrarrestar y recuperarse de problemas de seguridad.

Para cerrar este capítulo, se ha pedido a los ciudadanos españoles que establezcan un ranking de responsabilidad entre los principales actores que forman parte de la Sociedad de la Información.

Los usuarios consideran que son ellos mismos, principalmente, quienes deben velar en primera instancia por su seguridad en Internet, con un 40,7% de las menciones. En segunda instancia responsabilizan a las administraciones (27,4%), seguido en una tercera posición por los proveedores de servicios de Internet (19,1%). Por último, las empresas que crean herramientas de seguridad son consideradas como principales responsables por un 12,8% de los usuarios.

[17] Disponible en: http://www.oecd.org/dataoecd/53/34/40724457.pdf

Tabla 6: Consideración de quiénes son los responsables de la seguridad en Internet 3T10 (%)

Actor analizado	Primer responsable	Segundo responsable	Tercer responsable	Cuarto responsable
Usuarios	40,7%	18,4%	14,8%	26,1%
Administraciones	27,4%	21,8%	22,7%	28,0%
Proveedores de servicios de Internet	19,1%	29,3%	28,6%	23,0%
Empresas que crean herramientas de seguridad	12,8%	30,5%	33,8%	22,9%

Base: Total usuarios (n=3.538) *Fuente: INTECO*

7 SISTEMA DE INDICADORES DE LA SEGURIDAD DE LA INFORMACIÓN

7.1 Estructura y objetivos del sistema

El análisis mostrado en el *Estudio sobre seguridad de la información y la e-confianza de los hogares españoles* se puede sintetizar en el cálculo de seis indicadores que parametrizan la información resultante de la investigación de manera sistemática.

Tabla 7: Sistema de indicadores de seguridad y e-confianza

	Indicador
Indicadores de protección	**IS.1** Indicador de herramientas y medidas de seguridad
	IS.2 Indicador de conductas y hábitos de seguridad
Indicador de confianza	**IS.3** Indicador de e-confianza
Indicadores de riesgos	**IS.4** Indicador de incidencias de malware
	IS.5 Indicador de equipos con riesgo alto
	IS.6 Indicador de equipos con diseminación potencial alta

Fuente: INTECO

Los seis indicadores se clasifican en dos grupos: indicadores relacionados con la protección (IS.1 e IS.2) e indicadores relacionados con el riesgo y el nivel de incidencias (IS.4, IS.5, IS.6). En el primero se sitúan aquellos que miden y señalan la protección existente y en el segundo los que miden los riesgos.

El IS.3, que completa el listado, es la variable que presenta la percepción de seguridad general del usuario en su uso de Internet, la confianza que deposita en los mecanismos de protección que tiene instalados en el ordenador, y hábitos seguros de uso, así como su apreciación de que Internet es más seguro.

De este modo, el conjunto de indicadores se contrapesa: una disminución de las incidencias tiende a responder a un mayor equipamiento en seguridad y hábitos más prudentes para restablecer el equilibrio que viene marcado por una e-confianza elevada.

Los seis indicadores de seguridad toman valores que se encuentran entre 0 y 100 puntos. Por ello, en el caso, por ejemplo, del indicador IS.6, Indicador de equipos con diseminación potencial alta, que éste tome un valor de 20,4 no quiere decir que el 20,4% de los ordenadores tengan un riesgo de diseminación alto, sino que el resultado de los cálculos combinados para obtener su resultado arroja un valor de 20,4 puntos en una escala de 0 a 100.

De este modo, el sistema de indicadores de INTECO permite hacer un seguimiento de la evolución y las tendencias de la seguridad en Internet y la confianza de los hogares, con 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 seis 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 reducirlas.
- 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 entre política de seguridad de la Administración y el comportamiento individual de los usuarios.

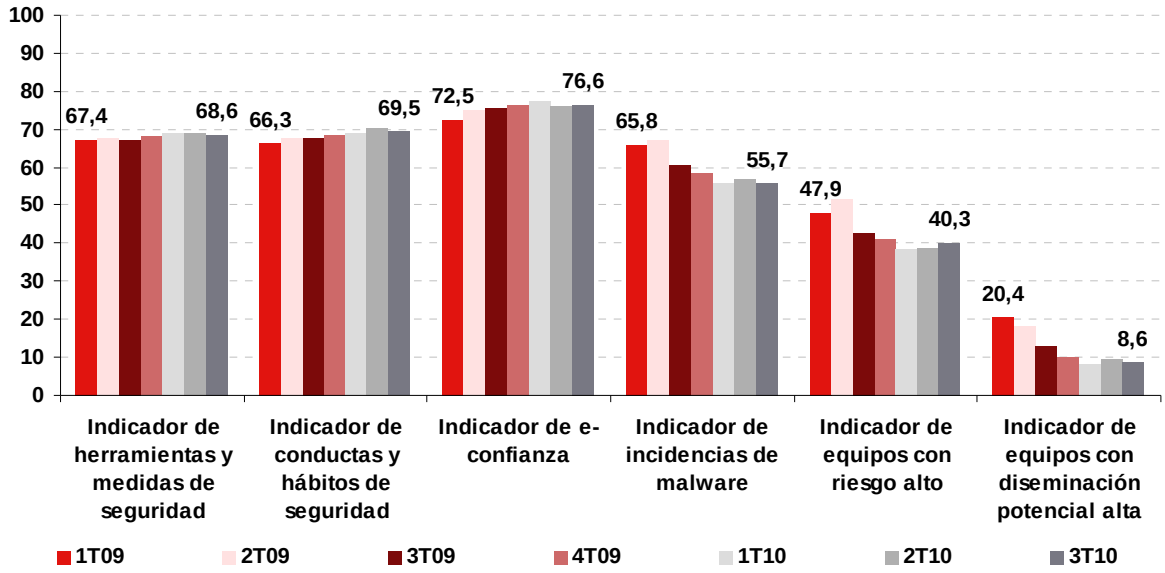
En general, los indicadores reflejan un cálculo combinado de distintos ítems y parámetros que componen cada uno de estos índices, como se verá a continuación.

7.2 Análisis de los indicadores de la seguridad de la información

El Gráfico 47 muestra la evolución general de los seis indicadores desde el primer trimestre de 2009 hasta el tercer trimestre de 2010.

Se aprecia una evolución favorable del sistema de indicadores: crecimientos moderados y constantes de los indicadores de protección de los hogares (*Indicador de herramientas y medidas de seguridad* e *Indicador de conductas y hábitos de seguridad*) se traducen en bajadas acusadas de los indicadores de riesgo de sus equipos (*Indicador de incidencias de malware*, *Indicador de equipos con riesgo alto* e *Indicador de equipos con diseminación potencial alta*). Como balance, el *Indicador de e-confianza* sigue mostrando un valor elevado, y una tendencia creciente desde principios de 2009.

Gráfico 47: Evolución del sistema de indicadores de la seguridad de la información (0-100 puntos)



Fuente: INTECO

A continuación se profundiza en las particularidades de cada uno de los indicadores del sistema.

7.2.1 Indicador de herramientas y medidas de seguridad

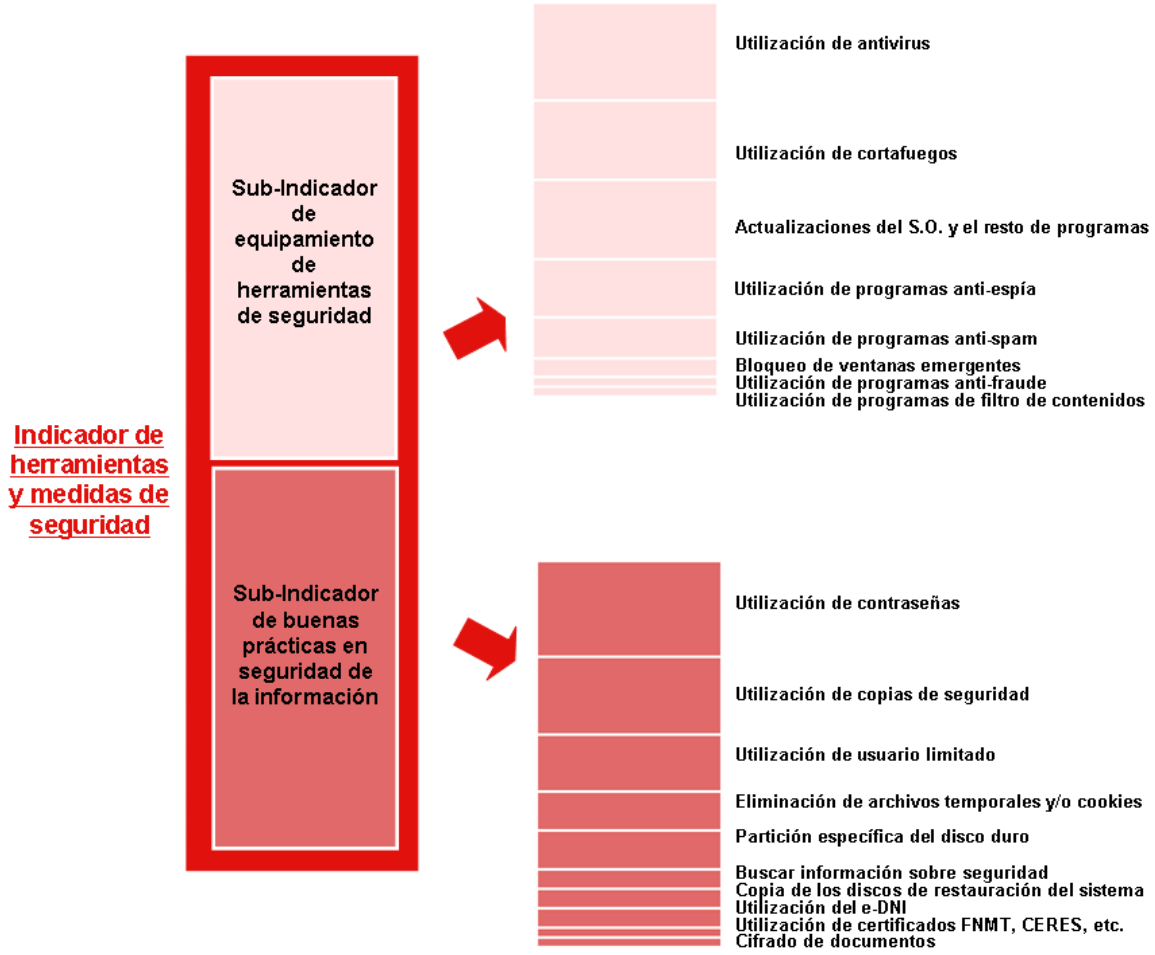
Este indicador compuesto mide el equipamiento y adopción de medidas de seguridad que existen en la actualidad. Su cálculo no sólo se centra en la propia seguridad del sistema, sino que también incluye medidas que favorecen la seguridad de la información.

Se compone de dos conceptos generales: por un lado mide el equipamiento pasivo en seguridad (herramientas) y por otro las medidas activas que los propios usuarios aplican sobre la seguridad del ordenador (buenas prácticas).

El peso en igual medida del sub-indicador de equipamiento en herramientas de seguridad y el sub-indicador de buenas prácticas en seguridad de la información conforman este indicador compuesto. Dentro de cada sub-indicador se tienen en cuenta las diferentes herramientas y buenas prácticas en la proporción que se observa en la Ilustración 1.

Se mide en una escala de 0 a 100 puntos, donde el máximo equipamiento y buenas prácticas en seguridad supondrían un valor de 100 y el mínimo un 0.

Ilustración 1: Indicador de herramientas y medidas de seguridad

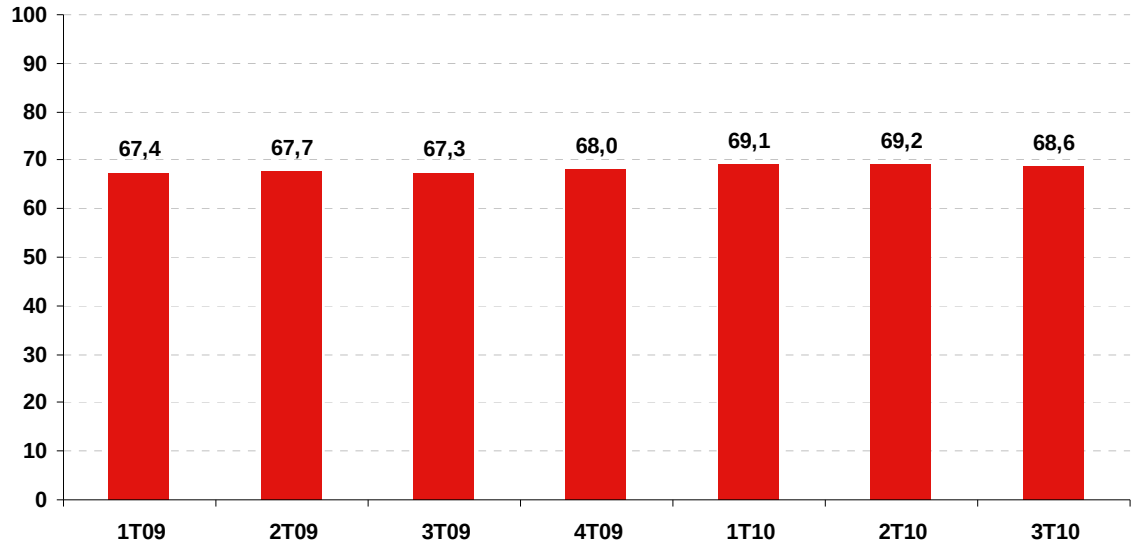


Fuente: INTECO

En este tercer trimestre de 2010 el indicador de herramientas y medidas de seguridad alcanza un valor de 68,6, lo que supone un ligerísimo retroceso con respecto a los datos del trimestre anterior.

¿Qué puede justificar este descenso? Dado que el indicador se compone de diferentes comportamientos, una valoración negativa en alguno o algunos de ellos puede tener un impacto directo en el valor total del indicador. Así, por ejemplo, este trimestre ha descendido la proporción de usuarios que declaran realizar copias de seguridad y los que siguen el hábito prudente de buscar información de seguridad.

Gráfico 48: Evolución del indicador de herramientas y medidas de seguridad (0-100 puntos)



Fuente: INTECO

7.2.2 Indicador de conductas y hábitos de seguridad

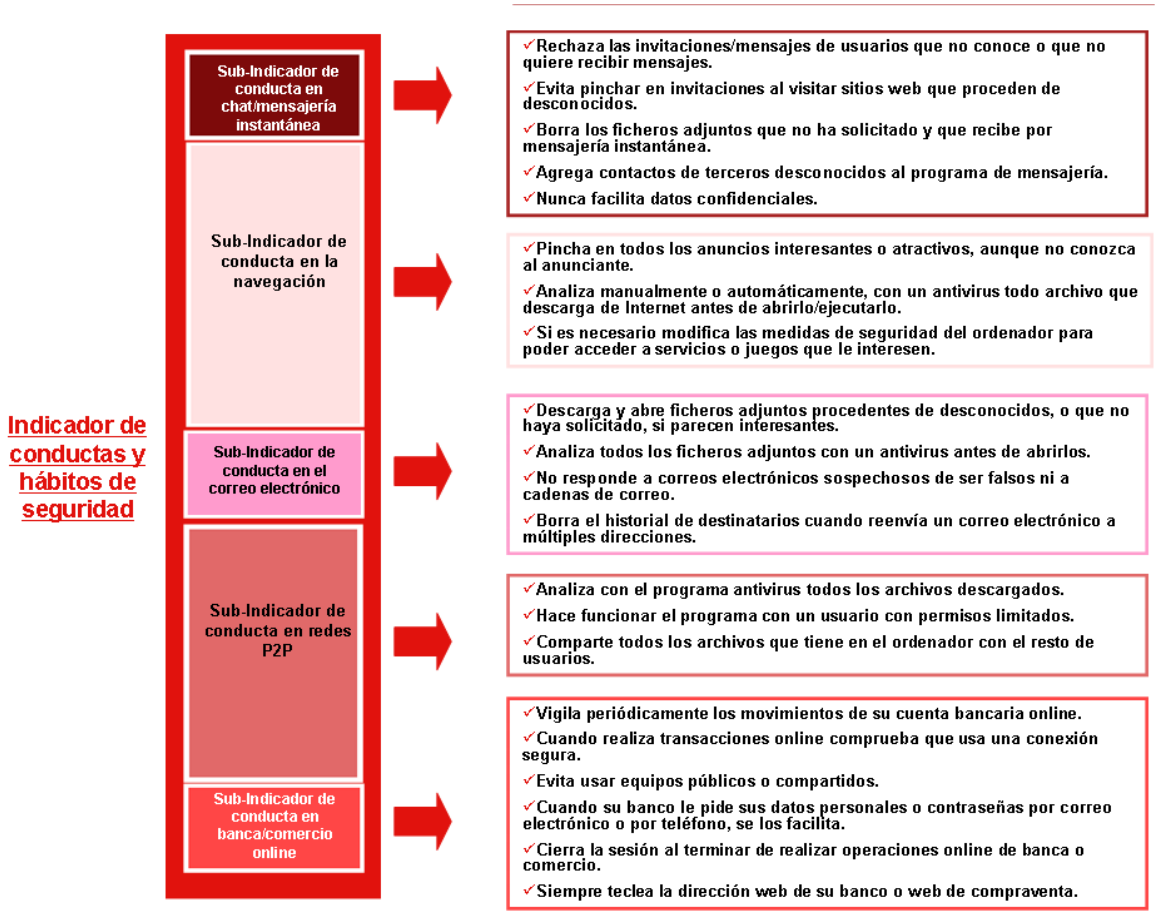
Mide el tipo de comportamiento y hábitos seguros durante la navegación por Internet y el uso de determinados servicios online, sintetizando la puntuación obtenida en diferentes aspectos.

Para el cálculo de este indicador compuesto se tiene en cuenta, en las proporciones que se pueden observar en la Ilustración 2, los siguientes sub-indicadores:

- Sub-indicador de conducta en el uso de chat y mensajería instantánea.
- Sub-indicador de conducta en la navegación.
- Sub-indicador de conducta en el correo electrónico.
- Sub-indicador de conducta en el uso de redes de intercambio de ficheros (P2P).
- Sub-indicador de conducta en la banca online y comercio electrónico.

Se mide en una escala de 0 a 100 puntos, donde la máxima prudencia supondría un valor de 100 y la mínima 0.

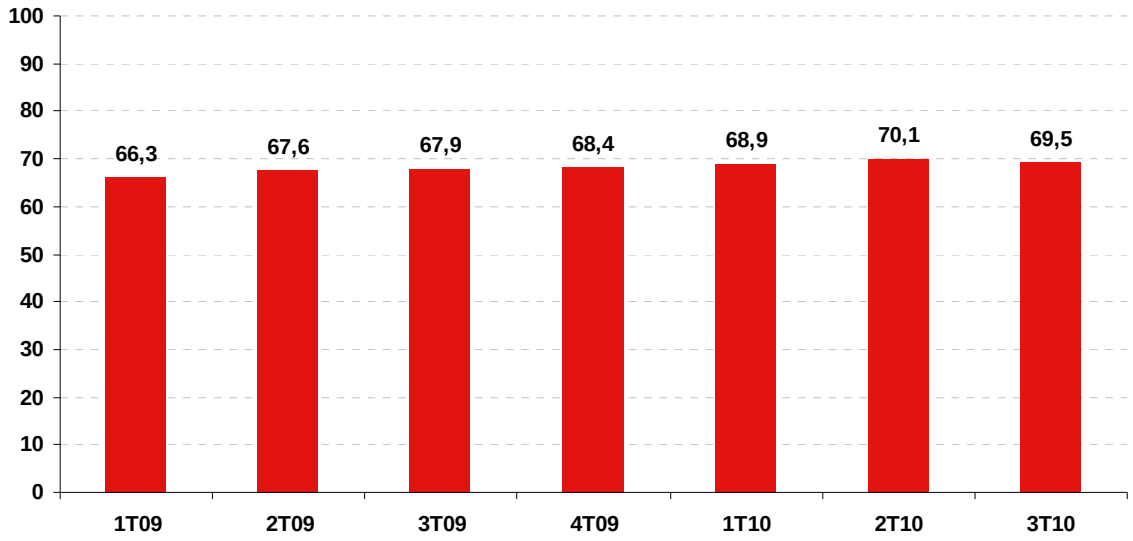
Ilustración 2: Indicador de conductas y hábitos de seguridad



Fuente: INTECO

El indicador de conductas y hábitos de seguridad alcanza en el 3er trimestre de 2010 un valor de 69,5, lo que supone un descenso de 6 décimas con respecto al trimestre anterior, confirmando la tendencia estable que lleva presentando el indicador en 2010.

Gráfico 49: Evolución del indicador de conductas y hábitos de seguridad (0-100 puntos)



Fuente: INTECO

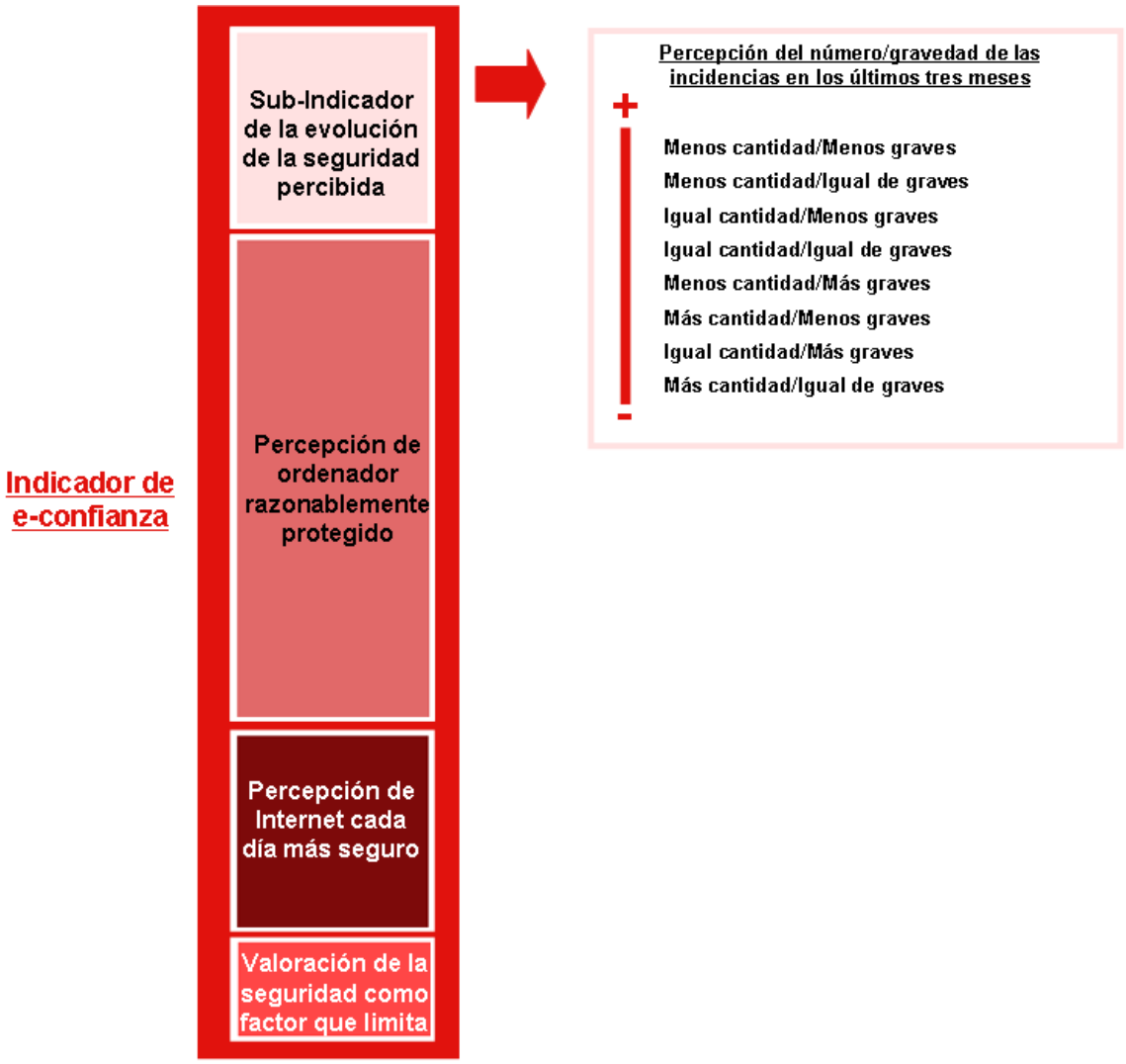
7.2.3 Indicador de e-confianza

Mide la percepción subjetiva de seguridad del propio usuario cuando usa Internet. Para el cálculo de este indicador compuesto se tiene en cuenta, en las proporciones que se pueden observar en la Ilustración 3, lo siguiente:

- Sub-indicador de la evolución de la seguridad percibida: analiza la percepción del número/gravedad de las incidencias de seguridad en los últimos tres meses.
- Percepción de protección en el ordenador.
- Percepción de seguridad de Internet.
- Valoración de la seguridad como factor que limita a la hora de utilizar nuevos servicios en Internet.

Se mide en una escala de 0 a 100 puntos, donde la máxima e-confianza supondría un valor de 100 y la mínima 0.

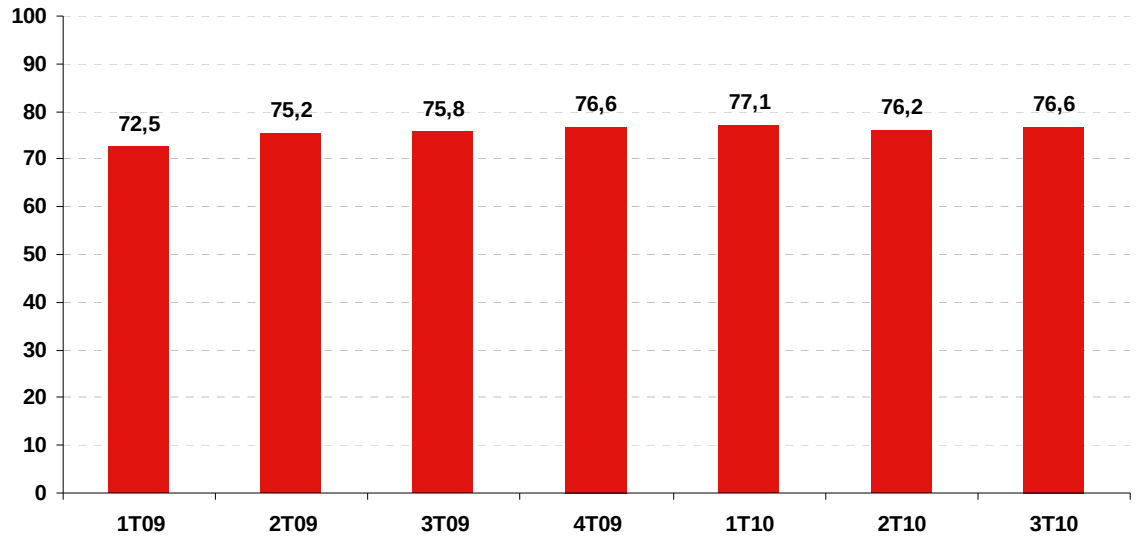
Ilustración 3: Indicador de e-confianza



Fuente: INTECO

En el siguiente gráfico se muestra la evolución del indicador de e-confianza. Con un nivel de 76,6, se mantiene estable y con ligeros cambios con respecto a las lecturas anteriores.

Gráfico 50: Evolución del indicador de e-confianza (0-100 puntos)



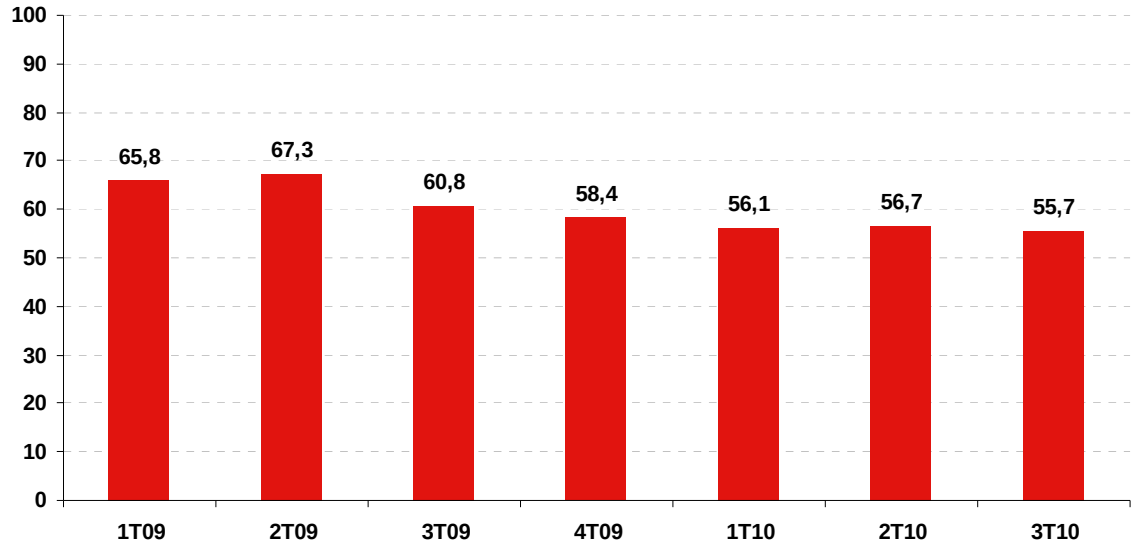
Fuente: INTECO

7.2.4 Indicador de incidencias de malware

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

Este indicador se sitúa en 55,7, alcanzando un nuevo mínimo histórico.

Gráfico 51: Evolución del indicador de incidencias de malware (0-100 puntos)



Fuente: INTECO

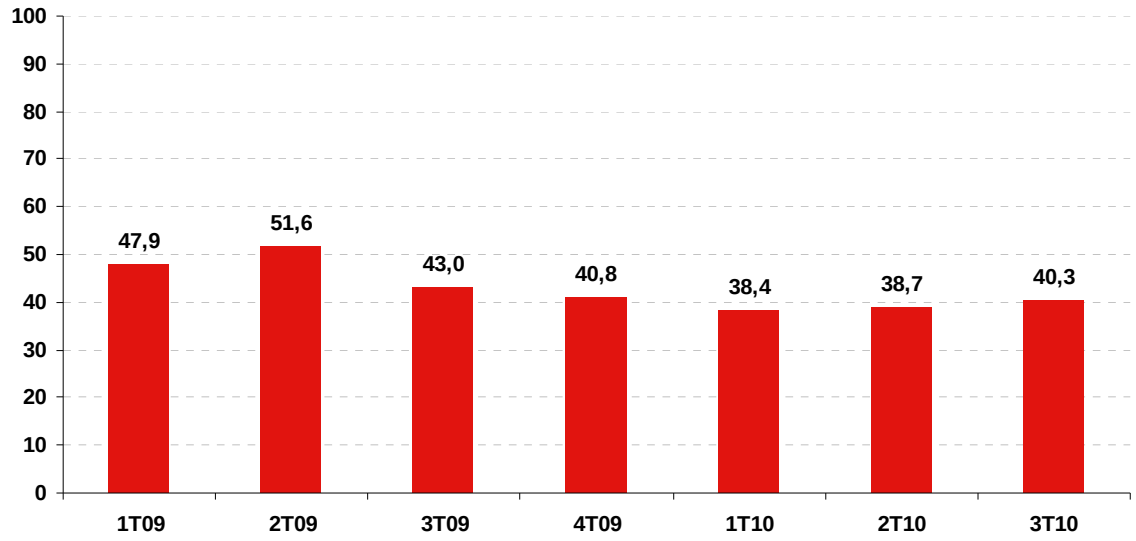
7.2.5 Indicador de ordenadores con riesgo alto

Indica el porcentaje de equipos domésticos en los que se ha detectado al menos una incidencia de malware con riesgo alto durante la auditoría remota.

Se cataloga el código malicioso detectado según tres grupos de riesgo, tal y como se explica en el apartado 4.2.4 al analizar la peligrosidad del código malicioso y el riesgo del equipo.

Este indicador alcanza un valor de 40,3 en el tercer trimestre de 2010.

Gráfico 52: Evolución del indicador de equipos con riesgo alto (0-100 puntos)



Fuente: INTECO

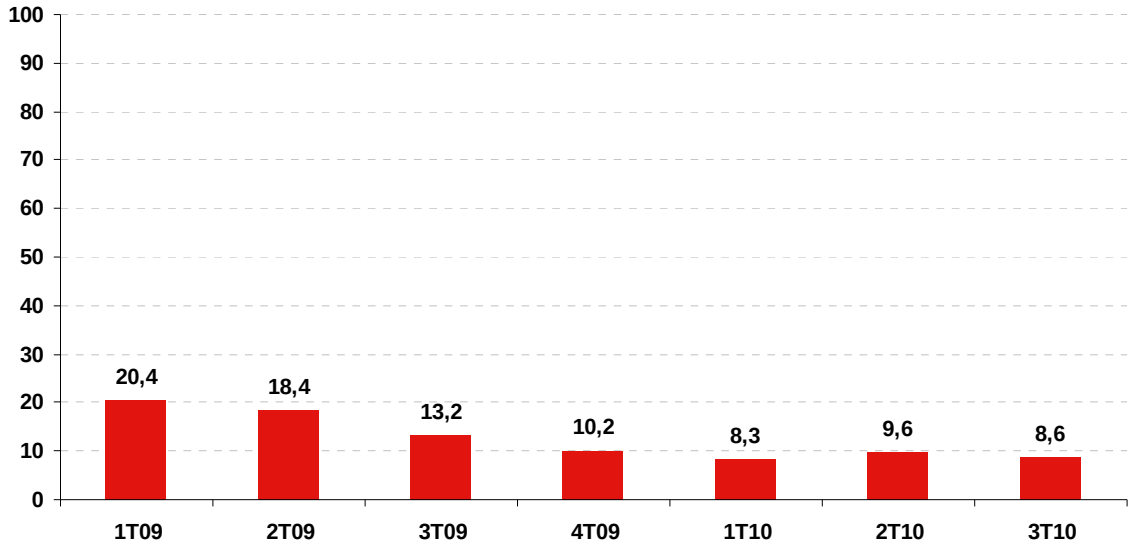
7.2.6 Indicador de ordenadores con diseminación potencial alta

Para el cálculo de este indicador sintético se consideran aquellas conductas y hábitos del usuario de las que, en mayor o menor medida, pudiera derivarse un alto grado de diseminación entre el resto de los usuarios y el propio sistema. Será un equipo con diseminación potencial alta si cumple las siguientes condiciones en combinación con que sea usuario de servicios de mensajería instantánea y descargue archivos de Internet:

- No disponer de antivirus activo.
- No disponer del sistema operativo actualizado.
- Existir alguna pieza de malware de riesgo alto y/o un script.

El indicador de ordenadores con diseminación potencial alta, con un valor de 8,6, confirma una línea descendiente desde principios de 2009.

Gráfico 53: Evolución del indicador de equipos con diseminación potencial alta (0-100 puntos)



Fuente: INTECO

8 CONCLUSIONES

Con respecto a las herramientas y al uso declarado, vuelven a imponerse los programas antivirus sobre el resto (92,5%), seguidos de cortafuegos (81,3%) y las actualizaciones del sistema operativo y programas (80,7%), todas ellas automatizables. Esto viene siendo habitual, por tanto, cabe comentar los hábitos y herramientas en los que todavía cabe margen de mejora. Este tercer trimestre de 2010, destaca la copia de seguridad de archivos, que desciende casi cuatro puntos porcentuales. De un 65,1% en el 2º trimestre de 2010 pasa a un 61,7% de usuarios que, en esta lectura, declaran utilizar la medida. Desciende también ligeramente la búsqueda de información. Ambas tienen en común que supone un trabajo continuo y sistemático por parte del usuario.

Los usuarios que reconocen no utilizar cada una de las herramientas analizadas, ¿qué argumentos utilizan para justificar esta falta de uso? En el caso de las medidas automatizables, el desconocimiento es el motivo de no uso alegado de forma mayoritaria en 6 de las 8 medidas automatizables. Así, es la razón más mencionada entre quienes no utilizan actualizaciones del sistema operativo (23,9%), cortafuegos (31,2%), programas de bloqueo de ventanas emergentes (32,0%), programas anti-espía (32,8%) y programas antifraude (40,6%). Resulta interesante destacar que en el caso de las medidas no automatizables, no solo es el desconocimiento sino que también es mayoría la sensación de que no se usan porque "no se necesitan" este tipo de medidas. Así este es el motivo principal para no realizar copias de seguridad (26,9%), utilizar contraseñas (57,9%) y trabajar con los permisos reducidos (40,4%).

Con respecto a las redes sociales, con cada vez más los usuarios y adeptos a estas plataformas: en este trimestre un 71,6% declara realizar un uso habitual de las mismas, y un 13% adicional lo hace de manera ocasional. Se trata, en su mayoría, de ciudadanos conscientes de su privacidad, y así el 66,2% de los encuestados manifiestan que sus perfiles solo pueden ser vistos por amigos y contactos.

Un dato que demuestra hasta qué punto los sistemas de envío masivo de correo basura están centralizados en ciertas mafias que los gestionan y controlan, se ha revelado este mes de septiembre. Aunque el incidente más común (declarado) es de nuevo la recepción de correos electrónicos no deseados o spam, de acuerdo con los datos empíricos facilitados por las redes de sensores de INTECO, en septiembre de 2010 se detectó que el 77,4% de los correos circulantes era basura. Este dato supone un importante descenso con respecto a trimestres anteriores, en los que el volumen de correos basura facilitados por las redes de sensores de INTECO se movía siempre en valores por encima del 90%. ¿Qué ha provocado este descenso? En este caso parece existir un origen claro. A mediados de septiembre, las operaciones de spamit.com fueron cerradas. Spamit.com era un grupo conocido que trabajaba con spammers y botnets para proporcionar las infraestructuras y recursos necesarios para gestionar las ganancias de

los negocios publicitados. Por tanto, se trataba de un sistema *underground* que, asociado con los spammers, conseguía gestionar los negocios anunciados en correos basura. En concreto spamit.com era responsable de gran parte de los conocidos anuncios de "*Canadian Pharmacy*", esto es, farmacias que venden sin receta y a precios bajos productos como Viagra, Xanax, etc. La desaparición de spamit.com ha hecho que los valores generales de spam durante la segunda mitad de septiembre, descendieran con respecto a los niveles habituales, mientras los atacantes se reabastecían con nuevas infraestructuras.

Con respecto al malware, el 53,6% de los usuarios alojan malware en septiembre de 2010, un dato que se mantiene relativamente estable en los últimos meses. En cuanto a su tipología, no se observan grandes diferencias con respecto a períodos anteriores: se trata, en su mayoría, de troyanos y adware. El nivel de diversificacón y heterogeneidad del código malicioso sigue siendo elevado. Se observa cierta estabilidad en el número de variantes únicas de malware encontradas cada mes, en torno a los 3.500 desde junio de 2010. Cada variante única detectada se avistaría sólo 2 veces de media.

En septiembre de 2010, un 38,1% de los equipos son considerados de riesgo alto, frente a un 10,3% de riesgo medio y un 5,2% de riesgo bajo. Se confirma la progresiva reducción de los niveles de riesgo de los equipos a lo largo del último año, sobre todo, en el caso de riesgo medio. En concreto en el mes de septiembre, quizás motivado por el menor número de análisis realizados, se observa también un ligero descenso del porcentaje de equipos con riesgo alto.

Para sentirse protegidos, los usuarios demandan que la Administración se implique más en la supervisión de la Red. Así, vigilar más de cerca lo que está pasando en Internet es la medida prioritaria para el 28% de los encuestados, mientras que desarrollar y ofrecer herramientas de seguridad gratuitas, lo es para el 26,4%.

ANEXO I: DISEÑO METODOLÓGICO DETALLADO

El *Estudio sobre la seguridad de la Información y la e-confianza de los hogares españoles* se realiza a partir de una metodología basada en el panel online dedicado.

En la definición de la metodología del estudio se ha considerado una fórmula que permita obtener información, con una perspectiva evolutiva, relativa al nivel de seguridad y e-confianza de los hogares españoles. La necesidad de unos datos robustos sobre los mismos hogares y usuarios en diferentes momentos del tiempo hace que el panel online dedicado resulte la metodología idónea para satisfacer los objetivos del proyecto.

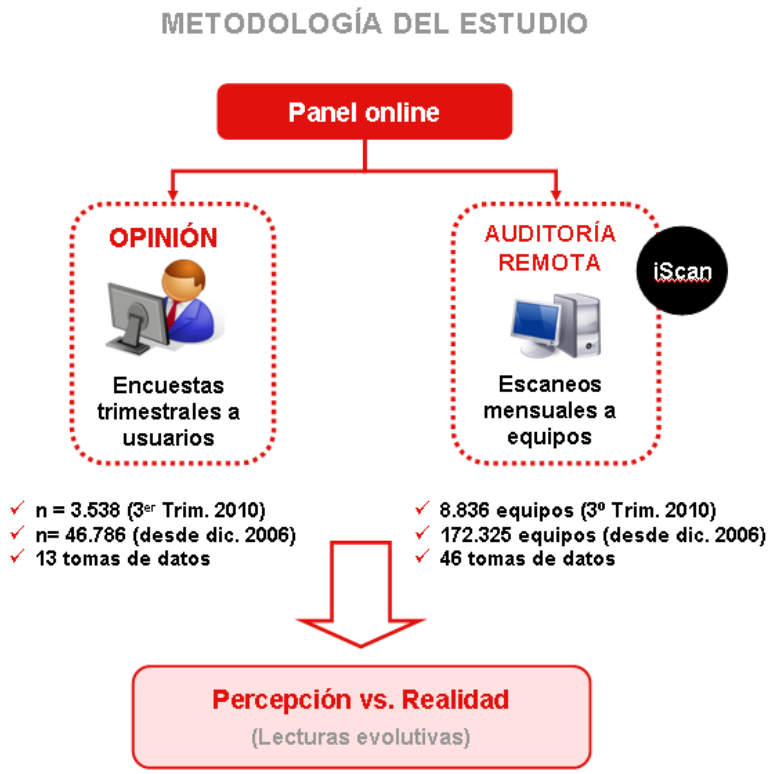
El presente informe constituye la decimotercera entrega del estudio, cuya primera lectura data de diciembre de 2006.

En la actualidad el panel está compuesto por 7.351 hogares con conexión a Internet repartidos por todo el territorio nacional. Sobre los miembros del panel se aplican dos técnicas diferenciadas, que permiten obtener dos tipos diferentes de información:

- Encuestas online a usuarios españoles de Internet mayores de 15 años con acceso frecuente desde el hogar, llevadas a cabo con una periodicidad trimestral. Los datos extraídos de las encuestas permiten obtener la percepción sobre la situación de la seguridad en Internet y nivel de e-confianza de los usuarios domésticos. En el período analizado en la presente entrega (3º trimestre de 2010), 3.538 usuarios han respondido a la encuesta. 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%, el error muestral para n=3.538 es de ±1,68%.

- Análisis online del nivel de seguridad real de los equipos informáticos existentes en los hogares, realizados mensualmente. Para ello, se utiliza el software iScan, desarrollado por INTECO, que analiza los sistemas y las incidencias de seguridad en los equipos gracias a la utilización conjunta de 46 motores antivirus. Este software se instala en los equipos y los analiza, detectando todo el malware residente en los mismos y recogiendo además datos del sistema operativo, de su estado de actualización y de las herramientas de seguridad instaladas. El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada. La muestra en este tercer trimestre de 2010 se compone de 3.846 hogares que escanearon online su ordenador entre julio y septiembre de 2010. El número total de análisis remotos de seguridad o escaneos realizados en el período ha sido 8.836.

Ilustración 4: Esquema de la metodología del estudio



Fuente: INTECO

La recogida de información responde al siguiente plan:

- Captación del panel dedicado, por medio de invitaciones por correo electrónico.
- Información del tipo de colaboración requerida, sistema de incentivos y condiciones de confidencialidad.
- 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.
- Control de cuotas según diseño muestral.

I Universo

Usuarios españoles de Internet mayores de 15 años con acceso frecuente a Internet desde el hogar. 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.

II Tamaño y distribución muestral

Para la encuesta, se ha extraído una muestra representativa de 3.538 usuarios de Internet, con participación estable en el panel en el trimestre comprendido entre julio y septiembre de 2010.

De la muestra se obtienen dos tipos diferentes de información: la proporcionada por los usuarios en las encuestas y la obtenida directamente mediante observación (análisis online de sus equipos). Dado que la periodicidad de extracción de datos es diferente (trimestral en el caso de las encuestas y mensual en el de los escaneos) y que las bases consideradas no son idénticas (por ejemplo, puede haber hogares en que se realice el análisis online pero no la encuesta, o viceversa), se presentan de forma separada: la Tabla 8 describe los tamaños muestrales de la encuesta y la Tabla 9 indica el número de equipos escaneados.

Tabla 8: Tamaños muestrales para las encuestas

Período	Fecha del trabajo de campo	Tamaño muestral
4º trimestre 2006	Diciembre de 2006 a enero de 2007	3.068
1er trimestre 2007	Febrero a abril de 2007	3.076
2º trimestre 2007	Mayo a julio de 2007	3.023
3er trimestre 2007	Agosto a diciembre de 2007	3.021
4º trimestre 2007	Agosto a diciembre de 2007	3.021
1er trimestre 2008	Enero a marzo de 2008	3.523
2º trimestre 2008	Abril a junio de 2008	2.860
3er trimestre 2008	*No disponible*	*n.d.*
4º trimestre 2008	*No disponible*	*n.d.*
1er trimestre 2009	Diciembre de 2008 a febrero de 2009	3.563
2º trimestre 2009	Marzo a mayo de 2009	3.521
3er trimestre 2009	Junio a septiembre de 2009	3.540
4º trimestre 2009	Octubre a diciembre de 2009	3.640
1er trimestre 2010	Enero a marzo de 2010	3.599
2º trimestre 2010	Abril a junio de 2010	3.519
3º trimestre 2010	Julio a septiembre de 2010	3.538

Fuente: INTECO

Tabla 9: Número de equipos escaneados mensualmente

Año 2007	Equipos escaneados	Año 2008	Equipos escaneados	Año 2009	Equipos escaneados	Año 2010	Equipos escaneados
Ene'07	2.910	Ene'08	4.659	Ene'09	5.649	Ene'10	4.079
Feb'07	2.979	Feb'08	4.450	Feb'09	4.325	Feb'10	3.751
Mar'07	2.839	Mar'08	3.893	Mar'09	4.695	Mar'10	4.024
Abr'07	4.618	Abr'08	4.102	Abr'09	4.954	Abr'10	3.746
May'07	3.389	May'08	4.610	May'09	4.677	May'10	3.499
Jun'07	3.408	Jun'08	3.889	Jun'09	4.293	Jun'10	3.279
Jul'07	3.701	Jul'08	3.187	Jul'09	3.971	Jul'10	3.337
Ago'07	3.552	Ago'08	2.793	Ago'09	3.677	Ago'10	2.716
Sep'07	3.003	Sep'08	2.617	Sep'09	4.520	Sep'10	2.783
Oct'07	4.523	Oct'08	2.421	Oct'09	4.294		
Nov'07	3.959	Nov'08	3.661	Nov'09	4.039		
Dic'07	3.376	Dic'08	4.286	Dic'09	4.452		

Fuente: INTECO

La afijación muestral responde a un modelo polietápico:

- Estratificación por Comunidades Autónomas para garantizar un mínimo de sujetos en cada una de ellas.
- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[18].

[18] 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: 19ª enero-marzo 2008")

Tabla 10: Distribución muestral por CCAA (%)

CCAA	Muestra obtenida 14ª oleada (julio-septiembre'10)	Muestra Teórica
Andalucía	15,8	15,2
Aragón	3,2	3,0
Asturias	2,8	2,5
Baleares	2,7	2,7
Canarias	4,4	4,7
Cantabria	1,7	1,3
Castilla-La Mancha	6,0	2,9
Castilla y León	3,1	5,4
Cataluña	14,8	18,5
Comunidad Valenciana	10,7	10,0
Extremadura	1,9	1,4
Galicia	6,1	4,5
La Rioja	0,8	0,7
Madrid	15,8	18,6
Murcia	2,7	2,5
Navarra	1,5	1,4
País Vasco	5,9	4,7

Base muestra julio 2010 – septiembre 2010 = 3.538 *Fuente: INTECO*

Aunque las desviaciones entre la muestra obtenida y la teórica han sido pequeñas, la muestra se ha equilibrado al universo en base a los datos poblacionales por CCAA, para el universo descrito anteriormente, y a las variables de cuota, para alcanzar un ajuste más perfecto.

En la Tabla 11 puede verse la distribución de las muestras en función de las variables demográficas usadas para establecer dichas cuotas.

Tabla 11: Distribución muestral por categorías sociodemográficas (%)

Concepto	Muestra obtenida 14ª oleada (julio-septiembre'10)	Muestra Teórica
Actividad		
Ocupados	53,8	71,7
Parado	18,2	4,6
Estudiantes	17,3	16,1
Jubilado	5,9	3,0
Otros Inactivos	4,7	4,6
Nivel de estudios		
Hasta primarios	9,9	*n.d.*
Secundarios	38,2	*n.d.*
FP de grado superior/Universitario Medio	35,0	*n.d.*
Universitarios superiores	13,6	*n.d.*
Tamaño hogar		
1	7,9	3,2
2	25,3	15,4
3	30,9	28,7
4 y mas	35,9	52,7
Tipo de hogar		
Sin pareja y con hijos	4,0	*n.d.*
En pareja y sin hijos	19,4	*n.d.*
En pareja y con hijos	32,5	*n.d.*
Con mis padres u otros familiares	32,0	*n.d.*
Comparto vivienda con personas que no son de mi familia	3,0	*n.d.*
Otro tipo de hogar	1,2	*n.d.*
Sexo		
Hombre	52,5	53,7
Mujer	47,5	46,3
Edad		
De 15 a 24 años	21,8	*n.d.*
De 25 a 34 años	28,2	*n.d.*
De 35 a 44 años	24,2	*n.d.*
De 45 a 54 años	15,9	*n.d.*
Más de 55 años	9,8	*n.d.*

Base muestra julio 2010 – septiembre 2010 = 3.538 *Fuente: INTECO*

Los datos finales de encuesta de esta oleada que son objeto de comparación con otras lecturas se han ponderado para ajustarse al mismo universo de estudio; son perfectamente homogéneos en cuanto a distribución geográfica, sexo, edad, tamaño del hogar y otras variables sociodemográficas relevantes. Es decir, no presentan variación en tales dimensiones a efectos del análisis.

III Captura de información

Entrevistas online y análisis de equipos informáticos a partir de un panel de usuarios de Internet.

El análisis de equipos informáticos se realiza con la herramienta iScan, un software multiplataforma propiedad de INTECO que se ha desarrollado en colaboración con la empresa de seguridad Hispasec. Este programa es transparente en todas sus versiones. La información que se recoge se trata anónimamente y de manera agregada.

A lo largo de todo el proceso se cumple estrictamente con la normativa vigente en materia de protección de datos de carácter personal.

iScan (INTECO Scanner)

La inspección realizada por iScan ha tenido en consideración, históricamente y de forma acumulada, los resultados de hasta 57 antivirus. Actualmente sólo se consideran 46. Esto es así porque existen motores que, con el paso del tiempo y por diferentes circunstancias (resultan redundantes, su marca ha desaparecido, etc) han ido siendo eliminados de la lista de motores válidos.

La herramienta de INTECO tiene como piedra angular una base de datos de más de 25 millones de archivos detectados por, al menos, uno de esos 46 antivirus. Esta base de datos está en constante crecimiento.

iScan compara todos los archivos de un sistema con la base de datos. Si el análisis detecta el archivo con 5 ó más antivirus, el fichero se considera potencialmente malicioso.

El uso de 46 antivirus asegura una mayor tasa de detección, pues ante las nuevas amenazas de carácter altamente indetectable es difícil que un espécimen escape a todos los motores.

El escaneo de iScan no da información sobre si un determinado código malicioso se encuentra activo en el sistema. Podría darse el caso de que un sistema aloja malware pero no se encuentra infectado. Imagínese, por ejemplo, que un investigador tiene un directorio con código malicioso para estudiar, su equipo sería catalogado por iScan como infectado pero dichas muestras nunca se habrían ejecutado en el sistema y por tanto no estaría infectado. Esto también ocurriría si un antivirus detecta un código malicioso y lo mueve a una carpeta de cuarentena sin ofuscarlo.

Con el fin de reducir el impacto de los falsos positivos se aplican una serie de filtros, que se explican a continuación:

Eliminación y ponderación de soluciones antivirus

a. *Eliminación de productos antivirus de perímetro que tras pruebas con grandes cantidades de malware y goodware[19] demostraron ser altamente paranoicos.*

b. *Eliminación de ciertas soluciones que comparten firmas, para sólo considerar un motor con el mismo conjunto de firmas.*

c. *Creación de un subconjunto de motores. Se han tomado los 11 antivirus más reputados (con mejor tasa de detección frente a especímenes detectados por más de 10 antivirus) para crear un subconjunto de productos que será referenciado como motores necesariamente exigidos. De este modo, para que un fichero sea marcado como malware, deberá ser detectado por 5 productos de los 46 considerados y, además, al menos uno de ellos deberá ser alguno de estos 11 motores exigidos.*

Verificación manual de un número acotado de ejemplares

El malware identificado se ordena por número de equipos en los que aparece cada ejemplar. Ante la imposibilidad de verificación de todos los ejemplares, se seleccionan los 50 ficheros más avistados y se analizan de forma manual mediante técnicas de análisis dinámico (monitorización de modificaciones de ficheros, registro y procesos, llamadas a funciones de la API de Windows, etc.) y estático (desensamblado y depurado). Este análisis busca determinar qué muestras han sido clasificadas incorrectamente como código malicioso una vez se ha llegado a esta fase del proceso de detección.

Contraste con bases de datos de software conocido y de ficheros inocuos

INTECO mantiene una base de datos de software de fabricantes confiables y de freeware[20] y shareware[21] confirmado como inocuo. Todos los ejemplares que siguen siendo detectados tras las dos primeras capas de filtrado son comparados con esta base de datos para eliminar más falsos positivos.

De igual forma, los ficheros son contrastados con la estadounidense National Software Reference Library del NIST (National Institute of Standards and Technology), base de datos de software conocido. Si se detectase que alguno de los ficheros señalados por iScan está en dicha base de datos y no forma parte de un kit de hacking o cracking, el archivo no será considerado como malicioso.

[19] Software y ficheros legítimos, archivos inocuos.

[20] Software gratuito.

[21] Software de descarga gratuita pero limitado en funcionalidad o tiempo de uso.

Eliminación de detecciones concretas y corrección de categorías incorrectamente determinadas

En primer lugar se elimina toda detección de la familia "Annihilator" porque se trata del nombre que emplean algunos antivirus para detectar (erróneamente) los ficheros legítimos del antivirus Panda. Las detecciones "WinVNC" y "VNCView" también son suprimidas pues designan una herramienta de gestión remota de equipos que -muy probablemente- puede haber sido instalada deliberadamente por el usuario.

Tras esto, se corrigen ciertas categorías de malware que fueron decididas de forma automática. Por ejemplo, todos los ficheros detectados como "shutdown", "patch", "wgapatch" y "keygen" son clasificados forzosamente como herramientas, con independencia de la categoría decidida por los antivirus.

Todos estos filtros son mejoras importantes de cara a la fiabilidad del estudio, pero no eliminan por completo la problemática de los falsos positivos (una problemática inherente a la industria antivirus).

Por otro lado, al exigir más condiciones de cara a marcar un fichero como malware, también se puede elevar la tasa de falsos negativos. Se trata de un compromiso entre capacidad de detección (utilización de varios antivirus) y detecciones incorrectas (falsos positivos).

En cualquier caso, a pesar de la fortaleza de la herramienta iScan y de las medidas adoptadas por INTECO para mitigar la incidencia de falsos positivos, se debe puntualizar que existen otras limitaciones intrínsecas a la metodología empleada que hacen que el análisis no sea infalible. Por ello, a pesar del rigor y robustez de nuestro análisis, los datos que el informe ofrece cuentan con un margen de error que da una perspectiva de los problemas actuales a los que se enfrenta la industria de seguridad a la hora de desarrollar sus programas antivirus.

IV Trabajo de campo

Realizado entre julio y septiembre de 2010.

V 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 participante período julio a septiembre de 2010: n= 3.538; error muestral ±1,68%.

Tabla 12: Errores muestrales de las encuestas (%)

Período	Tamaño muestral	Error muestral
Febrero a abril de 2007	3.076	±1,80%
Mayo a julio de 2007	3.023	±1,82%
Agosto a diciembre de 2007	3.021	±1,82%
Enero a marzo de 2008	3.523	±1,68%
Abril a junio de 2008	2.860	±1,87%
Julio a noviembre de 2008	*n.d.*	*n.d.*
Diciembre de 2008 a febrero de 2009	3.563	±1,68%
Marzo a mayo de 2009	3.521	±1,68%
Junio a octubre de 2009	3.540	±1,68%
Octubre a diciembre de 2009	3.640	±1,66%
Enero a marzo de 2010	3.599	±1,67%
Abril a junio de 2010	3.519	±1,68%
Julio a septiembre de 2010	3.538	±1,68%

Fuente: INTECO

VI Consistencia y robustez de la muestra

La consistencia de la muestra, en términos de un posible sesgo de auto-selección por motivo de aceptar el escaneo del equipo por parte del panelista, se analizó detalladamente al inicio del estudio, coincidiendo con la puesta en marcha del panel, concluyendo que la muestra no presenta sesgos significativos en este aspecto.

Para comprobar la robustez de los datos se realiza un seguimiento de los resultados tanto de escaneo como de encuestas a lo largo de la vida del panel.

- Los resultados obtenidos en cuanto a hábitos, opiniones y actitudes, así como el panel de indicadores de seguridad, muestran una consistencia considerable, que se corresponde con variables que se modifican con cierta lentitud en condiciones ambientales estables. Esta consistencia puede comprobarse extensamente a lo largo del informe de esta decimocuarta oleada, que compara el período julio-septiembre de 2010 con oleadas anteriores.

- Los datos de escaneo expresados como el porcentaje de detecciones del malware en los meses de vida del panel desde sus comienzos evidencian 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 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.

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 cómo están evolucionando las incidencias detectadas en los usuarios.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

http://www.inteco.es

OBSERVATORIO
INTECO

http://observatorio.inteco.es

	Canal Twitter del Observatorio de la Seguridad de la Información: http://twitter.com/ObservaINTECO
BLOG	Blog del Observatorio de la Seguridad de la Información: http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad/
	observatorio@inteco.es