Estudio sobre la Ciberseguridad y Confianza en los hogares españoles

Abril – Junio 2014

INDICE

Introducción al estudio

1. **Presentación**
2. **Objetivos**

Presentación

El Instituto Nacional de Ciberseguridad (INCIBE) 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 INCIBE, 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 abril hasta junio de 2014**. Los informes previos a este, y disponibles en las direcciones:

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

http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares-españoles-octubre-2014, abarca el análisis desde febrero a marzo 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

2

Definición y clasificación de las medidas de seguridad

2

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 que te ayudarán a proteger tus dispositivos: http://www.osi.es/herramientas-gratuitas

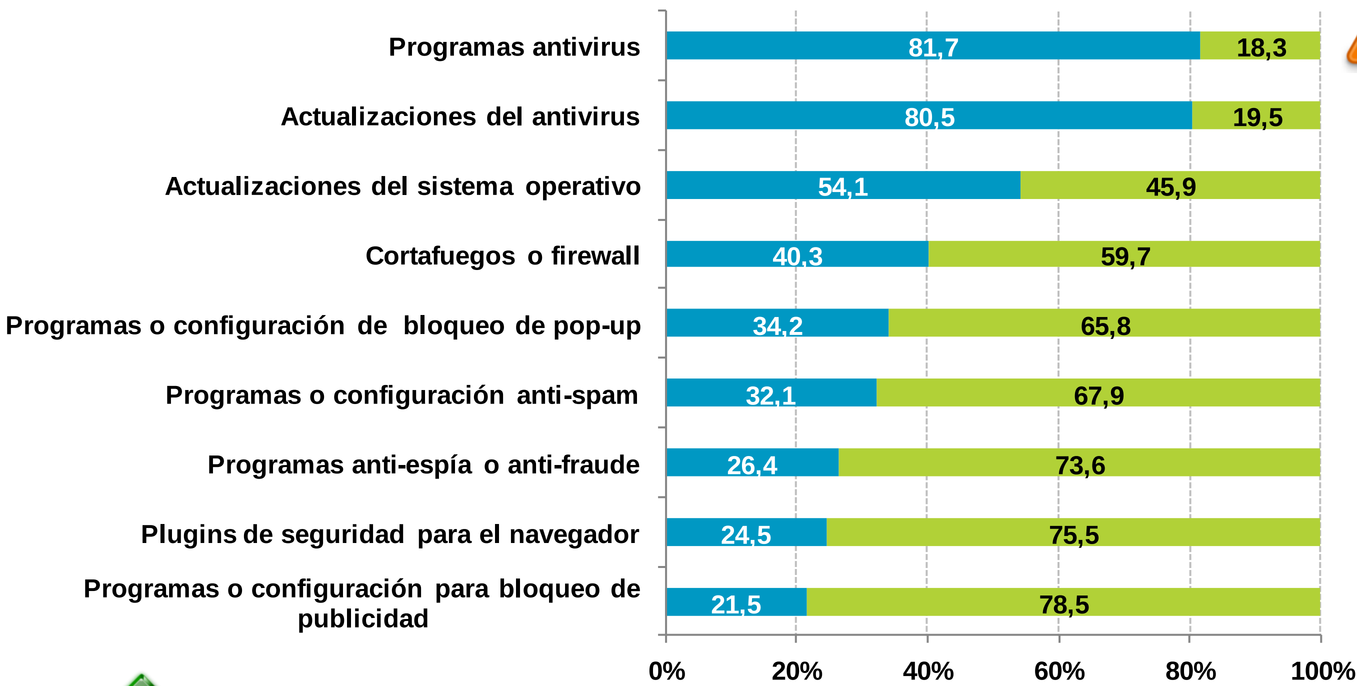
[2] Existen medidas de seguridad que por su condición se pueden clasificar en ambas categorías, tal es el caso de los programas antivirus y sus actualizaciones, o las del sistema operativo.
Un programa antivirus, por su naturaleza puede detectar tantos las amenazas existentes en el equipo como las amenazas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

Medidas de seguridad automatizables[1]

Destacan como principales medidas de seguridad automatizables el **software antivirus** (**81,7%**) y sus **actualizaciones** (**80,5%**).



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**.

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

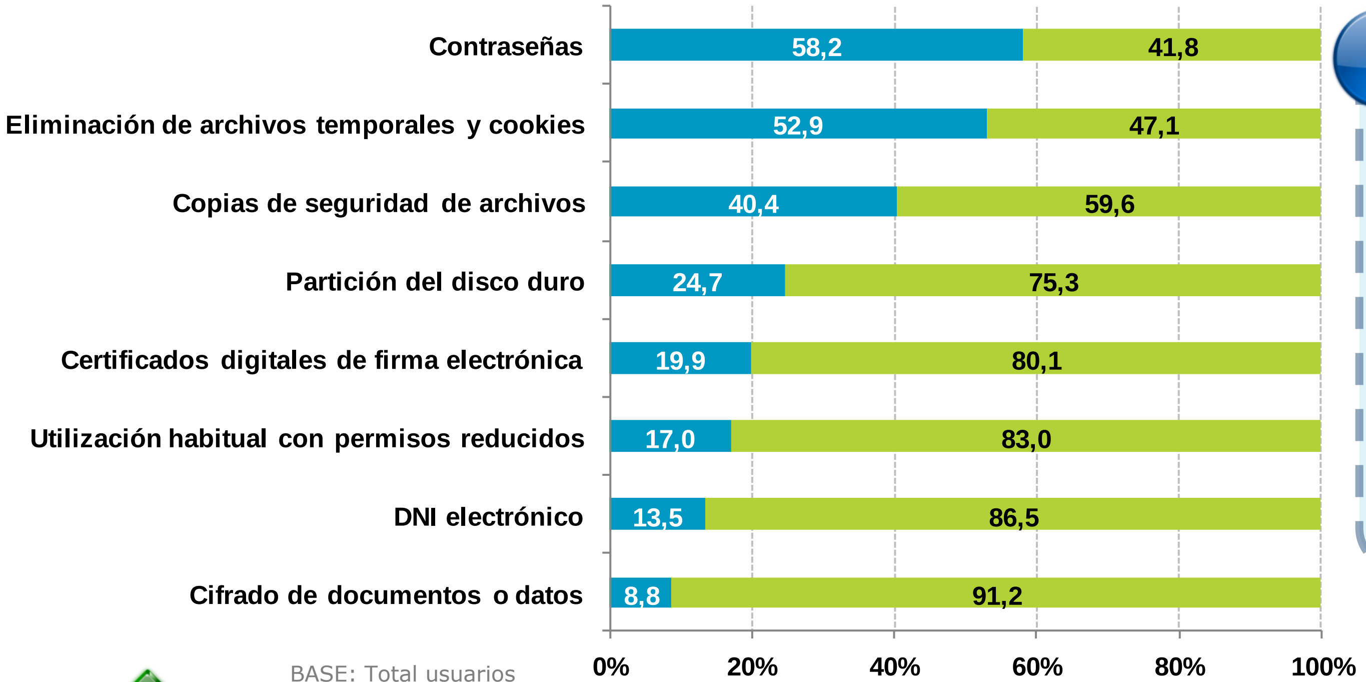
BASE: Total usuarios

Información para conocer las medidas de seguridad: INCIBE pone a tu disposición la Oficina de Seguridad del Internauta (www.osi.es), donde encontrarás 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 (81,7%).

Medidas de seguridad no automatizables o activas

Casi el 60% de los usuarios declaran utilizar **contraseñas** para proteger su equipo y/o documentos, y más de la mitad (**52,9%**) se preocupan por eliminar los **archivos temporales y cookies** generados durante la navegación a través de la red.



BASE: Total usuarios

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

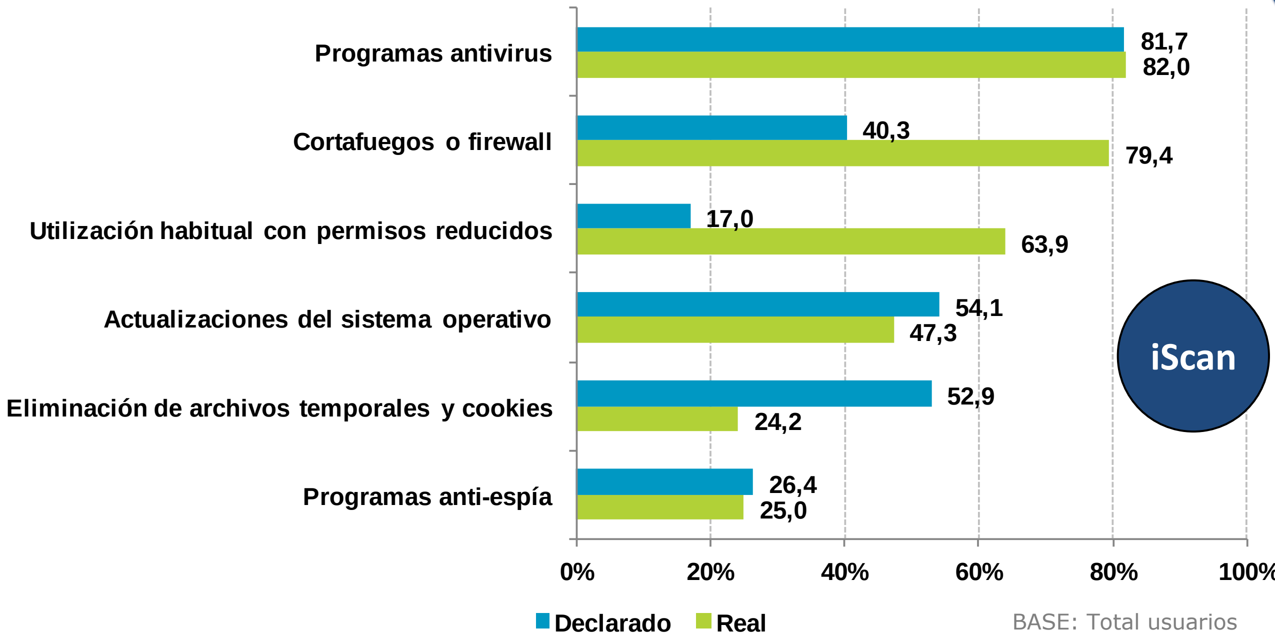
Son las principales medidas en cuanto a seguridad física se refiere así como cuando las medidas automatizables son eludidas.

Es muy importante gestionar correctamente las contraseñas y además, realizar copias de seguridad de los datos que queremos salvaguardar. Obtén más información sobre cómo realizar estas tareas:

- ✓ **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

El **17%** de los internautas encuestados declara el uso habitual de un **usuario con permisos reducidos** en el ordenador del hogar. Sin embargo, el dato real obtenido con iScan revela que el **63,9%** tiene una cuenta con **permisos limitados**.



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

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

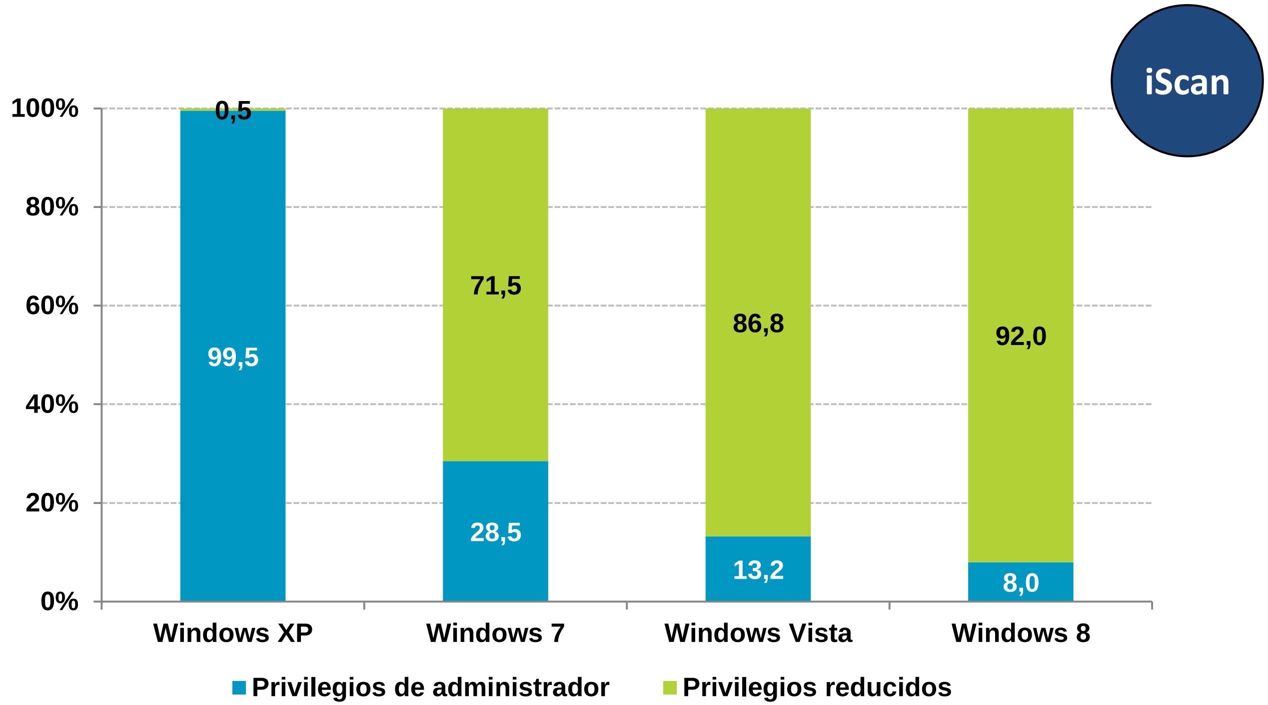
https://www.osi.es/es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

Para la obtención del dato real, se utiliza el software **iScan** desarrollado por INCIBE, 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 real de perfiles según nivel de privilegios en sistemas operativos Windows:

La diferencia entre el nivel de privilegios usado en las distintas versiones de los sistemas operativos de Microsoft se debe a la configuración por defecto aplicada a la cuenta de usuario.



BASE: Total usuarios de Microsoft Windows

Utiliza la cuenta de usuario estándar para el uso diario del ordenador. Haz uso de la cuenta de administrador sólo cuando sea estrictamente necesario. Más información sobre las cuentas de usuario y cómo configurarlas en: http://www.osi.es/cuentas-de-usuario

Motivos alegados para no utilizar medidas de seguridad

La falta de necesidad es el principal argumento entre aquellos usuarios que no utilizan medidas de seguridad automatizables. Únicamente en el caso de los **programas o configuración para bloquear la publicidad** y los **plugins de seguridad para el navegador**, el **desconocimiento** acerca de dichas herramientas supera a esta razón.

Medidas	Hogares que no utilizan en la actualidad (%) *	Motivos (%) **						
		No conoce	No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros
Programas antivirus	18,3	8,9	**28,7**	18,9	13,0	5,0	8,1	17,4
Actualizaciones antivirus[2]	19,5	7,1	**32,1**	22,8	6,4	2,3	4,8	24,4
Actualizaciones del sistema operativo	45,9	11,1	**33,8**	11,4	11,2	5,9	2,2	24,4
Cortafuegos o firewall	59,7	21,8	**27,6**	9,9	14,2	5,4	3,9	17,2
Programas o configuración de bloqueo de pop-up	65,8	23,9	**32,1**	6,1	13,1	7,1	3,9	13,8
Programas o configuración anti-spam	67,9	19,4	**34,9**	8,1	10,9	7,5	4,5	14,7
Programas anti-espía o anti-fraude	73,6	21,7	**30,0**	11,1	10,4	8,2	4,0	14,6
Plugins de seguridad para el navegador	75,5	**30,2**	29,3	5,8	12,7	6,8	2,8	12,4
Programas o configuración para bloqueo de publicidad	78,5	**33,0**	27,6	5,8	10,5	8,3	3,1	11,7

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

Información para conocer las medidas de seguridad: INCIBE pone a tu disposición la Oficina de Seguridad del Internauta (www.osi.es), donde encontrarás 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

Más del 40% no utiliza medidas de seguridad activas al considerar que **no son necesarias**. Destaca casi el **54%** de los usuarios que, por este motivo, **no utiliza contraseñas** para proteger el equipo y documentos en la actualidad.

2

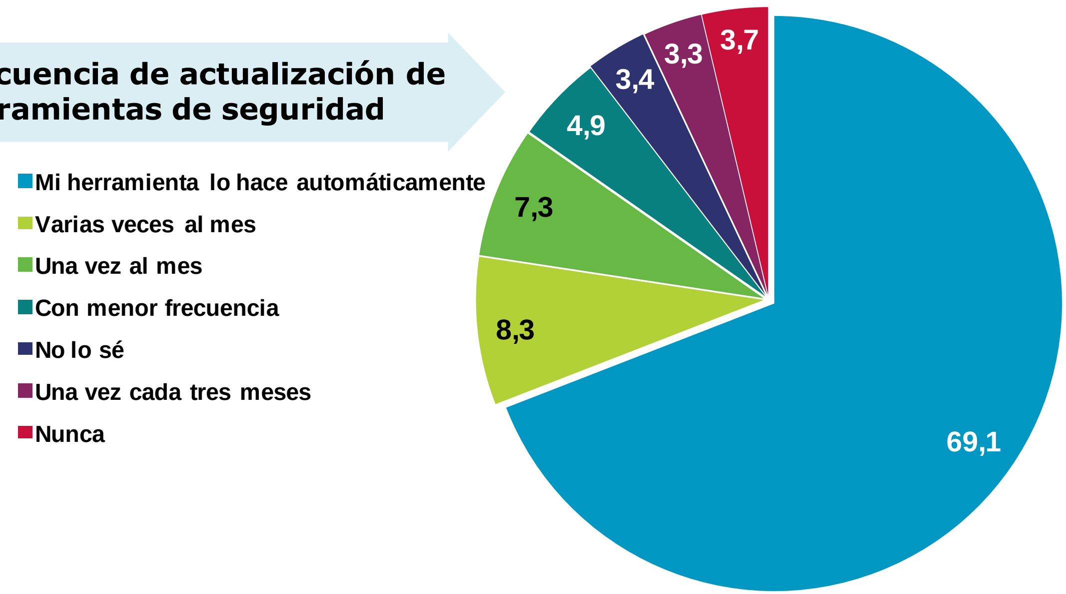
Medidas	Hogares que no utilizan en la actualidad (%) *	Motivos (%) **					
		No conoce	No necesita	Entorpecen	Desconfía	Ineficaces	Otros
Contraseñas (equipos y documentos)	41,8	10,7	**53,8**	9,9	5,9	3,8	15,9
Eliminación archivos temporales y cookies	47,1	21,7	**40,0**	8,5	6,3	4,1	19,4
Copia de seguridad de archivos	59,6	15,5	**45,5**	6,3	5,4	2,8	24,5
Partición del disco duro	75,3	24,1	**45,3**	7,1	4,3	1,9	17,3
Certificados digitales de firma electrónica	80,1	20,1	**49,8**	4,1	6,1	2,1	17,8
Utilización habitual con permisos reducidos	83,0	19,2	**49,6**	9,4	4,0	2,6	15,2
DNI electrónico	86,5	9,6	**51,9**	4,3	6,4	2,3	25,5
Cifrado de documentos o datos	91,2	31,9	**45,0**	5,9	4,2	1,3	11,7

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

Frecuencia de actualización y utilización

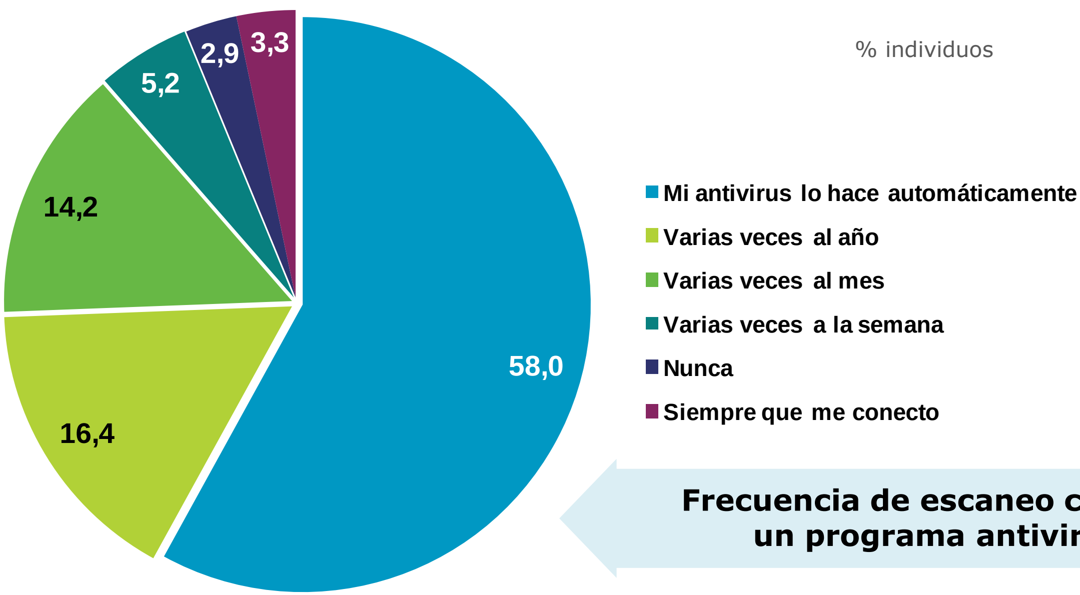
El **69,1%** de los usuarios permite que la **frecuencia de actualización** de las herramientas de seguridad sea determinada de forma **automática** por las propias herramientas.

Frecuencia de actualización de herramientas de seguridad



% individuos

BASE: Total usuarios



Frecuencia de escaneo con un programa antivirus

Un **58% delega** en el programa antivirus la **frecuencia de escaneo** de su equipo para detectar infecciones.

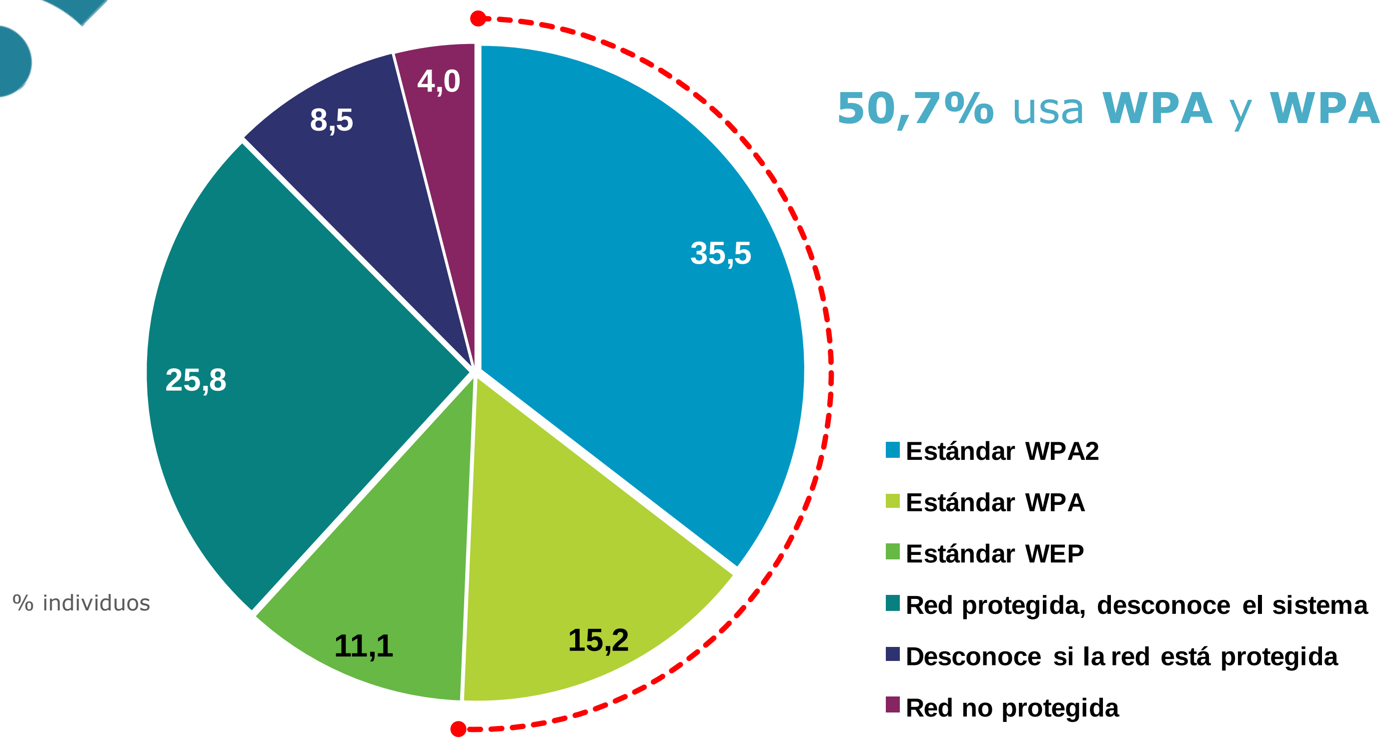
BASE: Usuarios que utilizan programas antivirus

Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi

2

Un **12,5%** de los usuarios deja su red inalámbrica Wi-Fi **desprotegida** y/o **desconoce** su estado.

50,7% usa **WPA** y **WPA2**



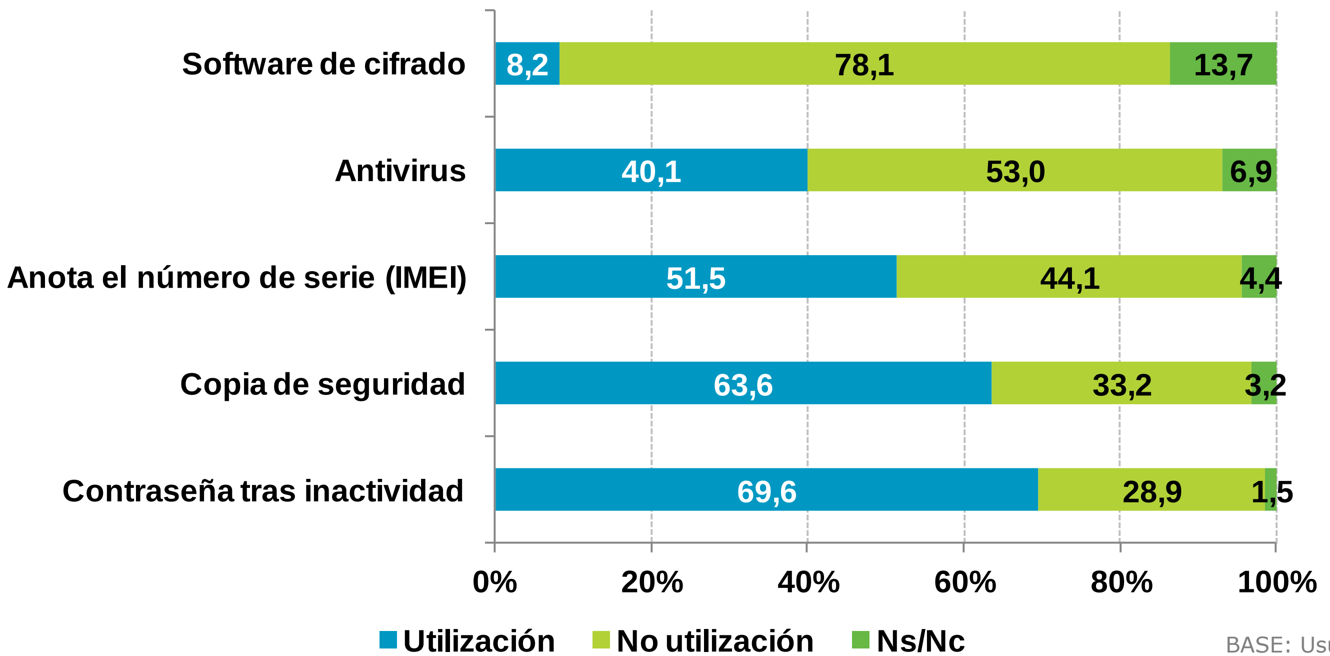
BASE: Usuarios Wi-Fi con conexión propia

Cómo configurar tu red Wi-Fi de modo seguro: http://www.osi.es/protege-tu-wifi

Medidas de seguridad utilizadas en smartphones

Únicamente un **8,2%** declara utilizar **software de cifrado** en su terminal móvil para evitar que la información que contienen sea accesible por terceros 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



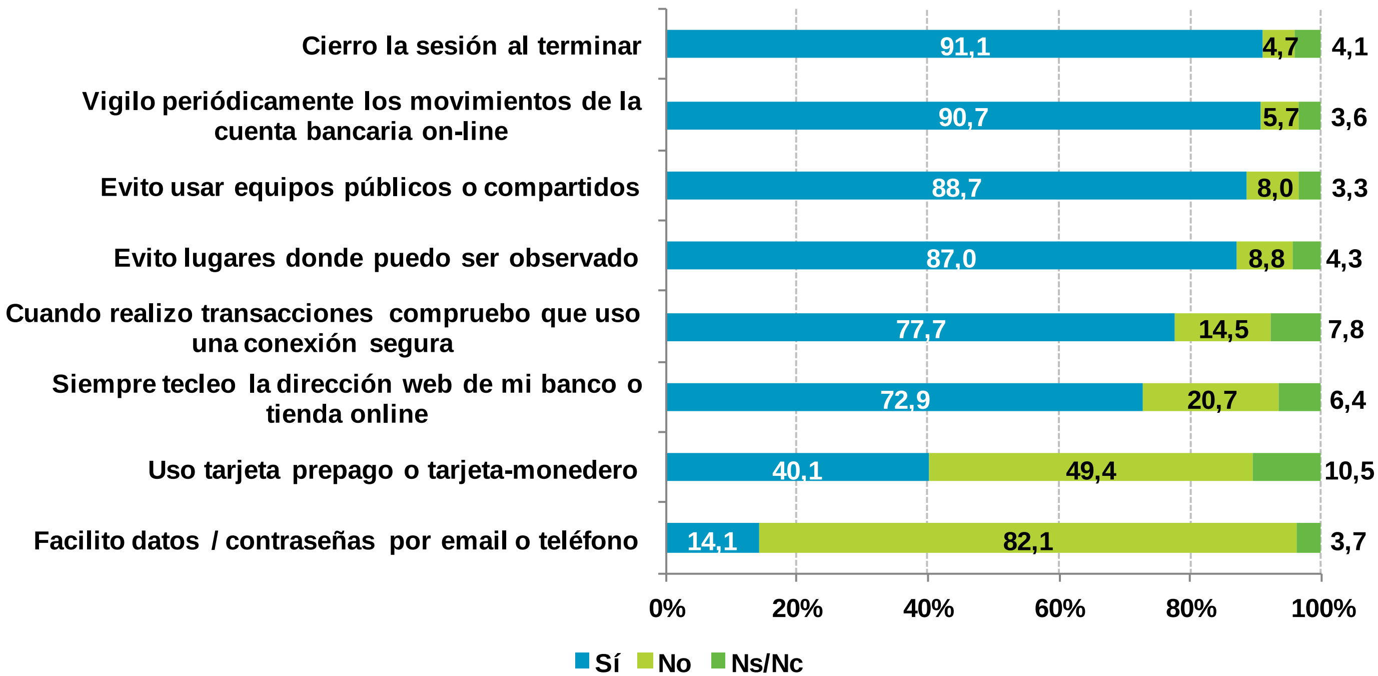
BASE: Usuarios que disponen de smartphone

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

3

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Los usuarios de los **servicios de banca y comercio a través de Internet** mantienen buenos hábitos de comportamiento. El uso de **tarjetas prepago o monedero** es secundado por un **40,1%** de usuarios de estos servicios.



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

Las entidades bancarias nunca solicitan datos y contraseñas del usuario. Dicha información es confidencial y únicamente debe ser conocida por el usuario.

Normalmente las entidades bancarias disponen de un aviso para alertar a sus clientes de estás prácticas. La finalidad es evitar fraudes online y/o telefónicos que buscan obtener los credenciales del usuario y conseguir acceso a sus cuentas.

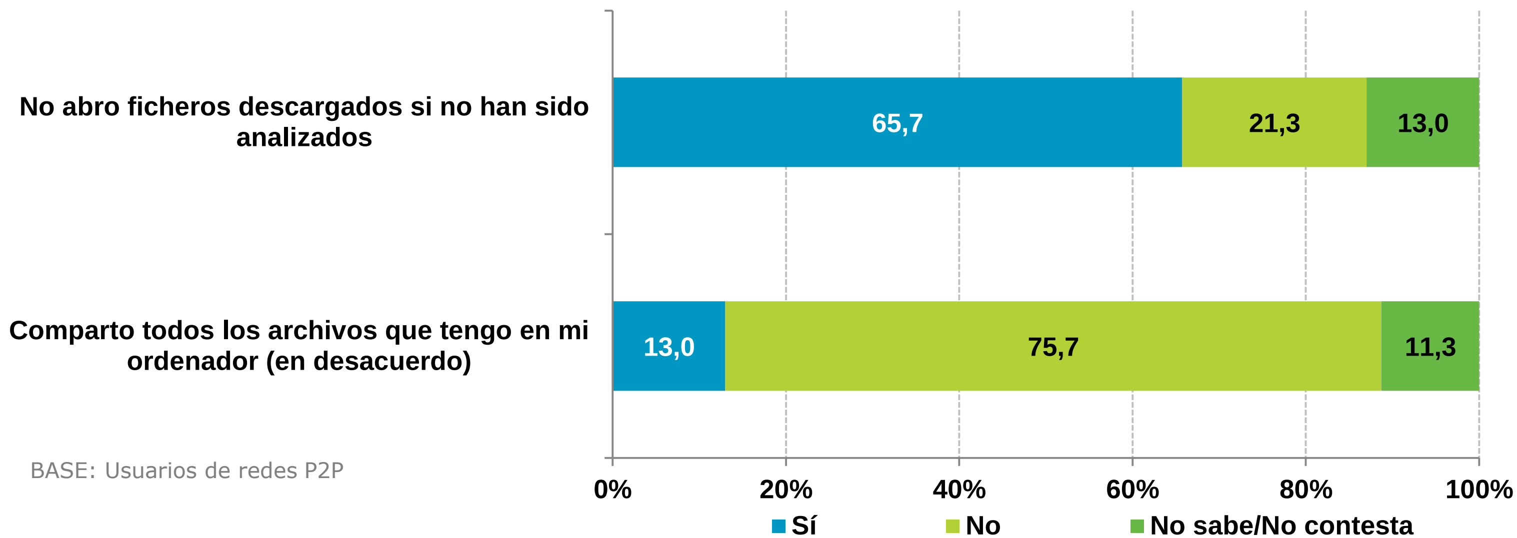
3

Medidas para protegerte al realizar trámites on-line: http://www.osi.es/pagos-online

Cómo detectar correos electrónicos falsos de banca en línea: http://www.osi.es/es/banca-electronica

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.



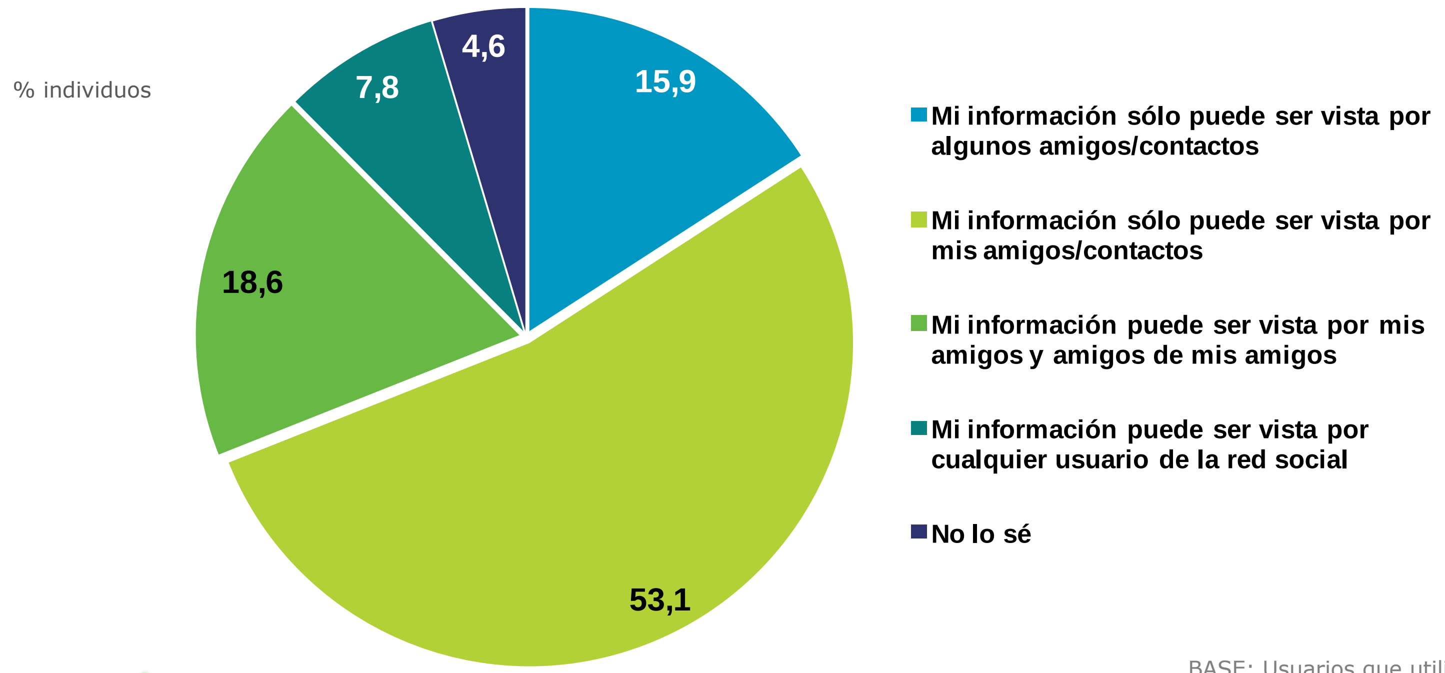
BASE: Usuarios de redes P2P

El **65,7% de los** panelistas no abre ficheros descargados a través de redes P2P, si no tiene la certeza de que han sido **analizados** con un antivirus.

Por otro lado, el **13%** comparte todos los ficheros del equipo informático en las redes P2P, exponiendo su información privada a cualquier usuario de estas redes de descarga.

Cómo usar las redes P2P con seguridad: http://www.osi.es/webs-de-descarga

Más de la mitad (**53,1%**) de los usuarios de redes sociales configura su perfil para que solo sea accesible por sus amigos y contactos. Sin embargo el **26,4%** (18,6 + 7,8) **expone los datos** publicados en su perfil de las redes sociales a **terceras personas y/o desconocidos**, e incluso un **4,6%** de los consultados **desconoce** el nivel de privacidad de su perfil.



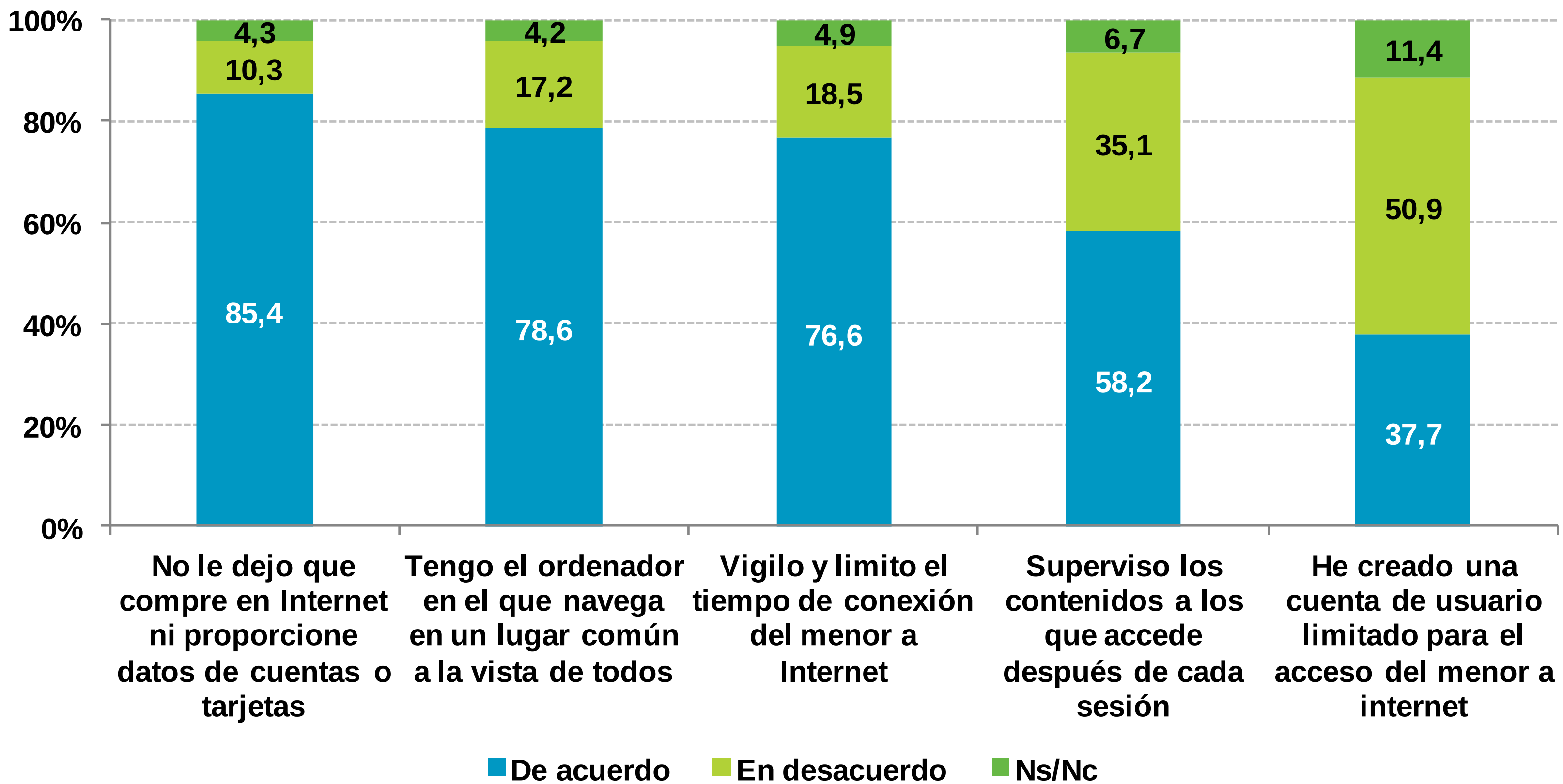
BASE: Usuarios que utilizan redes sociales

Cómo hacer un uso seguro de las redes sociales: http://www.osi.es/redes-sociales

Medidas coercitivas y de control

Exclusiva

Son **menos del 60%** aquellos usuarios que **supervisan los contenidos** a los que accede el menor tras cada sesión, y únicamente el **37,7%** ha creado una **cuenta con permisos limitados** para este.

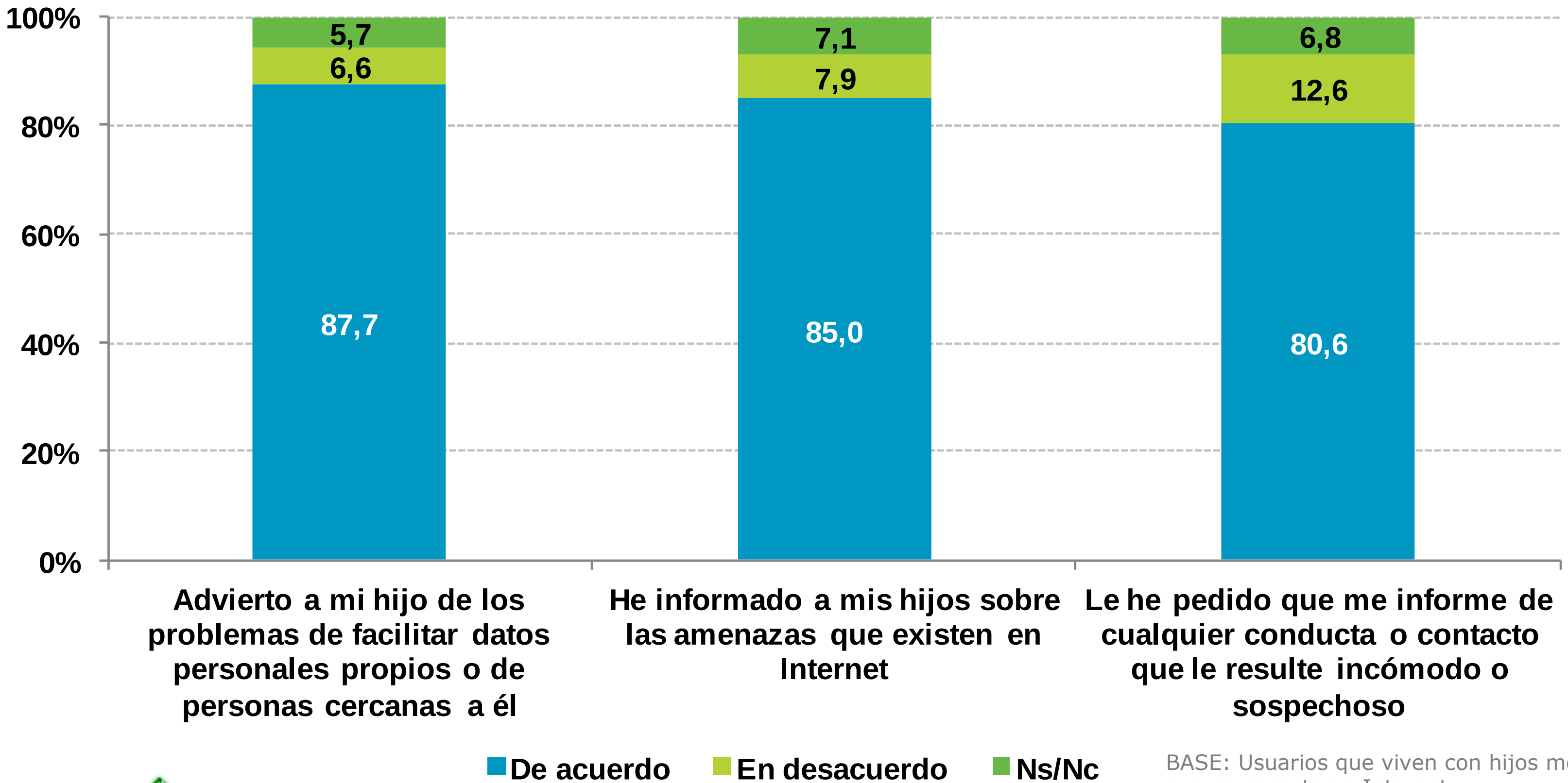


BASE: Usuarios que viven con hijos menores que se conectan a Internet

Medidas de comunicación, diálogo y educación

Exclusiva

Un amplio porcentaje de usuarios (**superior al 80%** en todos los casos) advierte e informa a sus hijos acerca de las amenazas que pueden hallar en Internet y los problemas derivados de ellas.



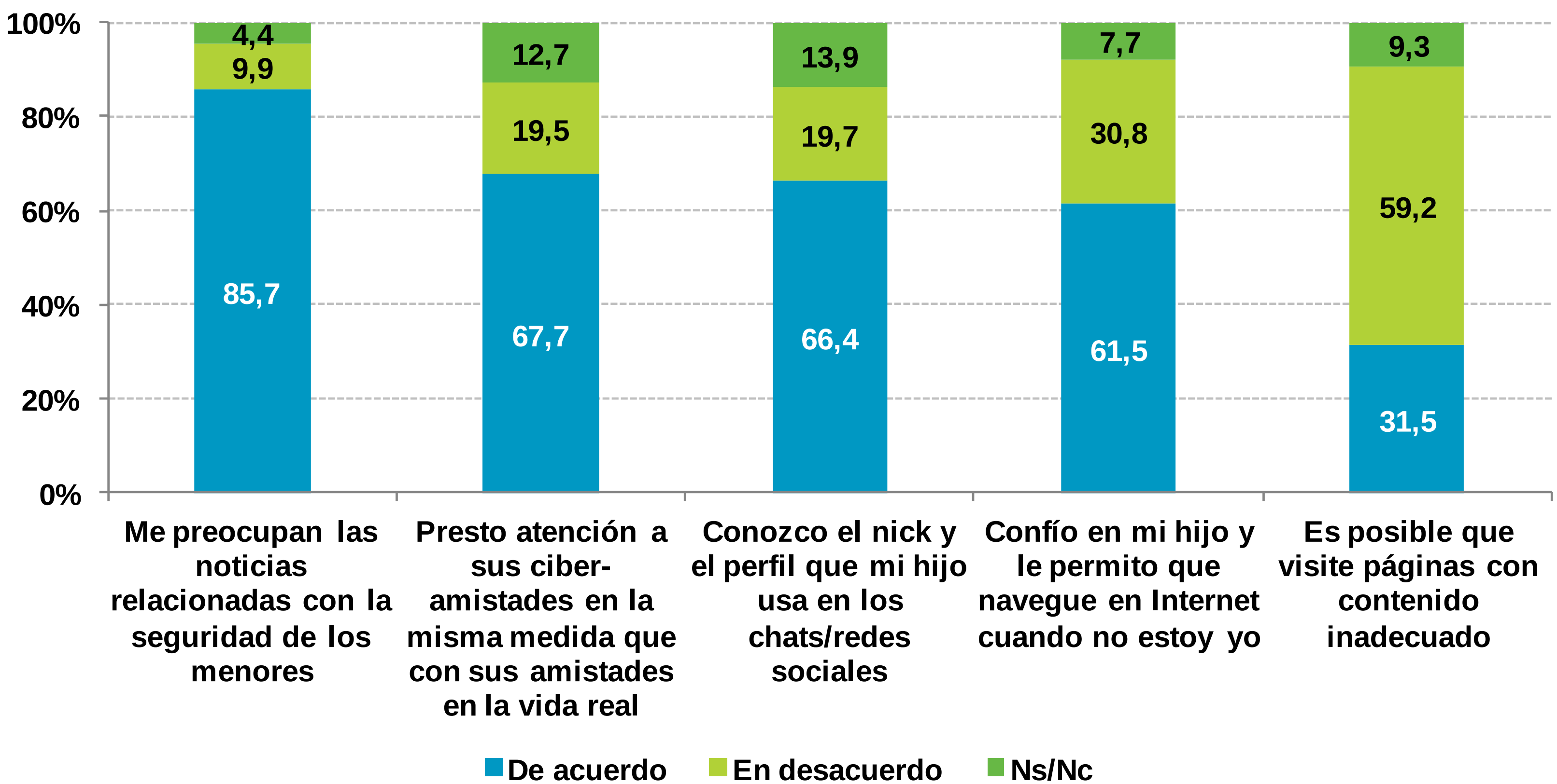
BASE: Usuarios que viven con hijos menores que se conectan a Internet

Cómo proteger a los menores en Internet: http://www.osi.es/proteccion-de-menores

Medidas de implicación de los padres en la navegación del menor

Al **85,7%** de los padres les preocupan las **noticias** relacionadas con la seguridad de los menores en Internet. Sin embargo su **implicación** en la navegación del menor es **inferior al 67,7%**.

Exclusiva



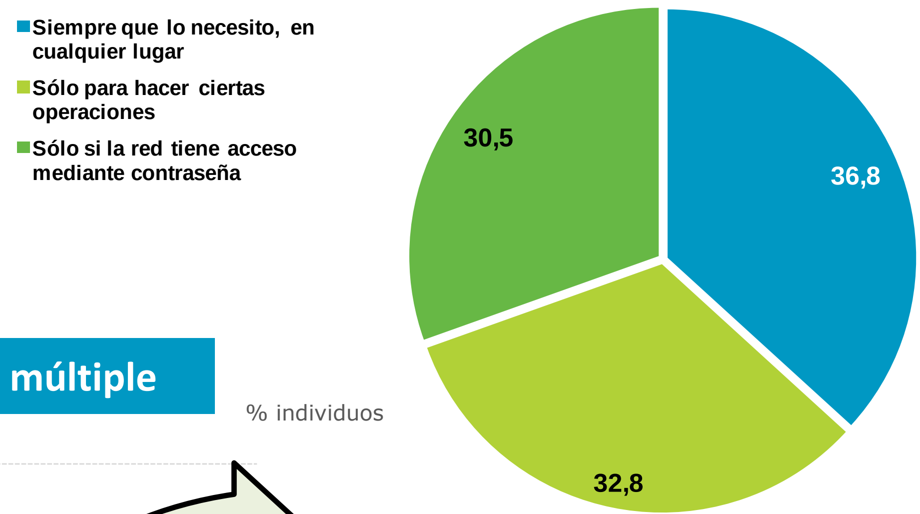
BASE: Usuarios que viven con hijos menores que se conectan a Internet

Hábitos de uso de las redes inalámbricas Wi-Fi

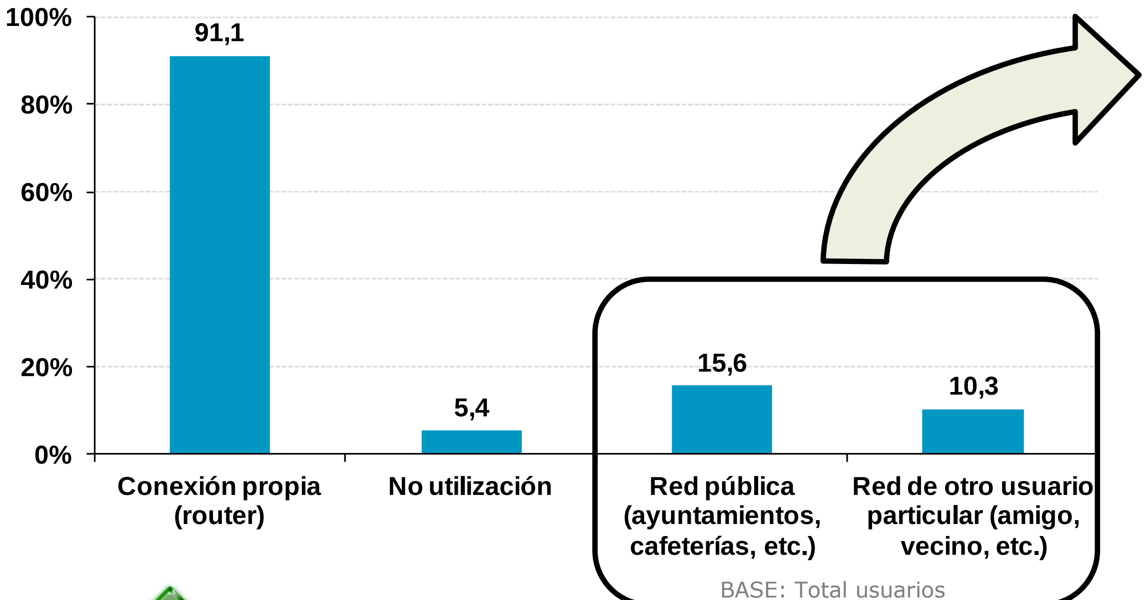
Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Respuesta múltiple

% individuos



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



BASE: Total usuarios

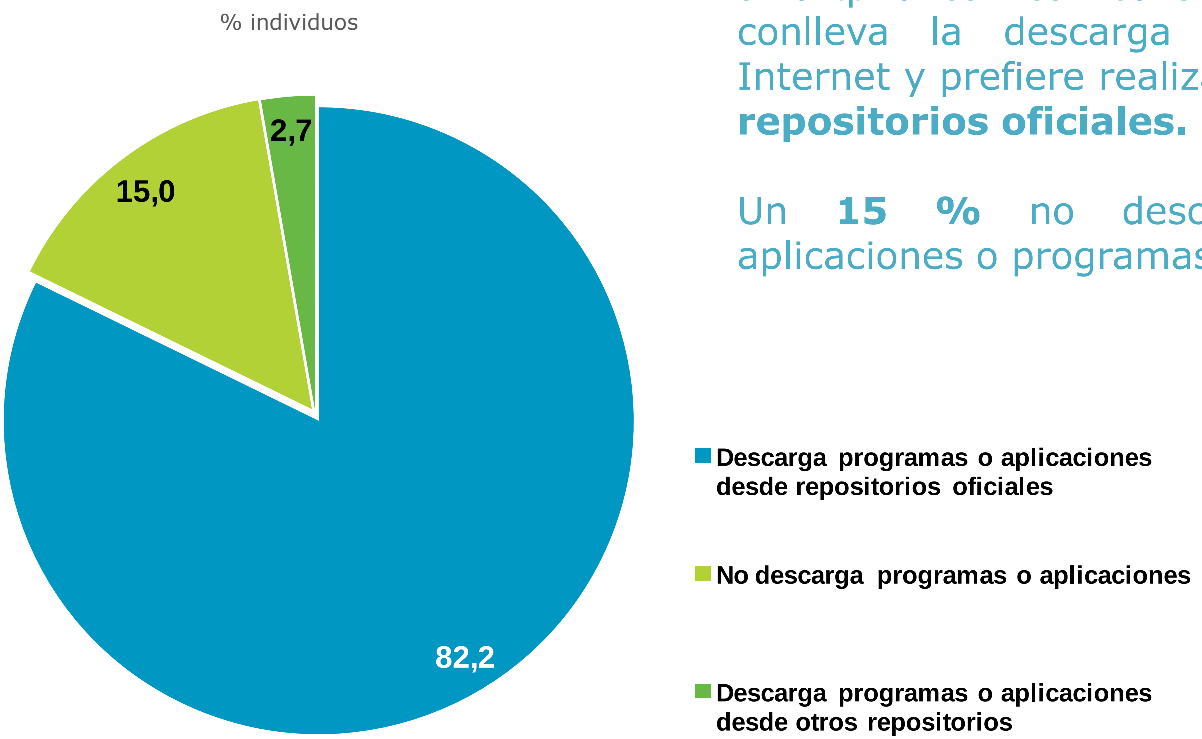
El **36,8%** de usuarios que se conecta a una red inalámbrica Wi-Fi pública lo hace **siempre que lo necesita** y **en cualquier lugar**, exponiendo la confidencialidad e integridad de sus datos.

Cómo conectarte a redes Wi-Fi públicas de forma segura: http://www.osi.es/wifi-publica

El **88,1%** de los internautas con acceso frecuente a Internet posee un Smartphone o teléfono móvil "inteligente".

La mayoría (**82,2%**) de usuarios de smartphones es consciente del riesgo que conlleva la descarga de aplicaciones desde Internet y prefiere realizarlas directamente desde **repositorios oficiales.**

Un **15 %** no descarga ningún tipo de aplicaciones o programas.



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

Incidentes de seguridad

4

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

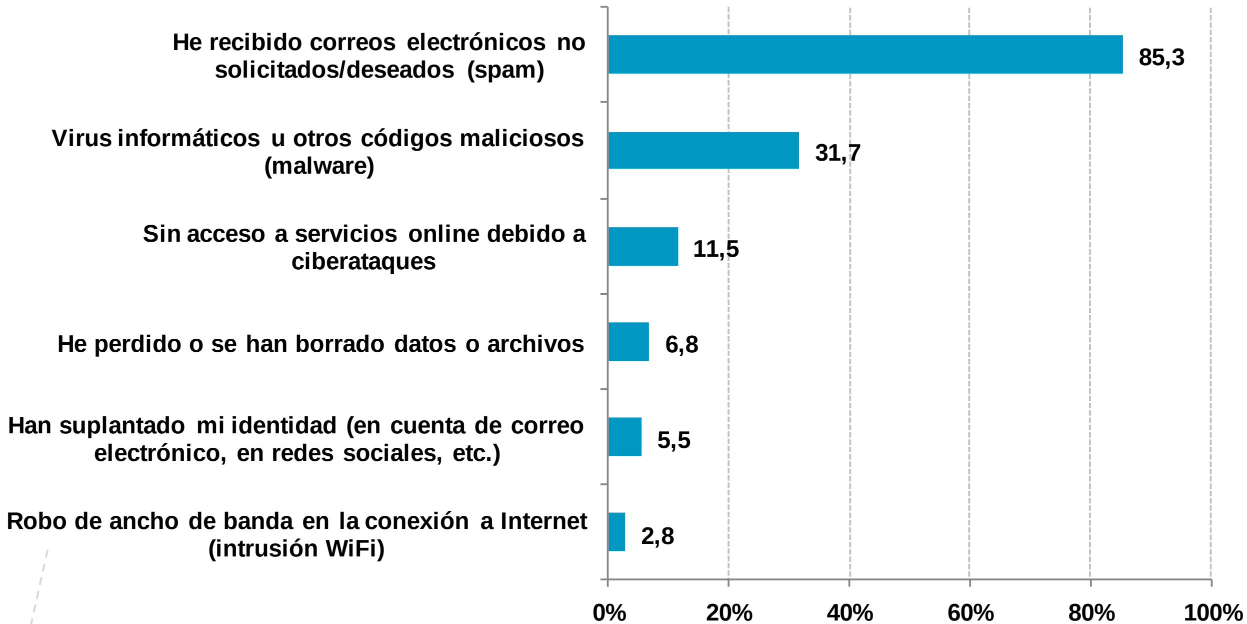
Incidencias de seguridad

Conoce en profundidad las amenazas que circulan por Internet y los riesgos que suponen:

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

Incidencias sufridas:

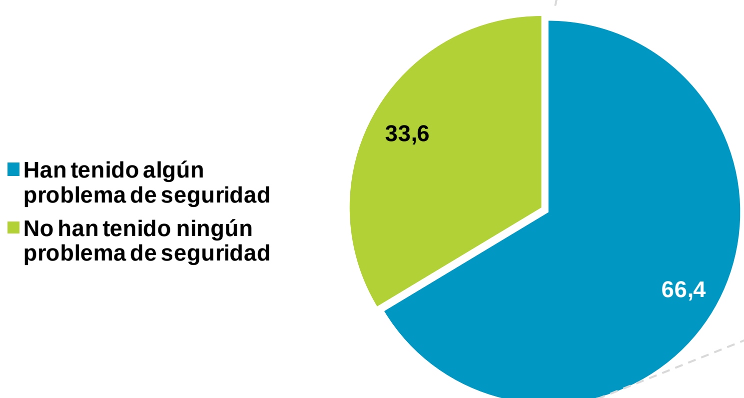
Respuesta múltiple



BASE: Usuarios que han sufrido alguna incidencia de seguridad

Afectados:

% individuos



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.

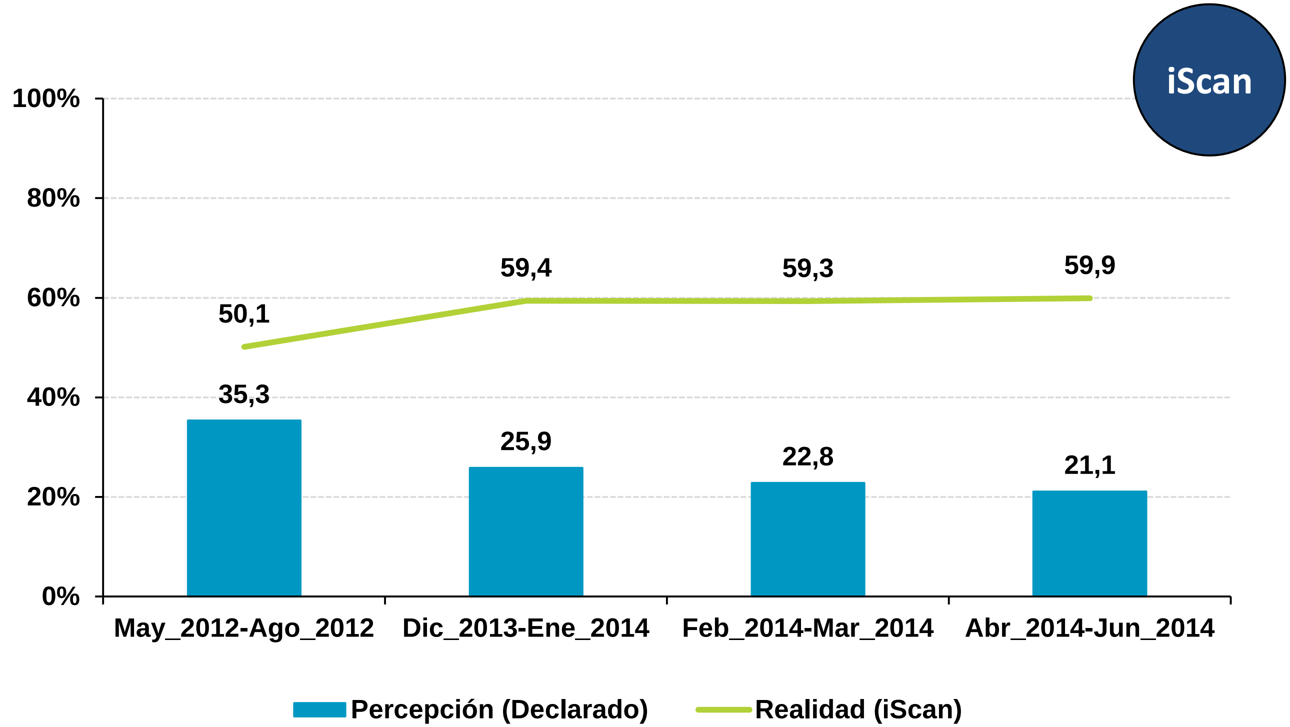
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

Evolución de los incidentes por malware

Existen **39 puntos porcentuales** entre las **incidencias de malware** reales en los equipos escaneados y las percibidas por el usuario durante el trimestre abril-junio

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 INCIBE, 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.

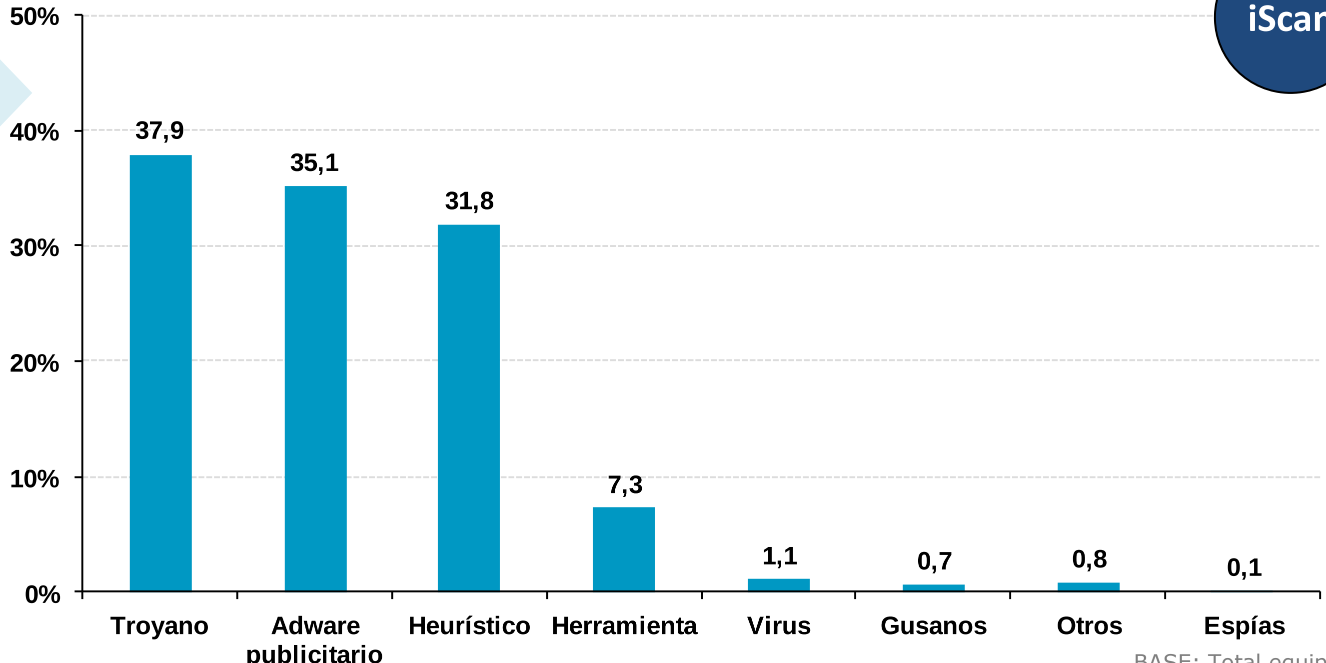
Tipología del malware detectado

El malware con mayor presencia en los equipos informáticos es aquel cuyo cometido es lograr un beneficio económico. Así el **troyano** se encontró en el **37,9%** de los ordenadores escaneados y el **adware publicitario** fue detectado en más de un tercio (**35,1%**).

iScan

4

Equipos que alojan malware según tipología



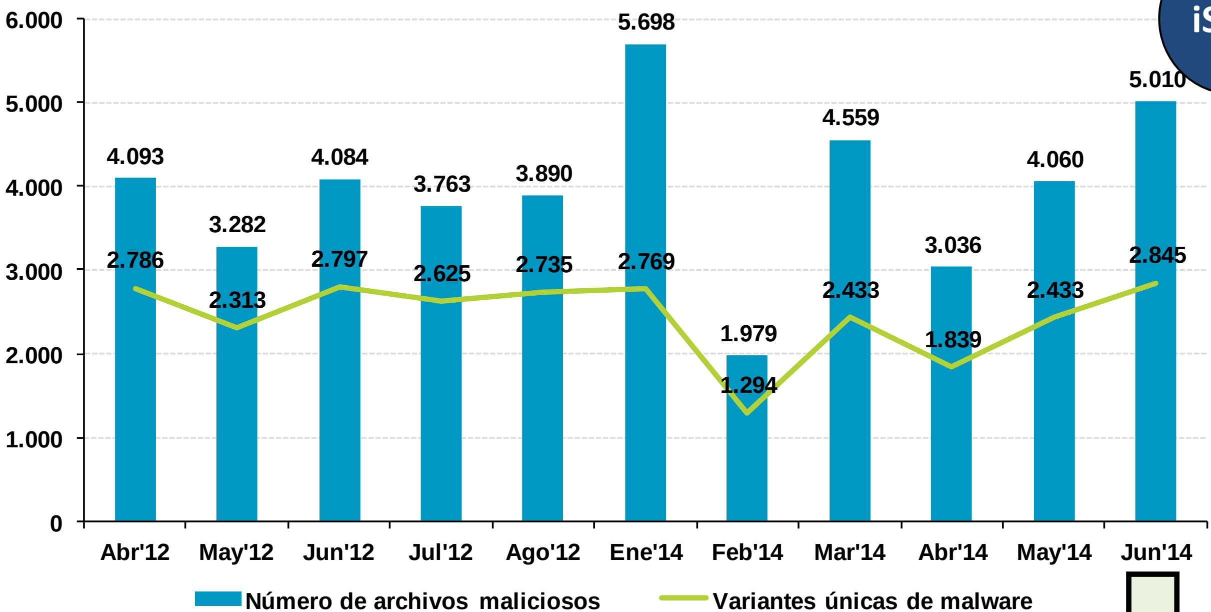
BASE: Total equipos

Tipos de malware: http://www.osi.es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

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.

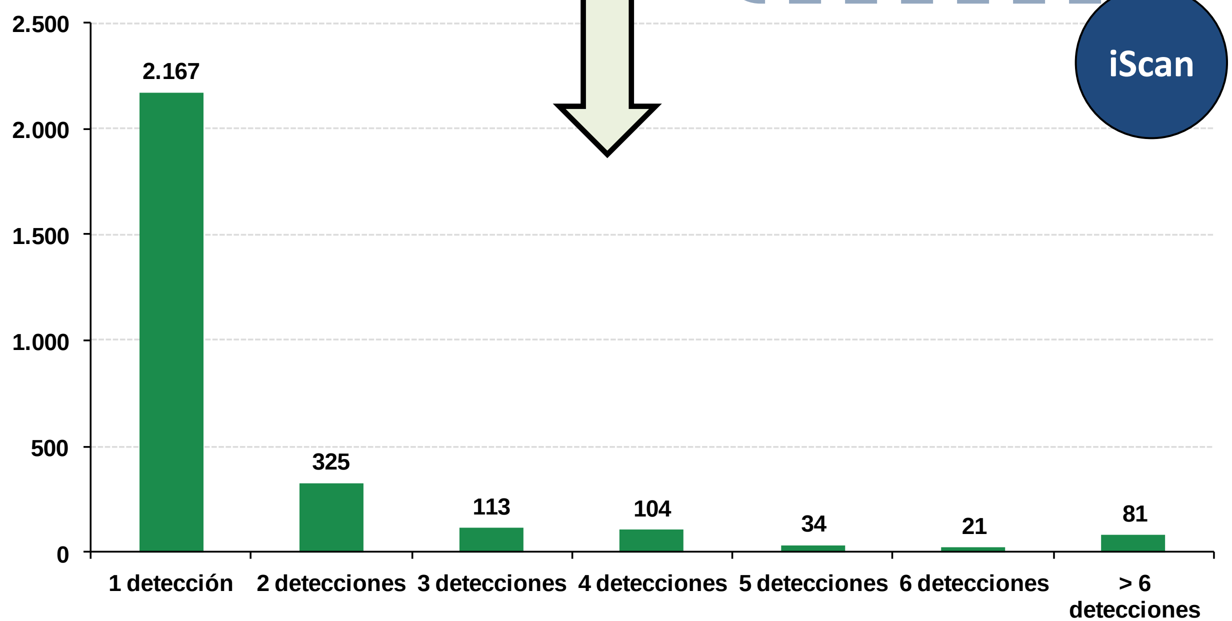
Diversificación del malware detectado



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 (jun. 14)



La gran variedad y personalización de código malicioso se manifiesta en el hecho de que el **76,1%** de las variantes únicas **fue detectada solo una vez**.

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.).

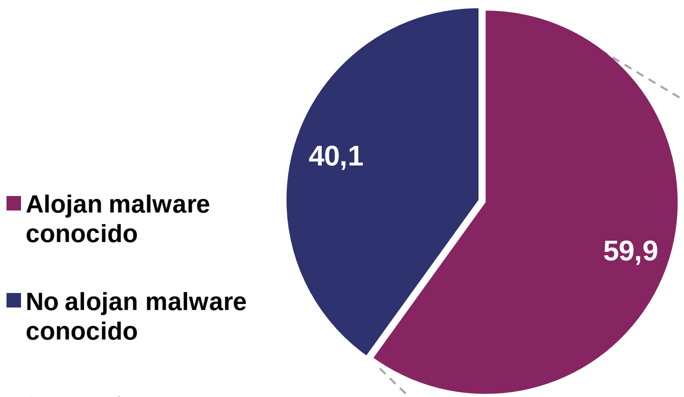
Peligrosidad baja: se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, *hacking tools*, etc.). En la mayoría de los casos son herramientas instaladas por el usuario 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.

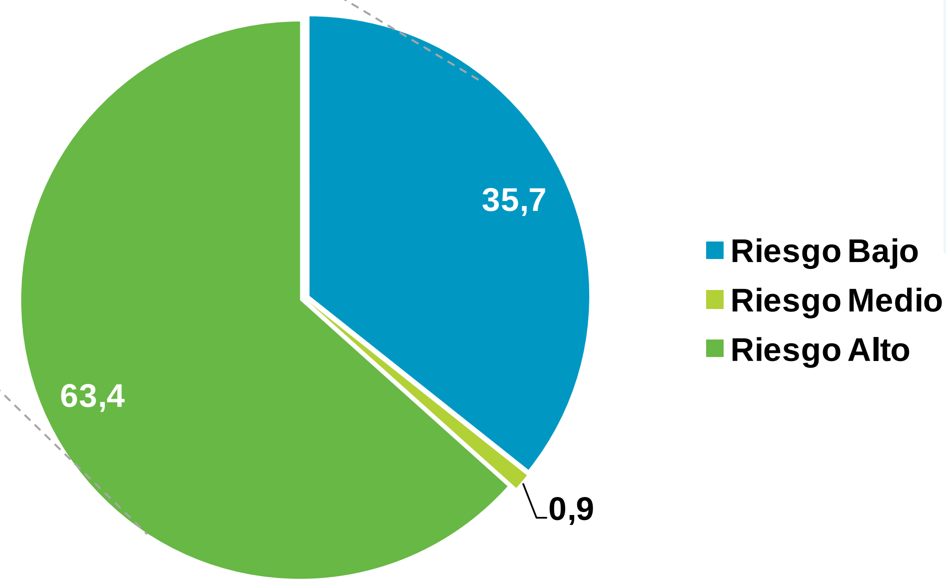
Peligrosidad del código malicioso y riesgo del equipo

Prácticamente el **60%** de los equipos analizados con iScan se encuentran infectados con al menos una muestra de malware conocida. De estos, casi dos de cada tres (**63,4%**) presentan un nivel de **riesgo alto** debido al <u>potencial peligro</u> que suponen los archivos maliciosos encontrados en ellos.

iScan



BASE: Total equipos

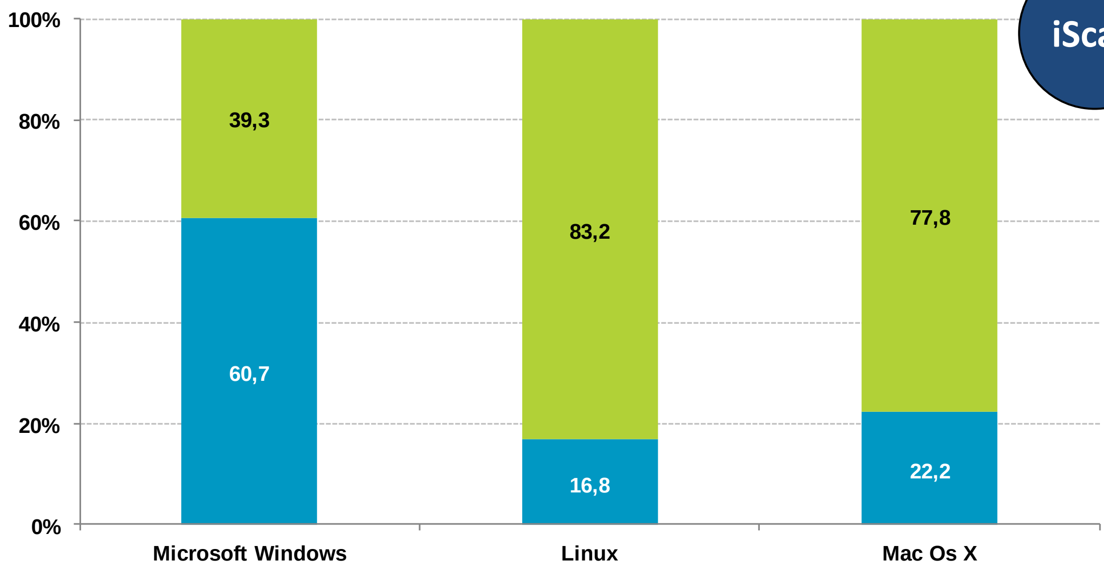


BASE: Total equipos infectados

Malware vs. sistema operativo y actualización

iScan

Equipos infectados según sistema operativo



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

4

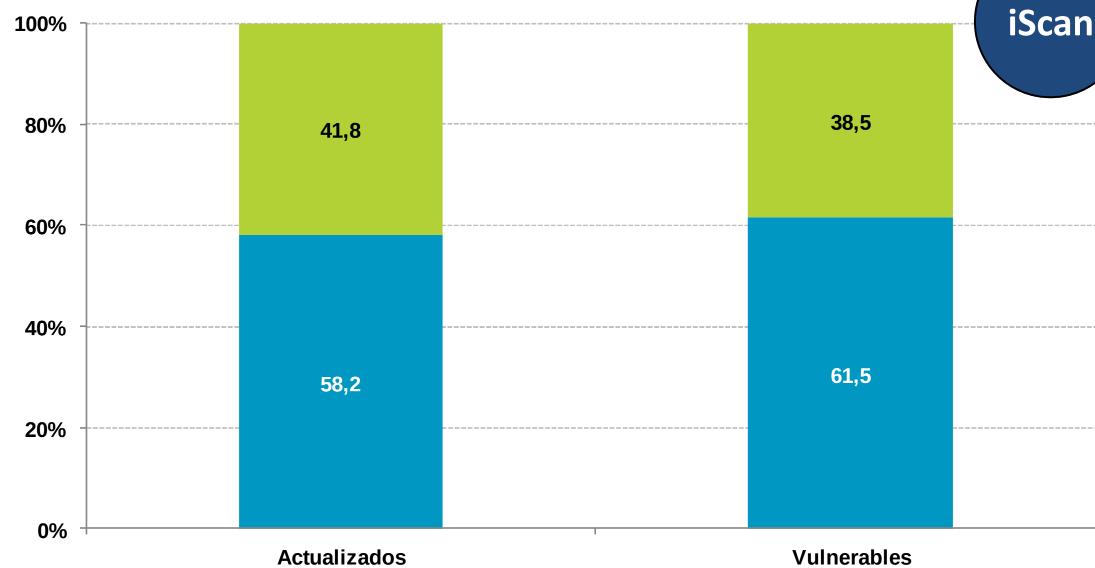
Infectados

No infectados

BASE: Total usuarios

Equipos infectados según estado de actualización

iScan

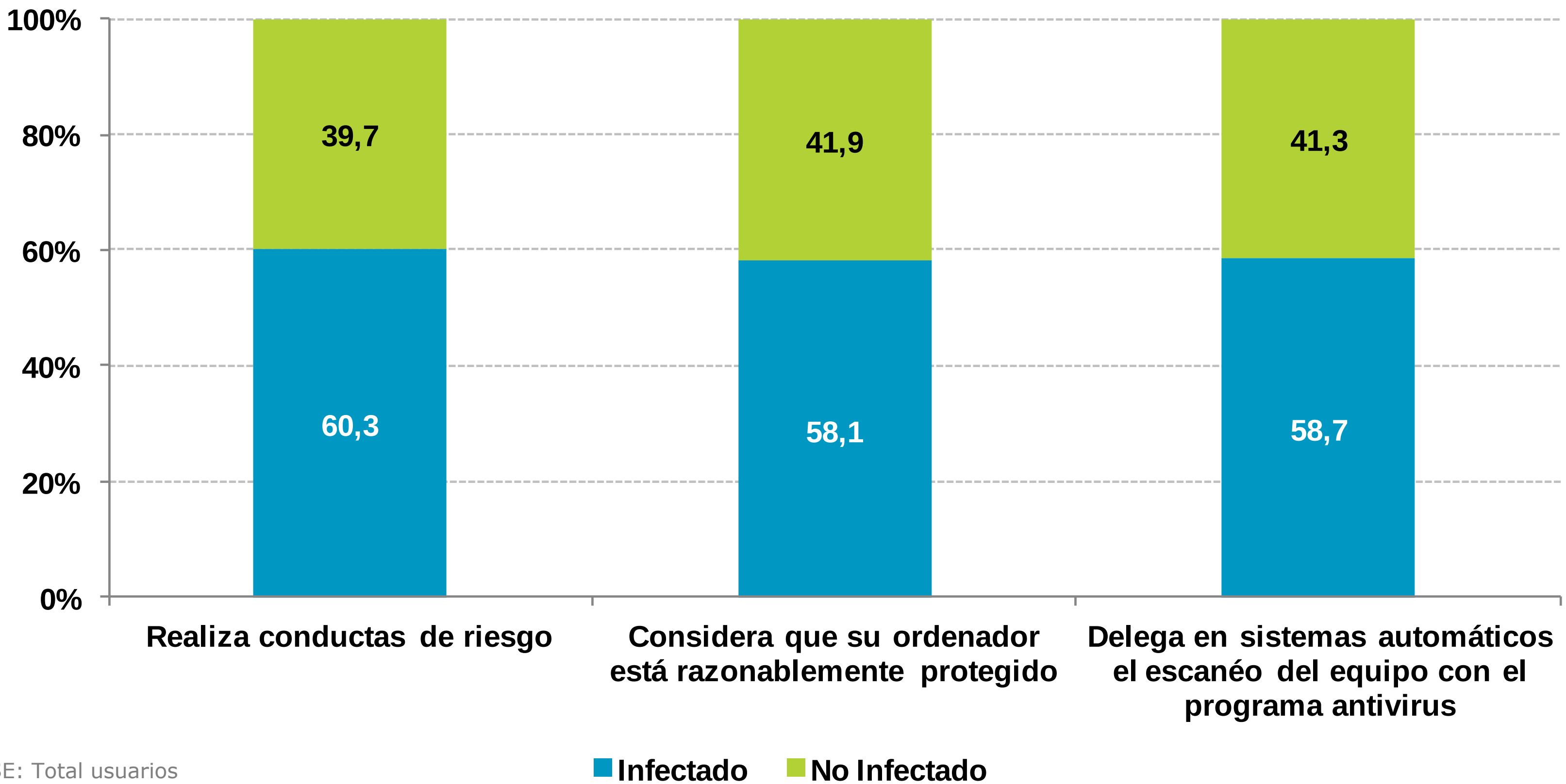


La diferencia entre los equipos que alojan malware según el estado de **actualización del sistema operativo** es de **3 puntos porcentuales** a favor de aquellos que cuentan con todos los **parches de seguridad** instalados.

Malware vs. hábitos de comportamiento

iScan detecta **infecciones** en 3 de cada 5 (**60,3%**) equipos de usuarios que llevan a cabo **conductas de riesgo** de manera consciente y de forma puntual.

También se detecta malware en el **58,1%** de los equipos de usuarios que consideran su **ordenador razonablemente protegido**, y en el **58,7%** de los ordenadores de usuarios que **delegan en sistemas automáticos** el escaneo con software antivirus.

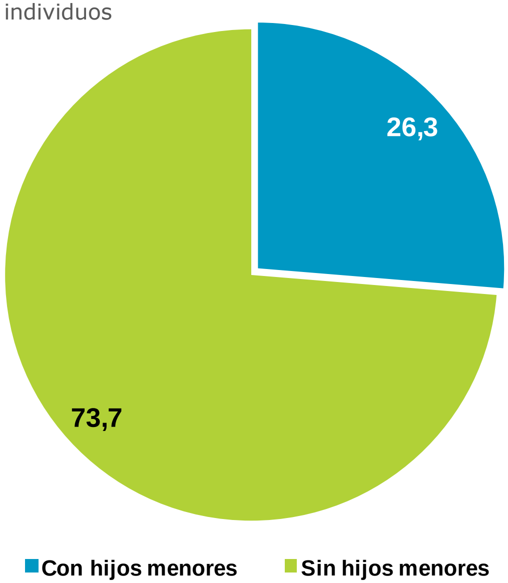


BASE: Total usuarios

Incidencias de seguridad en hogares con menores

Exclusiva

% individuos



BASE: Total usuarios

Incidencias de seguridad relacionadas con el menor:

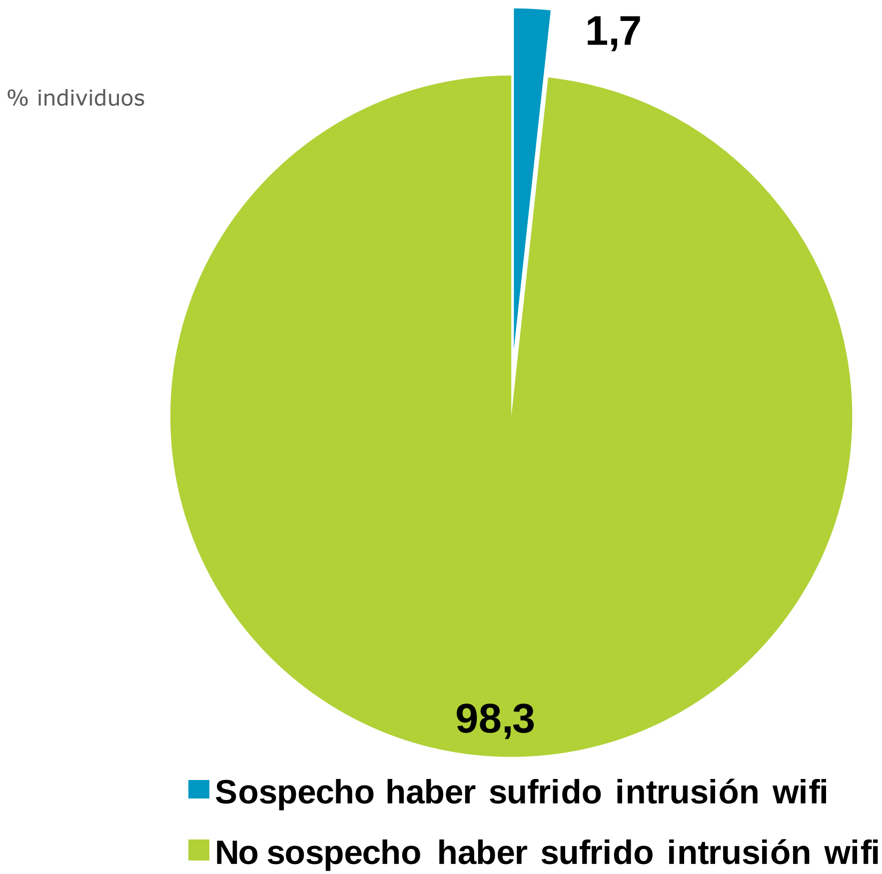
Respuesta múltiple

BASE: Usuarios que viven con hijos menores que se conectan a Internet

Incidencias de seguridad en redes inalámbricas Wi-Fi

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

http://www.osi.es/protege-tu-wifi



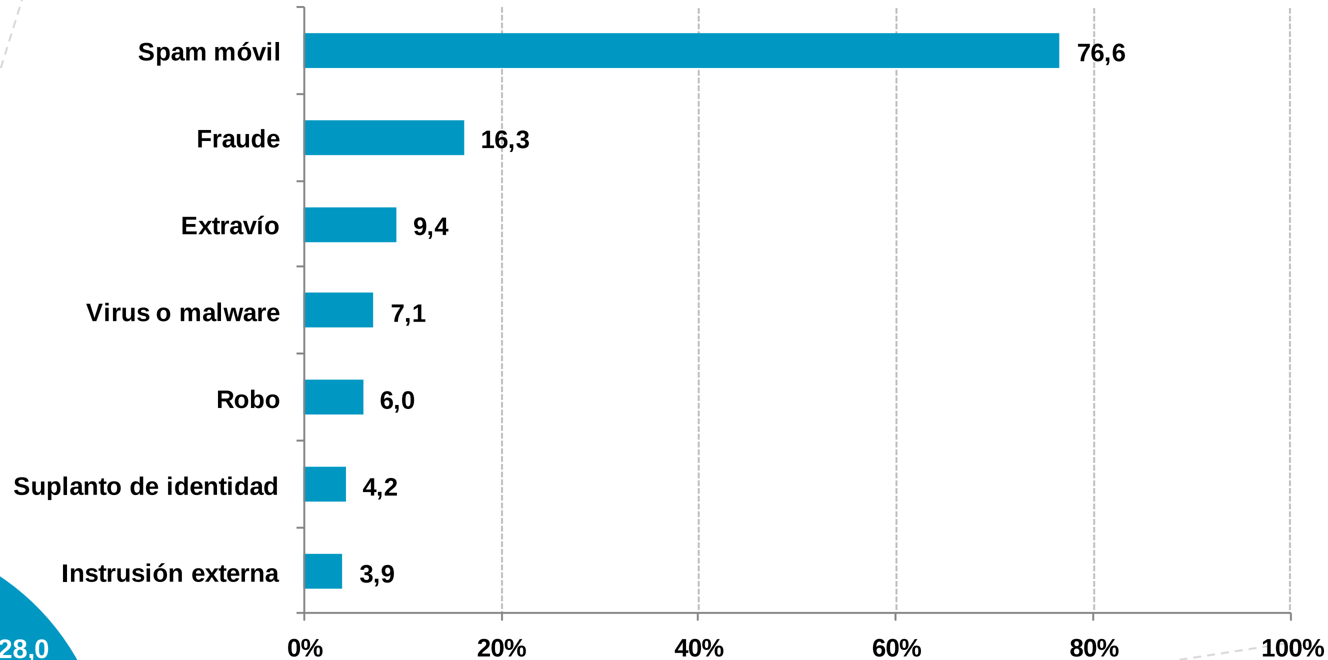
Únicamente un **1,7%** de panelistas *sospechan* que pueden haber sufrido una **intrusión en la red inalámbrica Wi-Fi** de su hogar, a pesar de que un porcentaje superior al 12% de los usuarios deja la red Wi-Fi desprotegida y/o desconoce su estado, y otro 11,1% utiliza el estándar WEP –sistema de cifrado obsoleto y totalmente comprometido– (enlace).

BASE: Usuarios con conexión Wi-Fi propia

Incidencias de seguridad en smartphones

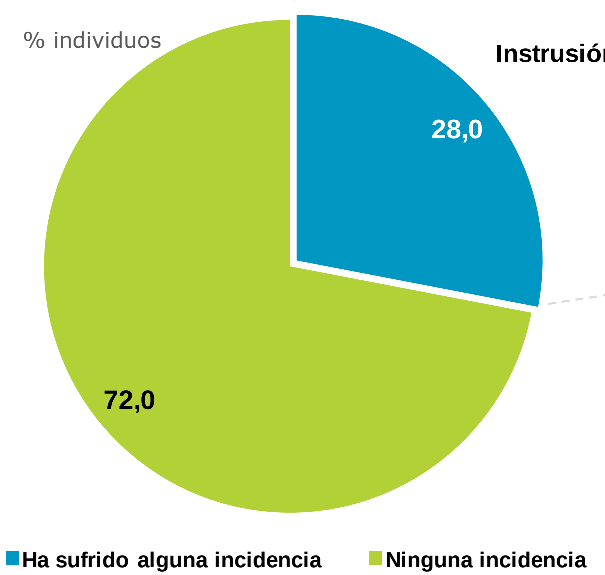
Incidencias sufridas:

Respuesta múltiple



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

Afectados:



BASE: Usuarios que disponen de smartphone

La **principal incidencia en dispositivos móviles** declarada por los panelistas que tuvieron problemas de seguridad es el **spam** (**76,6%**), destacándose ampliamente sobre el resto. La segunda incidencia con mayor ocurrencia es el fraude, sufrido por un 16,3% de los encuestados.

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	Incidencias (%)						
	Extravío	Robo	Virus o Malware	Suplanto de identidad	Intrusión externa	Spam	Fraude
Robo de datos	16,5	19,0	17,9	30,3	**45,5**	0,5	10,9
Pérdida de datos	**44,0**	27,0	28,6	18,7	12,7	3,4	5,4
Suplanto de identidad	21,7	19,8	14,0	**24,3**	14,0	1,9	8,0
Sustracción de datos online	11,8	**13,6**	12,5	6,1	7,7	2,4	7,6
Perjuicio económico	19,5	34,5	12,3	4,5	13,2	6,8	**54,6**
Suscripción a servicios no solicitados	9,8	9,7	18,7	18,9	29,7	16,4	**45,4**
Otro	0,8	0,0	**22,2**	4,8	0,0	1,9	0,0
Ninguna de las anteriores	25,5	27,7	27,4	25,9	23,8	74,2	9,5

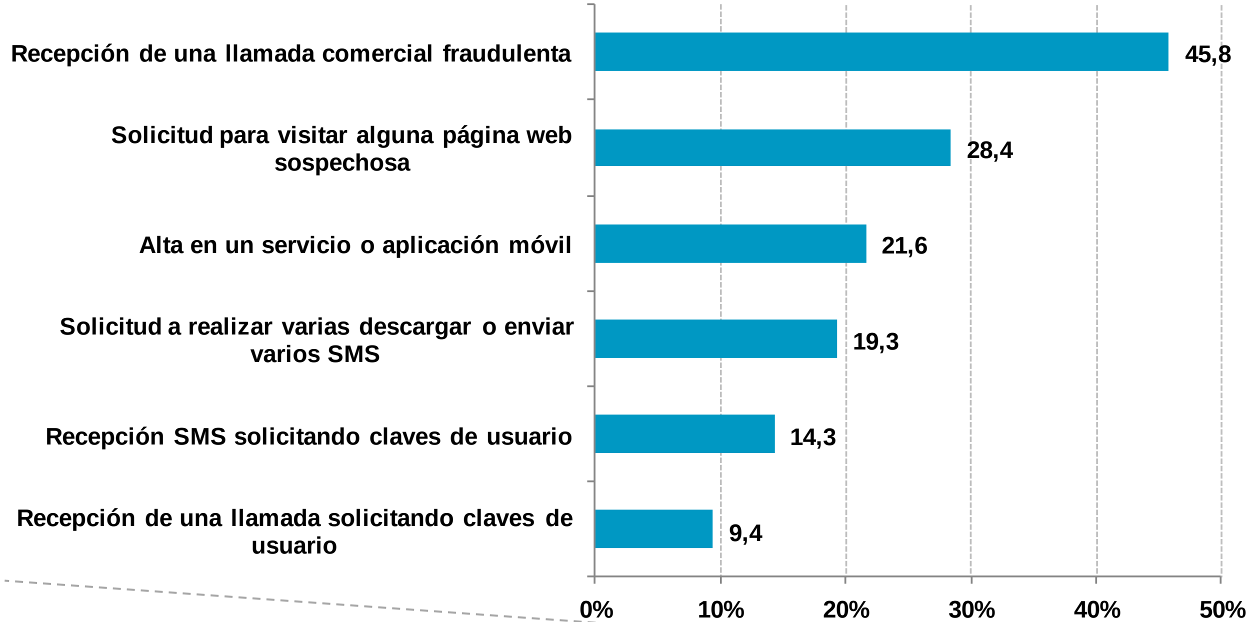
Cómo protegerte si tienes un iPhone/iPad: https://www.osi.es/es/actualidad/blog/2013/10/25/las-9-funcionalidades-de-seguridad-que-tienes-que-utilizar-si-tienes-un-i
Cómo protegerte si tienes una BlackBerry: https://www.osi.es/es/actualidad/blog/2013/12/11/las-9-funcionalidades-de-seguridad-que-tienes-que-utilizar-si-tienes-una-
Cómo protegerte 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

Manifestaciones del intento de fraude telefónico:

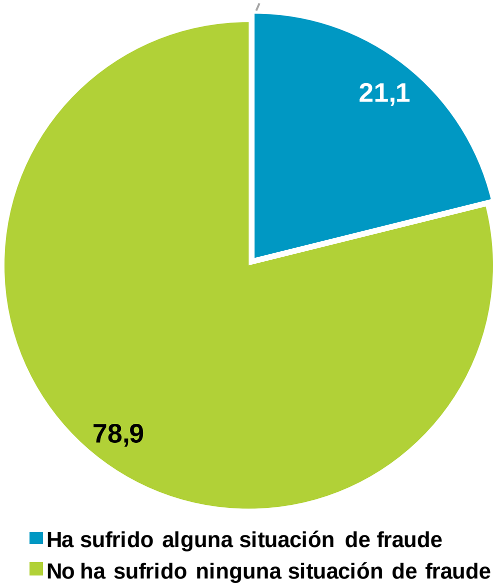
Respuesta múltiple



% individuos

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

Intento de fraude telefónico:



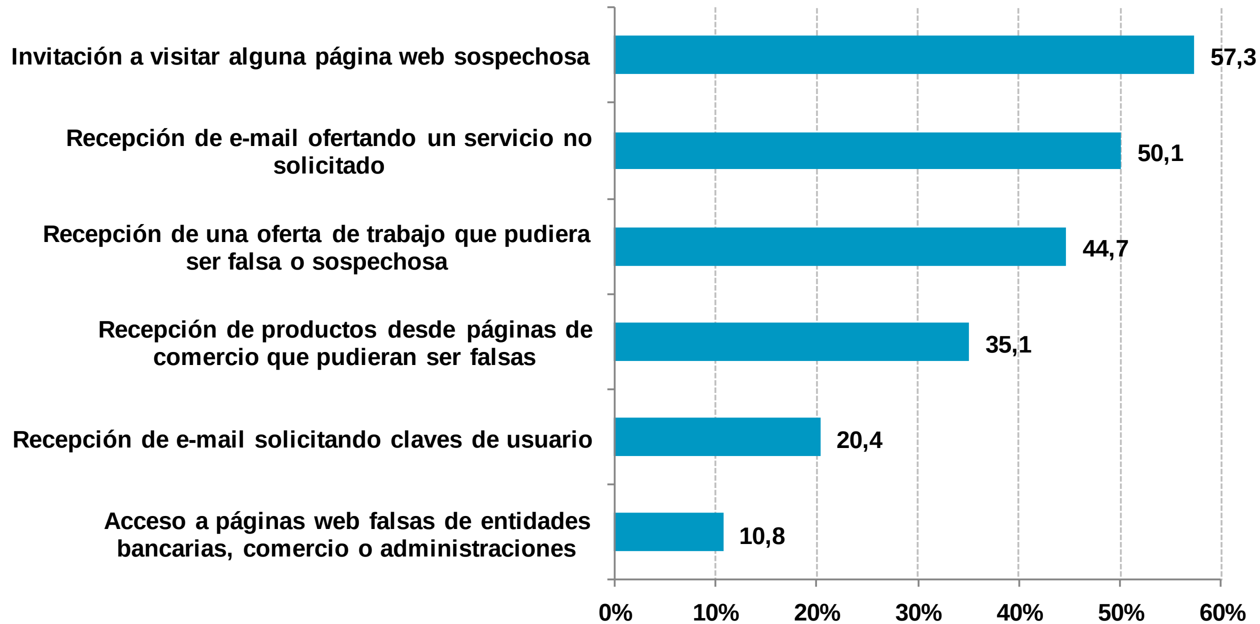
Ejemplo real de llamada telefónica fraudulenta: http://www.osi.es/actualidad/historias-reales/2014/06/06/historias-reales-me-llamaron-por-telefono-haciendose-pasar-por-microsoft-

BASE: Usuarios que disponen de dispositivo móvil o smartphone

Intento de fraude online y manifestaciones

Manifestaciones del intento de fraude online:

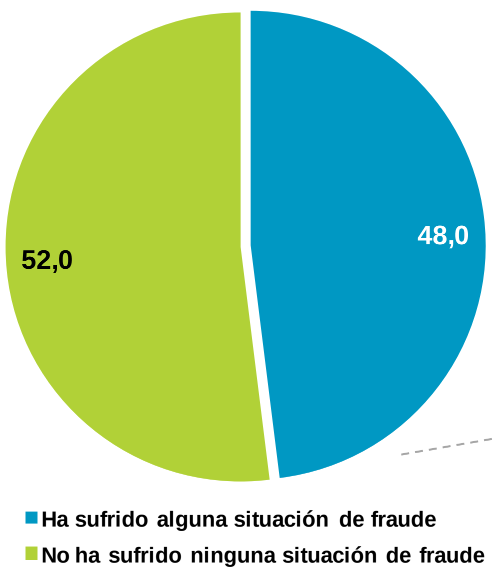
Respuesta múltiple



% individuos

BASE: Usuarios que han sufrido algún intento de fraude

Intento de fraude online:



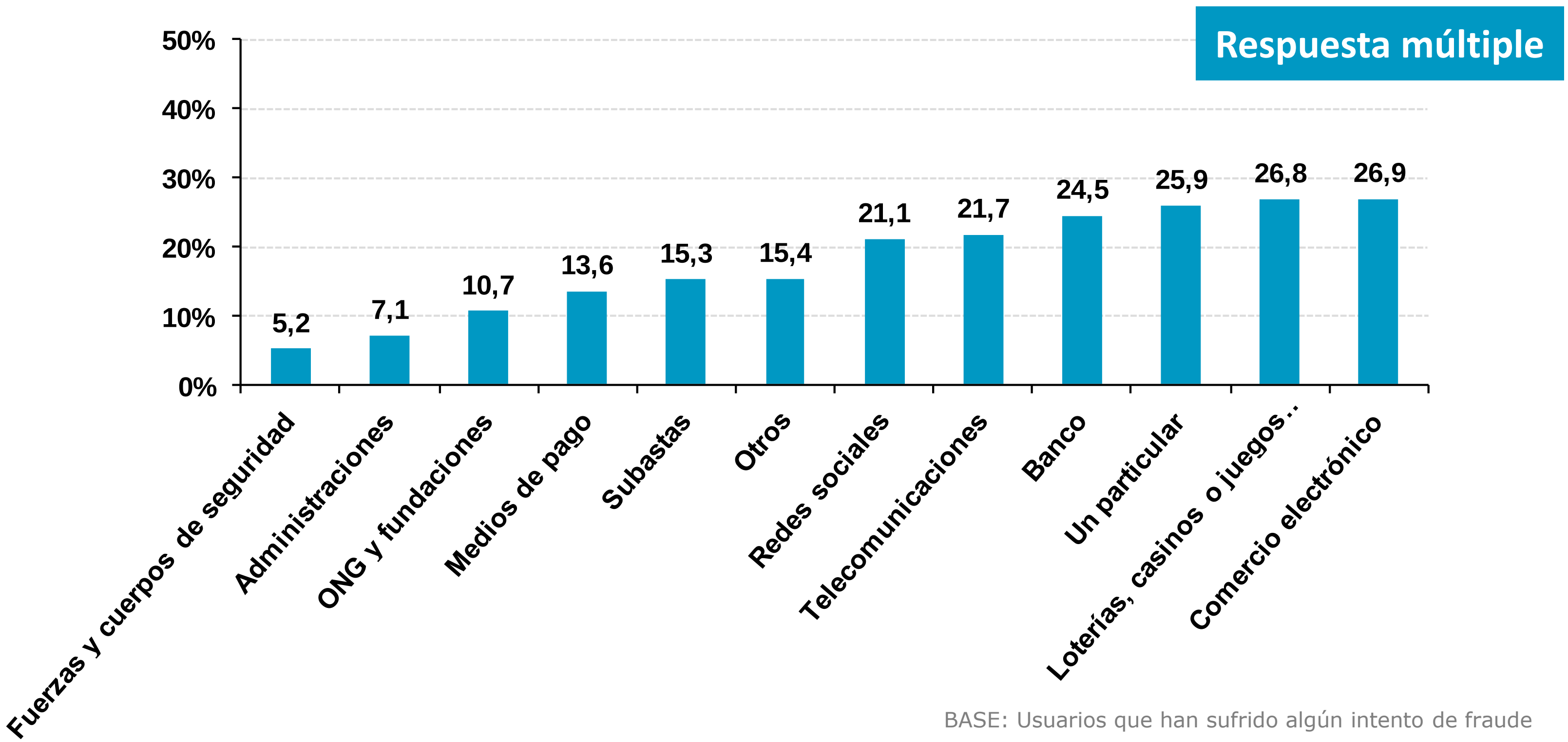
BASE: Total usuarios

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

5

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

Las **formas adoptadas** más comúnmente por el remitente de la comunicación sospechosa de ser fraudulenta, son la imagen de páginas de **"Comercio electrónico"** (**26,9%**) y **"Loterías, casinos y juegos online"** (**26,8%**).



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.

La principal forma adoptada por el remitente[5] es la **entidad bancaria** cuando se trata de **solicitar claves de usuario** (**54,3%**) y enviar invitaciones a **páginas web falsas** (*phishing*) de entidades bancarias, comercio, etc. (**63,1%**).

Manifestación del fraude	Forma adoptada por el remitente de la comunicación (%)											
	Banco	Comercio electrónico	Medios de pago	Redes sociales	Administraciones	Telecomunicaciones	ONG y fundaciones	Subastas	Loterías	Fuerzas y cuerpos de seguridad	Particular	Otros
Recepción de e-mail solicitando claves de usuario	**54,3**	27,2	27,7	32,0	16,5	31,7	16,2	23,4	33,7	12,9	33,0	7,0
Recepción de e-mail ofertando un servicio no solicitado	30,6	**37,2**	16,5	29,2	8,3	32,7	14,6	20,4	36,3	7,0	27,1	12,2
Recepción de e-mail con invitación a visitar alguna página web sospechosa	29,1	29,2	16,4	25,2	7,5	25,0	13,6	19,4	**34,4**	6,0	27,9	13,3
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	32,6	28,9	16,8	22,9	8,9	25,6	12,8	17,3	29,3	7,2	**37,7**	17,9
Recepción de productos desde páginas de comercio que pudieran ser falsas	31,8	**39,8**	19,7	33,0	10,0	30,1	16,1	23,4	36,0	6,5	27,6	11,7
Acceso a páginas web falsas de entidades bancarias, comercio o Administraciones	**63,1**	28,1	36,6	26,7	19,4	27,5	16,9	18,8	28,1	18,1	25,5	4,3

El *phishing* es la estafa más utilizada en Internet. Consiste en la creación y distribución de una página web similar a la de una entidad bancaria con la finalidad de obtener las claves de usuario: http://www.osi.es/es/banca-electronica

[5] Ver nota al pie número 4

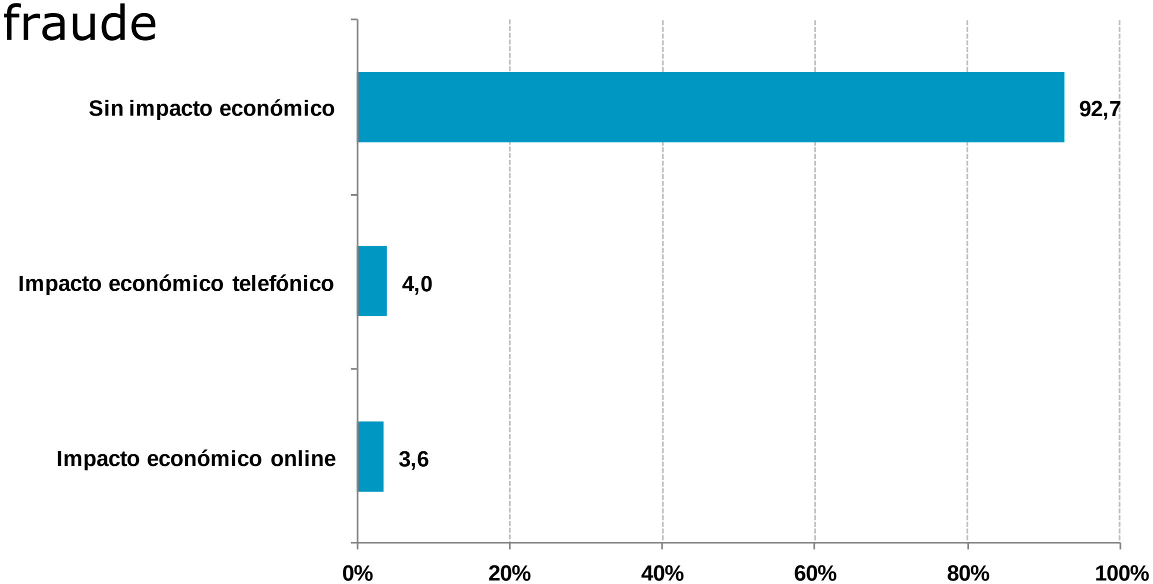
BASE: Usuarios que han sufrido cada tipo concreto de intento de fraude

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Impacto económico del fraude

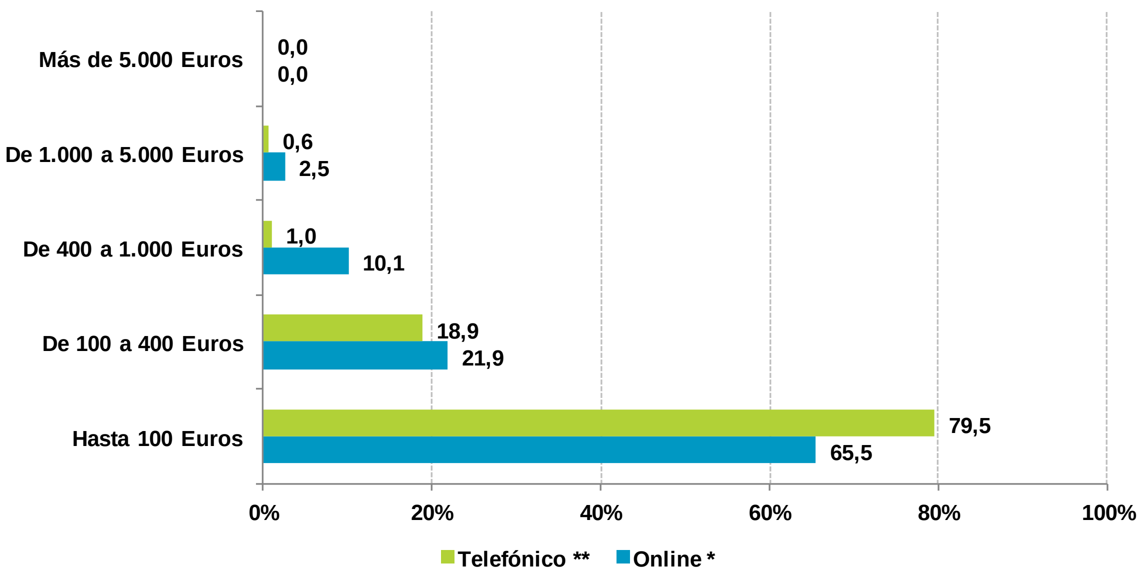
Únicamente un pequeño porcentaje de los intentos de fraude acaban suponiendo un **prejuicio económico** para la víctima.

De estos, en la mayoría de las ocasiones la cuantía es **inferior a 100 euros**.



BASE: Usuarios que han sufrido un intento de fraude

5



Distribución del impacto económico del fraude

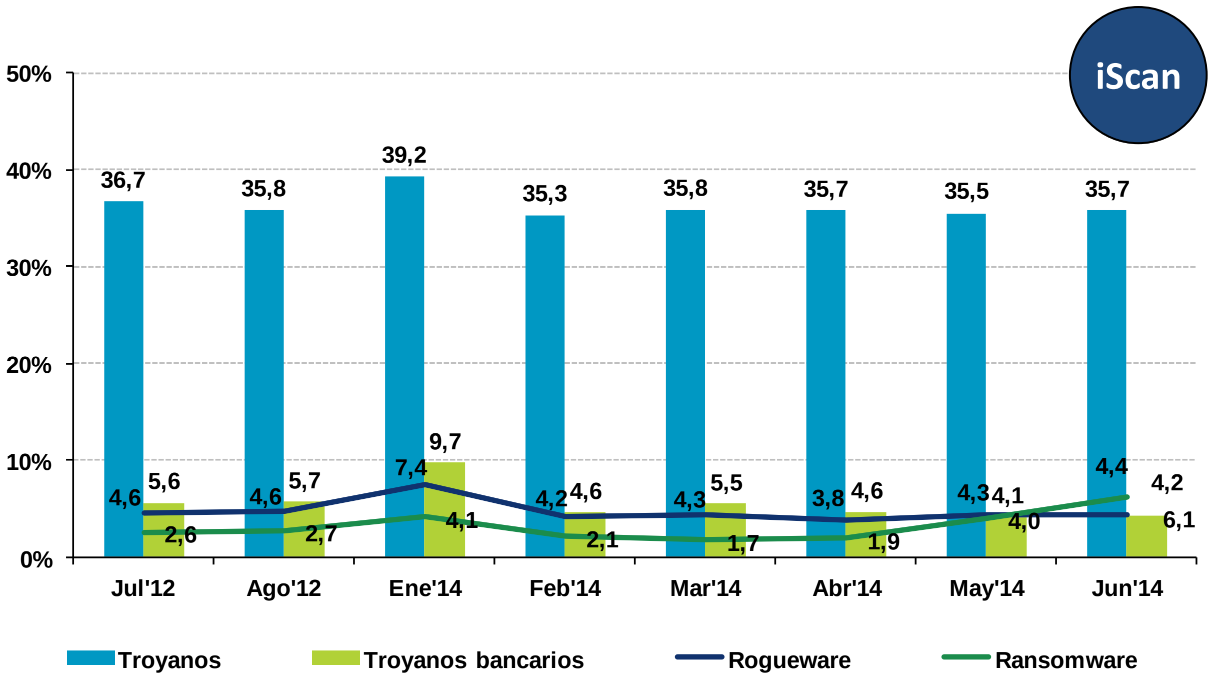
* BASE: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online

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

Fraude y malware

Los **troyanos bancarios** fueron las infecciones registradas por iScan en el **4,2%** de los equipos analizados en el mes de junio de 2014.

Evolución de equipos que alojan troyanos bancarios y rogueware



BASE: Total equipos

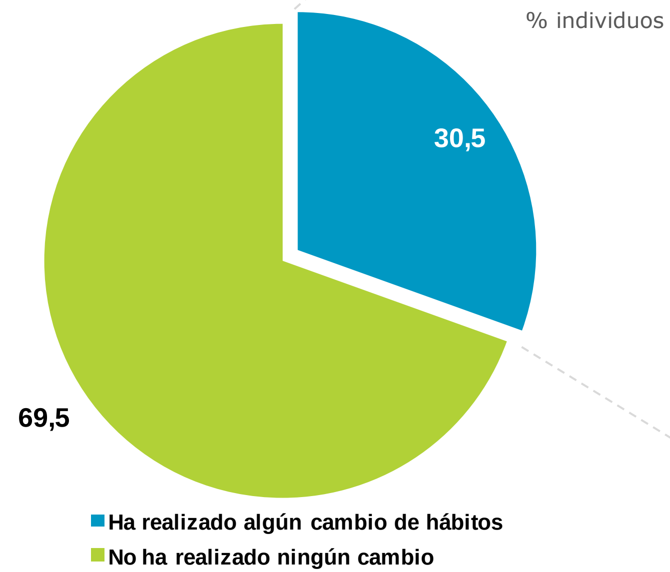
Tipología del malware analizado

✓ 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.

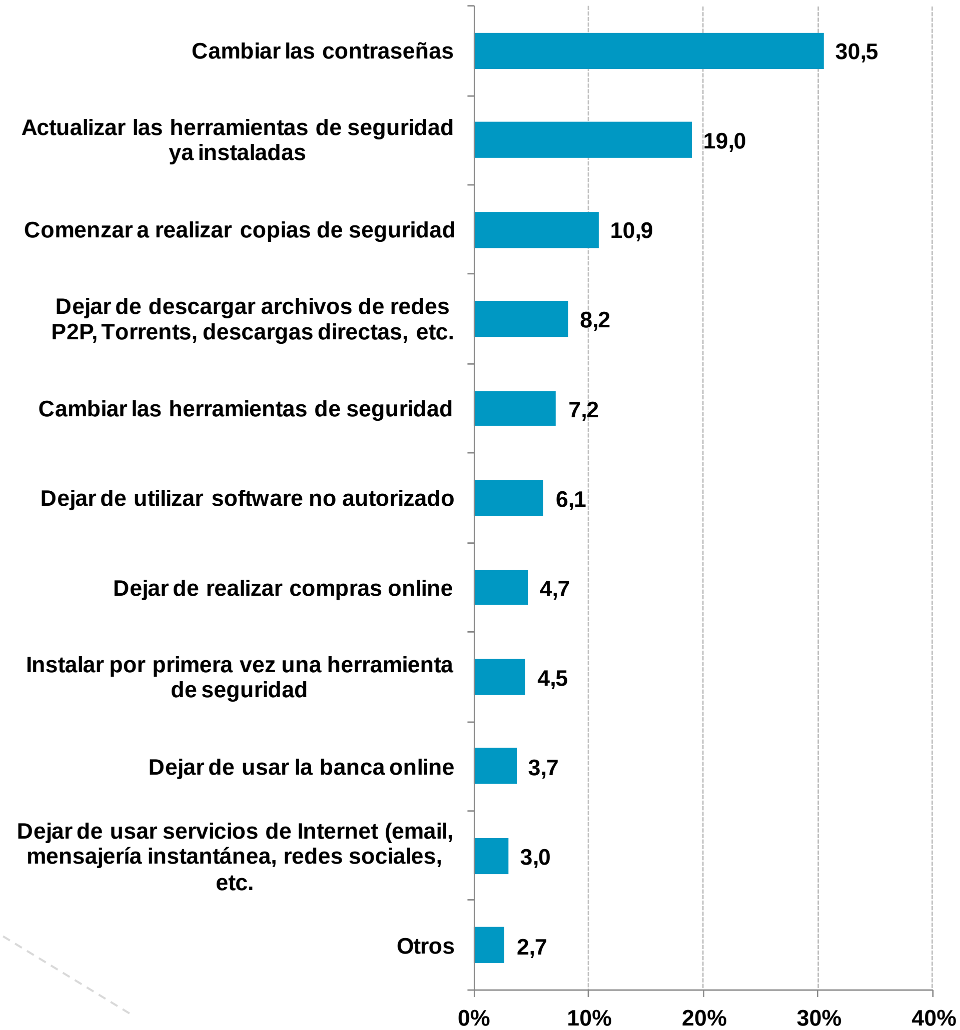
Cambios adoptados tras un incidente de seguridad



BASE: Total usuarios

Cambios realizados:

Respuesta múltiple



BASE: Usuarios que realizan algún cambio

5

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

La principal modificación de hábitos es el **cambio de contraseñas** (**43,7%**) a raíz de incidencias de **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	31,7	36,0	38,6	26,7	**43,7**	40,4
Actualizar herramientas	26,7	**30,8**	27,0	17,6	24,4	25,0
Realizar copias de seguridad	14,9	**25,1**	16,8	9,8	12,9	21,1
Cambiar herramientas	13,0	7,8	11,8	6,4	11,3	**22,5**
Abandonar software no autorizado	8,2	11,1	14,9	4,9	17,3	**20,6**
Instalar herramientas por 1ª vez	6,7	13,4	14,5	3,3	18,7	**21,8**

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

Las principales causas de modificación de hábitos de uso de servicios de Internet son las incidencias de **intrusión Wi-Fi**.

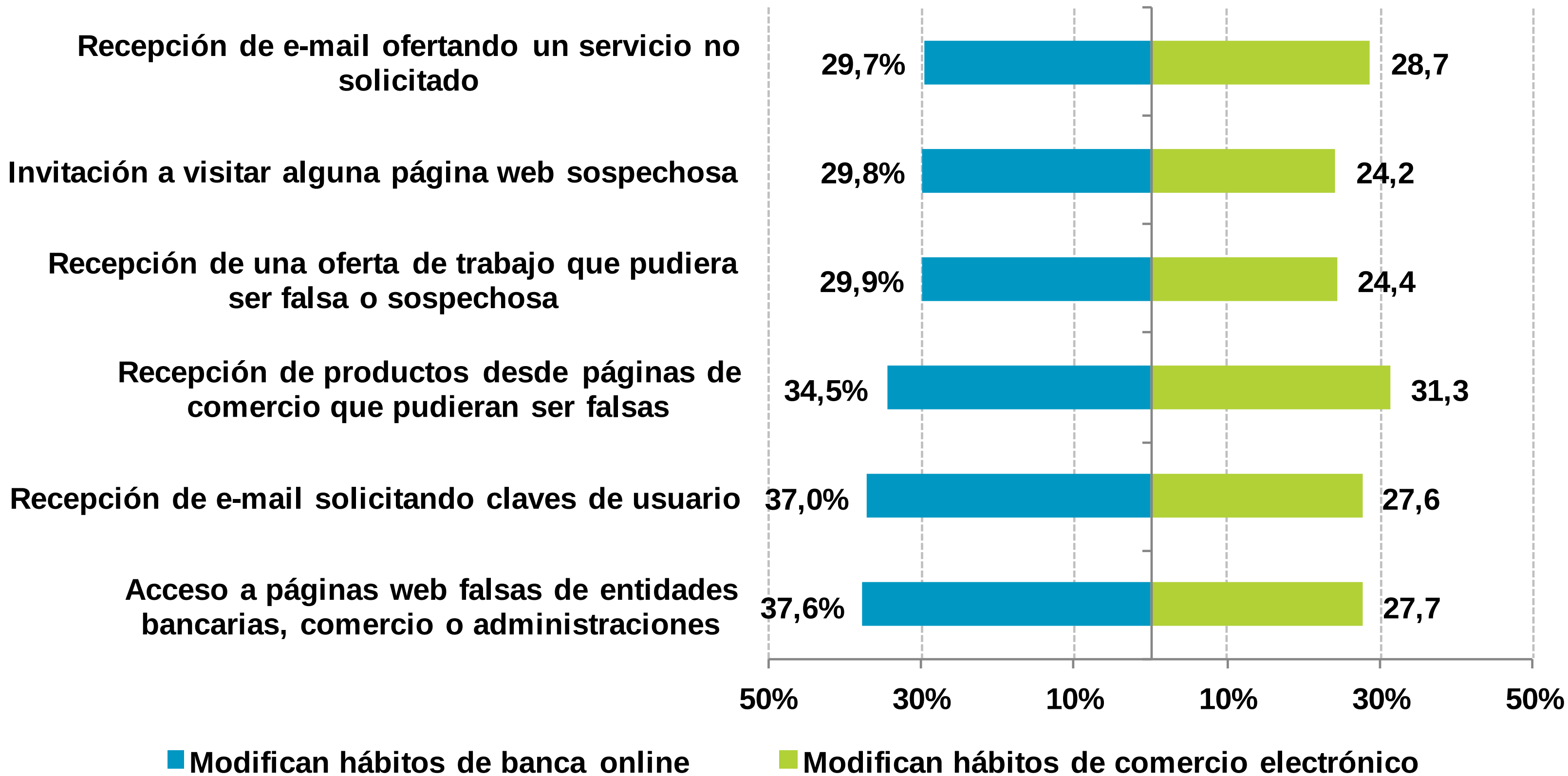
El **13,5%** deja de utilizar **servicios de Internet** después de una incidencia de **suplantación de identidad**.

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	9,7	17,1	18,3	7,3	14,6	**23,8**
Abandonar el comercio electrónico	6,6	14,9	7,7	3,1	12,3	**16,9**
Abandonar la banca online	5,1	14,5	9,5	2,8	12,3	**18,6**
Dejar de usar servicios de Internet	4,4	5,7	8,7	2,0	**13,5**	11,9

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

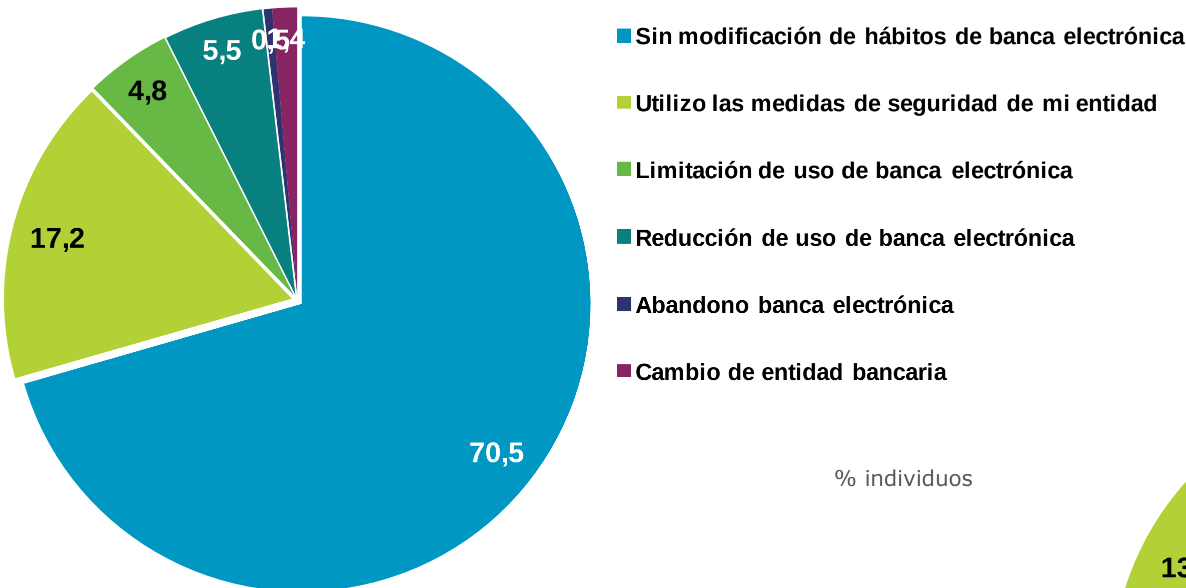
Influencia del intento de fraude en los servicios de banca online y comercio electrónico

La recepción de peticiones de **acceso a páginas web falsas** de entidades bancarias y/o comercio electrónico es la **principal causa de modificación de hábitos** por parte del **37,6%** y **27,7%** de usuarios de estos servicios, respectivamente.



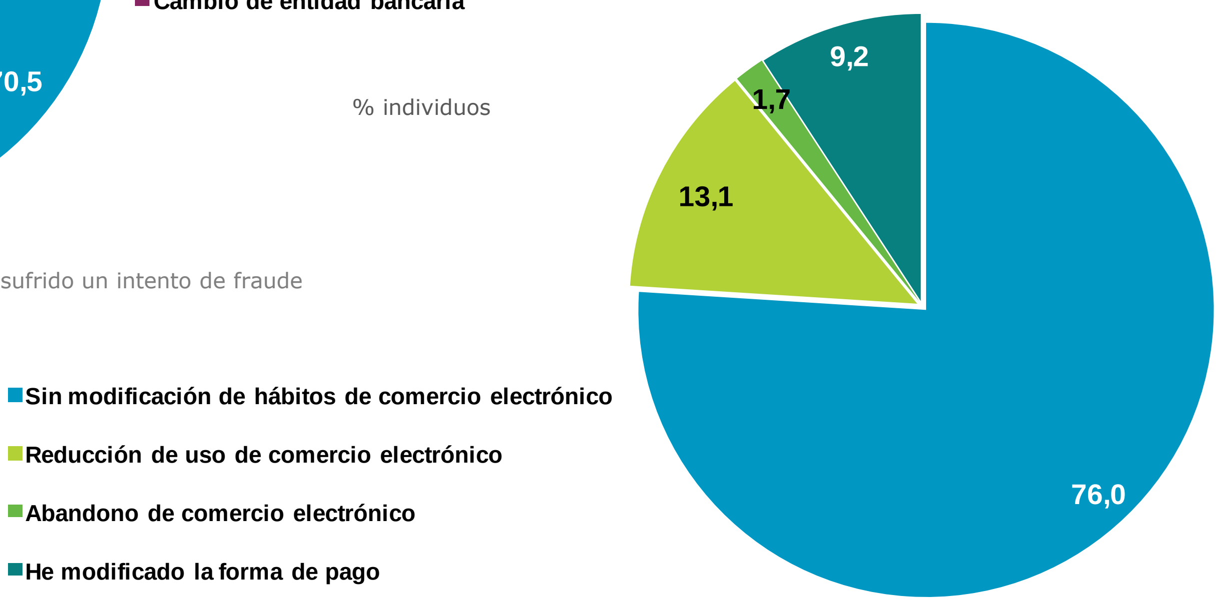
BASE: Usuarios que han sufrido un intento de fraude

Modificación de hábitos prudentes relacionados con los servicios de 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

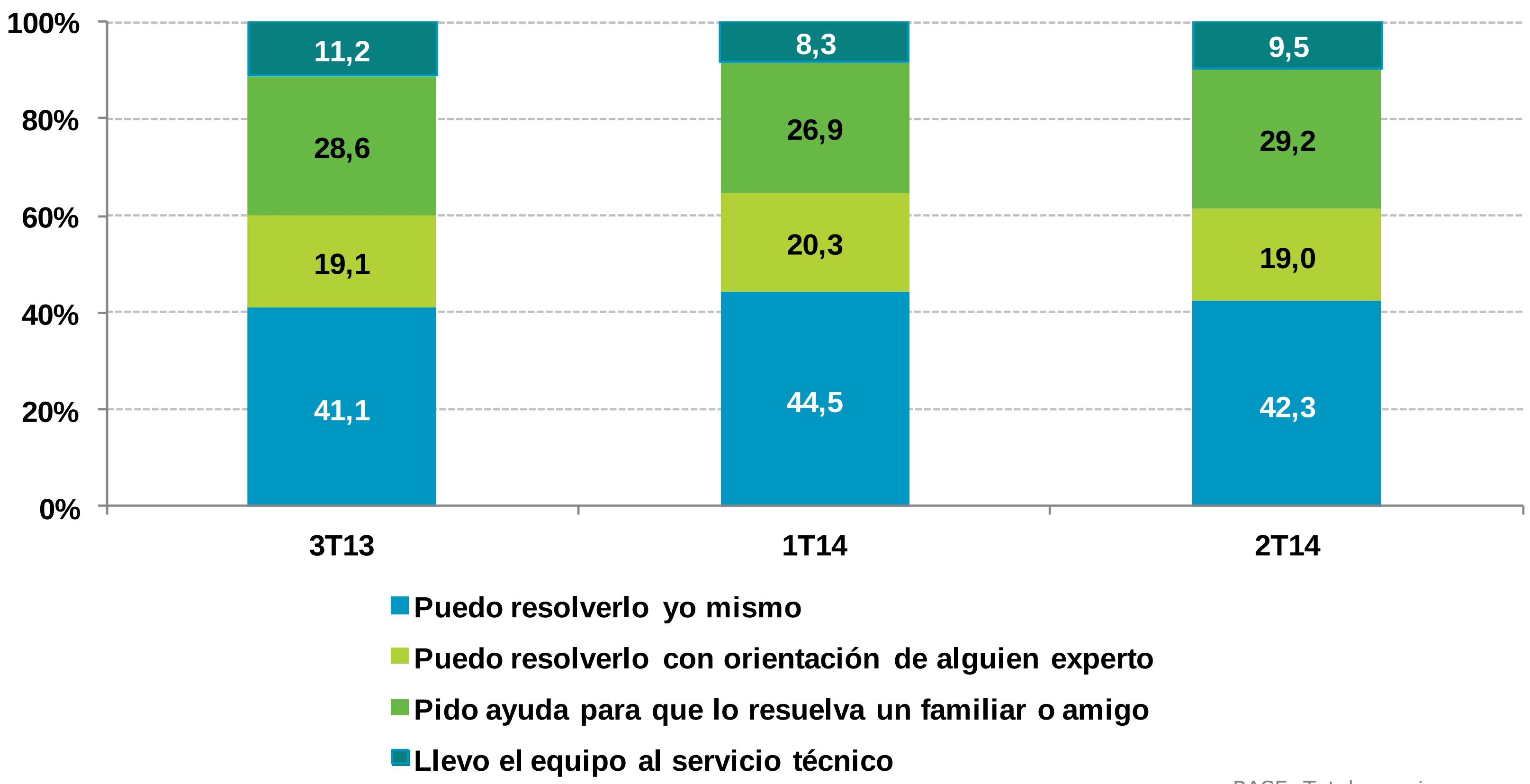


BASE: Usuarios que usan comercio electrónico y han sufrido un intento de fraude

Resolución de incidentes de seguridad

El **42,3%** de los internautas españoles declaran ser capaces de solucionar **ellos mismos** los problemas de seguridad y casi el **30%** solicita ayuda a un **familiar o amigo**.

El **servicio técnico profesional** es la opción declarada por menos del **10%** de la población española.

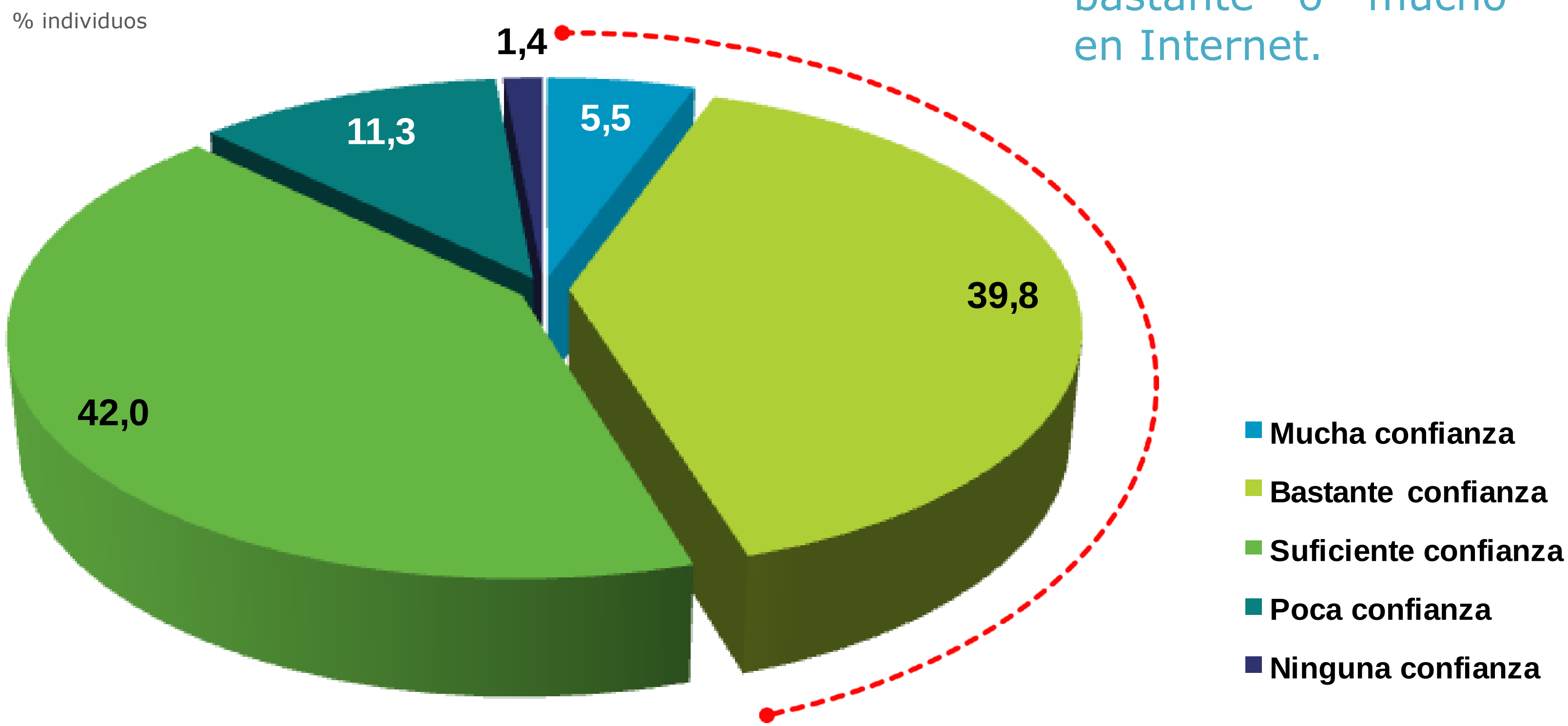


BASE: Total usuarios

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

6

Nivel de confianza en Internet



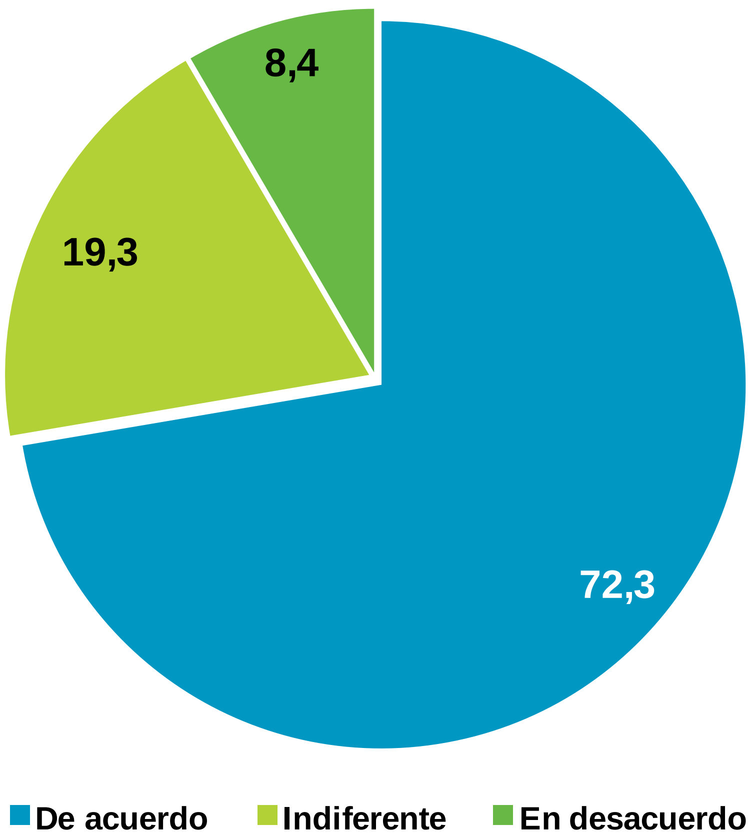
El **45,3% confía** bastante o mucho en Internet.

Apenas un **1,4%** de la población española **desconfía** de la red Internet.

BASE: Total usuarios

Valoración del ordenador personal como razonablemente protegido

% individuos

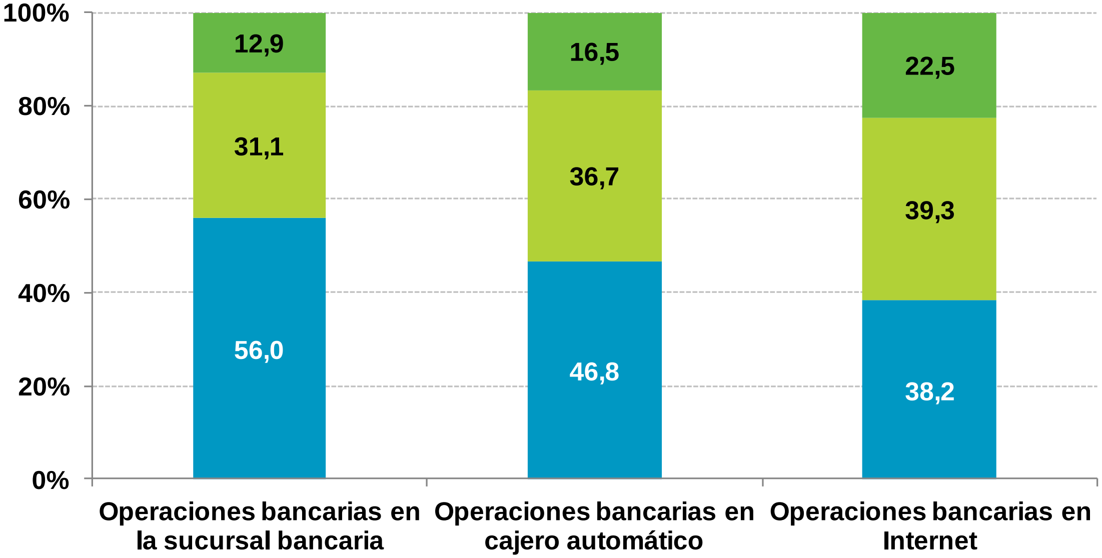


Casi tres de cada cuatro internautas (**72,3%**) opinan que su **equipo informático** se encuentra **razonablemente protegido** frente a las potenciales amenazas de Internet.

6

BASE: Total usuarios

Confianza online vs. confianza offline



Nivel de confianza en operaciones bancarias

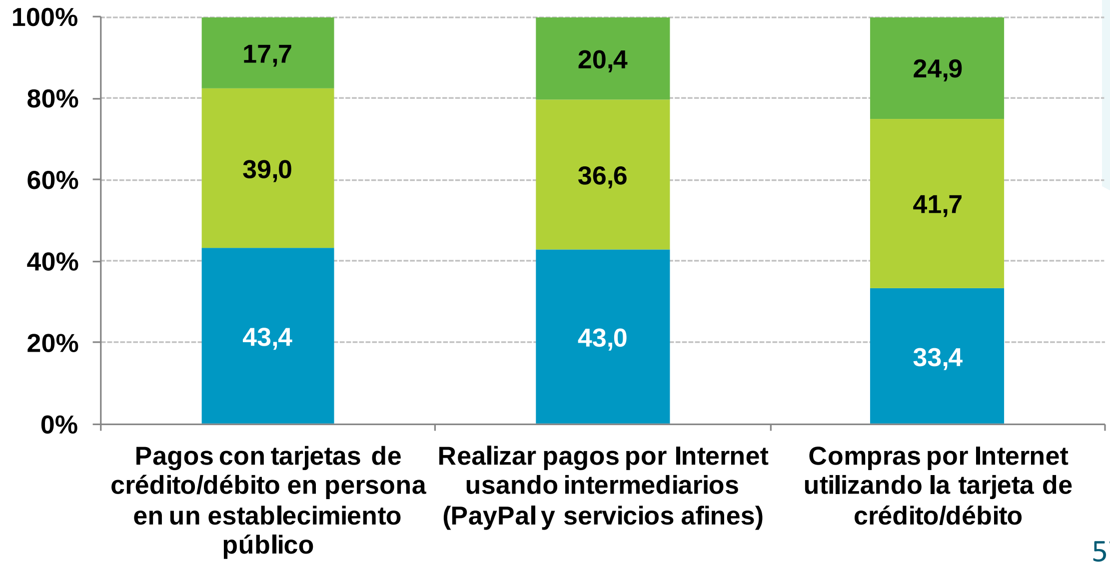
El usuario deposita mayor confianza en el trato con otra persona en la **entidad bancaria** (**56%**) que en aquellas **operaciones bancarias** realizadas a través de un **cajero automático** (**46,8%**) o mediante **Internet** (**38,2%**).

% individuos

6

Nivel de confianza en operaciones de compra-venta

El pago con **tarjeta de crédito/débito** en establecimiento público (**43,4%**) y el uso de intermediarios como **PayPal y servicios afines** (**43%**) para realizar pagos a través de Internet son las opciones preferidas por el usuario en **operaciones de compra-venta**.



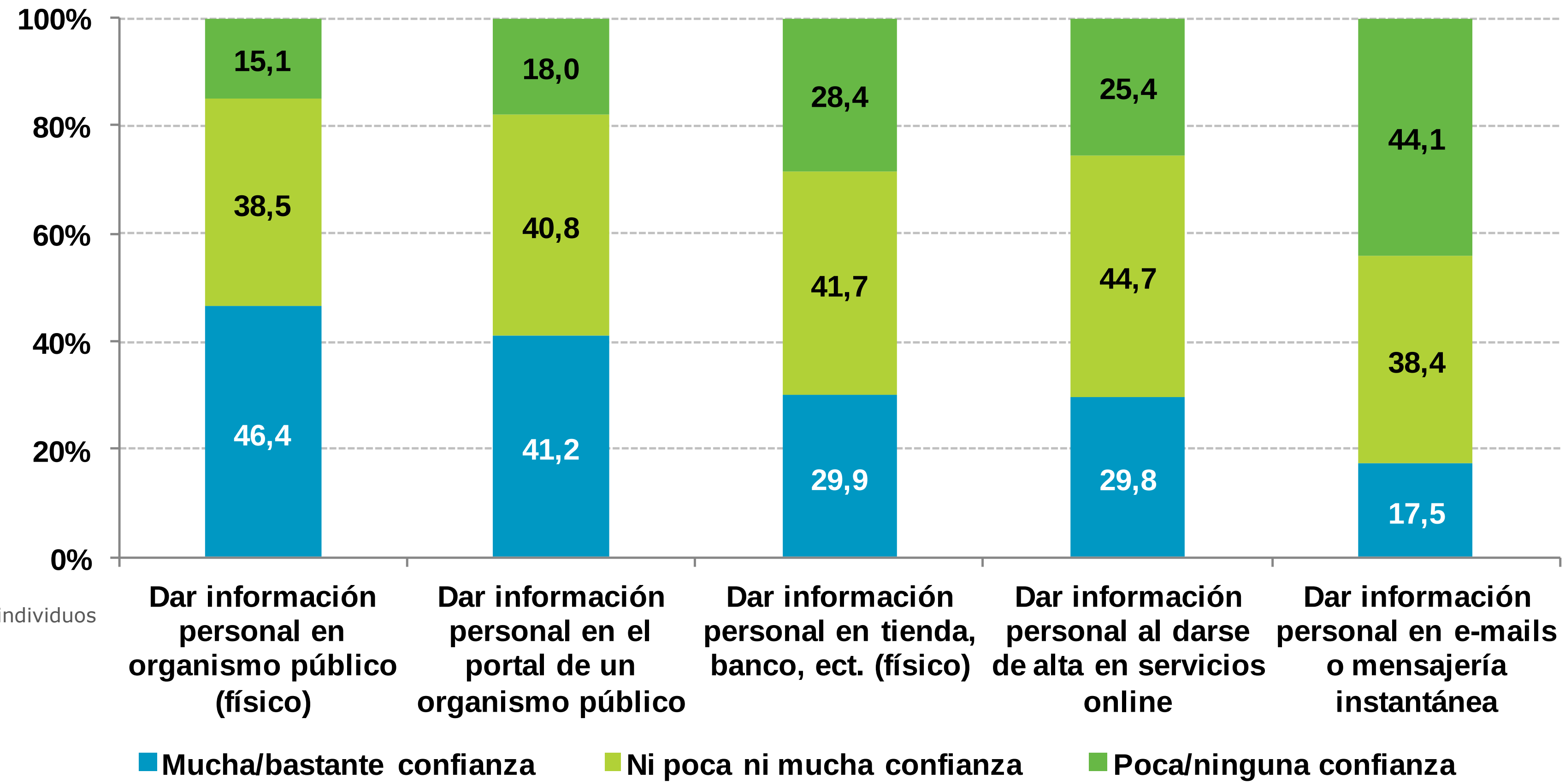
- Mucha/bastante confianza
- Ni poca ni mucha confianza
- Poca/ninguna confianza

BASE: Total usuarios

Confianza online vs. confianza offline

Un **17,5%** de la población afirma tener suficiente confianza para **facilitar información** de carácter personal a través de **correo electrónico, chat o mensajería instantánea**.

Nivel de confianza en facilitar datos personales

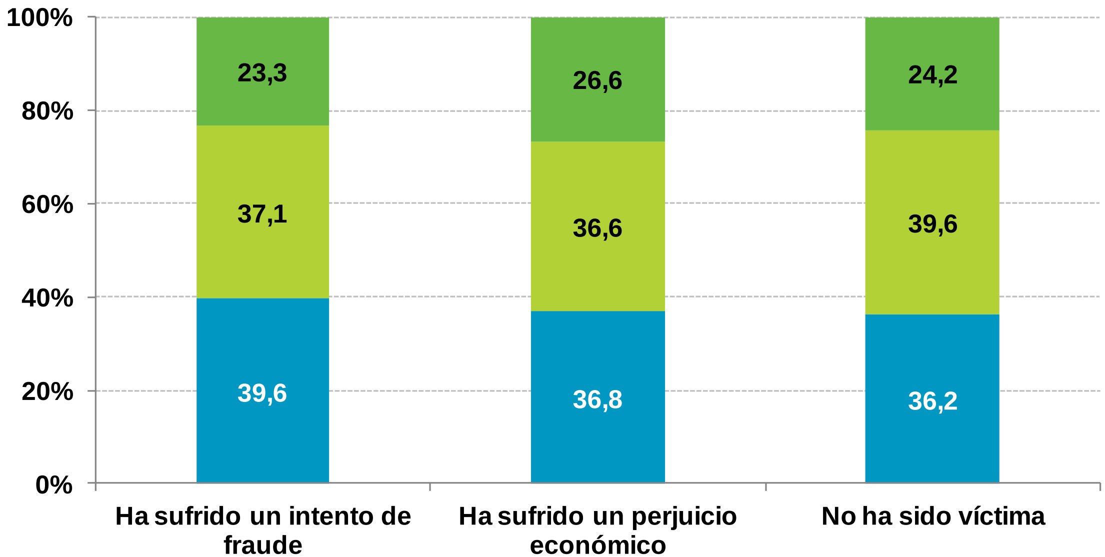


6

BASE: Total usuarios

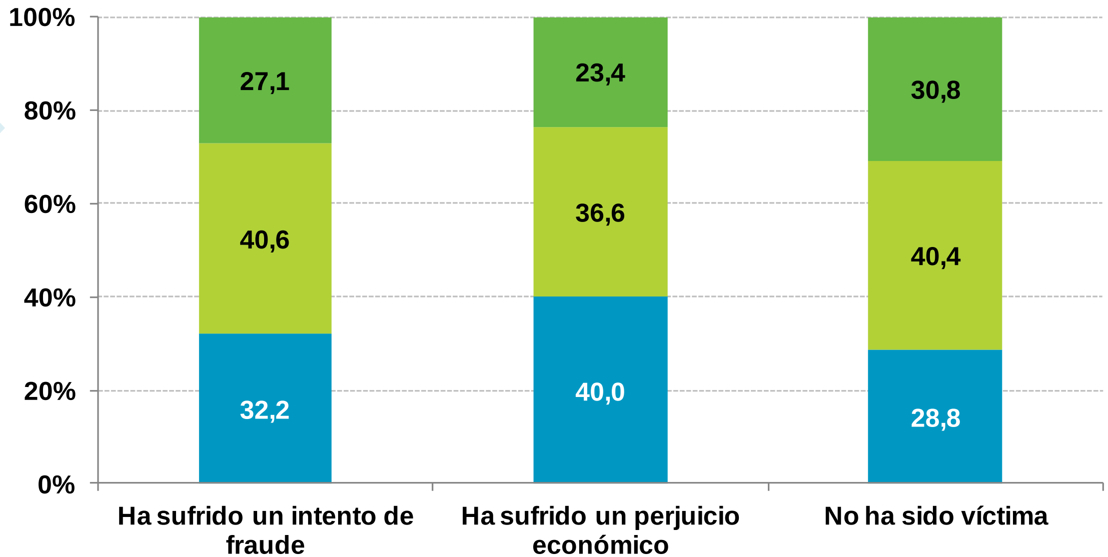
Confianza vs. fraude

Confianza al realizar operaciones bancarias en Internet



% individuos

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

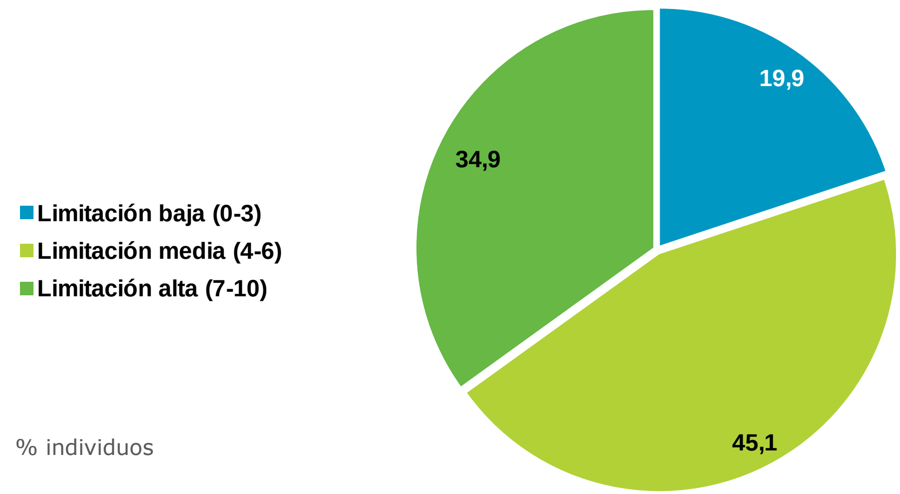


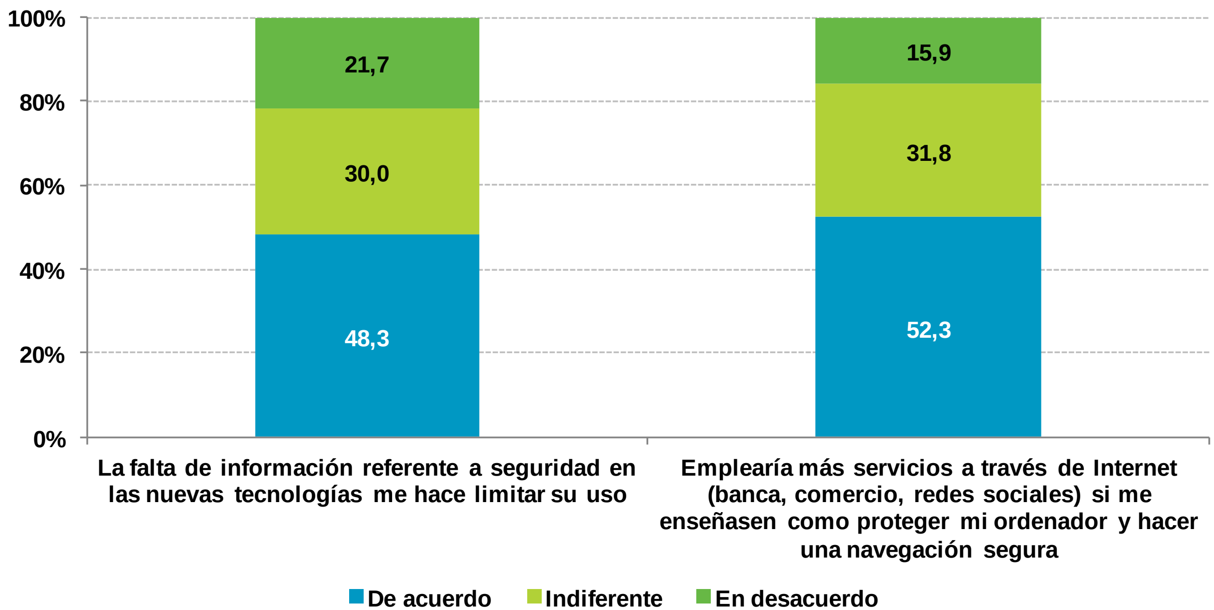
- Mucha/bastante confianza
- Ni poca ni mucha confianza
- Poca/ninguna confianza

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



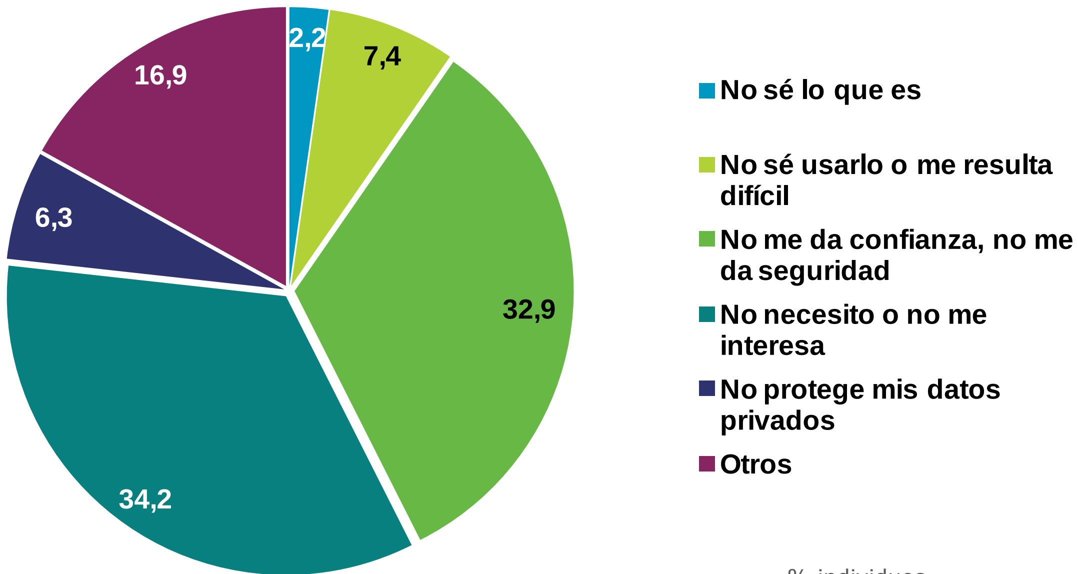


Limitaciones en el uso de Internet

BASE: Total usuarios

INSTITUTO NACIONAL DE CIBERSEGURIDAD

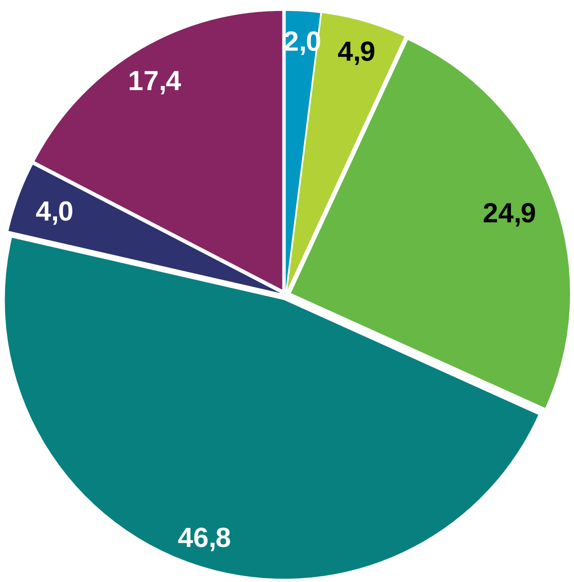
Razones para no utilizar banca online



% individuos

La **falta de necesidad y/o interés** es el **principal motivo** que alegan los usuarios para no utilizar los servicios de banca online (**34,2%**) y comercio electrónico (**46,8%**).

Razones para no utilizar comercio electrónico

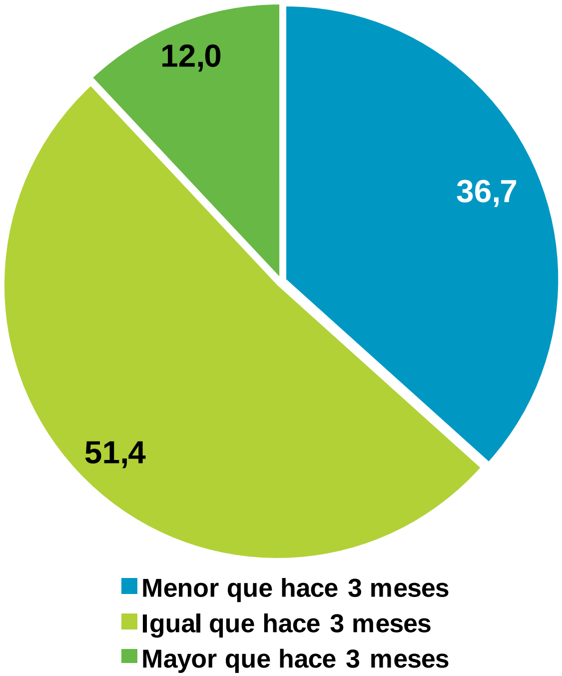


El **segundo motivo** concierne a la **falta de confianza** en estos servicios según el **32,9%** y **24,9%** de internautas que no usan la banca online y el comercio electrónico, respectivamente.

BASE : Usuarios que no utilizan el servicio

Percepción de los usuarios sobre la evolución en seguridad

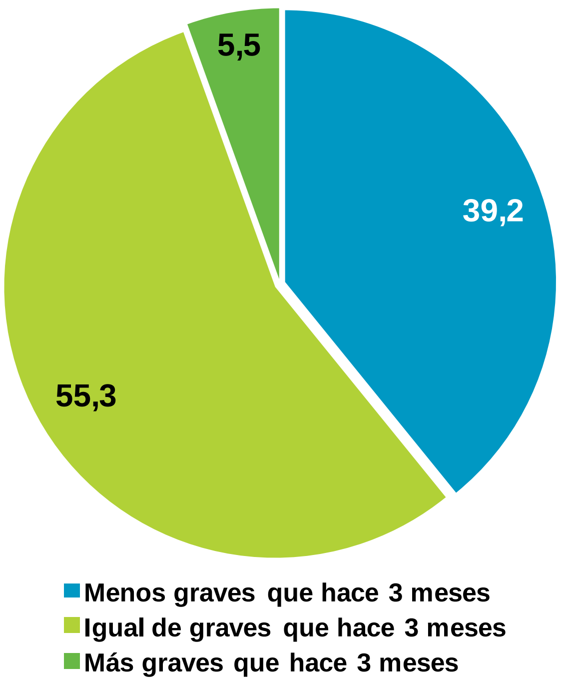
Número de incidencias



La percepción de los encuestados sobre las incidencias acontecidas en los últimos 3 meses con respecto a meses anteriores es que son **similares en cuanto a cantidad y gravedad** para **más de la mitad** (**51,4%** y **55,3%**, respectivamente).

% individuos

Gravedad de las incidencias



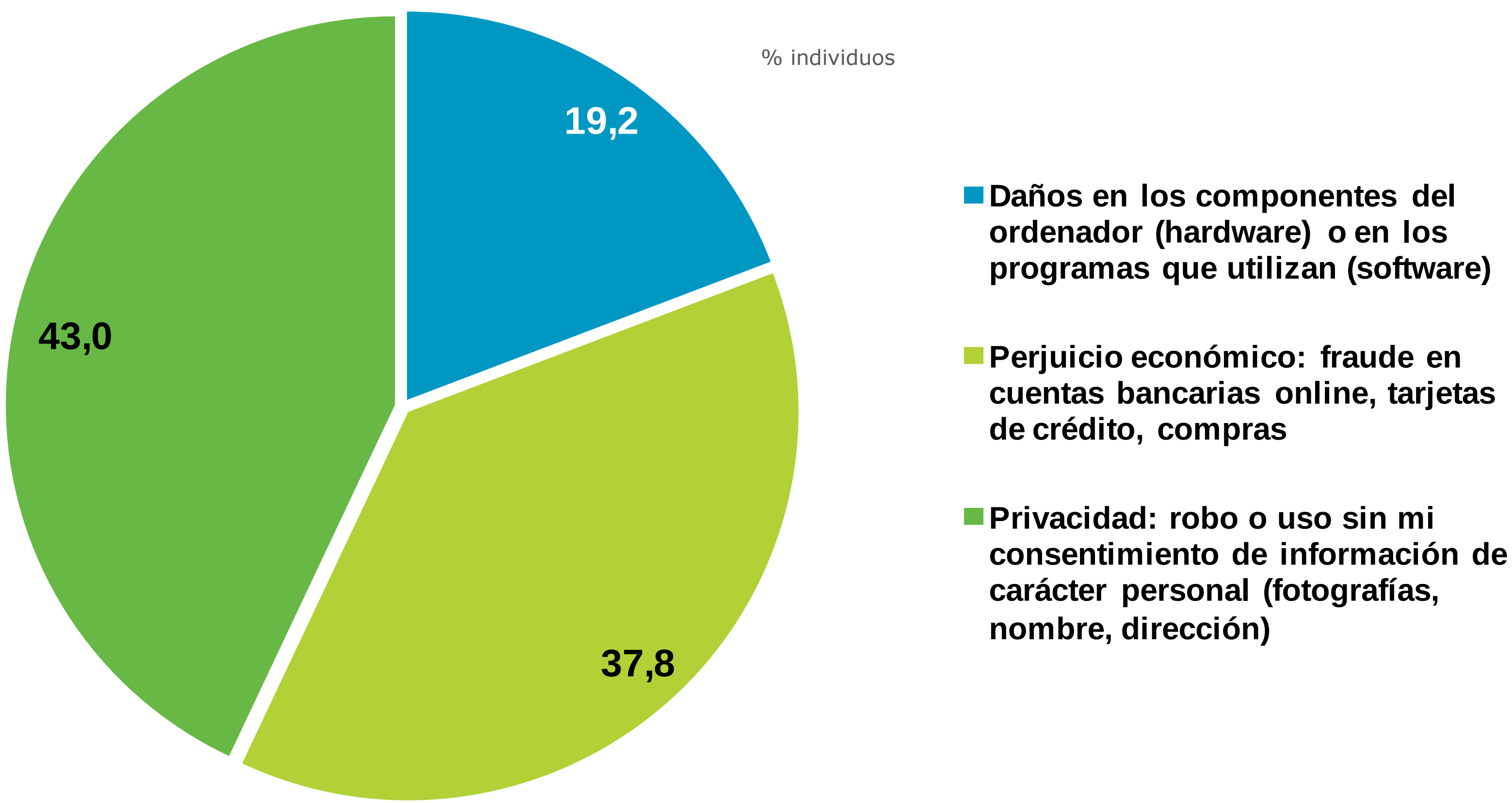
Más de un tercio (**36,7%**) percibe un **menor número** de incidencias en los últimos 3 meses y casi el **40%** las considera de **menor gravedad**.

BASE: Total usuarios

Percepción de riesgos en Internet

El **robo y uso de información personal** (**43%**) sin el consentimiento del usuario y el **perjuicio económico** (**37,8%**) derivado de un fraude son los principales riesgos en Internet percibidos por los internautas.

% individuos

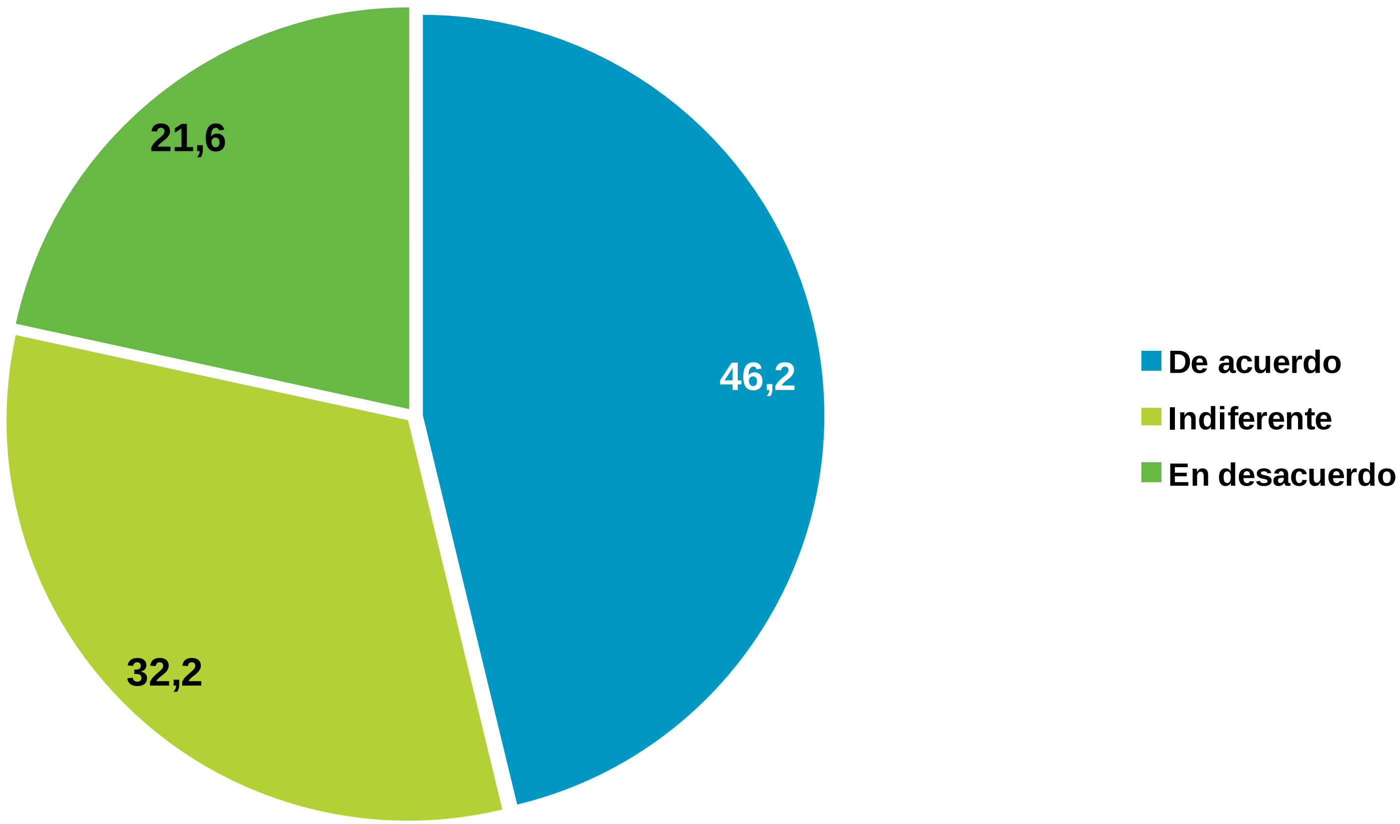


BASE: Total usuarios

Valoración de Internet cada día como más seguro

Un **46,2%** de los internautas españoles perciben **Internet cada día como más seguro**.

% individuos

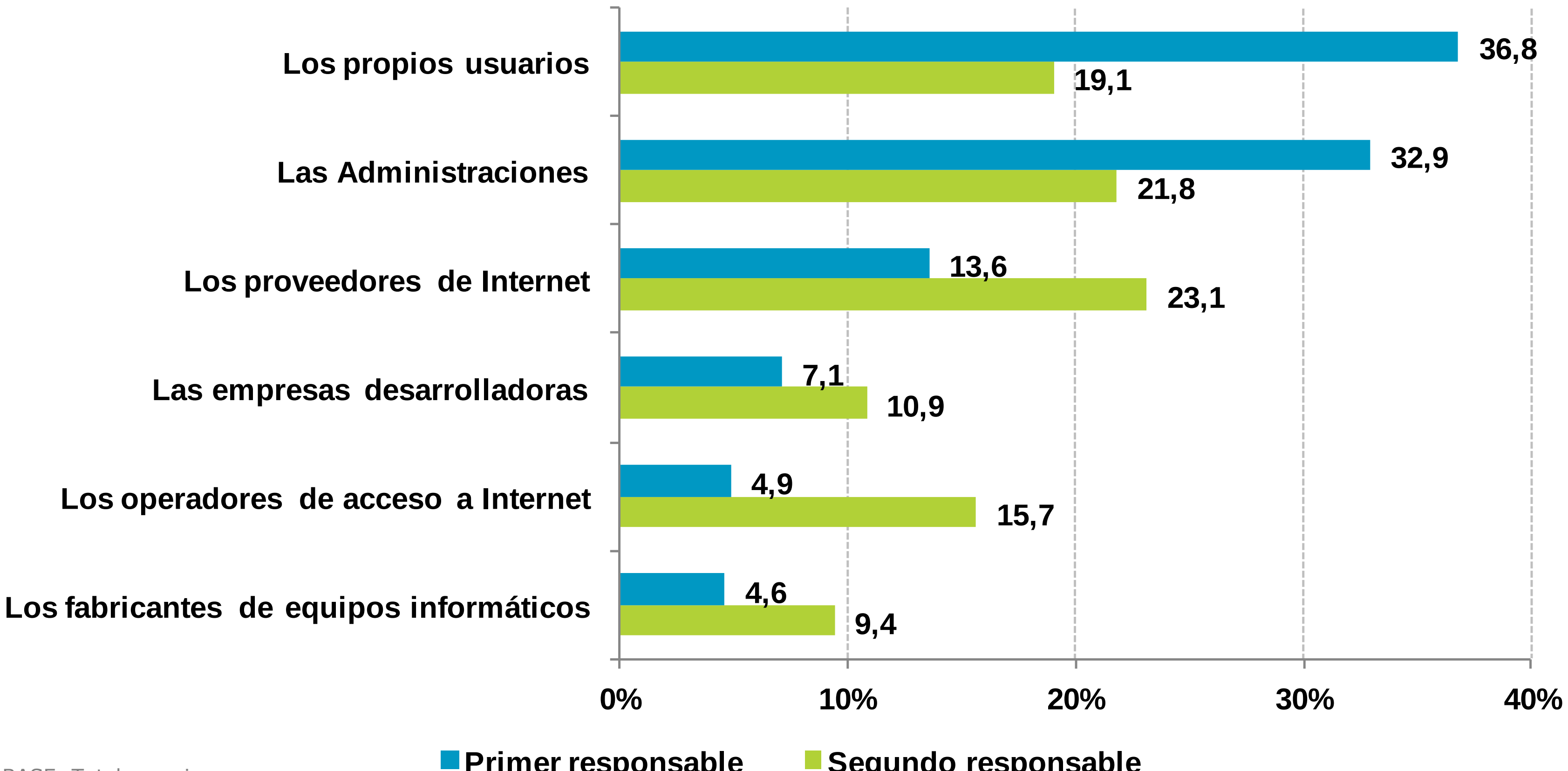


BASE: Total usuarios

Responsabilidad en la seguridad de Internet

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

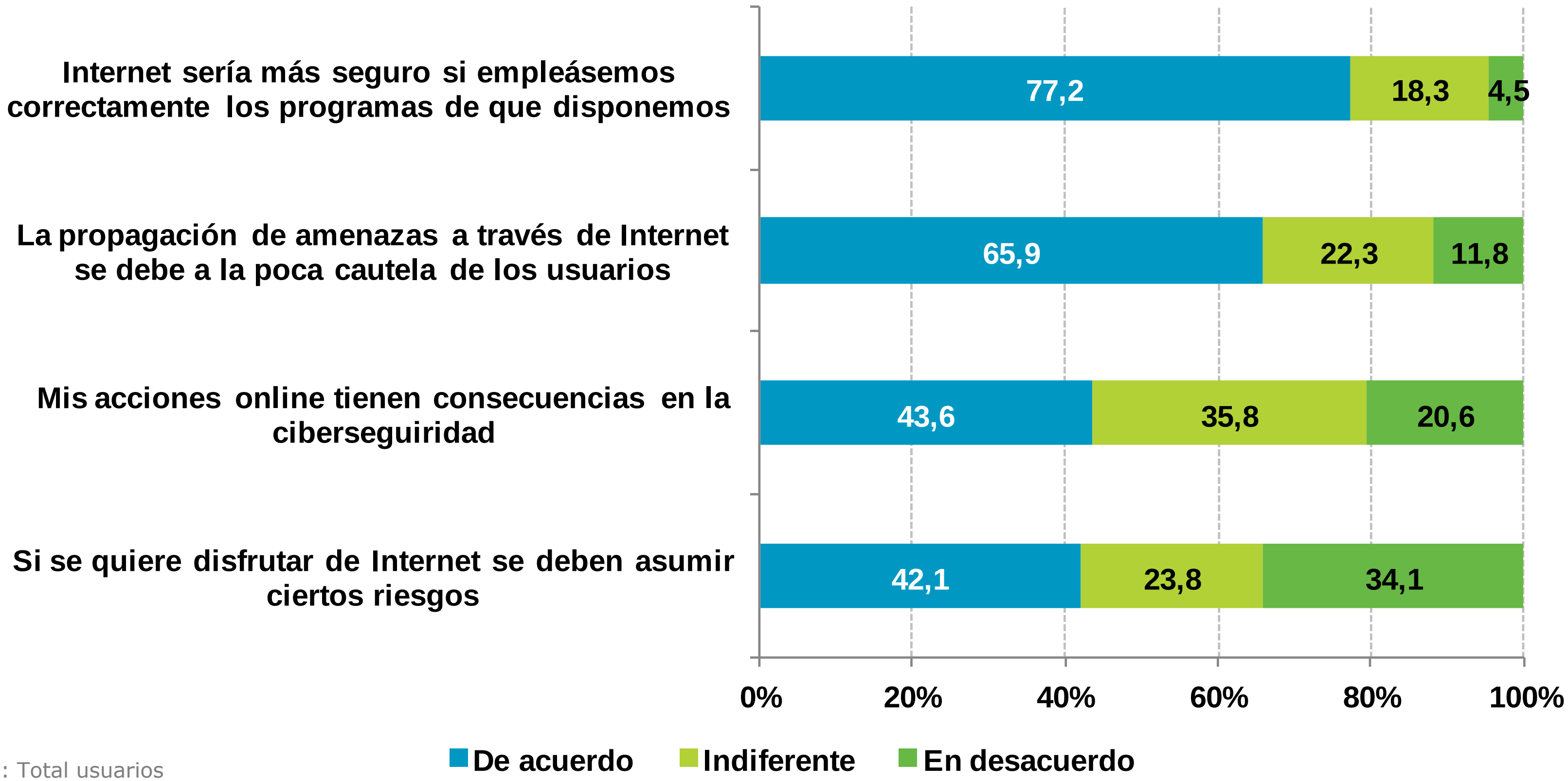
En opinión del **32,9%**, esta responsabilidad recae sobre las **Administraciones**.



BASE: Total usuarios

Rol del usuario

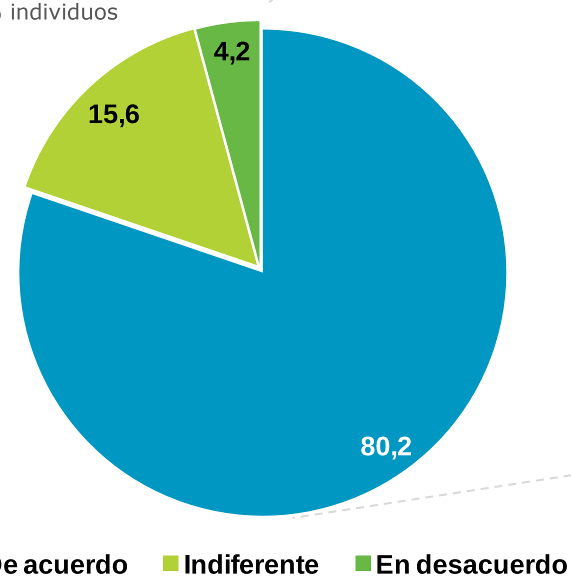
Una amplia mayoría de los internautas consideran que Internet sería más seguro **si se empleasen correctamente los programas** (**77,2%**) y que la **propagación de amenazas** a través de Internet se debe principalmente a la **poca cautela de los usuarios** (**65,9%**). Sin embargo, un **43,6%** creen que sus acciones online tienen **consecuencias en la ciberseguridad**, y otro **42,1%** opinan que se deben **asumir riesgos** para disfrutar de las experiencias que ofrece Internet.



BASE: Total usuarios

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

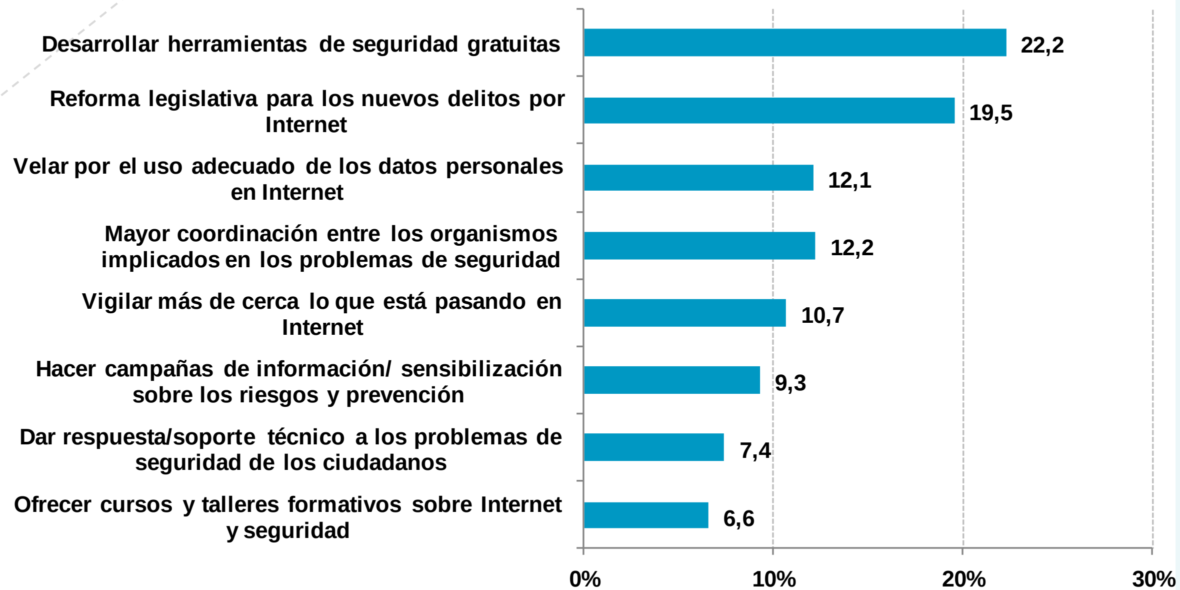
% individuos



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 con mayor presencia real en los equipos informáticos españoles son los programas antivirus (82%) y los cortafuegos (79,4%). En estos últimos, el nivel declarado es prácticamente la mitad del uso real.

El uso de las cuentas con permisos de administrador es, en Windows XP, prácticamente del 100%. En sistemas operativos posteriores se reduce su uso siendo del 28,5% en Windows 7, 13,2% en Windows Vista y llegando únicamente al 8% 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.

El 12,5% de los usuarios Wi-Fi con conexión propia no protege su red o desconoce si se aplica algún tipo de protección. Este porcentaje de personas que no se implican en la protección de su red inalámbrica aumenta casi al 50% si se agregan aquellos que usan el estándar WEP (11,1%), obsoleto y fácilmente eludible, o desconocen la tecnología que usan (25,8%).

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. Solo el uso de tarjetas monedero/prepago es utilizado por un número menor de usuarios (40,1%).

También se demuestran buenos hábitos en el uso de redes P2P entre los panelistas. Dos de cada 3 internautas no abre los ficheros descargados a través de estas redes si no tiene la certeza de haber sido analizados previamente mediante un antivirus. Tan solo el 13% de los usuarios de estas redes comparte todos sus archivos o no tiene control sobre lo que comparte (11,8%). En cuanto al uso de los smartphones, solo un 2,7% de los usuarios presentan comportamientos inseguros al descargar aplicaciones desde repositorios no oficiales.

En los hogares con menores que acceden a Internet los padres siguen buenas prácticas, destacando las medidas de comunicación, diálogo y educación (superior al 80%). La implicación en la navegación de los hijos es inferior al 68% y tan solo el 37,7% ha creado una cuenta con permisos limitados para su uso.

INCIDENTES DE SEGURIDAD

La incidencia más comúnmente sufrida continúa siendo el spam, afectando a más del 85% de las victimas de algún incidente, mientras que las relacionadas con virus y malware son declaradas únicamente por un 31,7% de aquellos usuarios que han sufrido alguna incidencia de seguridad. Considerando este porcentaje del total de usuarios, el 21,1% considera haber tenido alguna incidencia de malware. Sin embargo el impacto real casi triplica al declarado ya que iScan detecta un 60% de ordenadores infectados de malware durante el periodo estudiado. 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 (58,2%) que aquellos que no tienen aplicadas las actualizaciones (61,5%), la diferencia de infección no es excesiva, solo 3 puntos porcentuales por debajo.

Las principales incidencias relacionadas con los menores son haber facilitado información personal (14,3%) y el acceso a contenidos de carácter sexual (11,9%).

A pesar de el número de usuarios que potencialmente tiene su red inalámbrica expuesta, un porcentaje mínimo (solo el 1,7%) sospecha haber sufrido una intrusión en su red.

CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

El 48% de los panelistas han sufrido alguna vez un intento de fraude online, presentándose en el 27% de las ocasiones en la forma de comercio electrónico o loterías, casinos y juegos online. Los objetivos que el fraude persigue se mueve en cifras monetarias bajas para evitar la consideración de delito según el código penal. Así el 65,5% de los fraudes online y el 79,5% de los telefónicos estafaron menos de 100 euros, y entre 100 y 400 euros en el 22% y 19% de las ocasiones, respectivamente.

Entre los usuarios que han sufrido alguna incidencia de seguridad, casi un tercio (30,5%) 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 contraseñas 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 modificar su comportamiento en la red.

El 42,3% de los internautas piensa que pueden resolver por sí mismos los problemas de seguridad que puedan surgir al navegar por Internet.

CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

La confianza que los usurarios depositan en Internet es elevada: un 45,3% confía mucho o bastante en la Red mientras que solo un 1,4% desconfía totalmente de Internet. Así casi la mitad de los encuestados (46,2%) juzga Internet como cada día más seguro y un 72,3% estima que su ordenador está razonablemente protegido.

Para operaciones bancarias o de compra-venta, a los usuarios les da más confianza el trato personal que realizar estas acciones a través de la Red. La diferencia más notable –de casi 18 puntos porcentuales– se haya entre aquellos usuarios que confían en realizar operaciones bancarias en la sucursal (56%) y los que confían en efectuarlas online (38,2%). La operación que menos confianza genera entre los entrevistados es el pago a través de Internet utilizando la tarjeta de crédito/débito (33,4% de la población). En este ámbito, haber sufrido un intento de fraude o incluso un perjuicio económico no parece influir en el grado de confianza en tales servicios de banca online y comercio electrónico.

El 44% de los usuarios tiene poca confianza o ninguna a la hora de facilitar sus datos personales mediante un e-mail o mensajería instantánea. La mayor tasa de confianza se presenta al facilitar datos en un organismo público físico (46,4%), o bien en portales de organismos públicos (41,2%).

Respecto al papel que ejerce la Administración en la seguridad de la Red de redes, un 80,2% los usuarios consideran que ésta debería tener una mayor implicación con medidas tales como el desarrollo de herramientas de seguridad gratuitas y la reforma legislativa para los delitos de Internet con un 22,2% y un 19,5% respectivamente, de aquellos que consideran que la administración debe implicarse más en garantizar la seguridad en Internet.

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

Tamaño Muestral: 3.097 hogares encuestados y de ellos, 2.131 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 abril y junio 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=3.097 le corresponde una estimación del error muestral igual a ±1,76%.

8

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 Ciberseguridad (INCIBE) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es:

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Dirección: Marcos Gómez Hidalgo
Coordinación: Elena García Díez
Dirección técnica: Héctor R. Suárez
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:

INSTITUTO NACIONAL DE CIBERSEGURIDAD

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