



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

PLAN
AVANZA2010



Instituto Nacional
de Tecnologías
de la Comunicación

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

1^{er} trimestre de 2010 (12^a oleada)



Edición: Agosto 2010

El informe de la 12ª 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

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

SIGMADOS



La presente publicación pertenece al **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** y está bajo una licencia Reconocimiento-No comercial 2.5 España de Creative Commons, y por ello esta permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento:** El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INTECO como a su sitio web: www.inteco.es. Dicho reconocimiento no podrá en ningún caso sugerir que INTECO presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial:** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INTECO como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de INTECO. <http://creativecommons.org/licenses/by-nc/2.5/es/>

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format). Así, se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página <http://www.inteco.es>

ÍNDICE

PUNTOS CLAVE	6
I Medidas y hábitos de seguridad	6
II Incidencias de seguridad	7
III Consecuencias de las incidencias de seguridad y reacción de los usuarios ante ellas 7	
IV e-Confianza de los hogares españoles.....	8
1 INTRODUCCIÓN Y OBJETIVOS	9
1.1 Presentación	9
1.1.1 Instituto Nacional de Tecnologías de la Comunicación	9
1.1.2 Observatorio de la Seguridad de la Información.....	10
1.2 Estudio sobre la seguridad de la información y e-confianza en los hogares españoles.....	11
1.2.1 Objetivo general.....	11
1.2.2 Objetivos específicos	12
2 DISEÑO METODOLÓGICO	14
3 MEDIDAS Y HÁBITOS DE SEGURIDAD.....	16
3.1 Medidas de seguridad.....	16
3.1.1 Medidas automatizables y no automatizables: nivel de implantación y evolución	16
3.1.2 Estimaciones a futuro.....	20
3.1.3 Motivos alegados para no utilizar medidas de seguridad	22
3.1.4 Frecuencia de actualización y aplicación.....	24
3.2 Hábitos seguros de comportamiento en Internet	26
3.2.1 Navegación por Internet.....	26
3.2.2 Correo electrónico.....	28

3.2.3	Chats y mensajería instantánea.....	30
3.2.4	Banca en línea y comercio electrónico	31
3.2.5	Redes P2P	33
3.2.6	Redes sociales.....	34
3.3	Hábitos de seguridad en hogares con menores	37
3.3.1	Medidas coercitivas y de control	37
3.3.2	Medidas de comunicación, diálogo y educación.....	39
3.3.3	Medidas de implicación del padre en la navegación del hijo	40
4	INCIDENCIAS DE SEGURIDAD	42
4.1	Incidentes de seguridad por malware o código malicioso: conceptos previos .	43
4.2	Incidentes detectados	45
4.2.1	Evolución de las incidencias de malware.....	45
4.2.2	Tipología del código malicioso detectado	47
4.2.3	Diversificación del código malicioso detectado.....	49
4.2.4	Peligrosidad del código malicioso y riesgo del equipo.....	52
5	CONSECUENCIAS DE LAS INCIDENCIAS DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS ANTE ELLAS	55
5.1	Consecuencias de las incidencias de seguridad	55
5.2	Cambios adoptados tras una incidencia de seguridad	57
5.2.1	Cambios en las medidas o herramientas de seguridad	57
5.2.2	Cambios en el uso de servicios de Internet	58
5.3	Resolución de incidentes de seguridad	59
6	E-CONFIANZA DE LOS HOGARES ESPAÑOLES	61
6.1	e-Confianza en la Sociedad de la Información	61
6.2	Evolución de la percepción de la seguridad en Internet por parte de los usuarios	

6.3	Autorregulación vs. Tutelaje	68
6.3.1	Usuarios	68
6.3.2	Papel de la administración en la garantía de la Seguridad de la Información	70
6.3.3	Papel de otros actores en la garantía de la seguridad de la información	76
7	SISTEMA DE INDICADORES DE LA SEGURIDAD DE LA INFORMACIÓN	78
7.1	Estructura y objetivos del sistema	78
7.2	Análisis de los indicadores de la seguridad de la información	79
7.2.1	Indicador de herramientas y medidas de seguridad	80
7.2.2	Indicador de conductas y hábitos de seguridad	82
7.2.3	Indicador de e-confianza	84
7.2.4	Indicador de incidencias de malware	86
7.2.5	Indicador de ordenadores con riesgo alto	87
7.2.6	Indicador de ordenadores con diseminación potencial alta	87
8	CONCLUSIONES	89
	ANEXO I: DISEÑO METODOLÓGICO DETALLADO	92
I	Universo	93
II	Tamaño y distribución muestral	94
III	Captura de información	98
IV	Trabajo de campo	100
V	Error muestral	100
VI	Consistencia y robustez de la muestra	101
	ÍNDICE DE GRÁFICOS	103
	ÍNDICE DE TABLAS	107
	ÍNDICE DE ILUSTRACIONES	108

PUNTOS CLAVE

El presente informe constituye una nueva entrega 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 enero a marzo de 2010. Durante este tiempo se han realizado 3.599 encuestas y 11.854 análisis online a los 5.212 equipos que componen el panel.

Se exponen a continuación los puntos clave del análisis.

I Medidas y hábitos de seguridad

Como viene siendo habitual en trimestres anteriores, los antivirus son la herramienta de seguridad que más han declarado usar los panelistas, con un 92,3%, seguida de los cortafuegos (81,4%) y las actualizaciones del sistema operativo y programas (80,7%). El uso de contraseñas, utilizado por el 80% de los usuarios, es otra de las medidas de seguridad ampliamente extendidas entre los usuarios de Internet.

La mayoría de los usuarios delega en el sistema operativo la función de actualización, de forma que un 82,3% dice que es el propio sistema el que gestiona las actualizaciones de forma automática. Este dato confirma una tendencia, lenta pero constante, hacia la automatización de las actualizaciones.

Lo mismo se puede afirmar respecto a la frecuencia de análisis completo del equipo con el antivirus: los usuarios españoles confían en el propio producto para realizar el escaneo, y así una inmensa mayoría (64,2%) delega en el antivirus el chequeo del ordenador, con la periodicidad que la herramienta lo ejecute.

En general, en el manejo de la Red por parte de los hogares españoles predominan los hábitos de uso prudentes sobre los arriesgados. En el 1^{er} trimestre de 2010, un 84,4% de los panelistas afirma no responder a correos electrónicos sospechosos de ser falsos y un 85,3% rechaza invitaciones de mensajería instantánea o mensajes de personas desconocidas. En el contexto de banca y compraventa electrónicas, hasta un 83,6% de los usuarios de Internet españoles sigue la buena práctica de cerrar sesión después de realizar transacciones online, y cada vez más usuarios (un 74,7%) comprueban que están utilizando una conexión segura al realizar una transacción online.

Menos prudentes se muestran los usuarios en las redes P2P, y más concretamente cuando se trata de gestionar los privilegios de acceso. Sólo el 37,3% de los encuestados

reconoce hacer funcionar el equipo con permisos limitados. El dato, muy mejorable, muestra no obstante una evolución positiva continuada desde el 1^{er} trimestre de 2009, período en el que sólo el 29,4 de los usuarios de redes P2P afirmaban hacer uso de cuenta sin privilegios de administrador para conectarse al *peer to peer*.

Los usuarios españoles de redes sociales son cuidadosos con su privacidad, y así un 65% admite que sólo sus contactos pueden tener acceso a su perfil. Más restrictivos aún se muestran el 14,9% que manifiestan que sólo algunos de sus contactos pueden visualizar su perfil.

II Incidencias de seguridad

El spam o correo electrónico no deseado sigue siendo el incidente que a más usuarios afecta, con un 68,4% que afirma haberlo recibido alguna vez en los últimos 3 meses. La realidad, según los datos ofrecidos por la red de sensores de INTECO, es que el 93,7% del correo electrónico de marzo de 2010 es spam.

Por detrás del correo electrónico no deseado se encuentra el código malicioso: un 29,5% de usuarios dicen haber sufrido algún tipo de virus o malware en los últimos tres meses. El dato real para marzo proporcionado por iScan sitúa el nivel de infección en el 52,8%, lo que constituye un nuevo mínimo histórico de nivel de infección real (los informes correspondientes al tercer y cuarto trimestres de 2009 anunciaban también, respectivamente, mínimos históricos). Se trata de un dato muy positivo, y confirma la tendencia a la reducción del volumen de equipos infectados.

Los troyanos (34,6%) y el adware (30,4%) siguen siendo el código malicioso más detectado. La razón es clara: permiten lucrarse a los atacantes de forma rápida y directa. No ocurre lo mismo con el spyware o programas espías que, si bien permite lucrarse a sus creadores, se mantiene en mínimos de detección (2%)

Gracias a la bajada continua del nivel de infección, el nivel de riesgo en los equipos de los internautas españoles se mantiene en niveles moderados: en marzo de 2010 el porcentaje de ordenadores considerados de riesgo alto es de 34,9%, lo que supone un mínimo histórico.

La diversificación del malware continúa en este trimestre, y se observa sobre todo en la categoría de troyanos y adware.

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

El 41,2% de los usuarios declaran haber modificado sus hábitos en los últimos 3 meses como consecuencia de los incidentes de seguridad sufridos, frente al 58,8% que mantiene sus hábitos inalterables.

Los cambios se dirigen a dos áreas, principalmente (en mayor medida al primer grupo de acciones que al segundo): en primer lugar, se modifican las medidas o herramientas de seguridad que utilizan; en segundo lugar, se cambian de algún modo los hábitos del usuario en el uso de Internet.

¿Cómo resuelven los hogares españoles sus incidentes de seguridad? Se observa en este trimestre una enorme escalada de los usuarios que son capaces de resolver las incidencias por sí mismos: un 46,3% de panelistas así lo reconoce, lo que supone un incremento de 12 puntos porcentuales respecto al dato del 2º trimestre de 2009 (primero de la serie en el que se analiza esta variable). Los usuarios son cada vez más autónomos a la hora de buscar información y encontrar solución a los problemas de seguridad.

IV e-Confianza de los hogares españoles

A un 38,3% de usuarios Internet les genera *bastante* confianza, y a un 8,5%, *mucha*. Si añadimos el porcentaje de ciudadanos que reconocen que Internet les produce un nivel de confianza *suficiente* (43,2%), el resultado es que un 90% de los encuestados confía en la Red. Sólo un 9,2% admite tener *poca* confianza y un 0,7% adicional, *ninguna*.

Un 82,4% de los ciudadanos encuestados se muestran de acuerdo con la afirmación *Considero que mi ordenador está razonablemente protegido*, sin que existan cambios significativos desde hace un año.

En el caso de la afirmación *Internet es cada día más seguro*, un 49,2% de los usuarios de Internet se muestran de acuerdo con la sentencia. En este caso, trimestre tras trimestre se incrementa el porcentaje de ciudadanos que comparte esta opinión, lo que puede constituir un síntoma favorable de la adecuada evolución de la Sociedad de la Información.

Un 81,9% está *totalmente de acuerdo* o *de acuerdo* en que la Administración debe implicarse en este sentido para mejorar la seguridad, y solo un 3,3% no lo encuentra adecuado. Entre las medidas más demandadas a la Administración se encuentra, en primer lugar, la vigilancia cercana de lo que está pasando en Internet (28,4%). Por detrás de esta actuación, los ciudadanos requieren el desarrollo de herramientas de seguridad gratuitas que le permitan asegurar sus equipos y comunicaciones (25,9%). Como tercera opción, piensan que se deberían actualizar y reformar las leyes relativas a los delitos por Internet (11,7%).

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

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 duodécima 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.

Todo ello, con el fin de impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe pretende 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 duodécima entrega del estudio, cuya primera lectura data de diciembre de 2006.

En la actualidad el panel está compuesto por 5.212 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 (1º trimestre de 2010), 3.599 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 $n=3.599$ es de $\pm 1,66\%$.
- Auditoría remota online del nivel de seguridad real de los equipos informáticos existentes en los hogares, realizados mensualmente. Para ello, se utiliza el software iScan¹, 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 primer trimestre de 2010 se compone de 5.212 hogares que escanearon online su ordenador entre enero y marzo de 2010. El número total de análisis remotos de seguridad o escaneos realizados en el período ha sido 11.854.

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

Internet y las redes suponen un mundo no exento de riesgos. Para poder hacer un uso confiado de las tecnologías es necesario un correcto nivel de seguridad en los sistemas implicados. Es necesaria una seguridad adecuada, basada en unas medidas y hábitos responsables y en unas herramientas suficientes, para que los ciudadanos aumenten su confianza en el mundo de las nuevas tecnologías.

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 medidas que cree tener instaladas en su equipo y los resultados ofrecidos por iScan, 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 aquéllas 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 las medidas de seguridad mencionadas, agrupadas en automatizables (sombreadas) y no automatizables. En la columna derecha (para las herramientas en las que es posible), se contrasta el dato con el resultado obtenido por iScan, esto es, la realidad de la implantación de la herramienta.

Como viene siendo habitual, los antivirus son la herramienta de seguridad que más han declarado usar los panelistas, con un 92,3%, seguida de los cortafuegos (81,4%) y las actualizaciones del sistema operativo y programas (80,7%). El uso de antivirus y cortafuegos está culturalmente arraigado en los usuarios de Internet. Durante la expansión de la Red, suponían una de las pocas herramientas disponibles para proteger

los sistemas informáticos. Suelen estar siempre situadas en lo más alto de las declaraciones de uso de herramientas.

Desde que Microsoft introdujo en 2001 las actualizaciones automáticas, son cada vez más los usuarios que mantienen su sistema operativo actualizado. De hecho, desde 2009, se viene observando una tendencia cada vez mayor de diferentes programas a incluir actualizaciones automáticas entre sus funcionalidades, evitando así delegar esta responsabilidad en el usuario: Adobe, Flash, Opera, Firefox, etc, son solo algunos ejemplos de programas que permiten actualizar automáticamente su software.

El uso de contraseñas, utilizado por el 80% de los usuarios, es otra de las medidas de seguridad ampliamente extendidas entre los usuarios de Internet.

A la cola del uso de herramientas declarada por los panelistas se encuentra el DNI electrónico. En este trimestre sin embargo, aumenta considerablemente el uso (en comparación con el trimestre anterior), y casi un 20% de usuarios declara que lo utiliza.

¿Qué beneficios aporta el DNI electrónico?

El DNI electrónico tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo, al igual que el DNI tradicional. La gran ventaja del DNI electrónico es que permite la firma electrónica de documentos de forma cómoda para todos los ciudadanos. La Firma electrónica es un sistema de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma manuscrita, autenticando las comunicaciones generadas por el firmante. Al ser aceptado por todas las Administraciones Públicas, permite hacer operaciones online de forma segura, tales como hacer la declaración de la renta, pedir un certificado de empadronamiento, dar de alta en el registro de nacimientos o reclamar el derecho a la pensión...etc.

Tabla 1: Utilización declarada y real de medidas de seguridad automatizables y no automatizables 1T2010 (%)

Medidas de seguridad ²	Declarado 1T 10	Real Mar. 10
Programas antivirus	92,3%	85,6%
Cortafuegos o firewall	81,4%	
Actualizaciones del SO y programas	80,7%	63,4%
Contraseñas (equipos y documentos)	80,0%	
Eliminación de archivos temporales y cookies	78,9%	
Programas de bloqueo de ventanas emergentes	74,5%	
Programas anti-spam	67,8%	
Programas anti-espía	65,0%	
Copias de seguridad de archivos	63,3%	
Copia discos de restauración del sistema	60,6%	
Partición del disco duro	49,0%	
Búsqueda información sobre seguridad informática	48,7%	
Programas de control parental ³	35,1%	
Utilización habitual con permisos reducidos	38,5%	19,9%
Programas anti-fraude	38,3%	
Certificados digitales de firma electrónica	28,0%	
Cifrado de documentos o datos	21,7%	
DNI electrónico	19,9%	

Base: Total usuarios (n=3.599)

Fuente: INTECO

Se analiza a continuación el contraste entre percepción y realidad observado en algunas medidas:

- Los programas antivirus están instalados en un 85,6% de los equipos auditados; según declaraciones de los usuarios, en un 92,3%. En este caso, la brecha entre percepción y realidad no es excesiva.
- El sistema operativo está efectivamente actualizado en un 63,4% de los ordenadores; según declaraciones de los usuarios, un 80,7%. Existen 17 puntos porcentuales de diferencia entre la percepción de los usuarios y la realidad. Un equipo sin actualizar es un equipo expuesto a todo tipo de malware. Es importante que el usuario revise, al menos mensualmente, si su equipo se encuentra realmente actualizado. Para ello, se recomienda visitar la página oficial de Microsoft: www.windowsupdate.com.

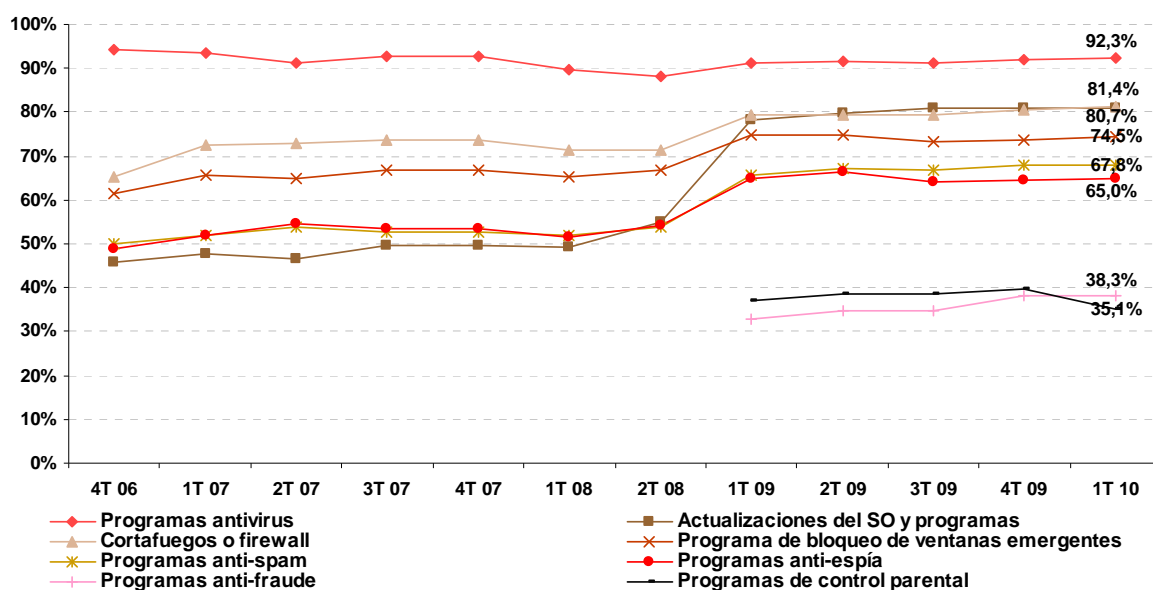
² Las medidas automatizables aparecen sombreadas.

³ Los datos referentes a los programas de filtro de contenidos (control parental para menores) se presentan sobre la muestra de usuarios con hijos menores que se conectan a Internet (19,3%).

- Se utilizan permisos reducidos en un 19,9% de los equipos; según declaraciones de los usuarios, en un 38,5%. En este dato es donde se observa la mayor discrepancia entre realidad y percepción (casi 20 puntos de diferencia). Utilizar el sistema como administrador para las tareas habituales puede resultar comprometido desde el punto de vista de la seguridad y estabilidad del equipo.

En el Gráfico 1 se puede determinar la evolución de las medidas automatizables. Con excepción del ligero descenso experimentado en este último trimestre en la adopción de programas de control parental, no se aprecian fuertes oscilaciones en el uso de las herramientas analizadas. En general, desde comienzos de 2009 los niveles de utilización declarada de medidas de seguridad automatizables se han mantenido bastante estables.

Gráfico 1: Evolución de la utilización declarada de medidas de seguridad automatizables⁴
(%)



Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

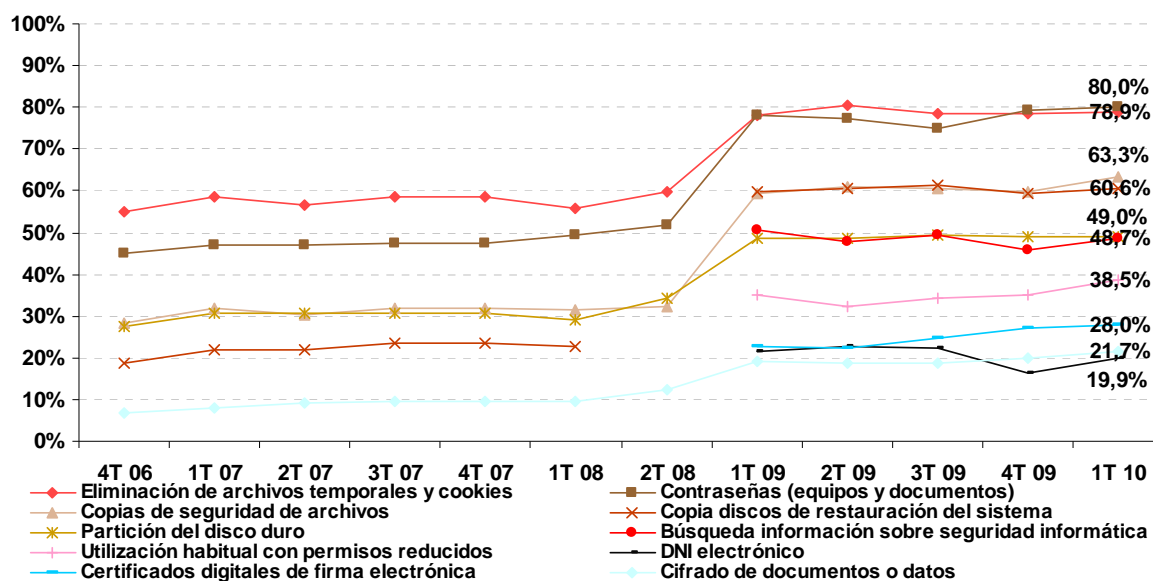
En el siguiente gráfico se observa la evolución de las herramientas clasificadas como no automatizables. También en este caso el comportamiento es bastante estable desde principios de 2009, con unos niveles de utilización declarada de contraseñas y de eliminación de cookies de alrededor del 80%. Las copias de seguridad de archivos (63,3%, en ligero repunte desde la lectura del 4º trimestre de 2009) y la realización de copia de los discos de restauración del sistema (60,6%) también son prácticas extendidas entre los usuarios domésticos. Destacan los crecimientos continuados del uso del equipo

⁴ 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 (19,3%).

con permisos reducidos (que en el 1^{er} trimestre de 2010 alcanza a un 38,5% de los encuestados) y del empleo de certificados digitales de firma electrónica (28%).

La utilización del DNI electrónico experimenta un ligero repunte con respecto a los datos del trimestre anterior, y se sitúa en un nivel de adopción cercano al 20%.

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



Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

3.1.2 Estimaciones a futuro

El Gráfico 3 muestra la intención declarada de uso de las medidas de seguridad automatizables en los tres meses siguientes a la realización de la encuesta. Las herramientas con menor nivel de adopción en el presente son aquellas que los panelistas tienen intención de incorporar en el futuro. Así, un 22,2% de los usuarios pretende usar un programa anti-fraude en los próximos 3 meses, un 20,3% manifiesta tener intención de utilizar los controles parentales y un 13,7% un programa anti-espías.

Gráfico 3: Intención declarada de uso de medidas de seguridad automatizables en los próximos 3 meses (datos del 1T 2010) (%)



Base: Total usuarios (n=3.599)

Fuente: INTECO

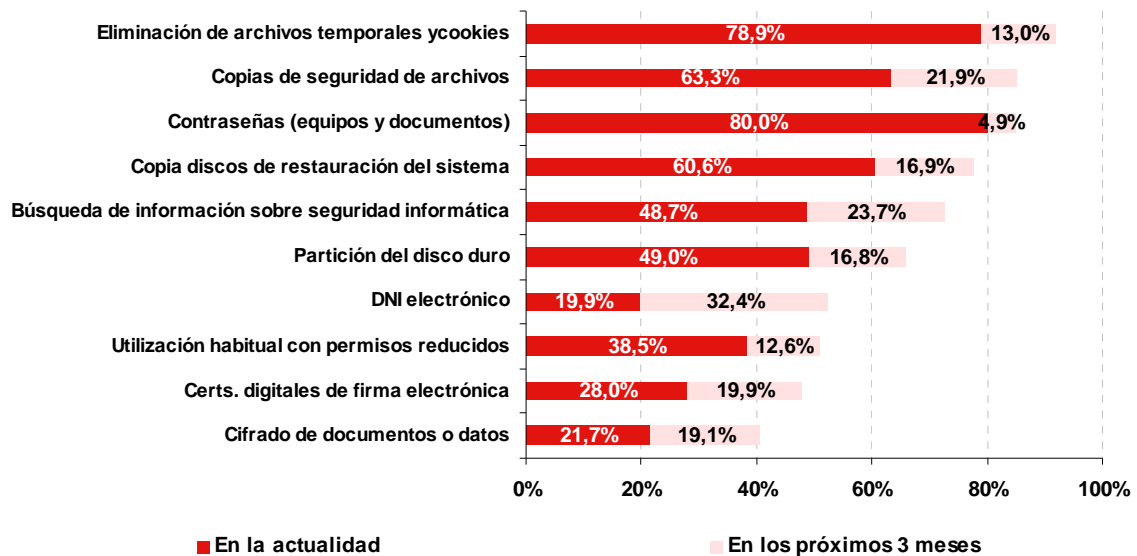
El Gráfico 4 reproduce el mismo análisis para las medidas no automatizables.

Una vez más, destaca la intención de incorporación del DNI electrónico a tres meses vista por parte de un 32,4% de usuarios.

Los ciudadanos se muestran proactivos a la incorporación del hábito de buscar información sobre seguridad de la información (un 23,7% declara tener pensado llevarlo a cabo en los tres meses siguientes a la realización de la encuesta) y a la realización de copias de seguridad de archivos importantes (21,9%).

En cierto modo relacionado con el DNI electrónico, el uso de certificados digitales y cifrado de documentos también es una medida de seguridad que los usuarios desean poner en práctica en un 19,9 y 19,1% respectivamente.

Gráfico 4: Intención declarada de uso de medidas de seguridad no automatizables en los próximos 3 meses (datos del 1T 2010) (%)



Base: Total usuarios (n=3.599)

Fuente: INTECO

3.1.3 Motivos alegados para no utilizar medidas de seguridad

A los usuarios que reconocen no utilizar en el presente, ni tener intención de incorporar a tres meses vista, cada una de las medidas analizadas, se les pregunta cuáles son los motivos para ello.

La Tabla 2 muestra los motivos alegados por los encuestados para no adoptar medidas automatizables.

Entre los poquísimos encuestados que no tienen intención de utilizar los antivirus (sólo un 4%), casi la mitad de ellos dice no necesitarlos. No está de más recordar que el empleo de estas herramientas es una capa de seguridad necesaria para combatir el malware, con independencia del sistema operativo del equipo.

El desconocimiento es lo que lleva a los usuarios a no utilizar muchas de las medidas de seguridad automatizables analizadas. Así, un 41,4% de los que no tienen intención de incorporar programas antifraude reconocen que es el desconocimiento de la herramienta lo que frena su uso. No conocer las herramientas es también el motivo mayoritario declarado por los panelistas que no usan cortafuegos (26,2%), programas de bloqueo (29,8%) y programas anti-espía (32,1%).

Una posibilidad es que los usuarios desconozcan estas medidas porque se encuentran integradas en suites antivirus módulos antifraude, anti-espía, etc. Cada vez más, los programas antivirus abarcan todas las modalidades posibles de malware, por lo que los usuarios tienden a usar una sola herramienta que lo integre todo.

Tabla 2: Motivos para no aplicar medidas de seguridad automatizables 1T2010 (%)

Medidas	% hogares que no tienen intención de utilizar	Motivos						
		No conoce	No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros
Programas antivirus	4,0%	2,7	49,4	10,3	12,7	0,2	4,7	20,0
Actualizaciones del SO y programas	7,9%	24,6	11,8	13,3	17,6	1,4	5,4	26,0
Cortafuegos o firewall	10,9%	26,2	18,3	9,8	21,6	0,2	7,6	16,3
Programas de bloqueo de ventanas emergentes	14,8%	29,8	13,6	7,5	21,6	3,8	8,2	16,5
Programas anti-spam	19,8%	17,3	27,8	9,3	14,7	1,8	11,5	17,7
Programas anti-espía	21,3%	32,1	14,6	9,2	14,8	3,8	9,9	15,5
Programas anti-fraude	39,5%	41,4	17,7	8,4	8,6	1,4	8,3	14,1
Programas de control parental ⁵	44,7%	13,2	47,5	3,6	10,1	1,1	11,1	13,5

Base: Usuarios que no tienen intención de utilizar cada medida

Fuente: INTECO

La Tabla 3 profundiza en los motivos de los usuarios para no aplicar las medidas de seguridad no automatizables.

La eliminación de archivos temporales y cookies es una medida muy extendida. Entre los pocos usuarios (solo un 8,1%) que reconocen no tener intención de adoptarla, es el desconocimiento el principal motivo en un 48% de las ocasiones.

También en el caso de uso de contraseñas, son minoría (15,1%) quienes afirman no mostrar intención de incorporar su utilización a corto plazo. Entre ellos, el 55,5% reconoce no necesitar esta medida. (Puede ser el caso, por ejemplo, de que el ordenador personal en los hogares sea usado siempre por una única persona, o que sea compartido entre miembros de la familia. La relación de confianza en este caso puede hacer creer innecesario el uso de contraseñas para la protección de documentos. Incluso en este caso, es recomendable proteger datos importantes con contraseñas.)

Del 22,5% de los encuestados que no tienen intención de realizar copias de seguridad (backup) de los archivos importantes, el 29,3% apela al desconocimiento de la medida para no hacerlo. (Ello a pesar de existir herramientas que permiten realizar copias de seguridad, algunas de ellas integradas en Windows).

Una partición separada para el sistema en el disco duro puede prevenir el daño en caso de desastre y facilitar la recuperación de datos. Sin embargo, un amplio 43,6% (del

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 (19,3%).

34,2% de los usuarios que no tienen intención de aplicar la medida) alega que no la conoce.

Aunque suponga una de las medidas de seguridad más eficaces, un 37,3% de los que no utilizan habitualmente el sistema con permisos reducidos alega que no necesita esta práctica. Es importante seguir realizando labores de concienciación para inculcar al usuario la importancia de la medida y el impacto positivo que podría suponer para la seguridad y estabilidad del sistema.

Tabla 3: Motivos para no aplicar medidas de seguridad no automatizables en 1T2010 (%)

Medidas	% hogares que no tienen intención de utilizar	Motivos						
		No conoce	No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros
Eliminación archivos temporales y cookies	8,1%	48,0	7,1	2,3	7,4	2,2	12,2	20,8
Contraseñas (equipos y documentos)	15,1%	6,9	55,5	0,7	12,1	0,9	6,8	17,1
Copia discos de restauración del sistema	22,5%	31,9	16,6	3,4	4,6	0,9	7,3	35,4
Copia de seguridad de archivos	22,5%	29,3	25,8	3,8	5,4	0,2	7,8	27,7
Búsqueda información sobre seguridad informática	27,5%	24,9	22,3	4,4	4,1	2,7	6,8	34,9
Partición del disco duro	34,2%	43,6	16,0	2,0	6,1	0,7	4,4	27,2
DNI electrónico	47,7%	20,6	21,5	3,4	3,1	5,2	6,9	39,2
Utilización habitual con permisos reducidos	49,9%	26,7	37,3	1,1	11,5	0,7	4,9	17,8
Certificados digitales de firma electrónica	52,1%	42,1	18,5	2,9	3,1	2,3	4,8	26,4
Cifrado de documentos o datos	59,9%	41,6	23,5	2,2	6,1	1,0	4,0	21,6

Base: Usuarios que no tienen intención de utilizar cada medida

Fuente: INTECO

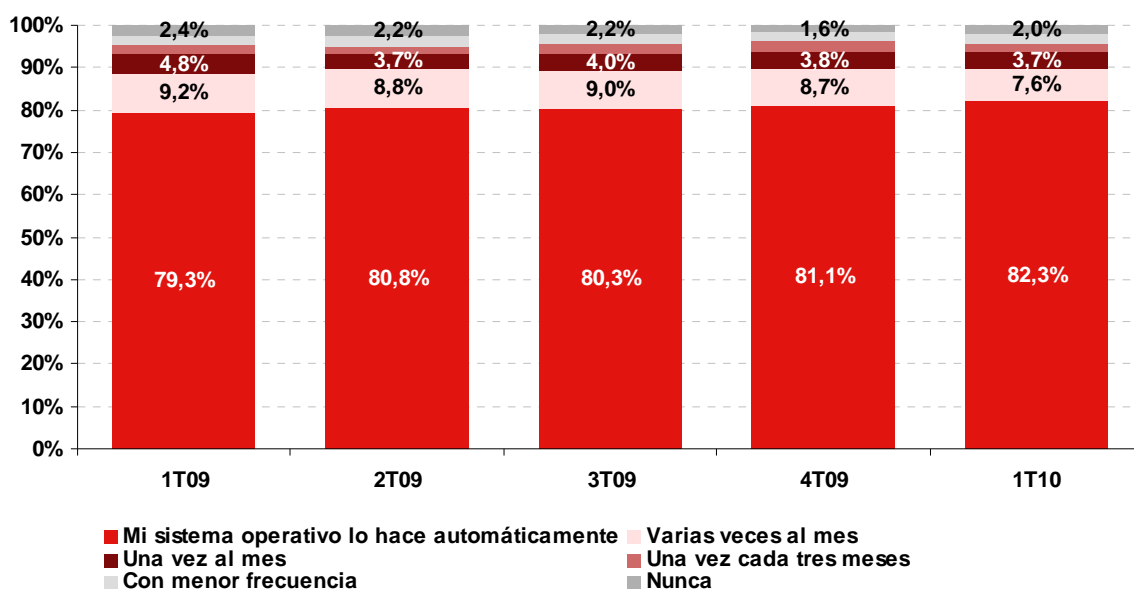
3.1.4 Frecuencia de actualización y aplicación

Las aplicaciones son actualizadas constantemente por parte de los fabricantes. En ocasiones se trata de actualizaciones destinadas a mejorar el producto, corregir errores o incluir nuevas funcionalidades. En el caso de las herramientas de seguridad, además, las actualizaciones permiten hacer frente a las nuevas amenazas. Por tanto es imprescindible que los programas se encuentren convenientemente actualizados en todo momento para ofrecer una máxima protección al usuario doméstico.

En el siguiente gráfico se puede observar la evolución de la frecuencia declarada de comprobación de la actualización de las diferentes herramientas de seguridad. La mayoría de los usuarios delega en el sistema operativo la función de actualización, de forma que un 82,3% dice que es el propio sistema el que gestiona las actualizaciones de

forma automática. Se observa una línea ascendente en este sentido, lenta pero constante, hacia la automatización de las actualizaciones.

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



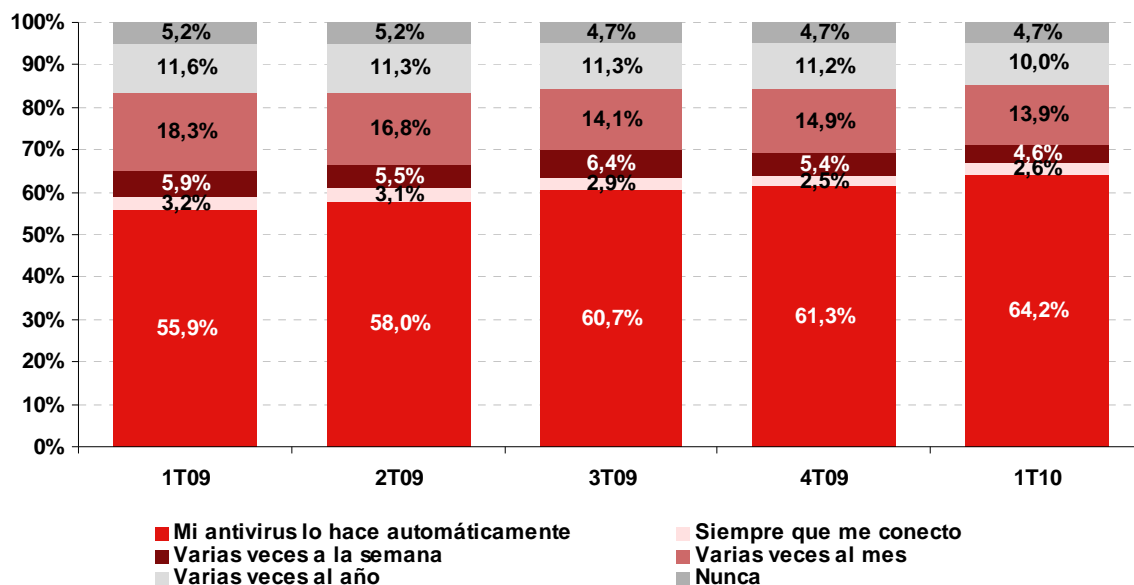
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

En el Gráfico 6 se estudia la evolución de la frecuencia de escaneo del ordenador con el programa antivirus. Para mantener estándares adecuados de protección, es necesario realizar un análisis del sistema operativo cada cierto tiempo, con el objetivo de buscar nuevas amenazas. La mayoría de los antivirus permiten realizar un análisis completo del disco duro del sistema para buscar archivos que han podido pasar desapercibidos en un momento dado durante el manejo de estos ficheros pero que, una vez actualizada su base de datos, podrían ser detectados como malware.

Los usuarios españoles confían en el propio producto para realizar el análisis, y así una inmensa mayoría (64,2%) delega en el antivirus el escaneo del equipo, con la periodicidad que la herramienta lo ejecute. Como aparece reflejado en el Gráfico 6, la proporción de quienes confían en el análisis automático del antivirus aumenta cada trimestre. (En la mayoría de los antivirus comerciales, el escaneo se realiza una vez al día, con lo que se puede considerar que supone una buena medida de seguridad permitir al antivirus realizar su trabajo de forma automática.)

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



Base: Total usuarios (n=3.599 en 1T10)

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 desacuerdo con la afirmación.

3.2.1 Navegación por Internet

Con respecto a la navegación por Internet, se analizan tres comportamientos prudentes:

- Pincho en todos los anuncios interesantes o atractivos, aunque no conozca al anunciante (*en desacuerdo*).
- Analizo, manual o automáticamente, con un antivirus todo archivo que descargo de Internet antes de abrirlo / ejecutarlo.
- 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*).

Cabe recordar que en las afirmaciones en las que se añade “en desacuerdo”, indica que el porcentaje de usuarios indicado no realiza esas prácticas a la hora de navegar en la Red y evitan así comportamientos que podrían derivar en situaciones peligrosas para su sistema y datos.

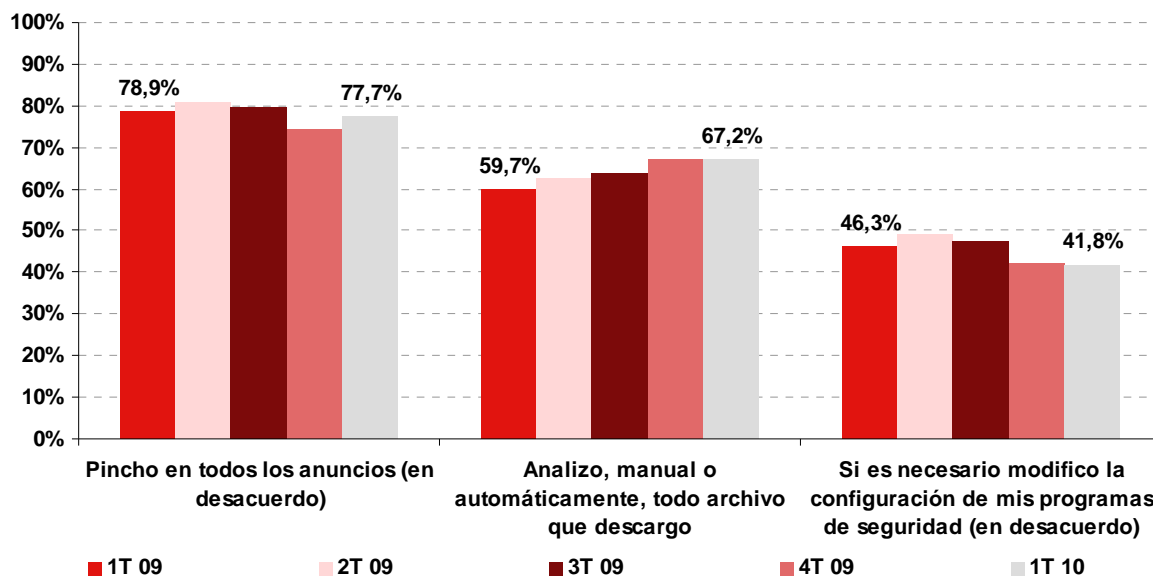
Remonta ligeramente, con respecto a los datos del 4º trimestre de 2009, el porcentaje de usuarios que se muestra en desacuerdo con pinchar en todos los anuncios. Así, en este 1er trimestre de 2010 un 77,7% de usuarios reconoce que no pincha indiscriminadamente en cualquier publicidad.

Se estabiliza el aumento de usuarios que analizan, manual o automáticamente, todo archivo descargado de la Red: un 67,2% de usuarios que declaran realizar esta práctica. Ello supone un avance constante y mantenido de esta buena práctica desde el 1er trimestre de 2009, momento en que un 59,7% de los encuestados señalaban seguir este comportamiento.

Para que esta práctica resulte totalmente efectiva, el análisis manual o automático de los ficheros descargados debe incluir todos los formatos de archivo (ejecutables, ofimáticos, PDF, etc.), puesto que todos pueden suponer una amenaza si son abiertos con software vulnerable. Además, debe incluirse en el análisis no solo los archivos descargados por web, sino también los que llegan por correo electrónico, los obtenidos a través del intercambio de archivos en redes, memorias USB, etc.

Por último, el porcentaje de usuarios que declara que no está de acuerdo con la afirmación “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” baja ligeramente y se sitúan en un 41,8% de los encuestados. En este caso, la evolución experimentada desde comienzos de 2009 es de signo negativo: los usuarios son ahora más favorables a asumir el comportamiento imprudente de modificar la configuración de sus programas que lo eran en el primer trimestre de 2009.

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



Base: Total usuarios (n=3.599 en 1T10)

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.
- Descargo y abro ficheros adjuntos a correos electrónicos procedentes de desconocidos, o que yo no haya solicitado, si me parecen interesantes (*en desacuerdo*).
- Analizo todos los ficheros adjuntos en el correo electrónico con un antivirus antes de abrirlos.
- Borro el historial de destinatarios cuando reenvío un correo electrónico a múltiples direcciones.

De los cuatro analizados, el hábito seguro relativo al correo electrónico que es más ampliamente seguido por los usuarios de Internet españoles es el de no responder a correos electrónicos sospechosos de ser falsos (84,4% en el 1^{er} trimestre de 2010). Se consolida así el ascenso general esta buena práctica de seguridad ha experimentado desde comienzos de 2009, momento en que un 73,6% de los encuestados la seguían.

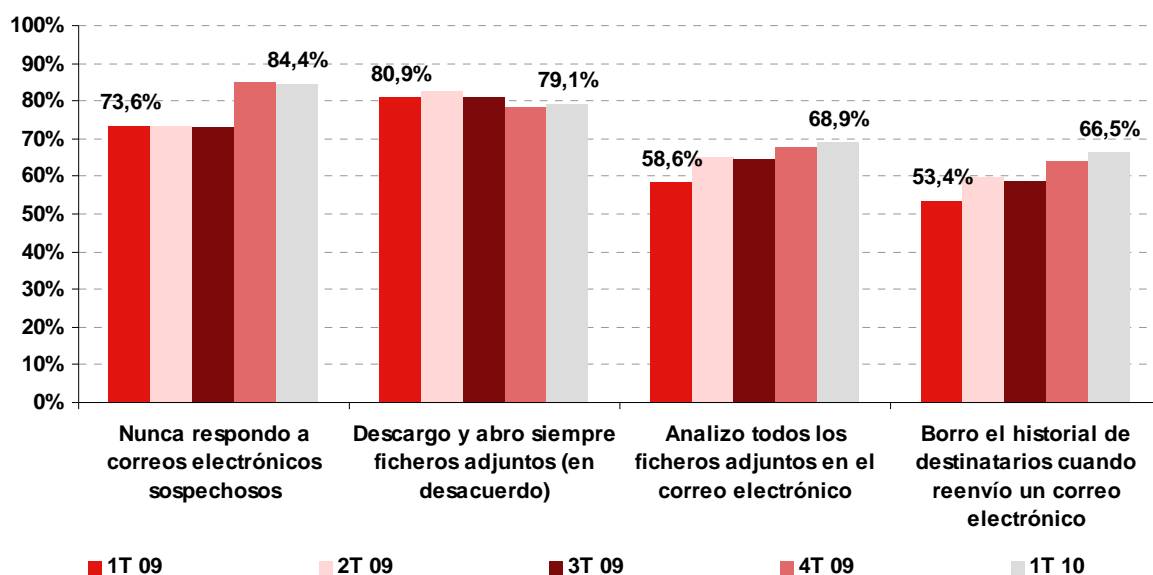
Un amplio 79,1% de usuarios se muestra en desacuerdo con la medida de descargar siempre ficheros adjuntos, incluso cuando proceden de desconocidos. Con pequeñas oscilaciones, este valor se ha mantenido estable.

El 68,9% de los encuestados afirma que analizan todos los ficheros adjuntos en el e-mail. La proporción de usuarios que adoptan este hábito prudente ha ido incrementándose de manera constante desde la primera lectura de 2009, donde un 58,6% de los españoles usuarios de Internet reconocían analizar siempre los adjuntos al correo electrónico.

A la hora de analizar archivos adjuntos o descargados a través de Internet, se puede conseguir una mayor seguridad analizando el archivo a través de servicios multimotor como [virustotal.com](http://www.virustotal.com). El hecho de leer el archivo con múltiples motores antivirus online aumenta la eficacia del análisis. En archivos con datos sensibles, sin embargo, el usuario puede considerar inadecuado utilizar a este tipo de servicios: si el archivo es tomado como positivo (es decir, infectado) por algún motor antivirus, es enviado al resto de casas antivirus para su análisis, comprometiendo así la posible confidencialidad del documento.

Cada vez son más los usuarios que borran el historial de destinatarios cuando reenvían correos electrónicos. En el 1^{er} trimestre de 2010, llegan al 66,5% de los encuestados. Ello ha supuesto un incremento de más de 13 puntos porcentuales desde el mismo período del año anterior, lo que supone un buen hábito de seguridad que parece ser puesto en práctica por más usuarios cada trimestre.

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



Base: Usuarios que utilizan el correo electrónico (n=3.599 en 1T10)

Fuente: INTECO

3.2.3 Chats y mensajería instantánea

En este capítulo 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)
- Evito pinchar en invitaciones a visitar sitios web que proceden de desconocidos.
- Rechazo las invitaciones / mensajes de usuarios que no conozco o de los que no quiero recibir mensajes.
- Borro los ficheros adjuntos que no he solicitado y que recibo por mensajería instantánea.
- Agrego contactos de terceros desconocidos al programa de mensajería (Messenger, ICQ) (*en desacuerdo*).

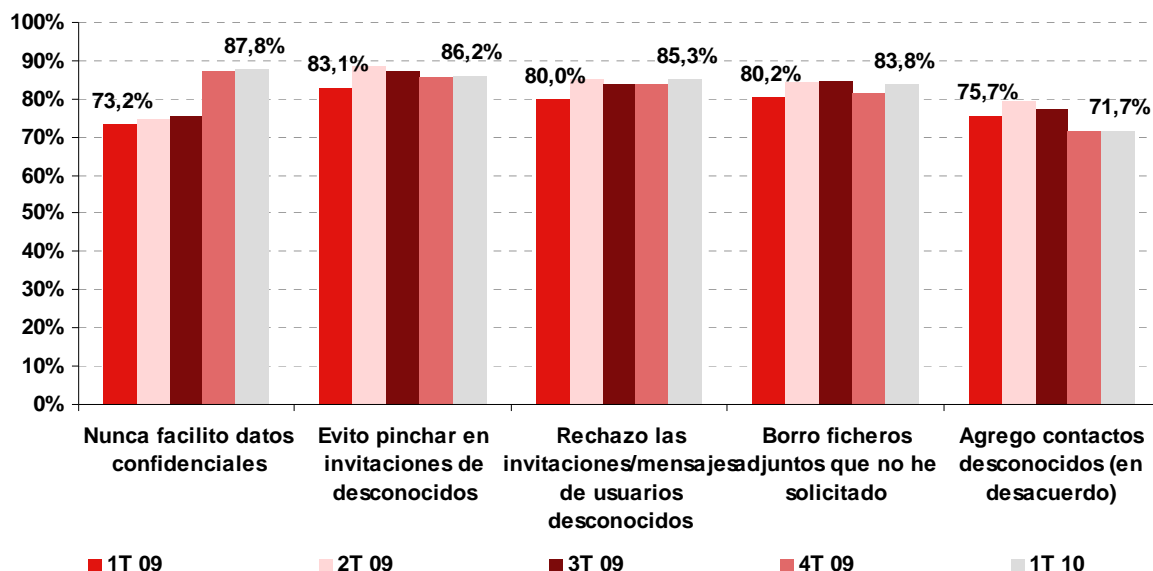
En el Gráfico 9 se muestra la evolución de los hábitos prudentes relacionados con chats y mensajería instantánea. Como comentario general, se aprecia un elevado nivel de cumplimiento de comportamientos seguros en estos servicios: de los cinco analizados, cuatro presentan una tasa de seguimiento superior al 80%.

Los usuarios son conscientes de los riesgos de proporcionar información sensible en chats o mensajería instantánea, y así un 87,8% reconocen no facilitar datos confidenciales a terceros. Se trata del máximo histórico, y representa un incremento de 14 puntos porcentuales desde el primer trimestre de 2009.

No pinchar links de desconocidos (86,2%), rechazar invitaciones o mensajes de personas desconocidas (85,3%) y borrar los ficheros adjuntos no solicitados (83,8%) son hábitos prudentes contemplados ampliamente por los usuarios de Internet españoles. En los tres casos, la tendencia observada desde principios de 2009 sugiere una estabilidad en los niveles de cumplimiento.

El hábito prudente seguido en menor medida es el de no añadir contactos no conocidos al sistema de mensajería instantánea: un 71,7% de usuarios se muestra en desacuerdo con la afirmación *Agrego contactos de terceros desconocidos al Messenger*. Se trata de un porcentaje importante de ciudadanos que se comportan de manera segura, pero es inferior a los niveles del resto de hábitos relativos al chat y/o mensajería instantánea, y su evolución parece señalar una tendencia a la baja: en el primer trimestre de 2009, un 75,7% de los panelistas decían no agregar contactos de desconocidos.

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



Base: Usuarios que utilizan mensajería instantánea y/o chats (n=2.982 en 1T10)

Fuente: INTECO

3.2.4 Banca en línea y comercio electrónico

A continuación 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.
- Evito usar equipos públicos o compartidos (café, estaciones o aeropuertos).
- Vigilo periódicamente los movimientos de la cuenta bancaria en línea.
- Cuando realizo transacciones en línea (pagos, compras, transferencias) compruebo que uso una conexión segura (protocolo https, validez y vigencia del certificado).
- Cuando mi banco me pide mis datos personales o contraseñas por correo electrónico o por teléfono se los facilito (*en desacuerdo*).
- Siempre tecleo la dirección web de mi banco en la barra de direcciones.

La banca electrónica se ha convertido en un jugoso objetivo para los creadores de malware. Los troyanos de hoy en día están específicamente diseñados en su mayoría para robar datos y credenciales relacionados con la banca online, de forma que puedan rentabilizar la inversión y lucrarse de las infecciones conseguidas. Los troyanos suelen estar específicamente diseñados para robar contraseñas de bancos

concretos. En un principio, atacaban principalmente a los bancos que no disponían de factores de autenticación adicionales a una contraseña (los que carecían de tarjeta de coordenadas, por ejemplo). Hoy en día se centran en todo tipo de bancos, desde los que no requieren de medidas adicionales a una contraseña para operar online, hasta los más avanzados que usan factores de autenticación adicionales como contraseñas de un solo uso o confirmación por móvil.

Hasta un 83,6% de los usuarios de Internet españoles cierran la sesión después de realizar transacciones online, con pocos movimientos al alza o a la baja desde principios de 2009. También estable se mantiene el cumplimiento del comportamiento prudente de evitar realizar transacciones económicas desde equipos públicos: en el primer trimestre de 2010, un 82,7% de los encuestados observan este hábito.

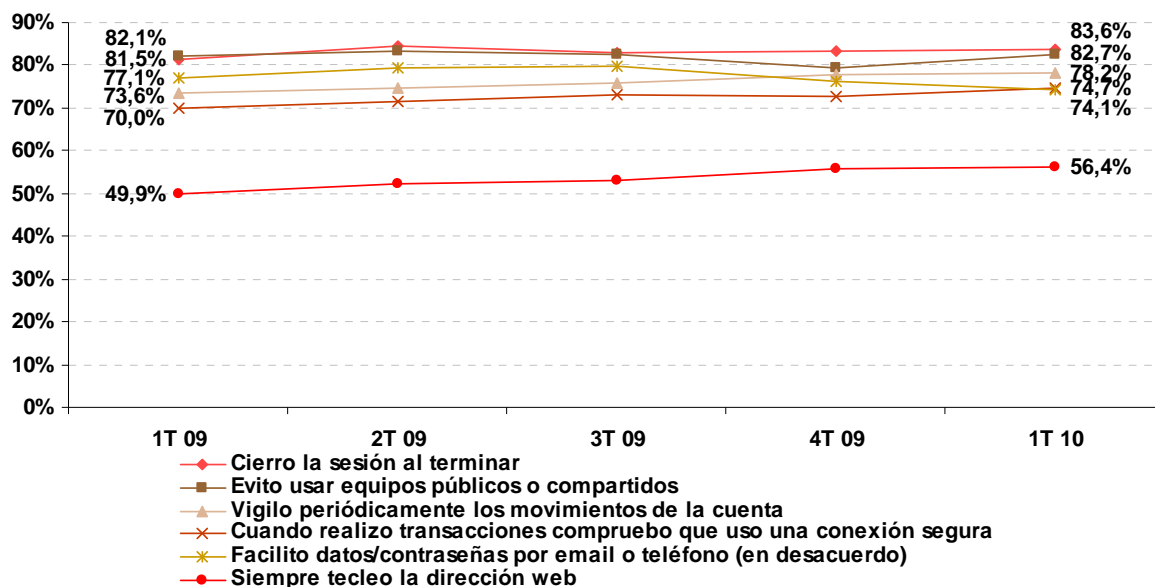
Una medida sencilla que ayuda a detectar de forma temprana un posible fraude es la vigilancia periódica de los movimientos de la cuenta bancaria online. En este caso, sí parece que ha habido una evolución positiva de este hábito prudente: en el primer trimestre de 2010, un 78,2% de los usuarios españoles de Internet observan esta práctica (frente al 73,6% un año atrás).

Cada vez más usuarios (un 74,7%) comprueban que están utilizando una conexión segura al realizar una transacción online. El porcentaje de usuarios que siguen este hábito ha aumentado 4,7 puntos porcentuales desde el primer trimestre de 2009.

Un 74,1% de los ciudadanos se muestra en desacuerdo con la afirmación *Facilito datos / contraseñas a mi banco por teléfono o e-mail*. El porcentaje, aunque importante, ha experimentado un ligero descenso desde principios de 2009. No está de más recordar que ninguna entidad bancaria solicitará datos personales de sus clientes a través del teléfono o correo electrónico.

Por último, el 56,4% de los panelistas afirman teclear siempre la dirección de su banco. El dato positivo es que la proporción de ciudadanos que adoptan este hábito prudente ha crecido considerablemente (6,5 puntos porcentuales) desde el primer trimestre de 2009. No obstante, todavía existe área para la mejora: ciertamente, un comportamiento tan sencillo para la seguridad del usuario como es teclear la dirección del banco (en lugar de pinchar un enlace, por ejemplo) debería ser adoptado de manera generalizada.

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=3.324 en 1T10) Fuente: INTECO

3.2.5 Redes P2P

En este epígrafe se analizan tres comportamientos que tienen que ver con la seguridad en la utilización de redes *peer to peer* o P2P:

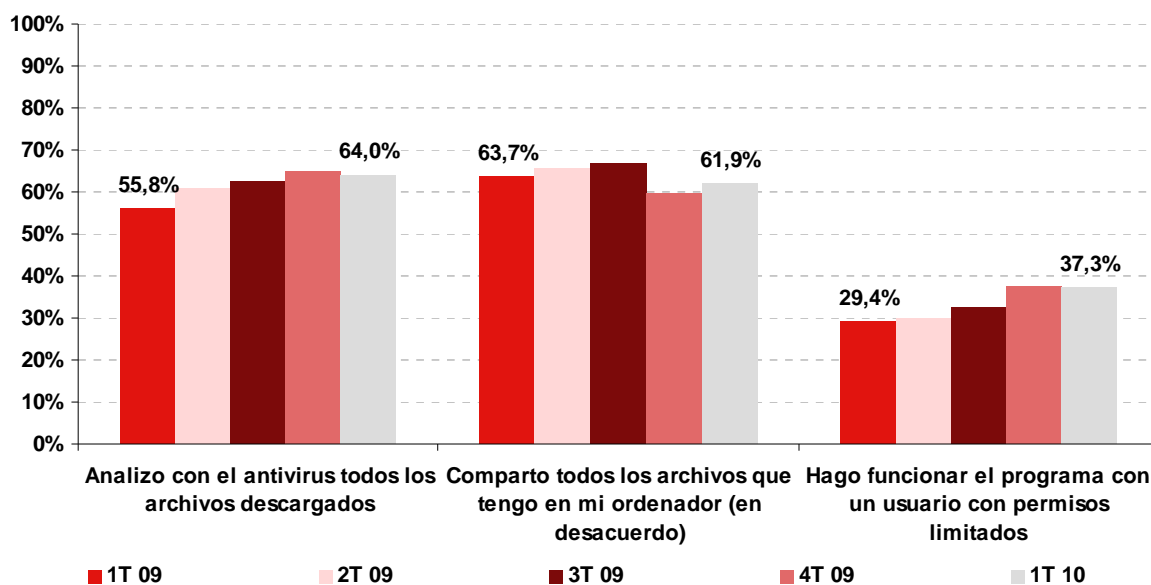
- Analizo con el programa antivirus todos los archivos descargados a través de redes P2P.
- Comparto todos los archivos que tengo en mi ordenador con el resto de usuarios P2P (*en desacuerdo*).
- Hago funcionar el programa de P2P con un usuario con permisos limitados.

El nivel de observación del hábito prudente de analizar con el antivirus todos los archivos descargados en redes *peer to peer* se sitúa en el 1^{er} trimestre en un 64% de los usuarios P2P españoles, en una clara tendencia ascendente iniciada en el 1^{er} trimestre de 2009.

Compartir todos los archivos en el sistema con las redes P2P supone exponer públicamente el disco duro: archivos de sistema, fotografías, vídeos, documentos, etc. Obviamente, esto supone un hábito imprudente desde el punto de vista de la seguridad y la intimidad. Un 61,9% se muestra en desacuerdo con la afirmación "Comparto todos los archivos que tengo en mi ordenador". A pesar de que se trata de un nivel correcto de cumplimiento, todavía existe un amplio margen de mejora en este indicador.

Menos prudentes se muestran los usuarios cuando se trata de gestionar los privilegios de acceso. Sólo el 37,3% de los encuestados reconoce hacer funcionar el equipo con permisos limitados, cuando se trata de conectarse a una red P2P. El dato, muy mejorable, muestra no obstante una evolución positiva continuada desde el 1^{er} trimestre de 2009, período en el que sólo el 29,4 de los usuarios de redes P2P afirmaban hacer uso de cuenta sin privilegios de administrador para conectarse al *peer to peer*.

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



Base: Usuarios que utilizan redes P2P (n=2.622 en 1T10)

Fuente: INTECO

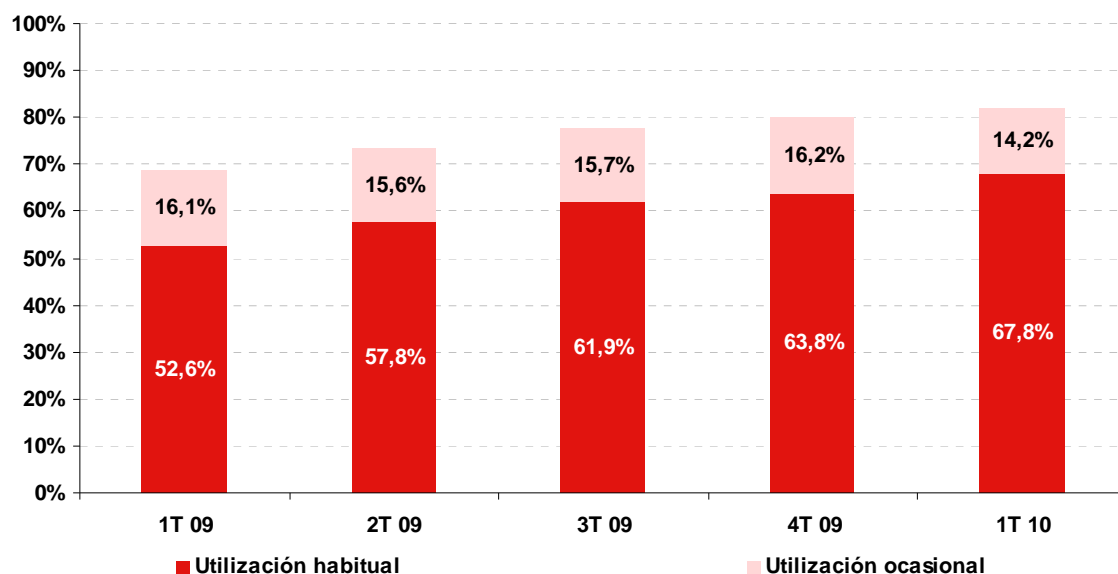
3.2.6 Redes sociales

Según las cifras de la consultora Nielsen para diciembre, el tiempo de permanencia en sitios de redes sociales como Facebook y Twitter aumentó 82% durante el 2009. Facebook fue la red social número uno con 206,9 millones de visitantes únicos en diciembre de 2009, lo que equivale al 67% de los usuarios de las redes sociales en todo el mundo.⁶

Los datos proporcionados por los usuarios de Internet españoles confirman que el uso de las redes sociales sigue su evolución imparable: en el primer trimestre de 2010, un 67,8% afirma utilizar habitualmente las redes sociales, y un 14,2% dice hacerlo esporádicamente.

⁶ http://digitalmedia.strategyeye.com/article/brzAEXrgBos/2010/01/25/social_network_use_soars_82_in_a_year/

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



Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

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

El mayor uso que se le da a las redes sociales es el envío de mensajes y comentarios privados, declarado por un 64,5%. Mantener el contacto y reencontrar a viejos amigos es mencionado por un 63,2%, y enviar mensajes públicos, por un 50,4%.

El 51,9% declara que usa las redes sociales para compartir fotografías y algo menos, un 25,4% de los usuarios, para compartir vídeos. Ver contenido multimedia y “cotillear” es mencionado por un 47%.

Usos más específicos como buscar empleo (16,3%), invitar a eventos (23%) o ligar (16,3%) son opciones mencionadas de manera más esporádica.

En general, se aprecia una mayor intensidad de uso en casi todos los servicios, de forma que el porcentaje que usuarios que menciona cada uno de los usos es superior en el primer trimestre de 2010 al porcentaje que lo manifestaba en trimestres anteriores.

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



Base: Usuarios que utilizan redes sociales (n=2.788 en 1T10)

Fuente: INTECO

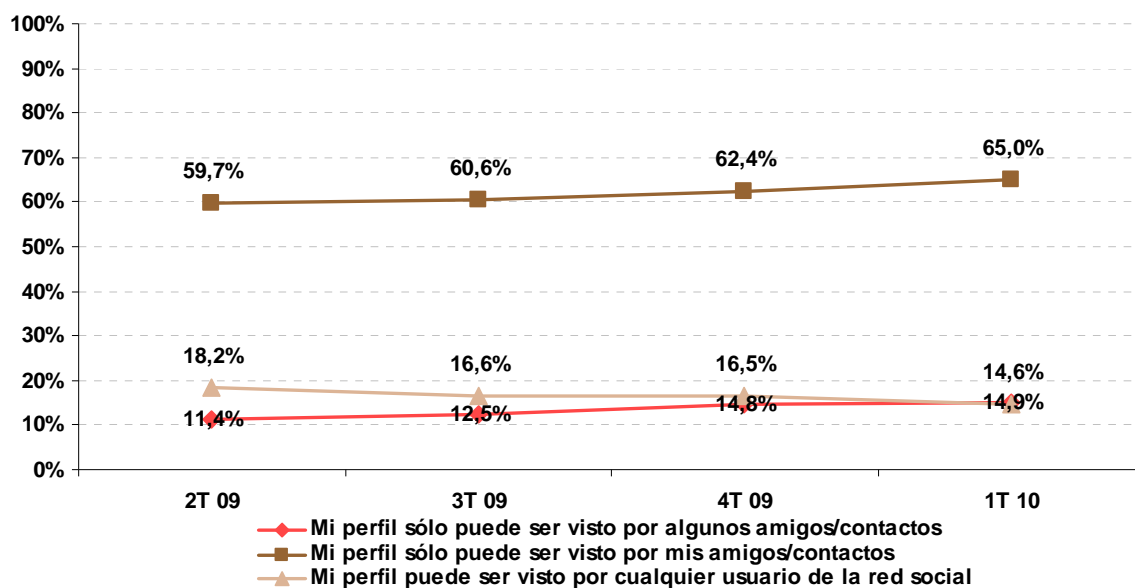
La información personal es el punto débil de las redes sociales, y por ello resulta interesante estudiar el nivel de privacidad que cada usuario asigna a su perfil.

Los usuarios españoles de redes sociales son cuidadosos con su privacidad, y así un 65% admite que sólo sus contactos pueden tener acceso a su perfil. Más restrictivos aún se muestran el 14,9% que manifiestan que sólo algunos de sus contactos pueden visualizar su perfil.

En el extremo menos prudente se encuentra el 14,6% de personas que tienen su perfil abierto a cualquier usuario de la red social.

En el Gráfico 14 se puede comprobar la evolución, lenta pero constante, hacia posturas más cuidadosas con su intimidad: el paulatino crecimiento de usuarios que restringen su perfil tanto a sus contactos, como a sólo alguno de sus contactos, se ve compensado con el paralelo descenso de personas cuyo perfil puede ser visitado por cualquier usuario de la red.

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



Base: Usuarios que utilizan redes sociales (n=2.788 en 1T10)

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 821 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.
- Tengo el ordenador en el que navega en un lugar común a la vista de todos.
- Vigilo y limito el tiempo de conexión del menor a Internet.
- Superviso los contenidos a los que accede después de cada sesión (historial).
- He creado una cuenta de usuario limitado para el acceso del menor a Internet.

La medida más adoptada es la prohibición al menor de realizar transacciones económicas en línea sin la presencia de un adulto. En el primer trimestre de 2010, un 91,8% de los hogares participantes en el estudio han impuesto esta norma; el dato del mismo período de 2009 era de 77,6%. El aumento de 14 puntos porcentuales puede ser indicio del aumento de la sensibilidad de los padres ante la problemática de fraudes online.

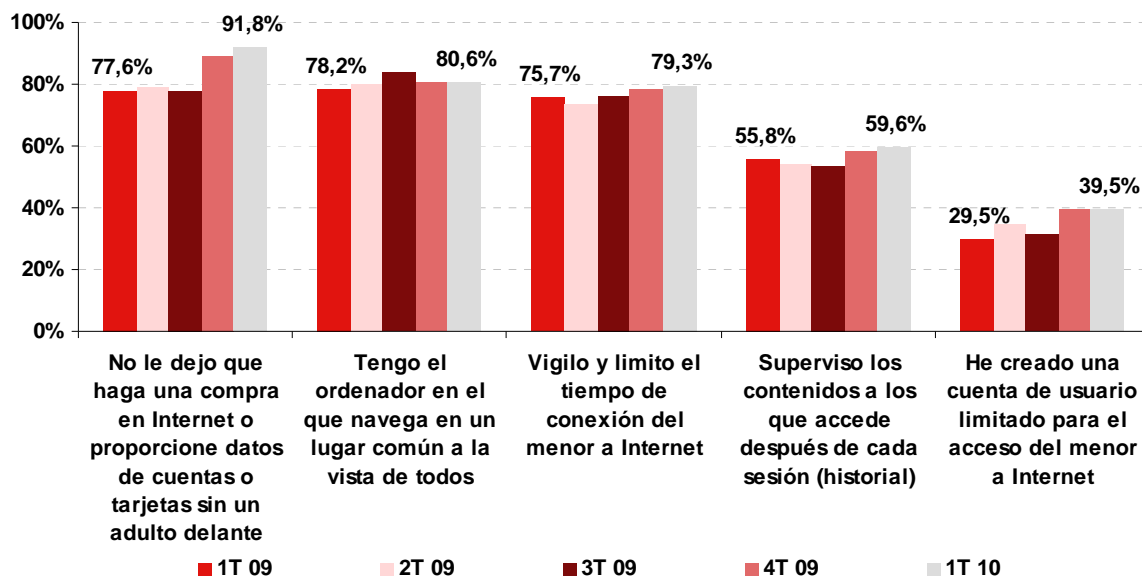
En un 80,6% de los hogares con menores conectados a Internet el ordenador se encuentra en un lugar común de la casa, sin que se hayan apreciado variaciones significativas en la adopción de esta buena práctica a lo largo de 2009.

El 79,3% de los padres limita el tiempo de conexión a Internet de los hijos, en una tendencia al alza iniciada en 2009. La vigilancia y limitación de los tiempos (horarios y días) de utilización de Internet por los menores es una recomendación básica para que el niño o adolescente haga un uso responsable de la Red.

Un 59,6% de los adultos dice supervisar los contenidos a los que accede el menor después de cada sesión. Se trata de una medida que, aunque mayoritaria, no es de adopción generalizada entre los hogares, lo que puede indicar el recelo de los padres a la hora de invadir la intimidad de sus hijos.

Por último, una medida que sigue siendo infrautilizada es la creación de cuentas separadas y sin privilegios para los diferentes miembros del hogar. Solo un 39,5% ha llevado a cabo esta medida en el primer trimestre de 2010, aunque su avance ha sido muy positivo desde el mismo período del año anterior, cuando sólo el 29,5% de los padres reconocían haber creado una cuenta de usuario específica para el hijo.

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=821 en 1T 2010) Fuente: INTECO

3.3.2 Medidas de comunicación, diálogo y educación

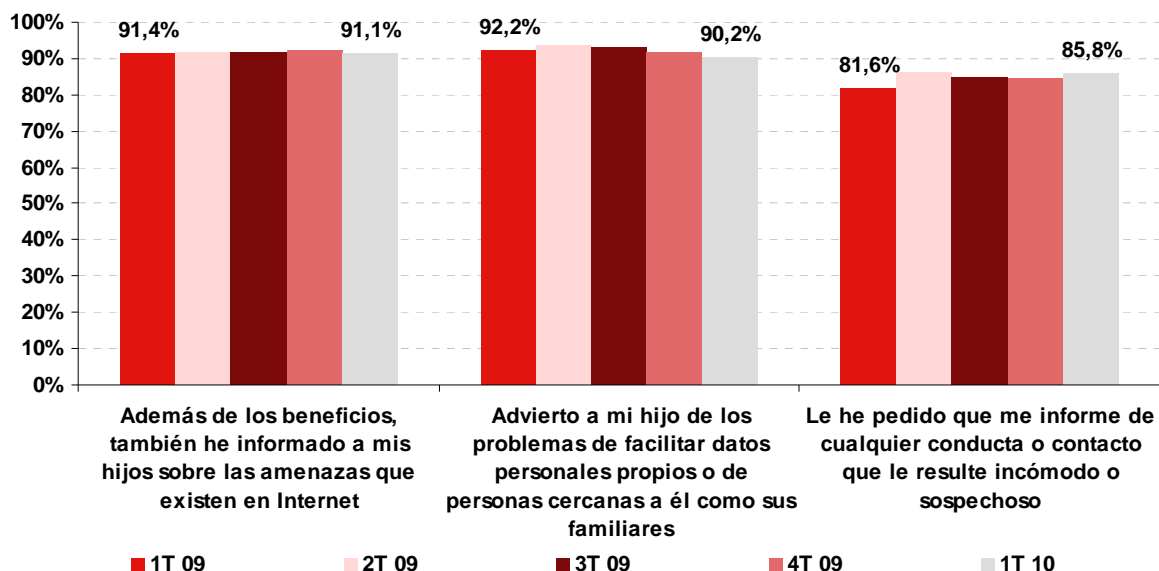
En esta categoría se analizan los siguientes comportamientos:

- Además de los beneficios, también he informado a mis hijos sobre las amenazas que existen en Internet.
- Advierto a mi hijo de los problemas de facilitar datos personales propios o de personas cercanas a él como sus familiares.
- Le he pedido que me informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.

Los hogares españoles con menores que utilizan a Internet se muestran favorables a adoptar medidas de carácter educativo. Así, el nivel de adopción de los tres comportamientos analizados es muy elevado (superior al 80% 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.

Especialmente notables son el hecho de informar a los menores de los peligros de la Red (91,1%) y la advertencia a los menores sobre los riesgos de dar información confidencial (90,2% de los adultos dicen llevar a cabo este hábito). En un 85,8% de los hogares se pide a los menores que comuniquen al adulto cualquier comportamiento sospechoso que detecten en la Red.

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=821 en 1T 2010) Fuente: INTECO

3.3.3 Medidas de implicación del padre en la navegación del hijo

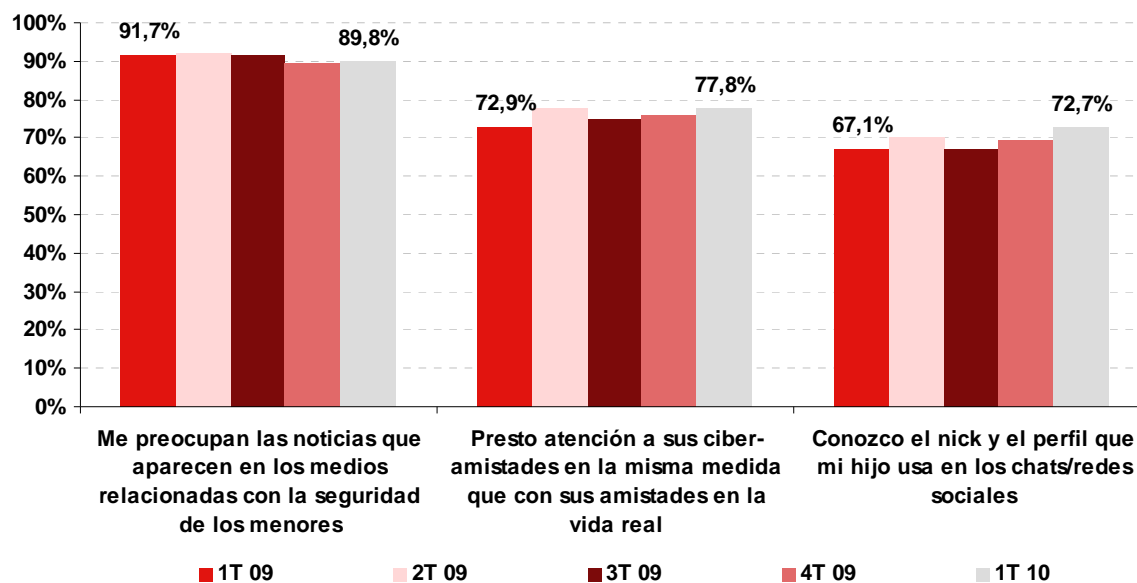
Se analiza aquí el nivel de acuerdo del adulto con una serie de afirmaciones, que constituyen indicios de la implicación de los padres en el uso que los hijos hacen de la Red. En concreto:

- Me preocupan las noticias que aparecen en los medios relacionadas con la seguridad de los menores.
- Presto atención a sus ciber-amistades en la misma medida que con sus amistades en la vida real.
- Conozco el nick y el perfil que mi hijo usa en los chats/redes sociales.

No hay duda de que a los padres les preocupa el uso que sus hijos hacen de la Red, y están implicados de manera activa en la navegación del hijo. Así, el 89,8% de los encuestados reconoce que les preocupan las noticias relacionadas con la seguridad de los menores en las TIC.

Un 77,8% dice que presta especial atención a las ciberamistades del hijo y un 72,7% conoce el nick y el perfil que el menor utiliza en chats o redes sociales. En ambos casos, los porcentajes de adopción de estas medidas han ido incrementándose paulatinamente desde comienzos de 2009, lo que podría sugerir una mayor proactividad de los padres 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=821 en 1T 2010) Fuente: INTECO

4 INCIDENCIAS DE SEGURIDAD

Se estudia en este epígrafe las incidencias de seguridad sufridas por los usuarios, para clasificar y entender las amenazas que sufren más a menudo los internautas españoles.

En la Tabla 4 se muestran las incidencias de seguridad que han afectado a los usuarios, ofreciéndose el doble dato de percepción (a partir de las respuestas de los encuestados) y realidad (construido con la información de la red de sensores de INTECO, en el caso del spam, e iScan, en el análisis del código malicioso).

El spam o correo electrónico no deseado sigue siendo el incidente que a más usuarios afecta, con un 68,4% que afirma haberlo recibido alguna vez en los últimos 3 meses. Aunque los filtros antispam de los sistemas de correo realizan una primera selección, resulta complejo eliminar todo el correo no deseado. La realidad, según los datos ofrecidos por la red de sensores de INTECO, es que el 93,7% del correo electrónico de marzo de 2010 es spam.

Por detrás del correo electrónico no deseado se encuentra el código malicioso: un 29,5% de usuarios dicen haber sufrido algún tipo de virus o malware en los últimos tres meses. El dato real para marzo proporcionado por iScan aumenta el nivel de infección hasta el 52,8%.

El robo de ancho de banda y la suplantación de identidad son situaciones ocurridas muy esporádicamente: el 82,7% y 83,9%, respectivamente, de encuestados, dicen no haberlas experimentado en ninguna ocasión.

Tabla 4: Incidencias de seguridad declaradas por los usuarios en función del momento de detección 1T2010 (%)

Incidencia	DECLARADO				REAL
	Nunca	Alguna vez	Alguna vez (último año)	Alguna vez (últimos 3 meses)	Mar 10
Recepción de correos electrónicos no deseados	11,7%	7,0%	12,9%	68,4%	93,7% ⁷
Virus u otros códigos maliciosos	22,2%	26,9%	21,4%	29,5%	52,8%
Robo de ancho de banda en la conexión a Internet (intrusión Wi-Fi)	82,7%	5,9%	6,7%	4,6%	
Víctima de suplantación de identidad	83,9%	5,7%	4,4%	6,1%	

Base: Total usuarios (n=3.599)

Fuente: INTECO

⁷ Estos datos proceden de la red de sensores de INTECO, disponibles en: https://ersi.inteco.es/index.php?option=com_sanetajax&Itemid=55&lang=es

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:

- **Trojanos 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 trojanos, 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 trojanos:
 - Bankers o trojanos 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 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 (espíar 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.

- **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

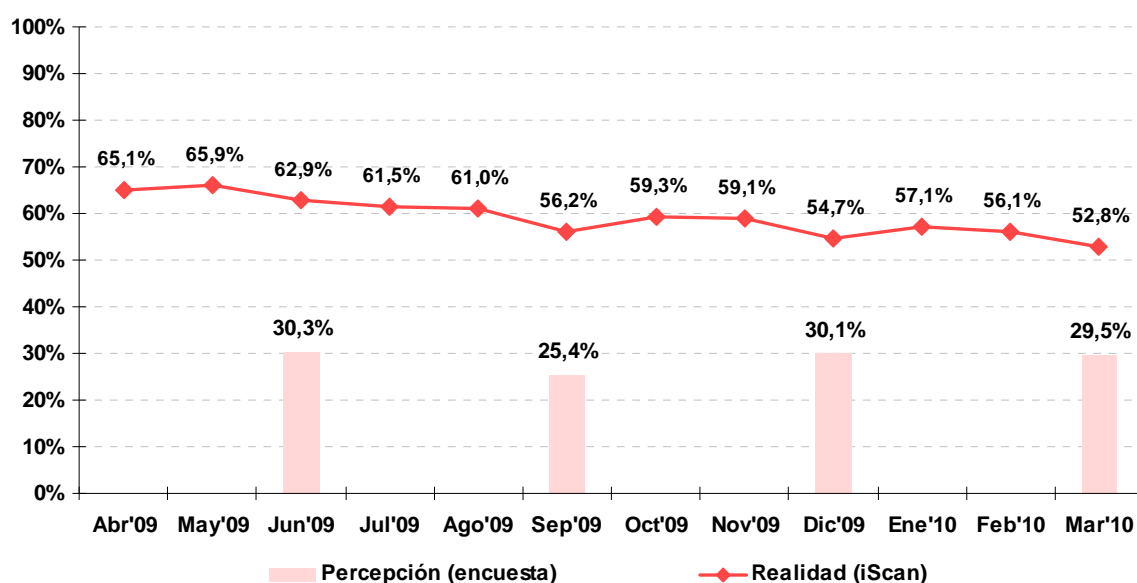
Este apartado está construido íntegramente a partir de los datos reales obtenidos del escaneo de los equipos de los panelistas gracias a la herramienta iScan desarrollada por INTECO. Una explicación más detallada de la herramienta se encuentra disponible en el *Anexo I: Diseño metodológico detallado*.

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). El análisis se realiza para los últimos 12 meses.

El nivel de equipos infectados en marzo de 2010 se sitúa en un 52,8%, lo que constituye un nuevo mínimo histórico de nivel de infección real (los informes correspondientes al tercer y cuarto trimestres de 2009 anunciaban también, respectivamente, mínimos históricos). Se trata de un dato muy positivo, y confirma la tendencia a la reducción del volumen de equipos infectados.

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



Percepción = declaran haber sufrido malware en los últimos 3 meses

Fuente: INTECO

Los usuarios siguen manteniendo una percepción de infección menor a la real, de solo un 29,5%. Existe un evidente salto entre percepción y realidad que en la última lectura alcanza a un 23,3% de ciudadanos cuyos equipos están infectados en el momento del escaneo, pero no creen estarlo en el momento de realización de la encuesta. La brecha, si bien ha existido a lo largo de los cuatro trimestres analizados, se ha ido reduciendo progresivamente motivada por la disminución del nivel de infección real de los equipos.

La diferencia entre percepción y realidad puede estar sustentada en varios factores:

- Si el antivirus está configurado para eliminar silenciosamente las amenazas que encuentran en los escaneos del sistema, el usuario no detecta realmente que ha estado infectado.
- El nivel de detección de los antivirus no puede llegar a cubrir a la totalidad del malware, por lo que pueden existir amenazas que pasen desapercibidas para los motores antivirus (además de para los usuarios).
- Pueden existir equipos que, en puridad, estén infectados (porque alojan algún archivo considerado malicioso teniendo en cuenta los criterios metodológicos de

diagnóstico de iScan), pero que el usuario no percibe como tal. Se trata, por ejemplo, de archivos tipo *herramientas*, conscientemente alojadas en el sistema por su dueño, y que en realidad no suponen un incidente de seguridad para el usuario.

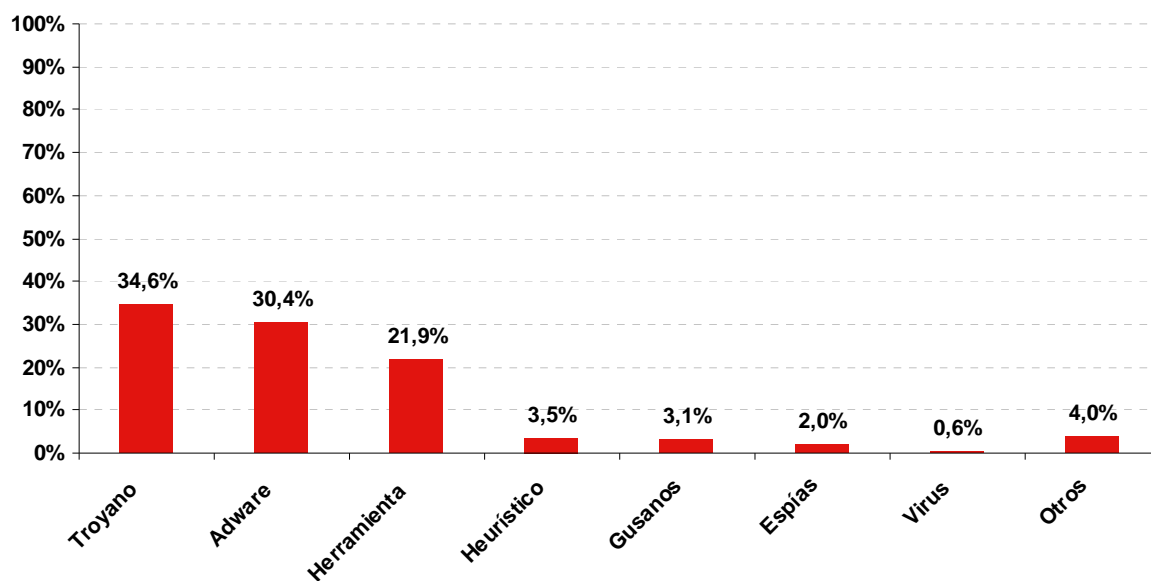
4.2.2 Tipología del código malicioso detectado

Se analiza en el siguiente gráfico el tipo de malware detectado en los sistemas. Los troyanos (34,6%) y el adware (30,4%) siguen siendo el código malicioso más detectado. La razón es clara: permiten lucrarse a los atacantes de forma rápida y directa.

No ocurre lo mismo con el spyware o programas espías que, si bien permite lucrarse a sus creadores, se mantiene en mínimos de detección (2%) ¿Por qué no se crea tanto software espía como troyanos y adware? Esto es posiblemente debido a varios factores:

- Parte del spyware instalado en los sistemas es *legal* y los antivirus evitan detectarlos. Se suelen instalar junto con otros programas, pidiendo *permiso* con letra pequeña. El usuario, no lee ni se percata de que está instalando otra aplicación junto con la que desea, aunque legalmente, se supone que ha leído un contrato y acepta la instalación.
- Los programas espía recopilan datos. Para que sus creadores obtengan un beneficio, es necesario a posteriori, realizar minería de datos para clasificar y sacar provecho de esos datos recopilados, por lo que requieren un arduo trabajo posterior. Con los troyanos y el adware el beneficio es más inmediato.

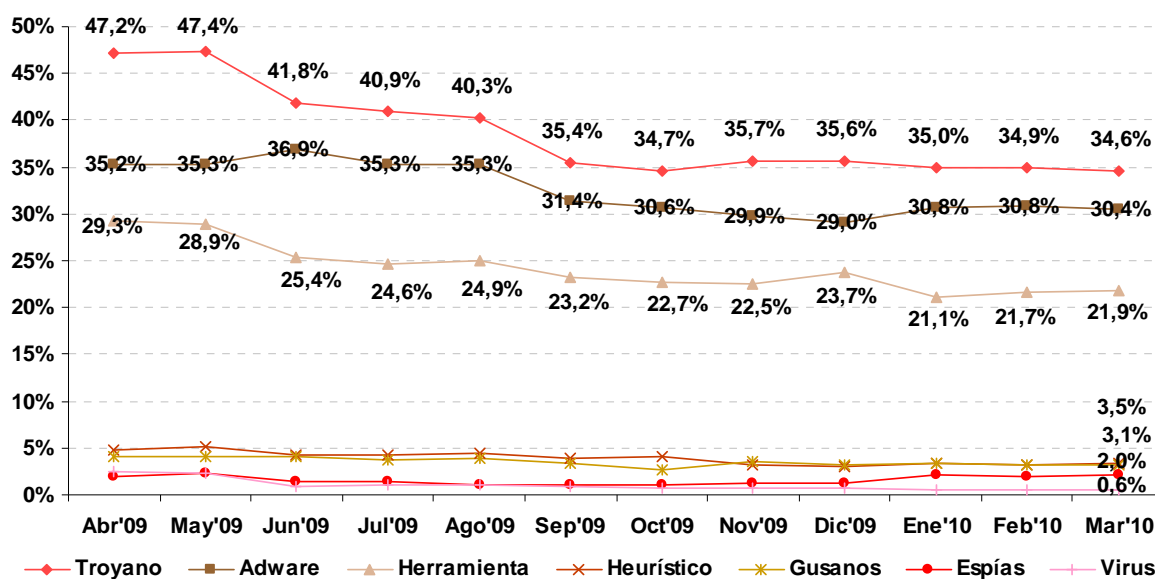
Gráfico 19: Equipos que alojan malware según tipología de código malicioso en mar. 10 (%)



Fuente: INTECO

En el Gráfico 20 se puede observar la evolución de los equipos que alojan malware según tipología. Los troyanos caen a su mínimo (34,6%), aunque con poca diferencia con respecto a trimestres anteriores. También el nivel de detección de adware (30,4%) y herramientas (21,9%) se reduce con respecto al existente doce meses atrás. El resto de tipos de código analizado (detecciones heurísticas, gusanos, espías y virus) se mantiene estable en el tiempo, y siempre con una presencia inferior al 5%.

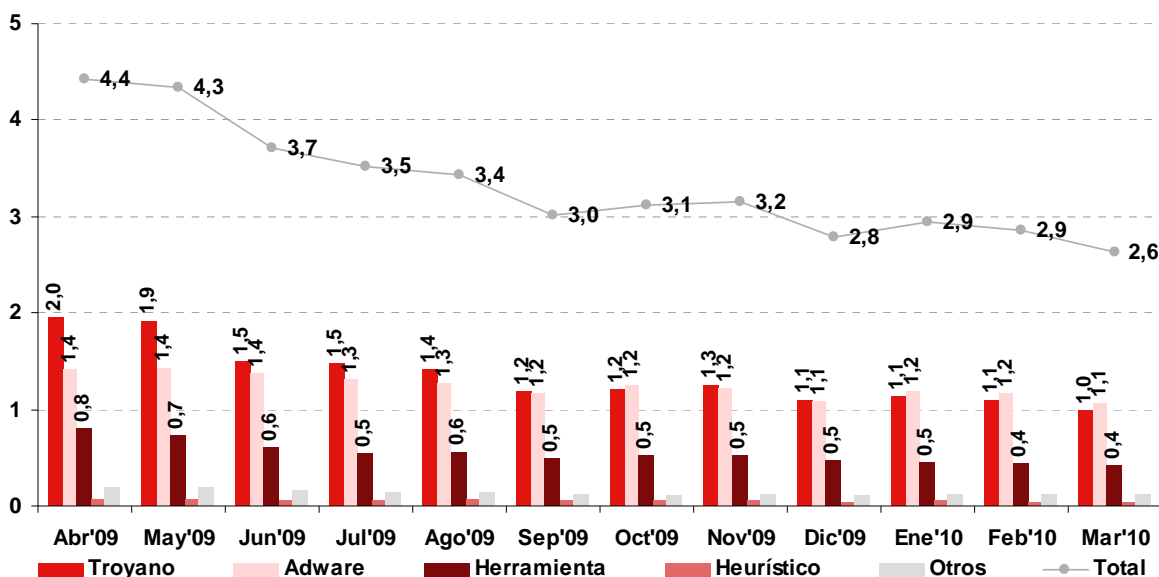
Gráfico 20: Evolución de equipos que alojan malware según tipología (%)



Fuente: INTECO

En marzo de 2010 los equipos auditados alojan, de media, 2,6 archivos infectados, de los cuales uno corresponde a la categoría de troyanos y 1,1 es catalogado como adware.

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



Fuente: INTECO

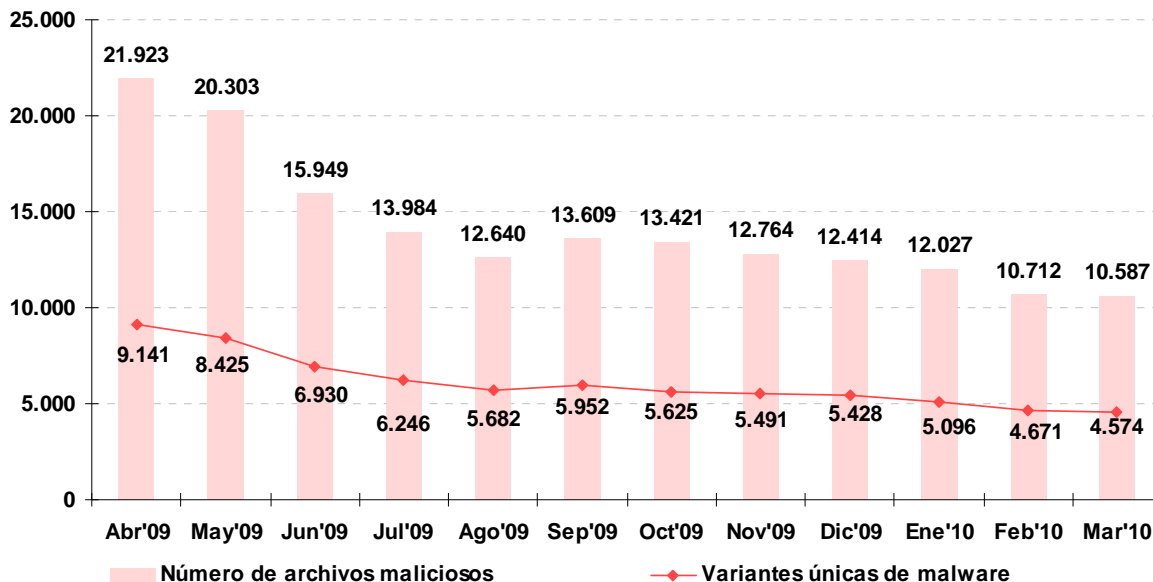
4.2.3 Diversificación del código malicioso detectado

Para los atacantes, es importante diversificar el código malicioso que ponen en circulación. A través de la introducción de ligeros cambios en los archivos, consiguen eludir a los antivirus y sistemas de seguridad y por tanto aumenta la efectividad del malware. Éstos se denominan *variantes*. A su vez, cada cierto tiempo, introducen nuevas características en el malware, manteniendo su filosofía original, lo que a su vez se denominan *familias*.

Variantes únicas de malware

En el siguiente gráfico se analiza la evolución de 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. Los datos confirman una vez más el elevado nivel de diversificación del código malicioso. Así, poniendo en relación ambos datos, cada variante única detectada se avistaría sólo 2,3 veces de media (marzo de 2010).

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

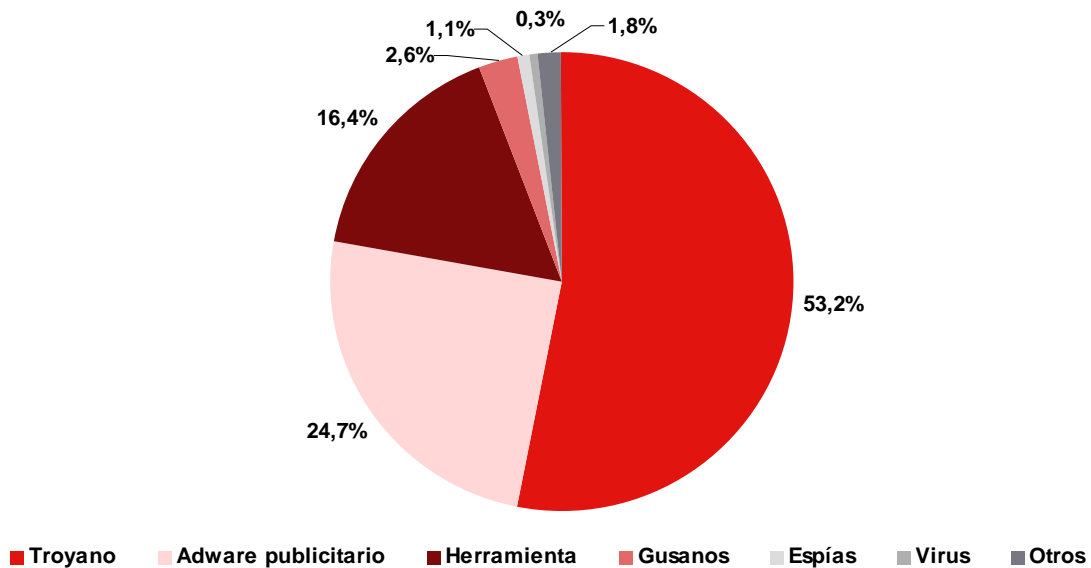


Fuente: INTECO

La diversificación se observa sobre todo, como indica el Gráfico 23 en la categoría de troyanos y adware, que son a su vez las categorías más detectadas. Las mafias que se dedican al negocio del crimen organizado relacionado con el malware, invierten una enorme cantidad de tiempo y recursos en la creación de nuevas variantes para maximizar beneficios.

Así, la categoría con más variantes es la de troyanos, con un 51,1%, junto con la de adware, con un 20,5%.

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

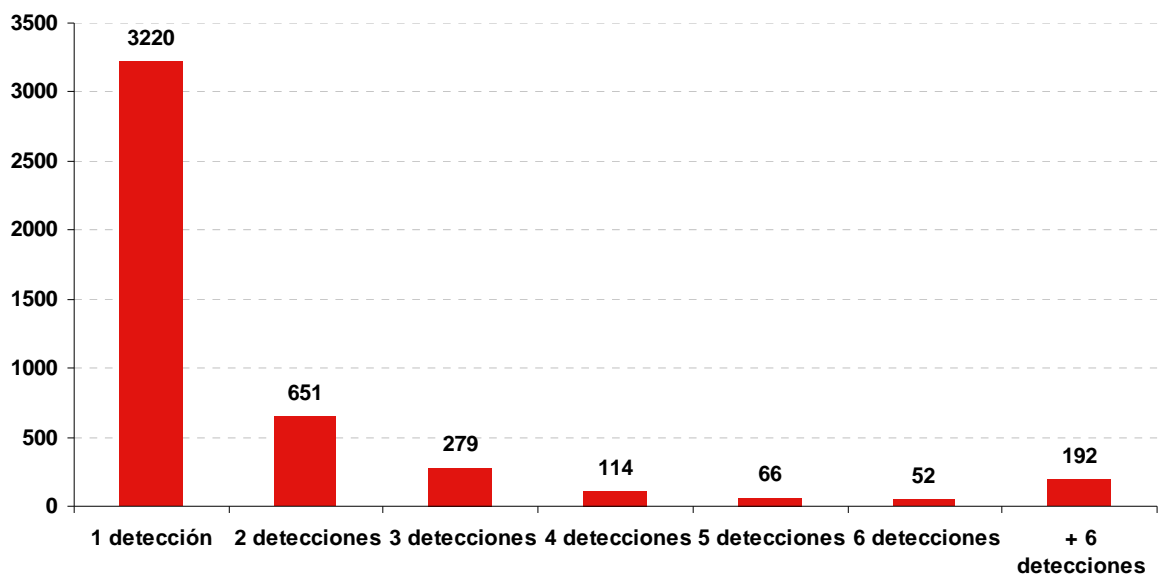


Fuente: INTECO

Número de detecciones de las variantes únicas

En marzo de 2010, 3.220 (de 4.574) muestras han sido avistadas solo una vez. El hecho de que el 70% de las muestras aparezcan una sola vez es síntoma de que se encuentran muy diversificadas. Esta gran cantidad de muestras únicas de malware hoy en día, no evita que la mayoría pertenezcan a un mismo tipo o familia concreta.

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



Fuente: INTECO

4.2.4 Peligrosidad del código malicioso y riesgo del equipo

Hasta ahora se ha analizado el volumen, la clasificación y el grado de diversificación del código malicioso. Este epígrafe aborda el nivel de peligrosidad del mismo.

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), scripts⁸, así como las detecciones heurísticas.

- **Riesgo bajo:** aquí se engloban las manifestaciones que menor nivel deafección 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.

⁸ 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 intrusión⁹, 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 error¹⁰. 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 (es decir, un equipo infectado con troyano y adware estará incluido en el grupo de riesgo alto - troyano -, y no en el medio - adware -).

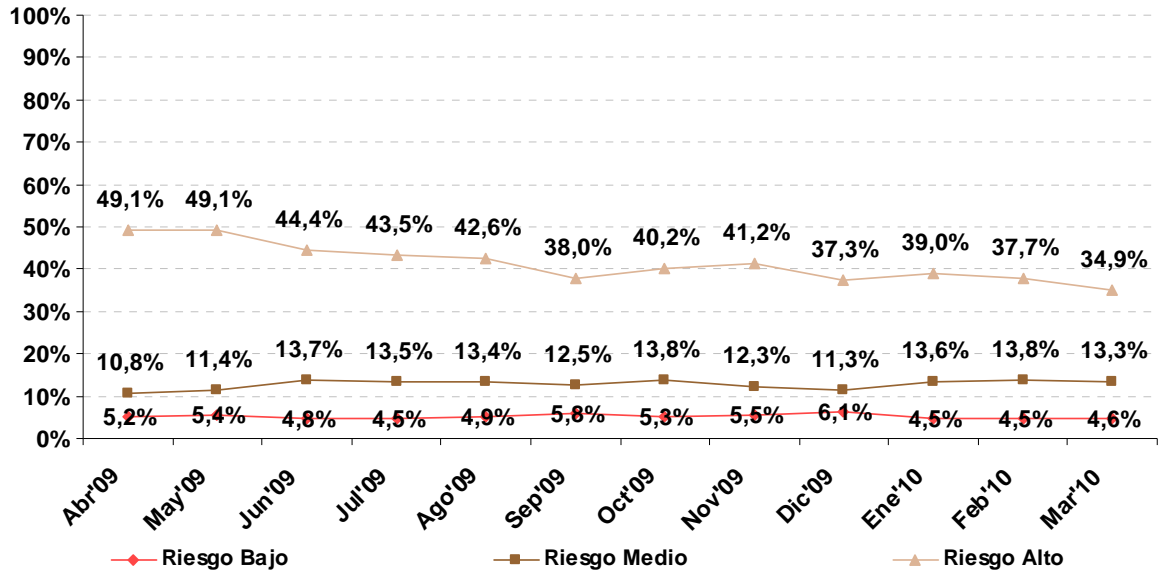
El nivel de riesgo en los equipos de los internautas españoles se ha reducido progresivamente, alcanzando en marzo de 2010 el mínimo histórico de ordenadores con riesgo alto (34,9%).

⁹ 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.

¹⁰ 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

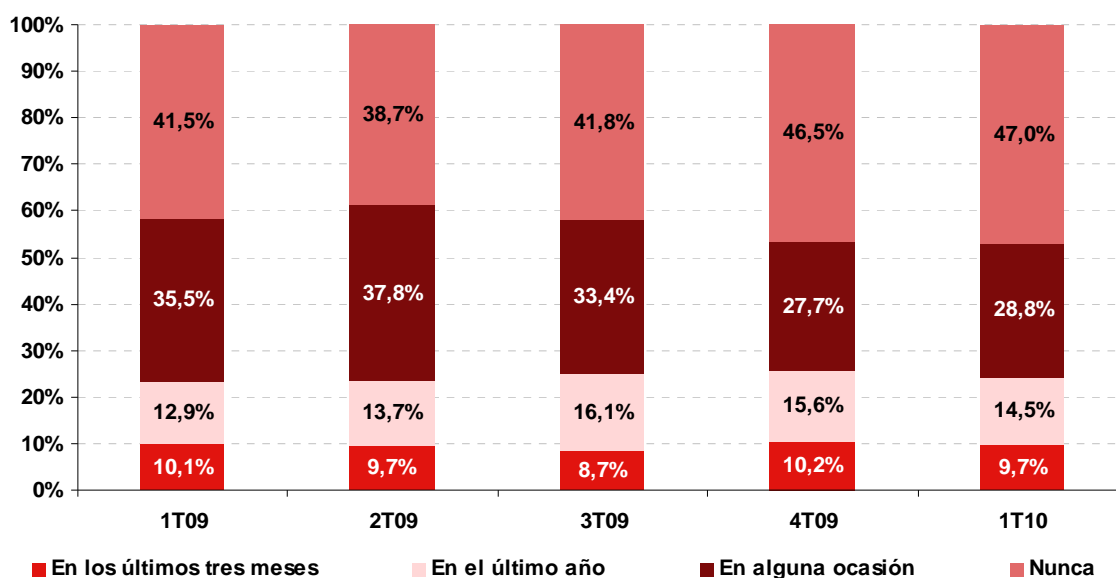
5.1 Consecuencias de las incidencias de seguridad

Se estudia en este apartado las consecuencias de las incidencias de seguridad, y en concreto se analiza la evolución de tres tipos de consecuencias: pérdida de datos, formateo o reinstalación del sistema operativo y daños en el hardware.

El Gráfico 26 muestra la evolución de la pérdida de datos como consecuencia de incidencias de seguridad. En el primer trimestre de 2010, un 9,7% de los usuarios de Internet españoles ha experimentado una pérdida de datos o archivos en los últimos tres meses, un 14,5% adicional dice haberlo sufrido en el último año y un 28,8% afirma que le ha ocurrido en alguna ocasión, con anterioridad a un año. Por último, un 47% de los panelistas nunca se ha enfrentado con una situación de pérdida de datos consecuencia de una incidencia de seguridad.

Parece que el análisis de la evolución histórica sugiere una paulatina reducción de este tipo de incidencias, ya que cada vez son más los ciudadanos que nunca han perdido archivos (desde el 41,5% en el primer trimestre de 2009 hasta el 47% en el primer trimestre de 2010).

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



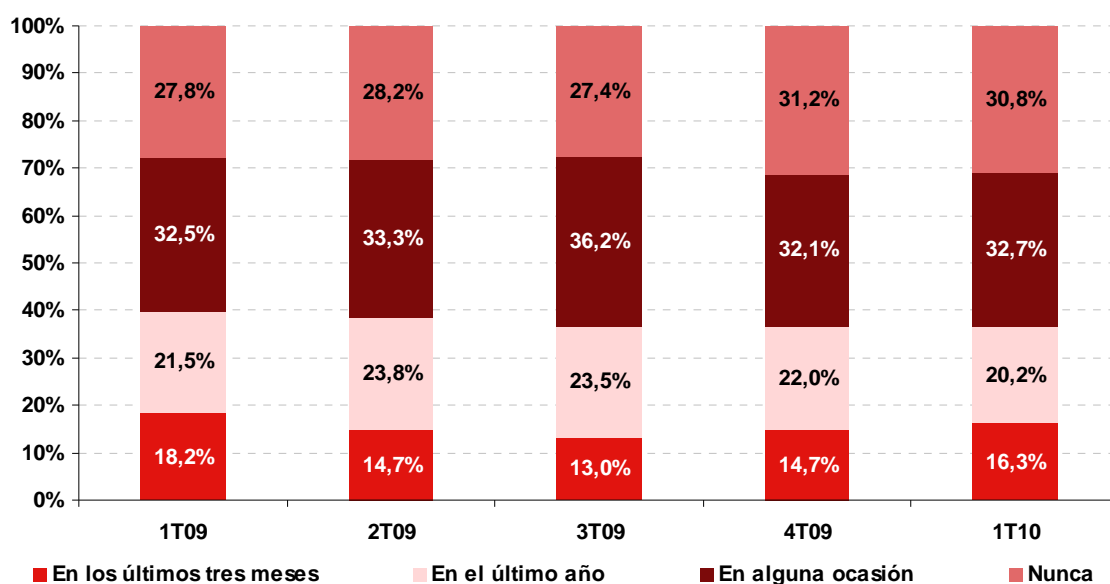
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

Un 16,3% de ciudadanos españoles usuarios de Internet ha tenido que formatear el disco duro y reinstalar el sistema operativo en los últimos tres meses, un 20,2% en el último año y un 32,7% en algún momento antes del último año. El resto, 30,9% de ciudadanos, no lo ha tenido que hacer nunca.

Los porcentajes se han mantenido muy estables desde el primer trimestre de 2009.

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



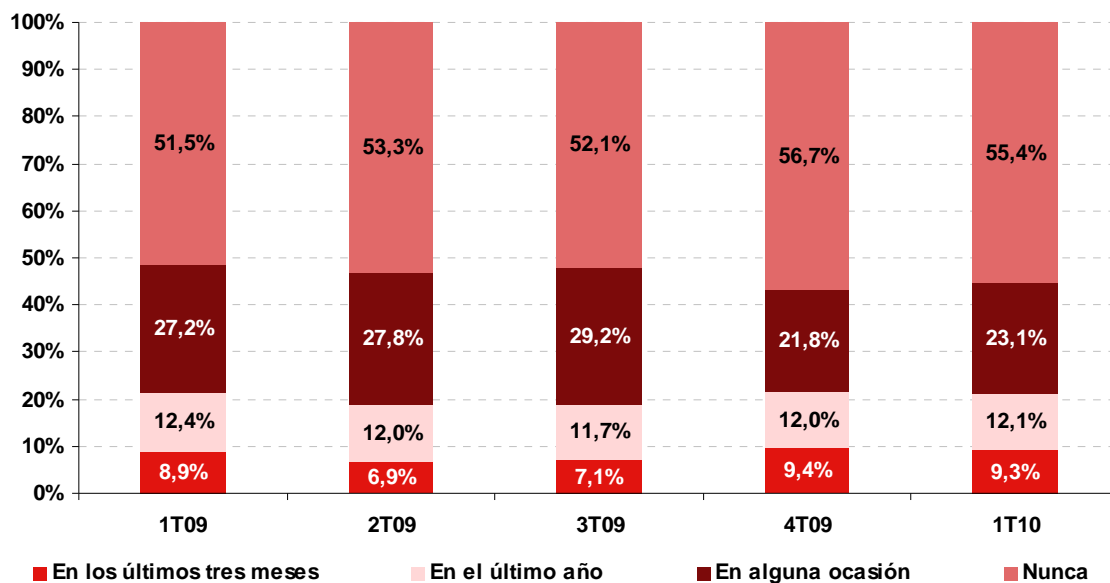
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

De las tres analizadas, la consecuencia que en menor medida ha afectado a los usuarios de Internet es la incidencia de daños en el hardware. Así, sólo un 9,3% de encuestados se ha enfrentado a este tipo de consecuencias en los últimos tres meses, frente a un 12,1% que lo ha hecho en el último año y un 23,1% que en algún momento anterior.

En cualquier caso, son mayoría (55,4%) quienes nunca han experimentado daños en el hardware a consecuencia de una incidencia de seguridad.

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



Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

5.2 Cambios adoptados tras una incidencia de seguridad

El 41,2% de los usuarios declaran haber modificado sus hábitos en los últimos 3 meses como consecuencia de los incidentes de seguridad sufridos, frente al 58,8% que mantiene sus hábitos inalterables.

Los cambios se dirigen a dos áreas, principalmente: en primer lugar, se modifican las medidas o herramientas de seguridad que utilizan; en segundo lugar, se cambian de algún modo los hábitos del usuario en el uso de Internet. Los siguientes subepígrafe profundizan en ambos.

5.2.1 Cambios en las medidas o herramientas de seguridad

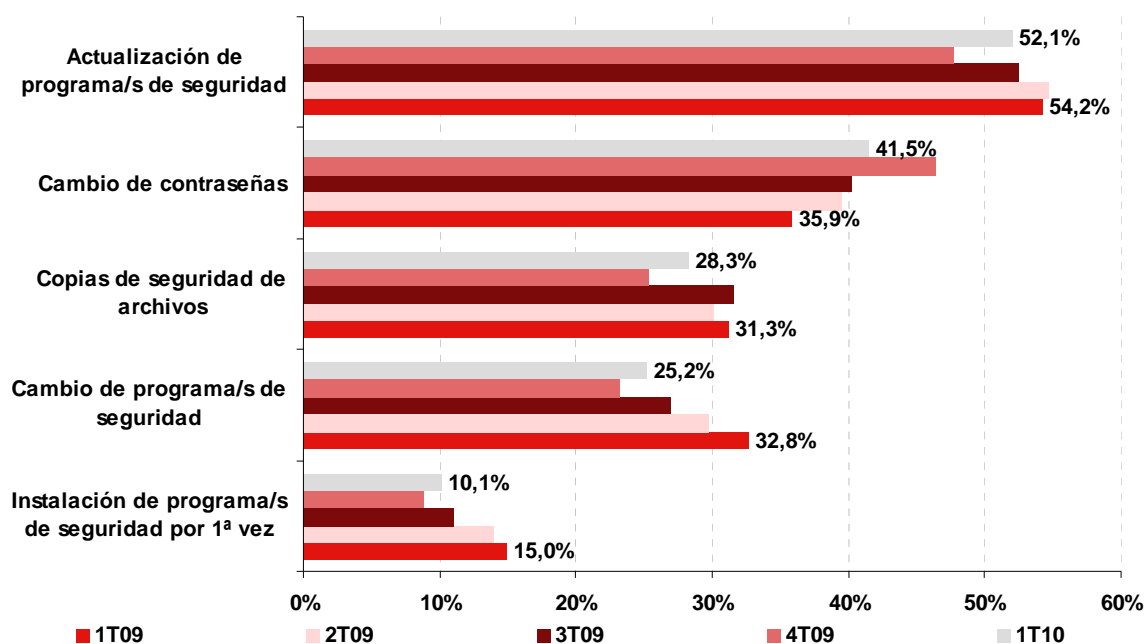
Tras sufrir un incidente de seguridad, la opción mayoritaria para muchos ciudadanos pasa por modificar sus herramientas o hábitos referidos a la protección de su sistema:

- Un 52,1% ha actualizado sus programas de seguridad a consecuencia del incidente. Esta reacción es la más adoptada por los usuarios (y a su vez, la mayor parte de las veces, la más efectiva).
- Un 41,5% ha optado por cambiar las contraseñas. Si el sistema ha sido comprometido, es muy posible que un potencial atacante haya robado las contraseñas que pueden quedar almacenadas, por ejemplo, en el navegador del sistema. Por esta razón es muy importante, tras un incidente de seguridad,

modificar las contraseñas de los servicios online a los que se accede, e incluso del sistema operativo.

- Un 28,3% decide realizar copias de seguridad, dato que se mantiene relativamente estable en los diferentes trimestres.
- Un 25,2% de los usuarios modifica sus programas de seguridad.
- Por último, solo un 10,1% instala programas de seguridad por primera vez tras un incidente.

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=1.444 en 1T10) Fuente: INTECO

5.2.2 Cambios en el uso de servicios de Internet

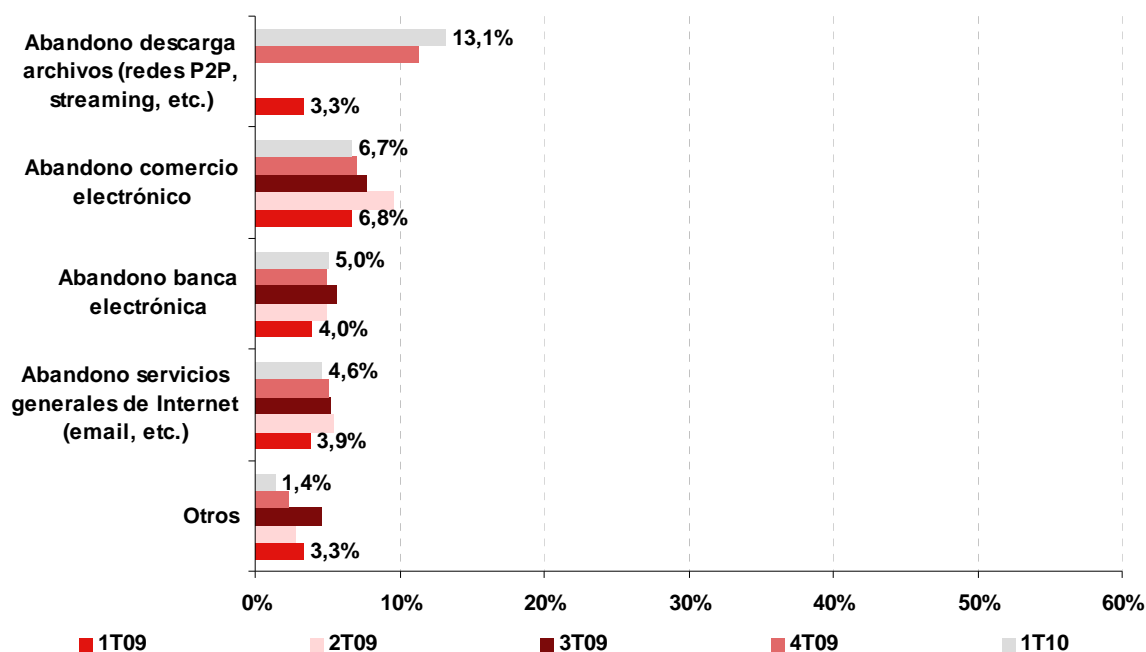
En el Gráfico 30 se estudia las reacciones de los usuarios que afectan a la modificación en el uso de los diferentes servicios de Internet. La pregunta a la que se pretende dar respuesta es: tras una incidencia de seguridad, ¿se abandona algún servicio de Internet?

El abandono de la descarga de archivos (a través de redes de pares, por ejemplo) es uno de los servicios que los usuarios parece considerar más prescindible. El porcentaje que abandona su uso alcanza el 13,1%, además de subir casi dos puntos porcentuales con respecto al trimestre anterior.

Con respecto al comercio electrónico, sólo un 6,7% de ciudadanos dice abandonarlo en el primer trimestre de 2010, después de sufrir un incidente. Con respecto al abandono de la banca online se sitúa en el 5% el porcentaje de usuarios que lo abandona tras un incidente.

El abandono de servicios generales de la red como correo electrónico, redes sociales, o mensajería instantánea, es la reacción menos popular entre los usuarios. Sólo un 4,6% decide prescindir de estas utilidades.

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=1.444 en 1T10) Fuente: INTECO

5.3 Resolución de incidentes de seguridad

¿Cómo resuelven los hogares españoles sus incidentes de seguridad? Se evalúan en este aspecto varias posiciones con respecto a la autonomía: desde llevar el ordenador al servicio técnico (la más dependiente), hasta la resolución del incidente por el propio usuario (la más autónoma). También se cuestionan grados intermedios de autonomía, como recurrir a familiares y amigos para asesorarse o las consultas a expertos para que el propio usuario, guiado por éste, la resuelva.

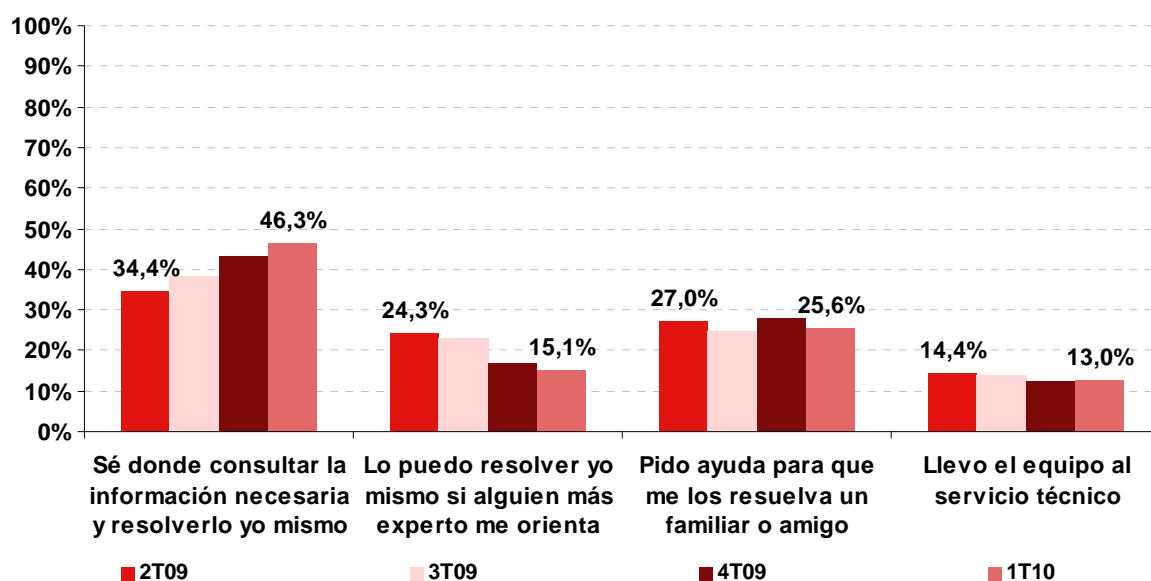
Se observa en este trimestre una enorme escalada de los usuarios que son capaces de resolver las incidencias por sí mismos: un 46,3% de panelistas así lo reconoce, lo que supone un incremento de 12 puntos porcentuales respecto al dato del 2º trimestre de 2009 (primero de la serie en el que se analiza esta variable). Los usuarios son cada vez

más autónomos a la hora de buscar información y encontrar solución a los problemas de seguridad.

El 15,1% admite ser capaz de resolver el incidente, siempre y cuando disponga de la figura de un experto que le oriente. Este tipo de ciudadanos, menos independientes que los anteriores, pero con un grado importante de autonomía en la resolución, ha ido disminuyendo progresivamente a lo largo de 2009. Parece que se ha ido produciendo un trasvase entre esta categoría y la anterior.

La opción de pedir ayuda para que resuelva el incidente alguien de confianza (25,6%) o llevar el equipo al servicio técnico (13%) implican un menor grado de iniciativa del ciudadano en la resolución de las incidencias, y se mantienen relativamente estables a lo largo de 2009.

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



Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

6 E-CONFIANZA DE LOS HOGARES ESPAÑOLES

Un sistema no se desarrolla ni avanza a menos que los usuarios confíen en él plenamente. En ocasiones, importantes avances tecnológicos, muy avanzados técnicamente, han quedado olvidados (o su penetración en la sociedad se ha retrasado) por la desconfianza que generaba su uso entre el público en general.

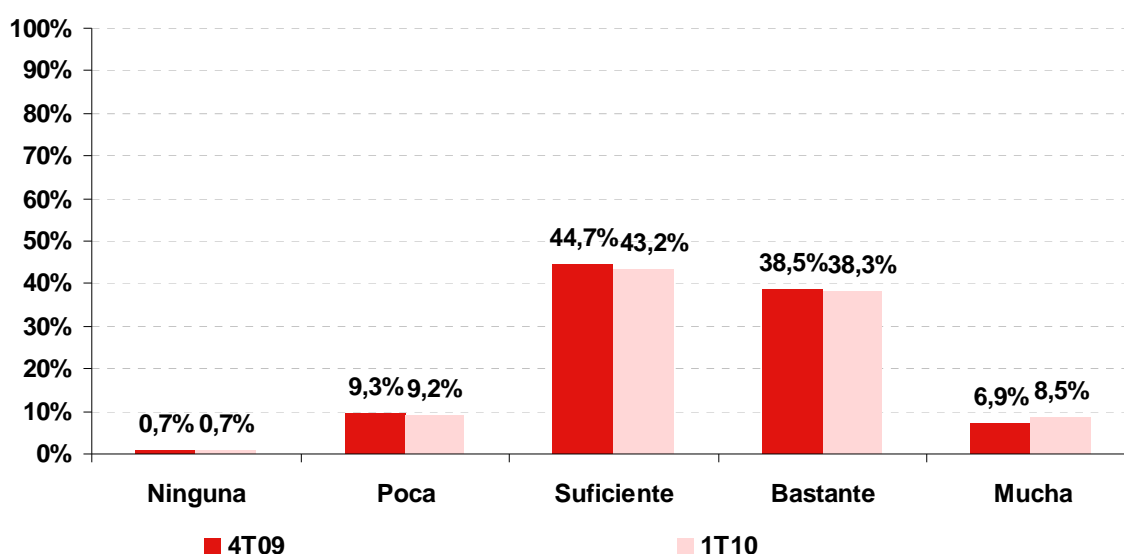
La seguridad es el elemento clave que debe ponerse de relieve para generar confianza en una herramienta como es hoy en día Internet. De lo seguro que se sientan los ciudadanos a la hora de utilizarlo dependerá su éxito y, por tanto, su desarrollo hacia una Sociedad de la Información cada vez más avanzada. Este capítulo mide el nivel de confianza en Internet percibido por los españoles.

Además, se describe la opinión de los usuarios sobre quiénes deben asumir la responsabilidad de garantizar una Red segura, y se identifican las actuaciones que se perciben como prioritarias para mejorar la situación de seguridad.

6.1 e-Confianza en la Sociedad de la Información

A un 38,3% de usuarios Internet les genera *bastante* confianza, y a un 8,5%, *mucha*. Si añadimos el porcentaje de ciudadanos que reconocen que Internet les produce un nivel de confianza *suficiente* (43,2%), el resultado es que un 90% de los encuestados confía en la Red. Sólo un 9,2% admite tener *poca* confianza y un 0,7% adicional, *ninguna*.

Gráfico 32: En general, ¿cuánta confianza le genera Internet? (1T 2010) (%)



Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

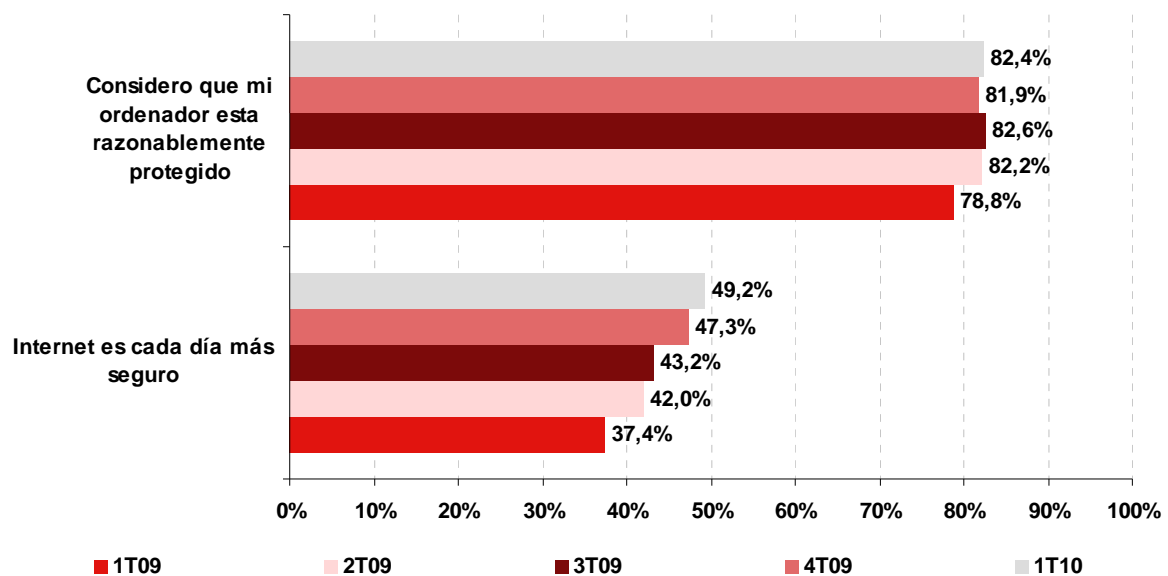
Se ha planteado al encuestado que muestre su grado de acuerdo o desacuerdo con las siguientes dos afirmaciones (los resultados se reflejan en el Gráfico 33):

- Considero que mi ordenador está razonablemente protegido.
- Internet es cada día más seguro.

Un 82,4% de los ciudadanos encuestados se muestran de acuerdo con la primera afirmación, sin que existan cambios significativos desde hace un año.

En el caso de la afirmación *Internet es cada día más seguro*, un 49,2% de los usuarios de Internet se muestran de acuerdo con la sentencia. En este caso, trimestre tras trimestre se incrementa el porcentaje de ciudadanos que comparte esta opinión, lo que puede constituir un síntoma favorable de la adecuada evolución de la Sociedad de la Información.

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



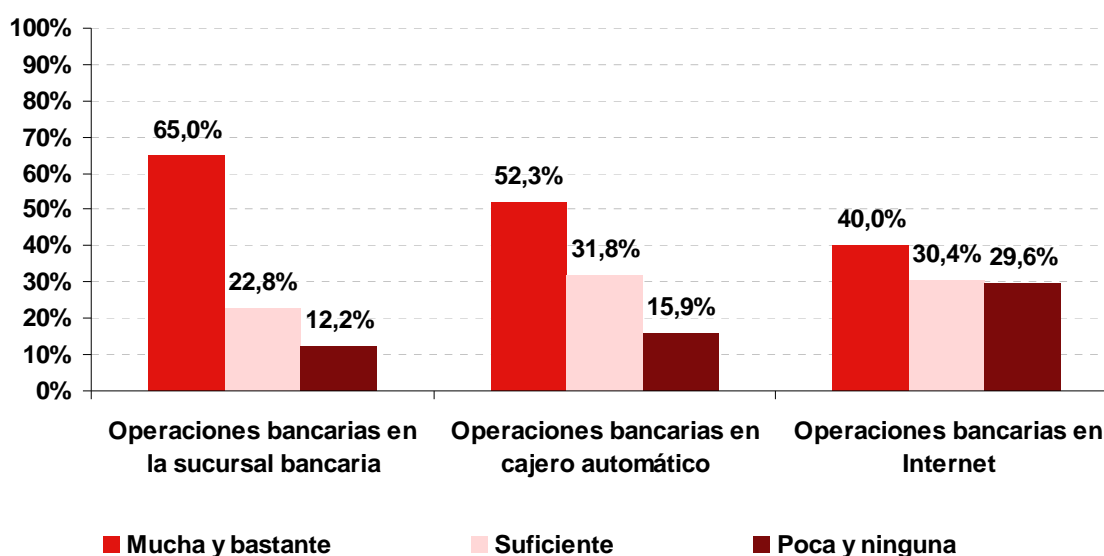
Base: Total usuarios (n=3.599 en 1T10)

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).

Operar directamente a través de la sucursal bancaria ofrece mucha o bastante confianza a un 65% de los encuestados. La segunda opción para los usuarios que más confianza genera es el uso del cajero automático: un 52,3% muestra que este tipo de operación les ofrece mucha y bastante confianza. Las operaciones bancarias por Internet, aunque con un menor porcentaje, ofrecen mucha y bastante confianza a un importante 40% de los encuestados.

Gráfico 34: Confianza en la realización de actividades físicas / online relacionadas con operaciones bancarias 1T 2010 (%)



Base: Total usuarios (n=3.599)

Fuente: INTECO

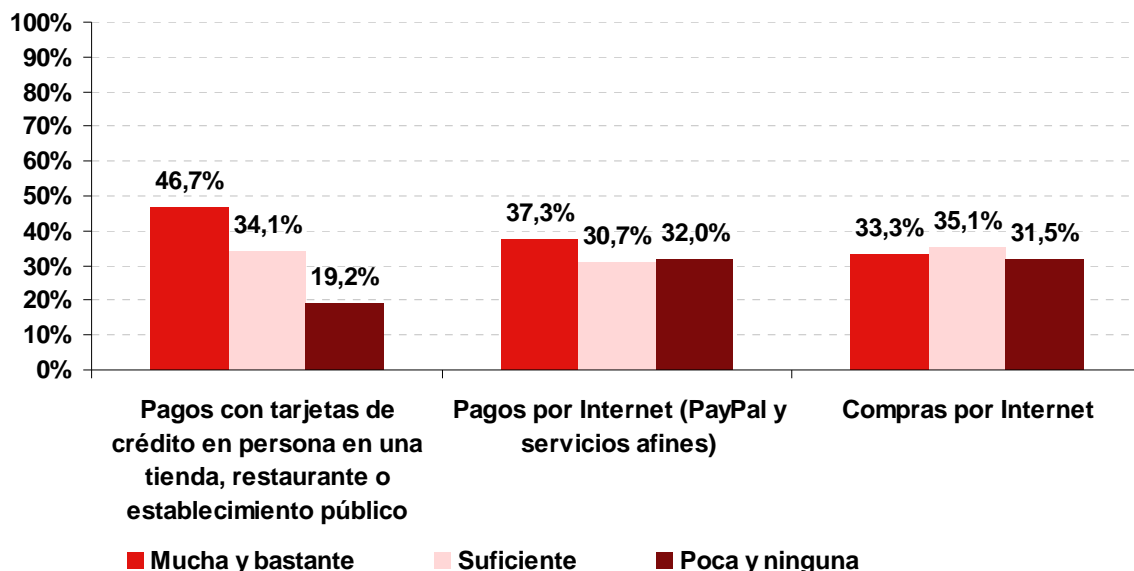
Con respecto a la realización de compraventas o transacciones de carácter económico, en el siguiente gráfico se puede comprobar el contraste entre la confianza que el ciudadano deposita en llevar a cabo estas actividades en el mundo físico o hacerlo en el entorno virtual.

Al igual que ocurría al analizar la realización de transacciones bancarias, 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.

Así, un 46,7% reconoce confiar mucho o bastante en el pago con tarjeta en un establecimiento físico, frente a un 34,1% que reconoce confiar de manera suficiente y sólo un 19,2% que confía poco o nada.

En el caso de los pagos por Internet a través de un sistema de pago seguro como PayPal, un 37,3% se muestra muy confiado hacia ellos. El porcentaje, en el caso de compras en Internet en general, es de 33,3%.

Gráfico 35: Confianza en la realización de actividades físicas / online relacionadas con pagos y transacciones de compraventa 1T 2010 (%)



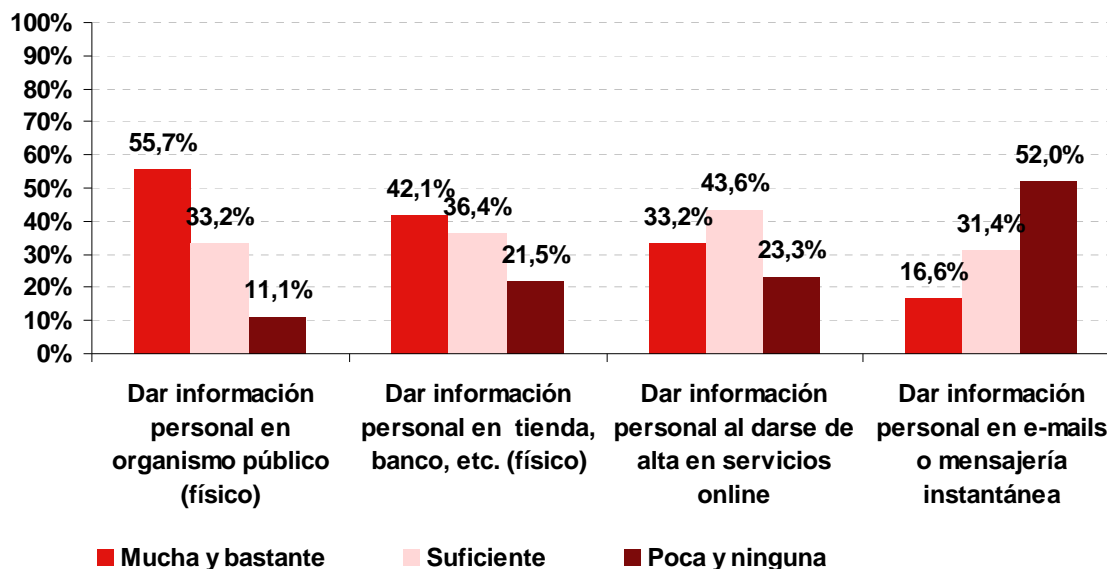
Base: Total usuarios (n=3.599)

Fuente: INTECO

También en el caso de operaciones referidas al intercambio de datos de carácter personal la confianza de los encuestados es superior cuando se llevan a cabo en un contexto físico que cuando suceden a través de la Red. 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* más de la mitad, hasta un 52,0%. Sin embargo, si la información es necesaria con el fin de darse de alta en algún servicio online, mayoritariamente los usuarios confían lo suficiente en el servicio, un 43,6%.

En el mundo físico, ofrecer datos personales a las administraciones públicas (Ayuntamientos, por ejemplo) es lo que más tranquilidad aporta a los usuarios. Un 55,7% dice que ofrece datos personales a estos organismos con mucha o bastante confianza. Los usuarios también se sienten relativamente confiados al proporcionar información de carácter personal en tiendas o bancos si es en persona: un 42,1% le ofrece mucha y bastante confianza este método.

Gráfico 36: Confianza en la realización de actividades físicas / online relacionadas con los datos personales 1T 2010 (%)



Base: Total usuarios (n=3.599)

Fuente: INTECO

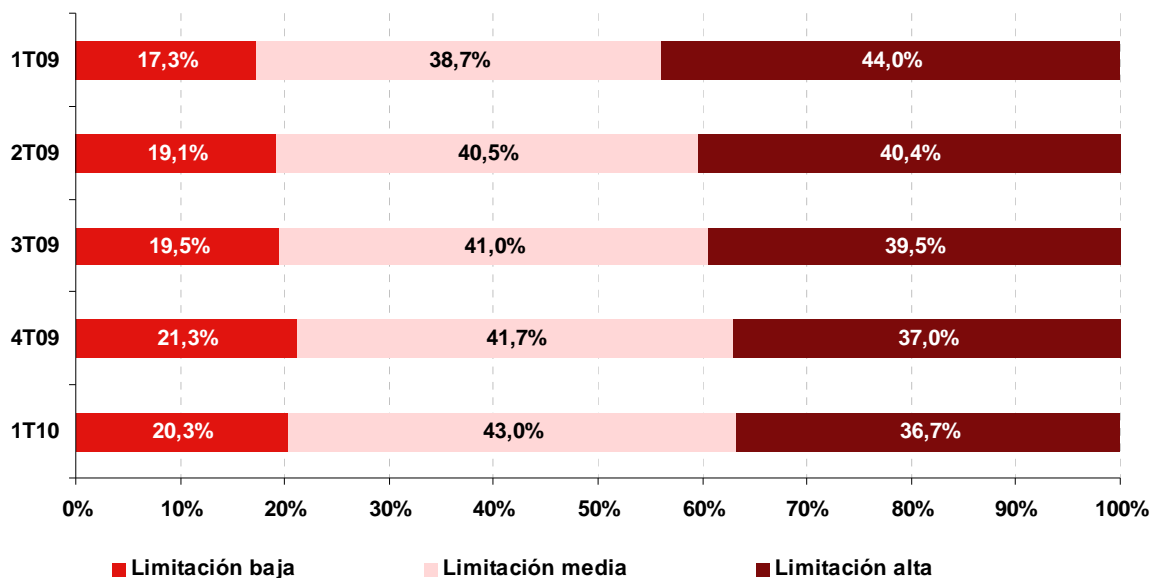
Una vez descrito en nivel general de confianza que los usuarios de Internet españoles depositan en Internet, el Gráfico 37 analiza el posible impacto de la seguridad (o falta de seguridad) sobre la utilización de Internet. Para ello, se pidió a los encuestados que respondieran en qué grado la seguridad limitaba la utilización de nuevos servicios en Internet¹¹.

En el primer trimestre de 2010, el 20,3% de los usuarios de Internet españoles consideran que la seguridad supone una limitación baja a la hora de utilizar nuevos servicios de Internet, frente a un 43% que responde que la limitación es media y un 36,7% en el caso de los que argumentan una limitación alta.

Los datos ofrecen una perspectiva evolutiva. Se observa un descenso lento, pero continuo, del porcentaje de usuarios que declara que la seguridad les limita a la hora de utilizar nuevos servicios: Desde un 44% hace un año a un 36,7% a principios de 2010.

¹¹ Se ofreció a los encuestados una escala del 0 al 10, donde el 0 equivale a "No limita nada" y el 10 a "limita totalmente". A efectos de presentación de datos, se han agrupado las respuestas siguiendo el siguiente criterio: limitación baja: 0-3; limitación media: 4-6; limitación alta: 7-10.

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



Base: Total usuarios (n=3.599)

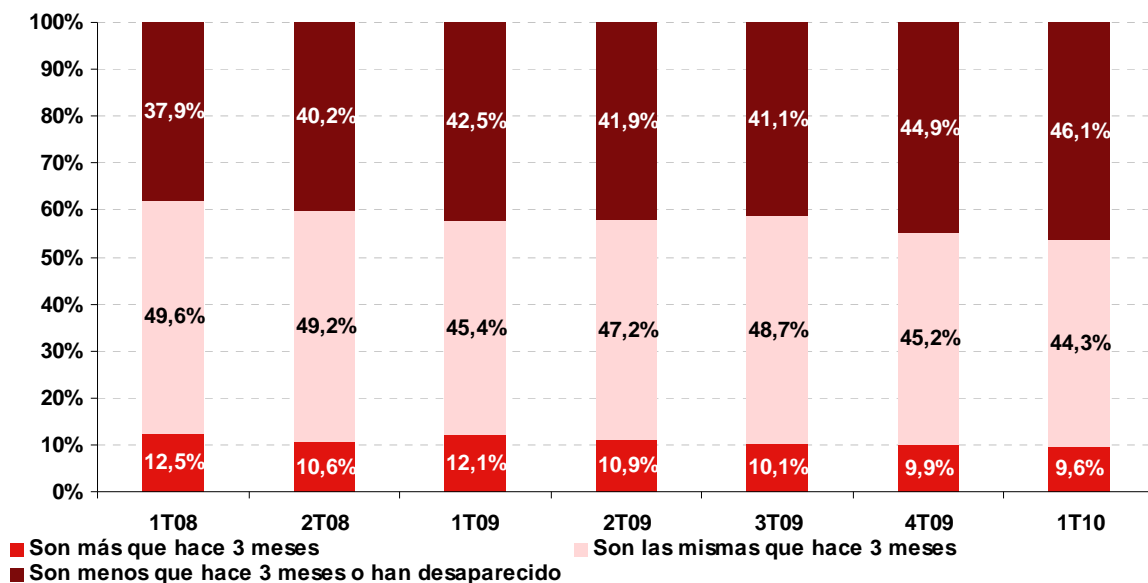
Fuente: INTECO

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

En el primer trimestre de 2010, un 46,1% de los usuarios piensan que el número de incidencias de seguridad es inferior al que había hace tres meses. Un 44,3% cree que son las mismas y un 9,6%, que son más que hace un trimestre.

La perspectiva histórica permite identificar tendencias. Parece que, de manera continuada, los ciudadanos cada vez perciben un menor número de incidencias de seguridad. Así, si en el primer trimestre de 2008 era un 37,8% a proporción de usuarios que consideraba que en ese momento el número de incidencias era inferior al pasado, dos años después el porcentaje alcanza un 46,1% de panelistas.

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



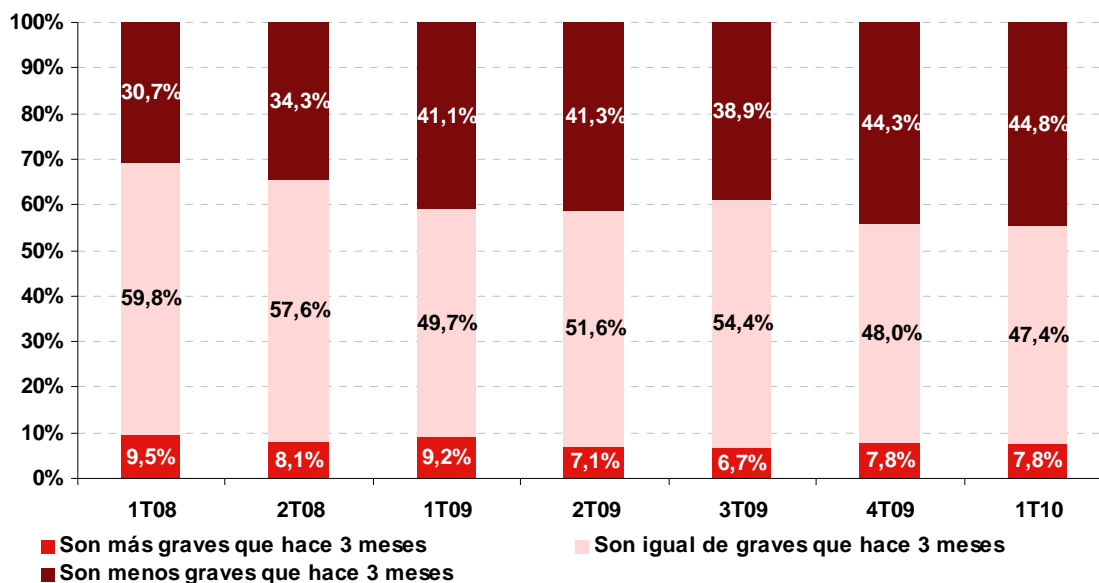
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

Los usuarios españoles perciben que cada vez hay menos incidencias de seguridad y, además, que éstas son menos graves. Así lo confirma el Gráfico 39, donde se puede comprobar cómo el porcentaje de usuarios que considera que las incidencias son en la actualidad menos graves que hace tres meses alcanza al 44,8% en el primer trimestre de 2010 (en el primer trimestre de 2008 era de sólo un 30,7%).

Un 47,4% piensa que son igual de graves y un 7,8%, en cambio, opina que en el momento actual las incidencias de seguridad son más graves que en el pasado.

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



Base: Total usuarios (n=3.599 en 1T10)

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.

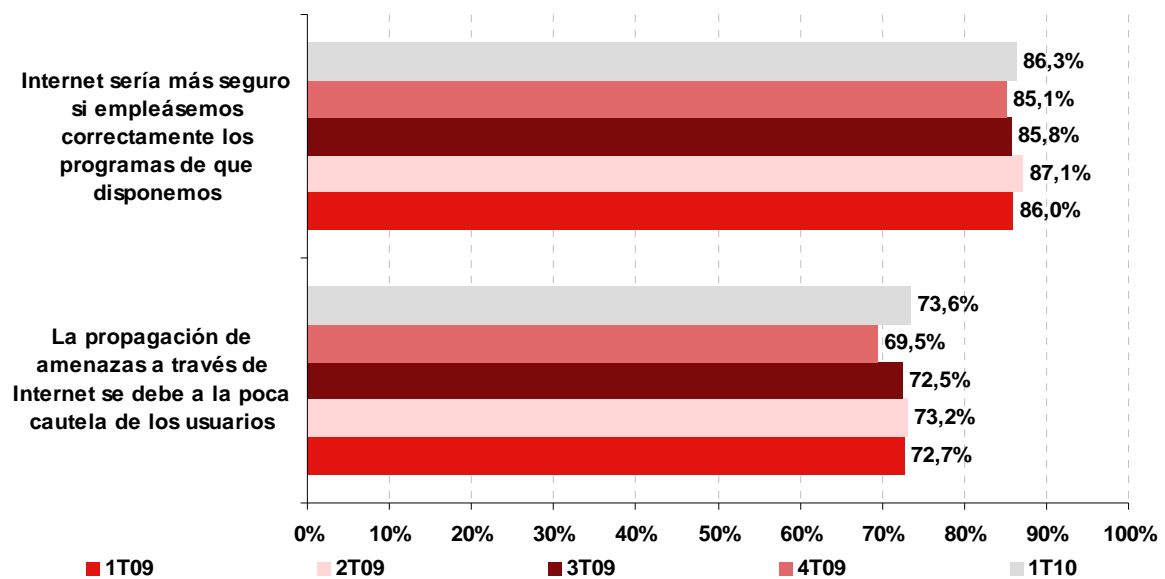
6.3.1 Usuarios

En este epígrafe profundizamos en dos medidas de autorregulación, analizando el nivel de acuerdo de los ciudadanos españoles con dos afirmaciones que implican cierta responsabilidad de los usuarios a la hora de asegurar la seguridad en Internet.

Una gran mayoría de usuarios (86,3%) se muestra de acuerdo en que un uso más adecuado de los programas de seguridad disponibles ayudaría a disponer de un Internet más seguro. No se han experimentado movimientos destacables de percepción en el último año.

También es mayoritaria la percepción de que la propagación de amenazas a través de la Red se debe a la poca cautela de los usuarios (73,6%).

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



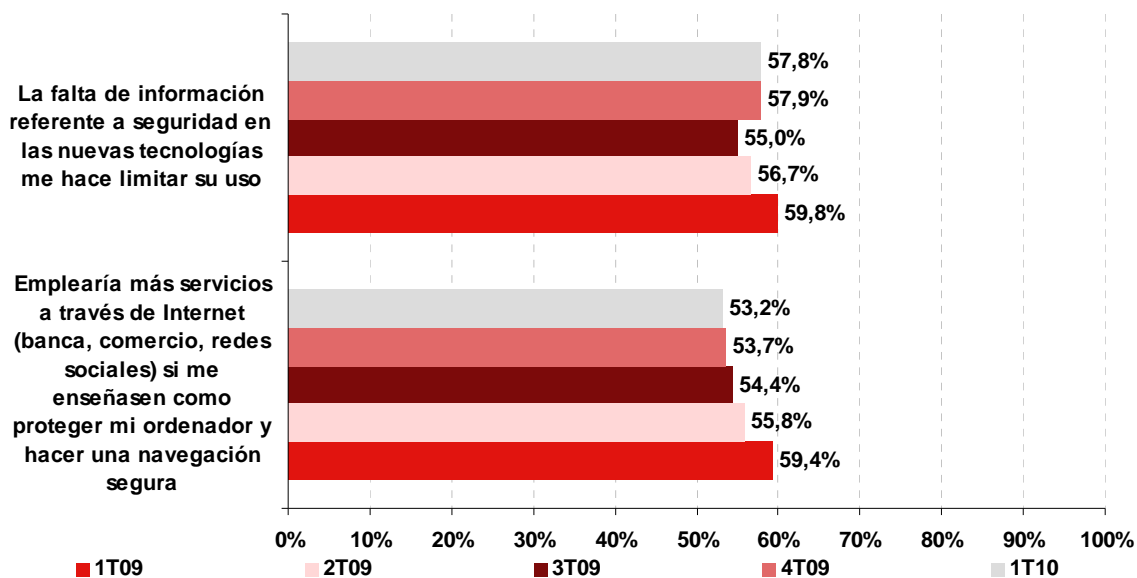
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

La información es uno de los pilares fundamentales para mantener unos hábitos seguros con respecto a la seguridad. En este sentido se le ha preguntado a los usuarios sobre cómo influye la falta de información a la hora de utilizar con seguridad los recursos disponibles en Internet. Un porcentaje estable en los últimos trimestres (53,2%) se muestra de acuerdo en que aprovecharía más y mejor los servicios de Internet si dispusiera de la información necesaria para proteger adecuadamente su equipo.

De la misma manera, un 57,8% confiesa que la falta de información sobre seguridad y buenos hábitos les limita para desarrollar tareas relacionadas con servicios en la Red. Este porcentaje también se ha mantenido estable en los últimos meses.

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



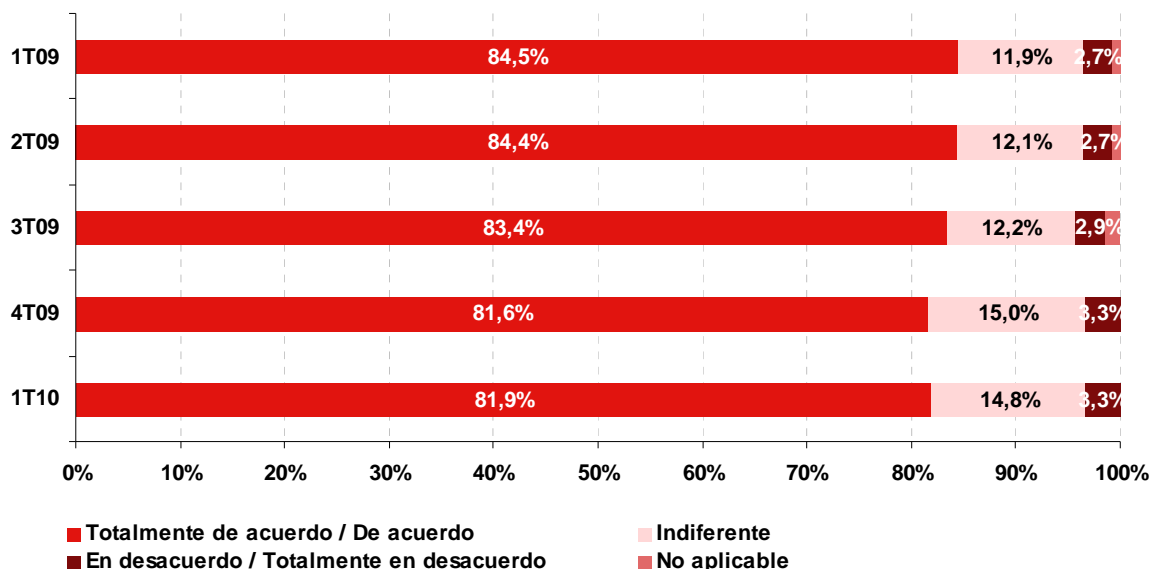
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

6.3.2 Papel de la administración en la garantía de la Seguridad de la Información

Se ha indagado en la opinión de los usuarios acerca de la participación de la Administración para ayudar a crear una Red más segura (tutelaje, según la definición manejada anteriormente). Un 81,9% está *totalmente de acuerdo* o *de acuerdo* en que la Administración debe implicarse en este sentido para mejorar la seguridad, y solo un 3,3% no lo encuentra adecuado.

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=3.599 en 1T10)

Fuente: INTECO

En la Tabla 5 se muestran las medidas concretas que los ciudadanos piden a la Administración para mejorar la seguridad de la Red.

Se han agrupado las medidas en varios grupos: medidas de vigilancia, de respuesta técnica, de sensibilización y de respuesta institucional y legislativa.

La medida más demandada a la Administración es la vigilancia cercana de lo que está pasando en Internet (28,4%). En segundo lugar, requieren el desarrollo de herramientas de seguridad gratuitas que le permitan asegurar sus equipos y comunicaciones (25,9%). Como tercera opción, piensan que se deberían actualizar y reformar las leyes relativas a los delitos por Internet (11,7%).

Tabla 5: Medidas demandadas a la Administración 1T 2010 (%)

Carácter de la medida	Medida	Medida prioritaria
Vigilancia	Vigilar más de cerca lo que está pasando en Internet	28,4%
	Velar por el uso adecuado de los datos personales en Internet	8,9%
Respuesta técnica	Dar respuesta/soporte técnico a los problemas de seguridad de los ordenadores de los ciudadanos	6,6%
	Desarrollar y ofrecer herramientas de seguridad gratuitas	25,9%
Sensibilización	Hacer campañas de información y sensibilización sobre los riesgos y cómo prevenirlos	6,1%
	Ofrecer cursos y talleres formativos sobre servicios de Internet y seguridad	3,7%
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	8,2%
	Actualización y reforma legislativa para los nuevos delitos por Internet	11,7%
TOTAL		99,5

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=3.053) Fuente: INTECO

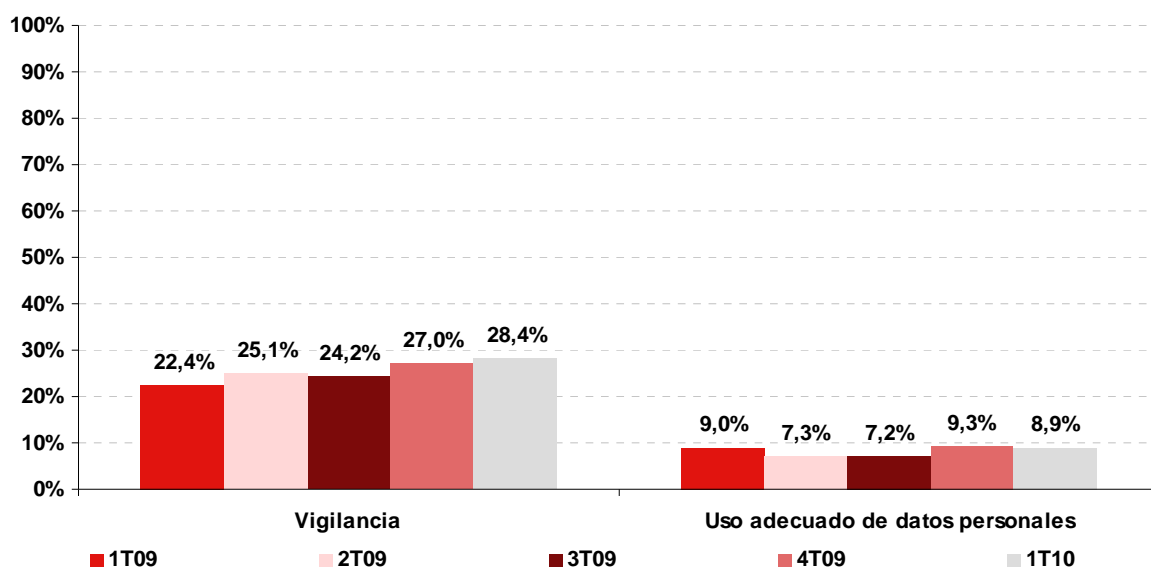
Se analiza a continuación la evolución en la demanda de medidas a la Administración.

Medidas de vigilancia

La medida de vigilar más de cerca lo que ocurre en Internet no es solo la más demandada a la Administración, con 28,4% de los ciudadanos que consideran que sería la primera medida a tomar, sino que además el porcentaje de usuarios que así lo perciben ha ido incrementándose paulatinamente desde el primer trimestre de 2009 (donde sólo el 22,4% de ciudadanos confiaba en la prioridad de esta medida).

La medida de velar por el uso adecuado de los datos personales, con un 8,9% menciones, se mantiene sin cambios importantes a lo largo del año.

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=3.053) Fuente: INTECO

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

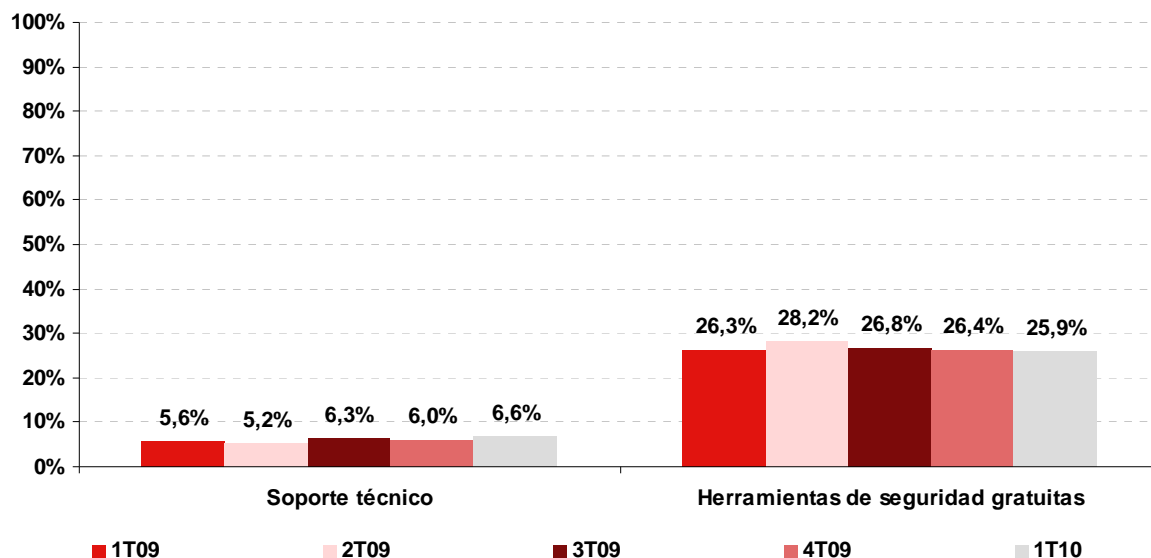
- El Observatorio de la Seguridad de la Información de INTECO (<http://observatorio.inteco.es>) tiene como objetivo vigilar, estudiar y describir la situación general de seguridad en Internet. Así, los informes periódicos del Observatorio (de los que este documento forma parte) son el registro escrito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

Los usuarios que piden a la Administración un soporte técnico con el que puedan resolver sus dudas se mantiene ligeramente al alza en el último año, alcanzando en el primer trimestre de 2010 un 6,6% de los usuarios a favor de esta medida, solo un punto por encima del dato de hace un año.

La demanda de herramientas de seguridad gratuitas, alegada por un 25,9% de los usuarios, se ha mantenido en niveles elevados y estables desde principios 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=3.053) Fuente: INTECO

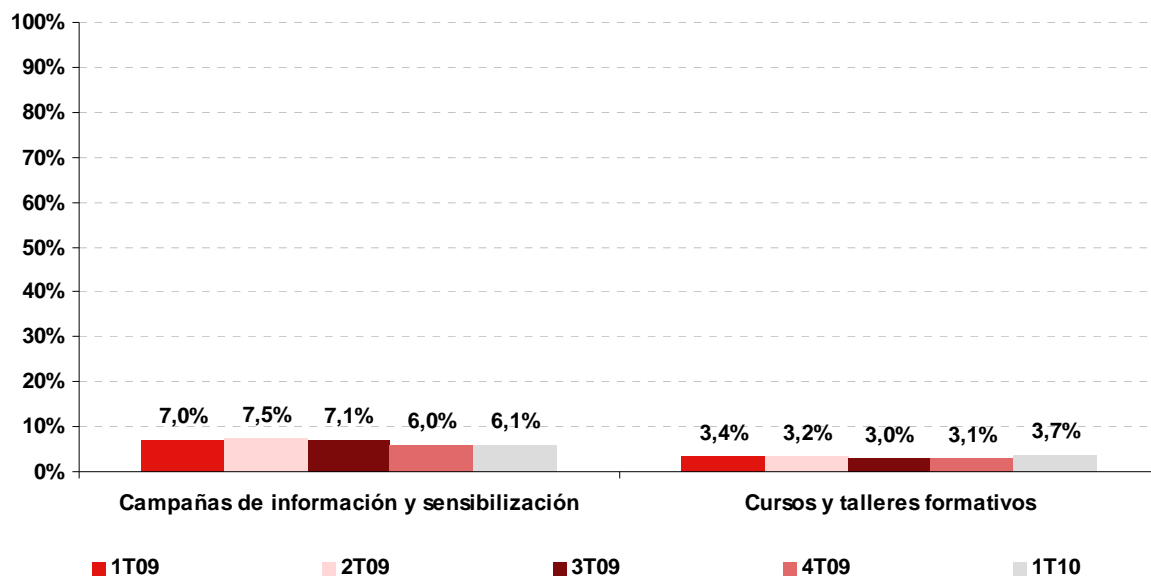
Se destacan a continuación algunas iniciativas de la Administración que tienen que ver con respuesta técnica:

- 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_Gratis/.

Medidas de sensibilización

En general, las medidas de sensibilización son poco demandadas a la Administración. Un 6,1% demanda como medida prioritaria la implementación de campañas de información y sensibilización, en una tendencia moderadamente decreciente. Menos aún (3,7%, bastante estable a lo largo de los cinco períodos analizados) son los que consideran prioritaria la organización de cursos y talleres formativos en materia de seguridad informática.

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



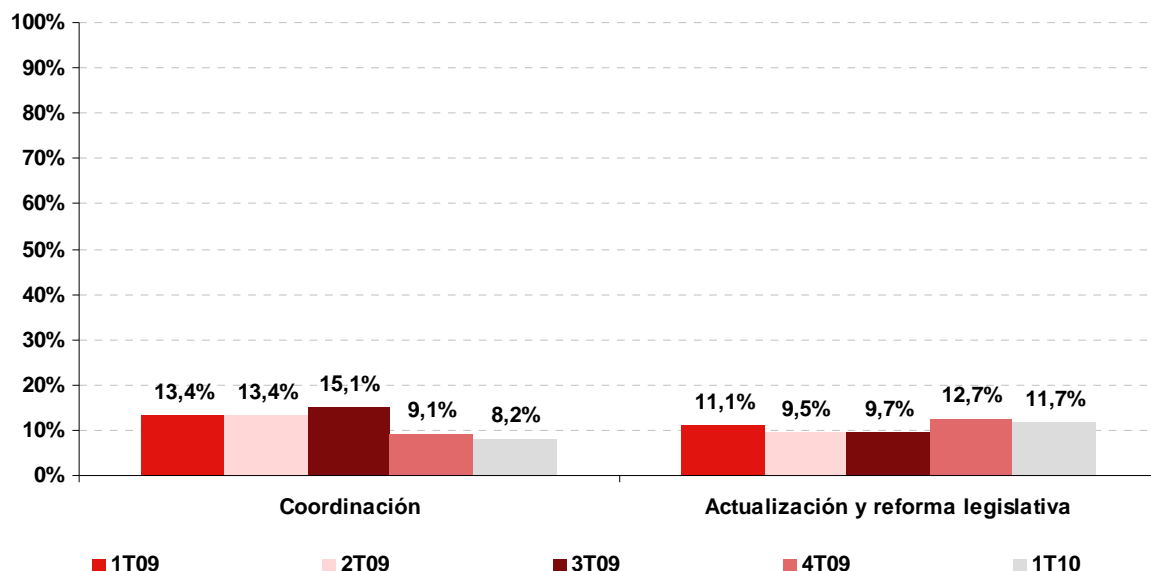
Base: Usuarios que se muestran totalmente de acuerdo y de acuerdo con la afirmación La Administración tiene que implicarse más en mejorar la seguridad en Internet (n=3.053) Fuente: INTECO

Medidas de respuesta institucional y legislativa

Con respecto a las medidas de respuesta institucional, se consolida la bajada de porcentaje de usuarios que requiere una mayor coordinación entre los diferentes organismos institucionales para agilizar y mejorar la seguridad. Del 13,4% que lo demandaba como prioritario en el primer trimestre de 2009, con un pico de 15,1% en el tercer trimestre de 2009, en esta última lectura son un 8,2% los que estiman que una mayor coordinación es la primera medida a adoptar por la Administración.

La actualización y reforma legislativa es una medida prioritaria para el 11,7% de los ciudadanos, con ligeros altibajos desde el inicio de las lecturas.

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=3.053) Fuente: INTECO

Las acciones de coordinación han sido 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.

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*¹², 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.

La Tabla 6 ilustra en qué medida ven como responsables los ciudadanos a los diferentes actores descritos.

Sin duda, los usuarios se ven a sí mismos como responsables, con un indiscutible 38,1%. Como se ha confirmado con análisis anteriores, son conscientes de que sus hábitos en cuestión de seguridad tienen una repercusión muy directa sobre la seguridad global en Internet. Por detrás de ellos, un 28,4% considera que el principal responsable es la Administración.

El tercer responsable son los proveedores de servicios de Internet con un 20%. Por último, el cuarto responsable para los usuarios son las empresas que crean herramientas de seguridad, con un 13,5% de menciones.

Tabla 6: Consideración de quiénes son los responsables de la seguridad en Internet 1T10 (%)

Actor analizado	Primer responsable	Segundo responsable	Tercer responsable	Cuarto responsable
Usuarios	38,1%	17,8%	16,9%	27,2%
Administraciones	28,4%	22,7%	21,6%	27,2%
Proveedores de servicios de Internet	20,0%	28,5%	28,7%	22,7%
Empresas que crean herramientas de seguridad	13,5%	30,9%	32,8%	22,8%

Base: Total usuarios (n=3.599)

Fuente: INTECO

¹² <http://www.oecd.org/dataoecd/53/34/40724457.pdf>

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
	IS.4 Indicador de incidencias de malware
Indicadores de riesgos	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 aquéllos que miden y señalan la protección existente y en el segundo aquéllos 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.

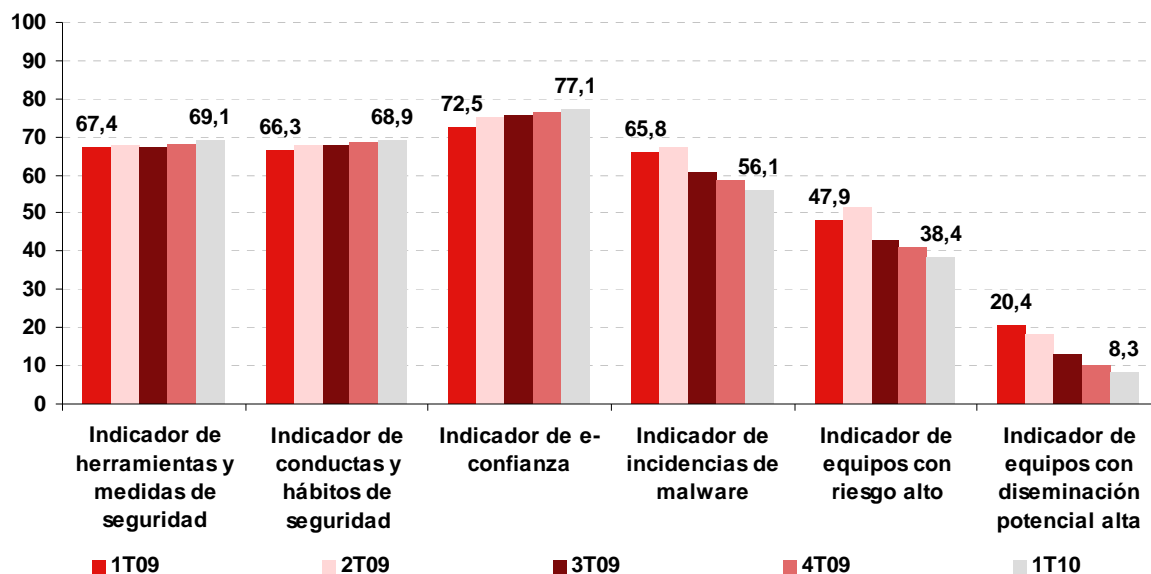
7.2 Análisis de los indicadores de la seguridad de la información

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

En el análisis conjunto del sistema se confirma el funcionamiento de los indicadores: los indicadores de protección han aumentado de manera moderada, pero constante, a lo largo de 2009. Este incremento en los dos indicadores, *Indicador de herramientas y medidas de seguridad* e *Indicador de conductas y hábitos de seguridad*, guarda relación con el importantísimo descenso de los tres indicadores de riesgos.

Como consecuencia del aumento progresivo de la seguridad y de la reducción importante y continuada del nivel de riesgo de los equipos, el indicador de e-confianza experimenta una evolución positiva.

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

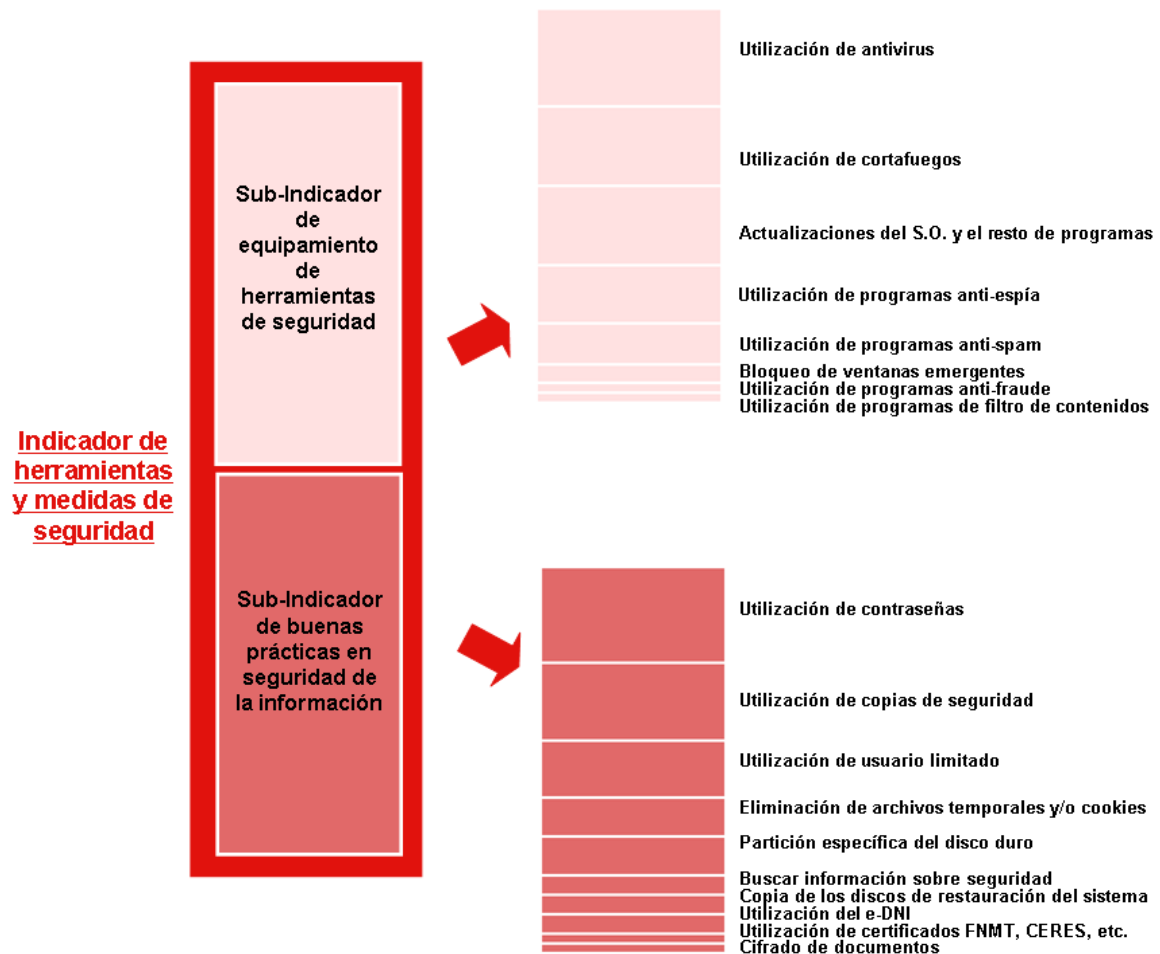
Este indicador compuesto mide el equipamiento y adopción de medidas de seguridad que existen en la actualidad. Su cálculo no sólo se centra en la propia seguridad del sistema, sino que también incluye medidas que favorecen la seguridad de la información.

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.

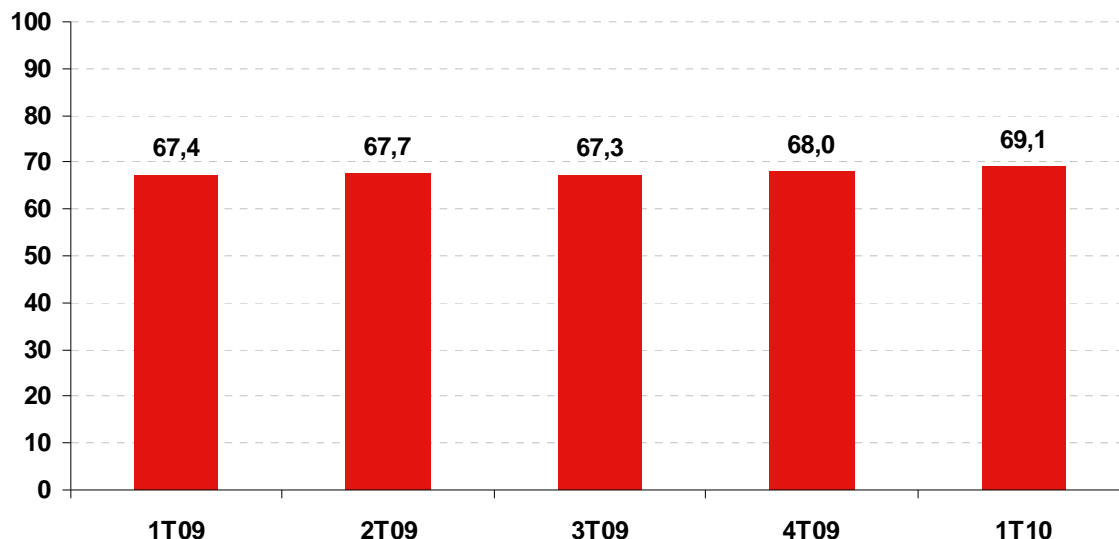
Ilustración 1: Indicador de herramientas y medidas de seguridad



Fuente: INTECO

El indicador de herramientas y medidas de seguridad ha experimentado una evolución positiva lenta, pero continuada, a lo largo de 2009. Este primer trimestre de 2010 alcanza un valor de 69,1, lo que representa un incremento de casi 2 puntos desde el mismo período del año anterior.

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

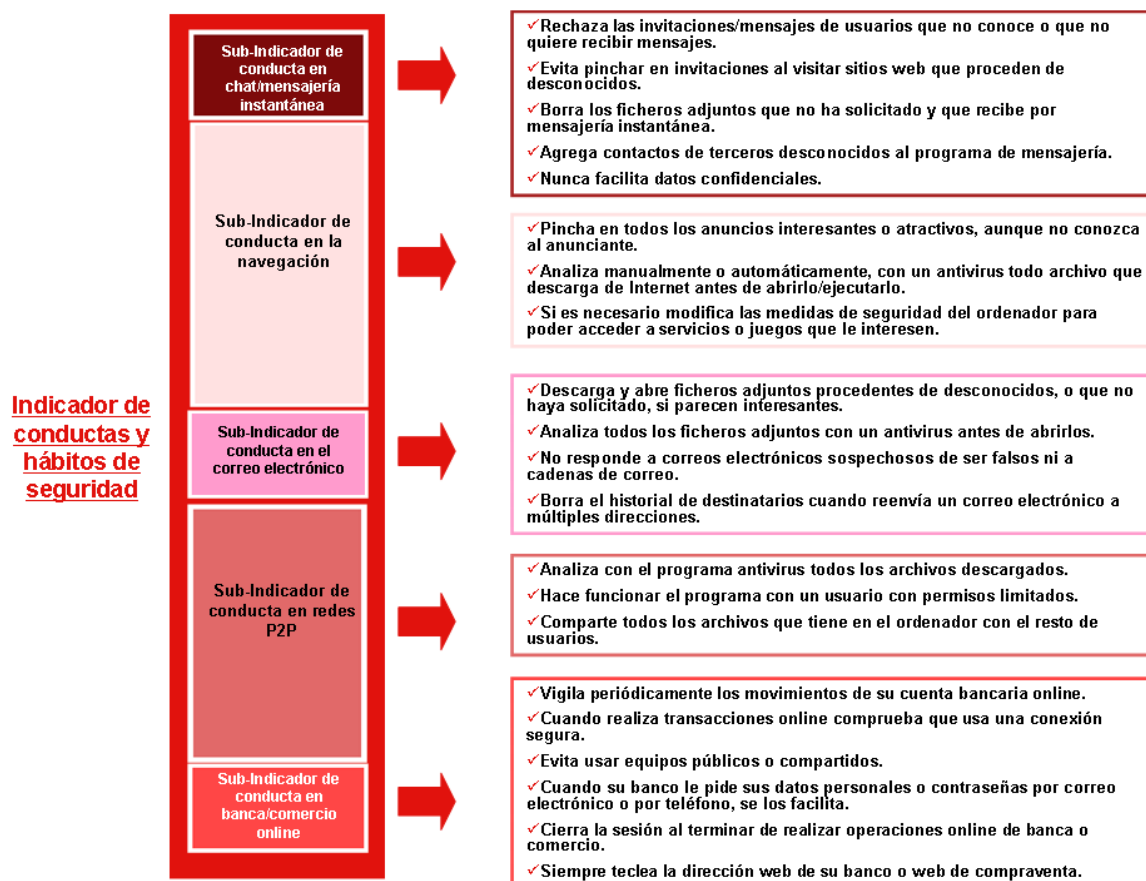
Mide el tipo de comportamiento y hábitos seguros durante la navegación por Internet y el uso de determinados servicios online, sintetizando la puntuación obtenida en los siguientes aspectos.

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.

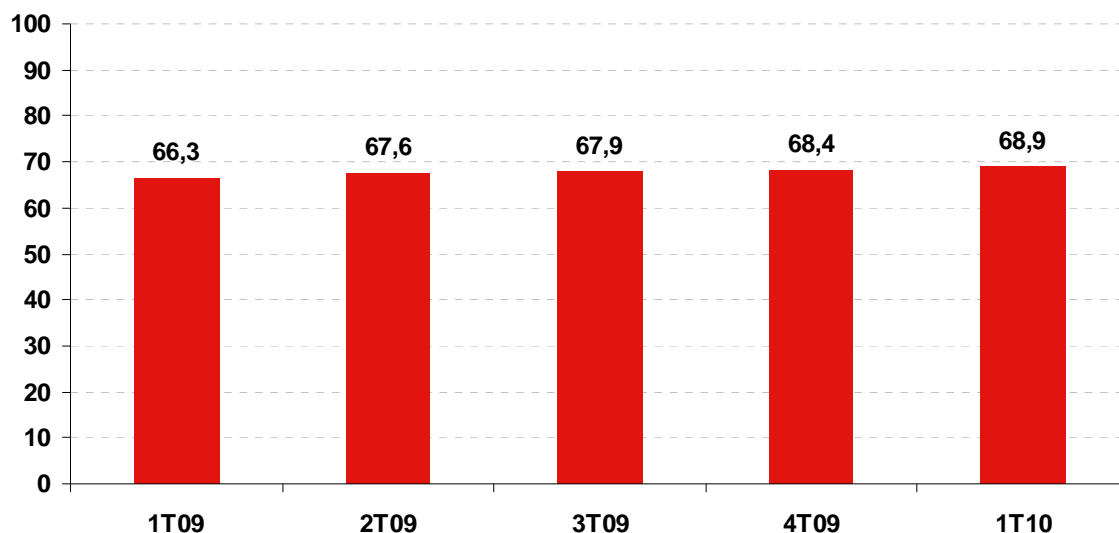
Ilustración 2: Indicador de conductas y hábitos de seguridad



Fuente: INTECO

El indicador de conductas y hábitos de seguridad, igual que el de herramientas analizado anteriormente, experimenta una lenta evolución positiva, alcanzando hasta el 68,9 en el primer trimestre de 2010 (2,6 puntos más que el nivel que ofrecía la lectura del primer trimestre de 2009).

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



Fuente: INTECO

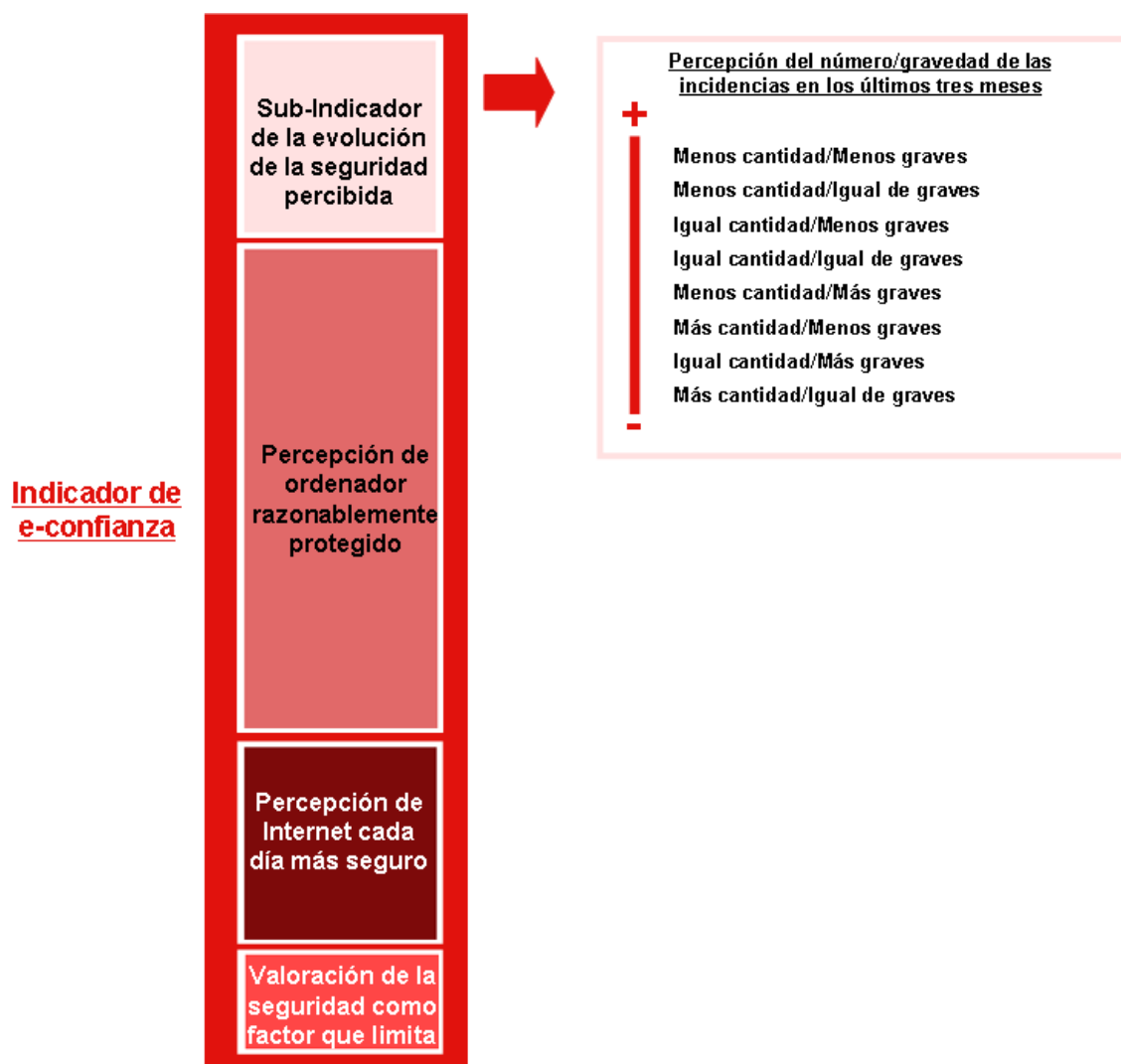
7.2.3 Indicador de e-confianza

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.

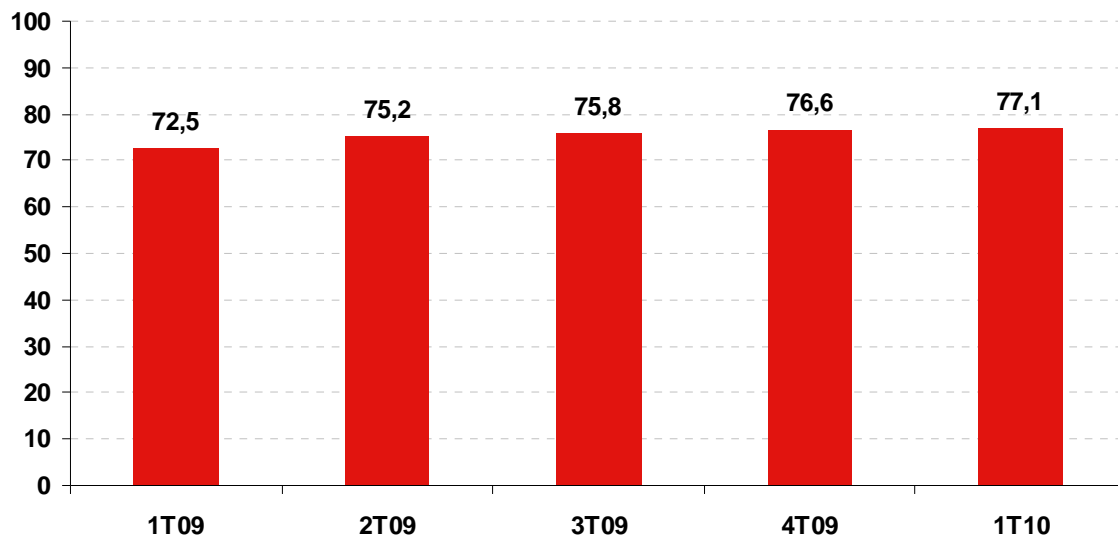
Ilustración 3: Indicador de e-confianza



Fuente: INTECO

En el siguiente gráfico se muestra la evolución del indicador de e-confianza. Este primer trimestre de 2010 alcanza un valor de 77,1. Desde el primer trimestre de 2009, el valor de este indicador se ha ido incrementando de manera continuada, lo que representa un indicio positivo de la evolución del nivel de confianza de los usuarios de Internet españoles.

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

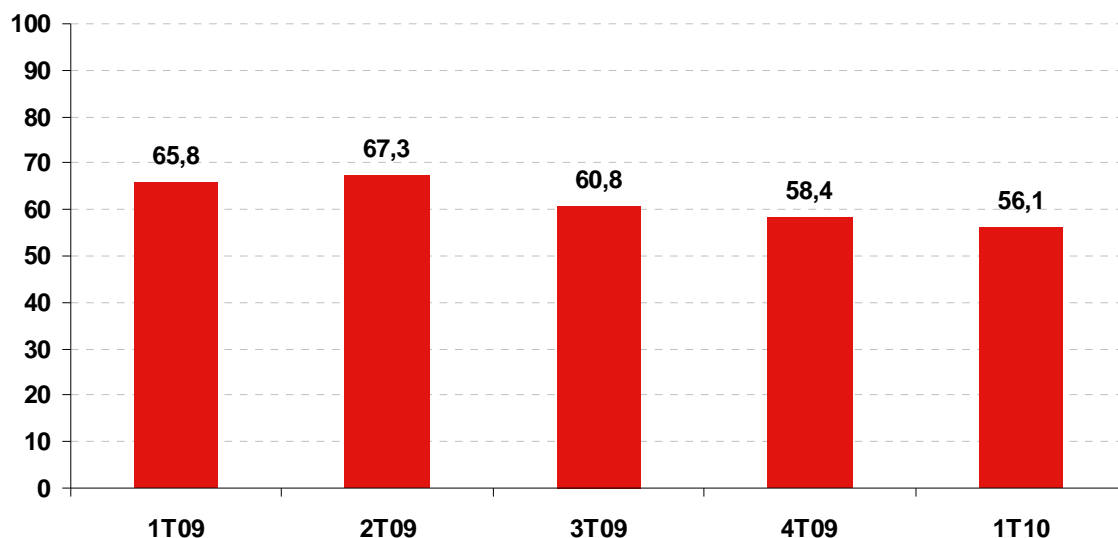


Fuente: INTECO

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. De nuevo, al haberse alcanzado un mínimo histórico de infección, este valor desciende por cuatro trimestre consecutivo, llegando al 56,1 en el primer trimestre de 2010, casi diez puntos menos que el mismo período del año anterior.

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



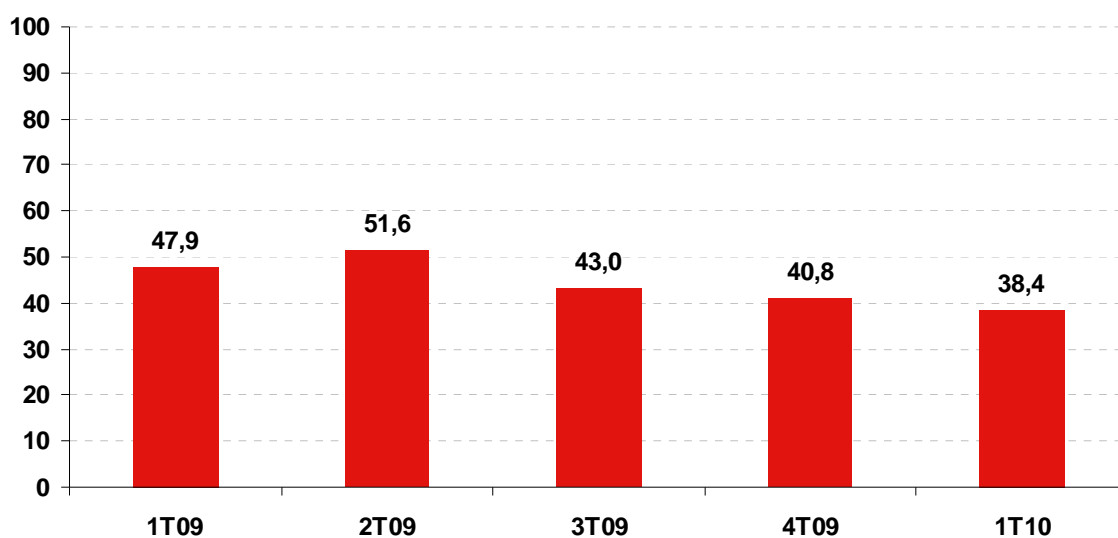
Fuente: INTECO

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 4 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 trimestre se alcanza otro mínimo en este indicador, con un valor de 38,4. Se aprecia un descenso de este tipo de ordenadores con riesgo alto de infección, en casi 10 puntos con respecto al primer trimestre de 2009.

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



Fuente: INTECO

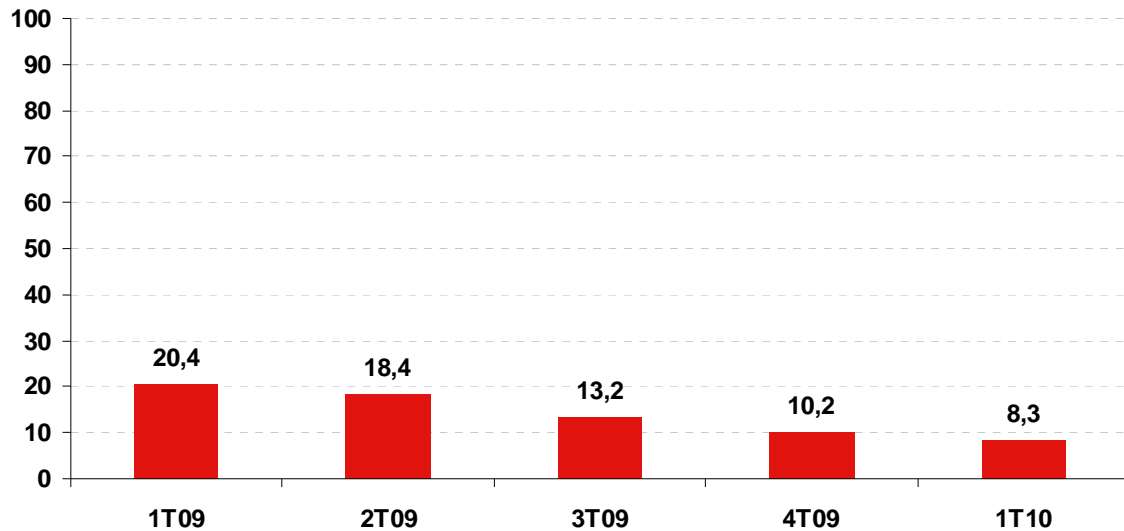
7.2.6 Indicador de ordenadores con diseminación potencial alta

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 descenso¹³ de este indicador continúa en los últimos trimestres, mostrando un nuevo mínimo en 8,3 puntos, lo que indica que cada vez existen menos sistemas con riesgo de suponer un foco de infección importante para el resto de sistemas informáticos.

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



Fuente: INTECO

¹³ Nótese que un valor más bajo en este indicador es un dato positivo ya que representa los equipos de los que se puede derivar un alto grado de diseminación entre el resto de los usuarios y el propio sistema.

8 CONCLUSIONES

A medida que se publican más ediciones del *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles* –este presente constituye la duodécima entrega trimestral– se puede obtener una perspectiva más aproximada sobre el punto en el que se sitúa la seguridad para los españoles: sus equipos, sus comportamientos y la existencia o no de alguna relación entre ambos.

Desde hace tiempo se advierte a los usuarios que la seguridad debería estar basada en, al menos, tres puntos fundamentales:

- **La utilización de una cuenta de usuario sin privilegios, evitando el uso del administrador en Windows.** Esto es lo que puede llevar a una mayor protección contra el malware y contra actuaciones imprudentes del propio usuario.
- **Actualización del sistema.** No sólo Windows, sino todos los programas instalados en el equipo deben estar actualizados a la última versión de su rama. La actualización constante es de importancia vital, pues una gran parte del malware actual aprovecha vulnerabilidades conocidas que ya tienen parche.
- **Información.** Mantenerse informado sobre tendencias de seguridad, malware y estado en general de la seguridad en la red es fundamental. Sólo a través de una información adecuada puede el usuario tener conciencia sobre los peligros y por tanto evitarlos o, en su caso, combatirlos.

Además de estos pilares, es importante la instalación y configuración adecuada de las herramientas de seguridad oportunas (incluyendo antivirus).

Con respecto al primer punto, aunque todavía existe un amplio margen de mejora, se progresa lentamente y ya se alcanza un 38,5% de usuarios que declara llevar a cabo esta práctica.

Las actualizaciones del sistema operativo siempre ha sido una medida adoptada por una inmensa mayoría, hasta un 80,7% declarado en el último trimestre.

Con respecto a la búsqueda de información sobre seguridad de la información, con un 48,7% de usuarios que dicen hacerlo, se mantienen estas cifras desde hace varios trimestres en un nivel constante. Existen a lo largo del estudio otros datos positivos que constituyen un indicio de la creciente proactividad del usuario en el autoaprendizaje, como es la enorme escalada de usuarios que son capaces de resolver las incidencias por sí mismos: un amplio 46,3% (que supone un incremento de más de 12 puntos respecto al año anterior).

Aunque se mencionan de manera relevante estas medidas primarias, lo cierto es que la seguridad se consigue a través de la conjunción de muchos métodos, y en esto los usuarios españoles demuestran unos muy buenos hábitos. Por ejemplo, los ciudadanos siguen instalando un antivirus, la herramienta reina de la seguridad en Windows, con más de un 85% de usuarios que utilizan antivirus realmente (declarados, más de un 90%). También muestran una adecuada predisposición a la adopción de otras medidas, como por ejemplo el DNI electrónico, donde casi un 20% declara usarlo actualmente, y más de un 30% piensa hacerlo en los próximos tres meses. Como último ejemplo, se puede hablar del alto grado de concienciación: los usuarios parecen tener claro que no deben facilitar datos confidenciales a terceros, y un importante 87,8% afirma que no realiza este imprudente hábito. Este valor ha ascendido sustancialmente desde un 75,6% declarado en el segundo trimestre de 2009.

No se pueden ofrecer datos concluyentes al respecto, pero quizás una mejora en los hábitos, unida a una mayor concienciación además de otros factores (como la imparable adopción de Windows Vista, que ya alcanza casi al 28% de los usuarios) han contribuido a la consecución, este trimestre, de un nuevo mínimo en el ratio de infección de equipos. Aunque los usuarios mantienen una percepción de infección del 29,5%, la realidad es que el 52,8% de los equipos alojan algún malware. Si bien es una cifra elevada, lleva en descenso desde hace más de un año. El tipo troyano sigue siendo el protagonista de las infecciones.

Por tanto, se percibe una tendencia clara desde que comenzó el estudio en 2006, en la que los usuarios españoles mejoran su seguridad cada trimestre de forma paulatina y metódica. En este sentido el indicador de herramientas y medidas de seguridad así lo demuestra. La conclusión, analizando las incidencias y nivel de infección, es que una pequeña mejora en los hábitos, puede llevar a grandes avances en la seguridad que eviten fraudes e incidentes (y los ciudadanos son conscientes de ello, pues un 82,4% achaca a la falta de cautela de los propios usuarios, el que las amenazas se propaguen, un dato casi 12 puntos por encima del trimestre anterior).

Pero siempre existe margen de mejora, y no son sólo los usuarios los que deben embarcarse en esta tarea. Dadas las amenazas actuales, cualquier esfuerzo es necesario, y toda ayuda bienvenida. Se incluyen a continuación una serie de reflexiones sobre algunos puntos con el objetivo de que permitan mejorar a corto plazo la seguridad de los internautas españoles:

- Como punto de información de referencia para usuarios, se refiere al lector a la Oficina de Seguridad del Internauta (www.osi.es), iniciativa puesta en marcha por el Gobierno con el objetivo de proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden surgir en la navegación.

- Windows 7, con enormes mejoras en la seguridad (en concreto el manejo del usuario sin privilegios, medida fundamental para evitar el malware) ha entrado en el mercado con un alto grado de aceptación por parte de los usuarios, muy por encima de Windows Vista y mejorando además las ya de por sí excelentes mejoras con las que venía equipado ese sistema operativo. A medida que los usuarios migren hacia él, el malware deberá adaptarse. Muy relacionado con esto, Microsoft abandona Windows 2000 y Windows XP Service Pack 2 en julio de 2010. Si bien puede ser un acicate para el cambio, muchos usuarios o empresas que no puedan actualizar su sistema operativo se quedarán sin parches oficiales de seguridad, con lo que puede resultar un arma de doble filo desde el punto de vista de los niveles de infección.
- Compañías como Adobe (responsable del lector de PDF más popular y del omnipresente reproductor Flash) está empezando a mejorar su política de seguridad sustancialmente, algo que repercutirá sin duda en los niveles de infección de los internautas. En los últimos tiempos, a medida que Microsoft blinda su software, los programas de Adobe (y sus fallos de seguridad) se están convirtiendo en la vía de entrada preferida de muchas familias de malware.

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.

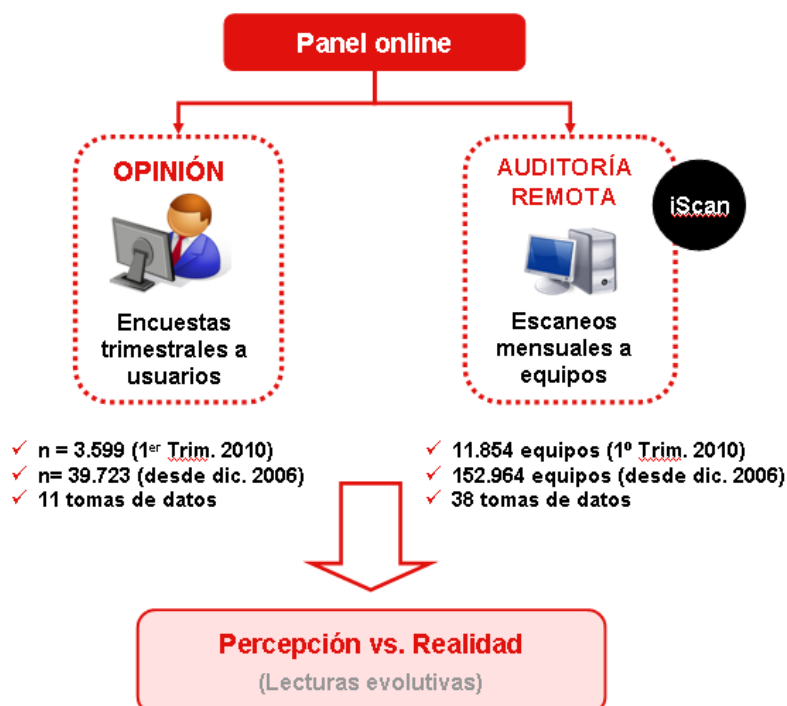
En la definición de la metodología del estudio, se ha considerado una fórmula que permita obtener información, con una perspectiva evolutiva, relativa al nivel de seguridad y e-confianza de los hogares españoles. La necesidad de unos datos robustos sobre los mismos hogares y usuarios en diferentes momentos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

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

En la actualidad el panel está compuesto por 5.212 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 (1º trimestre de 2010), 3.599 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 $n=3.599$ es de $\pm 1,66\%$.
- 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 primer trimestre de 2010 se compone de 5.212 hogares que escanearon online su ordenador entre enero y marzo de 2010. El número total de análisis remotos de seguridad o escaneos realizados en el período ha sido 11.854.

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 3.599 usuarios de Internet, con participación estable en el panel en el trimestre comprendido entre enero y marzo 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
1º trimestre 2007	Febrero a abril de 2007	3.076
2º trimestre 2007	Mayo a julio de 2007	3.023
3º trimestre 2007	Agosto a diciembre de 2007	3.021
4º trimestre 2007	Agosto a diciembre de 2007	3.021
1º trimestre 2008	Enero a marzo de 2008	3.523
2º trimestre 2008	Abril a junio de 2008	2.860
3º trimestre 2008	<i>No disponible</i>	<i>n.d.</i>
4º trimestre 2008	<i>No disponible</i>	<i>n.d.</i>
1º trimestre 2009	Diciembre de 2008 a febrero de 2009	3.563
2º trimestre 2009	Marzo a mayo de 2009	3.521
3º trimestre 2009	Junio a septiembre de 2009	3.540
4º trimestre 2009	Octubre a diciembre de 2009	3.640
1º trimestre 2010	Enero a marzo de 2010	3.599

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		
May'07	3.389	May'08	4.610	May'09	4.677		
Jun'07	3.408	Jun'08	3.889	Jun'09	4.293		
Jul'07	3.701	Jul'08	3.187	Jul'09	3.971		
Ago'07	3.552	Ago'08	2.793	Ago'09	3.677		
Sep'07	3.003	Sep'08	2.617	Sep'09	4.520		
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 hábitat¹⁴.

¹⁴ 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 oleada enero-marzo 2008")

Tabla 10: Distribución muestral por CCAA (%)

CCAA	Muestra obtenida 12ª oleada (enero-marzo'10)	Muestra Teórica
Andalucía	15,8	15,2
Aragón	3,2	3,0
Asturias (Principado de)	2,8	2,5
Balears (Illes)	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
Comunitat Valenciana	10,7	10,0
Extremadura	1,9	1,4
Galicia	6,1	4,5
La Rioja	0,8	0,7
Madrid (Comunidad de)	15,8	18,6
Murcia (Región de)	2,7	2,5
Navarra (Comunidad Foral de)	1,5	1,4
País Vasco	5,9	4,7

Base muestra enero 2010 – marzo 2010 = 3.599

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 12ª oleada (ene-mar'10)	Muestra Teórica
Actividad		
Ocupados	53,6	71,7
Parado	18,3	4,6
Estudiantes	15,6	16,1
Jubilado	7,3	3,0
Otros Inactivos	5,0	4,6
Nivel de estudios		
Hasta primarios	13,2	<i>n.d.</i>
Secundarios	38,3	<i>n.d.</i>
FP de grado superior/Universitario Medio	34,9	<i>n.d.</i>
Universitarios superiores	13,6	<i>n.d.</i>
Tamaño hogar		
1	7,9	3,2
2	28,1	15,4
3	28,8	28,7
4 y mas	35,2	52,7
Tipo de hogar		
Sin pareja y con hijos	4,7	<i>n.d.</i>
En pareja y sin hijos	21,6	<i>n.d.</i>
En pareja y con hijos	35,3	<i>n.d.</i>
Con mis padres u otros familiares	33,7	<i>n.d.</i>
Comparto vivienda con personas que no son de mi familia	3,2	<i>n.d.</i>
Otro tipo de hogar	1,5	<i>n.d.</i>
Sexo		
Hombre	52,5	53,7
Mujer	47,5	46,3
Edad		
De 15 a 24 años	21,8	<i>n.d.</i>
De 25 a 34 años	28,2	<i>n.d.</i>
De 35 a 44 años	24,2	<i>n.d.</i>
De 45 a 54 años	15,9	<i>n.d.</i>
Más de 55 años	9,8	<i>n.d.</i>

Base muestra enero 2010 – marzo 2010 = 3.599

Fuente: INTECO

Los datos finales de encuesta de este primer trimestre de 2010 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 goodware¹⁵ 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 freeware¹⁶ y shareware¹⁷ 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.

¹⁵ Software y ficheros legítimos, archivos inocuos.

¹⁶ Software gratuito.

¹⁷ 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 enero y marzo 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 enero a marzo de 2010: $n=3.599$; error muestral $\pm 1,66\%$.

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	<i>n.d.</i>	<i>n.d.</i>
Diciembre de 2008 a febrero de 2009	3.563	±1,68%
Marzo a mayo de 2009	3.521	±1,68%
Junio a septiembre de 2009	3.540	±1,68%
Octubre a diciembre de 2009	3.640	±1,66%
Enero a marzo de 2010	3.599	±1,66%

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 duodécima oleada, que compara el período enero-marzo 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 hogares españoles.

ÍNDICE DE GRÁFICOS

Gráfico 1: Evolución de la utilización declarada de medidas de seguridad automatizables (%)	19
Gráfico 2: Evolución de la utilización declarada de medidas de seguridad no automatizables (%)	20
Gráfico 3: Intención declarada de uso de medidas de seguridad automatizables en los próximos 3 meses (datos del 1T 2010) (%)	21
Gráfico 4: Intención declarada de uso de medidas de seguridad no automatizables en los próximos 3 meses (datos del 1T 2010) (%)	22
Gráfico 5: Evolución de la frecuencia declarada de comprobación de la actualización de herramientas de seguridad (%)	25
Gráfico 6: Evolución de la frecuencia declarada de escaneo del ordenador con el programa antivirus (%)	26
Gráfico 7: Evolución de los hábitos prudentes relacionados con la navegación por Internet (%)	28
Gráfico 8: Evolución de los hábitos prudentes relacionados con el correo electrónico (%)	29
Gráfico 9: Evolución de los hábitos prudentes relacionados con chats y mensajería instantánea (%)	31
Gráfico 10: Evolución de los hábitos prudentes relacionados con banca en línea y comercio electrónico (%)	33
Gráfico 11: Evolución de los hábitos prudentes relacionados con las redes P2P (%)	34
Gráfico 12: Evolución de la utilización declarada de redes sociales (%)	35
Gráfico 13: Evolución de los usos declarados de las redes sociales (posibilidad de respuesta múltiple) (%)	36
Gráfico 14: Evolución del nivel de privacidad del perfil del usuario de redes sociales (%)	37
Gráfico 15: Evolución de los hábitos relacionados la supervisión de los menores en el uso de Internet manifestados (medidas coercitivas y de control) (%)	39

Gráfico 16: Evolución de los hábitos relacionados la supervisión de los menores en el uso de Internet manifestados (medidas de comunicación, diálogo y educación) (%).....	40
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) (%)	41
Gráfico 18: Evolución de equipos que alojan malware (%)	46
Gráfico 19: Equipos que alojan malware según tipología de código malicioso en mar. 10 (%)	47
Gráfico 20: Evolución de equipos que alojan malware según tipología (%).....	48
Gráfico 21: Evolución del número medio de archivos maliciosos por equipo.....	49
Gráfico 22: Evolución del número total de archivos maliciosos y variantes únicas de malware	50
Gráfico 23: Categorías de código malicioso de las variantes únicas, marzo 2010 (%).....	51
Gráfico 24: Número de detecciones de cada variante única de malware, marzo 2010	51
Gráfico 25: Evolución del nivel de riesgo de los equipos (%).....	54
Gráfico 26: Evolución de las consecuencias de las incidencias de seguridad: pérdida de datos (%)	55
Gráfico 27: Evolución de las consecuencias de las incidencias de seguridad: formateo y reinstalación del SO (%)	56
Gráfico 28: Evolución de las consecuencias de las incidencias de seguridad: daños en el hardware (%)	57
Gráfico 29: Evolución de las reacciones adoptadas tras sufrir un incidente de seguridad: cambio en las medidas y herramientas de seguridad (%).....	58
Gráfico 30: Evolución de las reacciones adoptadas tras sufrir un incidente de seguridad: cambio en el uso de los servicios de Internet (%)	59
Gráfico 31: Evolución de la forma de resolución de las incidencias de seguridad (%)	60
Gráfico 32: En general, ¿cuánta confianza le genera Internet? (1T 2010) (%).....	61
Gráfico 33: Evolución del porcentaje de usuarios que se muestran totalmente de acuerdo y de acuerdo con... (%).....	62

Gráfico 34: Confianza en la realización de actividades físicas / online relacionadas con operaciones bancarias 1T 2010 (%).....	63
Gráfico 35: Confianza en la realización de actividades físicas / online relacionadas con pagos y transacciones de compraventa 1T 2010 (%)	64
Gráfico 36: Confianza en la realización de actividades físicas / online relacionadas con los datos personales 1T 2010 (%).....	65
Gráfico 37: Evolución de la seguridad como factor que limita la utilización de nuevos servicios (%)	66
Gráfico 38: Evolución de la percepción del número de las incidencias de seguridad con respecto a hace 3 meses (%)	67
Gráfico 39: Evolución de la percepción de la gravedad de las incidencias de seguridad con respecto a hace 3 meses (%)	68
Gráfico 40: Evolución del porcentaje de usuarios que se muestran <i>totalmente de acuerdo</i> y <i>de acuerdo</i> con... (%).....	69
Gráfico 41: Evolución del porcentaje de usuarios que se muestran <i>totalmente de acuerdo</i> y <i>de acuerdo</i> con... (%).....	70
Gráfico 42: Evolución del nivel de acuerdo con la opinión La Administración tiene que implicarse más en mejorar la seguridad en Internet (%)	71
Gráfico 43: Evolución de las medidas de vigilancia demandadas a la Administración (%)	73
Gráfico 44: Evolución de las medidas de respuesta técnica demandadas a la Administración (%).....	74
Gráfico 45: Evolución de las medidas de sensibilización demandadas a la Administración (%)	75
Gráfico 46: Evolución de las medidas de respuesta institucional y legislativa demandadas a la Administración (%).....	76
Gráfico 47: Evolución del sistema de indicadores de la seguridad de la información (0-100 puntos).....	80
Gráfico 48: Evolución del indicador de herramientas y medidas de seguridad (0-100 puntos).....	82

Gráfico 49: Evolución del indicador de conductas y hábitos de seguridad (0-100 puntos)	84
Gráfico 50: Evolución del indicador de e-confianza (0-100 puntos)	86
Gráfico 51: Evolución del indicador de incidencias de malware (0-100 puntos)	86
Gráfico 52: Evolución del indicador de equipos con riesgo alto (0-100 puntos).....	87
Gráfico 53: Evolución del indicador de equipos con diseminación potencial alta (0-100 puntos).....	88

ÍNDICE DE TABLAS

Tabla 1: Utilización declarada y real de medidas de seguridad automatizables y no automatizables 1T2010 (%).....	18
Tabla 2: Motivos para no aplicar medidas de seguridad automatizables 1T2010 (%)	23
Tabla 3: Motivos para no aplicar medidas de seguridad no automatizables en 1T2010 (%)	24
Tabla 4: Incidencias de seguridad declaradas por los usuarios en función del momento de detección 1T2010 (%).....	42
Tabla 5: Medidas demandadas a la Administración 1T 2010 (%)	72
Tabla 6: Consideración de quiénes son los responsables de la seguridad en Internet 1T10 (%)	77
Tabla 7: Sistema de indicadores de seguridad y e-confianza	78
Tabla 8: Tamaños muestrales para las encuestas	94
Tabla 9: Número de equipos escaneados mensualmente	95
Tabla 10: Distribución muestral por CCAA (%)	96
Tabla 11: Distribución muestral por categorías sociodemográficas (%).....	97
Tabla 12: Errores muestrales de las encuestas (%).....	101

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Indicador de herramientas y medidas de seguridad	81
Ilustración 2: Indicador de conductas y hábitos de seguridad	83
Ilustración 3: Indicador de e-confianza	85
Ilustración 4: Esquema de la metodología del estudio	93



Instituto Nacional
de Tecnologías
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>