

La seguridad en Internet no es una cuestión de máquinas y tecnología, sino de personas.

- *Las herramientas de seguridad son útiles y necesarias, pero no suficientes; además son imprescindibles unos hábitos de uso basados en la precaución y protección.*
- *El 72 por ciento de los usuarios tiene algún código malicioso en su ordenador, que en el 52 por ciento de los casos es de alto riesgo. Los troyanos son el malware con más variantes y más difusión.*
- *Internet se ha convertido en un medio imprescindible y las incidencias en la seguridad no limitan su uso. No obstante, el 58,3% de los usuarios utilizaría más servicios online si le enseñaran a protegerse.*

Madrid, 19 de junio de 2007.- Las incidencias relacionadas con la seguridad y la confianza de los usuarios en la Red son un factor crítico que condiciona el desarrollo de la Sociedad de la Información en España, retrasando la adopción y extensión de servicios a través de Internet, como el comercio electrónico, la administración electrónica o la banca online.

De la mano de Enrique Martínez, director general de INTECO, y Pablo Pérez, gerente del Observatorio y coordinador del equipo de trabajo, se presenta la Primera Oleada del **Estudio sobre la Seguridad de la Información y e-Confianza de los Hogares Españoles**, realizado por el Observatorio de la Seguridad de la Información de INTECO – **Instituto Nacional de Tecnologías de la Comunicación**. Para la elaboración del Estudio se han realizado, entre diciembre de 2006 y enero de 2007, más de 6.000 encuestas a hogares y se han analizado más de 3.000 ordenadores de los hogares panelizados.

El estudio muestra, por primera vez, los hábitos que afectan a la seguridad en Internet: equipamiento de seguridad en los hogares, las medidas que los usuarios toman antes y después de las incidencias y la percepción relativa a la seguridad en Internet existente en los hogares españoles. Refleja también la creciente exigencia por parte de los usuarios a las administraciones públicas de que “hagan de Internet un lugar seguro”.

Perfil de los hogares: equipamiento y uso de Internet

El 90 % de los hogares participantes en el estudio acceden a Internet a través de Banda Ancha. El hogar es el principal núcleo de acceso para el 78% de los encuestados, siendo que cuando se conectan desde el hogar, el 76% se conectan principalmente desde un PC de

sobremesa, el 22% desde un portátil y el 2% desde otros dispositivos (móvil, PDA, videoconsola). Del total, **un 60% se conecta más de 5 horas a la semana desde el hogar**. Se constata también una amplia experiencia en Internet, ya que el **90% afirma utilizarla desde hace al menos 2 años y el 65,4% desde hace más de cinco años**.

La práctica totalidad de los encuestados utiliza el correo electrónico, **el 75% utiliza programas de descarga de archivos y el 46% deja desatendido el ordenador al menos una vez al día**. Destacan usos como el chat (66,6%), la banca online (63,3%), los pagos por Internet (26,9%) o la videoconferencia (19,8%).

Medidas de seguridad en los hogares españoles

En relación con la seguridad de la información, **los usuarios de Internet utilizan principalmente medidas de seguridad que no exigen ninguna participación activa (automatizadas)**, existiendo un **déficit en la incorporación de medidas que reclaman mayor proactividad por parte del usuario**.

Entre estas herramientas, los **programas antivirus son la más generalizada** y está instalado y activo en el 87% de los hogares (si bien, paradójicamente, el 95% el declara tenerlo instalado). La segunda medida con mayor penetración son los cortafuegos, del que disponen un 76% de los encuestados. Por otro lado, las medidas que implican un comportamiento más activo del usuario, como las copias de seguridad, apenas son utilizadas por el 35% de los usuarios.

Entre las **razones para no implementar medidas de seguridad**, las más importantes son las derivadas del desconocimiento o de la percepción de que es innecesaria. Las medidas más valoradas son los antivirus, los cortafuegos y los programas anti-espía. Es destacable el hecho de que un gran porcentaje de los usuarios que no utilizan programas antivirus alegan no hacerlo porque este entorpece el uso del ordenador y la navegación por Internet.

En cuanto a las **previsiones** a corto plazo, el mayor incremento se registra en programas de protección ante el correo basura y el software espía, así como en las actualizaciones de seguridad y las copias de seguridad de archivos importantes.

Los usuarios con mejor protección son los que utilizan un mayor número de servicios. Según el estudio, el 64% de los equipos están suficientemente protegidos. Dependiendo del tipo de medidas utilizadas podemos distinguir entre: un **35,6% de los ordenadores que tienen una protección avanzada** (utilizan tanto medidas proactivas como automatizables), **el 36,1% una protección básica** (utilizan medidas automatizables) y **el 28,3% una protección deficiente** (presentan carencias en el uso de ambos tipos de medidas).

Hábitos de de seguridad en los hogares españoles

Los usuarios declaran que tienen un comportamiento “bastante prudente” en su utilización de Internet.

Se puede categorizar a los internautas según su comportamiento y hábitos de seguridad como:

- **Prudentes y no solidarios (58%):** Tienen un enfoque individualista de la seguridad centrado en la defensa del equipo particular y no comparten experiencias para la defensa solidaria.
- **Prudentes y solidarios (33%):** Añaden a la protección individual la preocupación por compartir y la mutua ayuda en temas de seguridad.
- **Temerario (8%):** No atiende a las normas y hábitos básicos de la prudencia. No modifica sus hábitos a pesar de sufrir incidencias de gravedad.

El comportamiento **temerario implica a menos del 10%** de los usuarios, pero en ellos se concentra **gran parte del riesgo total** del sistema:

- Una mayor presencia de malware en sus equipos (mayor número de incidencias)
- Mayor porcentaje de malware de riesgo alto
- Como consecuencia de sus hábitos imprudentes, concentran los casos detectados de ordenadores con mayor capacidad de dispersión de las amenazas.

Su comportamiento se caracteriza por abrir correos de remitentes desconocidos, desactivar las medidas de seguridad de los equipos, compartir archivos y software no verificado (a través de redes P2P), agregar contactos a gestores de mensajería instantánea o pulsar los enlaces de sus conversaciones sin saber quién o qué está tras ellos.

Incidencias de seguridad

El **72% de los ordenadores domésticos** para acceso a Internet **presentan** algún tipo de **código malicioso o malware**, detectándose **malware con riesgo alto** en **más del 50%** de los equipos analizados.

Así, más algo más del 50% de los ordenadores de los usuarios domésticos analizados tienen troyanos y más del 40% adware publicitario, un 25% herramientas de intrusión, un 10% programas espía y un 10% virus.

De entre el malware encontrado aquel que genera un **mayor número de variantes** distintas son los **troyanos (48,7%)** y el **adware publicitario (34,6%)**

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

Es destacable el hecho de que aun a pesar de utilizar más de 30 motores de búsqueda de código malicioso, un 8,9% del mismo es detectado en los equipos de manera heurística, esto es, este posible malware aún no estaba recogido en sus catálogos.

En cuanto al efecto de las incidencias en los usuarios, las consecuencias más habituales son la actualización, renovación e instalación de nuevas barreras de protección (el 10% instaló su primer antivirus, el 20% cambia de antivirus), el cambio de opinión y comportamiento respecto a la seguridad, siendo más prudentes, y reclamando mayor implicación de la administración. Un dato importante en este punto, es que **las incidencias apenas modifican el uso de los servicios, debido al carácter de imprescindible que Internet está adquiriendo.**

Percepción de seguridad y e-Confianza de los usuarios en el uso de Internet

Aunque casi la mitad de los hogares indican que utilizarían más servicios si supieran reducir su riesgo, el análisis señala que, en general, **las incidencias de seguridad no provocan que los usuarios abandonen servicios o dejen de utilizar Internet.**

Si bien es cierto que existe un **efecto de retraso en la incorporación** a la Sociedad de la Información relacionado con la falta de confianza en Internet, dicho efecto debe buscarse **entre los “no usuarios”**, es decir, aquellos que no se sienten suficientemente protegidos como para incorporarse y moverse plenamente en la Red.

Así las cosas, los usuarios habituales de Internet han englobado de tal forma los servicios online en su estilo de vida que se les hace muy difícil prescindir de los mismos. En este contexto, **las incidencias sufridas se interpretan como avisos para aumentar su equipamiento de protección y/o para mostrarse más prudentes en sus hábitos, pero no se interpretan como avisos de que deben abandonar o reducir el uso de Internet.** Simplemente, para muchos usuarios, la segunda alternativa no parece posible.

A pesar de las incidencias declaradas, y del conocimiento del riesgo bastante realista que manifiestan los usuarios, la sensación general es de confortable seguridad en el uso de

Internet. La gran mayoría considera que su conexión y su equipo les garantizan una navegación segura.

Los análisis realizados ponen de manifiesto que **la e-confianza de los internautas se sitúa en torno a los 76,4 puntos de media en una escala del 0 a 100**. Esta e-confianza es elevada en todos los grupos de usuarios, sin distinción de sus hábitos de riesgo o del nivel de equipamiento en seguridad. Esta percepción de seguridad solo se ve afectada después de sufrir numerosas incidencias y se recompone ampliando las medidas de protección y moderando las conductas de riesgo. Cuando no se consigue recomponer la percepción de seguridad, aumenta la demanda de una mayor intervención de la Administración.

La seguridad en Internet no es una cuestión de máquinas y tecnología, sino de personas.

Es destacable el hecho de que a pesar de que tanto las medidas de seguridad como el comportamiento de los usuarios reducen el número de incidencias detectadas en los ordenadores, **son estas últimas acciones las que hacen disminuir de manera más significativa el código malicioso encontrado en los ordenadores.**

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

Así pues, se constata que **la instalación de herramientas de seguridad, siendo necesaria, no es suficiente**; además es preciso tomar otras acciones complementarias: buenas prácticas y hábitos de seguridad adecuados. **La seguridad en Internet no es pues una cuestión de máquinas y tecnología, sino de personas.**

Con el Estudio se han identificado **tres debilidades**:

- La conducta temeraria, posiblemente la principal vulnerabilidad empírica del sistema, se reduce firmemente con la edad. **Es propia de jóvenes, principalmente varones que viven en el hogar paterno y no comparten su equipo con otras personas.** También, se ha detectado que el uso compartido del terminal es un factor positivo de reducción de las incidencias.
- Una segunda vulnerabilidad del sistema, de menor intensidad, proviene de los **usuarios de Internet con menor experiencia y déficit de equipamiento en seguridad**, que no consiguen reducir su riesgo real a pesar de mostrar unos hábitos prudentes de navegación.

- La tercera vulnerabilidad del sistema, que afecta a la mayoría de los usuarios, consiste en que estos tienden a hacer **residir la e-confianza en el equipamiento y en las soluciones individuales, despreocupándose de los hábitos de seguridad**, que se han demostrado fundamentales para mantener la seguridad de los equipos.

Por todo ello, **es necesario que los usuarios sean conscientes de la utilidad de las herramientas de seguridad** como los antivirus, cortafuegos, antispam (correo no deseado), actualizaciones de seguridad, etc. **Pero también deben conocer sus limitaciones de dichas soluciones informáticas, las amenazas reales, y las recomendaciones adicionales**, para que no se cree una falsa sensación de seguridad. Es imprescindible, para aumentar la seguridad, el proporcionar a los usuarios de una **mayor formación de cara a realizar un uso responsable y seguro de las nuevas tecnologías, con hábitos de uso basados en la precaución y la protección.**

Por tanto se hace necesario un esfuerzo en dos frentes: por un lado, potenciar el uso de dispositivos de seguridad y, por otro lado, remarcar la necesidad de un uso responsable de los equipos, para que esos dispositivos sean realmente eficaces.

Aquí es donde se muestra clave la acción de la **Administración**: creando una **cultura de seguridad** que canalice la información relativa tanto a los sistemas de protección como a las prácticas seguras.

El papel de la Administración: Tutelaje vs. Autorregulación

Los resultados del estudio señalan que el **72% de los usuarios** opina que la **Administración Pública** debe encargarse de **hacer de Internet un lugar seguro, y el 58%** afirma que emplearía **más servicios si le enseñaran a proteger su ordenador.**

Paralelamente, el 85% opina que Internet sería más seguro si empleásemos correctamente las utilidades de los programas que disponemos, y el 67% de los encuestados considera que la propagación de amenazas a través de Internet es resultado de la poca cautela que sus usuarios manifiestan.

Los usuarios piden a la Administración que:

- **Controle y vigile** más de cerca lo que está pasando en Internet
- Que **informe y alerte** a los usuarios extendiendo una cultura de seguridad.
- Que sea más rápidos en la **persecución de los delitos o prácticas abusivas.**

El papel que los usuarios asignan a la Administración en materia de seguridad parece consistir en ser una última instancia. El resultado debe garantizar la seguridad cuando las

medidas al alcance del usuario y los hábitos prudentes de navegación se revelan insuficientes. En general, esta intervención es aceptada y reclamada por más del 70% de los usuarios.

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

Sobre INTECO

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**, sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio con sede en León, cuya misión es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información. Para ello, INTECO desarrolla actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Innovación en soluciones TIC para la Pyme, e-Salud y e-Democracia.

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

Sobre el Estudio

El Observatorio de INTECO presenta la primera oleada (diciembre-enero 2007) del “Estudio sobre Seguridad de la Información y eConfianza de los hogares españoles”. Este informe es el primero de cuatro diagnósticos anuales cuya finalidad es el diagnóstico, evaluación y seguimiento de la seguridad, confianza y nivel de incidencias de seguridad de los hogares usuarios de Internet en España.

Las incidencias relacionadas con la seguridad y la confianza de los usuarios en la Red son un factor crítico que condiciona el desarrollo de la Sociedad de la Información en España, retrasando la adopción y extensión de servicios a través de Internet, como el comercio electrónico, la administración electrónica o la banca online.

Por ello, uno de los principales objetivos del informe es analizar la relación entre los problemas de seguridad y la ralentización del desarrollo de la sociedad de la información. Un conocimiento que permitirá promover iniciativas públicas que mejoren la seguridad individual y generen un clima de confianza en la sociedad de la información.

En concreto, el Estudio se centra en los aspectos de seguridad informática, incidencias reales, percepción de la seguridad y gravedad de los episodios de riesgo. Se realiza una investigación exhaustiva sobre todo lo concerniente a estos temas: desde equipamiento tecnológico general del hogar y hábitos de uso de Internet al sistema de indicadores estadísticos únicos sobre el nivel de seguridad informática en los hogares españoles. Los resultados del Estudio reflejan los hábitos de seguridad, incluyendo en este apartado las medidas informáticas de seguridad adoptadas por los usuarios, motivos para su no utilización, así como previsiones futuras de implantación en los hogares españoles.

Se incluyen resultados para la percepción de seguridad sobre incidencias, servicios y actitudes de comportamiento que muestran los usuarios españoles de Internet. Dentro de este apartado destacamos lo que los usuarios señalan como el **papel de la Administración** o los niveles de autorregulación y tutelaje que demandan los ciudadanos.

De los datos recogidos del análisis de los escaneos proceden los **resultados del nivel de incidencias reales de seguridad**: abarcando datos de equipos infectados, códigos maliciosos (*malware*) más frecuentes y sus características. También se ofrecen datos cruzados a nivel de actualizaciones y sistemas operativos.

Por último se construye una serie de indicadores estadísticos que sintetizan todos los datos de manera sistemática. Los resultados de cada una de las oleadas trimestrales permiten actualizar dicho **sistema de indicadores**, genuinos en Europa, gracias a los cuales es posible:

- Realizar un seguimiento de las políticas públicas
- Analizar las tendencias del malware y la evolución del sector empresarial de la seguridad.
- Difundir entre la sociedad la cultura de la seguridad, para con ello sensibilizar a la opinión pública sobre estas materias para reducir las incidencias de seguridad y reforzar la e-confianza.

Metodología

El Estudio sobre Seguridad de la Información y e-Confianza en los hogares españoles que presenta el Observatorio de INTECO es un informe análisis que ofrece una información única e inédita sobre incidencias de seguridad y comportamientos de los hogares españoles conectados a Internet, y que gracias a sus **novedosa metodología** basada en

los escaneos mensuales gracias al software residente en los equipos informáticos de los hogares panelizados, permite extraer conclusiones que reflejan fielmente las características técnicas y sociodemográficas de los hogares españoles usuarios de Internet en cuestiones de seguridad de la información y confianza electrónica.

El **universo analizado** incluye a los usuarios españoles mayores de 15 años con acceso frecuente a Internet –al menos una vez al mes- desde el hogar. Una muestra que incluye todas las comunidades autónomas, tamaños de hogar, edad, sexo, actividad laboral y tamaño de hábitat. Además de haber realizado una **encuesta online entre 6.357 usuarios**, una de las novedades del informe es el **escaneo de los ordenadores** de acceso principal a Internet desde el hogar de un total de **3.068 panelistas**.