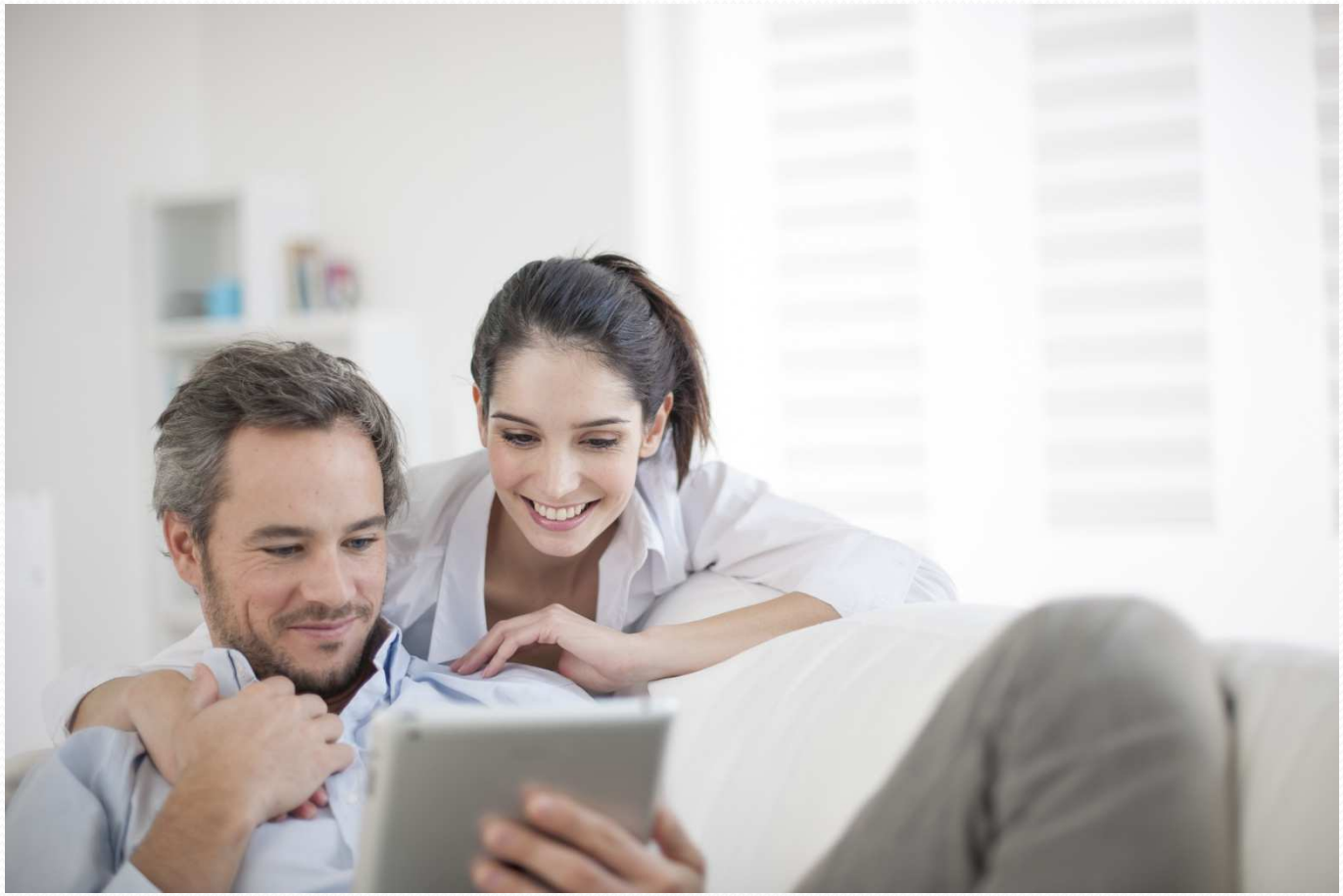
Estudio sobre la Ciberseguridad y Confianza en los hogares españoles



Febrero – Marzo 2014

INDICE

1. **Introducción al estudio**
   Presentación, Objetivos

2. **Medidas de seguridad**
   Definición y clasificación de las medidas de seguridad, Uso de medidas de seguridad en el ordenador del hogar, Motivos alegados para no utilizar medidas de seguridad, Frecuencia de actualización y utilización, Medidas de seguridad utilizadas en redes inalámbricas Wi-Fi, Medidas de seguridad utilizadas en smartphones

3. **Hábitos de comportamiento en la navegación y usos de Internet**
   Banca en línea y comercio electrónico, Descargas en Internet, Redes sociales, Hábitos de uso de las redes inalámbricas Wi-Fi, Hábitos de uso en smartphones

4. **Incidentes de seguridad**
   Tipos de malware, Incidencias de seguridad, Evolución de los incidentes por malware, Tipología del malware detectado, Diversificación del malware detectado, Peligrosidad del malware y riesgo del equipo, Malware vs. sistema operativo y actualización, Malware vs. hábitos de comportamiento, Incidencias de seguridad en las redes inalámbricas Wi-Fi, Incidencias de seguridad en smartphones

5. **Consecuencias de los incidentes de seguridad y reacción de los usuarios**
   Consecuencias de los incidentes de seguridad, Intento de fraude telefónico y manifestaciones, Intento de fraude online y manifestaciones, Seguridad y fraude online y telefónico, Cambios adoptados tras un incidente de seguridad, Resolución de incidentes de seguridad

6. **Confianza en el ámbito digital en los hogares españoles**
   e-Confianza y limitaciones en la Sociedad de la Información, Percepción de los usuarios sobre la evolución en seguridad, Responsabilidad en la seguridad de Internet

7. **Conclusiones**

8. **Alcance del estudio**

Introducción al estudio

1. **Presentación**
2. **Objetivos**

Presentación

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es, han diseñado y promovido el:

Estudio sobre la Ciberseguridad y Confianza en los hogares españoles.

Esta investigación es referente en el diagnóstico sobre el estado de la ciberseguridad en los hogares digitales españoles, analizando la adopción de medidas de seguridad y el nivel de incidencia de situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que los hogares españoles depositan en la Sociedad de la Información.

Los datos presentados en este informe han sido extraídos siguiendo diferentes metodologías:

- Dato declarado: Obtenido de las encuestas online realizadas a los 3.010 hogares que han conformado la muestra del estudio.
- Dato real: Para ello se utiliza el software **iScan** desarrollado por INTECO, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 50 motores antivirus. Los datos así extraídos se representan en el presente informe con siguiente etiqueta: iScan

El software **iScan** se instala en los equipos y los analiza, detectando el malware residente en los mismos y recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas.

Los datos reflejados en **este informe abarcan** el **análisis desde febrero hasta marzo de 2014**. El informe previo a este y disponible en esta dirección:

http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares-españoles, abarca el análisis desde diciembre de 2013 a enero de 2014

Objetivos

El **objetivo general** de este estudio es hacer un **análisis del estado real** de la **ciberseguridad y confianza digital** entre los usuarios españoles de Internet y, al mismo tiempo, contrastar el nivel real de incidentes que sufren los equipos con las percepciones de los usuarios y mostrar la evolución temporal de estos indicadores.

Además se trata de **impulsar** el **conocimiento especializado y útil** en materia de **ciberseguridad y privacidad**, para mejorar la implantación de medidas por parte de los usuarios

Así mismo se pretende reforzar la **adopción de políticas y medidas** por parte de la Administración, orientando iniciativas y políticas públicas tanto en la generación de confianza en la Sociedad de la Información, como en la mejora individual de la seguridad, sustentadas en una percepción realista de los beneficios y riesgos de las mismas.

Medidas de seguridad

1. Definición y clasificación de las medidas de seguridad
2. Uso de medidas de seguridad en el ordenador del hogar
3. Motivos alegados para no utilizar medidas de seguridad
4. Frecuencia de actualización y utilización
5. Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi
6. Medidas de seguridad utilizadas en smartphones

Definición y clasificación de las medidas de seguridad

Medidas de seguridad[2]

Son programas o acciones utilizadas por el usuario para proteger el ordenador y los datos que se encuentren en este. Estás herramientas y acciones pueden ser realizadas con la intervención directa del usuario **(automatizables y no automatizables)** y pueden ser también medidas anteriores o posteriores a que ocurra la incidencia de seguridad **(proactivas, reactivas o ambas).**

Medidas automatizables

Son aquellas medidas de **carácter pasivo** que, por lo general, **no requieren de ninguna acción por parte del usuario**, o cuya configuración permite una puesta en marcha automática.

Medidas no automatizables

Son aquellas medidas de **carácter activo** que, por lo general, **sí requieren una actuación específica por parte del usuario** para su correcto funcionamiento.

Medidas proactivas

Son aquellas medidas utilizadas para **prevenir y evitar**, en la medida de lo posible, la ocurrencia de incidencias de seguridad y minimizar las posibles **amenazas desconocidas y conocidas**.

Medidas reactivas

Son aquellas medidas que son utilizadas para **subsanar** una incidencia de seguridad, es decir, son las medidas que se utilizan para eliminar **amenazas conocidas y /o incidencias ocurridas**.

Herramientas de seguridad y útiles gratuitos para proteger el equipo informático, donde encontrar programas que te ayudarán a protegerte.
http://www.osi.es/herramientas-gratuitas

[2] Existen medidas de seguridad que por su condición se pueden clasificar en ambas categorías, tal es el caso de los programas antivirus y sus actualizaciones, o las del sistema operativo.
Un programa antivirus, por su naturaleza puede detectar tantos las amenazas existentes en el equipo como las amenazas que intenten introducirse en él.

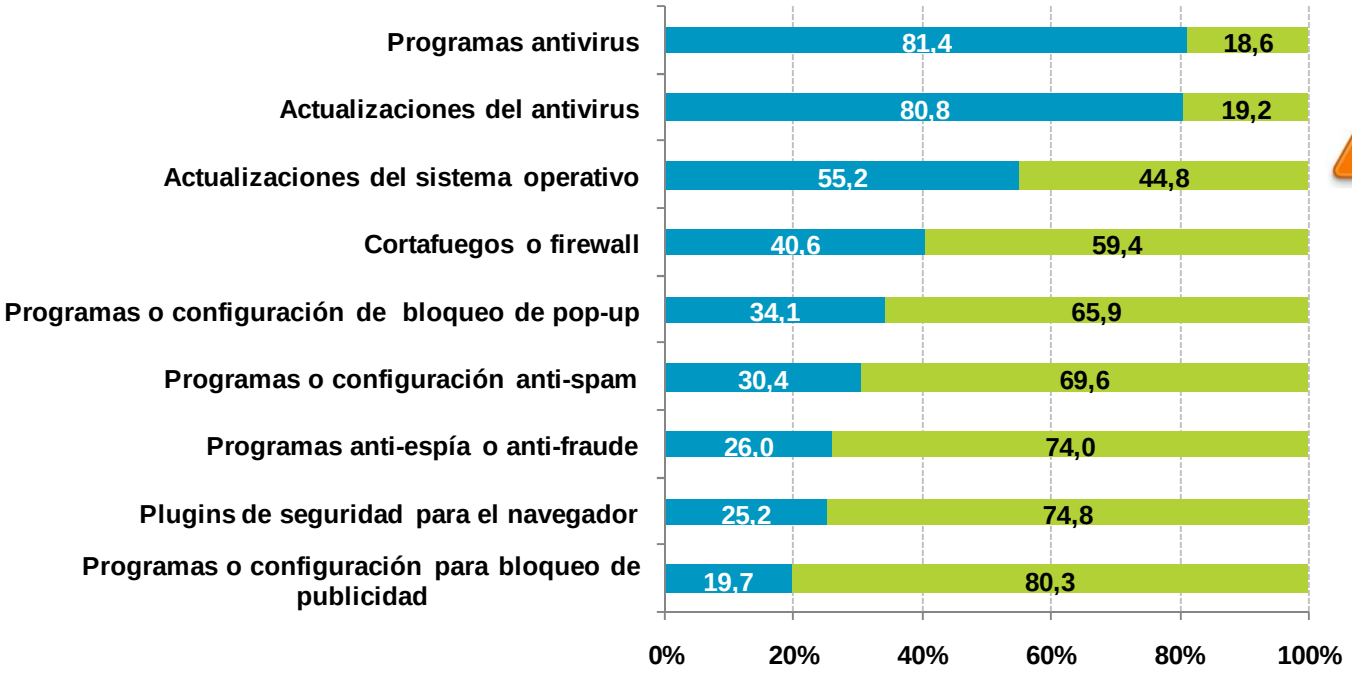
Definición y clasificación de las medidas de seguridad

	Medidas automatizables	Medidas no automatizables
Proactivas	• Cortafuegos o firewall	• Contraseñas • Copias de seguridad de archivos • Partición del disco duro • Certificados digitales de firma electrónica • Utilización habitual de permisos reducidos • DNI electrónico • Cifrado de documentos o datos
Proactivas y reactivas	• Programa antivirus • Actualizaciones del sistema operativo y programas • Actualizaciones del antivirus	
Reactivas	• Plugins para el navegador • Programas de bloqueo de ventanas emergentes • Programas de bloqueo de banners • Programas anti-spam • Programas anti-fraude	• Eliminación de archivos temporales o cookies

Uso de medidas de seguridad en el ordenador del hogar

Medidas de seguridad automatizables[1]

Destaca la utilización mayoritaria del **software antivirus**, declarado por un 81,4% de la población, y de sus **actualizaciones** (**80,8%**) como principales medidas de seguridad.



A menudo el usuario piensa que la única y mejor solución es el antivirus, olvidando que existen **otras medidas de seguridad de igual o mayor importancia**.

BASE: Total usuarios

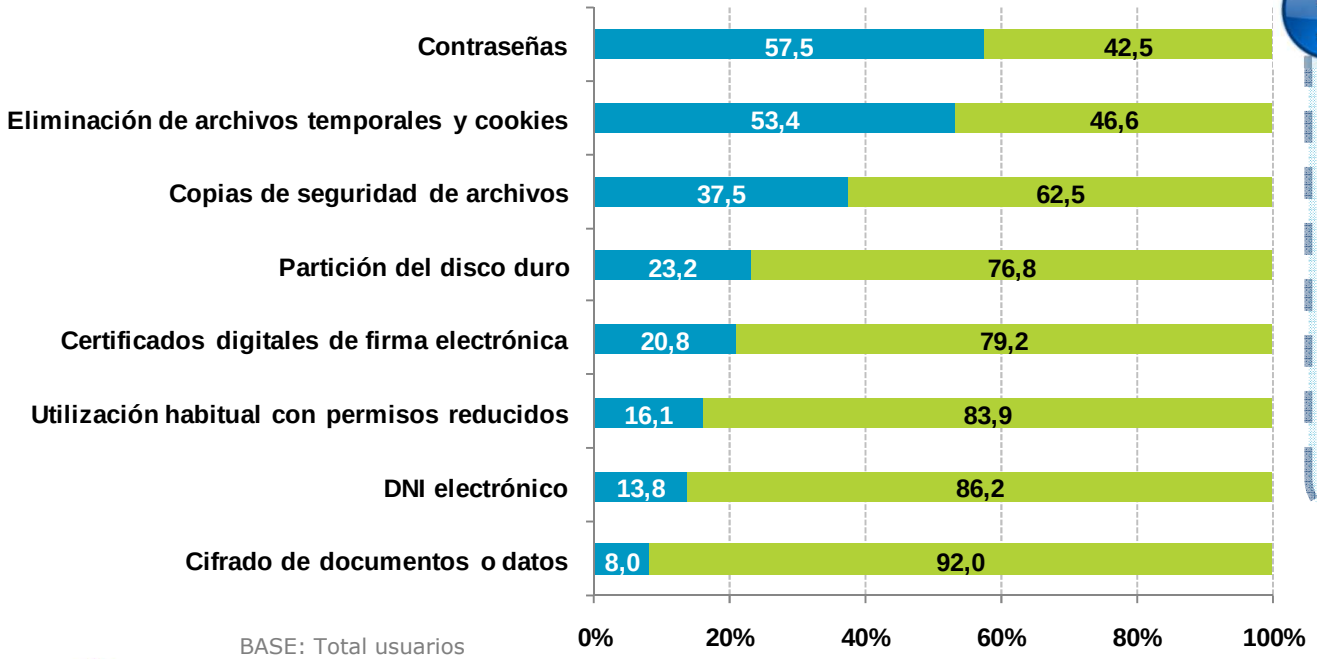
Información para conocer las medidas de seguridad: INTECO pone a disposición de los usuarios la Oficina de Seguridad del Internauta (www.osi.es), donde encontrarán herramientas, consejos y noticias que te ayudará a estar más protegido.

[1] Los datos referentes a las actualizaciones antivirus se presentan sobre la submuestra de usuarios que declaran utilizar antivirus (81,4%).

Uso de medidas de seguridad en el ordenador del hogar

Medidas de seguridad no automatizables o activas

Las medidas activas más utilizadas son las **contraseñas** (**57,5%**) y el borrado de **archivos temporales y cookies** (**53,4%**) generados durante la navegación a través de la red Internet.



BASE: Total usuarios

Las herramientas de seguridad activas son una capa más de seguridad que ofrecer a nuestros sistemas.

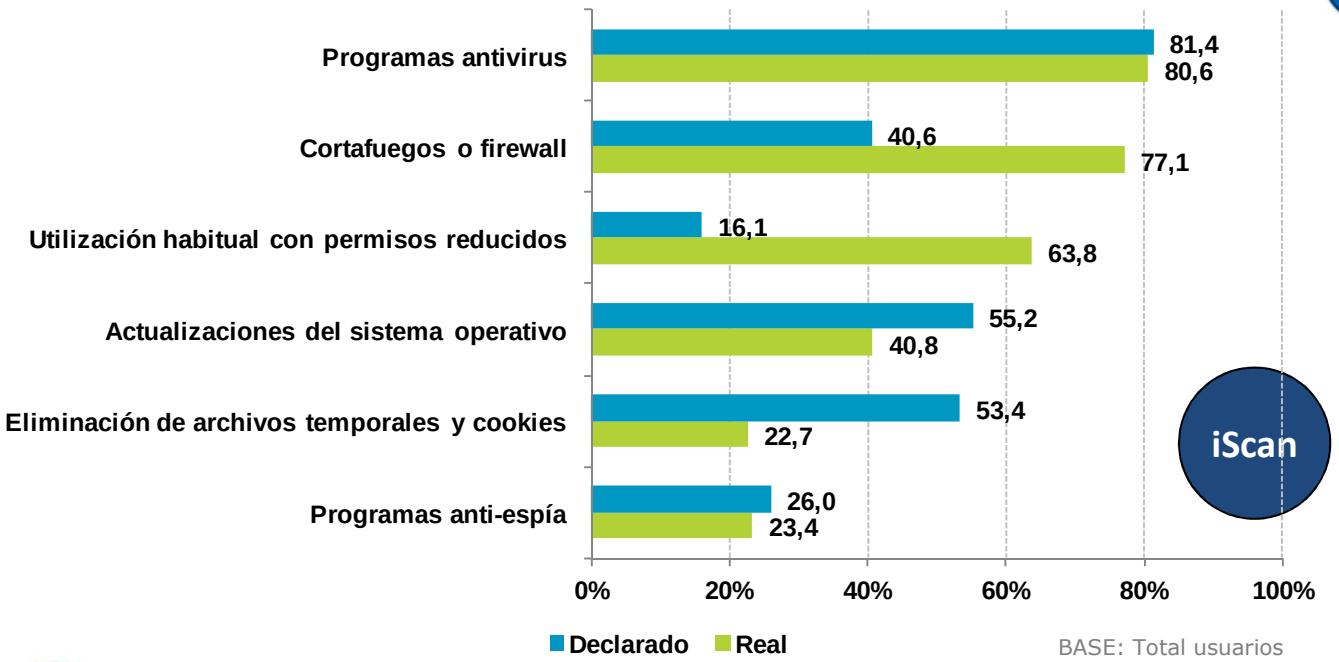
Son las principales medidas en cuanto a seguridad física se refiere así como cuando las medidas automatizables son eludidas.

Son especialmente importantes una buena gestión de las contraseñas y realizar copias de seguridad de nuestros datos. Para obtener más información sobre cómo realizar ambas visita:

- ✓ **Contraseñas:** http://www.osi.es/contrasenas
- ✓ **Copias de seguridad:** http://www.osi.es/copias-de-seguridad-cifrado

Uso de medidas de seguridad declarado vs. real

Únicamente el **16,1%** de los internautas encuestados declara utilizar habitualmente un **usuario con permisos reducidos** en el ordenador del hogar. Sin embargo, el dato real obtenido con iScan revela que el **63,8%** tiene una cuenta con **permisos limitados**.



BASE: Total usuarios

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

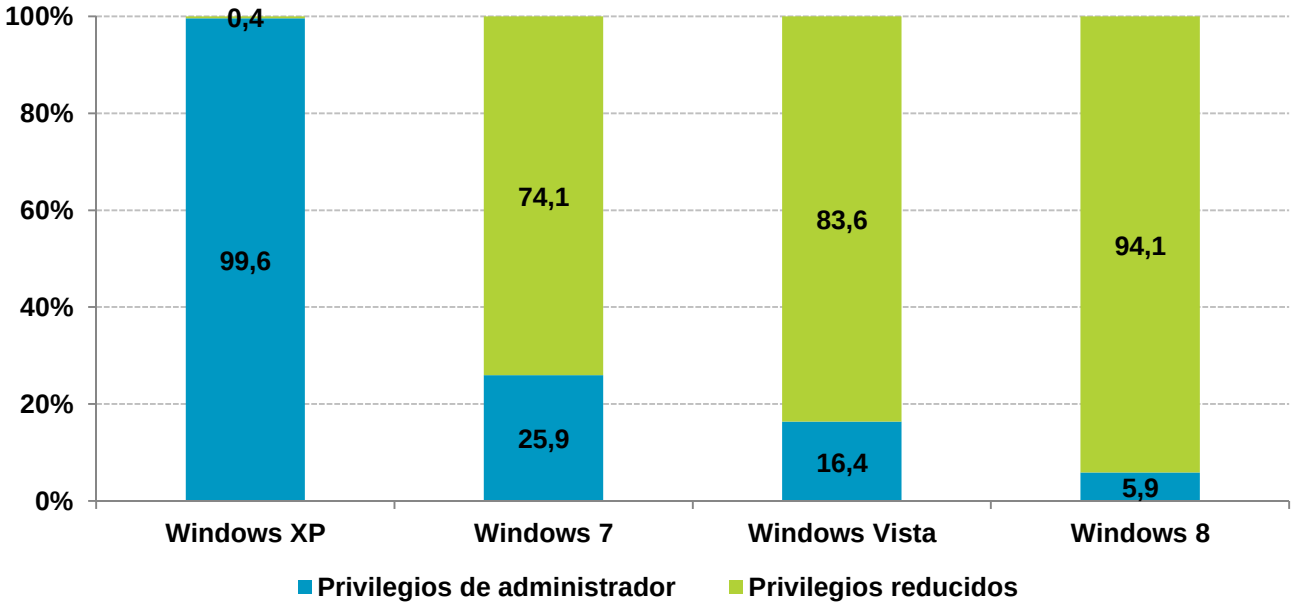
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

Para la obtención del dato real, se utiliza el software **iScan** desarrollado por INTECO, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 50 motores antivirus.

El software **iScan** se instala en los equipos y los analiza, detectando el malware residente en los mismos y recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas.

Uso de medidas de seguridad en el ordenador del hogar

Uso real de perfiles según nivel de privilegios en sistemas operativos Windows:



iScan

BASE: Total usuarios de Microsoft Windows

La diferencia apreciable en el nivel de privilegios utilizado en los distintos versiones de los sistemas operativos de Microsoft se debe fundamentalmente a la configuración por defecto de dichos sistemas operativos.

Utilice habitualmente la cuenta limitada (privilegios reducidos), solo es necesario recurrir a la de administrador en momentos puntuales, más información sobre las cuentas y cómo configurarlas: http://www.osi.es/cuentas-de-usuario

Motivos alegados para no utilizar medidas de seguridad

La no utilización de medidas de seguridad automatizables se debe principalmente a la opinión del usuario de **falta de necesidad** de las mismas.

Medidas	Hogares que no utilizan en la actualidad (%) *	Motivos (%) **						
		No conoce	No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros
Programas antivirus	18,6	7,0	**31,8**	20,5	13,1	5,8	4,1	17,6
Actualizaciones antivirus[2]	19,2	8,8	**30,9**	19,5	10,6	4,2	3,2	22,7
Actualizaciones del sistema operativo	44,8	14,4	**33,3**	10,8	10,7	4,9	2,3	23,6
Cortafuegos o firewall	59,4	22,2	**29,0**	10,1	14,9	3,9	3,7	16,1
Programas o configuración de bloqueo de pop-up	65,9	25,5	**33,1**	6,6	10,6	5,3	4,9	14,1
Programas o configuración anti-spam	69,6	19,9	**36,7**	6,7	10,4	5,6	4,8	16,0
Programas anti-espía o anti-fraude	74,0	23,4	**31,8**	11,2	9,5	6,9	3,0	14,2
Plugins de seguridad para el navegador	74,8	30,3	**31,2**	6,0	11,1	5,9	2,8	12,7
Programas o configuración para bloqueo de publicidad	80,3	**32,5**	30,4	6,1	9,0	6,0	2,9	13,1

* BASE: Total usuarios
** BASE: Usuarios que no utilizan la medida de seguridad en la actualidad

Información para conocer las medidas de seguridad: INTECO pone a disposición de los usuarios la Oficina de Seguridad del Internauta (www.osi.es), donde encontrarán herramientas, consejos y noticias que te ayudará a estar más protegido.

[2] Ver nota al pie número 1.

Motivos alegados para no utilizar medidas de seguridad

Un alto porcentaje de usuarios –**superior al 42%** en todos los casos– **no utiliza** medidas de seguridad activas al considerar que **no las necesitan**.

Destaca el caso de la no **utilización de contraseñas** para proteger el equipo con un **55,7%** de los usuarios

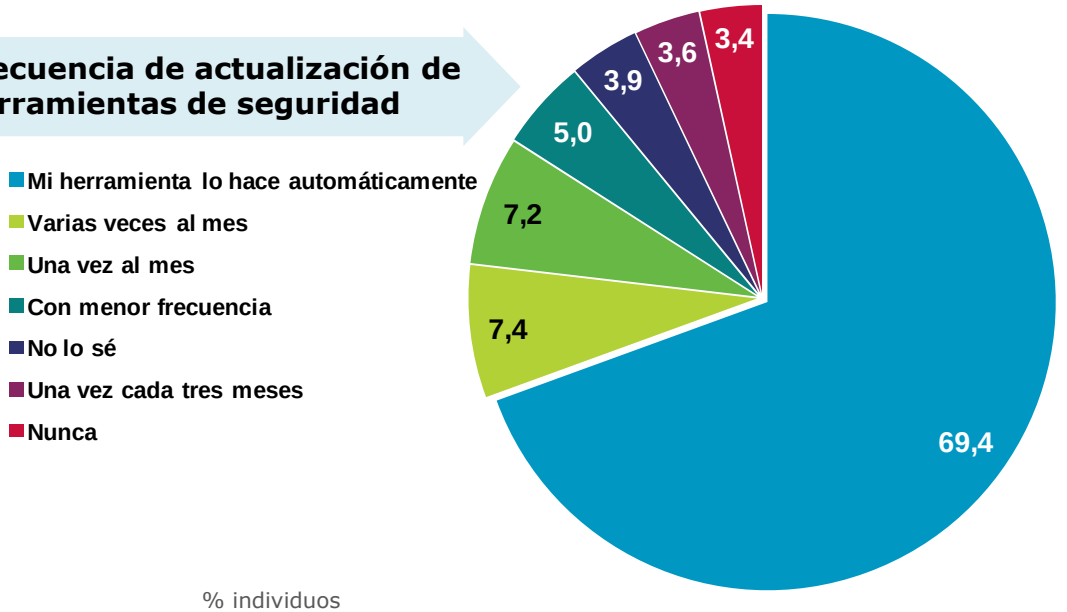
Medidas	Hogares que no utilizan en la actualidad (%) *	Motivos (%) **					
		No conoce	No necesita	Entorpecen	Desconfía	Ineficaces	Otros
Contraseñas (equipos y documentos)	42,5	10,2	**55,7**	8,5	5,1	4,8	15,7
Eliminación archivos temporales y cookies	46,6	21,1	**42,2**	9,7	4,7	3,6	18,7
Copia de seguridad de archivos	62,5	15,5	**46,5**	6,7	4,7	3,1	23,6
Partición del disco duro	76,8	24,5	**45,3**	7,4	3,1	2,8	16,9
Certificados digitales de firma electrónica	79,2	20,7	**48,3**	5,3	5,8	1,7	18,2
Utilización habitual con permisos reducidos	83,9	18,4	**51,8**	9,7	3,1	2,8	14,2
DNI electrónico	86,2	9,9	**52,0**	4,2	6,6	1,3	26,0
Cifrado de documentos o datos	92,0	28,3	**48,5**	6,8	3,5	1,3	11,6

* BASE: Total usuarios
** BASE: Usuarios que no utilizan la medida de seguridad en la actualidad

Frecuencia de actualización y utilización

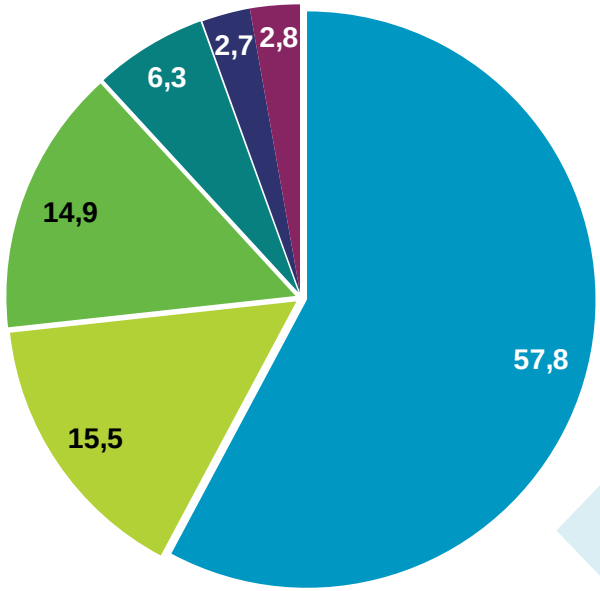
El **69,4%** de los usuarios declara que la **frecuencia de actualización** de las herramientas de seguridad se determina de manera **automática** por las propias herramientas.

Frecuencia de actualización de herramientas de seguridad



% individuos

BASE: Total usuarios



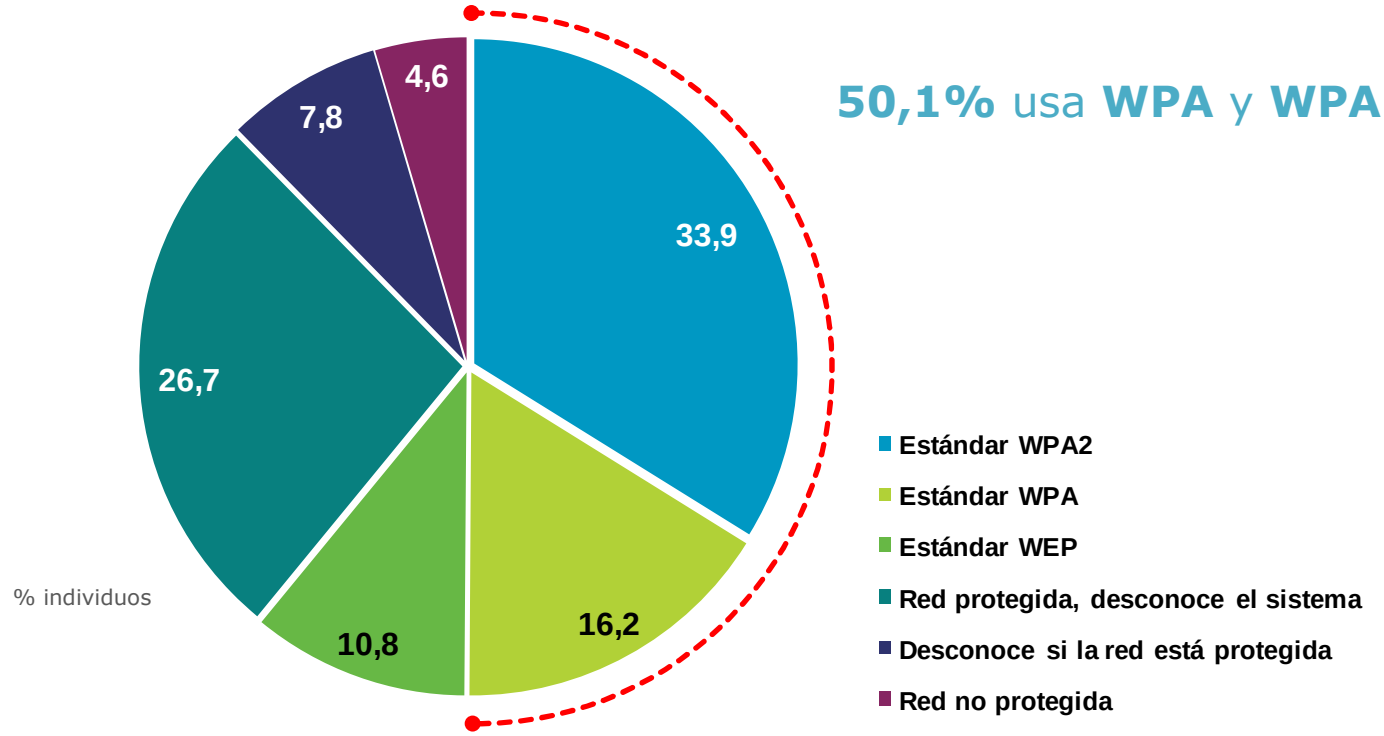
Frecuencia de escaneo con un programa antivirus

BASE: Usuarios que utilizan programas antivirus

El **57,8%** de los usuarios **no se implica** en el escaneo de su equipo para detectar infecciones, dejando que sea el propio programa antivirus el que lo haga **de manera predeterminada**.

Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi

Únicamente un **12,4%** de los usuarios deja su red inalámbrica Wi-Fi **desprotegida** y/o **desconoce** su estado.



50,1% usa **WPA** y **WPA2**

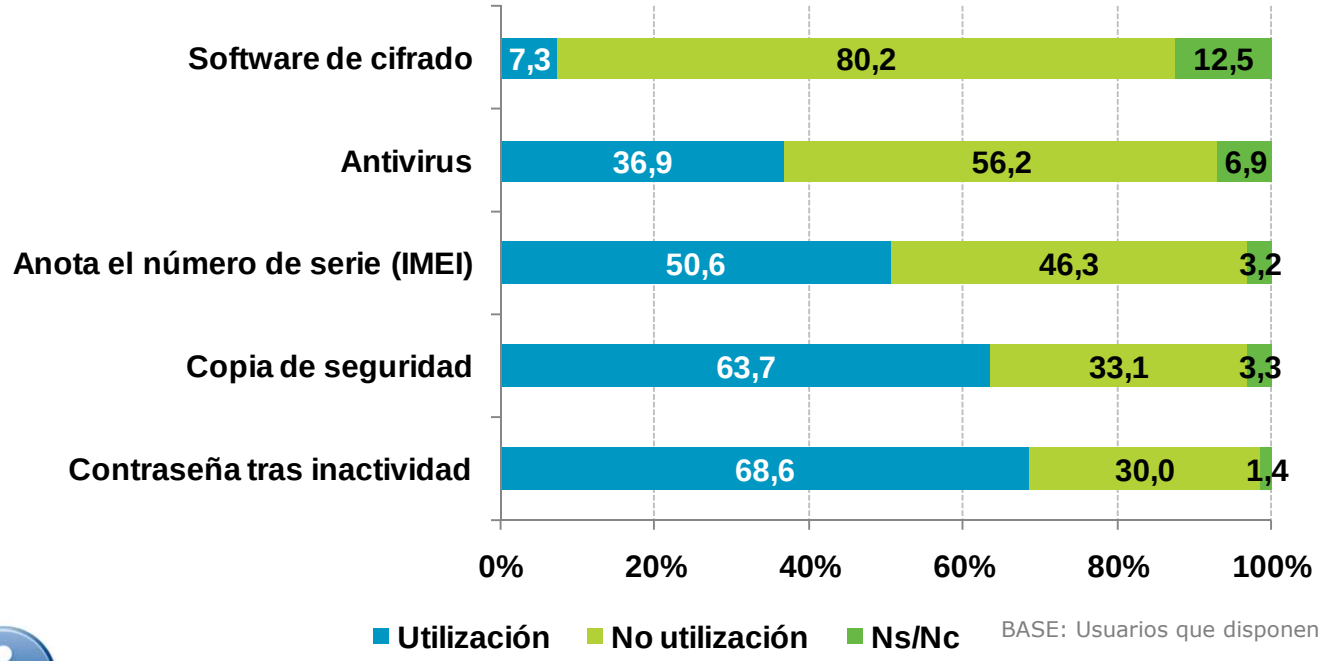
BASE: Usuarios Wi-Fi con conexión propia

Para conocer cómo configurar tu red Wi-Fi de modo seguro encontrarás toda la información en: http://www.osi.es/protege-tu-wifi

Medidas de seguridad utilizadas en smartphones

La mitad de los usuarios (**50,6%**) tiene anotado **el número de serie (IMEI)** de su teléfono móvil para **rastrear** o **desactivar el terminal** a través de la operadora de telefonía móvil, **en caso de pérdida o robo**.

Recomendaciones para proteger y/o conservar la información almacenada en los dispositivos móviles: http://www.osi.es/smartphone-y-tablet



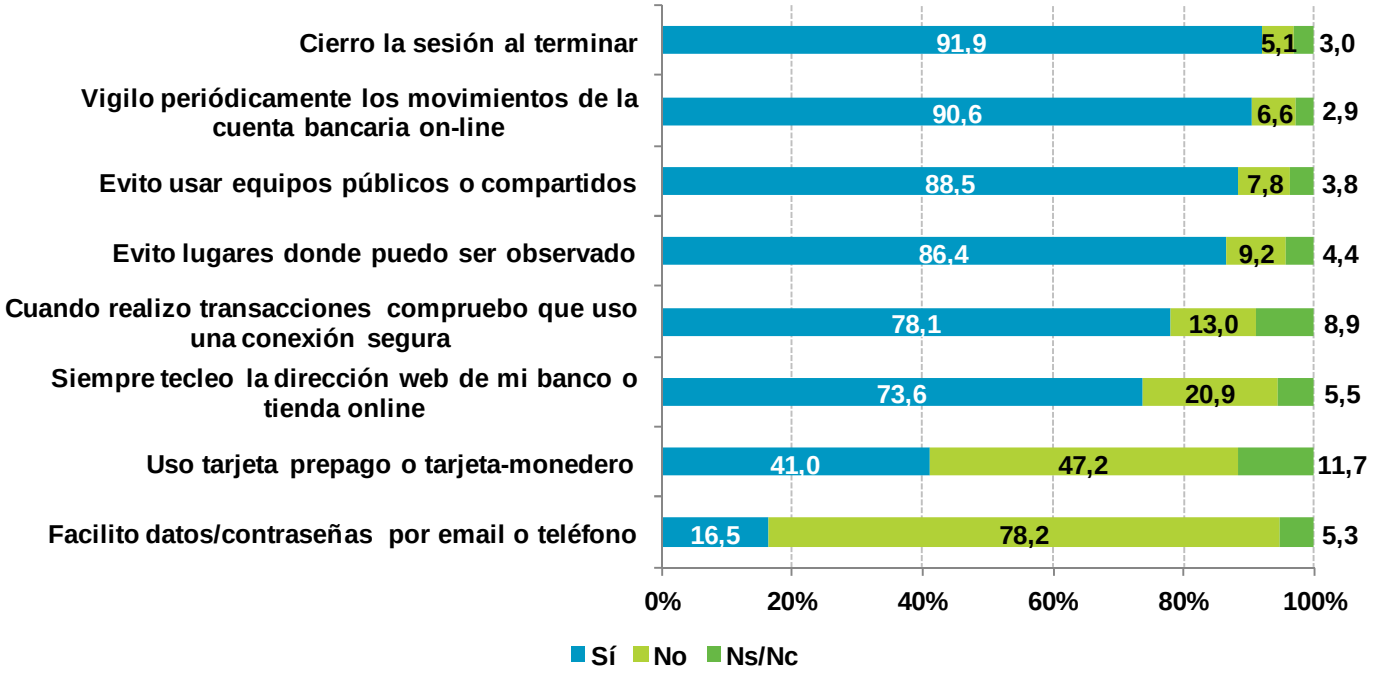
BASE: Usuarios que disponen de smartphone

El número de serie o IMEI (*International Mobile Equipment Identity*) se muestra en la pantalla del dispositivo al introducir el código ***#06#**

1. Banca en línea y comercio electrónico
2. Descargas en Internet
3. Redes sociales
4. Hábitos de uso de las redes inalámbricas Wi-Fi
5. Hábitos de uso en smartphones

Banca en línea y comercio electrónico

La mayoría de usuarios –superior al **73%**– mantiene buenos hábitos de comportamiento referentes a los **servicios de banca y comercio a través de Internet**. Únicamente el uso de **tarjetas prepago o monedero** es secundado por un porcentaje menor de usuarios (**41%**).



BASE: Usuarios que utilizan banca online y/o comercio electrónico

Para conocer qué medidas utilizar para protegerte al realizar trámites on-line visita:

http://www.osi.es/pagos-online

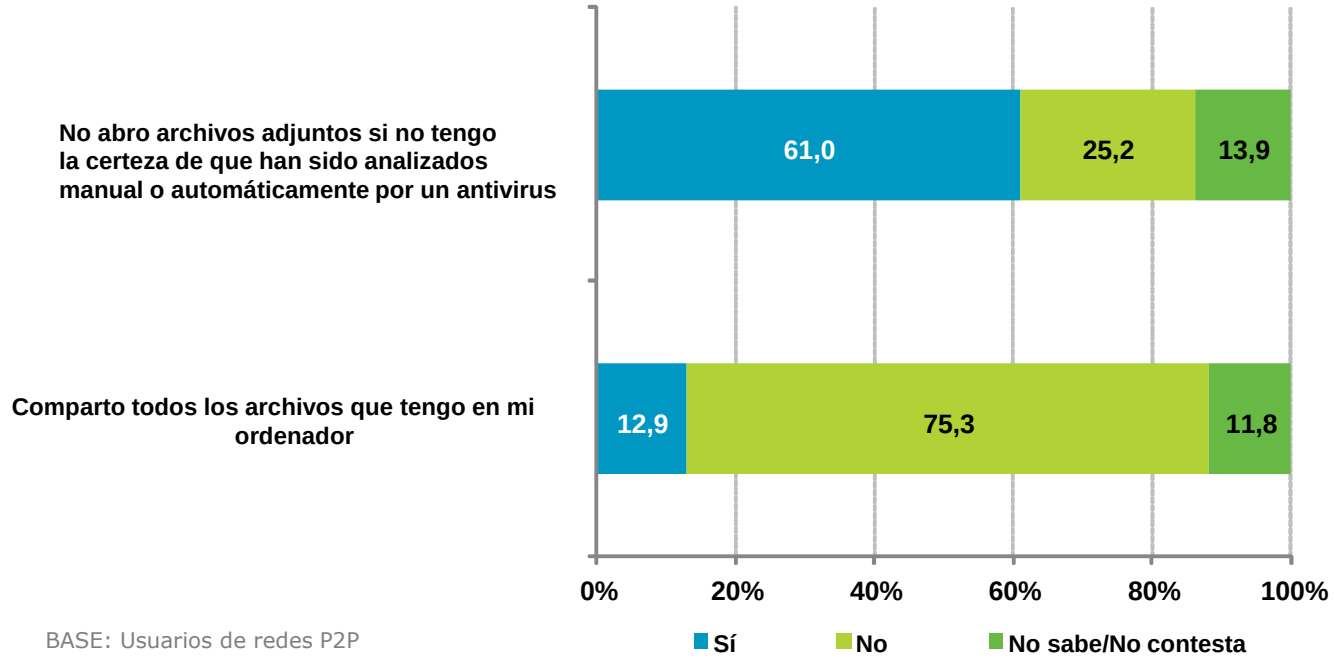
La utilización de las tarjetas prepago o monedero que ofrecen las entidades bancarias para realizar pagos online, evitan exponer los datos de la tarjeta de crédito o débito.

Además, en caso de ocurrir alguna incidencia, únicamente se comprometería la cantidad de crédito cargado por el usuario en dicha tarjeta, quedando protegido el saldo total de la cuenta bancaria.

No todas las entidades permiten este tipo de tarjetas.

Descargas en Internet

Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de malware. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como por ejemplo novedades de software, cinematográficas, musicales, etc.) logran el objetivo de infectar el equipo informático de usuarios poco precavidos.

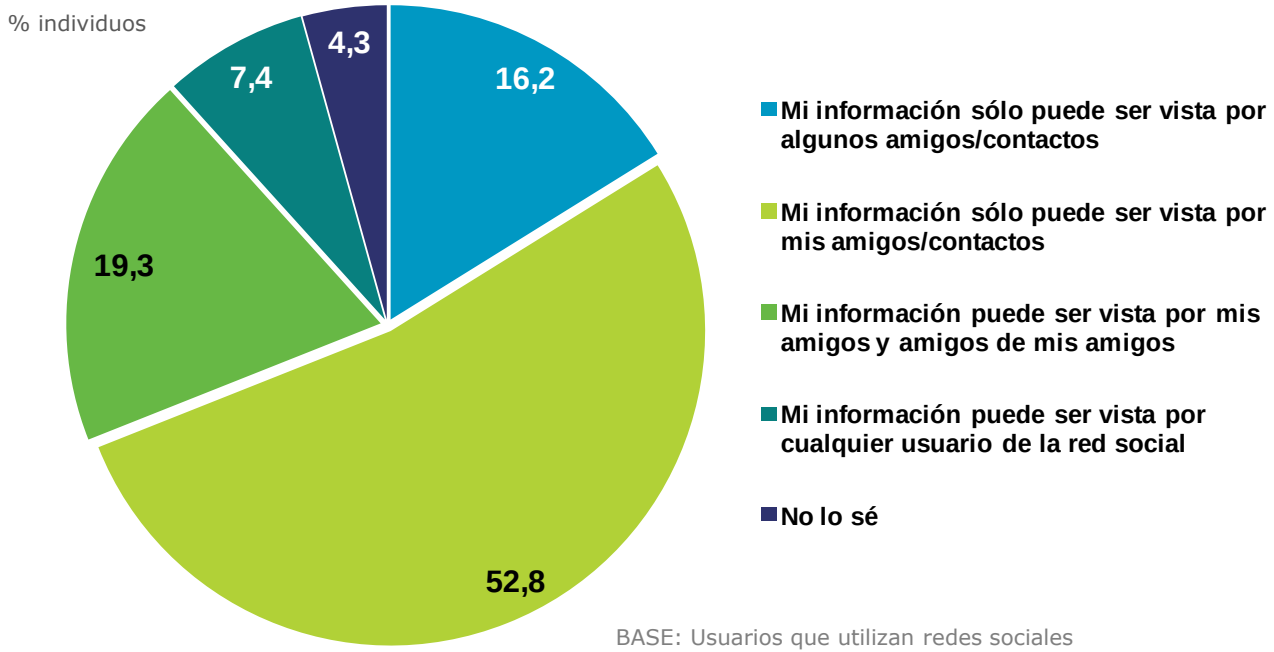


BASE: Usuarios de redes P2P

El **61%** de usuarios de redes P2P no abre archivos adjuntos si no tiene la certeza de que han sido analizados manual o automáticamente por un antivirus.

Para conocer cómo protegerte en las redes P2P:
http://www.osi.es/webs-de-descarga

Un **26,7%** (19,3 + 7,4) de los usuarios de redes sociales **expone los datos** publicados en su perfil a **terceras personas y/o desconocidos**, e incluso un **4,3%** de los consultados **desconoce** el nivel de privacidad de su perfil.



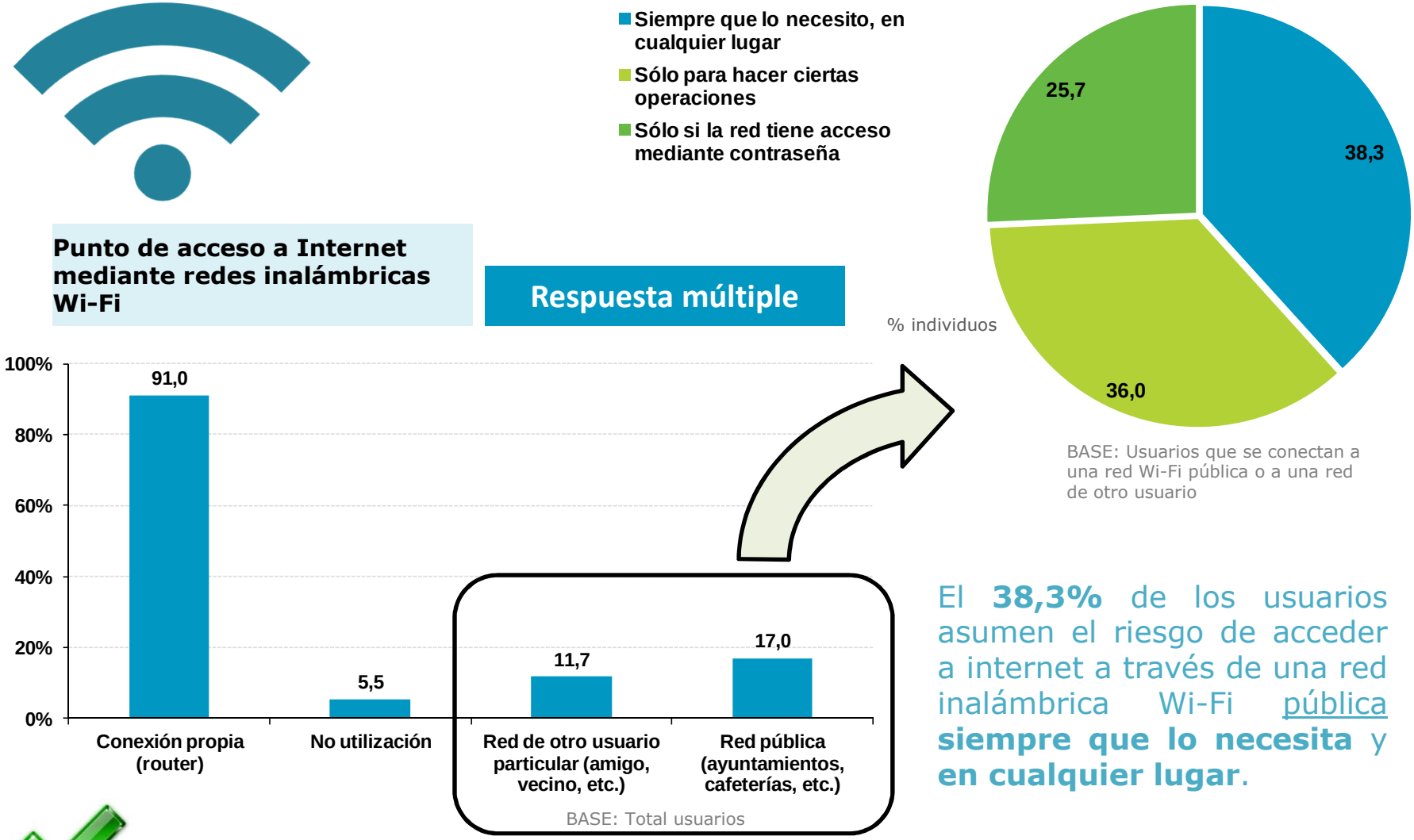
BASE: Usuarios que utilizan redes sociales

Para conocer cómo protegerte en las redes sociales y configurar los perfiles de cada una:
http://www.osi.es/redes-sociales

Hábitos de uso de las redes inalámbricas Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Respuesta múltiple



El **38,3%** de los usuarios asumen el riesgo de acceder a internet a través de una red inalámbrica Wi-Fi pública **siempre que lo necesita** y **en cualquier lugar**.

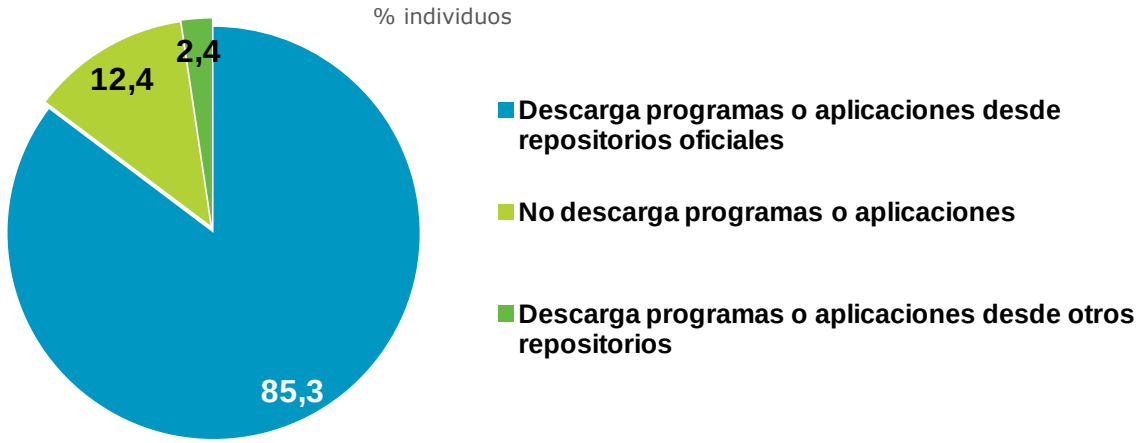
Consejos para conectarse seguro en redes Wi-Fi públicas:
http://www.osi.es/es/actualidad/blog/2013/07/05/redes-wifi-publicas-conectate-con-prudencia

Hábitos de uso en smartphones

Un **86,8%** de internautas con acceso frecuente a Internet posee un Smartphone o teléfono móvil "inteligente "

La gran mayoría (**85,3%**) prefiere realizar las descargas de aplicaciones directamente desde **repositorios oficiales.**

Un **12,4 %** no descarga ningún tipo de aplicaciones o programas.



BASE: Usuarios que disponen de smartphone

La ejecución o utilización de programas y/o archivos provenientes de fuentes dudosas puede suponer problemas de seguridad y la instalación en el dispositivo móvil de cualquier tipo de malware.

Incidentes de seguridad

1. Tipos de malware
2. Incidencias de seguridad
3. Evolución de los incidentes por malware
4. Tipología del malware detectado
5. Diversificación del malware detectado
6. Peligrosidad del malware y riesgo del equipo
7. Malware vs. sistema operativo y actualización
8. Malware vs. hábitos de comportamiento
9. Incidencias de seguridad en redes inalámbricas Wi-Fi
10. Incidencias de seguridad en smartphones

Tipos de malware

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario. Comúnmente se conocen como virus, en realidad se trata de un término más amplio que engloba otras tipologías.

Troyanos o caballos de Troya. *Bankers* o troyanos bancarios , *Backdoors* o puertas traseras, *Keyloggers* o capturadores de pulsaciones, *Dialers* o marcadores telefónicos, *Rogueware*

***Adware* o software publicitario**

Herramientas de intrusión

Virus

Archivos sospechosos detectados heurísticamente. Técnica empleada por los antivirus para reconocer códigos maliciosos que no se encuentran en la base de datos de virus del antivirus

***Spyware* o programas espía**

Gusano o *worm*

Otros. *Exploit, Rootkits , Scripts, Lockers* o *Scareware* , *Jokes* o bromas

Mas información: http://www.inteco.es/glossary/Formacion/Glosario/

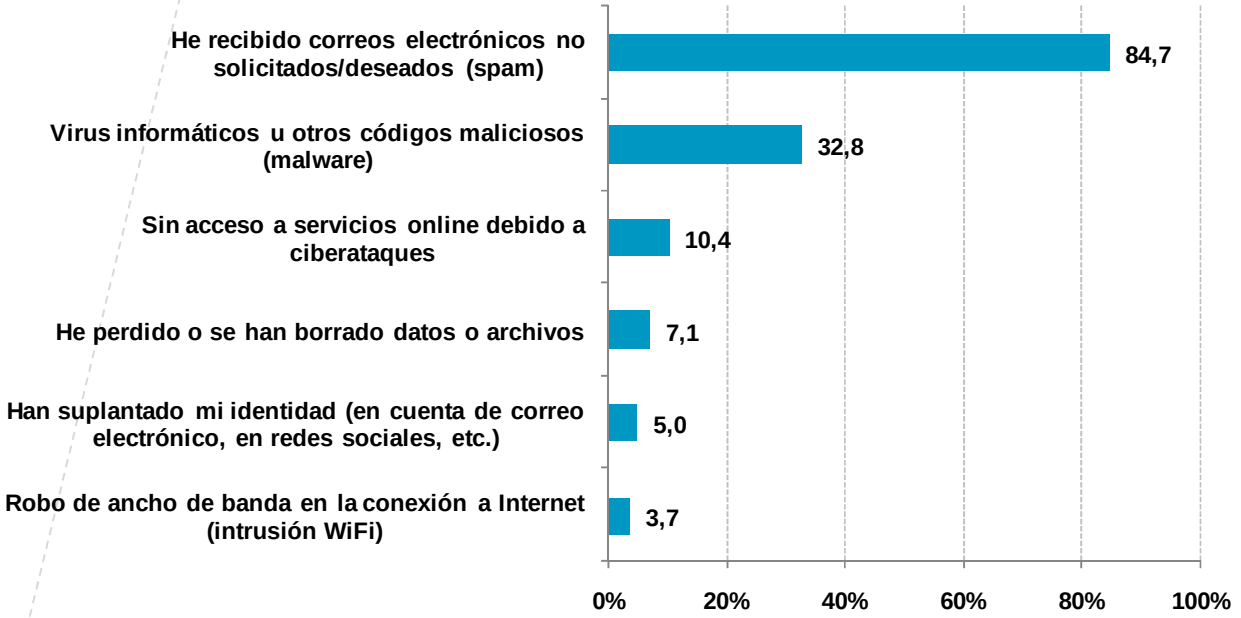
Incidencias de seguridad

Para conocer más en profundidad los riesgos de las amenazas e incidencias de seguridad:

http://www.osi.es/contra-virus

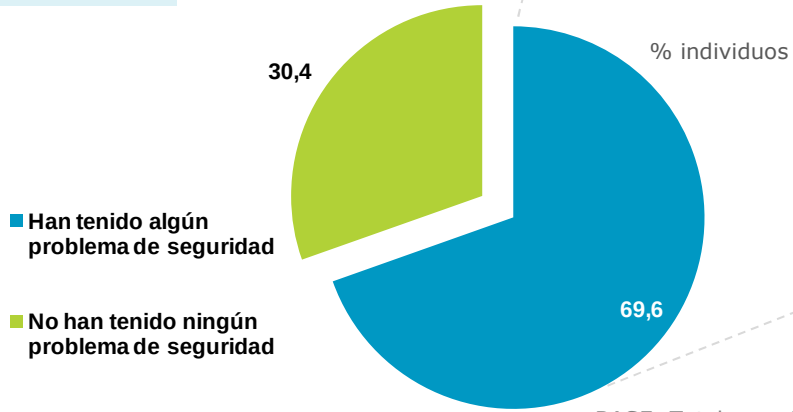
Incidencias sufridas:

Respuesta múltiple



BASE: Usuarios que han sufrido alguna incidencia de seguridad

Afectados:



BASE: Total usuarios

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

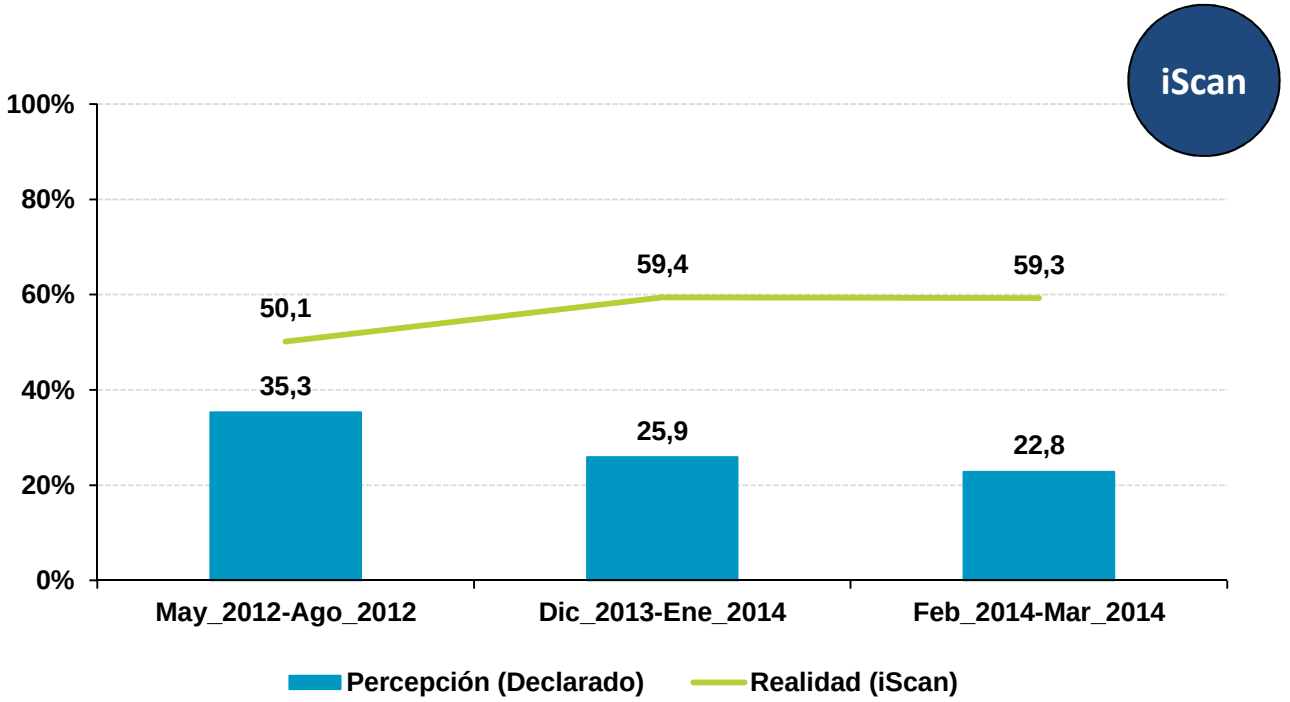
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

Evolución de los incidentes por malware

iScan revela que existe **una amplia brecha** entre las **incidencias reales de malware y las percibidas** por el usuario, (**37 puntos porcentuales**) .

Se denomina malware a todos aquellos programas malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.



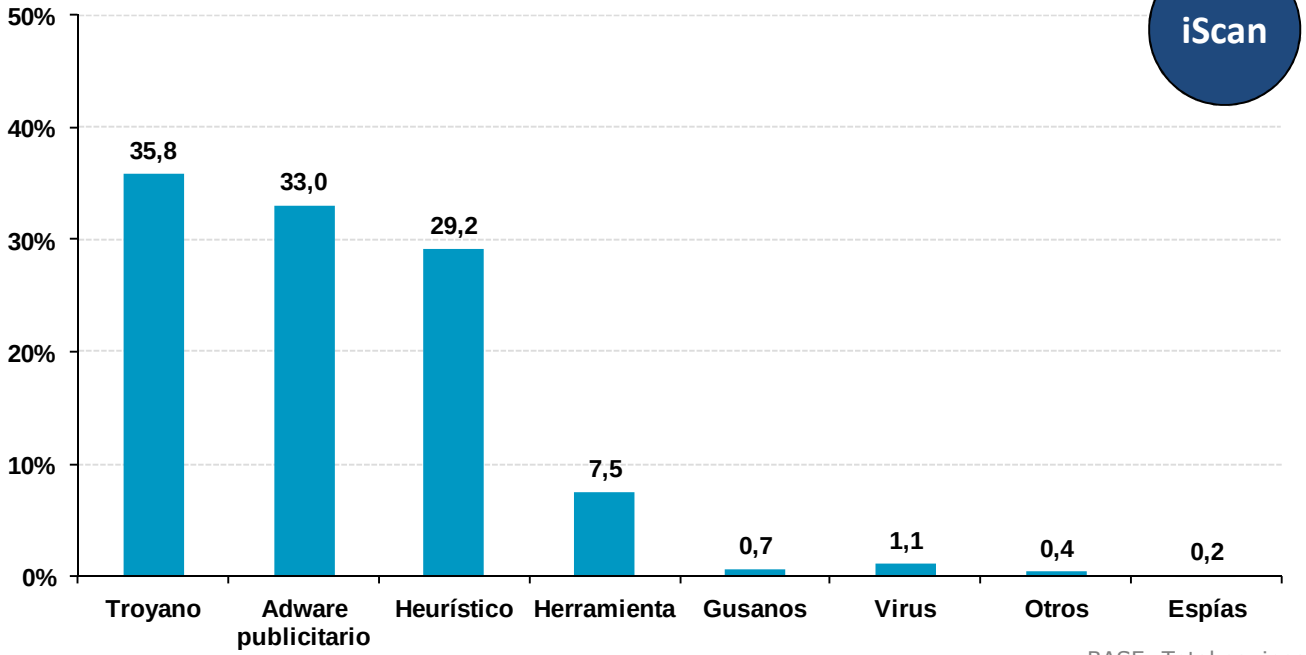
BASE: Total usuarios

Para la obtención del dato **real** se utiliza el software **iScan**, desarrollado por INTECO, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 50 motores antivirus. El software **iScan** se instala en los equipos y los analiza, detectando el malware residente en los mismos y recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas.

Tipología del malware detectado

El **troyano** sigue siendo el tipo de malware **más detectado** en los ordenadores españoles, llegando a presentarse en el **35,8%** de los ordenadores escaneados durante marzo de 2014. Ocupando una segunda posición se encuentra el **adware publicitario** detectado en un tercio de los equipos (**33%**).

Equipos que alojan malware según tipología (mar. 14)

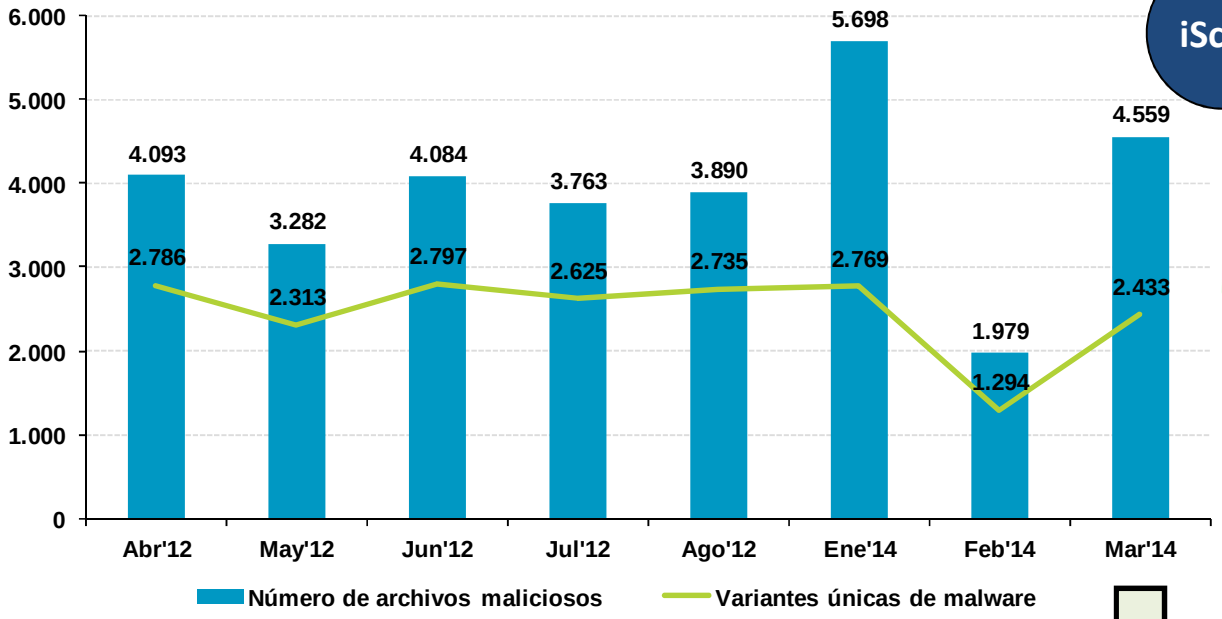


BASE: Total equipos

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

Diversificación del malware detectado

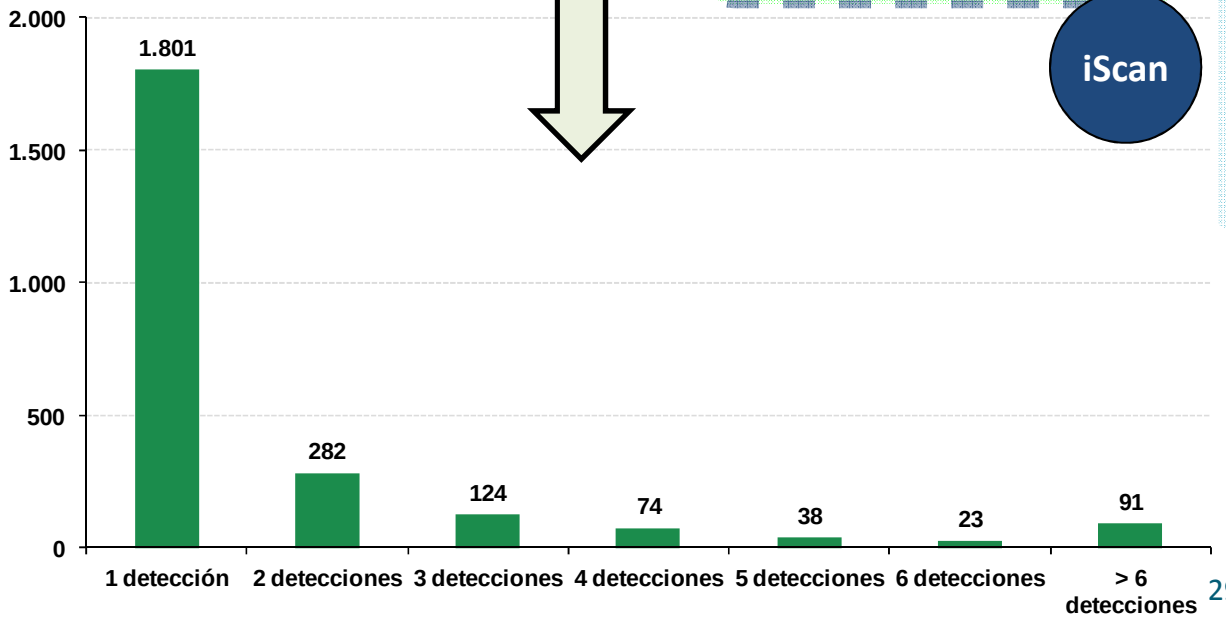


iScan

Evolución del número total de archivos maliciosos y variantes únicas de malware detectadas

Una variante única de malware (comúnmente conocidos como virus), es cada una de las diferentes muestras detectadas, independientemente del número de veces que aparecen en los equipos escaneados.

Número de detecciones de cada variante única de malware (mar. 14)



iScan

El **74,02%** de las variantes únicas **fue detectada tan sólo una vez**. Esto pone de manifiesto la gran variedad de código malicioso existente.

BASE: Equipos que alojan malware

Peligrosidad del código malicioso y riesgo del equipo

Para determinar el nivel de riesgo[3] de los equipos analizados, se establece la peligrosidad del malware detectado en función de las posibles consecuencias sufridas.

La clasificación se realiza en base a los siguientes criterios:

Peligrosidad alta: se incluyen en esta categoría los tipos de malware 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), o minan el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.

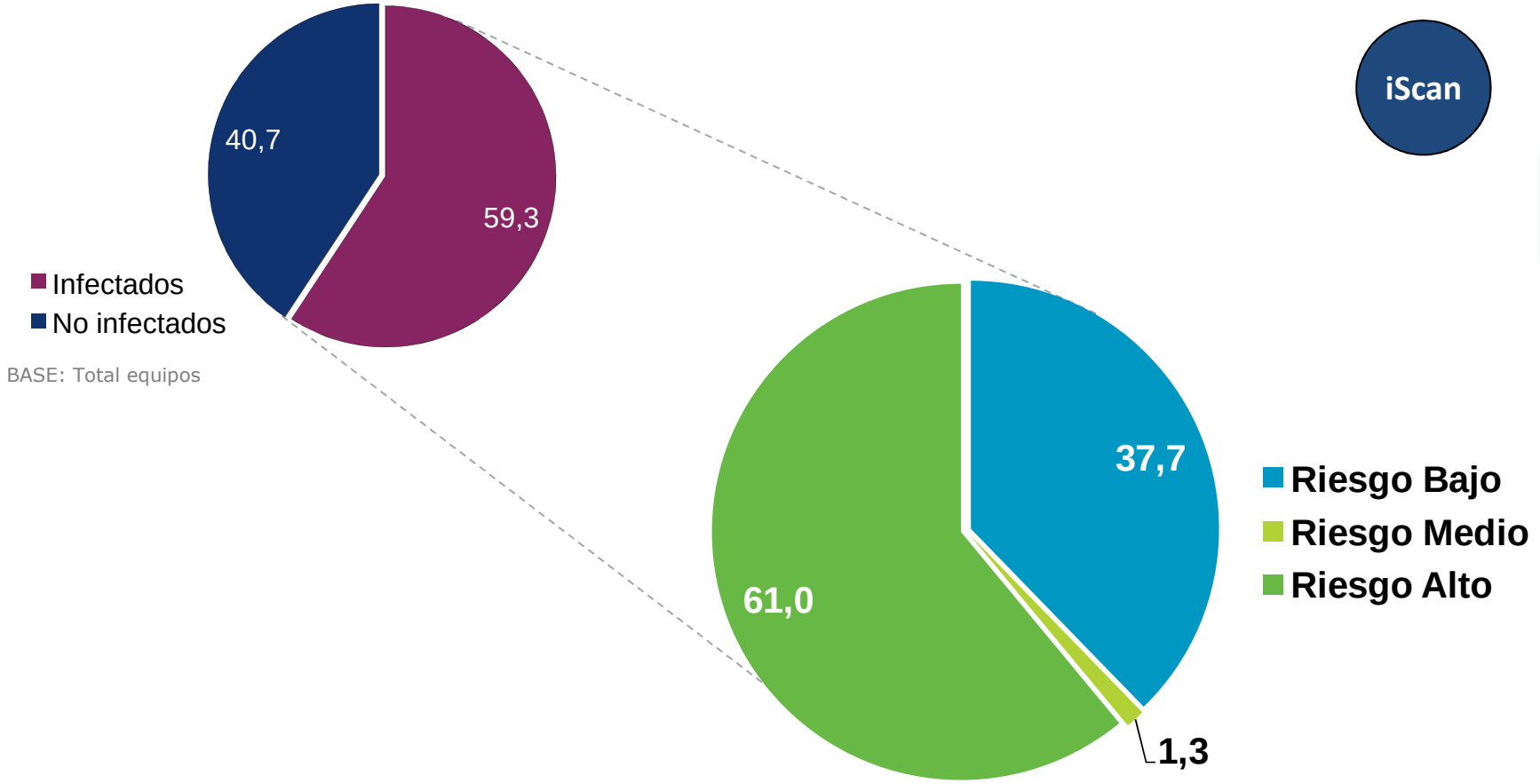
Peligrosidad media: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema: no perjudican de forma notoria su rendimiento, abren ventanas no deseadas al navegar, incrustan publicidad en páginas web legítimas que realmente no contienen publicidad, o facilitan la captura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

Peligrosidad baja: se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, *hacking tools*, 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 baja peligrosidad los 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, ya que estos no son capaces de ejecutarse sobre los equipos de los usuarios.

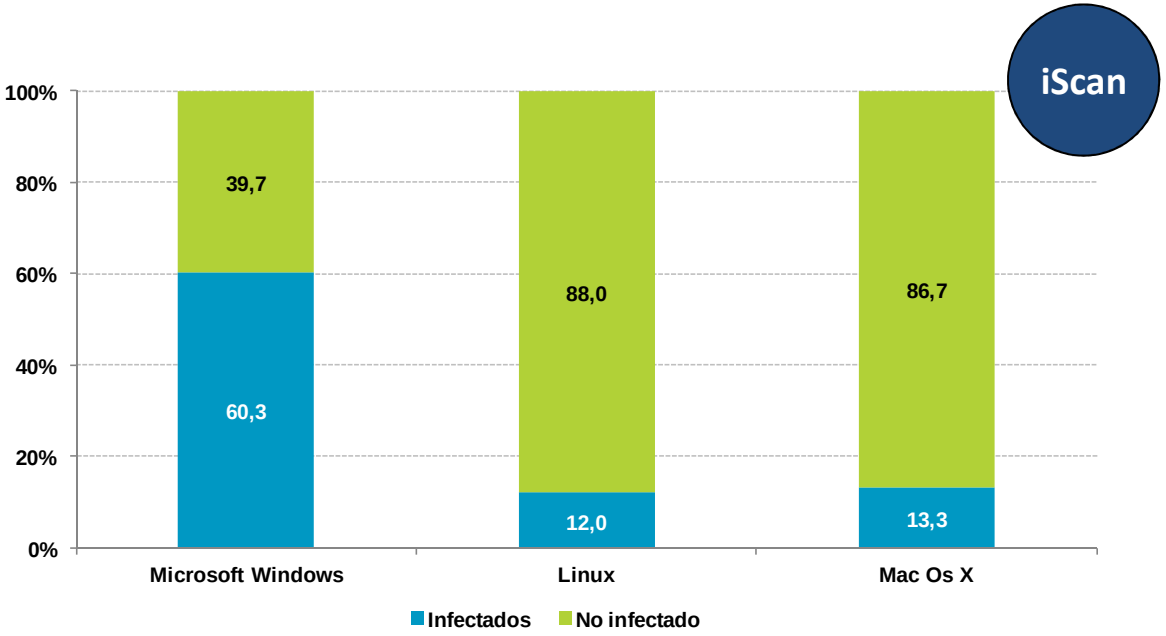
[3] Se establece como el nivel de riesgo de cada equipo el de mayor nivel de entre el malware que aloje. Es decir, un equipo en el que se detecte un software malicioso de peligrosidad alta y otro de peligrosidad media, siempre será incluido en el grupo de equipos con un nivel de riesgo alto.

Peligrosidad del código malicioso y riesgo del equipo

Un **59,3%** de los equipos analizados con iScan presentan al menos una **infección**, y de estos, el **61%** se encuentran muestras con un nivel de **riesgo alto** debido al potencial peligro que suponen dichos archivos maliciosos.



Malware vs. sistema operativo y actualización



Equipos infectados según sistema operativo

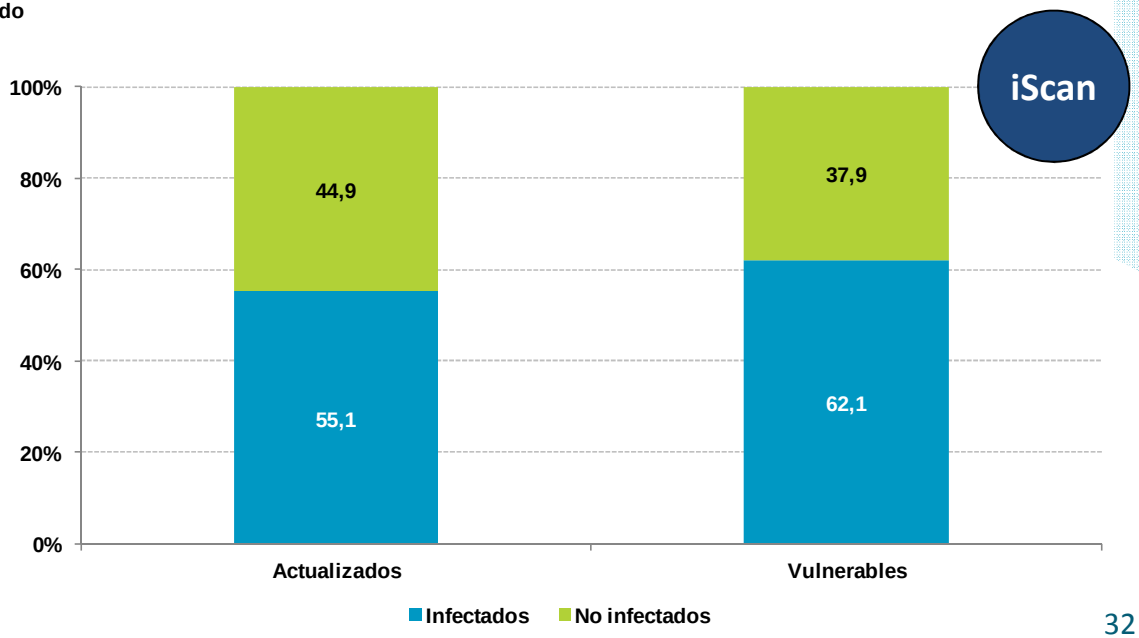
iScan detecta **malware** en más del **60%** de máquinas con sistemas operativos Microsoft Windows.

Infectados
No infectados

BASE: Total usuarios

Equipos infectados según estado de actualización

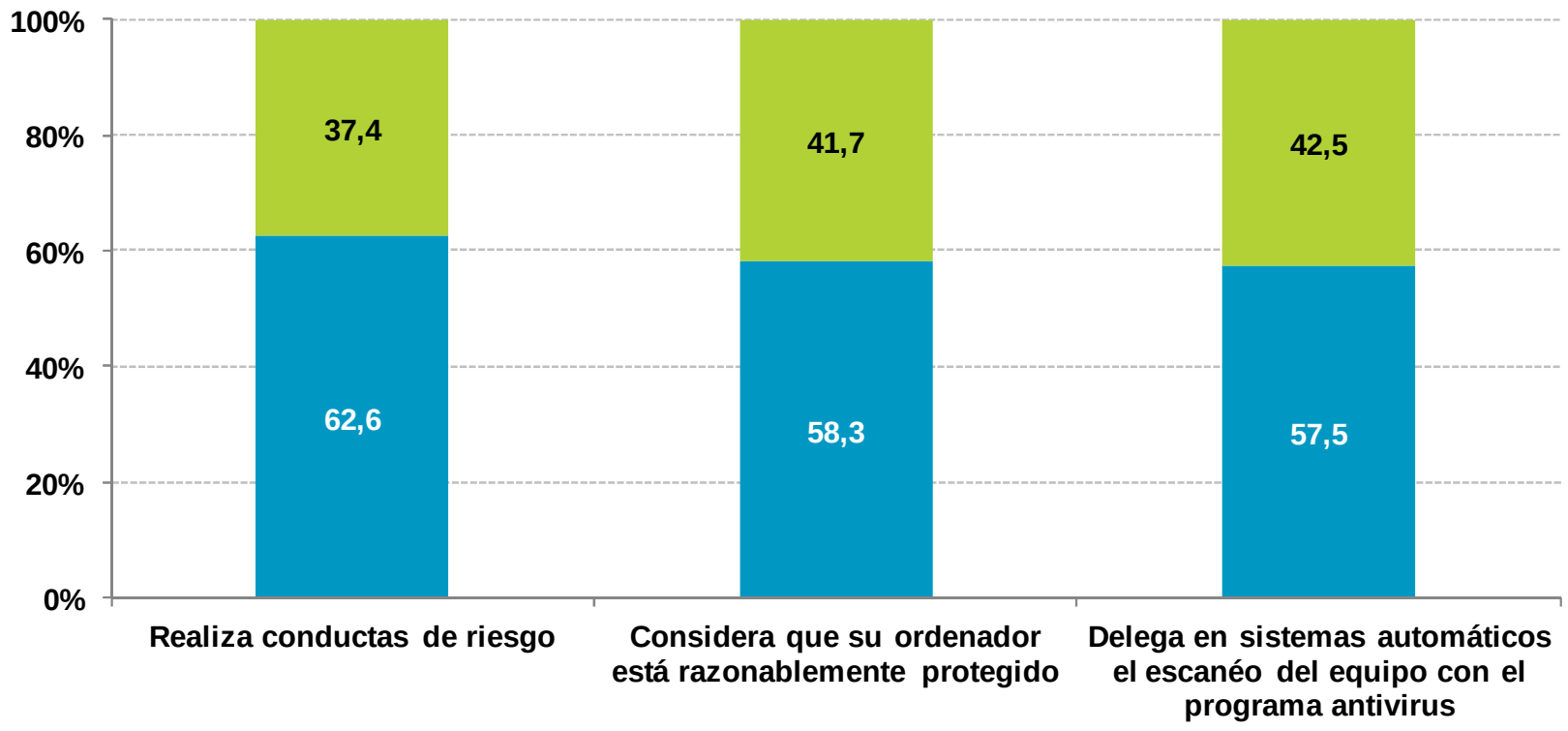
Existen **7 puntos porcentuales** de diferencia entre los equipos que alojan malware según el estado de **actualización del sistema operativo**, a favor de aquellos que cuentan con todos los **parches de seguridad** instalados.



Malware vs. hábitos de comportamiento

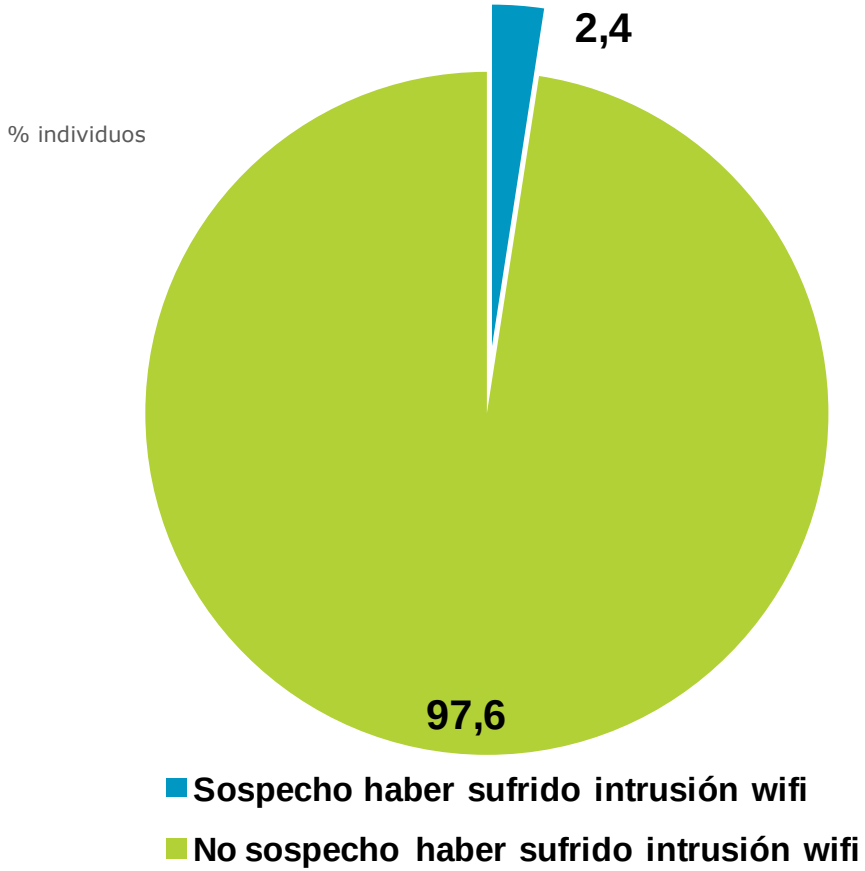
El **58,3%** de los usuarios que consideran su ordenador razonablemente protegido han tenido infección en el mismo, al igual que el **57,5%** de los usuarios que delegan en sistemas automáticos el escaneo del equipo con el programa antivirus.

Resulta destacable el **62,6%** de infecciones que tienen lugar entre aquellos usuarios que llevan a cabo **conductas de riesgo** de manera consciente y de forma puntual.



BASE: Total usuarios

Incidencias de seguridad en redes inalámbricas Wi-Fi



Cómo saber si alguien está conectado a tu red inalámbrica Wi-Fi:

http://www.osi.es/es/actualidad/blog/2014/03/17/como-saber-si-alguien-se-esta-conectado-tu-red-wifi

Aunque más del 12% de los usuarios deja la red Wi-Fi desprotegida y/o desconoce su estado, y otro 10,8% utiliza el estándar WEP -sistema de cifrado obsoleto y totalmente comprometido–, únicamente un **2,4%** de panelistas *sospechan* que pueden haber sufrido una **intrusión** en la red inalámbrica Wi-Fi de su hogar.

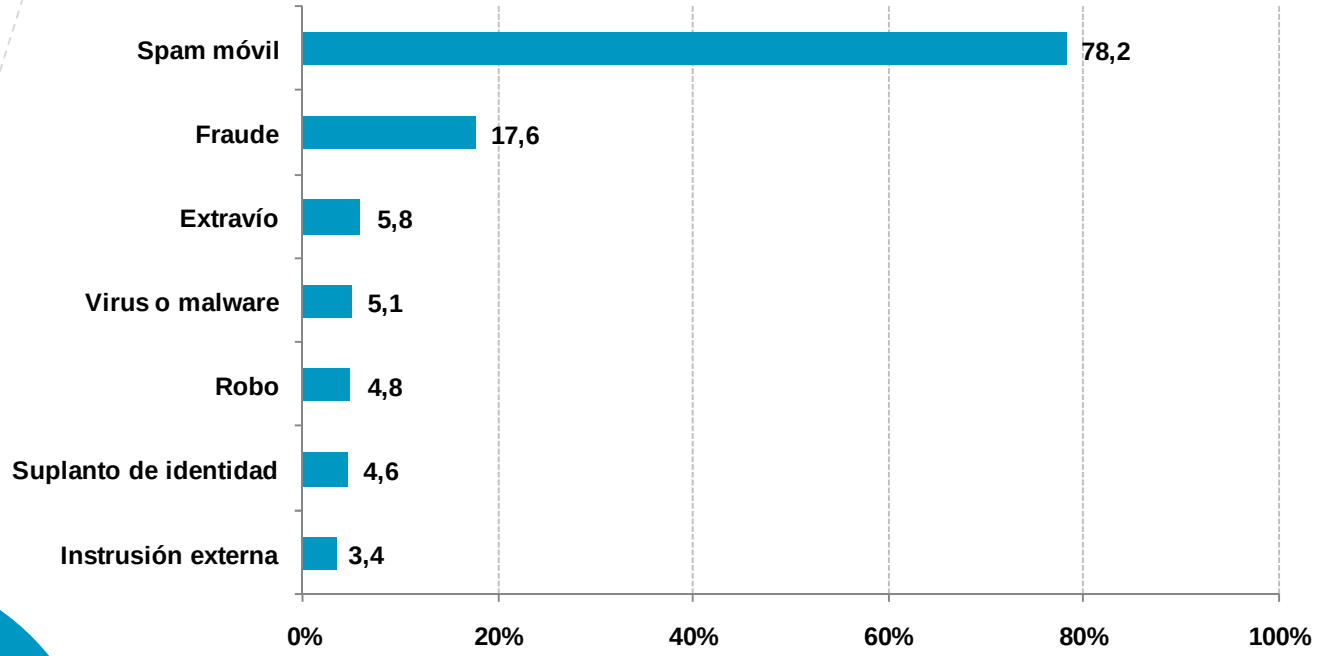
4

BASE: Usuarios con conexión Wi-Fi propia

Incidencias de seguridad en smartphones

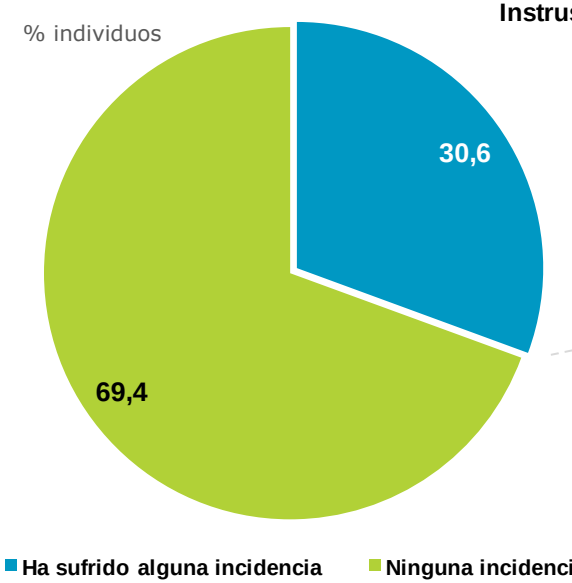
Incidencias sufridas:

Respuesta múltiple



BASE: Usuarios que disponen de smartphone y han sufrido una incidencia de seguridad

Afectados:



La **principal incidencia móvil** que los internautas consideran haber sufrido es el **spam móvil**, alegado por un **78,2%** de los encuestados. La segunda incidencia sufrida, el fraude, declarada por un 17,6% de los encuestados.

BASE: Usuarios que disponen de smartphone

Consecuencias de los incidentes de seguridad y reacción de los usuarios

1. Consecuencias de los incidentes de seguridad
2. Intento de fraude telefónico y manifestaciones
3. Intento de fraude online y manifestaciones
4. Seguridad y fraude online y telefónico
5. Cambios adoptados tras un incidente de seguridad
6. Resolución de incidentes de seguridad

5

Consecuencias de incidentes de seguridad en dispositivos móviles

Consecuencias de incidentes de seguridad en dispositivos móviles

Las **principales consecuencias** de las incidencias de seguridad acontecidas entre usuarios de dispositivos móviles debidas a un fraude, son el **perjuicio económico** (**54%**) y la **suscripción a servicios no solicitados** (**49,7%**).

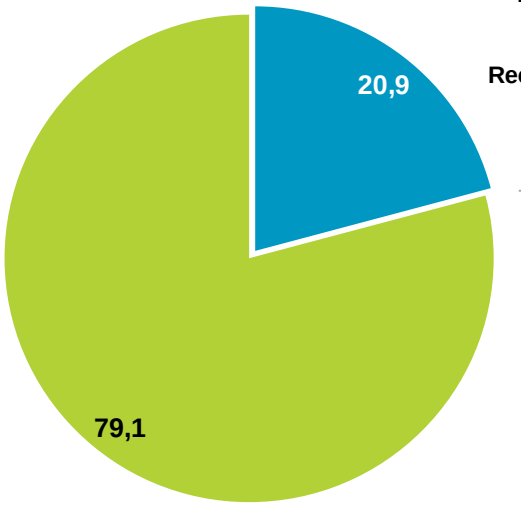
Consecuencias	Incidencias (%)						
	Extravío	Robo	Virus o Malware	Suplantación de identidad	Intrusión externa	Spam	Fraude
Robo de datos	18,1	15,7	**23,9**	8,9	12,1	1,5	2,7
Pérdida de datos	23,0	**31,9**	7,7	26,1	17,1	3,4	5,8
Suplantación de identidad	13,9	10,3	0,0	**31,7**	3,9	2,5	5,0
Sustracción de datos online	16,6	2,9	**34,9**	16,7	17,3	0,5	3,2
Perjuicio económico	43,0	43,9	19,2	20,2	29,3	10,5	**54,0**
Suscripción a servicios no solicitados	9,3	9,3	44,7	12,1	31,7	13,4	**49,7**
Otro	1,6	0,0	3,3	0,0	**8,6**	3,4	1,8
Ninguna de las anteriores	31,5	23,6	30,9	30,1	13,2	**73,4**	8,5

Conoce más sobre cómo defenderte si tienes un iPhone/iPad
https://www.osi.es/es/actualidad/blog/2013/10/25/las-9-funcionalidades-de-seguridad-que-tienes-que-utilizar-si-tienes-un-i
Conoce más sobre cómo defenderte si tienes una BlackBerry
https://www.osi.es/es/actualidad/blog/2013/12/11/las-9-funcionalidades-de-seguridad-que-tienes-que-utilizar-si-tienes-una-
Conoce más sobre cómo defenderte si tienes un Android
https://www.osi.es/es/actualidad/blog/2013/10/18/las-nueve-funcionalidades-de-seguridad-que-tienes-que-utilizar-si-tienes-

BASE: Usuarios que disponen de smartphone y sufre cada una de las incidencias

Intento de fraude telefónico y manifestaciones

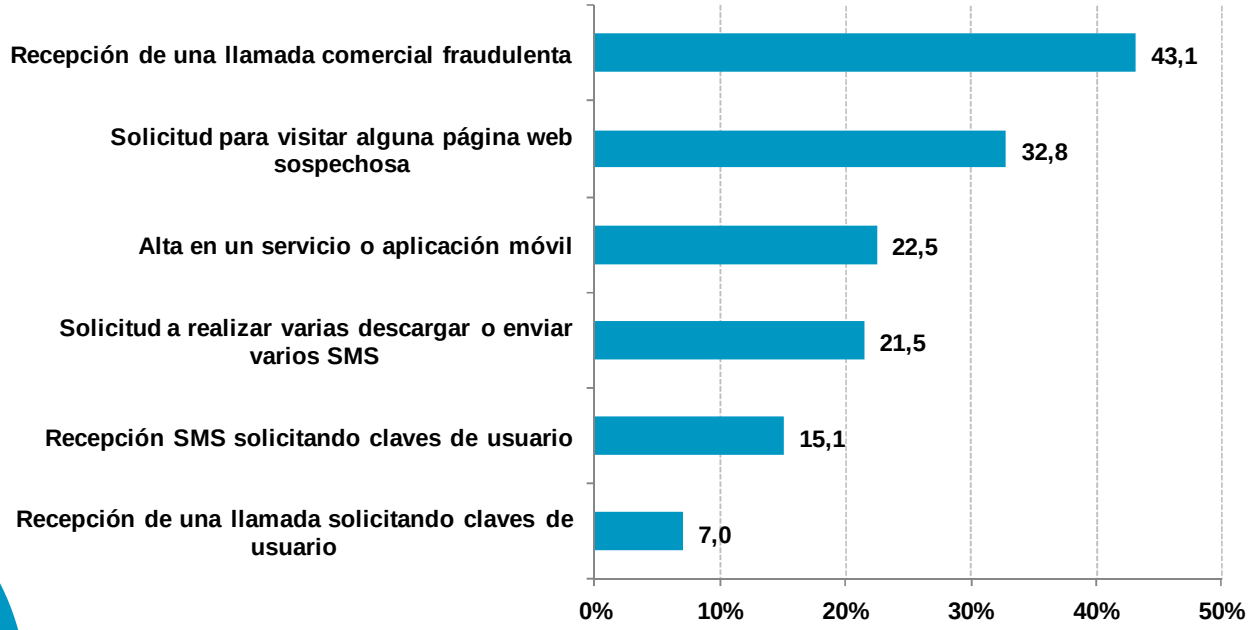
Intento de fraude telefónico:



BASE: Usuarios que disponen de dispositivo móvil o smartphone

Manifestaciones del intento de fraude telefónico:

Respuesta múltiple

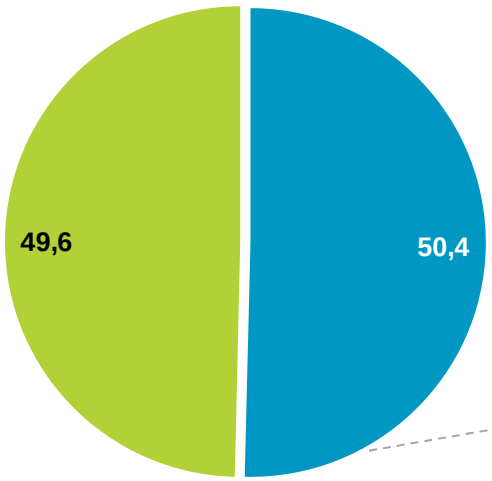


% individuos

BASE: Usuarios que disponen de dispositivo móvil o smartphone y han sufrido algún tipo de fraude

Intento de fraude online y manifestaciones

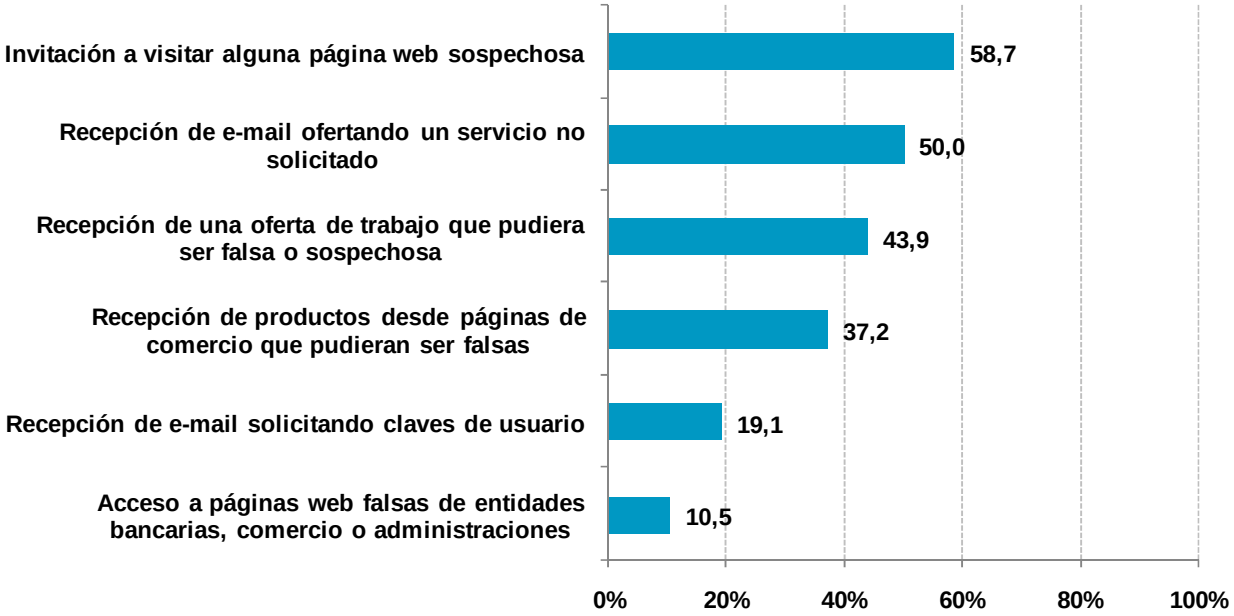
Intento de fraude online:



BASE: Total usuarios

Manifestaciones del intento de fraude online:

Respuesta múltiple



% individuos

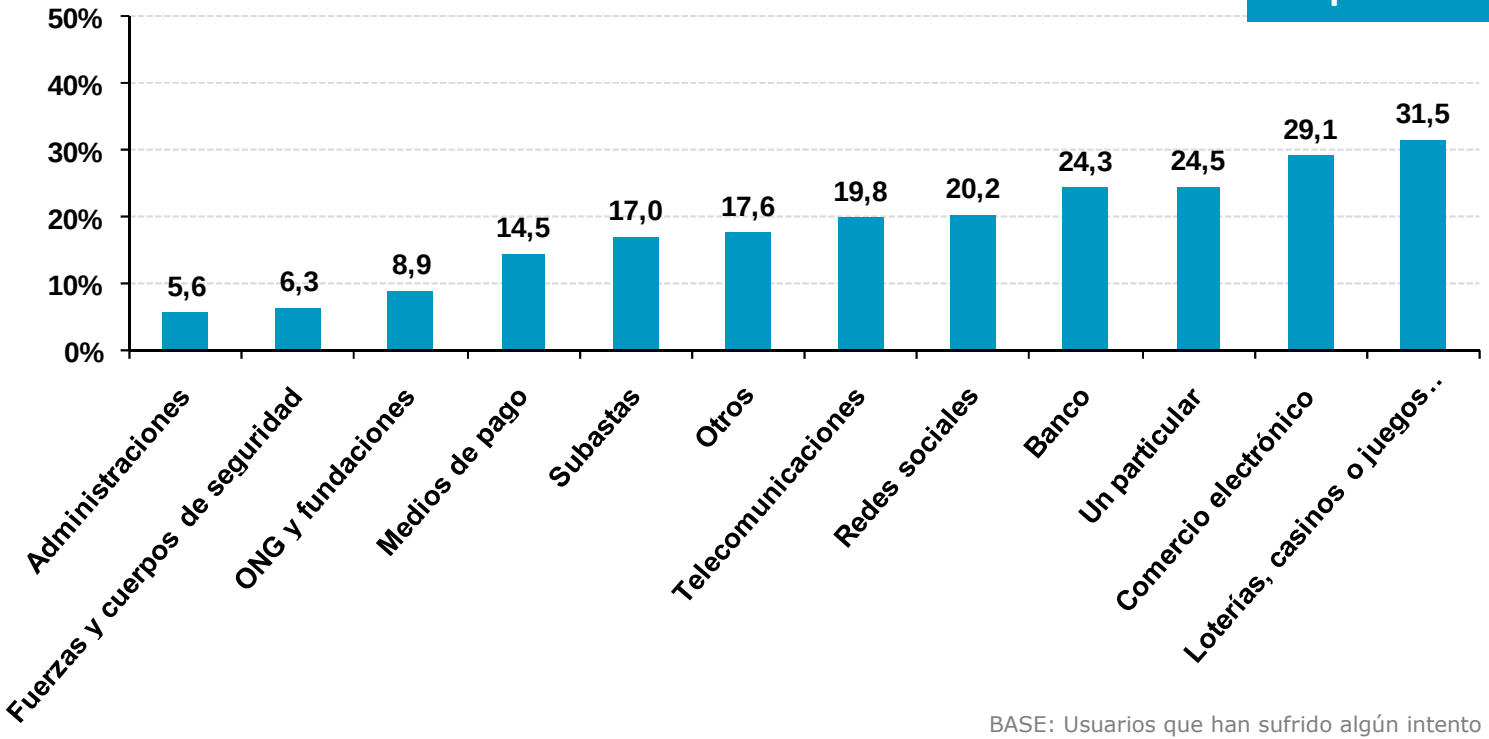
BASE: Usuarios que han sufrido algún intento de fraude

Conoce más en profundidad el fraude online:
http://www.osi.es/fraude-online

Intento de fraude online: forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta[4]

La principal **forma adoptada** por el remitente de la comunicación sospechosa de ser fraudulenta, es la imagen de **"Loterías, casinos y juegos online"** (**31,5%**), seguida del **comercio electrónico** (**29,1%**).

Respuesta múltiple



BASE: Usuarios que han sufrido algún intento de fraude

[4] Los literales utilizados en el cuestionario son los siguientes: Banco o entidades financieras, Páginas de comercio electrónico o compraventa online, Entidades de medios de pago (tarjetas de crédito, PayPal, etc.), Redes sociales, páginas de contactos, Organismos de la Administración Pública, Operadores de telecomunicaciones (telefonía fija, móvil, Internet), Organizaciones sin ánimo de lucro (ONGs, fundaciones, museos, etc.), Páginas de subastas online, Páginas de loterías, casinos o juegos online, Fuerzas y cuerpos de seguridad del Estado, Un particular, Otros.

Seguridad y fraude online y telefónico

Analizando los datos según la manifestación del fraude, la principal forma adoptada por el remitente[5] es el **envío de e-mails solicitando claves de usuario** (**56,8%**) y de invitaciones a **páginas web falsas** (*phishing*) de entidades bancarias, comercio, etc. (**55,5%**).

Manifestación del fraude	Forma adoptada por el remitente de la comunicación (%)											
	Administraciones	Otros	ONG y fundaciones	Particular	Subastas	Telecomunicaciones	Redes sociales	Loterías	Comercio electrónico	Medios de pago	Banco	Fuerzas y cuerpos de seguridad
Recepción de e-mail solicitando claves de usuario	9,5	14,1	12,6	26,8	19,2	24,1	25,1	35,0	29,6	31,9	**56,8**	10,7
Recepción de e-mail ofertando un servicio no solicitado	6,1	14,1	12,2	25,1	24,4	31,1	23,2	**42,8**	40,7	19,1	27,4	6,6
Recepción de e-mail con invitación a visitar alguna página web sospechosa	6,6	16,5	9,8	27,1	19,5	21,7	27,1	**37,5**	32,4	17,7	29,2	7,1
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	7,4	21,8	10,5	**34,5**	18,2	21,0	21,0	33,5	32,8	19,5	27,9	7,6
Recepción de productos desde páginas de comercio que pudieran ser falsas	6,3	13,6	12,8	30,8	20,2	28,3	28,7	42,6	**42,7**	23,4	31,4	9,5
Acceso a páginas web falsas de entidades bancarias, comercio o Administraciones	18,9	7,3	16,6	25,8	19,2	30,4	21,4	35,5	24,2	29,9	**55,5**	21,1

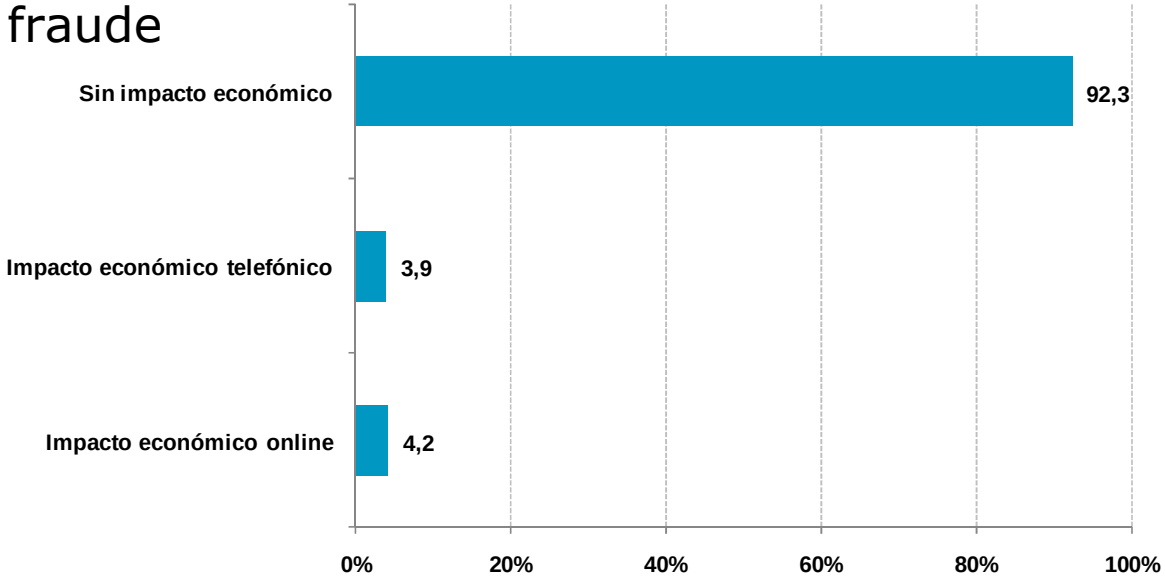
El phishing es la estafa más utilizada en Internet que consiste en la creación y distribución de una página web similar a la de una entidad bancaria cuyo fin es la obtención de claves de usuario.

[5] Ver nota al pie número 4

BASE: Usuarios que han sufrido cada tipo concreto de intento de fraude

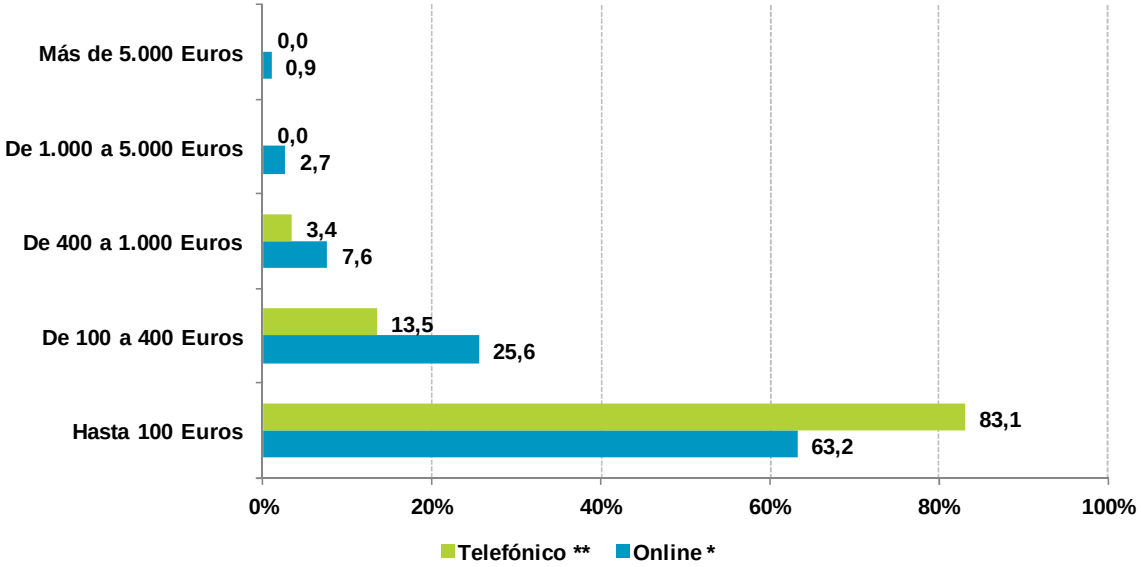
Impacto económico del fraude

Un pequeño porcentaje (alrededor del **4%**) de los intentos de fraude acaban logrando su objetivo y suponen un **impacto económico** para la víctima.



BASE: Usuarios que han sufrido un intento de fraude

Distribución del impacto económico del fraude



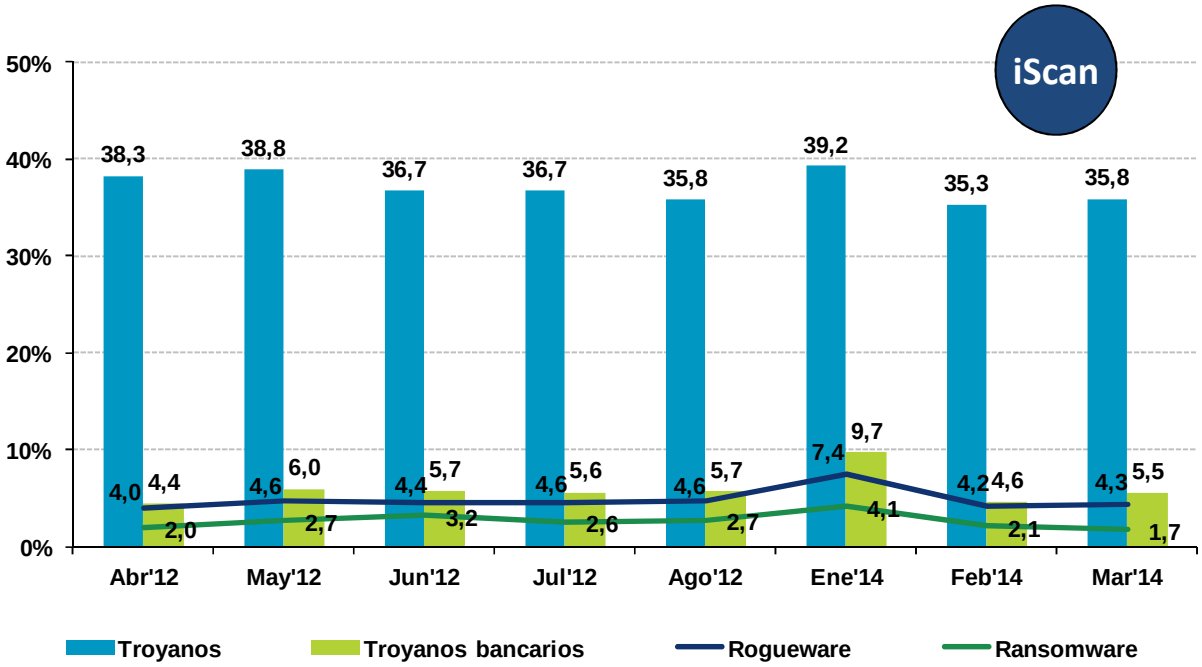
* BASE: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online

** BASE: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude telefónico

Fraude y malware

Los **troyanos bancarios** representan el **5,5%** de las infecciones registradas por iScan en los equipos analizados en el mes de marzo.

Evolución de equipos que alojan troyanos bancarios y rogueware



Tipología del malware analizado

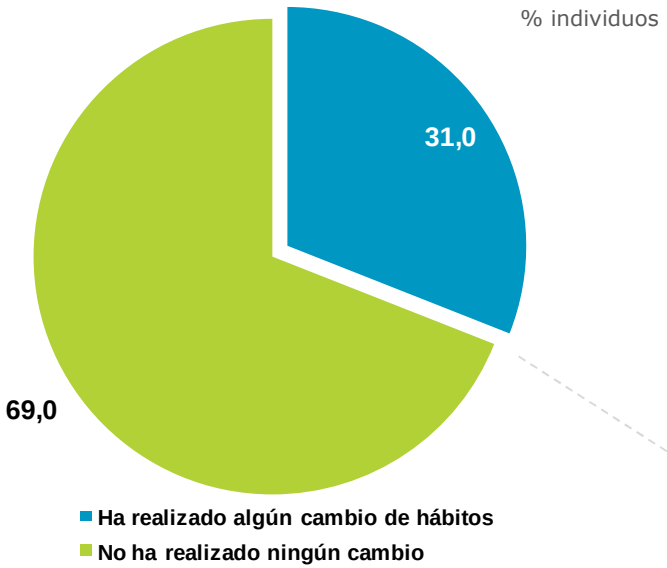
✓ Troyano bancario:
malware que roba información confidencial a los clientes de banca y/o plataformas de pago online.

✓ Rogueware o rogue:
malware que hace creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto del pago suele ser la compra de un falso antivirus, que resulta ser en realidad el malware en sí.

✓ Ransomware:
malware que se instala en el sistema tomándolo como "rehén" y pidiendo al usuario una cantidad monetaria a modo de rescate (*ransom* en inglés) a cambio de una supuesta desinfección.

BASE: Total equipos

Cambios adoptados tras un incidente de seguridad



BASE: Total usuarios

Cambios realizados:

Respuesta múltiple

BASE: Usuarios que realizan algún cambio

Cambios adoptados tras un incidente de seguridad

Cambios en los hábitos y medidas de seguridad según el tipo de incidencia

De manera general, la mayoría de usuarios modifica sus hábitos y medidas de seguridad tras una incidencia de **intrusión Wi-Fi**.

El **cambio de contraseñas** se lleva a cabo principalmente (**49,7%**) ante incidencias de tipo **suplantación de identidad**.

Cambio en los hábitos	Incidencia (%)					
	Malware	Pérdida de archivos o datos	Servicios inaccesibles debido a ciberataques	Recepción de spam	Suplantación de identidad	Intrusión Wi-Fi
Cambiar contraseñas	28,4	26,4	38,1	24,6	**49,7**	47,3
Actualizar herramientas	29,6	22,2	**30,4**	17,9	26,8	**30,4**
Realizar copias de seguridad	12,1	20,1	16,3	8,2	17,0	**25,9**
Cambiar herramientas	14,1	18,0	16,1	7,0	14,5	**21,1**
Abandonar software no autorizado	7,9	13,7	13,8	4,8	25,1	**27,9**
Instalar herramientas por 1ª vez	8,1	16,4	7,8	4,1	18,1	**19,2**

BASE: Usuarios que han sufrido cada una de los incidentes de seguridad

Cambios en el uso de servicios de Internet según el tipo de incidencia

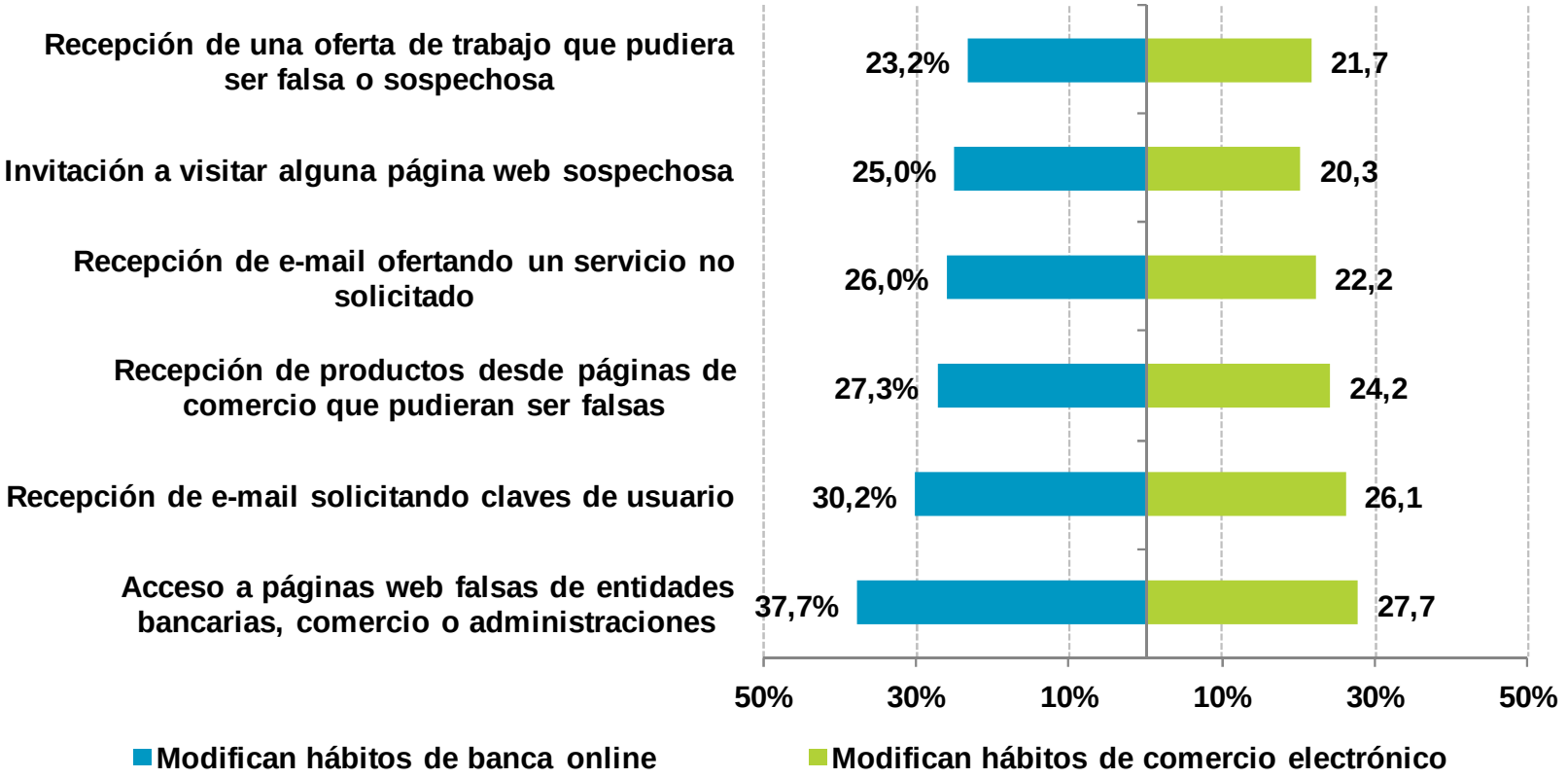
Tras una incidencia de **pérdida de archivos o datos,** el **21,1%** de usuarios abandona las **descargas desde Internet**, mientras el **16,7%** deja de usar el servicio de **banca online** después una **suplantación de identidad**.

Cambio en el uso de servicios	Incidencia (%)					
	Malware	Pérdida de archivos o datos	Servicios inaccesibles debido a ciberataques	Recepción de spam	Suplantación de identidad	Intrusión Wi-Fi
Abandonar descargas	12,7	**21,1**	14,8	8,2	17,2	19,0
Abandonar el comercio electrónico	3,5	8,8	6,7	2,4	10,4	**14,0**
Abandonar la banca online	3,8	8,8	6,4	2,6	**16,7**	11,4
Dejar de usar servicios de Internet	1,9	7,3	4,0	1,2	9,6	**16,2**

BASE: Usuarios que han sufrido cada una de los incidentes de seguridad

Influencia del intento de fraude en los servicios de banca online y comercio electrónico

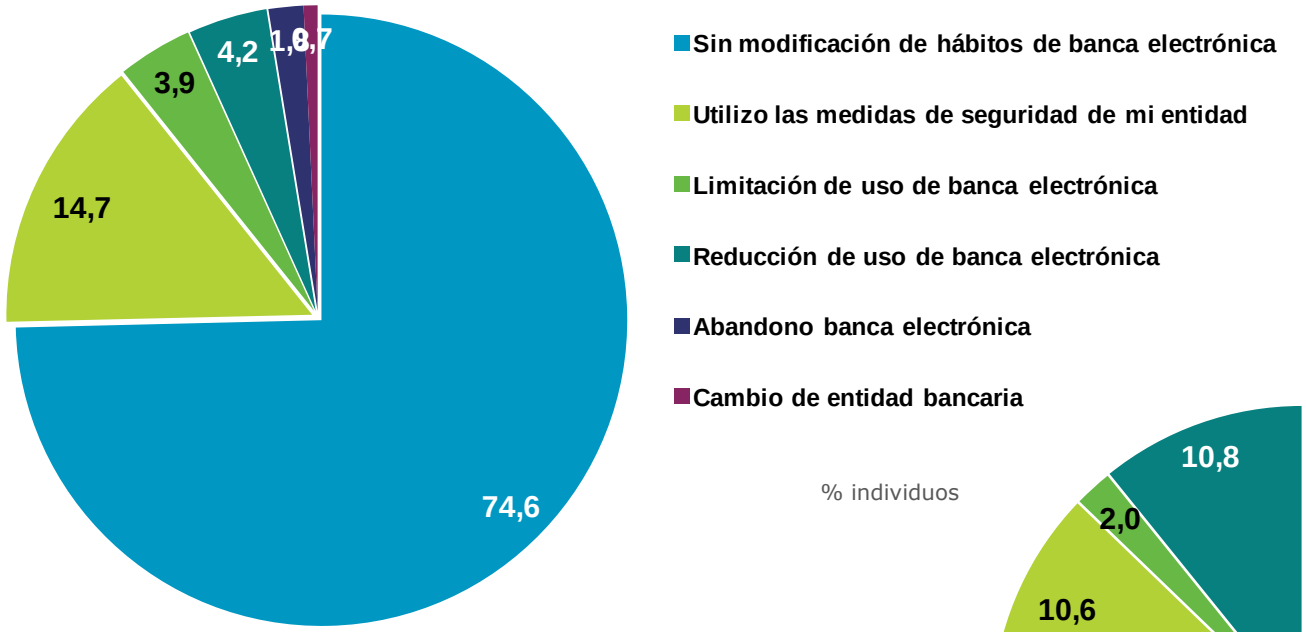
La **principal causa de modificación de hábitos** por parte del **37,7%** de usuarios del servicio de banca online y del **27,7%** de comercio electrónico es la recepción de peticiones de **acceso a páginas web falsas de este tipo de entidades**.



BASE: Usuarios que han sufrido un intento de fraude

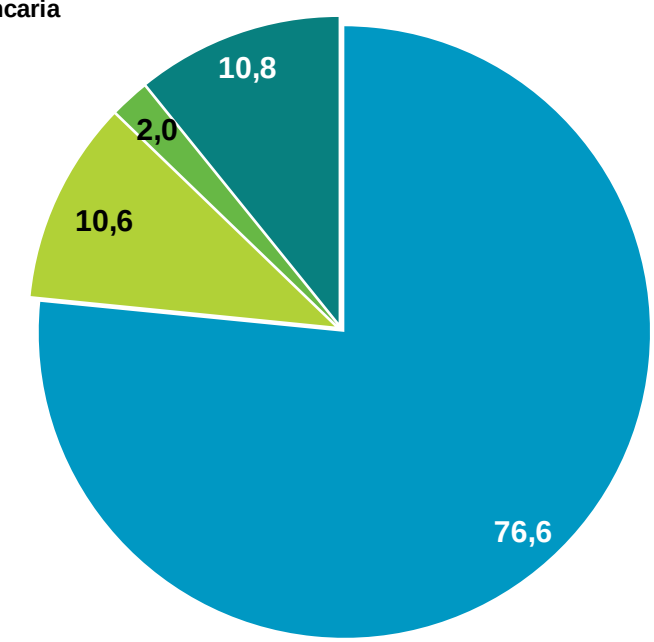
Cambios adoptados tras un incidente de seguridad

Modificación de hábitos prudentes relacionados con la banca online y comercio electrónico tras sufrir un intento de fraude



% individuos

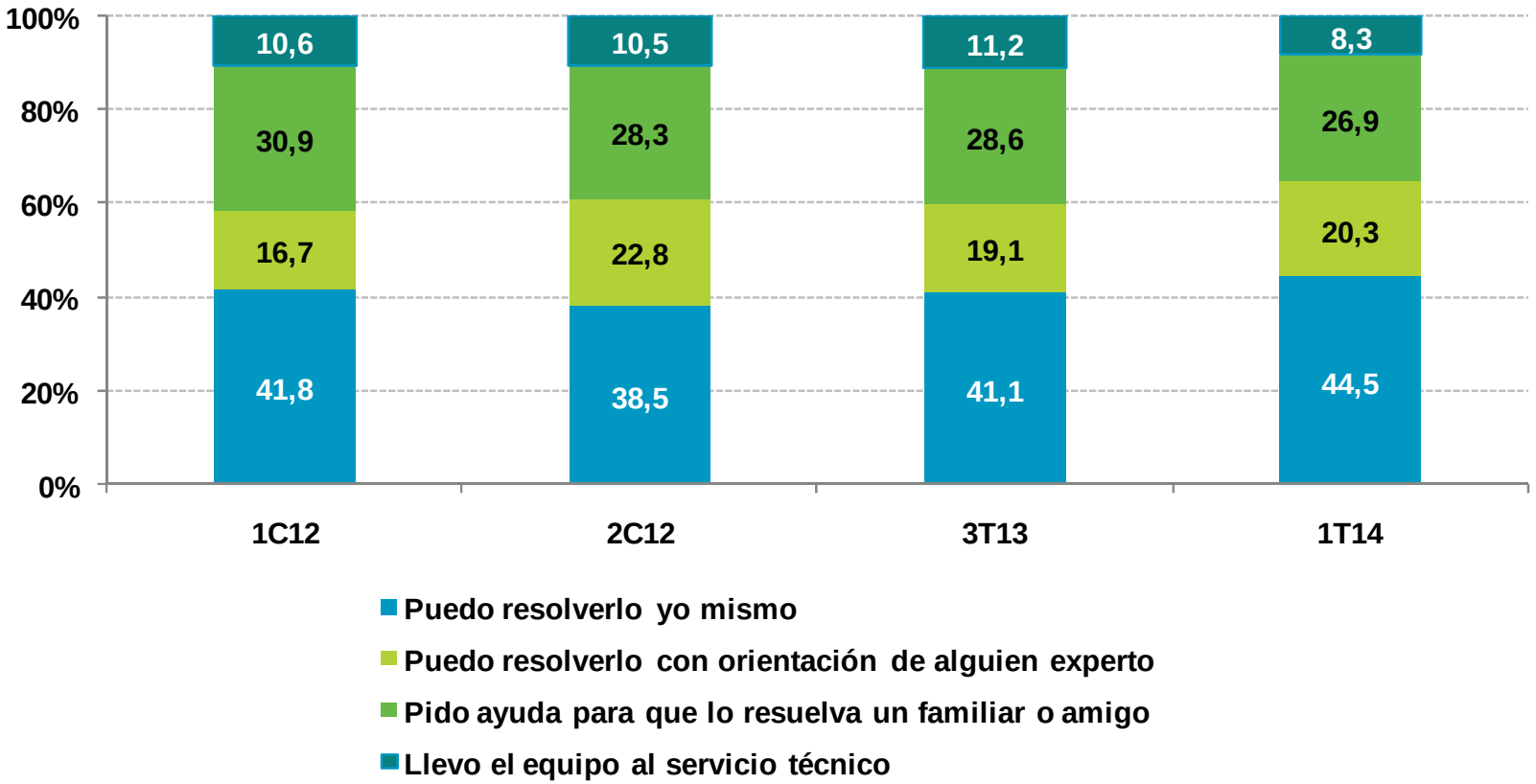
BASE: Usuarios que usan banca online y han sufrido un intento de fraude



BASE: Usuarios que usan comercio electrónico y han sufrido un intento de fraude

Resolución de incidentes de seguridad

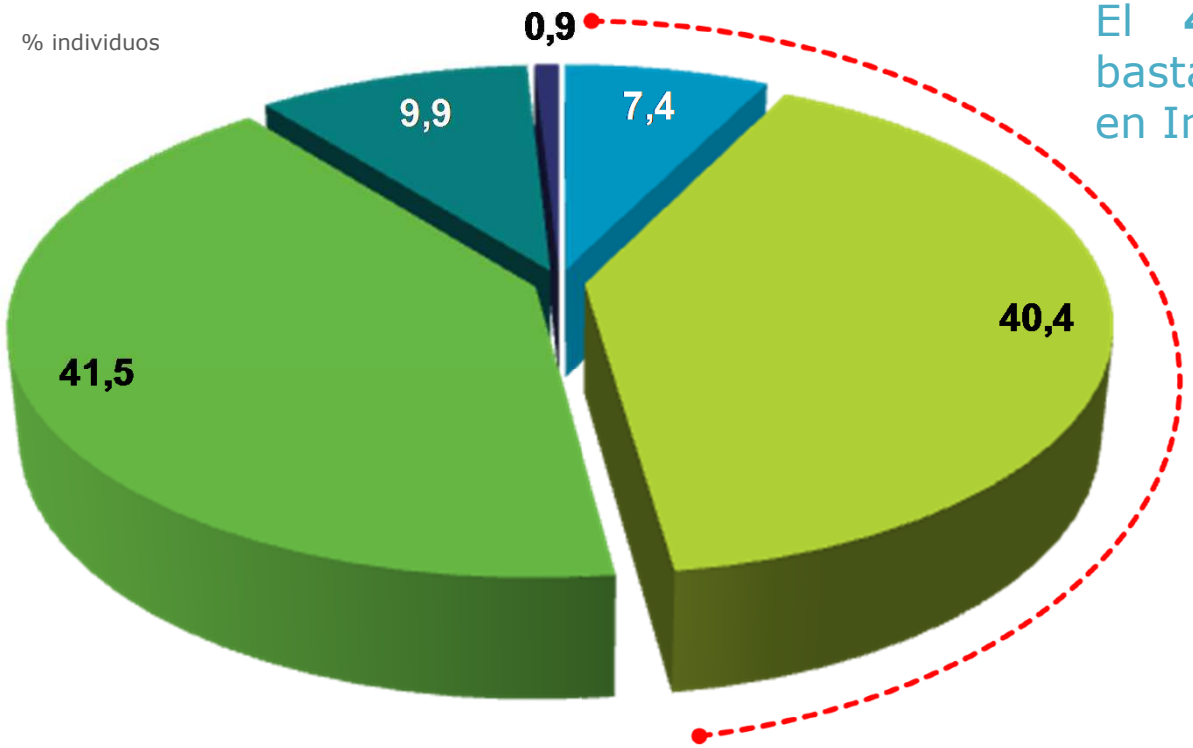
El **44,5%** de los internautas españoles declaran ser capaces de solucionar **ellos mismos** los problemas de seguridad, y otro **20,3%** también lo logra con la **orientación de un experto**.



BASE: Total usuarios

1. e-Confianza y limitaciones en la Sociedad de la Información
2. Percepción de los usuarios sobre la evolución en seguridad
3. Responsabilidad en la seguridad de Internet

Nivel de confianza en Internet



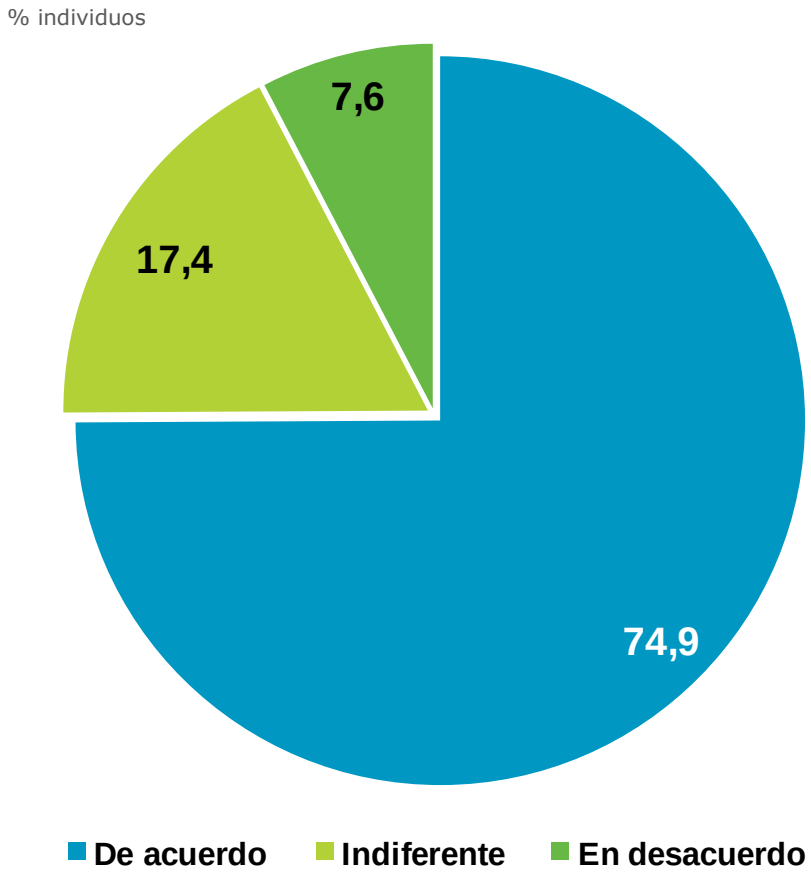
El **47,8%** **confía** bastante o mucho en Internet.

6

Menos de un **1%** de la población española **desconfía** de la red.

BASE: Total usuarios

Valoración del ordenador personal como razonablemente protegido

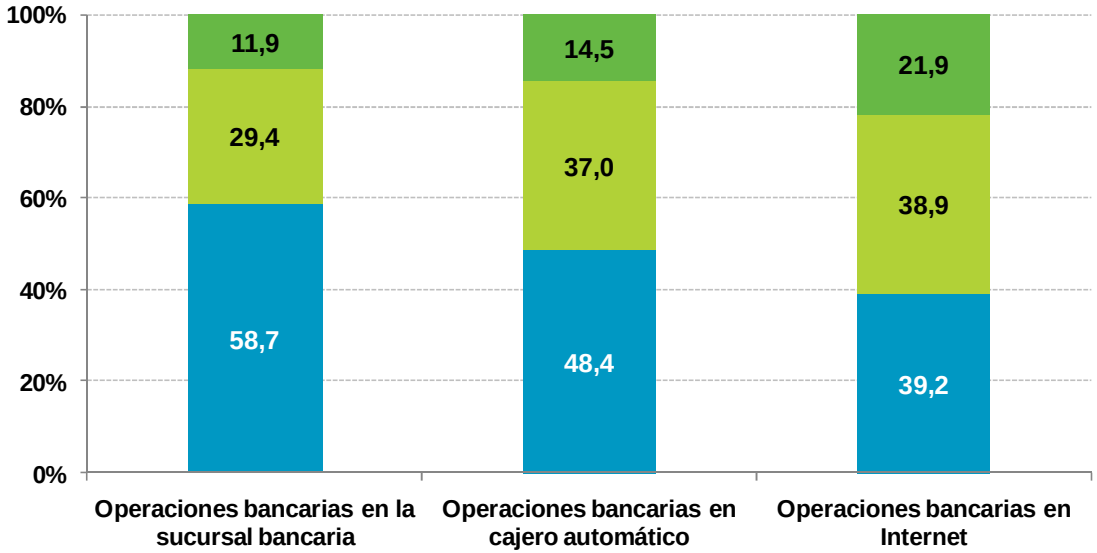


Tres cuartas partes de la población (**74,9%**) declaran considerar su **ordenador personal razonablemente protegido** frente a las potenciales amenazas de la red de redes.
El **7,6%** se muestra precavido al **discrepar** ante tal afirmación.

6

BASE: Total usuarios

Confianza online vs. confianza offline



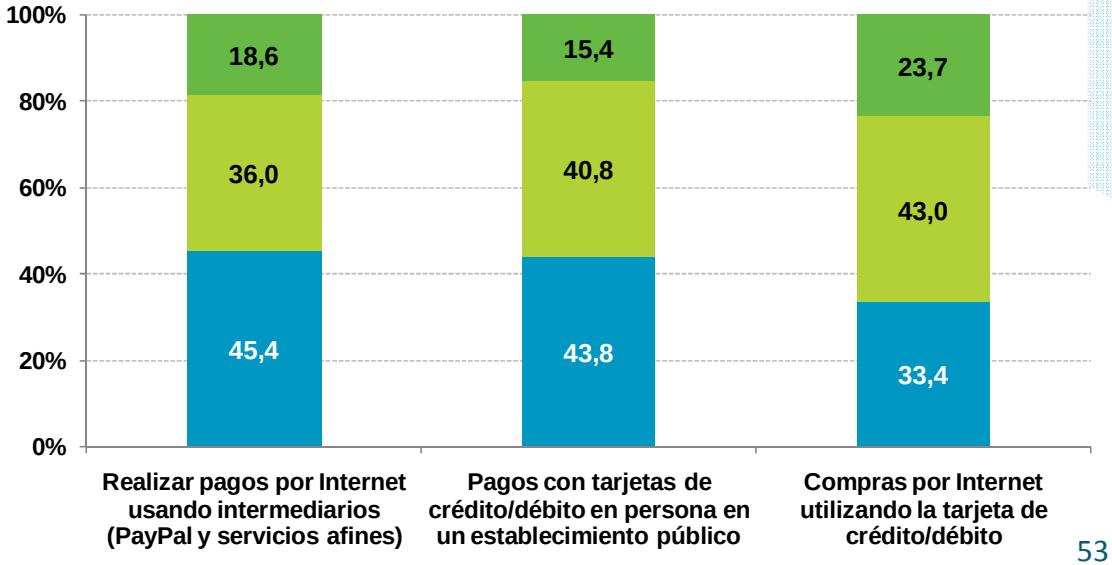
Nivel de confianza en operaciones bancarias

El usuario confía más en las **operaciones** mediante el trato con la persona **en la entidad bancaria** (**58,7%**) que en aquellas realizadas a través de un **cajero automático** (**48,4%**) o **por Internet** (**39,2%**).

% individuos

Nivel de confianza en operaciones de compra-venta

Sin embargo, para **operaciones de compra-venta**, la mayoría se decanta por utilizar un intermediario como **PayPal y servicios afines** (**45,4%**) para realizar pagos a través de Internet frente a la **tarjeta de crédito/débito** (**33,4%**), incluso en establecimiento público (**43,8%**).

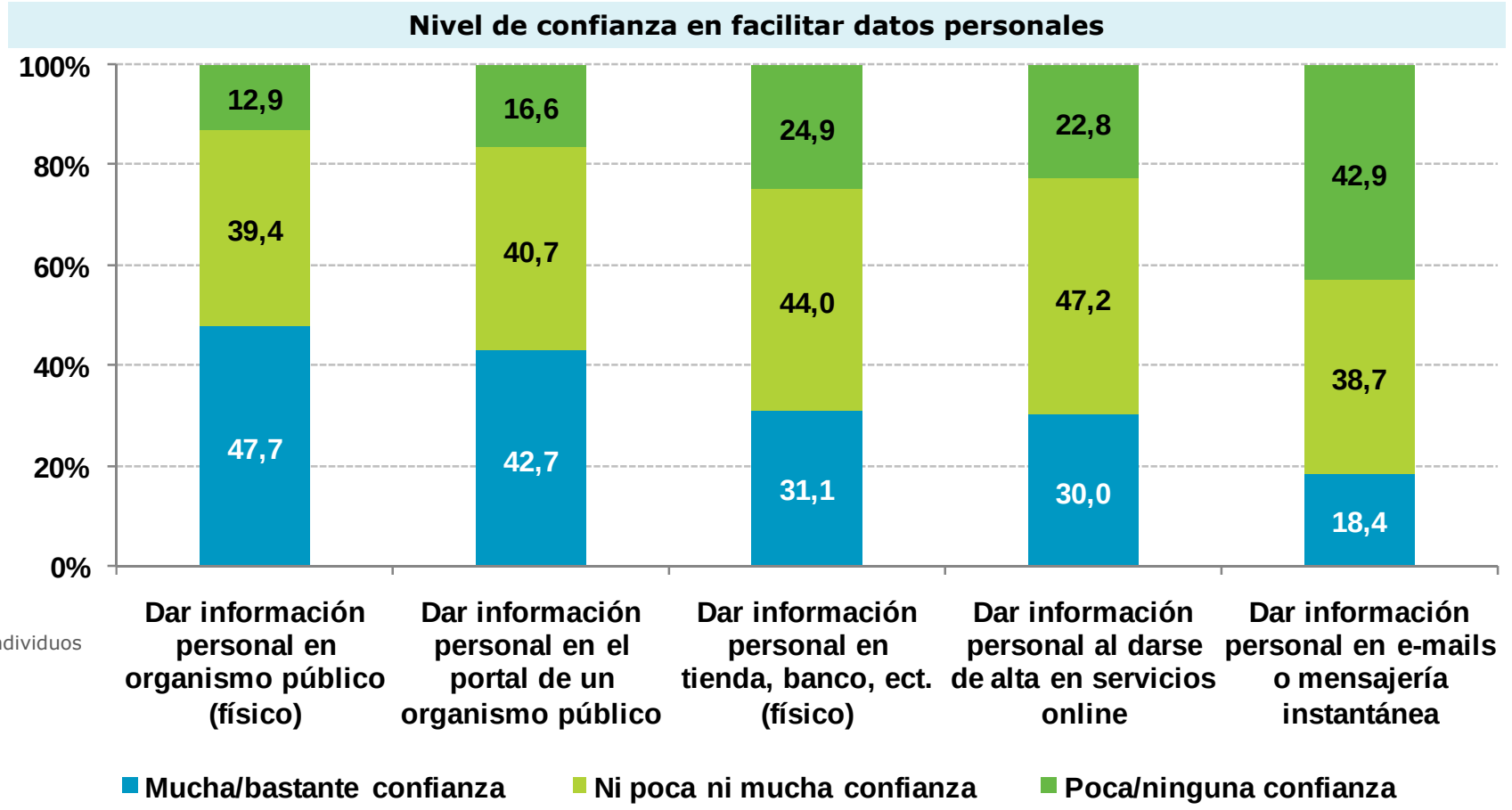


- Mucha/bastante confianza
- Ni poca ni mucha confianza
- Poca/ninguna confianza

BASE: Total usuarios

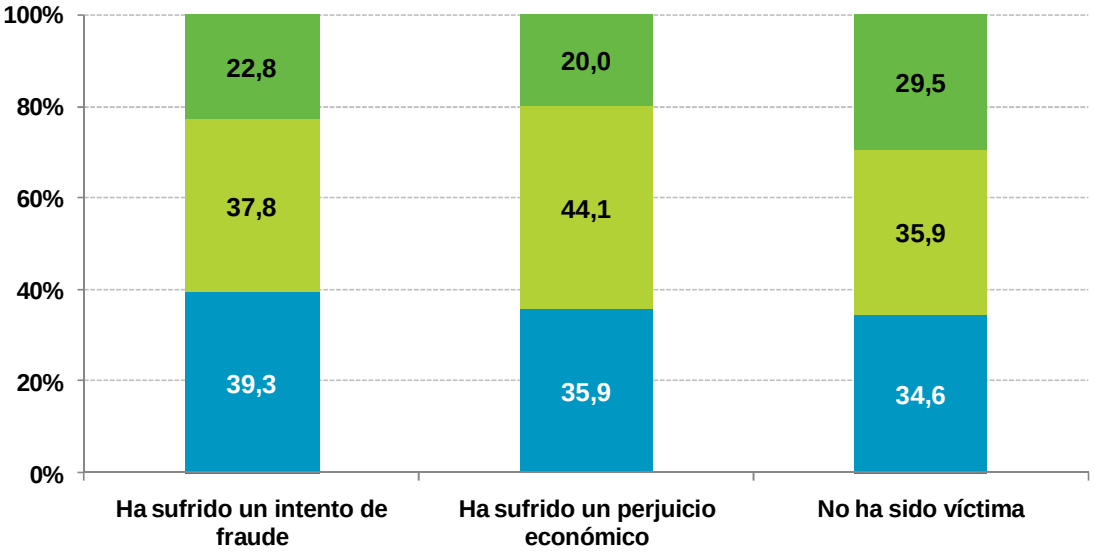
Confianza online vs. confianza offline

Un **18,4%** de la población declara tener suficiente confianza para **facilitar información** de carácter personal a través de **correo electrónico, chat o mensajería instantánea**.



BASE: Total usuarios

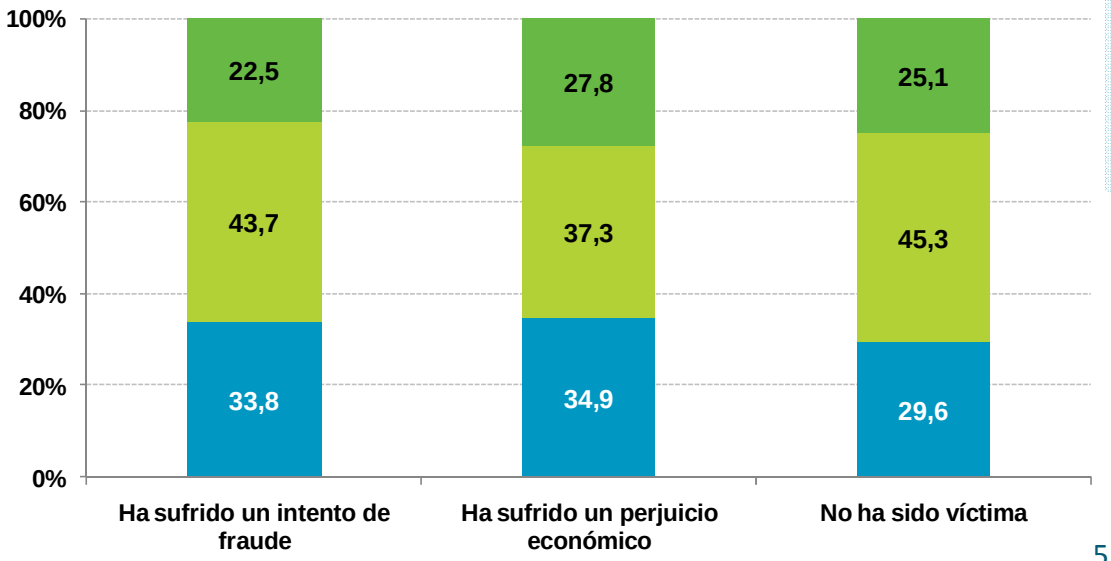
Confianza vs. fraude



Confianza al realizar operaciones bancarias en Internet

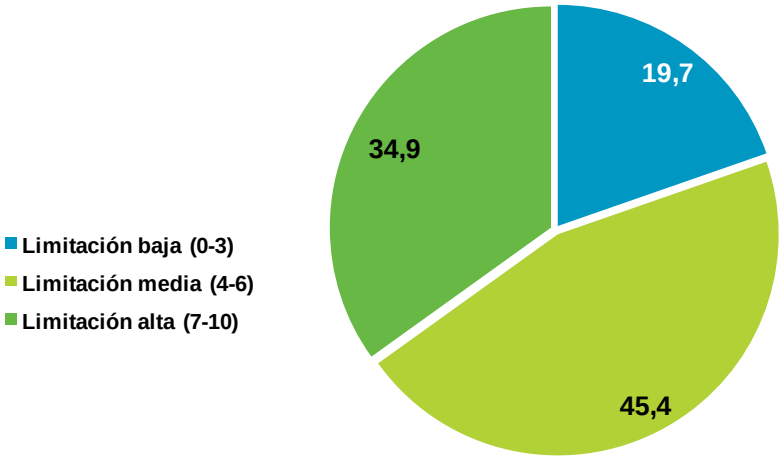
% individuos

Confianza al realizar compras por Internet utilizando la tarjeta de crédito/débito



BASE: Usuarios de banca online o comercio electrónico

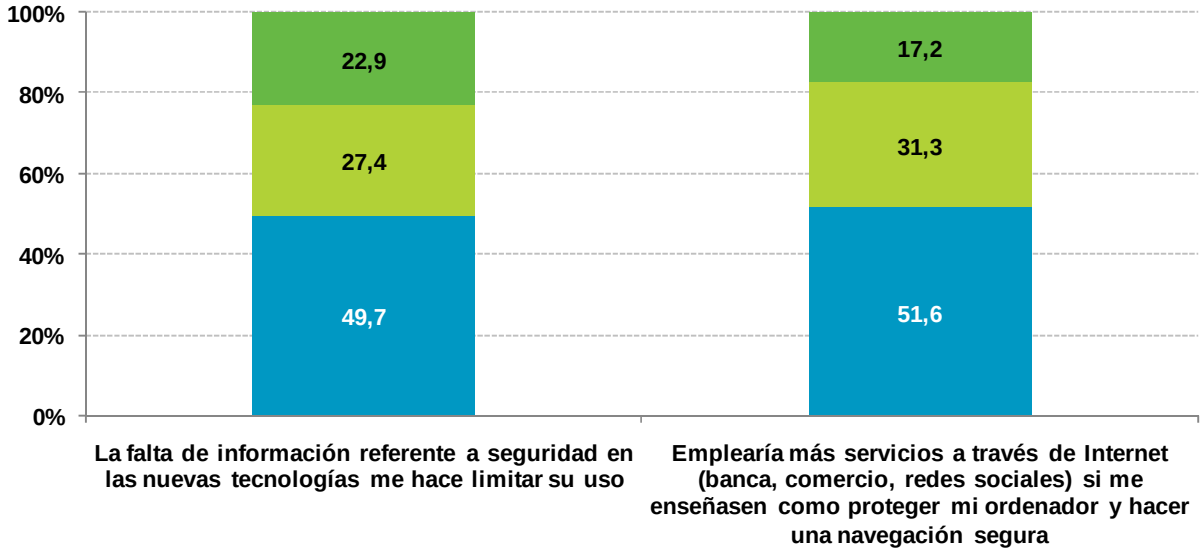
Limitación a causa de problemas de seguridad



Seguridad como factor limitante en la utilización de nuevos servicios

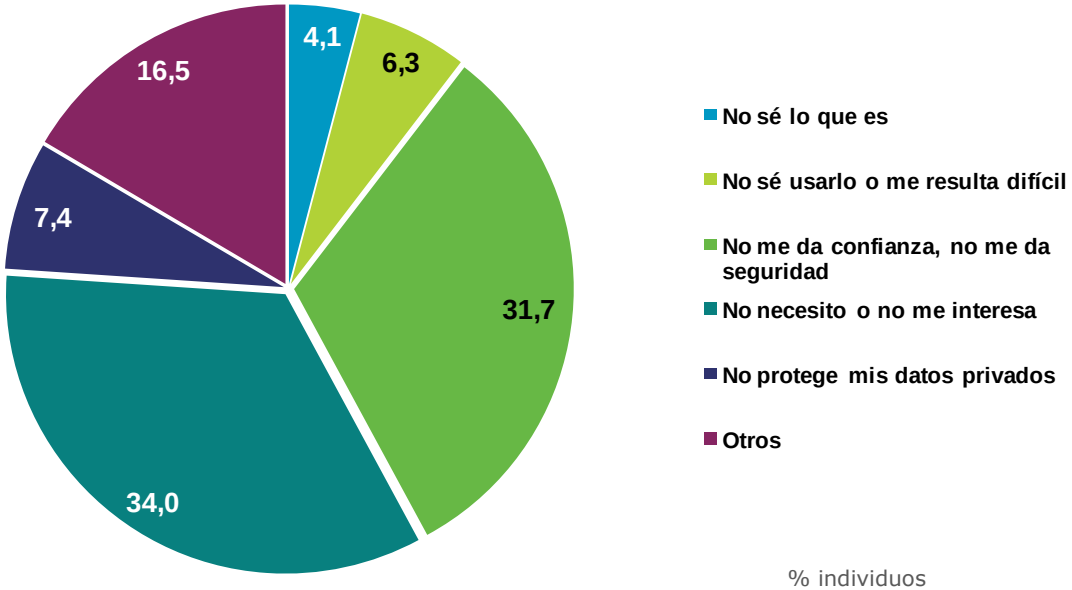
% individuos

Limitaciones en el uso de Internet



BASE: Total usuarios

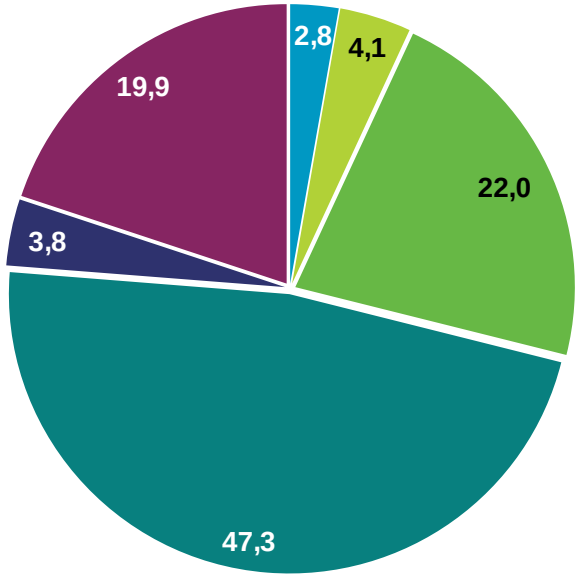
Razones para no utilizar banca online



% individuos

La **falta de necesidad y/o interés** es el **principal motivo** que alegan los usuarios para no utilizar los servicios de banca online (**34%**) y comercio electrónico (**47,3%**).

Razones para no utilizar comercio electrónico

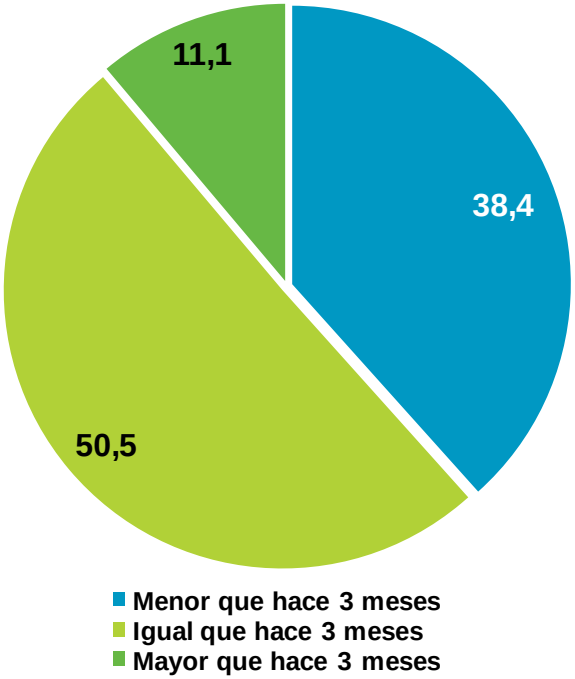


Como **segundo motivo** se encuentra la **falta de confianza en estos servicios**: el **31,7%** y **22%** para el servicio de banca online y comercio electrónico respectivamente.

BASE : Usuarios que no utilizan el servicio

Percepción de los usuarios sobre la evolución en seguridad

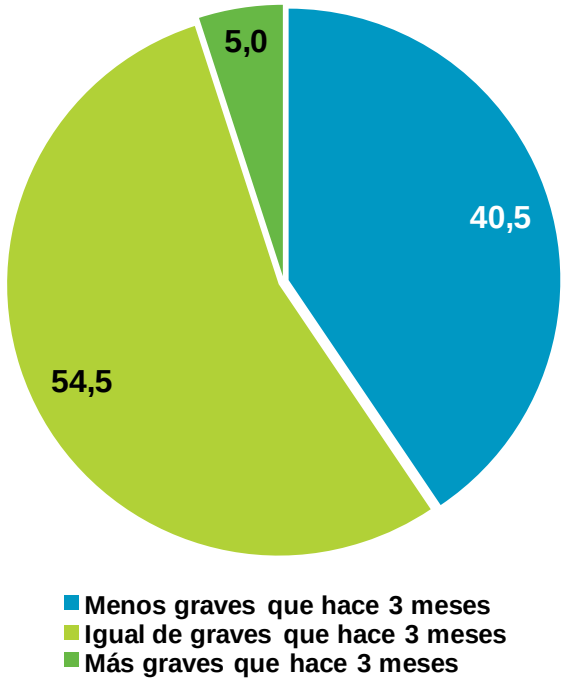
Número de incidencias



La percepción de los encuestados sobre las incidencias acontecidas respecto a meses anteriores es que son similares **en cuanto a cantidad (50,2%) y** menores **en cuanto a gravedad (40,5%).**

Gravedad de las incidencias

% individuos

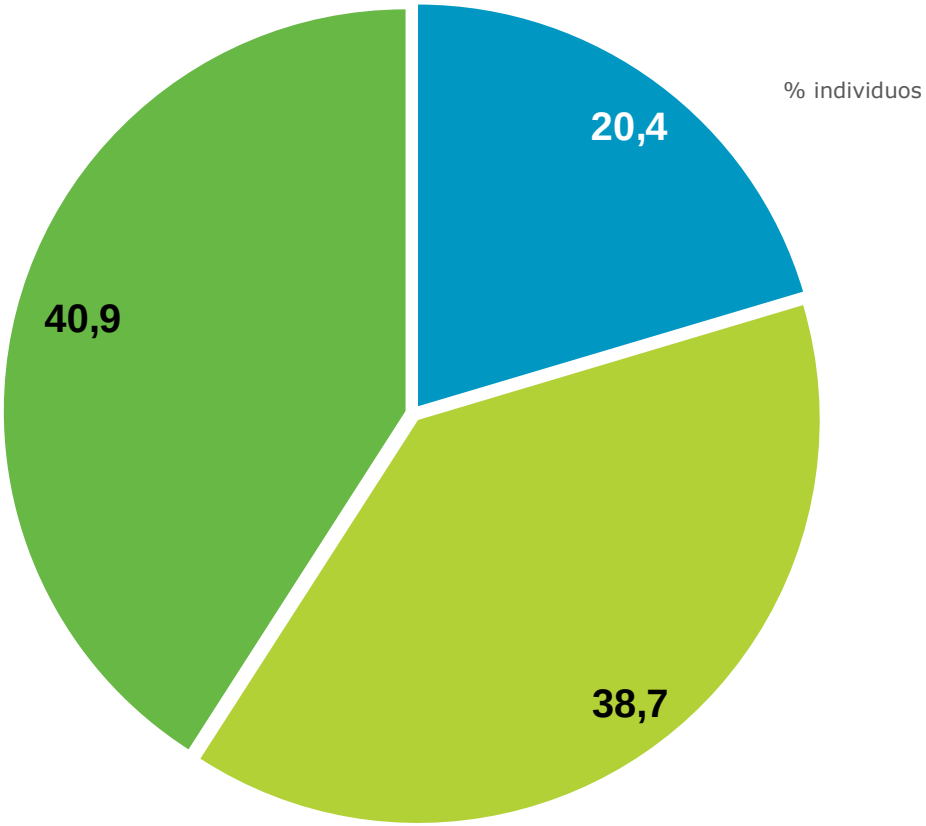


BASE: Total usuarios

6

Percepción de riesgos en Internet

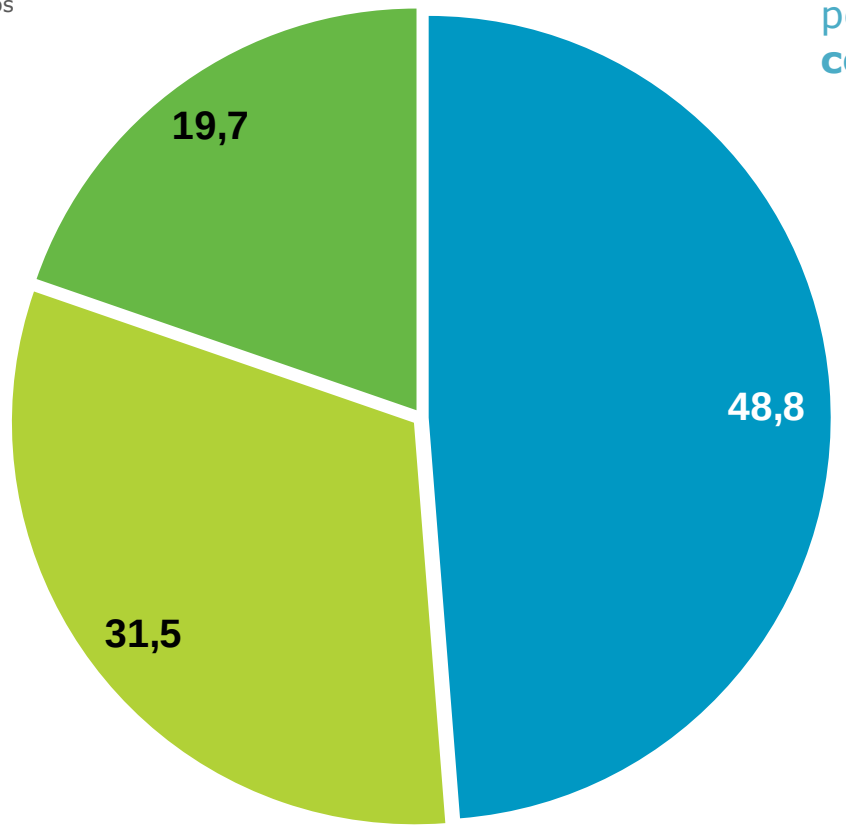
El **robo y uso de información personal** (nombre, dirección, fotografías, etc.) sin el consentimiento del usuario así como el **perjuicio económico** derivado de un fraude, son los principales riesgos en Internet percibidos por los internautas (**40,9%** y **38,7%** respectivamente).



BASE: Total usuarios

Valoración de Internet cada día como más seguro

% individuos



Prácticamente la mitad de los internautas españoles (**48,8%**) perciben **Internet cada día como más seguro**.

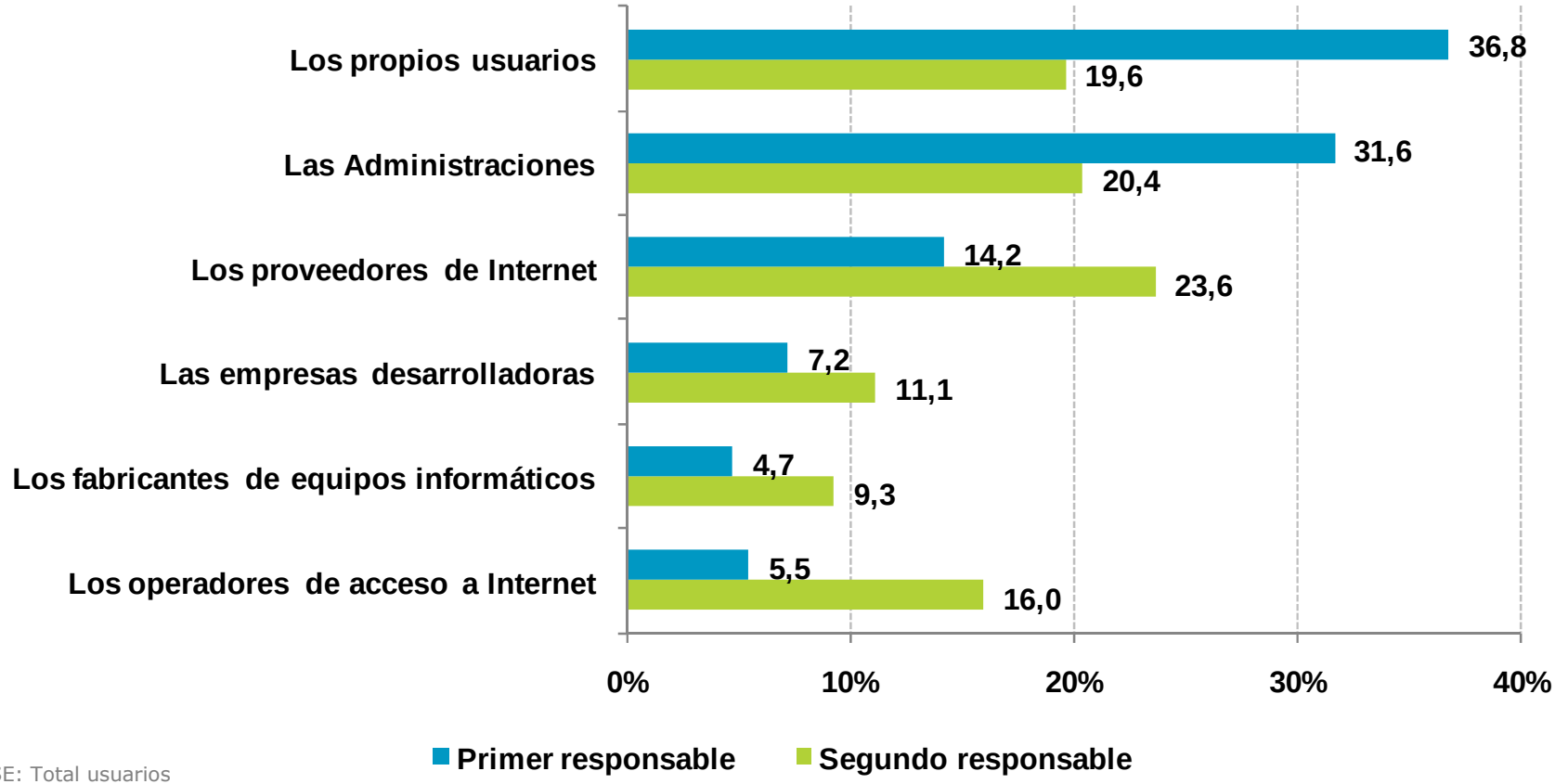
6

BASE: Total usuarios

Responsabilidad en la seguridad de Internet

Más de un tercio (**36,8%**) de los panelistas asumen la responsabilidad de sus acciones considerando que son **los propios usuarios** los principales responsables de la seguridad en Internet.

En opinión del **31,6%**, esta responsabilidad recae principalmente sobre las **Administraciones**.

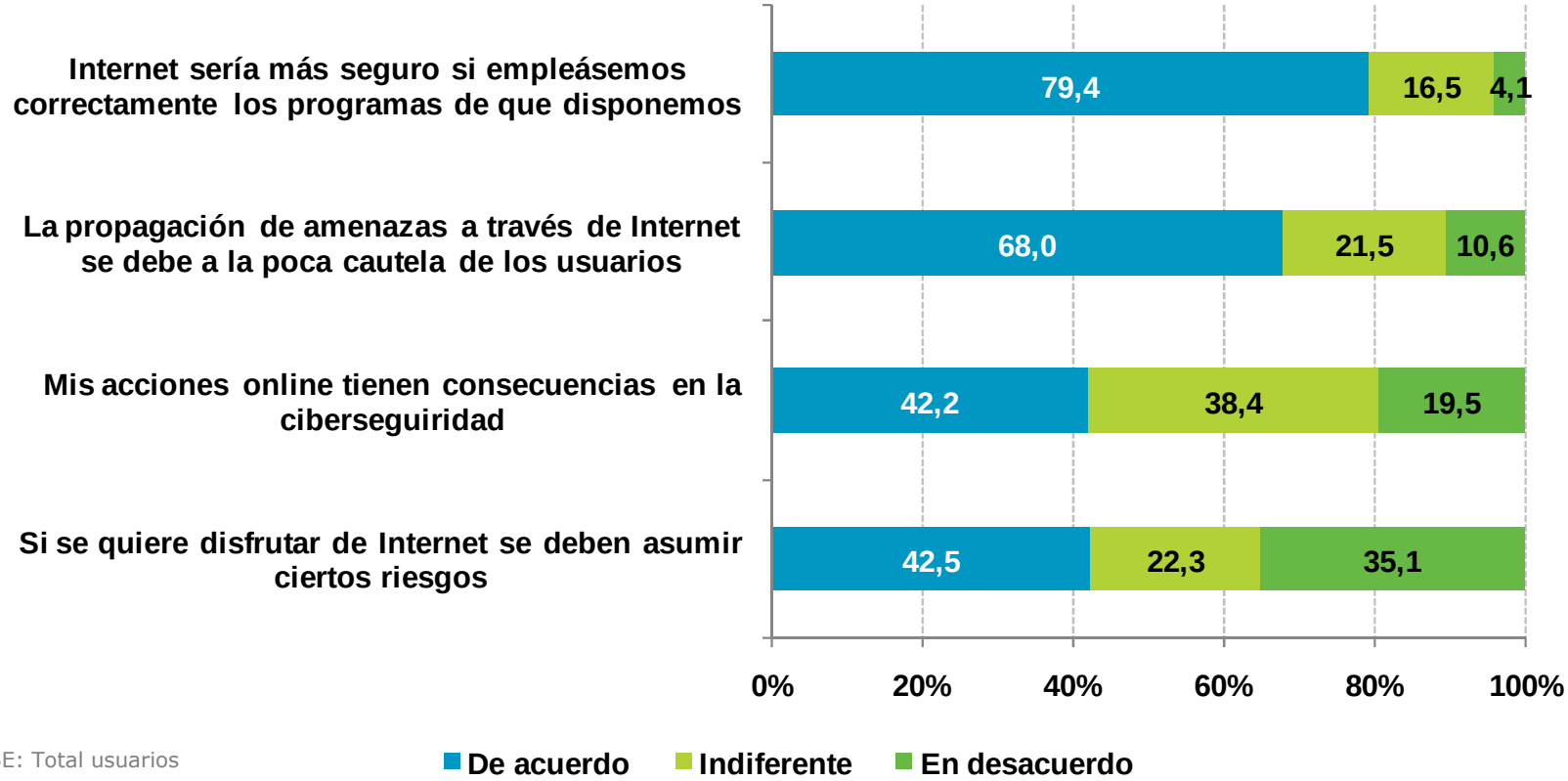


BASE: Total usuarios

Rol del usuario

Casi un **80%** de usuarios consideran que Internet sería más seguro **si se empleasen correctamente los programas de seguridad** y aproximadamente un **70%** opinan que la propagación de amenazas a través de Internet se debe principalmente a la **poca cautela de los usuarios**.

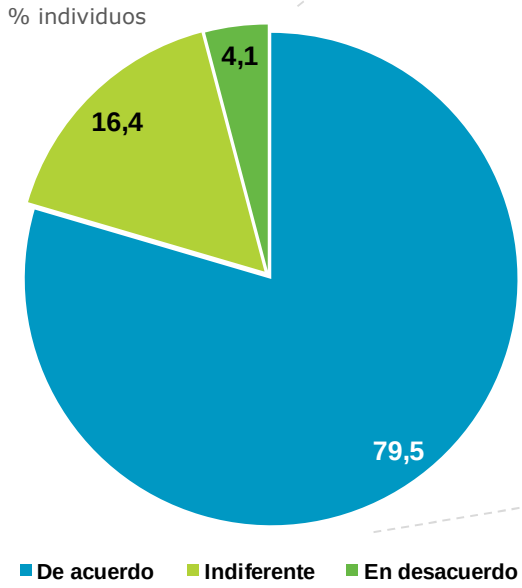
El **42,2%** de usuarios creen que sus acciones online tienen **consecuencias en la seguridad**, y otro **42,5%** opinan que se deben **asumir riesgos** para disfrutar de Internet.



BASE: Total usuarios

Responsabilidad en la seguridad de Internet

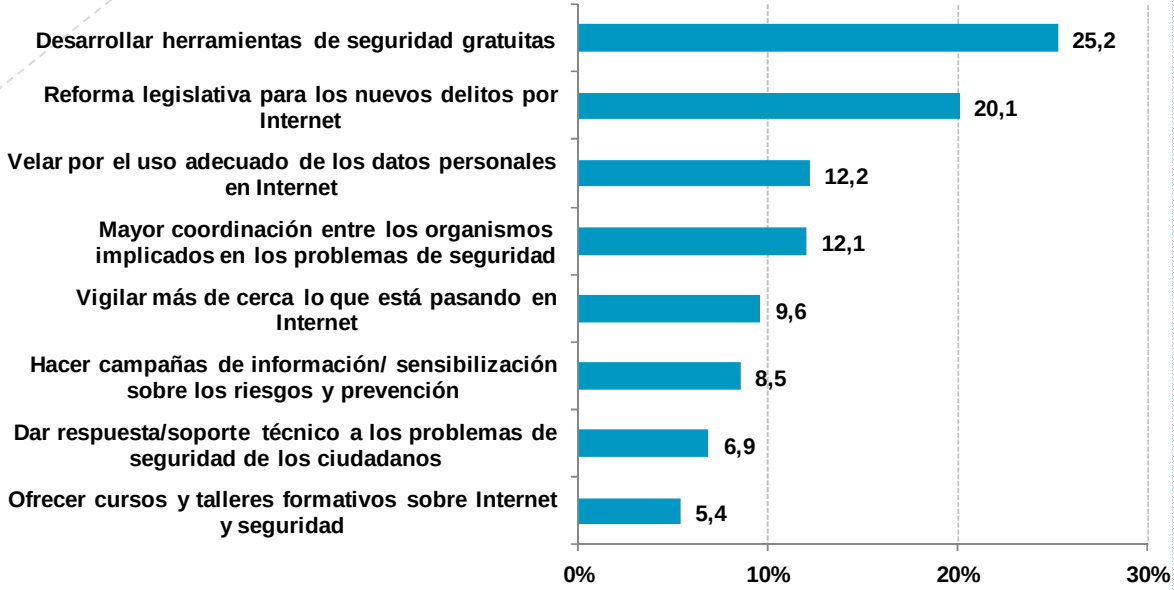
Papel de la Administración en la garantía de la seguridad de la información de los ciudadanos



BASE: Total usuarios

Medidas prioritarias a tomar por la Administración

Respuesta múltiple



BASE: Usuarios que están de acuerdo o totalmente de acuerdo con que la Administración debe de implicarse más

6

MEDIDAS DE SEGURIDAD

Las medidas de seguridad más aplicadas según la lectura real son los programas antivirus (80,6%) y los cortafuegos (77,1%). En estos últimos, el nivel declarado es menor que el real en más de 36 puntos porcentuales.

Mientras que con Windows XP el uso de las cuentas de administrador es prácticamente del 100%, en sistemas posteriores se reduce su uso siendo de 25,9% en Windows 7, 16,4% en Windows Vista y llegando a un mínimo del 5,9% en el caso de Windows 8. Esto se debe a la configuración por defecto de las distintas versiones. Con el fin de soporte de Windows XP y la presumible migración de usuarios a sistemas más actuales se consigue dar la vuelta al uso de esta medida de seguridad.

Aunque solo el 12,4% de los panelistas no protege su red Wi-Fi o desconoce su grado de protección, el porcentaje de personas que no se implican en la protección de su red inalámbrica aumenta casi al 50% si añadimos aquellos que usan el estándar WEP (10,8%), obsoleto y fácilmente eludible, o desconocen la tecnología que usan (26,7%).

HÁBITOS DE COMPORTAMIENTO EN LA NAVEGACIÓN Y USOS DE INTERNET

En el ámbito de la banca en línea y comercio electrónico, la mayoría de panelistas, siempre en un porcentaje superior al 73%, sigue buenas prácticas. Sólo el uso de tarjetas monedero/prepago es utilizado por un número menor de usuarios (41%), aunque su popularidad aumenta desde periodos anteriores.

También el uso seguro de redes P2P es una norma entre los panelistas. Solo el 12,9% de los usuarios de estas redes comparte todos sus archivos y el 11,8% no tiene control sobre lo que comparte. Sin embargo, tres de cada cinco (61%) panelistas analiza todo fichero descargado mediante esta tecnología con un software antivirus.

En cuanto al uso de los smartphones, solo un 2,4% de los usuarios que disponen de ellos tienen comportamientos inseguros y descargan aplicaciones desde repositorios no oficiales.

Conclusiones

INCIDENTES DE SEGURIDAD

La incidencia más comúnmente sufrida ha sido de lejos el spam, que ha afectado casi al 85% de aquellas victimas de algún incidente, mientras que aquellas relacionadas con virus y malware son declaradas únicamente por un 32,8%. Sin embargo, el impacto real del malware en los sistemas de los panelistas está 37 puntos porcentuales por encima del impacto declarado: casi en el 60% de equipos informáticos. En otras palabras, de cada 5 usuarios 3 son victimas de algún tipo de malware, y solo 1 de ellos es consciente. Esta brecha sigue una tendencia ascendente en los últimos periodos, que indica que el malware se oculta cada vez mejor ante el usuario y los programas antivirus.

Además, se comprueba que aunque los equipos totalmente actualizados están menos expuestos al malware (55,1%) que aquellos que no tienen aplicadas las actualizaciones (62,1%), la diferencia de infección no es excesiva, solo 7 puntos porcentuales por debajo. A pesar de el número de usuarios que potencialmente tiene su red inalámbrica expuesta, solo el 2,4% sospecha haber sufrido una intrusión en su red.

CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

La mitad de los encuestados declara haber sufrido alguna vez un intento de fraude online. Este fraude se presenta en forma de: páginas de loterías, casinos y juegos online en el 31,5% de los casos y en el 29,1% en forma de páginas de comercio electrónico. Los objetivos en el impacto económico del fraude persiguen cifras bajas para evitar la consideración de delito según el código penal. Así el 63,2% de los fraudes online y el 83,1% de los telefónicos estafaron menos de 100 euros, y entre 100 y 400 euros en el 25,6% y 13,5% de las ocasiones, respectivamente.

Entre los usuarios que han sufrido un intento de fraude, casi un tercio (31%) modifica sus hábitos, siendo el cambio de contraseñas y la actualización de las herramientas ya instaladas las medidas más populares. Las incidencias que en general promueven a los usuarios a cambiar son la intrusión Wi-Fi y la suplantación de identidad. El spam, incidencia más extendida entre los fraude online, es la que menos empuja a los usuarios a cambiar su comportamiento en la red.

Una mayoría de usuarios de banca online que han sufrido un intento de fraude (74,6%) no cambia su comportamiento respecto a la banca. En cuanto al comercio electrónico este porcentaje se sitúa en el 76,6% respecto a los usuarios que usan comercio electrónico que han sufrido un intento de fraude.

El 44,5% piensa que puede resolver ellos mismos los problemas de seguridad que puedan surgir.

CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

En cuanto al nivel de confianza en Internet entre los panelistas, el 47,8% que tiene mucha o bastante confianza en Internet, y prácticamente la mitad (48,8%) valora la Red como cada día más segura. Además, tres cuartas partes de los usuarios (74,9%) piensa que su equipo está razonablemente protegido.

Aun así, los usuarios son reticentes a usar directamente sus tarjetas de crédito o debito en operaciones online, y otorgan mayor confianza al trato personal o a través de intermediarios en las operaciones bancarias y de compra/venta.

El haber sido victima de un intento de fraude o incluso haber sufrido perdidas económicas no parece influir en el grado de confianza de los panelistas en la banca online o comercio electrónico, aunque sí se aprecia una ligera tendencia a no ser victimas de fraude en aquellos que confían menos.

En cuanto al papel de la administración en la seguridad en la red, cuatro de cada cinco usuarios (79,5%) piensa que debería implicarse más. Entre las medidas que estos usuarios consideran que se deberían tomar destacan el desarrollo de herramientas de seguridad gratuitas (25,2%), una reforma penal que cubra los nuevos tipos de delitos informáticos (20,1%), cuidar el correcto uso de datos personales (12,2%) y mejorar la coordinación de los organismos en la respuesta a los incidentes de seguridad (12,1%).

Alcance del estudio

El "*Estudio sobre la Ciberseguridad y Confianza de los hogares españoles*" se realiza a partir de una metodología basada en el panel online dedicado y compuesto por aquellos hogares con conexión a Internet repartidos por todo el territorio nacional.

Los datos extraídos de la encuesta, realizada con una periodicidad trimestral, permiten obtener la percepción sobre la situación de la seguridad en Internet y nivel de e-confianza de los usuarios.

Ficha técnica

Universo: Usuarios españoles de Internet de más de 15 años con acceso frecuente a Internet desde el hogar (al menos una vez al mes).

Tamaño Muestral: 3.010 hogares encuestados y de ellos, 2.092 hogares encuestados y equipos escaneados.

Ámbito: Península, Baleares y Canarias.

Diseño Muestral: Para cada CC.AA., estratificación proporcional por tipo de hábitat, con cuotas de segmento social y número de personas en el hogar.

Trabajo de Campo: El trabajo de campo ha sido realizado entre febrero y marzo de 2014 mediante entrevistas online a partir de un panel de usuarios de Internet.

Error Muestral: Asumiendo criterios de muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5, y para un nivel de confianza del 95,5%, se establecen que al tamaño muestral n=3.010 le corresponde una estimación del error muestral igual a ±1,79%.

El informe del *"Estudio sobre la Ciberseguridad y Confianza de los hogares españoles"* ha sido elaborado por el siguiente equipo de trabajo del Instituto Nacional de Tecnologías de la Comunicación (INTECO) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es:

Dirección: Marcos Gómez Hidalgo
Coordinación: Elena García Díez
Dirección técnica: Héctor R. Suárez
Soporte: Equipo Contenidos e Investigación en Ciberseguridad

Dirección: Alberto Urueña López
Equipo técnico:
Raquel Castro García-Muñoz
Santiago Cadenas Villaverde

Así mismo se quiere agradecer su colaboración en la realización de este estudio a:

HISPASEC

GfK

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es