ontsi INTECO Instituto Nacional de Tecnologías de la Comunicación

# Estudio sobre la Ciberseguridad y Confianza en los hogares españoles

**Junio 2014**

# INDICE

# 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 3.074 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.

# 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 se pone en marcha automáticamente.

### 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

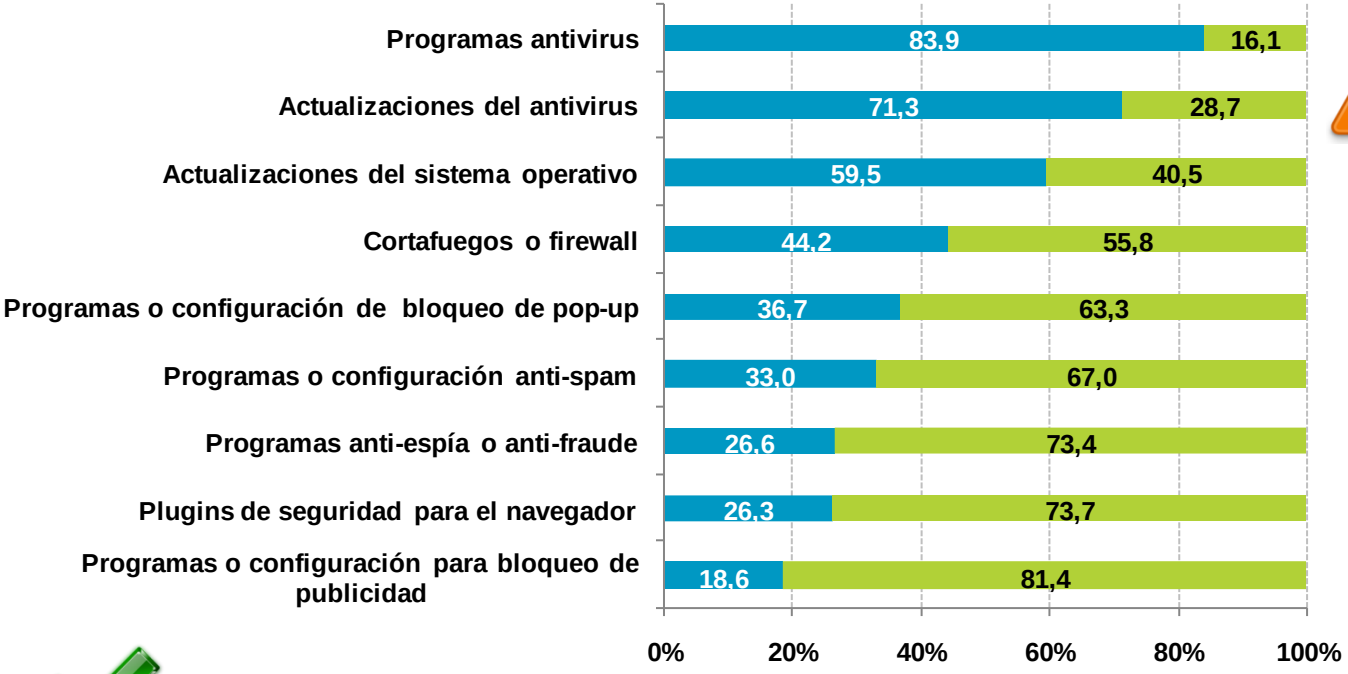
| | Medidas automatizables | Medidas no automatizables |
|---|---|---|
| Proactivas | • Cortafuegos o firewall | • Contraseñas<br>• Copias de seguridad de archivos<br>• Partición del disco duro<br>• Certificados digitales de firma electrónica<br>• Limitación de permisos vía administración del equipo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

# Uso de medidas de seguridad en el ordenador del hogar



## Medidas de seguridad automatizables[1]

A finales de 2013 la herramienta de seguridad automatizable más utilizada por los usuarios es el **software antivirus**, que alcanza casi un 84% de la población, sufriendo una reducción de **3 puntos porcentuales** en el uso declarado de por parte de los usuarios con respecto al año anterior (87% en el periodo de mayo a agosto de 2012).




BASE: Total usuarios

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**.

**Información para conocer las medidas de seguridad:** INTECO pone a disposición de los usuarios la **Oficina de Seguridad del Internauta** www.osi.es

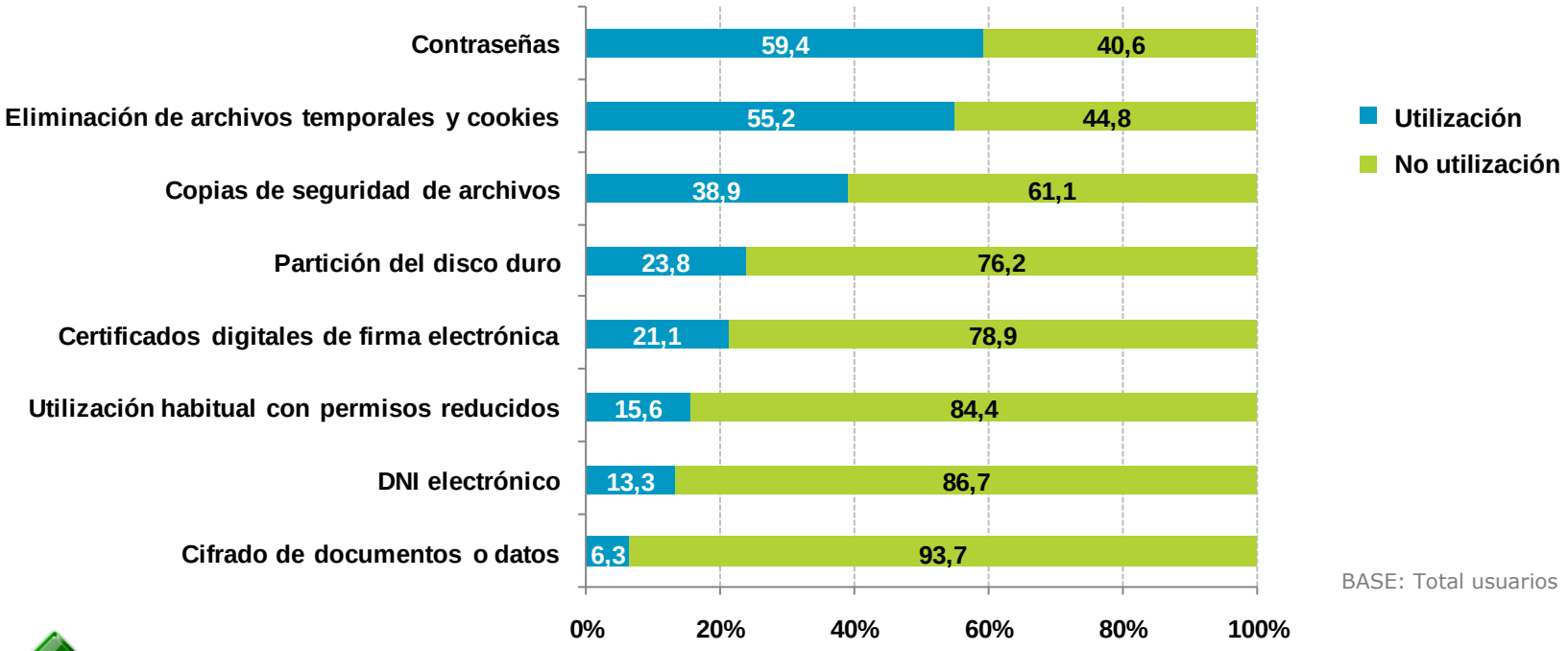
[1] Los datos referentes a las actualizaciones antivirus se presentan sobre la submuestra de usuarios que declaran utilizar antivirus (83,9%).

# Uso de medidas de seguridad en el ordenador del hogar

## Medidas de seguridad no automatizables o activas

Entre las medidas activas, las más utilizadas son las **contraseñas** (**59,4%**) y el borrado de **archivos temporales y cookies** (**55,2%**) generadas en la navegación






BASE: Total usuarios

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:

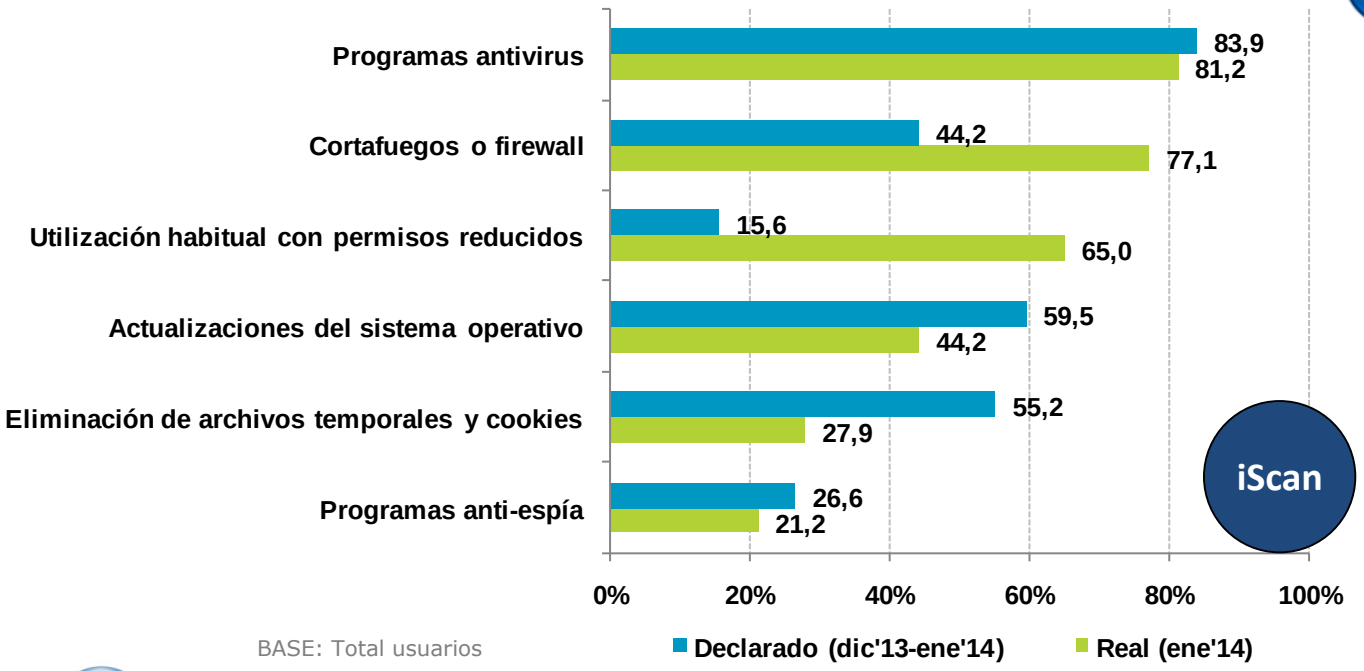
- ✓ **Contraseñas:** http://www.osi.es/contrasenas
- ✓ **Copias de seguridad:** http://www.osi.es/copias-de-seguridad-cifrado

# Uso de medidas de seguridad en el ordenador del hogar

## Uso de medidas de seguridad declarado vs. real

Un **59,5%** de panelistas declara **instalar las actualizaciones** del **sistema operativo**. Sin embargo, el dato real revela que lo hace el **44,2%**.






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.

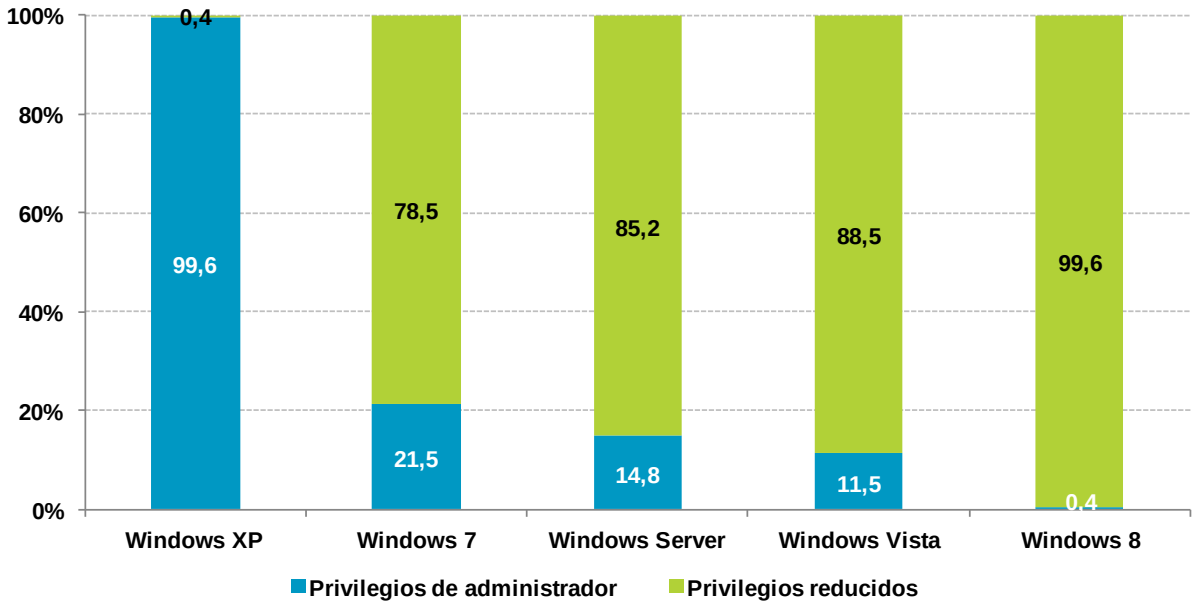
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

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 de los usuarios en el sistema operativo, según el nivel de privilegios (sistemas Windows):

iScan




BASE: Total usuarios de Microsoft Windows

La diferencia en el nivel de privilegios en las distintas versiones de los sistemas operativos de Microsoft se debe fundamentalmente a la configuración por defecto de dichos sistemas operativos. Esto confirma que el usuario confía mucho en las configuraciones por defecto del sistema operativo utilizado y pocas veces cambia estas configuraciones.
Los sistemas operativos basados en Linux y/o OSX **por defecto no tienen privilegios de administrador** en sus cuentas de usuario.

**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

El hecho de no utilizar medidas de seguridad automatizables se debe principalmente al **desconocimiento** y a la creencia del usuario de su **falta de necesidad** de la misma.



| Medidas | Hogares que no utilizan en la actualidad (%) * | Motivos (%) ** | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | No conoce | No necesita | Precio | Entorpecen | Desconfía | Ineficaces | Otros |
| Programas antivirus | 16,1 | 8,3 | **27,4** | 24,5 | 9,6 | 5,9 | 6,7 | 17,6 |
| Actualizaciones antivirus | 28,7 | 8,3 | **25,9** | 23,0 | 9,1 | 5,3 | 5,5 | 22,9 |
| Actualizaciones del sistema operativo | 40,5 | 13,2 | **28,4** | 14,2 | 9,6 | 4,6 | 4,0 | 26,0 |
| Cortafuegos o firewall | 55,8 | 24,7 | **26,9** | 9,4 | 12,7 | 4,6 | 3,9 | 17,9 |
| Programas o configuración de bloqueo de pop-up | 63,3 | **28,9** | 27,8 | 6,1 | 12,2 | 4,6 | 5,0 | 15,4 |
| Programas o configuración anti-spam | 67,0 | 19,3 | **36,3** | 6,0 | 10,2 | 6,6 | 5,0 | 16,6 |
| Programas anti-espía o anti-fraude | 73,4 | 25,2 | **27,1** | 11,9 | 8,1 | 7,8 | 4,5 | 15,4 |
| Plugins de seguridad para el navegador | 73,7 | **36,5** | 26,0 | 5,5 | 10,7 | 5,0 | 3,2 | 13,1 |
| Programas o configuración para bloqueo de publicidad | 81,4 | **37,3** | 25,2 | 6,3 | 9,7 | 5,6 | 3,6 | 12,3 |

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

# Motivos alegados para no utilizar medidas de seguridad



Un alto porcentaje de usuarios que no utilizan medidas de seguridad, **no lo hace porque** consideran que **no las necesitan.**

Alegando este motivo, destaca la **no utilización de contraseñas** para proteger el equipo y documentos por parte del **54,1%** de los internautas españoles que no las utilizan en la actualidad.

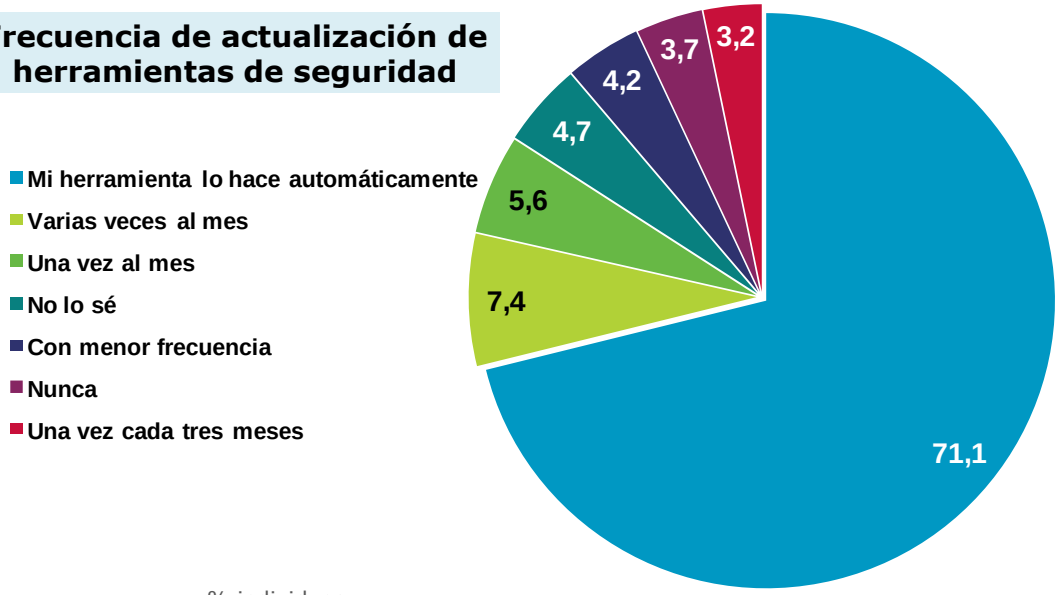
| Medidas | Hogares que no utilizan en la actualidad (%) * | Motivos (%) ** | | | | | |
|---|---|---|---|---|---|---|---|
| | | No conoce | No necesita | Entorpecen | Desconfía | Ineficaces | Otros |
| Contraseñas (equipos y documentos) | 40,6 | 12,5 | **54,1** | 6,3 | 5,2 | 4,6 | 17,3 |
| Eliminación archivos temporales y cookies | 44,8 | 24,4 | **35,9** | 7,2 | 5,7 | 3,5 | 23,3 |
| Copia de seguridad de archivos | 61,1 | 14,1 | **44,6** | 5,5 | 3,9 | 2,3 | 29,6 |
| Partición del disco duro | 76,2 | 27,1 | **42,3** | 6,0 | 3,4 | 2,4 | 18,8 |
| Certificados digitales de firma electrónica | 78,9 | 20,8 | **47,0** | 3,6 | 5,0 | 1,8 | 21,8 |
| Utilización habitual con permisos reducidos | 84,4 | 20,0 | **49,6** | 7,3 | 3,5 | 2,5 | 16,9 |
| DNI electrónico | 86,7 | 9,5 | **49,4** | 3,2 | 6,3 | 1,9 | 29,7 |
| Cifrado de documentos o datos | 93,7 | 31,5 | **45,8** | 3,5 | 3,6 | 1,6 | 14,1 |

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

# Frecuencia de actualización y utilización

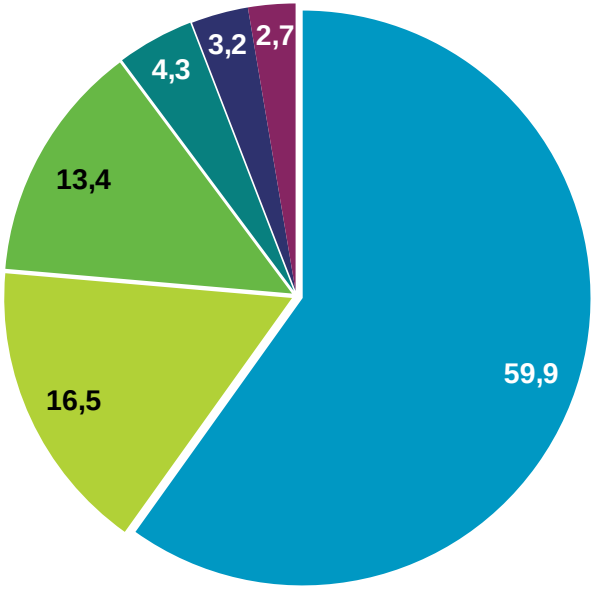
Un **71,1%** de los usuarios declara que la actualización de sus herramientas de seguridad se hace de forma automática por las propias herramientas.

## Frecuencia de actualización de herramientas de seguridad




% individuos

BASE: Total usuarios




## Frecuencia de escaneo con un programa antivirus

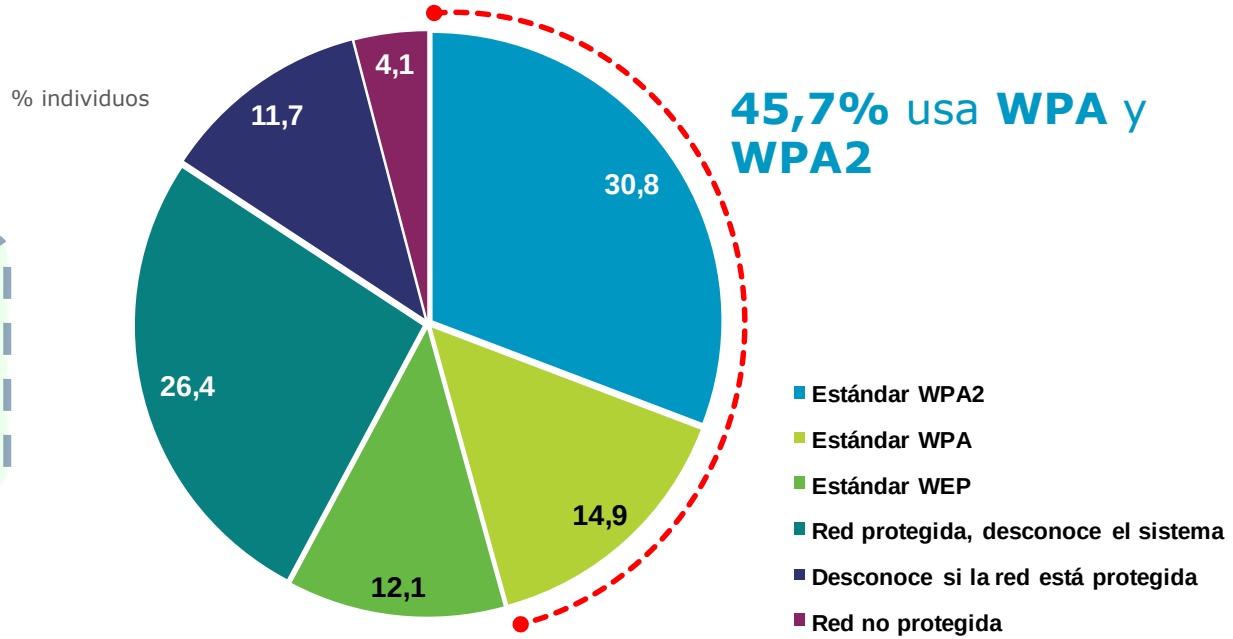
BASE: Usuarios que utilizan programas antivirus

**Tres de cada cinco** usuarios que tiene programa antivirus **no se implica** en el escaneo de su equipo para detectar infecciones de malware y deja que sea el programa el que lo haga **de manera predeterminada**.

# Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi



Según el estudio, sólo el **16%** de los usuarios deja su red inalámbrica Wi-Fi **desprotegida** y/o **desconoce** si lo está.




**45,7%** usa **WPA** y **WPA2**

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

BASE: Usuarios Wi-Fi con conexión propia

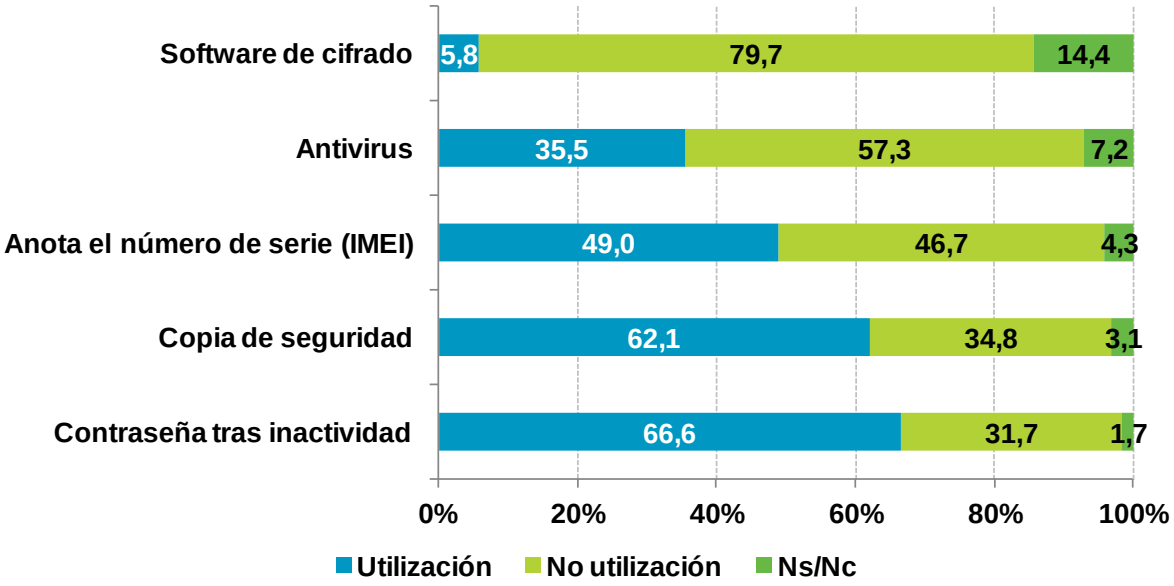
**WPA2** es el sistema más seguro hasta la fecha para cifrar las conexiones inalámbricas.

**WPA** también es un buen sistema de cifrado que todavía continúa utilizándose en dispositivos antiguos que no soportan WPA2.

Por otro lado, el sistema de cifrado **WEP**, además de estar obsoleto, se encuentra totalmente comprometido por lo que utilizarlo conlleva un alto riesgo de intrusión en la red inalámbrica Wi-Fi.

# Medidas de seguridad utilizadas en smartphone

**Dos tercios** de la población con smartphone utiliza el **código PIN** y/o **contraseña después de inactividad** en su dispositivo móvil, y realiza **copias de seguridad** de los archivos para evitar perderlos.




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#**

**Recomendaciones para proteger y/o conservar la información almacenada en los dispositivos móviles**

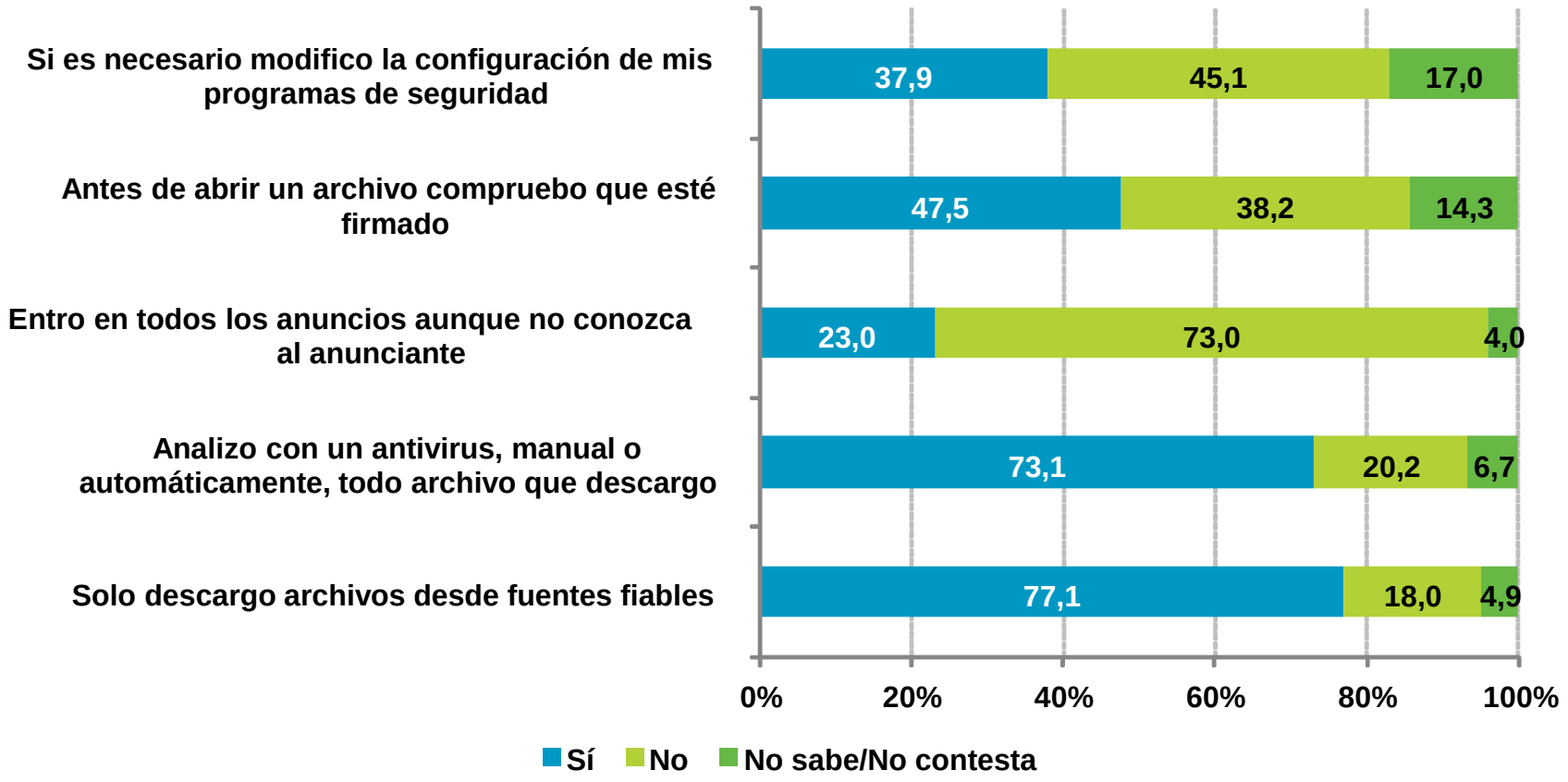
- ✓ Tener apuntado el número de serie (IMEI) para rastrear o desactivar el terminal a través de la operadora de telefonía móvil, en caso de pérdida o robo.
- ✓ Activar el código PIN para evitar el acceso automático al encender el terminal.
- ✓ Activar el bloqueo automático del teléfono móvil para evitar accesos no autorizados.
- ✓ Realizar copias de seguridad de los datos.
- ✓ Cifrar la información sensible almacenada en el dispositivo.
- ✓ Utilizar un software antivirus para analizar los ficheros.

Para más información: http://www.osi.es/smartphone-y-tablet

# Hábitos de comportamiento en la navegación y uso de Internet

# Uso de Internet

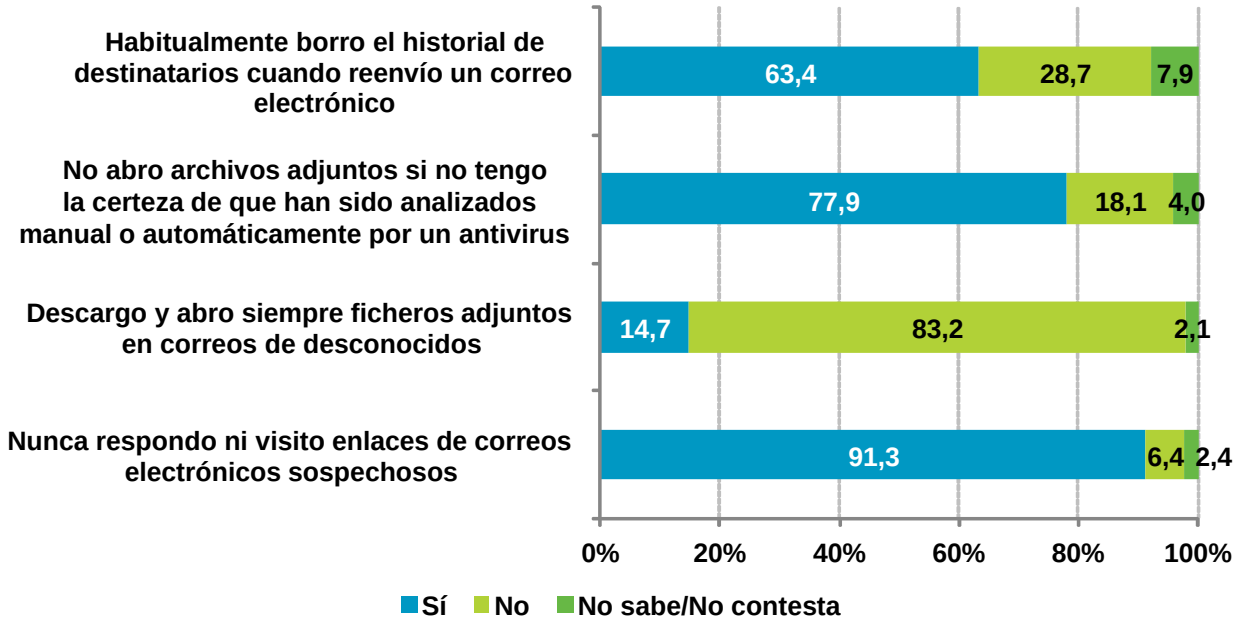
Casi un **38%** de los usuarios declara que **modifica la configuración** de los programas de seguridad, si es necesario, para mejorar la experiencia de navegación y uso de Internet.




BASE: Total usuarios

# Correo electrónico

**Un 28,7%** de la población que utiliza el correo electrónico **no elimina** el historial de destinatarios cuando reenvía un e-mail.




BASE: Usuarios que utilizan correo electrónico

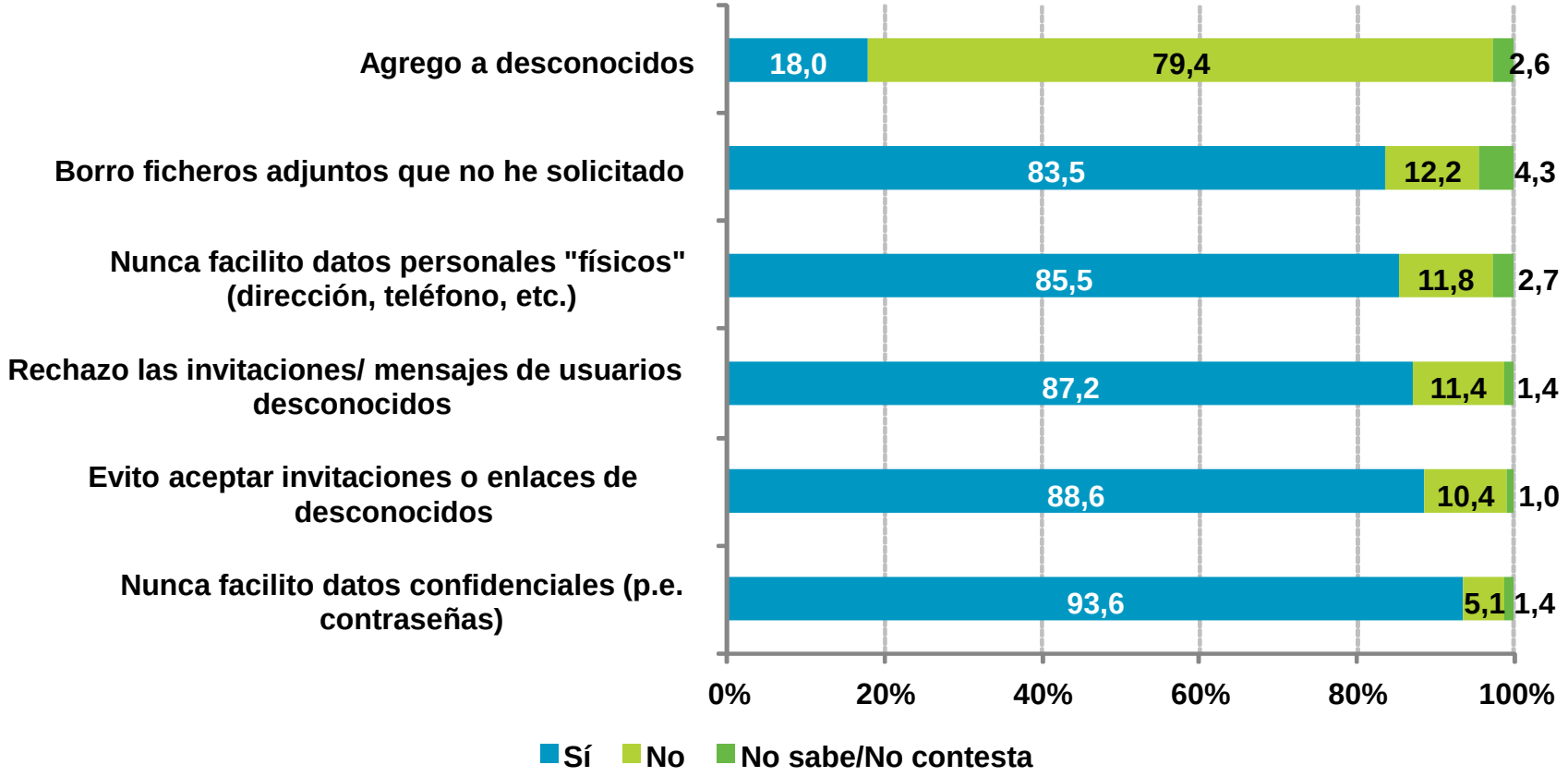
Enviar el historial de destinatarios al reenviar un correo electrónico favorece la **difusión** y **recolección** de direcciones de email válidas entre los atacantes que recolectan direcciones de correo para uso malicioso, como es la emisión de correos no deseados (spam).

La mayoría de las **cadenas** de email y los ***hoax*** (bulos o bromas) son creados con la finalidad de **recopilar** direcciones de correo, confiando en que serán reenviados por los usuarios a toda la lista de contactos.

La importancia de la Copia Oculta (CCO):
https://www.osi.es/es/actualidad/blog/2013/10/29/correos-para-muchos-destinatarios-haz-uso-de-cco

# Chats y mensajería instantánea

El **93,6%** de los usuarios de mensajería instantánea **no facilita nunca** información confidencial, como contraseñas, a través de chat o mensajería instantánea.

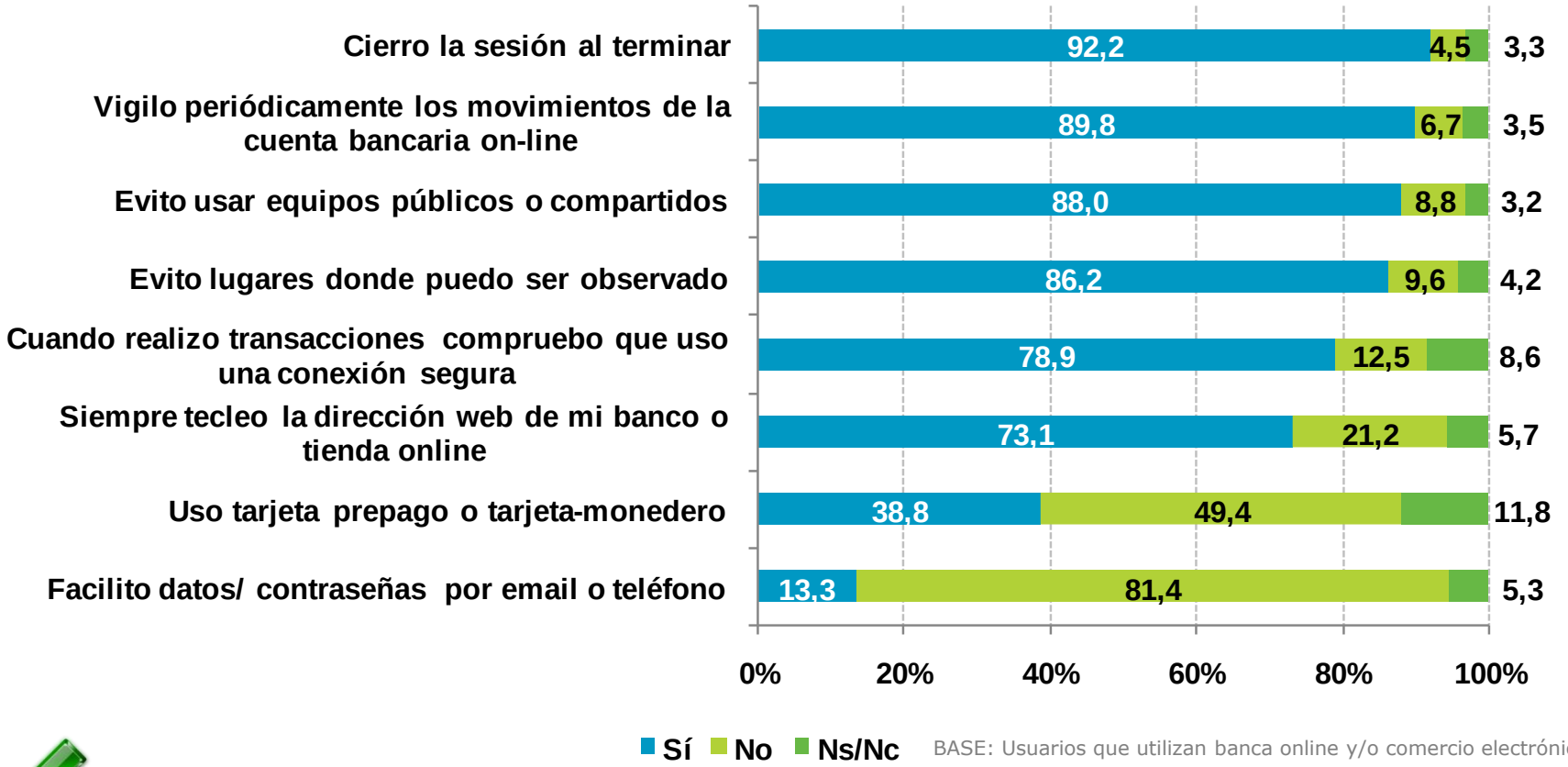



BASE: Usuarios que utilizan mensajería electrónica y/o chats

Para protegerse en mensajería instantánea, tienes más información en:
http://www.osi.es/mensajeria-instantanea

# Banca en línea y comercio electrónico

**El 38,8%** de los usuarios de comercio electrónico utiliza **tarjetas prepago** o **monedero** para realizar pagos a través de Internet.

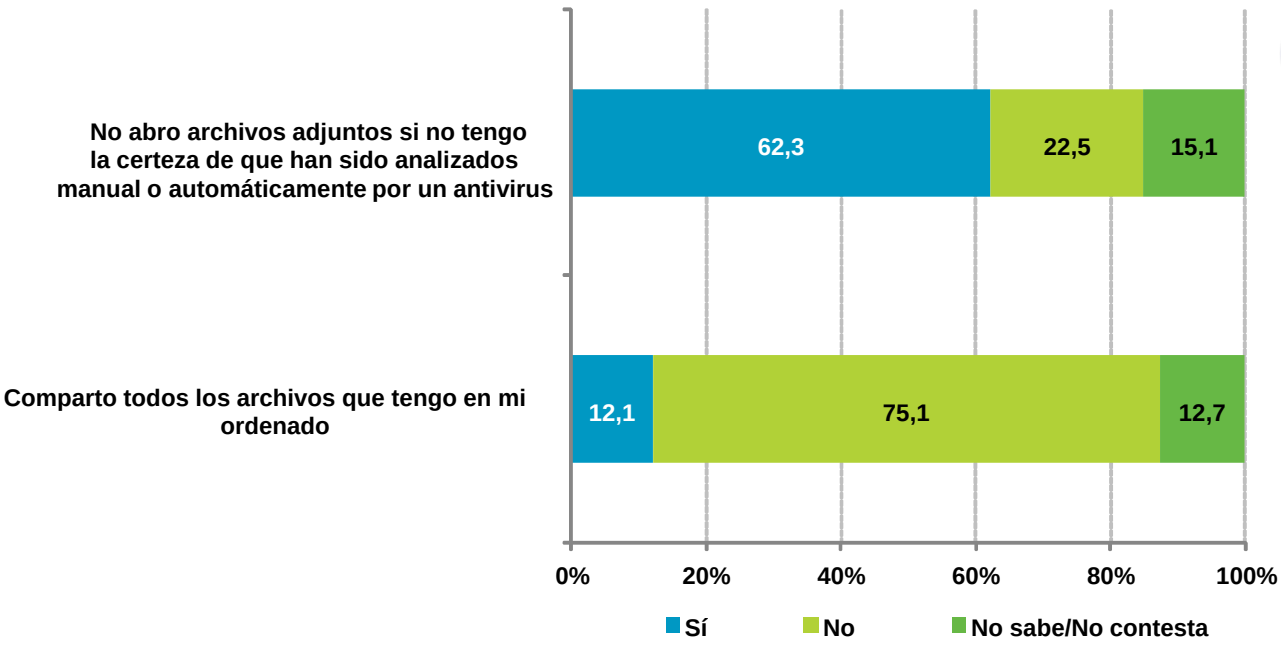



BASE: Usuarios que utilizan banca online y/o comercio electrónico

Para conocer qué medidas utilizar para protegerte al realizar trámites on-line visita:
http://www.osi.es/es/banca-electronica
https://www.osi.es/es/actualidad/blog/2014/03/28/aprendiendo-verificar-la-legitimidad-de-un-sitio-web

# Descargas en Internet

Según declaraciones de los usuarios de redes P2P, un **62,3%** no abre ficheros descargados si no tiene la certeza de que han sido **analizados** con el antivirus.



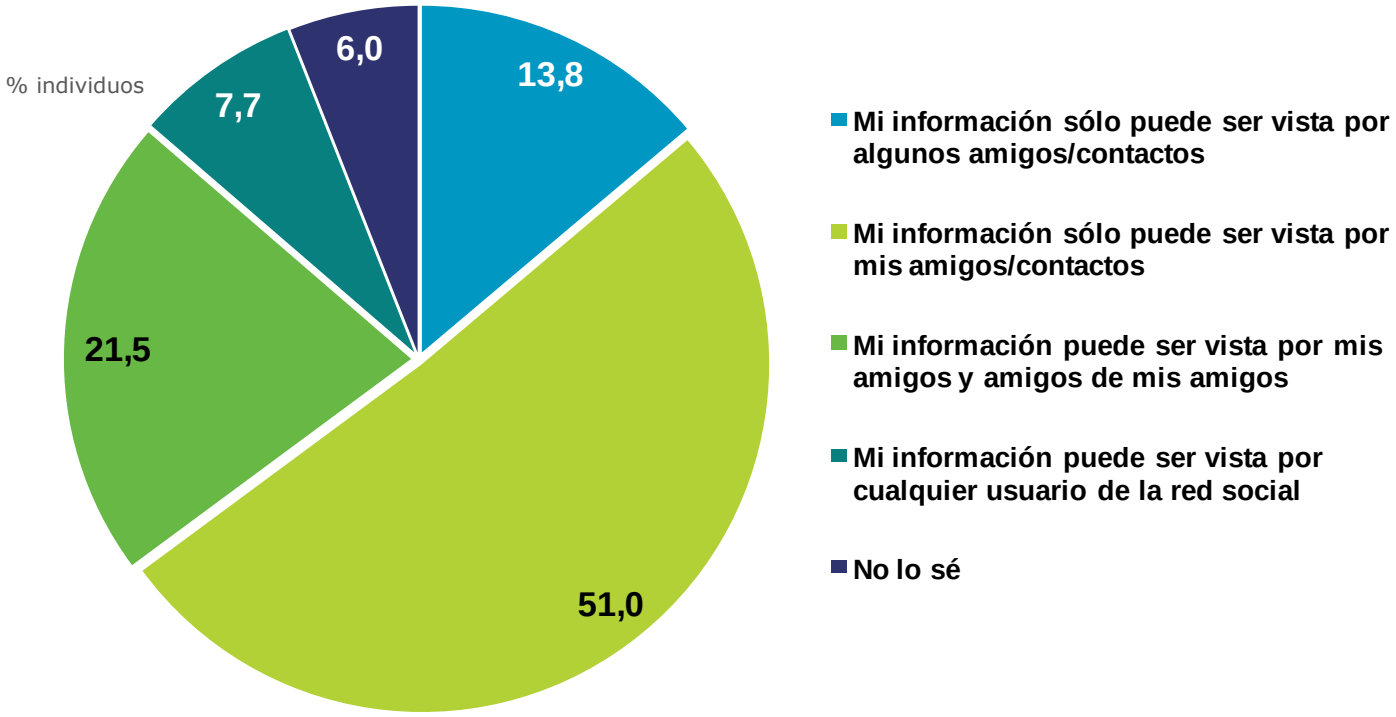

BASE: Usuarios de redes P2P

Las redes de descarga P2P (del inglés *peer to peer*, redes de pares o entre iguales) son aquellas en las que el contenido no se aloja en un servidor al que los clientes se conectan, sino que cada ordenador conectado a ellas actúa como tal servidor compartiendo el contenido almacenado en su disco duro.

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

# Redes sociales

Casi un **30%** (21,5 + 7,7) de los usuarios de redes sociales, **tiene su perfil abierto a terceras personas y/o desconocidos**, e incluso un **6%** de los consultados **desconoce** el nivel de privacidad de su perfil.




BASE: Usuarios que utilizan redes sociales

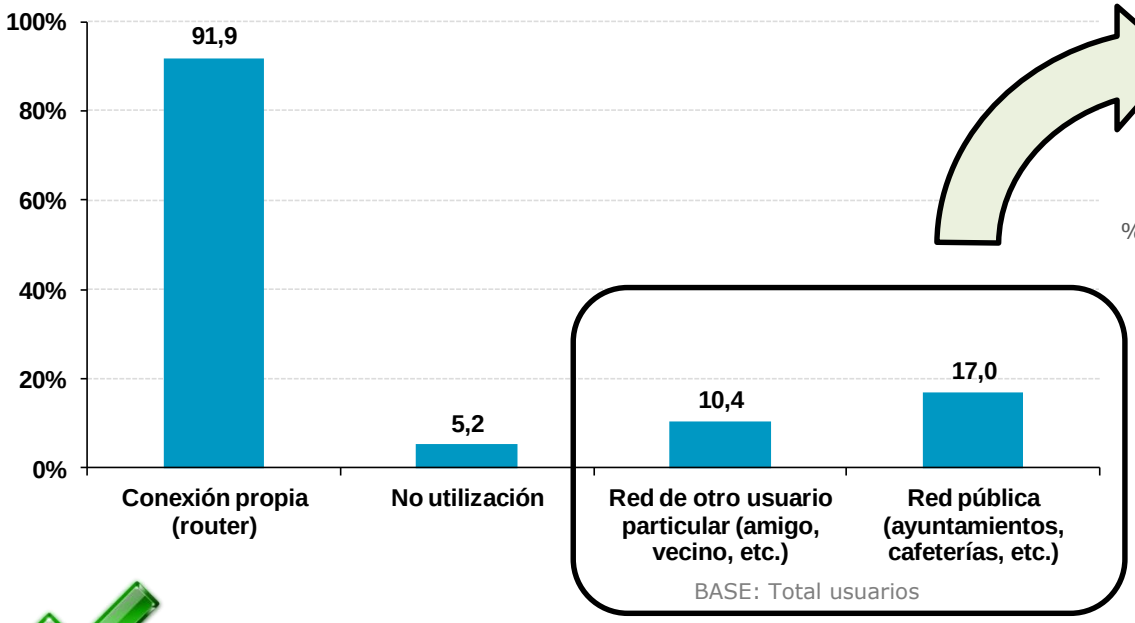
**Para conocer cómo protegerte en las redes sociales y configurar los perfiles de cada una:**
http://www.osi.es/redes-sociales

# Hábitos de uso de las redes inalámbricas Wi-Fi

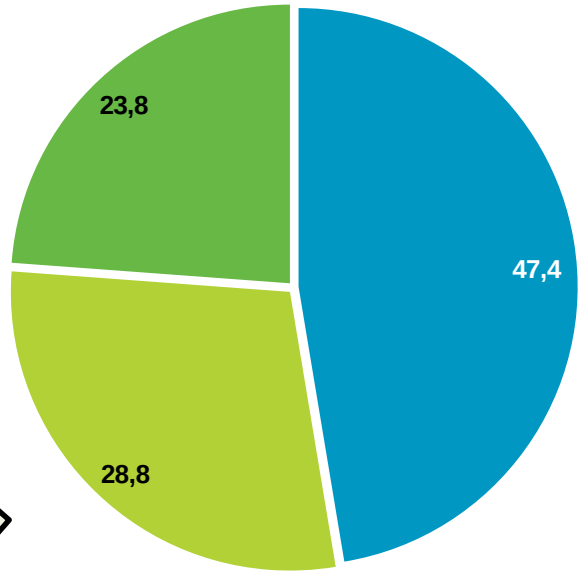


**Punto de acceso a Internet mediante redes inalámbricas Wi-Fi**

**Respuesta múltiple**




BASE: Total usuarios

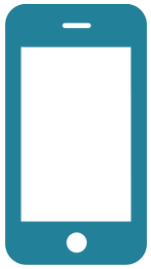



BASE: Usuarios que se conectan a una red Wi-Fi pública o a una red de otro usuario

El 47,4% de los usuarios que accede a internet a través de una red inalámbrica Wi-Fi pública, lo hace **siempre que lo necesita** y **en cualquier lugar**.

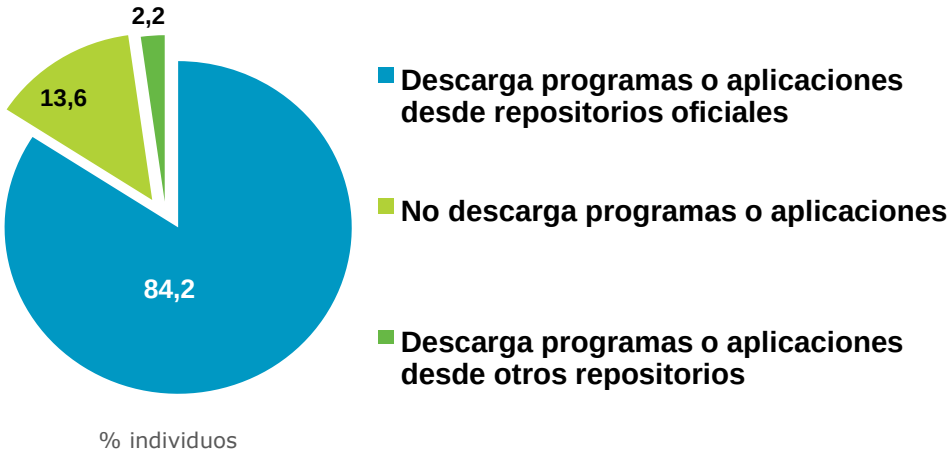
Consejos para conectarse seguro en redes Wi-Fi públicas:
https://www.osi.es/es/actualidad/blog/2013/07/05/redes-wifi-publicas-conectate-con-prudencia

# Hábitos de uso en smartphone



Un **82,8%** de internautas con acceso frecuente a Internet posee un Smartphone o teléfono móvil "inteligente "

De ellos, un **84%** únicamente descarga programas y/o aplicaciones desde **repositorios oficiales**



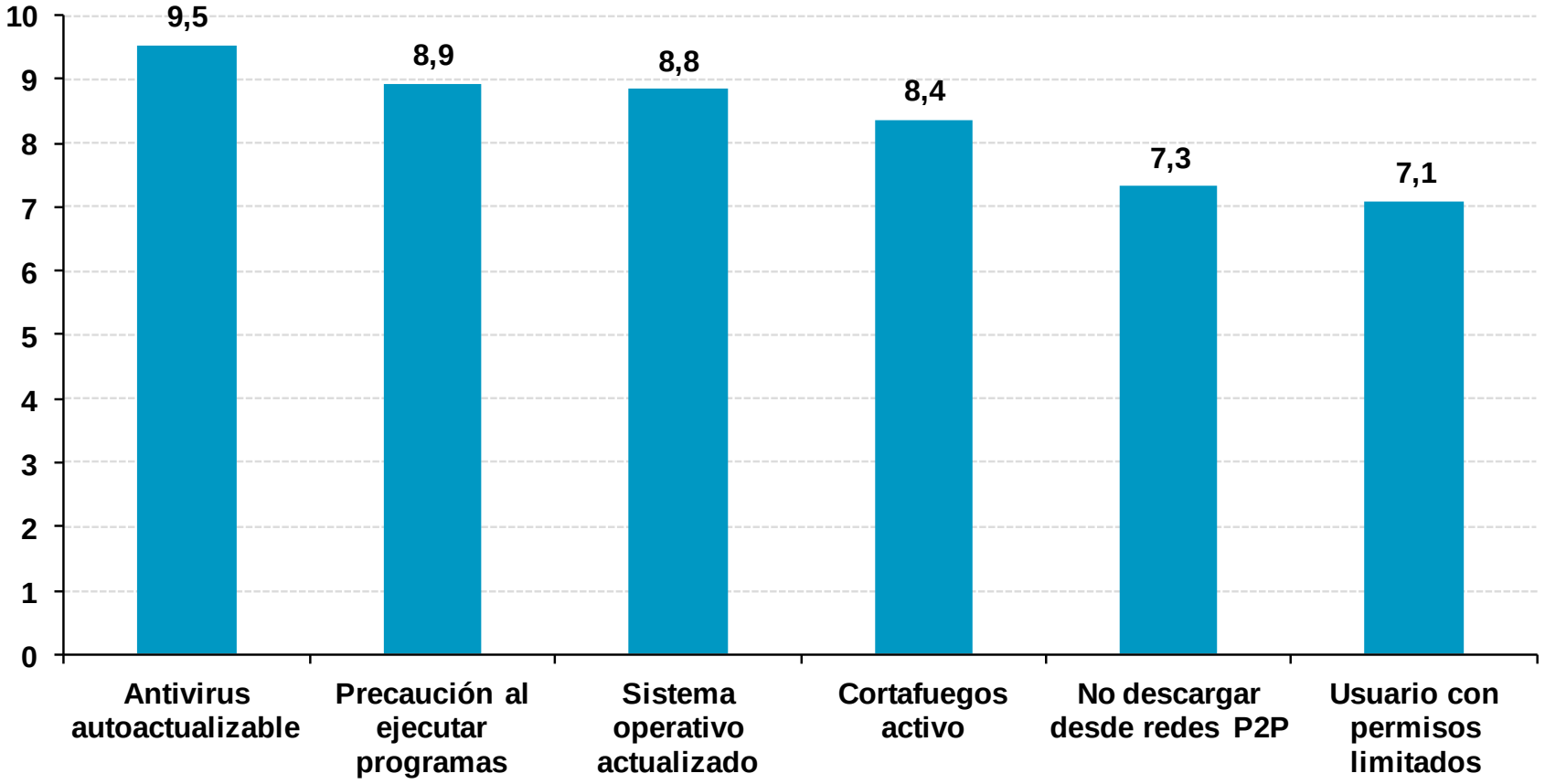

% individuos

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.

BASE: Usuarios que disponen de smartphone

# Valoración de las medidas de seguridad

La medida de seguridad mejor valorada por los usuarios es el **antivirus** auto-actualizable, relegando la **precaución al ejecutar programas** a una segunda posición.




BASE: Total usuarios

Para valorar la importancia de las herramientas de seguridad se ha utilizado un baremo de 0 a 10.

# Incidentes de seguridad

# 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/

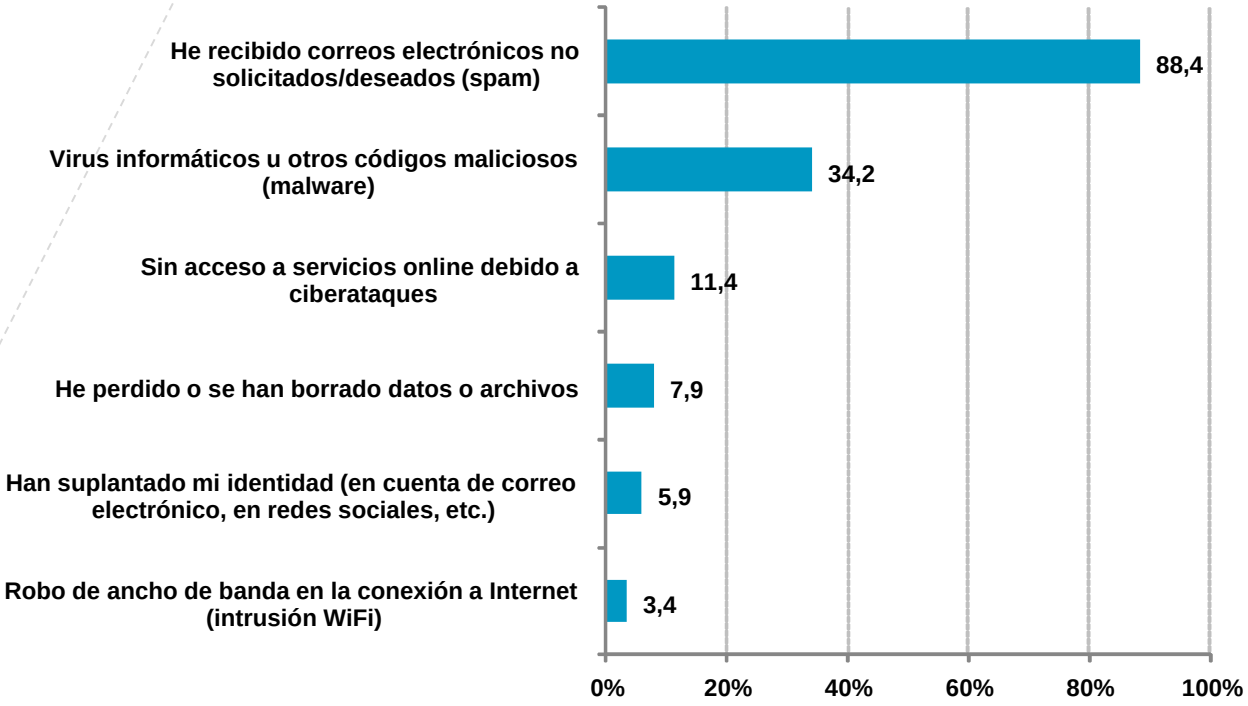
# Incidencias de seguridad

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.

**Incidencias sufridas:**

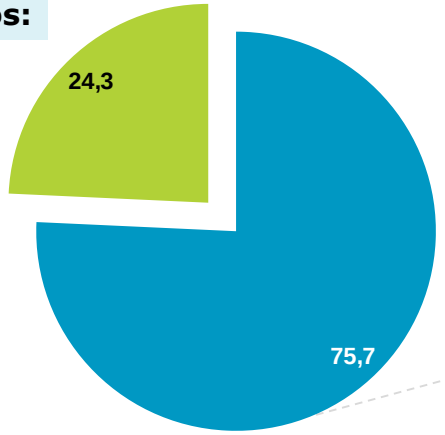
**Respuesta múltiple**




% individuos

BASE: Usuarios que han sufrido alguna incidencia de seguridad

**Afectados:**




BASE: Total usuarios

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

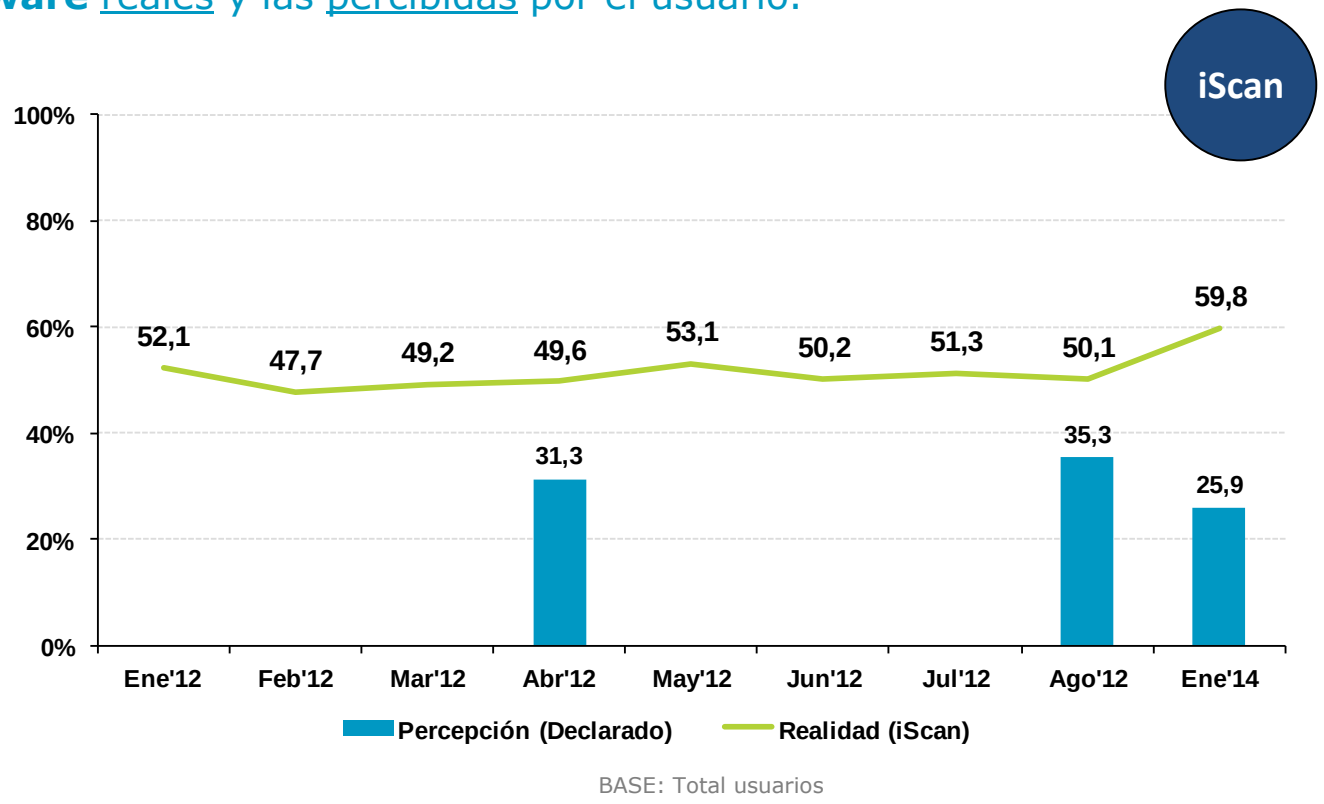
http://www.osi.es/contra-virus

# Evolución de los incidentes por malware

iScan revela que existe **una amplia brecha (de 33 puntos porcentuales)** entre las **incidencias de malware** reales y las percibidas por el usuario.

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

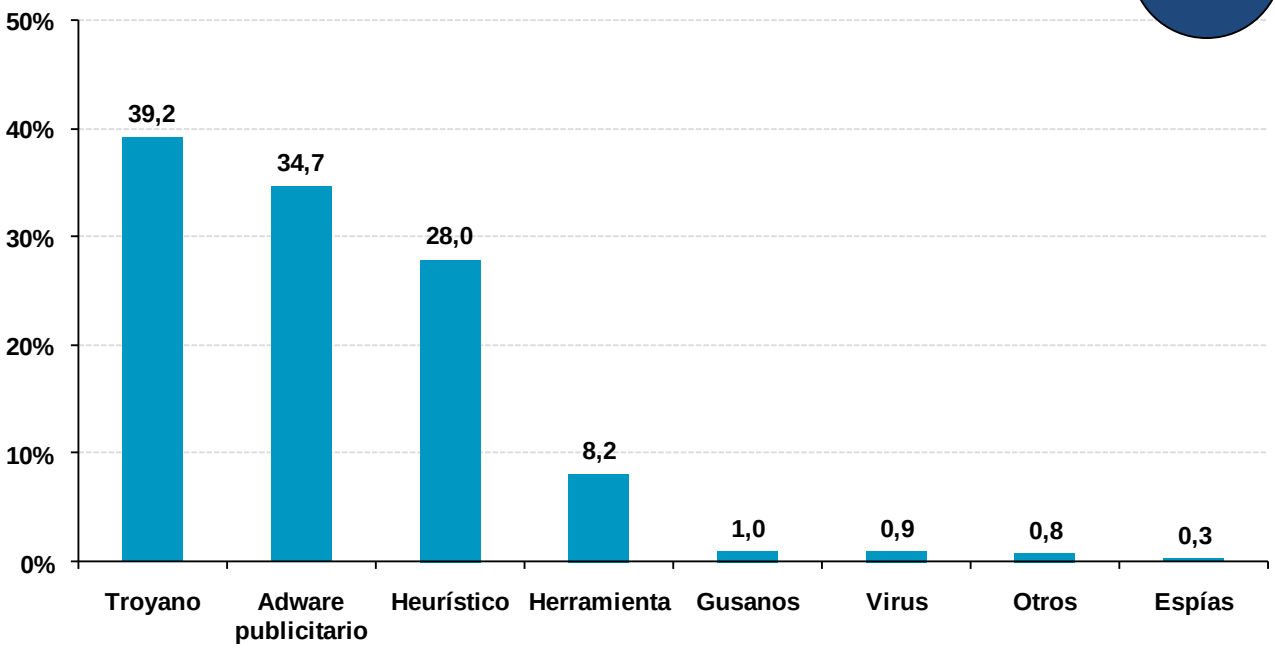
Para la obtención del dato **real** se utiliza el software **iScan**, desarrollado por INTECO, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 50 motores antivirus. El software **iScan** se instala en los equipos y los analiza, detectando el malware 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 malware con **mayor presencia** en los equipos españoles es el tipo **troyano** (en casi un **40%** de los ordenadores escaneados en enero de 2014). En un segundo lugar se encuentra el **adware publicitario** detectado en más de un tercio de los equipos (**34,7%**).

**Equipos que alojan malware según tipología (ene. 14)**

iScan

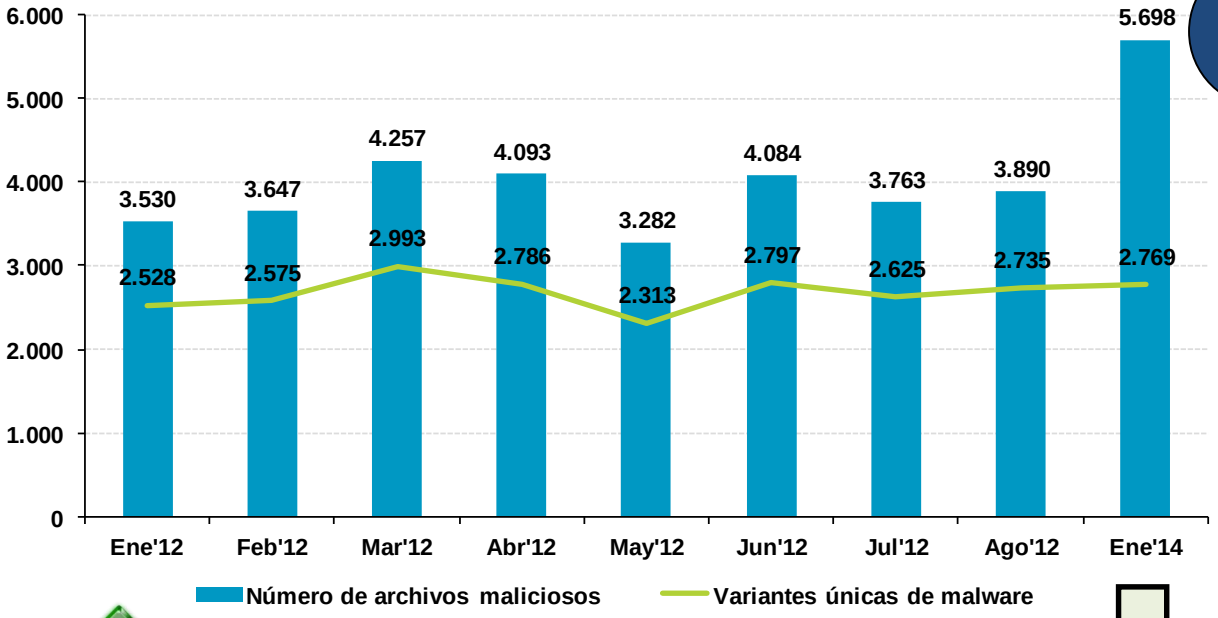



Se denomina malware a todos aquellos programas malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

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

BASE: Total equipos

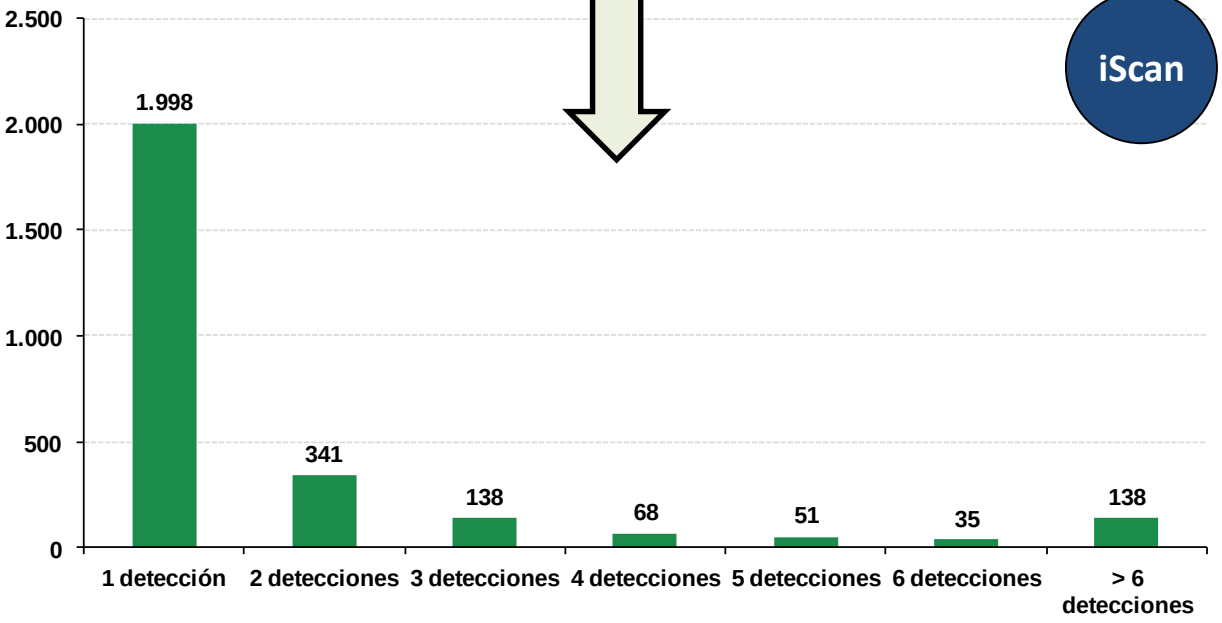
# Diversificación del malware detectado




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.




iScan

**Número de detecciones de cada variante única de malware (ene. 14)**

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 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); o minan el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.

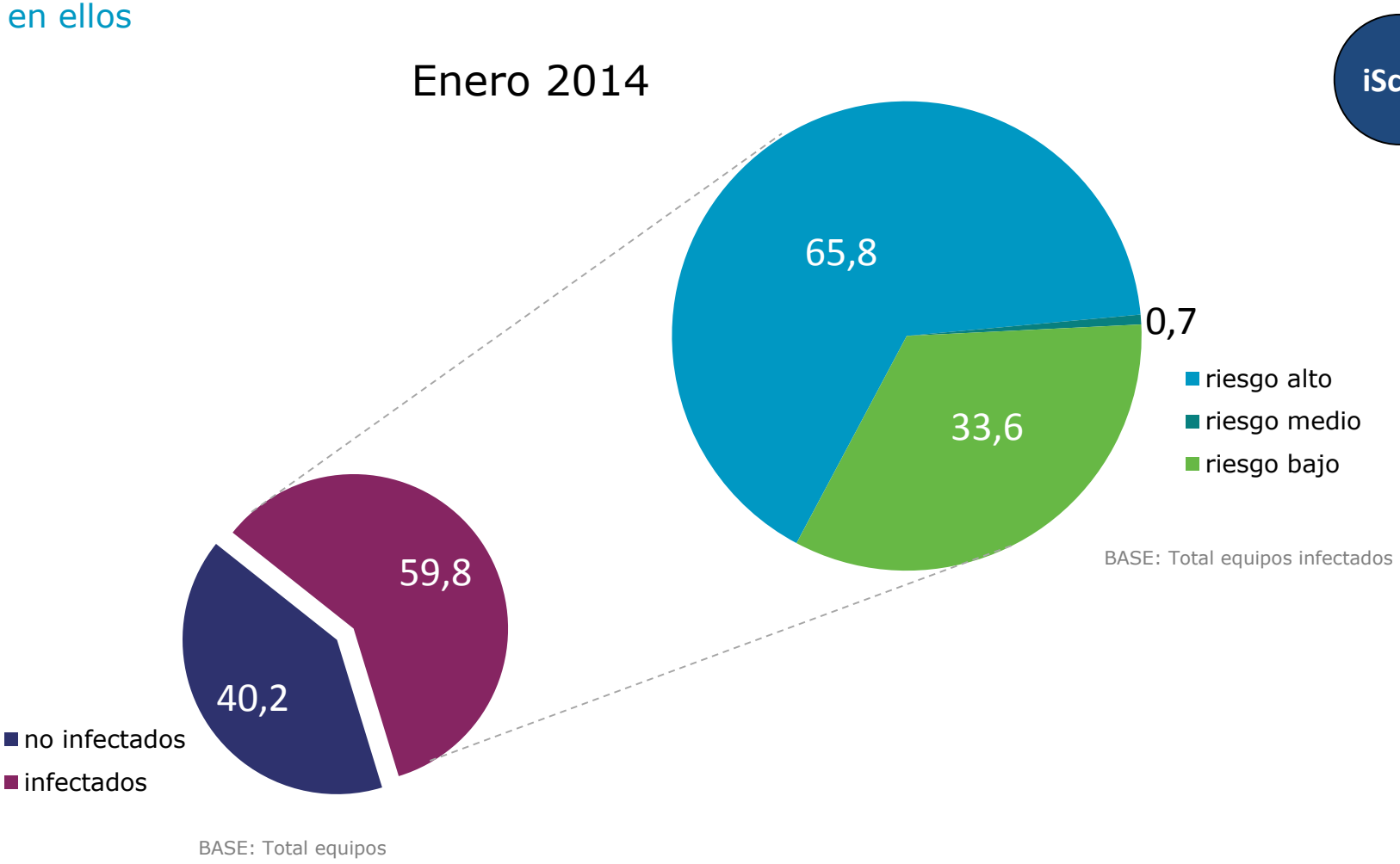
**Peligrosidad media**: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema: no perjudican de forma notoria su rendimiento; abren ventanas no deseadas al navegar; incrustan publicidad en páginas web legítimas que realmente no contienen publicidad; o facilitan la captura 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.

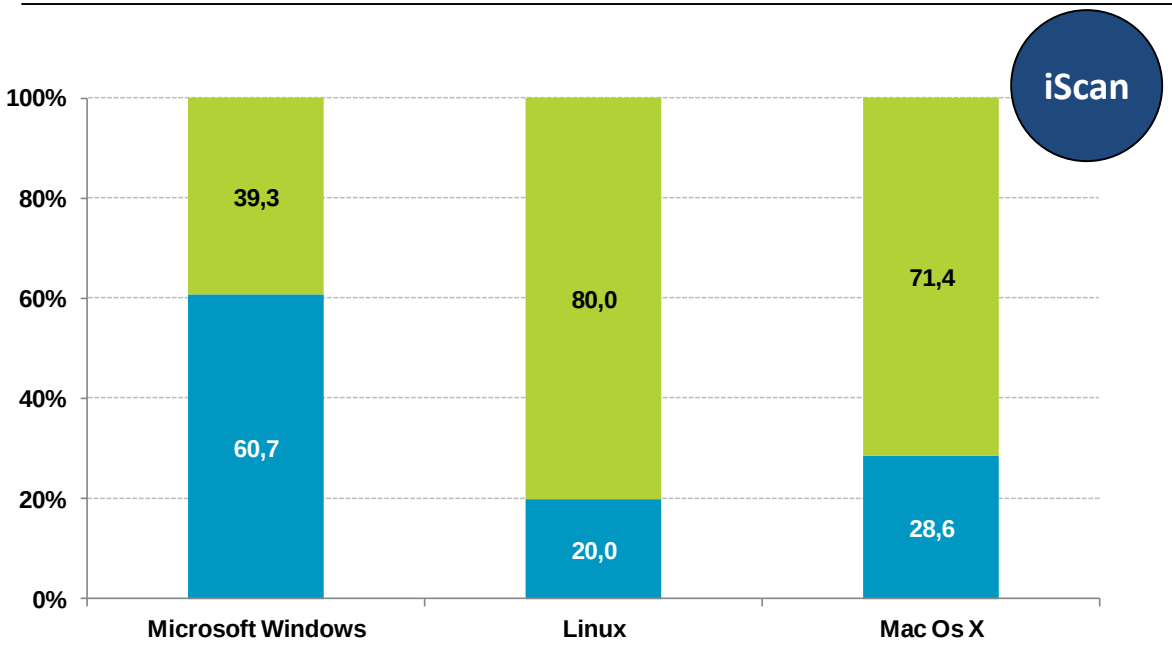
[3] Se establece como el nivel de riesgo de cada equipo el de mayor nivel de entre el malware que aloje. Es decir, un equipo en el que se detecte un software malicioso de peligrosidad alta y otro de peligrosidad media, siempre será incluido en el grupo de equipos con un nivel de riesgo alto.

# Peligrosidad del código malicioso y riesgo del equipo

**Dos de cada tres** equipos analizados con iScan están infectados y presentan un nivel de **riesgo alto** debido al potencial peligro que suponen los archivos maliciosos encontrados en ellos



# Malware vs. sistema operativo y actualización




**Equipos infectados según sistema operativo (ene. 14)**

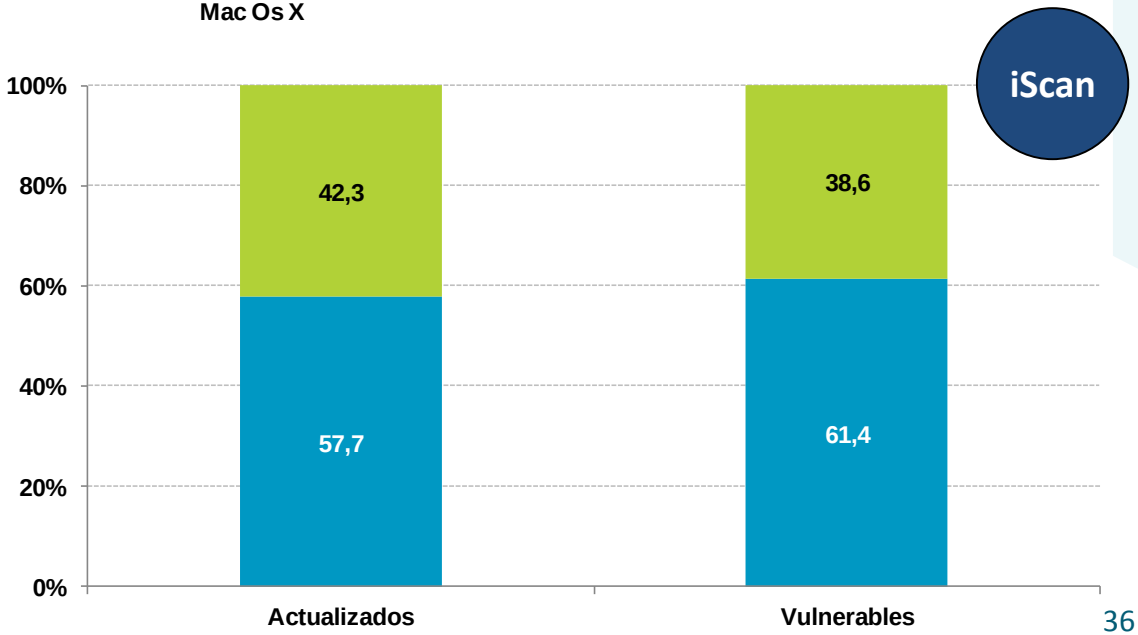
En el mes de enero de 2014, iScan detecta **malware** en el **60%** de máquinas con sistemas operativos Microsoft Windows.

Infectados

No infectados

**Equipos infectados según estado de actualización (ene. 14)**

Existen **4 puntos porcentuales** de diferencia entre equipos que alojan malware según el estado de **actualización** del sistema operativo.

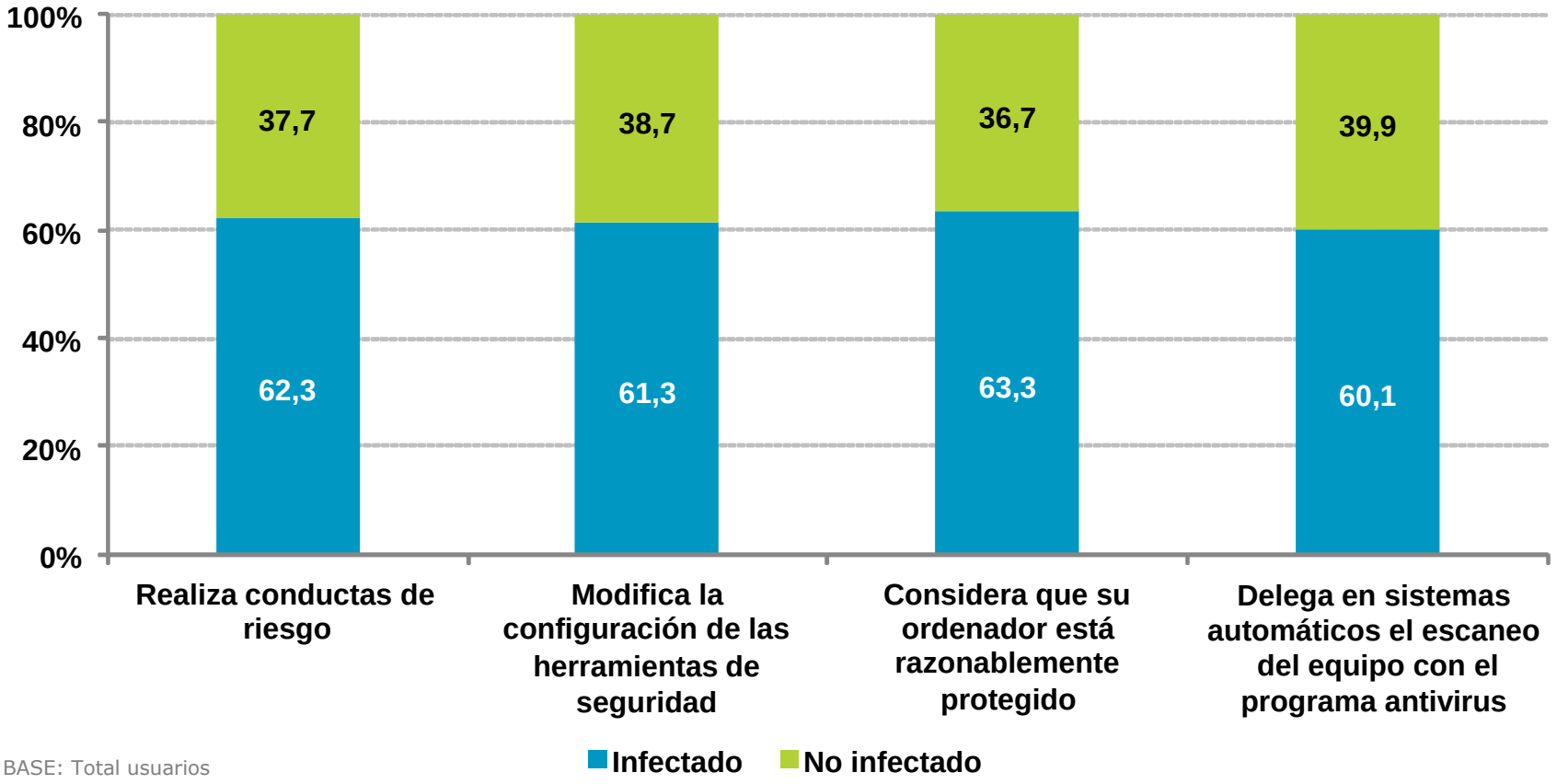



BASE: Total usuarios

# Malware vs. Hábitos de comportamiento

iScan detecta, en el mes de enero de 2014, un **mayor número de equipos infectados** entre aquellos usuarios que **no mantienen buenos hábitos de seguridad** al hacer uso de la Red.

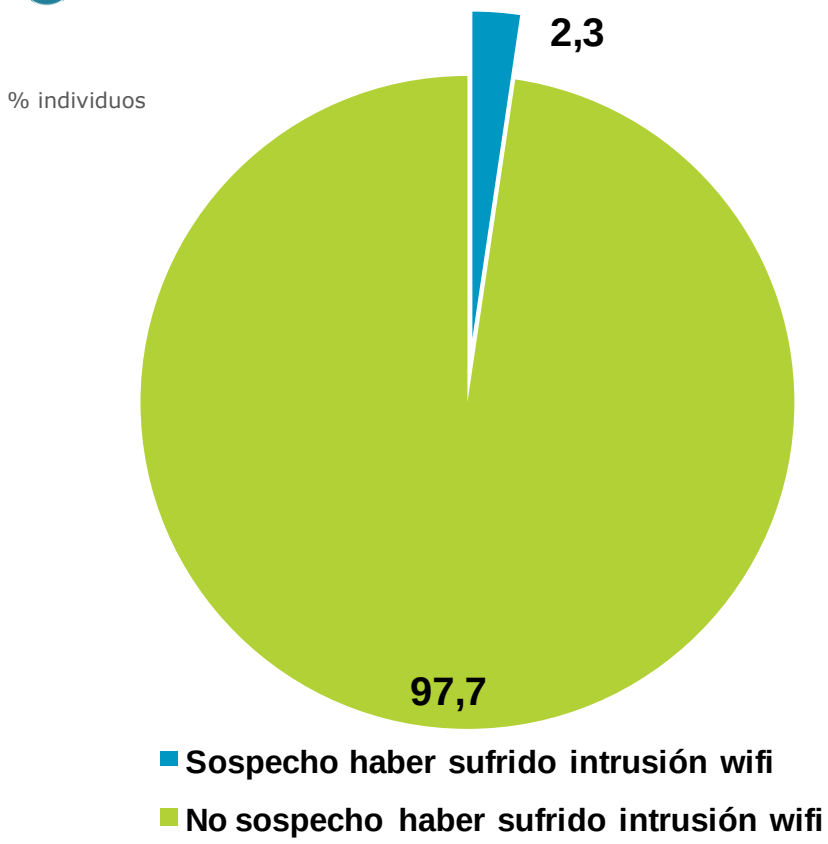
El **63,3%** de los usuarios que consideran su ordenador razonablemente protegido han tenido infección en el mismo, así como el **60,1%** de los usuarios que delegan en sistemas automáticos el escaneo del equipo con el programa antivirus




BASE: Total usuarios

# Incidencias de seguridad en redes inalámbricas Wi-Fi

Únicamente un **2,3%** de los panelistas encuestados *sospechan* haber sufrido una **intrusión** en la red inalámbrica Wi-Fi de su hogar.




**Pautas para mejorar la seguridad de la red Wi-Fi**

- ✓ Utilizar el sistema de cifrado WPA2 o WPA.
- ✓ Cambiar la contraseña que el fabricante del router utiliza por defecto.
- ✓ Modificar el nombre identificador de red (SSID) y la contraseña configurada por el operador.
- ✓ Utilizar una contraseña lo suficientemente segura (con una longitud de, al menos, 16 caracteres, conteniendo mayúsculas, minúsculas, números y signos de puntuación de manera pseudoaleatoria, y evitando datos personales o relacionados con el usuario).

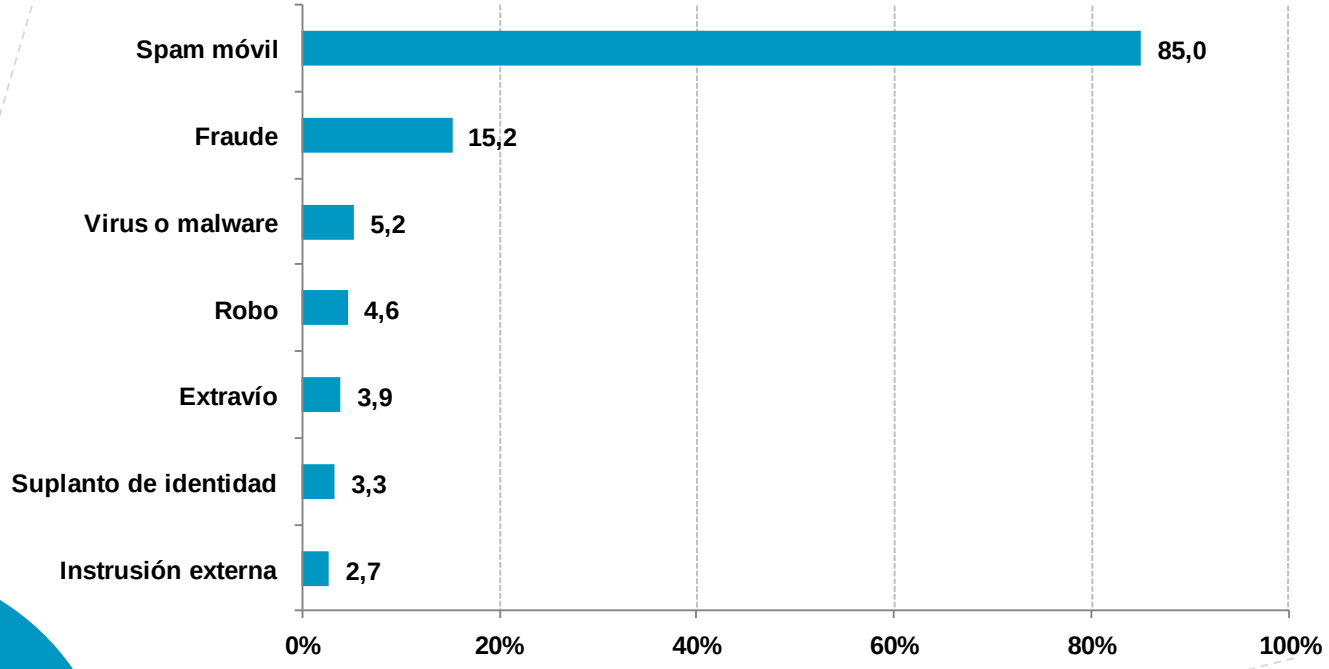
4

BASE: Usuarios con conexión Wi-Fi propia

# Incidencias de seguridad en smartphones

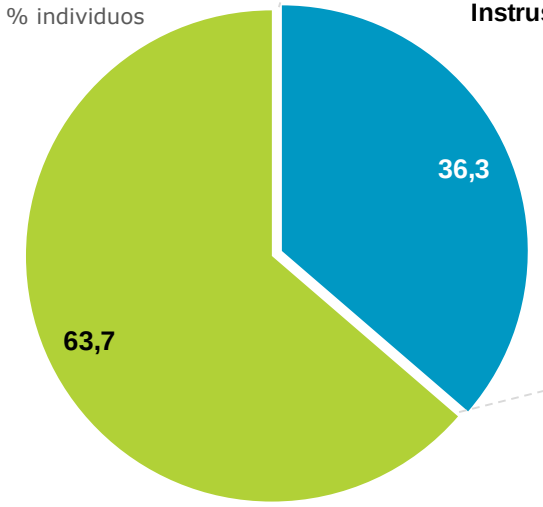
**Incidencias sufridas:**

**Respuesta múltiple**




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

**Afectados:**




Al igual que ocurre en el ordenador del hogar, la **principal** incidencia de seguridad ocurrida en smartphones es la recepción de correos no deseados (**spam**).

BASE: Usuarios que disponen de smartphone

# Consecuencias de los incidentes de seguridad y reacción de los usuarios

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

5

# Consecuencias de incidentes de seguridad en dispositivos móviles

Las **principales consecuencias** de las incidencias de seguridad en los dispositivos móviles son el **perjuicio económico** (**43,9%**) y la **suscripción a servicios no solicitados** (**50,2%**).

| Consecuencias | Incidencias (%) | | | | | | |
|---|---|---|---|---|---|---|---|
| | Extravío | Robo | Virus o Malware | Suplanto de identidad | Intrusión externa | Spam | Fraude |
| Robo de datos | 8,4 | 18,5 | 10,7 | 10,8 | **27,1** | 0,1 | 2,2 |
| Pérdida de datos | **38,7** | 29,3 | 18,4 | 18,3 | 14,1 | 2,2 | 5,7 |
| Suplanto de identidad | **28,5** | 19,4 | 14,0 | 25,1 | 8,6 | 1,7 | 7,7 |
| Sustracción de datos online | 1,3 | 2,9 | 4,8 | **21,6** | 14,2 | 1,4 | 4,0 |
| Perjuicio económico | 32,1 | 38,8 | 6,5 | 27,9 | 15,9 | 6,9 | **43,9** |
| Suscripción a servicios no solicitados | 1,5 | 15,4 | 13,2 | 19,2 | 42,9 | 14,1 | **50,2** |
| Otro | 3,5 | 3,1 | 7,2 | 0,0 | **4,0** | 2,7 | 3,0 |
| Ninguna de las anteriores | 21,1 | 14,8 | 47,7 | 37,5 | 18,9 | **75,9** | 12,1 |

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.

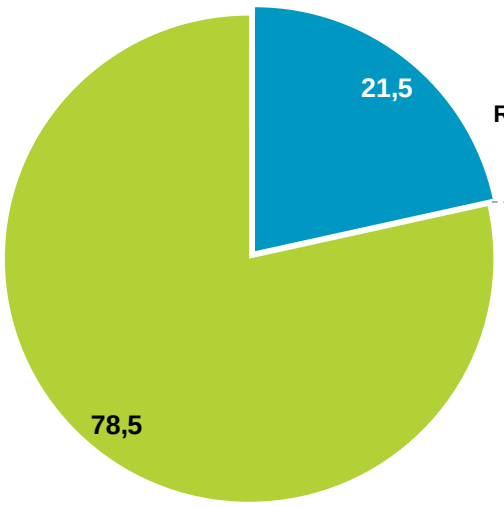
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

5

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

# Intento de fraude telefónico y manifestaciones

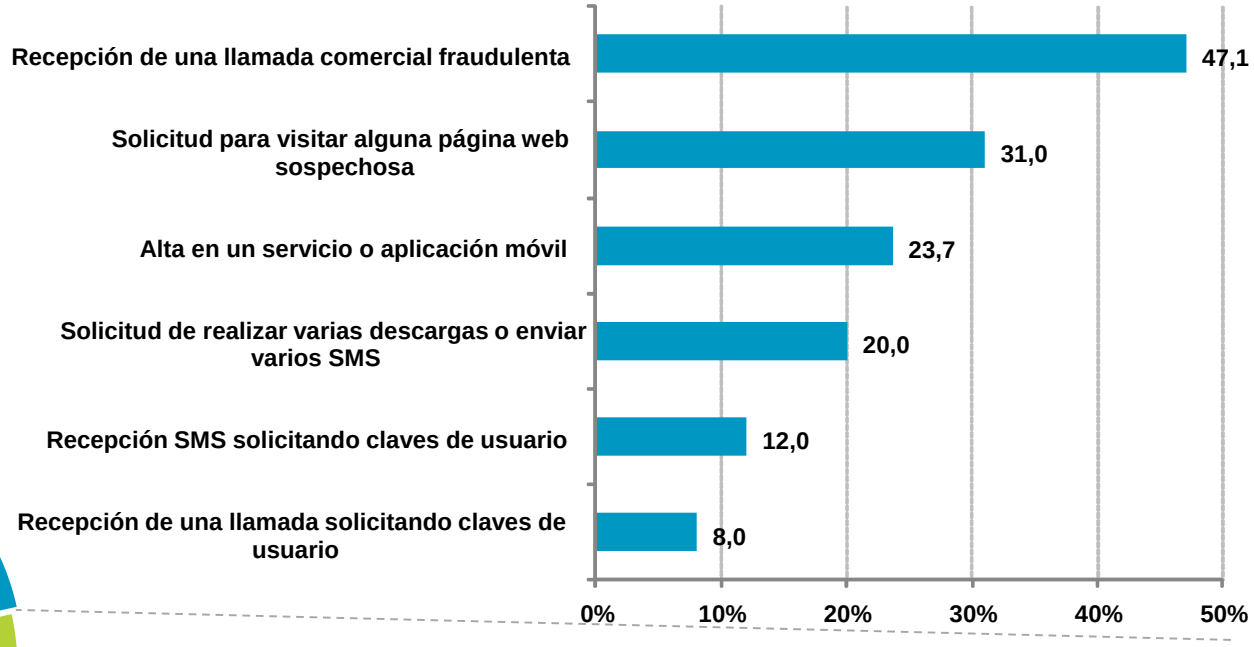
**Intento de fraude telefónico:**




BASE: Usuarios que disponen de dispositivo móvil o smartphone

**Manifestaciones del intento de fraude telefónico:**

**Respuesta múltiple**

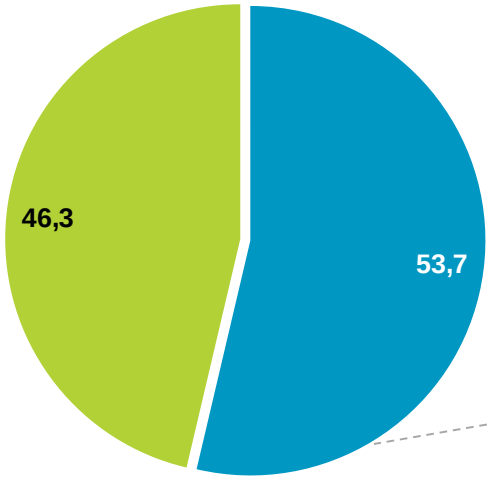



% individuos

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

# Intento de fraude online y manifestaciones

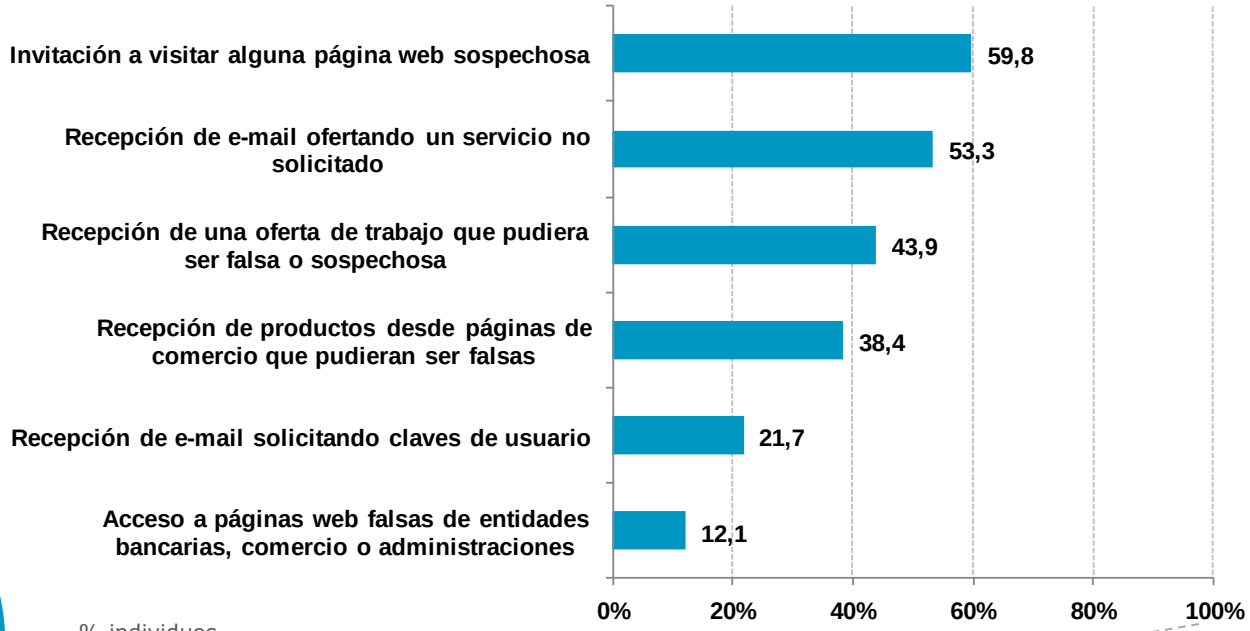
**Intento de fraude online:**




BASE: Total usuarios

**Manifestaciones del intento de fraude online:**

**Respuesta múltiple**




% individuos

BASE: Usuarios que han sufrido algún intento de fraude

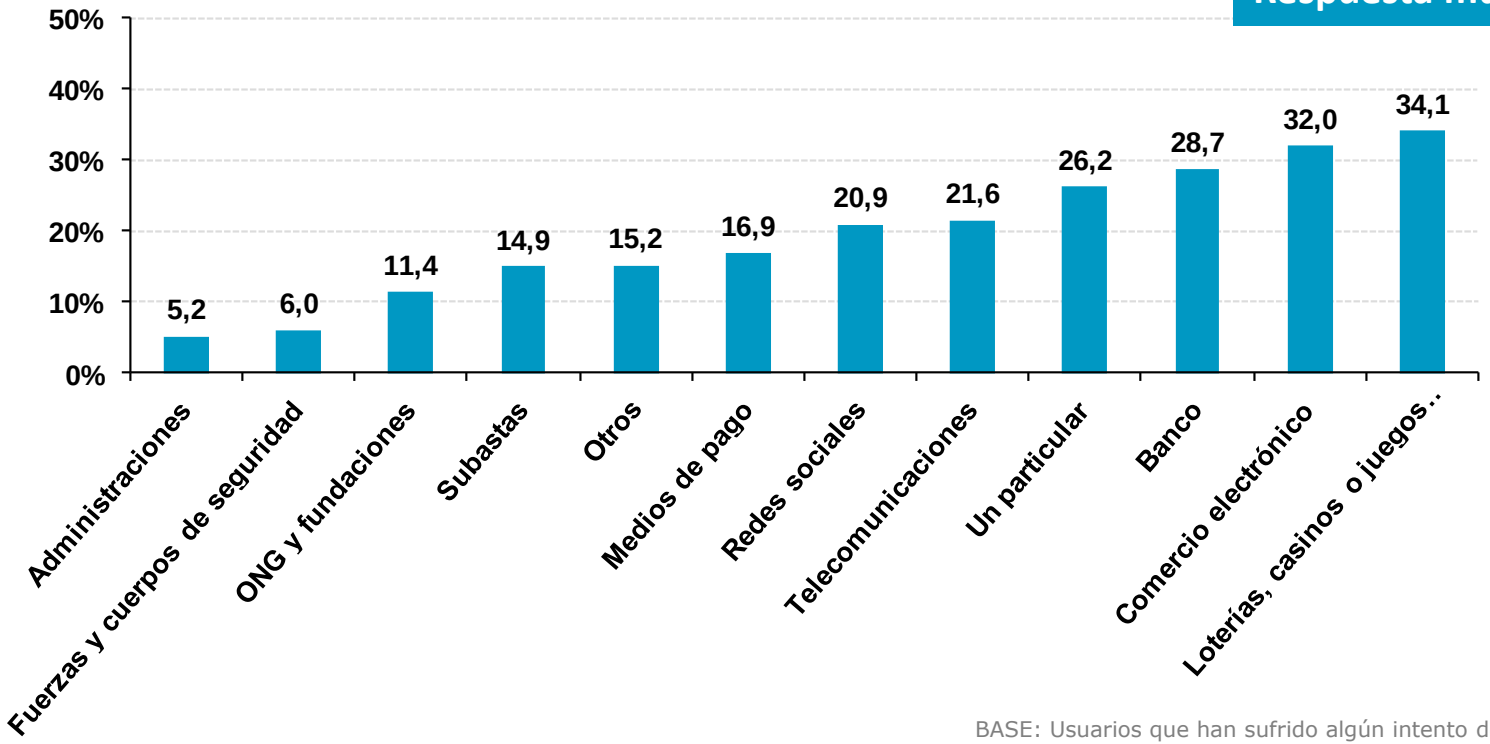
Conoce más en profundidad el fraude online:
http://www.osi.es/fraude-online

# Seguridad y fraude online y telefónico

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

De forma general, la principal **forma adoptada** por el remitente de la comunicación sospechosa de ser fraudulenta, es la imagen de **"Loterías, casinos y juegos online"**, seguida del comercio electrónico y las entidades bancarias.

**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 la **entidad bancaria** cuando se trata de **solicitar claves de usuario** (**58,6%**) y enviar invitaciones a **páginas web falsas** (*phishing*) de entidades bancarias, comercio, etc. (**65,8%**).

| 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 | 12,6 | 10,7 | 16,9 | 26,7 | 20,1 | 23,6 | 27,3 | 36,4 | 33,4 | 29,3 | **58,6** | 7,2 |
| Recepción de e-mail ofertando un servicio no solicitado | 6,4 | 13,3 | 15,3 | 27,3 | 21,5 | 30,5 | 25,7 | **46,0** | 42,3 | 22,7 | 31,0 | 6,5 |
| Recepción de e-mail con invitación a visitar alguna página web sospechosa | 6,2 | 14,2 | 13,3 | 29,6 | 18,8 | 24,1 | 24,5 | **39,5** | 35,1 | 21,1 | 34,1 | 6,9 |
| Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa | 7,3 | 16,9 | 15,5 | **40,4** | 18,9 | 22,3 | 23,6 | 39,2 | 32,3 | 20,2 | 33,1 | 6,7 |
| Recepción de productos desde páginas de comercio que pudieran ser falsas | 8,0 | 11,9 | 16,5 | 29,5 | 23,7 | 26,5 | 27,9 | 45,1 | **46,6** | 24,6 | 34,8 | 9,2 |
| Acceso a páginas web falsas de entidades bancarias, comercio o Administraciones | 11,7 | 3,2 | 13,4 | 28,8 | 19,6 | 21,1 | 26,0 | 34,3 | 26,4 | 32,1 | **65,8** | 15,4 |

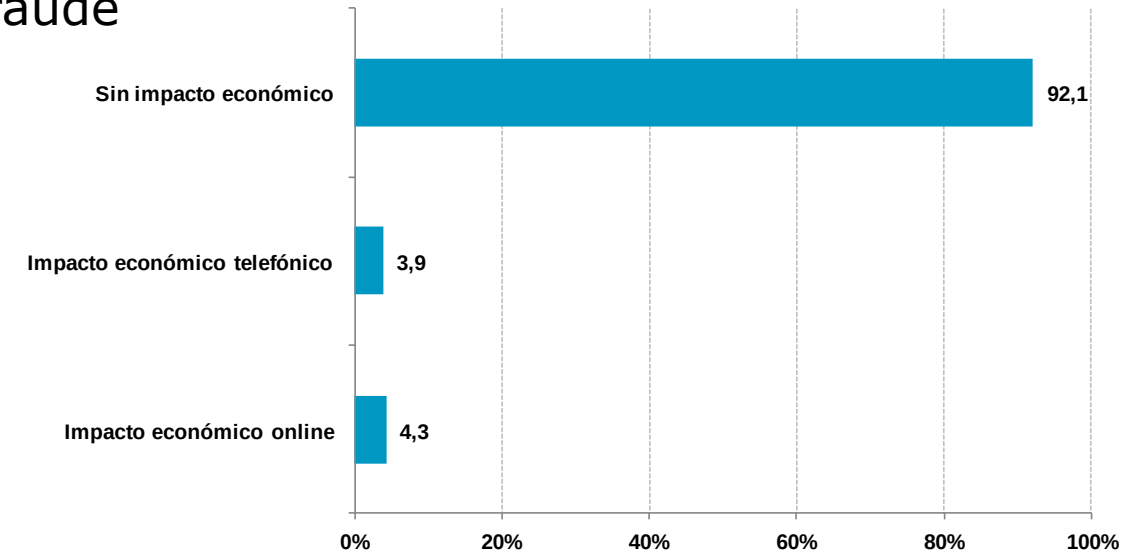
5

[5] Ver nota al pie número 4

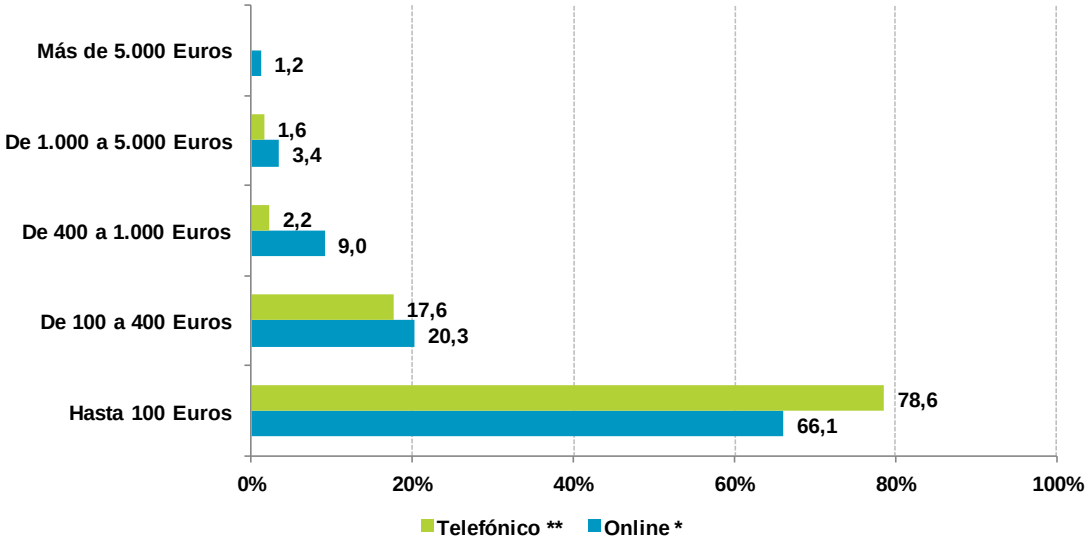
BASE: Usuarios que han sufrido cada tipo concreto de intento de fraude

# Impacto económico del fraude

El impacto económico que supone el fraude es, en la mayoría de los casos (el **92,6%** de los **fraudes telefónicos** y el **88%** de los **fraudes online**), inferior a 400€, coincidiendo con la línea que separa la falta del delito según el Código Penal español.




BASE: Usuarios que han sufrido un intento de fraude




**Distribución del impacto económico**

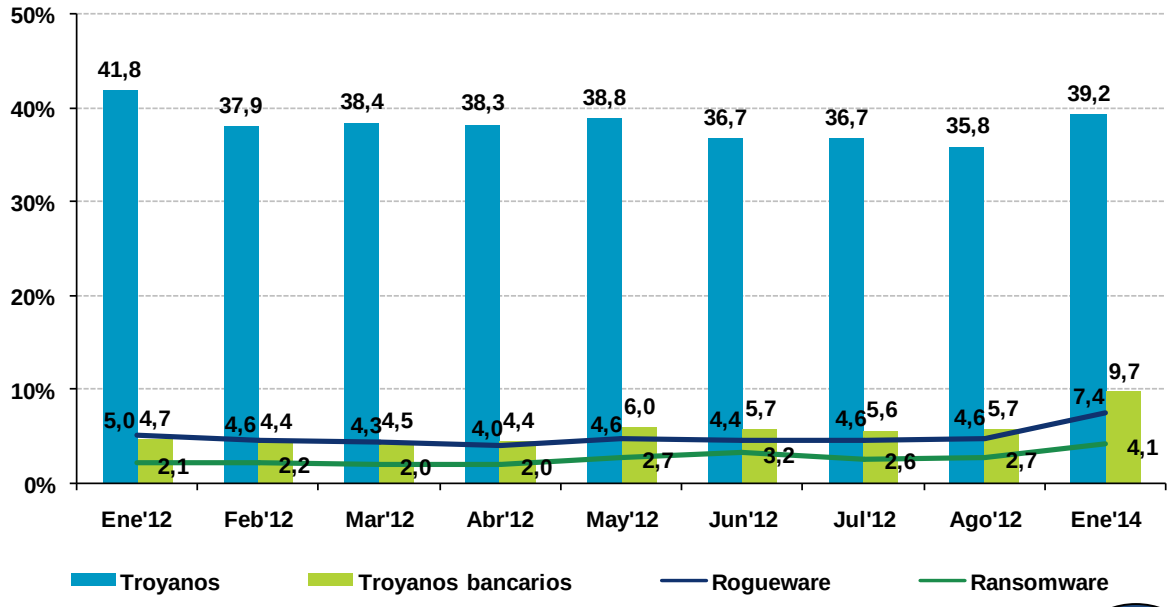
* BASE: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online

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

## Fraude y malware

Los **troyanos bancarios** representan el **9,7%** de las infecciones registradas por iScan en los equipos analizados.

**Evolución de equipos que alojan troyanos bancarios y rogueware**




iScan

BASE: Total equipos

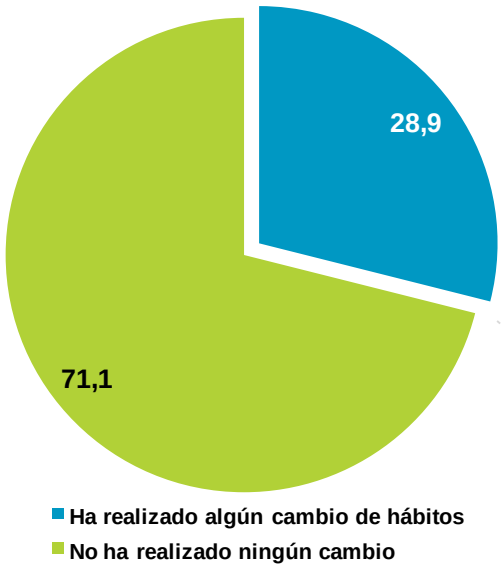
**Tipología del malware analizado**

✓ 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.

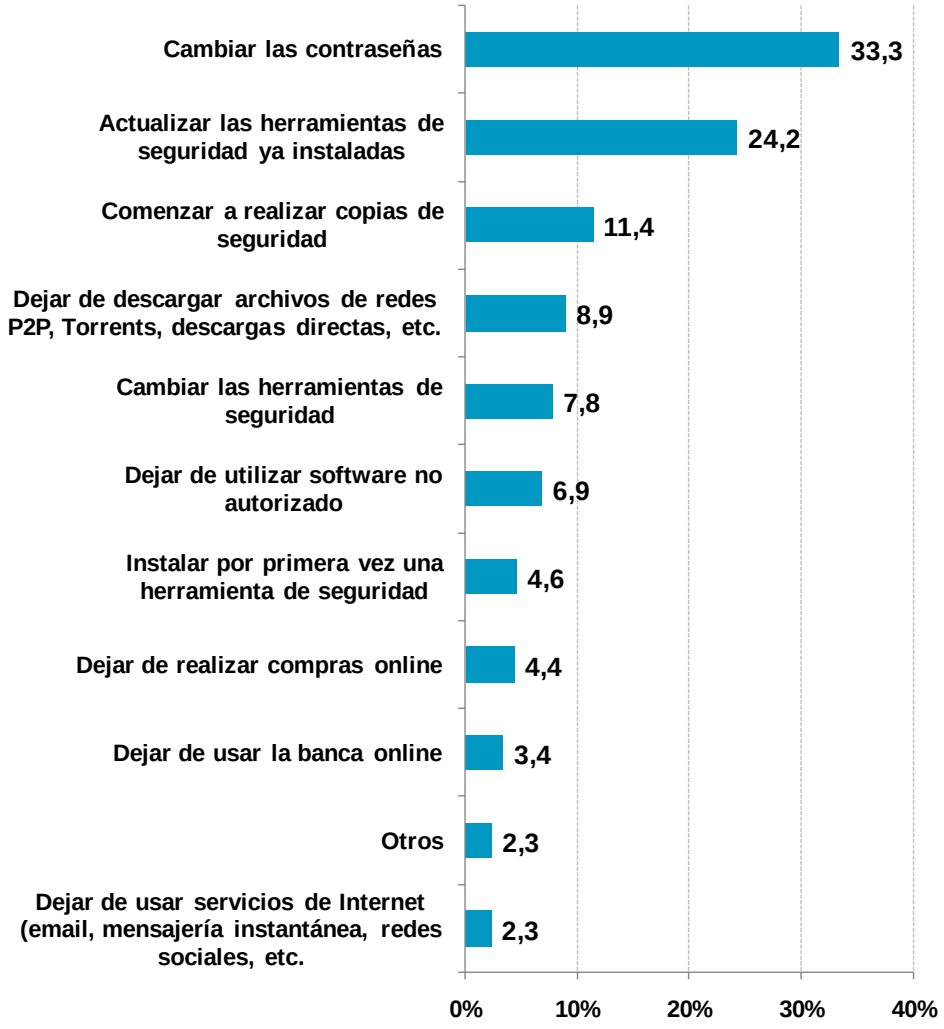
# Cambios adoptados tras un incidente de seguridad




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

El **cambio de contraseñas** se lleva a cabo principalmente (**54%**) ante incidencias de tipo **suplantación de identidad**, y tras sufrir una incidencia de **malware**, el **31,6%** de los usuarios **actualizan las herramientas** de seguridad.



| 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 | 35,2 | 44,5 | 36,8 | 27,4 | **54,0** | 48,5 |
| Actualizar herramientas | **31,6** | 27,0 | 31,5 | 20,8 | 20,5 | 22,8 |
| Realizar copias de seguridad | 13,3 | **18,5** | 15,5 | 9,6 | 14,7 | 17,3 |
| Cambiar herramientas | 12,8 | **17,9** | 13,3 | 6,5 | 14,1 | 16,9 |
| Abandonar software no autorizado | 10,3 | 12,2 | 12,9 | 5,5 | 12,7 | **15,9** |
| Instalar herramientas por 1ª vez | 7,4 | **14,0** | 10,8 | 3,6 | 15,9 | 9,1 |

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

# Cambios adoptados tras un incidente de seguridad

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

Tras una incidencia de **suplantación de identidad** el **13,7%** de usuarios los usuarios abandona el servicio de banca a través de Internet.

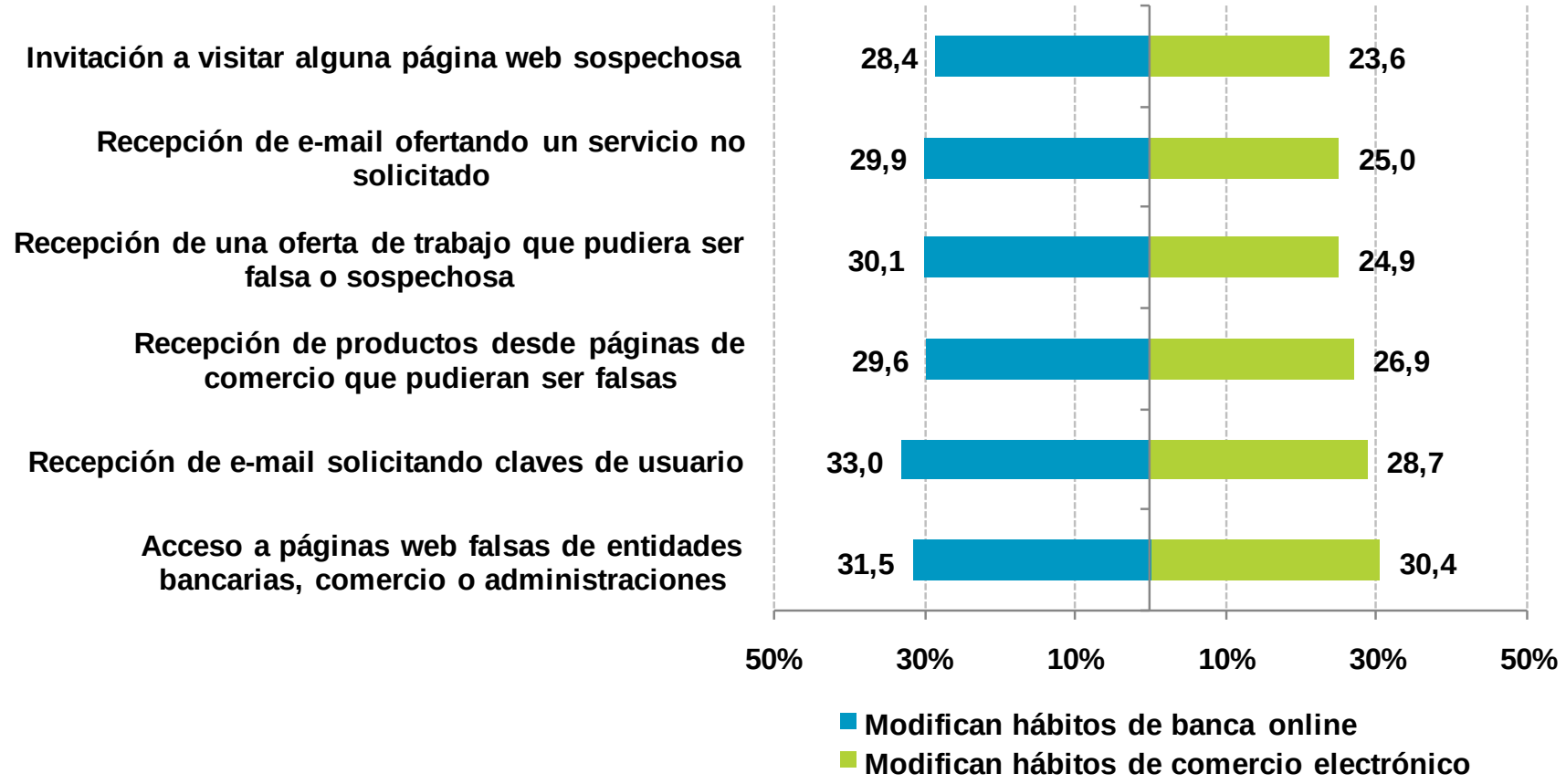
| Cambio en el uso de servicios | Incidencia (%) | | | | | |
|---|---|---|---|---|---|---|
| | Malware | Pérdida de archivos o datos | Servicios inaccesibles debido a ciberataques | Recepción de spam | Suplantación de identidad | Intrusión Wi-Fi |
| Abandonar descargas | 10,3 | 15,7 | 10,1 | 7,5 | 13,7 | **19,2** |
| Abandonar el comercio electrónico | 6,0 | 9,2 | 10,6 | 2,6 | 11,7 | **16,5** |
| Abandonar la banca online | 5,1 | 5,8 | 8,3 | 2,3 | **13,7** | 8,9 |
| Dejar de usar servicios de Internet | 3,1 | 10,4 | 5,0 | 1,0 | 6,7 | **18,2** |



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

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

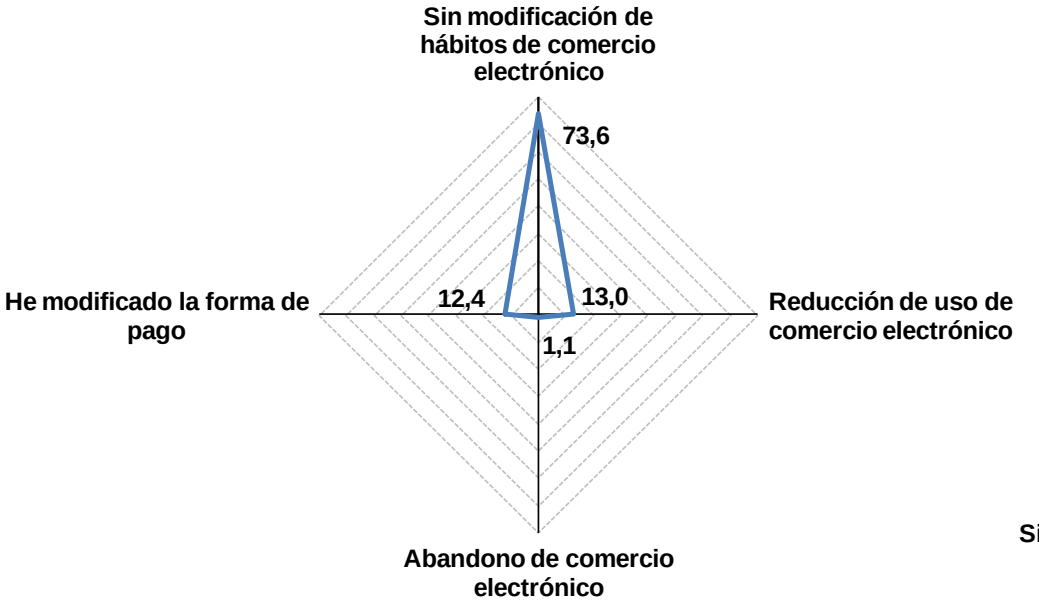
## De forma general un mayor porcentaje de usuarios de banca en línea reaccionan ante un intento de fraude modificando sus hábitos




BASE: Usuarios que han sufrido un intento de fraude

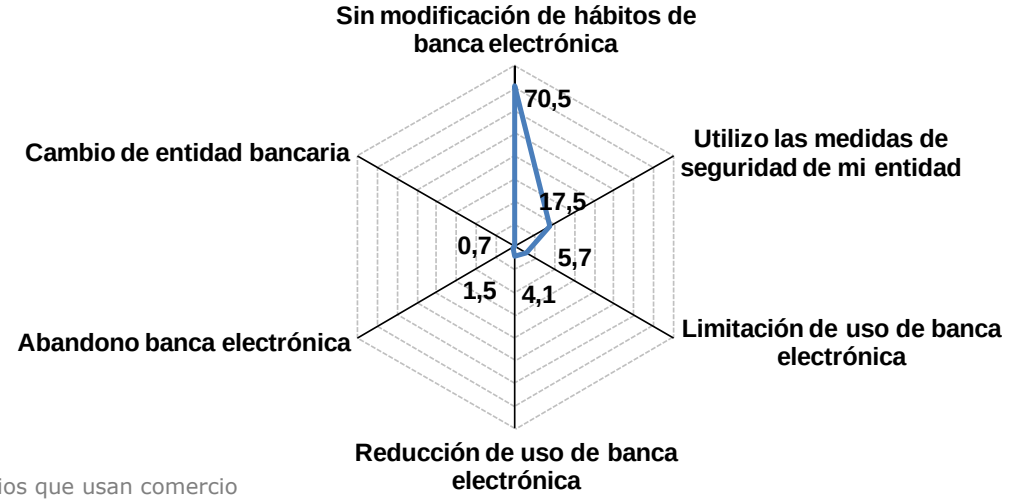
# Cambios adoptados tras un incidente de seguridad

## Modificación de hábitos 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

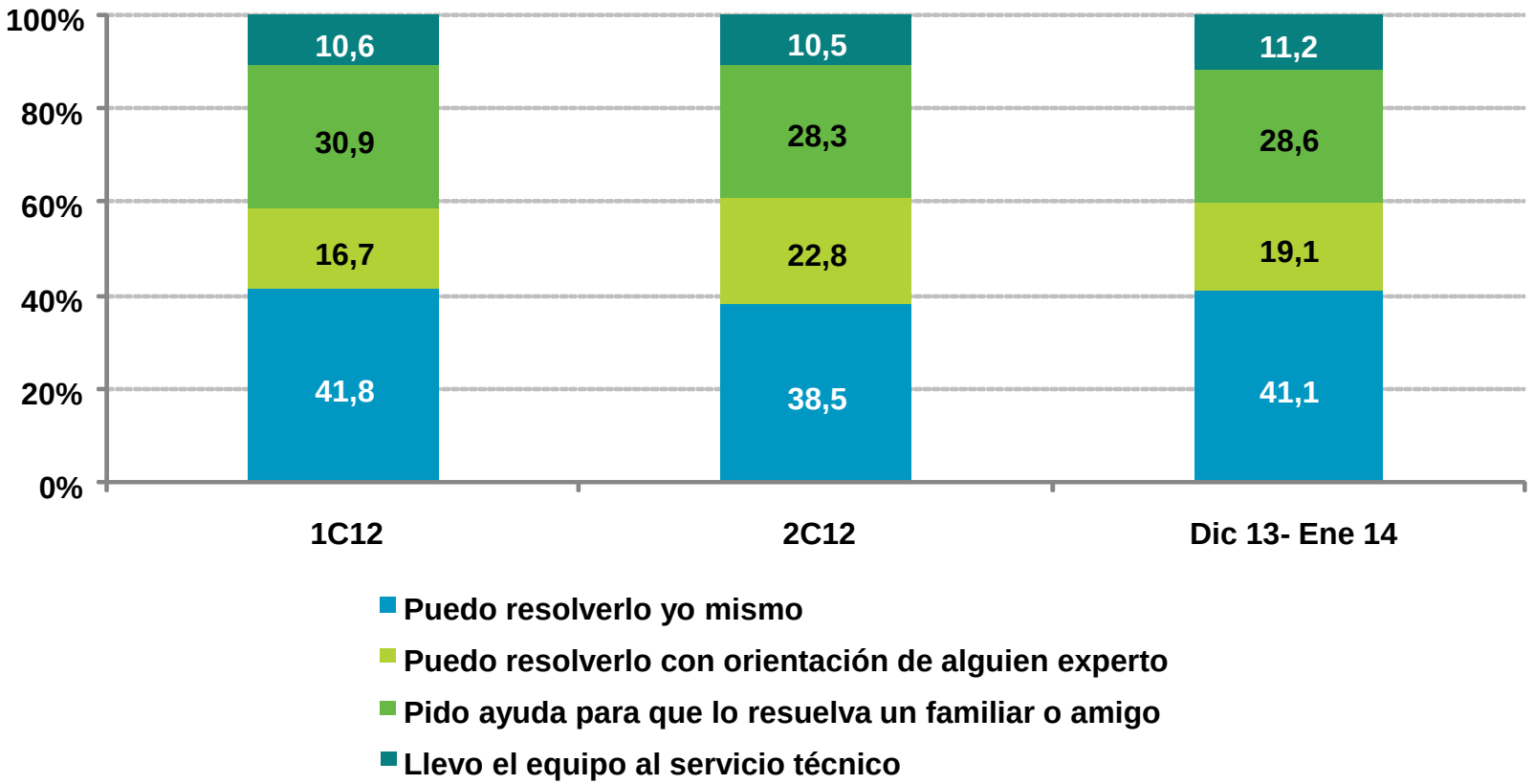



BASE: Usuarios que usan comercio electrónico y han sufrido un intento de fraude

# Resolución de incidentes de seguridad

El 41,1% de los usuarios habituales de Internet confían en solucionar ellos mismos los problemas de seguridad. Además un 19% de los usuarios lo hacen ellos mismos con la orientación de un experto.

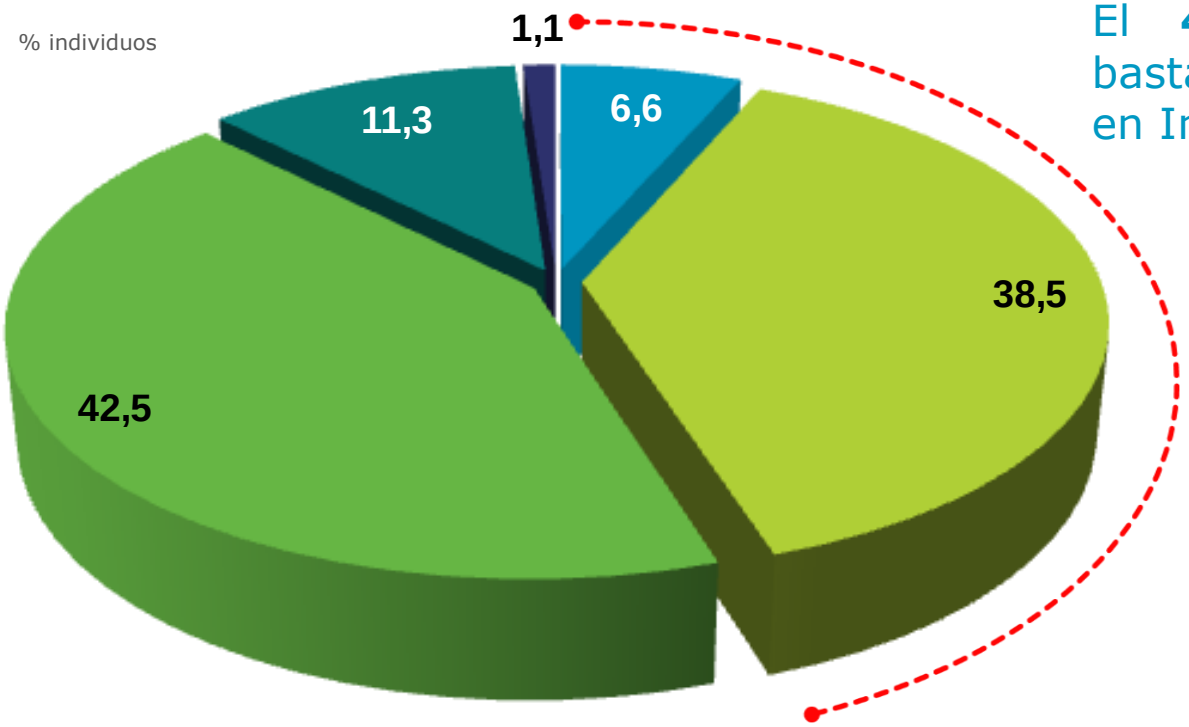
Tan sólo el **11%** acuden a un **servicio técnico profesional** para resolver las incidencias de seguridad.




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

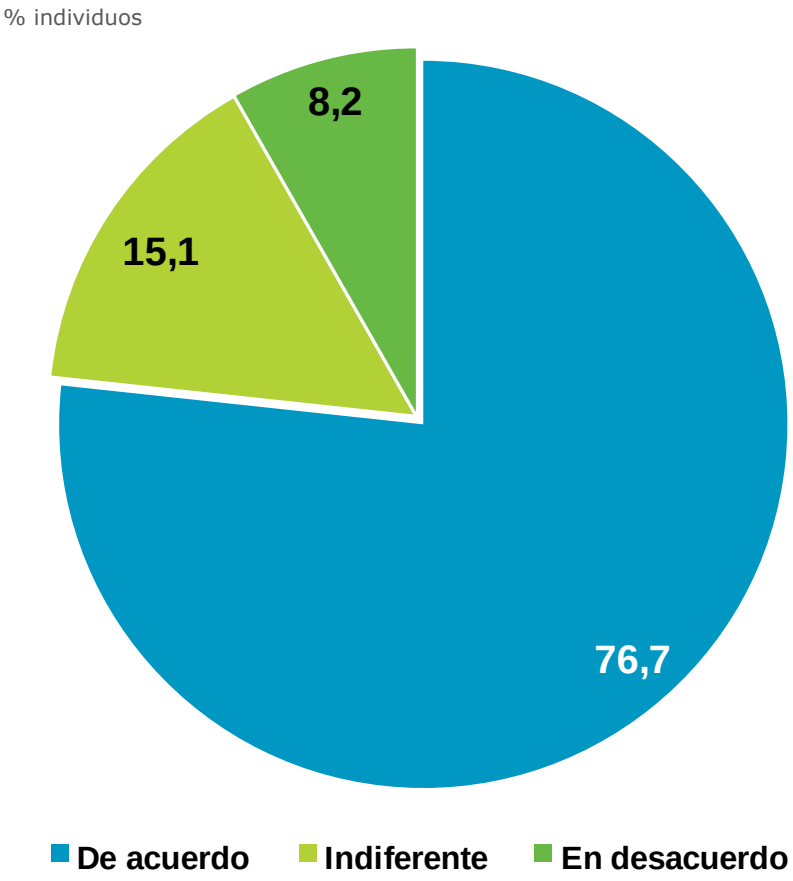



El **45,1%** **confía** bastante o mucho en Internet.

Únicamente al **1%** de los internautas le produce **desconfianza** Internet.

BASE: Total usuarios

# Valoración del ordenador personal como razonablemente protegido

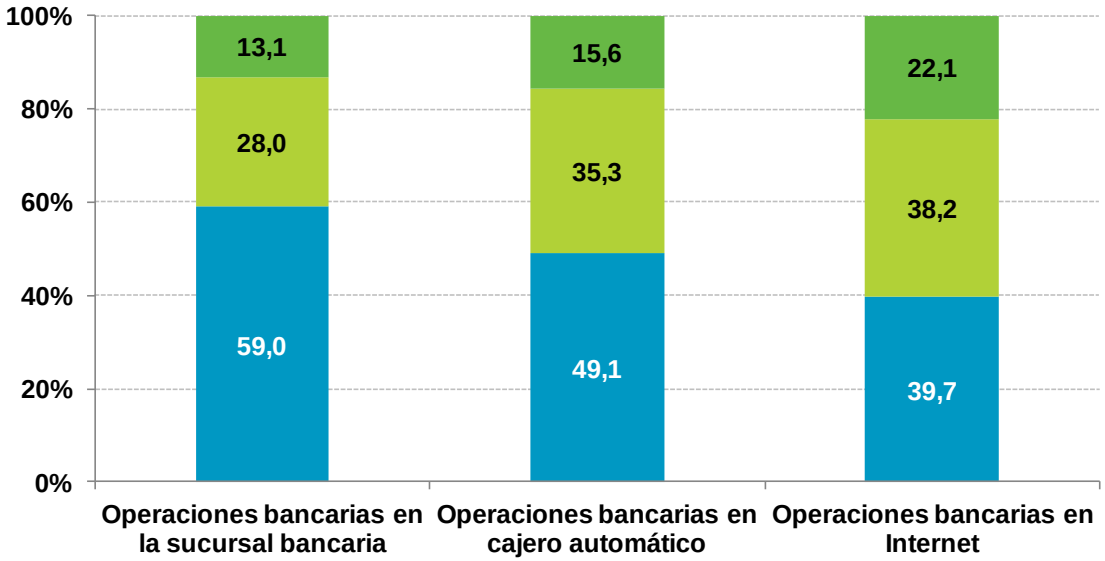



**Tres cuartas partes** de los internautas consideran **disponer de suficiente protección** en el equipo informático del hogar, mientras que al **15%** este hecho le resulta **indiferente**.

6

BASE: Total usuarios

# Confianza online vs. confianza offline




**Nivel de confianza en operaciones bancarias**

De manera general, para el usuario generan más confianza las operaciones en persona que aquellas realizadas a través de Internet.

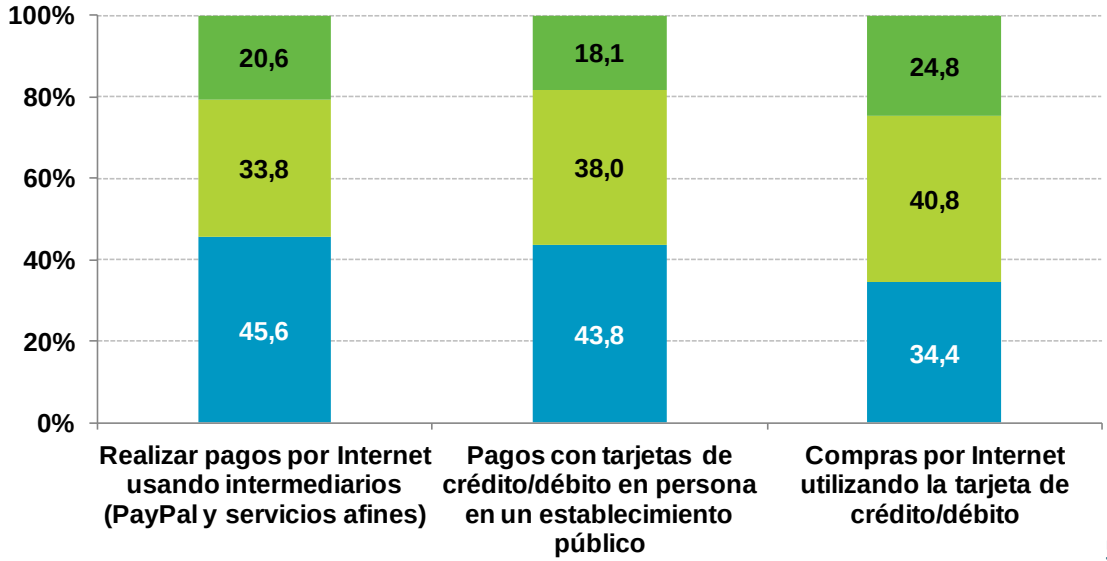
Esta brecha digital es menor en la realización de operaciones de compraventa (9,4%) que en las operaciones bancarias (19,3%).

6

% individuos

**Nivel de confianza en operaciones de compra-venta**

Realizar pagos a través de Internet utilizando intermediarios como Paypal supone una mayor confianza que el pago con tarjeta en un establecimiento público.

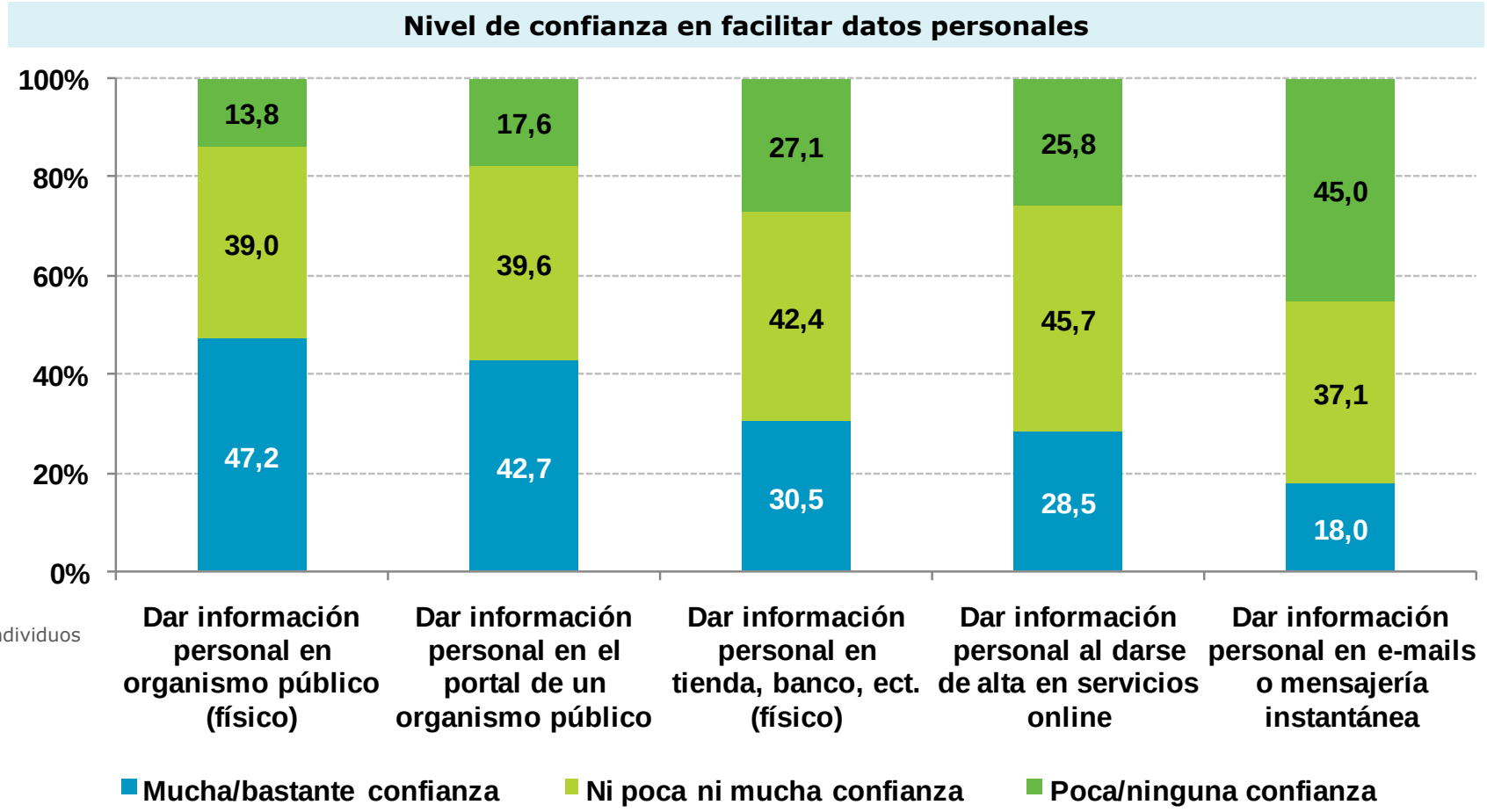



- Mucha/bastante confianza
- Ni poca ni mucha confianza
- Poca/ninguna confianza

BASE: Total usuarios

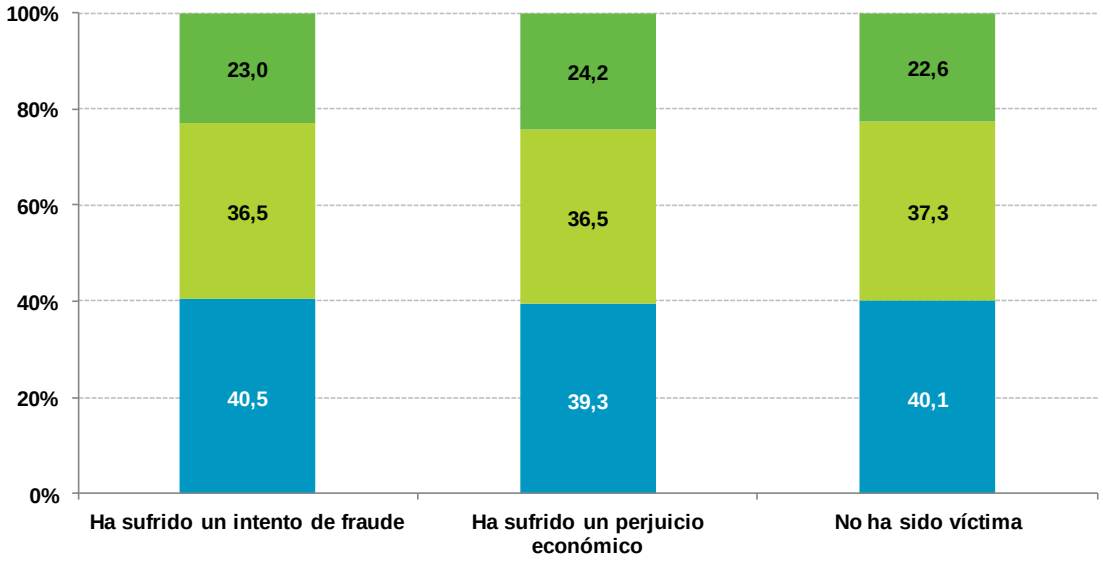
# Confianza online vs. confianza offline

Un **18%** de los internautas tiene bastante o mucha confianza al **facilitar información** de carácter personal mediante un **email, chat o mensajería instantánea**.




BASE: Total usuarios

# Confianza vs. fraude

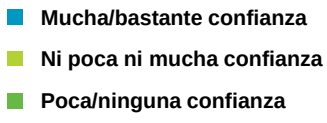



**Confianza al realizar operaciones bancarias en Internet**

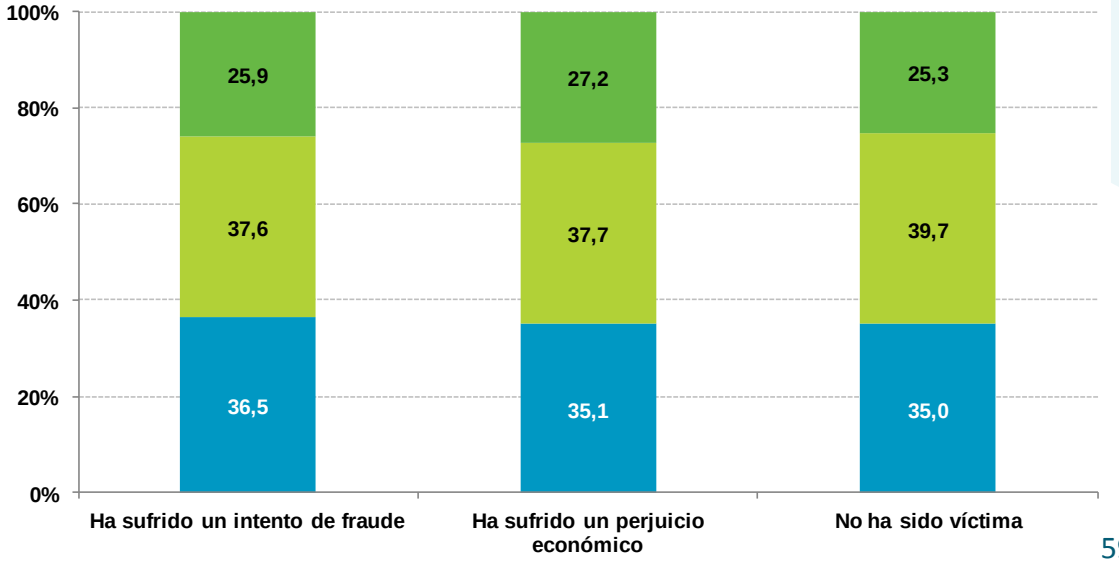
La **confianza** en la banca online y comercio electrónico entre usuarios españoles es alta incluso **tras haber sufrido un intento de fraude**: en torno al **40%** en el caso de la banca en línea y al 36% en comercio electrónico.

6

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




% individuos



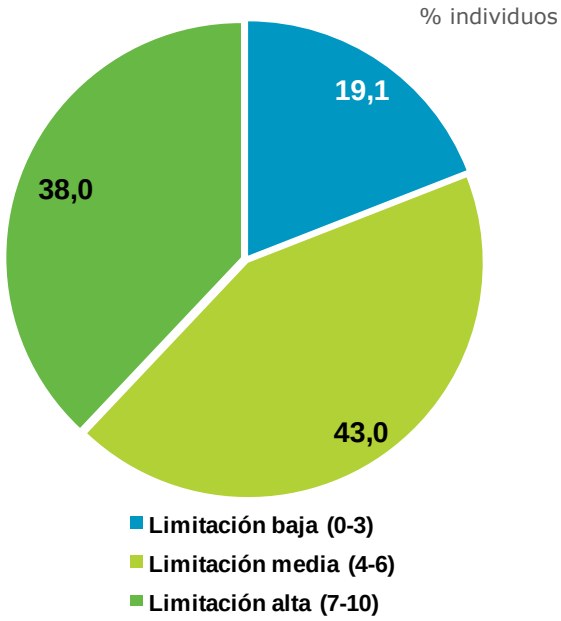

BASE: Usuarios de banca online o comercio electrónico

# Limitación a causa de problemas de seguridad

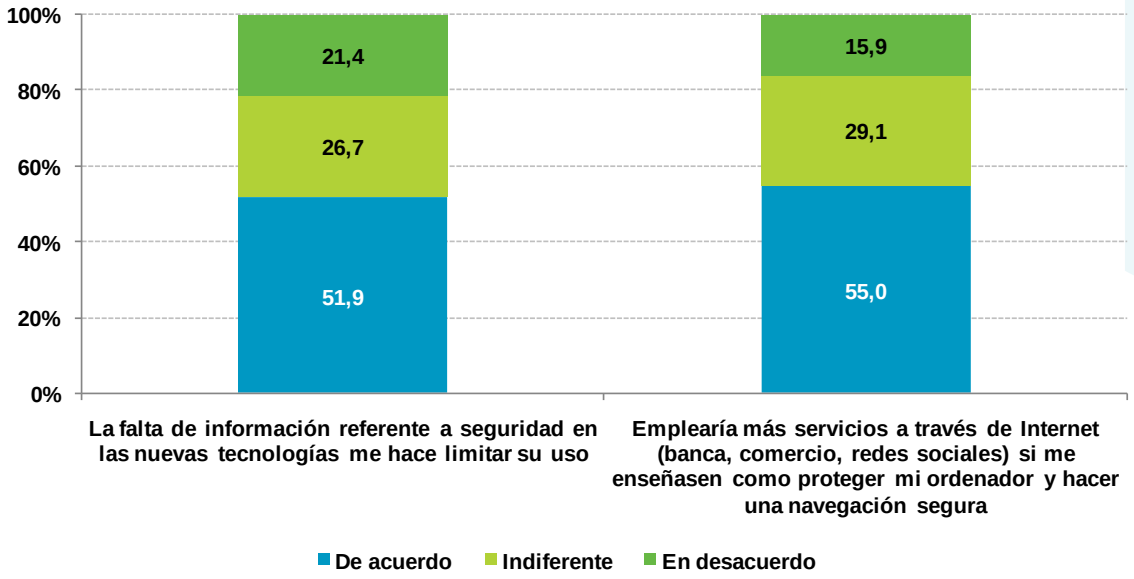
La seguridad supone un **factor limitante importante** para la utilización de nuevos servicios para el **38%** de los panelistas encuestados.

Más de la mitad de los usuarios opinan que estas limitaciones proceden de la **falta de información** (**52%**) referente a seguridad en el uso de las nuevas tecnologías y en la **protección de su ordenador personal** (**55%**).

**Seguridad como factor limitante en la utilización de nuevos servicios**



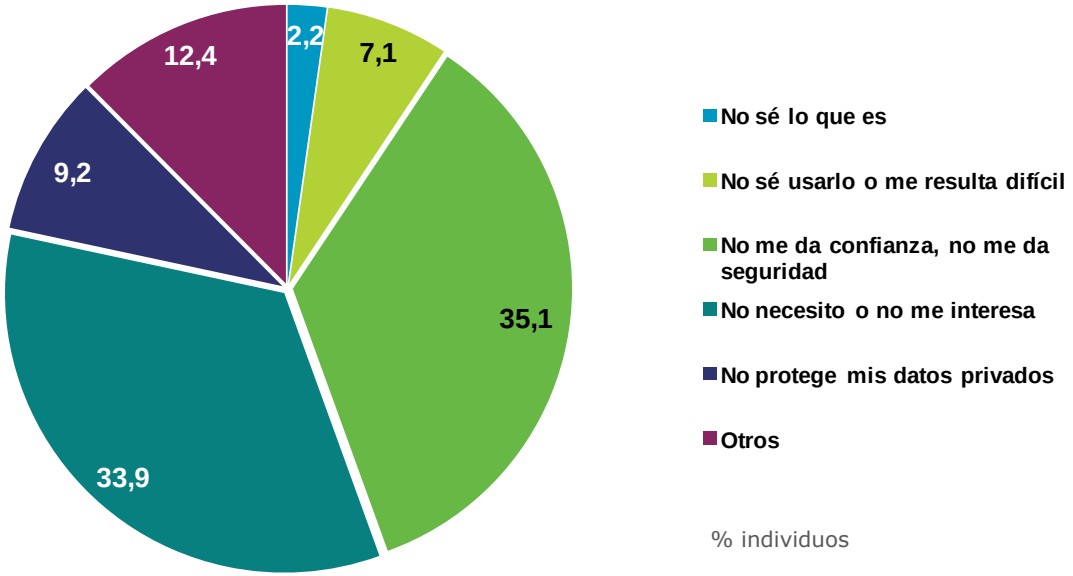

**Limitaciones en el uso de Internet**




BASE: Total usuarios

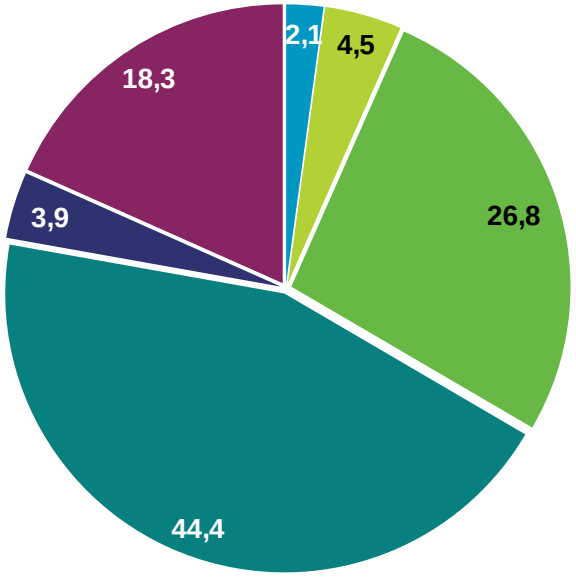
# e-Confianza y limitaciones en la Sociedad de la Información

## Razones para no utilizar banca online




% individuos

## Razones para no utilizar comercio electrónico

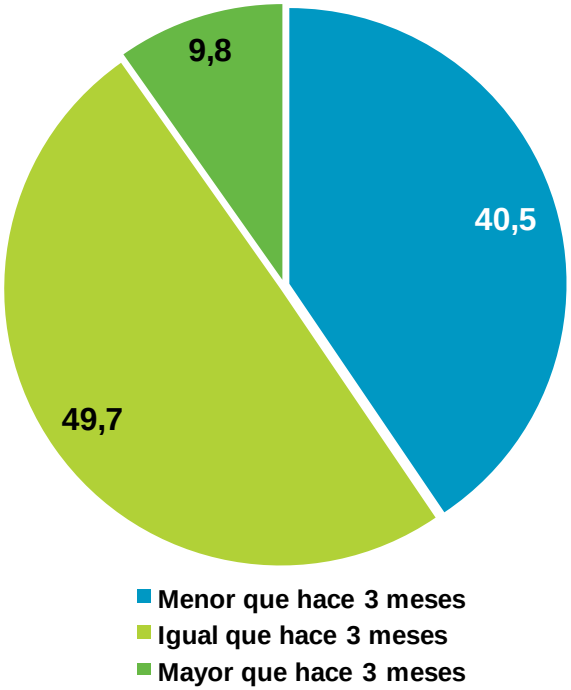



La **falta de confianza en el servicio** es el principal motivo que alegan los usuarios para no utilizar la banca electrónica (**35,1%**), mientras que baja hasta el **26,8%** en el caso del comercio a través de Internet.

BASE : Usuarios que no utilizan el servicio

# Percepción de los usuarios sobre la evolución en seguridad

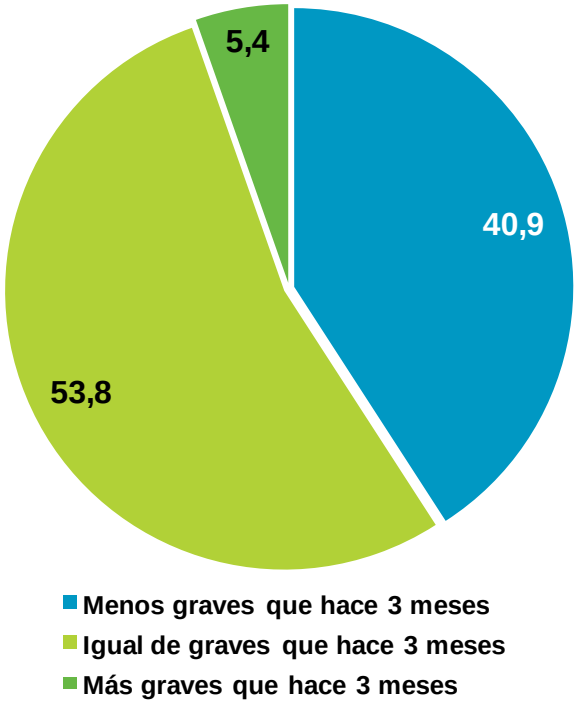
## Número de incidencias




La percepción de los encuestados sobre las incidencias acontecidas en los últimos 3 meses con respecto a meses anteriores es que son **similares en cuanto a cantidad y gravedad** para prácticamente **la mitad**, e incluso **menores** para el **40%.**

## Gravedad de las incidencias

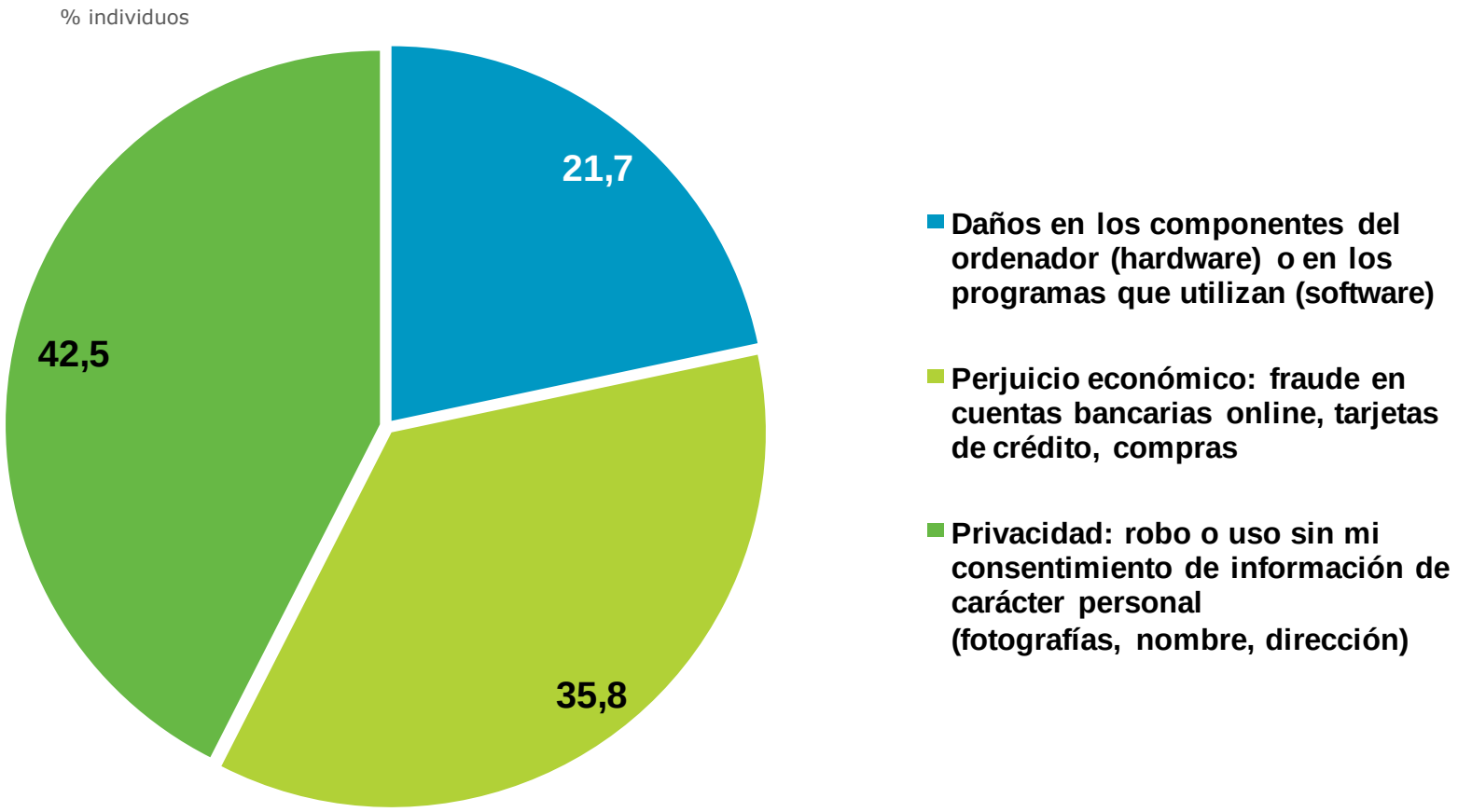
% individuos




BASE: Total usuarios

## Percepción de riesgos en Internet

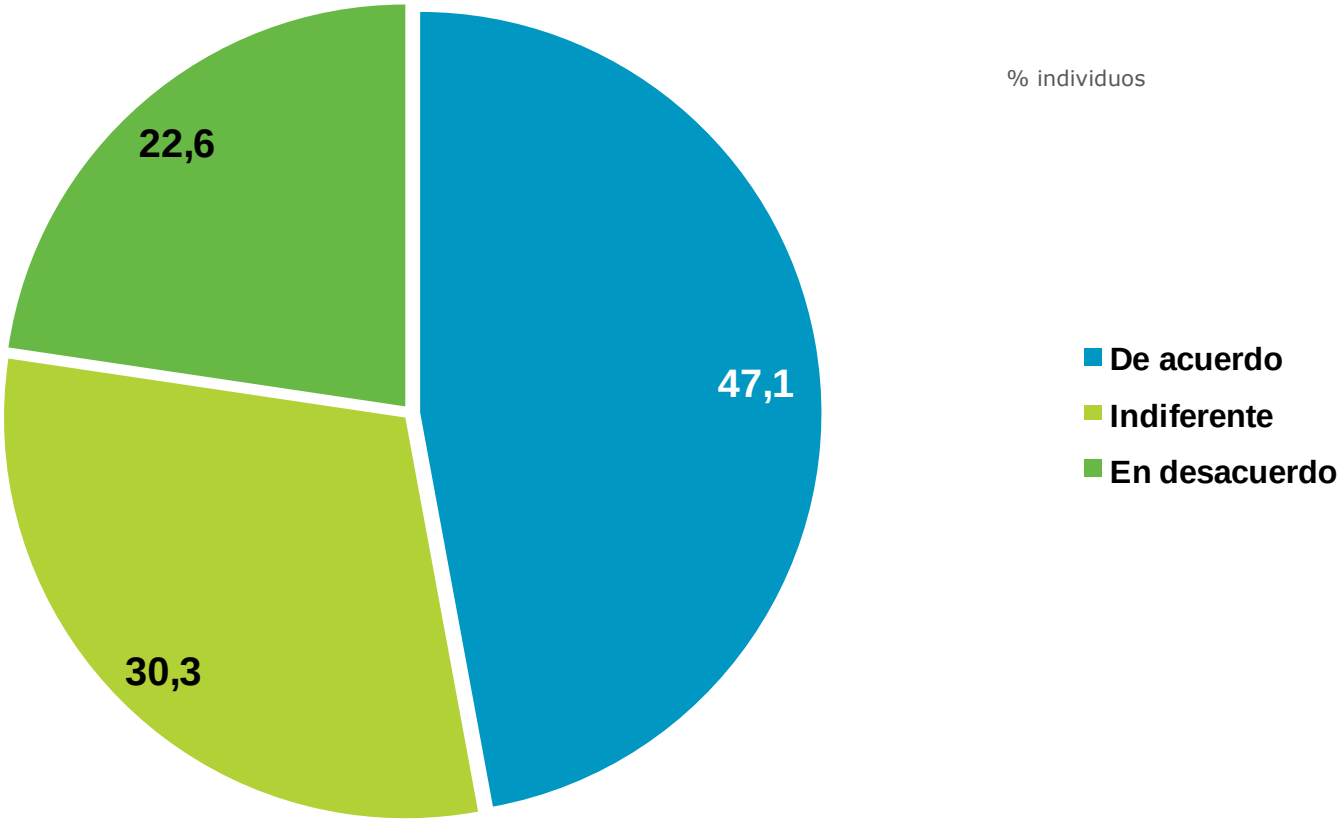
El **mayor riesgo** percibido por los panelistas es el **robo y uso de información personal** (nombre, dirección, fotografías, etc.) sin el consentimiento del usuario.




BASE: Total usuarios

## Valoración de Internet cada día como más seguro

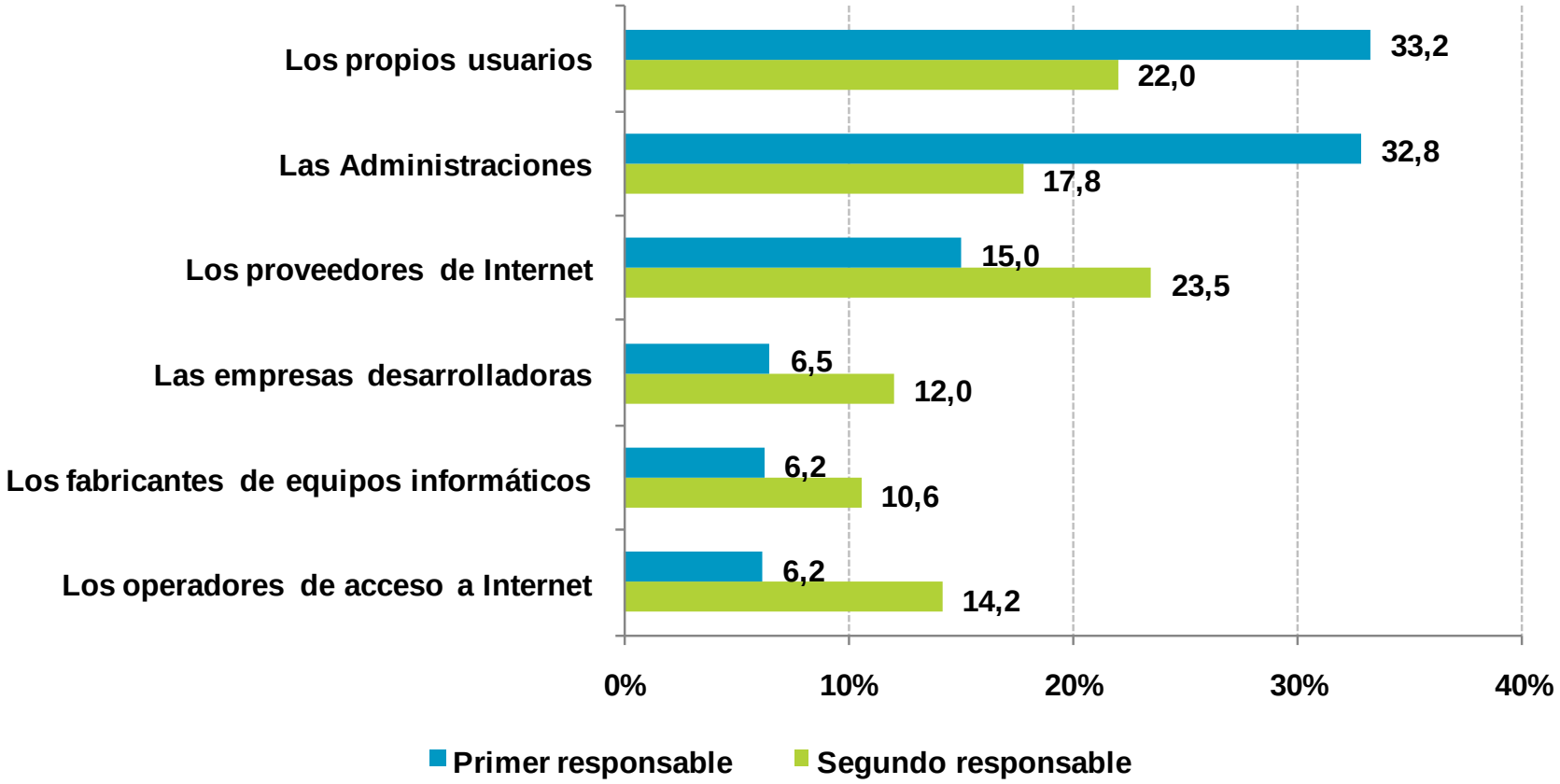
El **47,1%** de los panelistas consideran que **Internet es cada día más seguro**. Sin embargo un **22,6%** se muestran en desacuerdo con tal afirmación.




BASE: Total usuarios

# Responsabilidad en la seguridad de Internet

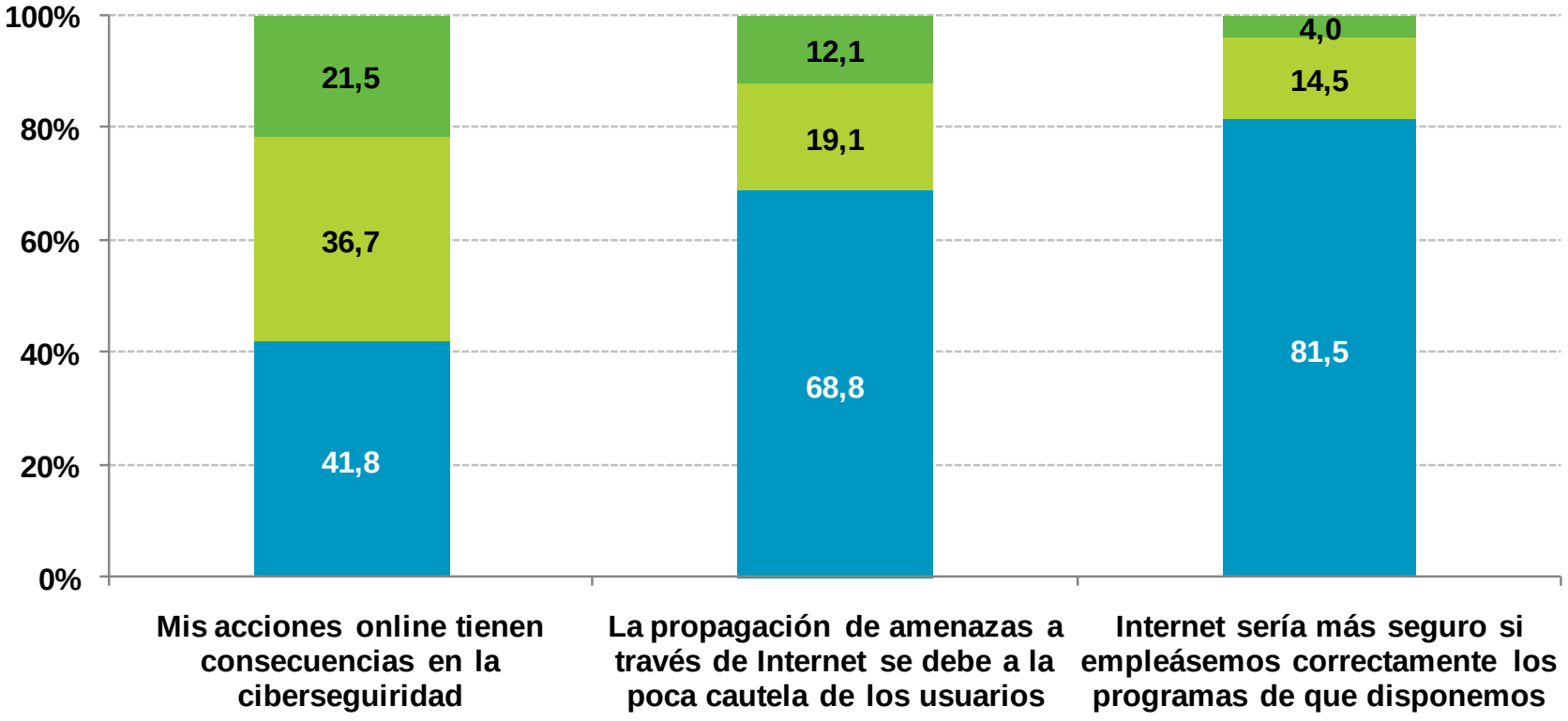
Un **33,2%** de los panelistas asumen la responsabilidad de sus acciones en el uso de Internet y consideran que son **los propios usuarios** los principales responsables de la seguridad en la Red, seguido muy de cerca por el **32,8%** que opinan que **las Administraciones** son las responsables.




BASE: Total usuarios

## Rol del usuario

La mayoría de usuarios (**81,5%**) consideran que Internet sería más seguro **si se empleasen correctamente los programas**. Además casi un **70%** opinan que la propagación de amenazas a través de Internet se debe principalmente a la **poca cautela de los usuarios**. Sin embargo **tan sólo un 42%** creen que sus acciones online tienen **consecuencias en la seguridad**.

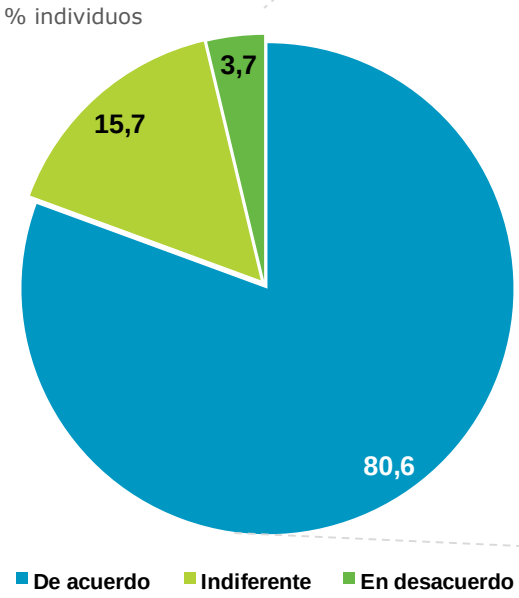



BASE: Total usuarios

# Responsabilidad en la seguridad de Internet

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

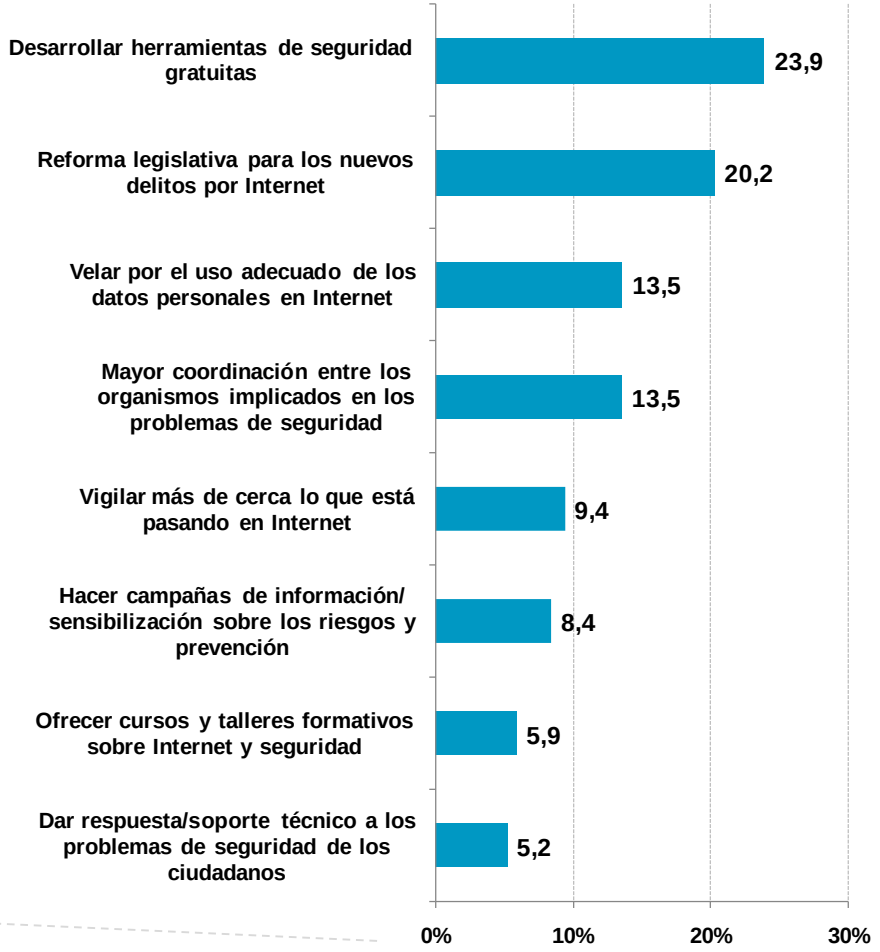
**Ocho de cada diez** internautas considera que la Administración debería implicarse más en mejorar la seguridad en Internet




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

# Conclusiones

## MEDIDAS DE SEGURIDAD

Las principales medidas de seguridad utilizadas de manera real por los panelistas son los programas antivirus (81,2%) y los cortafuegos (77,1%). El dato declarado por los panelistas da un valor similar en cuanto a la utilización de programas antivirus (83,9%), sin embargo da un valor menor para el caso del uso de cortafuegos (44,2%).

Aunque el 59,5% declara instalar actualizaciones del sistema operativo en el ordenador del hogar, el dato real revela que lo hace el 44,2%.

El hecho de no utilizar medidas de seguridad automatizables se debe principalmente al desconocimiento y a la creencia del usuario de su falta de necesidad de la misma. A modo de ejemplo, destaca que el 54,1% de los internautas que no utilizan medidas de seguridad alegan que no lo hacen porque no las necesitan.

## HÁBITOS DE COMPORTAMIENTO EN LA NAVEGACIÓN Y USOS DE INTERNET

El 37,9% de los usuarios opta por modificar la configuración de los programas de seguridad si es necesario para mejorar la experiencia de navegación y uso de Internet.

El 77,9% de los usuarios del correo electrónico declaran no abrir archivos adjuntos si no tienen la certeza de que han sido analizados manual o automáticamente por un antivirus.

El 38,8% de los usuarios de comercio electrónico utiliza tarjetas prepago o monedero para realizar pagos a través de Internet.

## INCIDENTES DE SEGURIDAD

Tres de cada cuatro usuarios de Internet ha tenido algún problema de seguridad en los últimos tres meses, de los que el 88,4% ha recibido correos electrónicos no solicitados/deseados (spam).

Aumenta el porcentaje de equipos que han tenido infección, el dato real revela que el 59,8% de los equipos están infectados mientras que el dato declarado o percibido por los internautas es del 25,9%.

El 36,6% de los usuarios de smartphone ha tenido alguna incidencia de seguridad en su terminal siendo la recepción de correos no deseados (spam) la principal.

# Conclusiones

## CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

Tras un incidente de seguridad, el 28,9% de los usuarios ha realizado algún cambio en sus hábitos de uso y así, el 33,3% de ellos ha cambiado contraseñas y el 24,2% ha actualizado las herramientas de seguridad ya instaladas.

El 53,7% de los usuarios ha sufrido alguna situación de fraude; por ejemplo, el 59,8% de estos ha sido invitado a visitar alguna página web sospechosa, el 53,3% ha recibido un e-mail ofertando un servicio no deseado o el 43,9% recibió una oferta de trabajo falsa o sospechosa.

Las principales consecuencias tras una incidencia de seguridad en el dispositivo móvil son el perjuicio económico (43,9%) y la suscripción a servicios no solicitados (50,2%).

El 41,1% de los usuarios habituales de Internet confían en solucionar ellos mismos los problemas de seguridad. Además un 19% de los usuarios lo hacen ellos mismos con la orientación de un experto.

## CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

El 45,1% de los internautas declara tener mucha o bastante confianza en Internet, sin embargo a la hora de utilizar servicios concretos como el de la banca online se detecta que un 35,1% de usuarios declara no usar el servicio porque no le da confianza o no lo ve seguro.

El 76,7% de los internautas considera que su ordenador está razonablemente protegido, un 8,2% piensa que no lo está, mientras que el 15,1% no le da importancia a este hecho.

A la hora de facilitar información personal a través de e-mail o mensajería instantánea, un 45% de usuarios se muestra desconfiado, mientras que el 18% declara tener mucha o bastante confianza.

# Alcance del estudio

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 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 mayores de 15 años con acceso frecuente a Internet desde el hogar (al menos una vez al mes).

**Tamaño Muestral:** 3.074 hogares encuestados y de ellos, 2.127 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 diciembre de 2013 y enero 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=3.074 le corresponde una estimación del error muestral igual a ±1,77%.

Nota: Debido a innovaciones metodológicas realizadas para el presente estudio, algunos datos pueden sufrir alteraciones con respecto a anteriores publicaciones.

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