Estudio sobre la Ciberseguridad y confianza en los hogares españoles

Oleada Julio – Diciembre 2017

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

Mayo 2018

INDICE

Introducción al estudio

1. **Presentación**
2. **Objetivos**

Presentación

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es, ha 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 3.695 hogares que han conformado la muestra del estudio.
- Dato real: Para ello se utiliza el software **Pinkerton** desarrollado por Hispasec Sistemas, que analiza los sistemas recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas. **Pinkerton** también detecta la presencia de malware en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 50 motores antivirus. Los datos así extraídos se representan en el presente informe con la siguiente etiqueta:

Los datos reflejados en **este informe abarcan el análisis desde julio hasta diciembre de 2017**.

Presentación

1

El actual estudio recoge información concerniente a datos presentados en estudios sobre la ciberseguridad y confianza en los hogares españoles realizados con anterioridad.

El objetivo es poder contrastar dicha información con la obtenida en el presente estudio, y de este modo determinar la evolución experimentada en el ámbito de la ciberseguridad y confianza digital.

Para designar a cada estudio se han utilizado las nomenclaturas que se exponen a continuación:

- **2S15**, estudio realizado en el segundo semestre de 2015 (julio - diciembre).
- **1S16**, estudio realizado en el primer semestre de 2016 (enero - junio).
- **2S16**, estudio realizado en el segundo semestre de 2016 (julio - diciembre).
- **1S17**, estudio realizado en el primer semestre de 2017 (enero - junio).
- **2S17**, estudio realizado en el segundo semestre de 2017 (julio - diciembre).

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 y dispositivos móviles 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

1. Definición y clasificación de las medidas de seguridad
2. Uso de medidas de seguridad en el ordenador del hogar
3. Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi
4. Uso de medidas de seguridad en dispositivos Android
5. Motivos de no utilización de medidas de seguridad

Definición y clasificación de las medidas de seguridad

Medidas de seguridad[1]

Son programas o acciones utilizadas por el usuario para proteger el ordenador y los datos que se encuentren en este. Estas 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: https://www.osi.es/herramientas

Guía de Privacidad y Seguridad en Internet : https://www.osi.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf

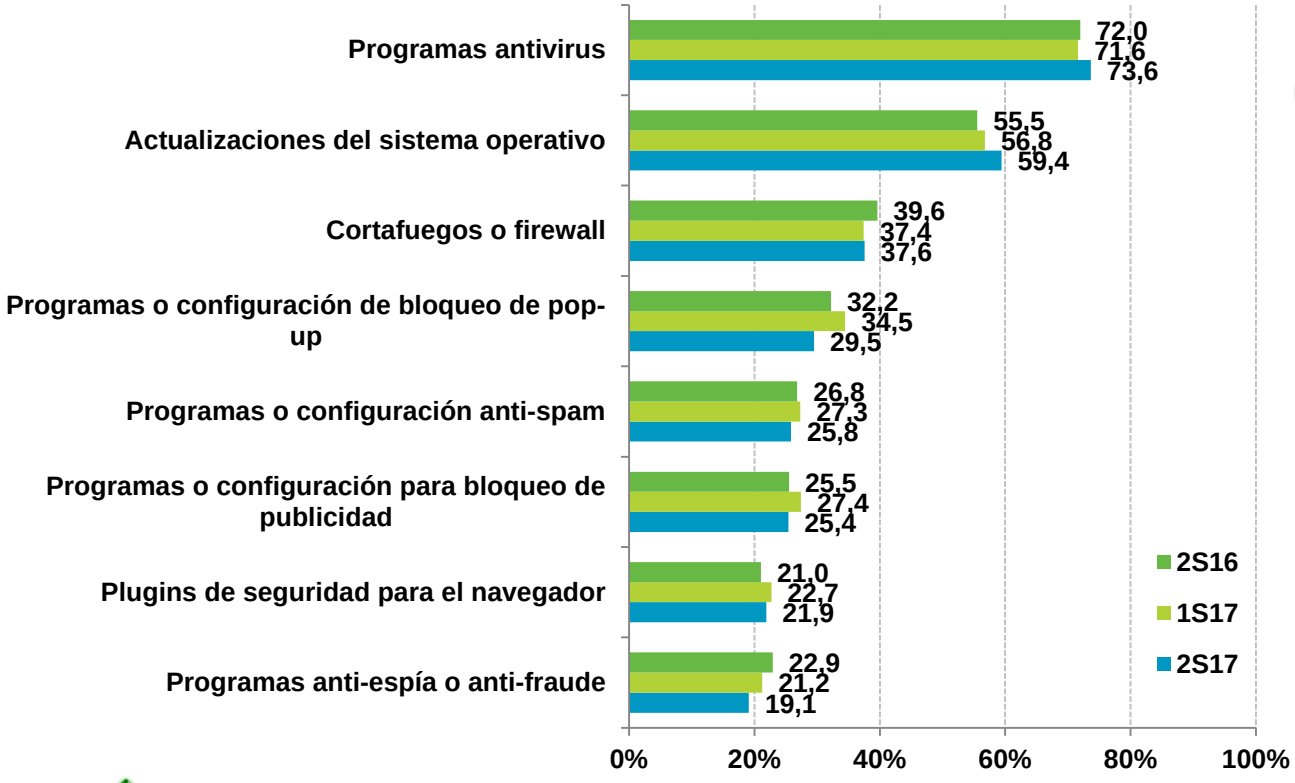
[1] Existen medidas de seguridad que por su condición se pueden clasificar en varias categorías, tal es el caso de los programas antivirus y sus actualizaciones, o las del sistema operativo. Un programa antivirus, por su naturaleza puede detectar tanto las amenazas existentes en el equipo como aquellas 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 • Uso de máquinas virtuales
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

Se aprecia un crecimiento en la utilización de **programas antivirus** (**+2,0 p.p.**) y **actualizaciones del sistema operativo** (**+2,6 p.p.**) durante el segundo semestre de 2017.



La funcionalidad de los programas antivirus no se limita únicamente a eliminar el malware presente en el equipo. Su cometido más importante es prevenir y evitar las infecciones de malware.

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

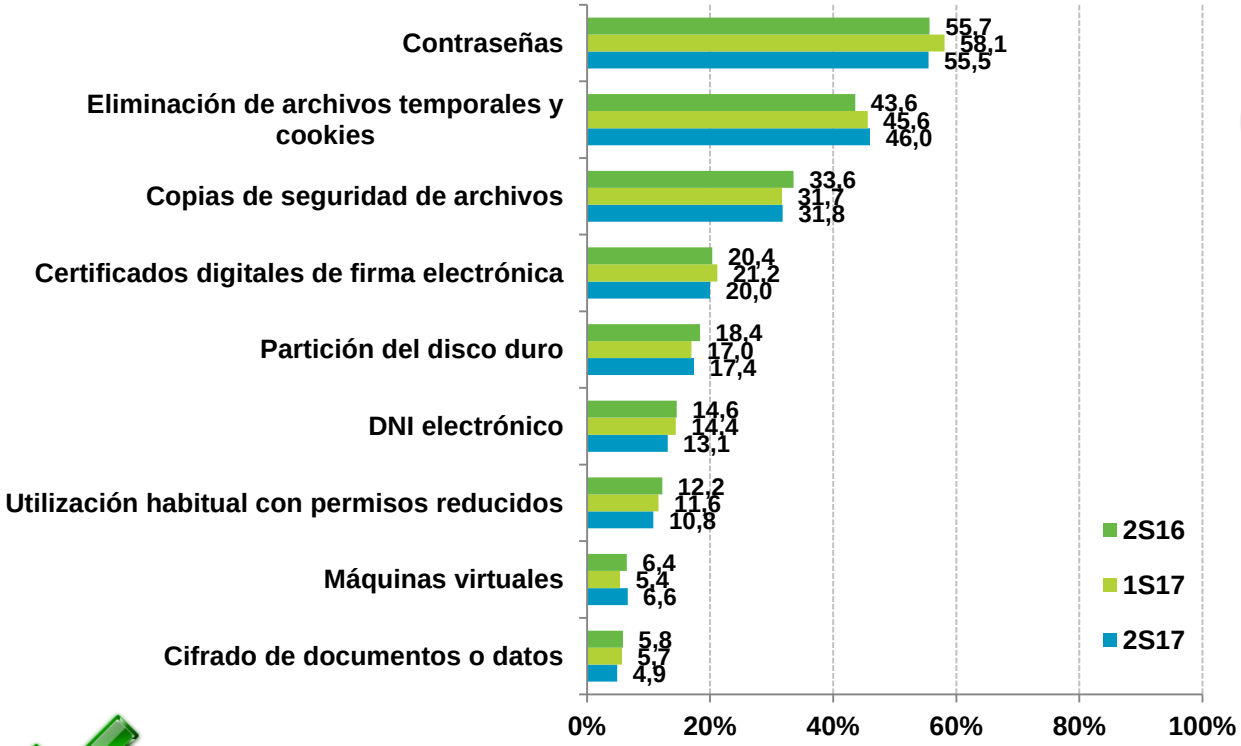
BASE: Usuarios de PC

¿Sabes por qué son importantes las actualizaciones de seguridad? https://www.osi.es/es/actualizaciones-de-seguridad

Uso de medidas de seguridad en el ordenador del hogar

Medidas de seguridad no automatizables o activas

El uso de **contraseñas** por parte de los usuarios disminuye **-2,6 p.p**. desde el estudio anterior, situándose nuevamente en valores similares a los observados a finales de 2016.



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

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

BASE: Usuarios de PC

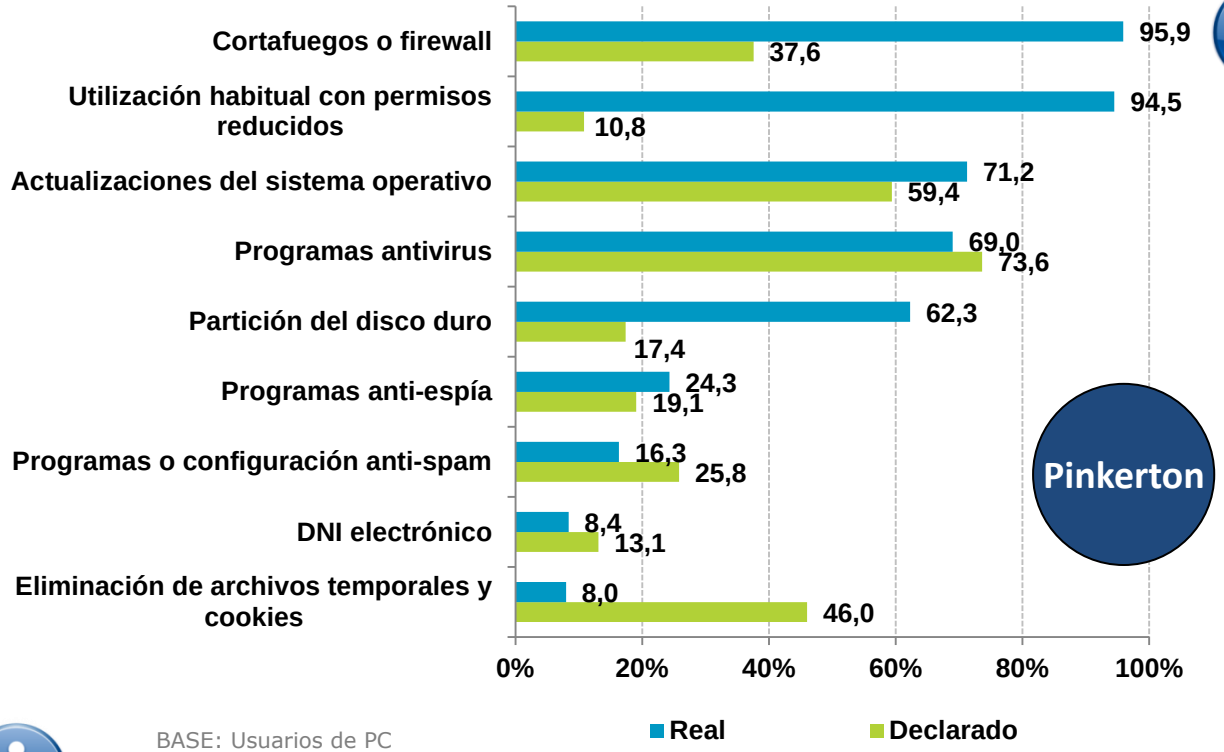
Es muy importante gestionar correctamente las contraseñas y además, realizar copias de seguridad de los datos que queremos salvaguardar. Obtén más información sobre cómo realizar estas tareas:

- ✓ **Contraseñas:** https://www.osi.es/contrasenas
- ✓ **Copias de seguridad:** https://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

Aumenta la brecha entre el uso real y declarado de **programas cortafuegos** (**58,3 p.p.**) y **usuario habitual con permisos reducidos** (**83,7 p.p.**). Los datos son favorables a la **utilización real**.



BASE: Usuarios de PC

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 muchas tipologías.

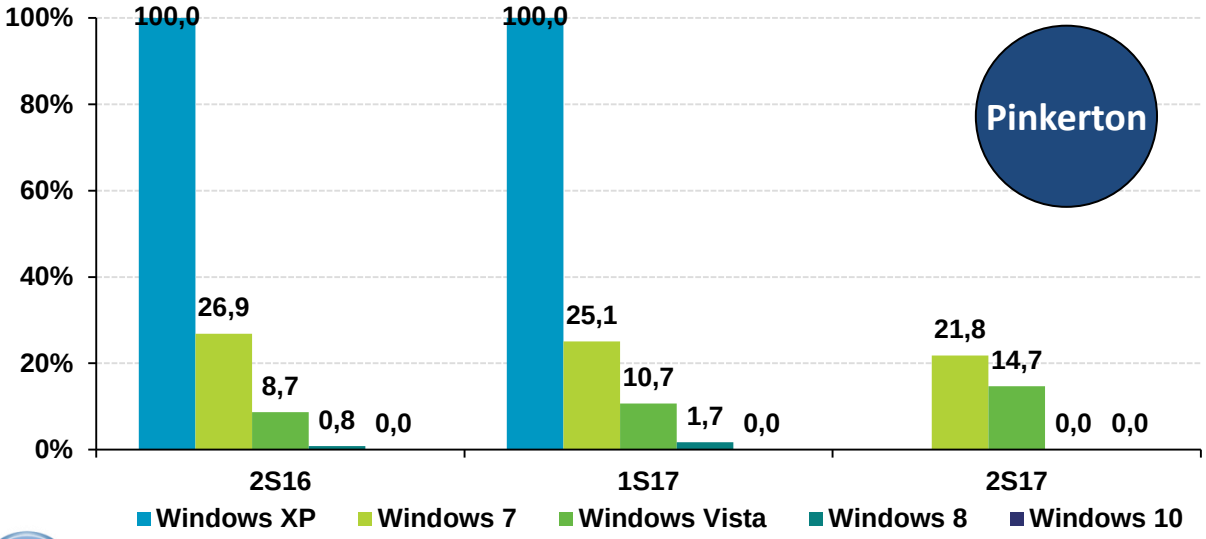
https://www.osi.es/es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

Para la obtención del dato real se utiliza el software **Pinkerton** desarrollado por Hispasec Sistemas, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 50 motores antivirus. **Pinkerton** 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 con privilegios de administrador en 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: https://www.osi.es/cuentas-de-usuario



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

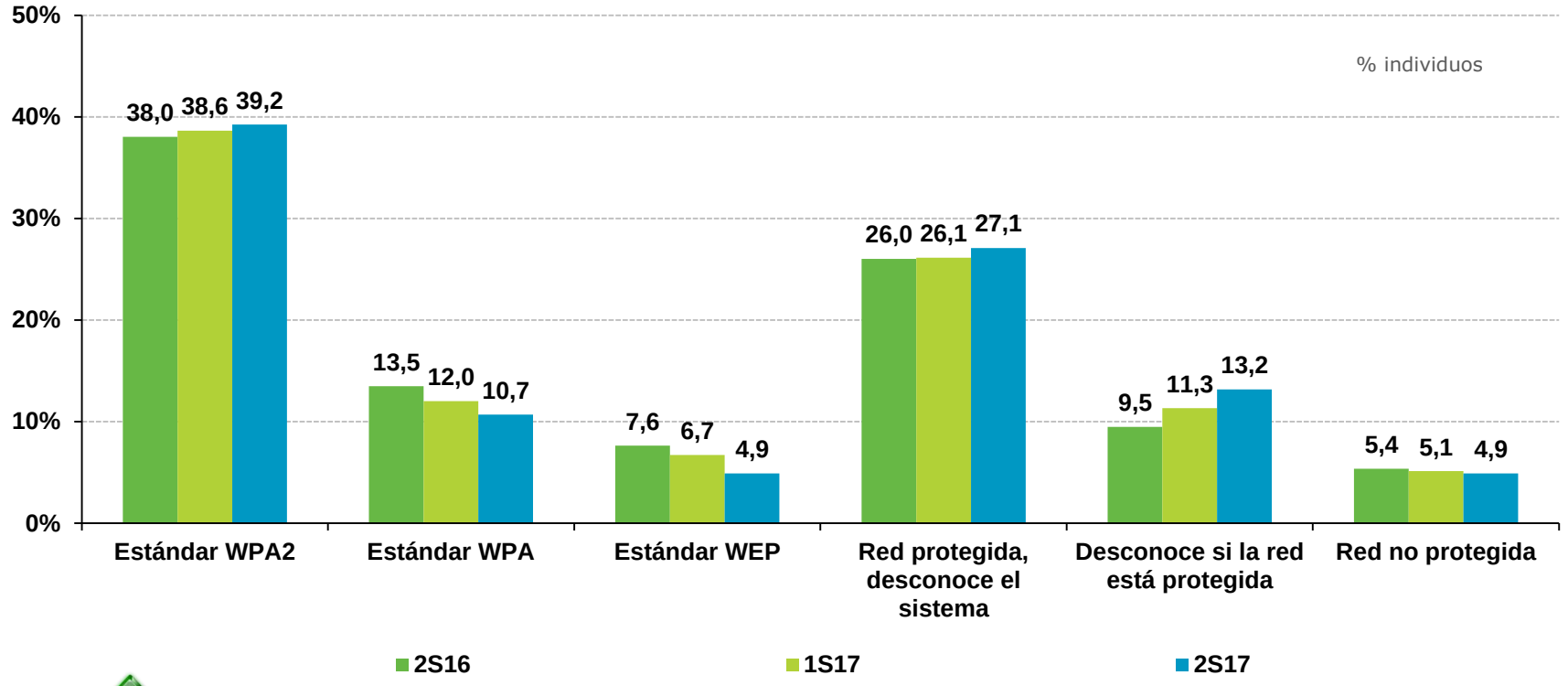
BASE: Usuarios de Microsoft Windows

Pueden existir sistemas operativos Windows 10 identificados como otras versiones anteriores. Esto es debido al proceso de actualización llevado a cabo por Microsoft, que permite la instalación de Windows 10 sobre una versión de Windows 7, 8 u 8.1, manteniendo archivos de la antigua versión del sistema operativo para facilitar una posible restauración de dicha versión.

Por otro lado, a partir de 2S17, Microsoft Windows XP, deja de contemplarse a efectos del presente estudio al tratarse de un sistema operativo obsoleto y sin soporte desde Abril de 2014.

Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi

El desconocimiento del estado de la red inalámbrica Wi-Fi del hogar se incrementa nuevamente en este periodo (**+1,9 p.p.**) llegando al **13,2%** de usuarios.



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

BASE: Usuarios Wi-Fi con conexión propia

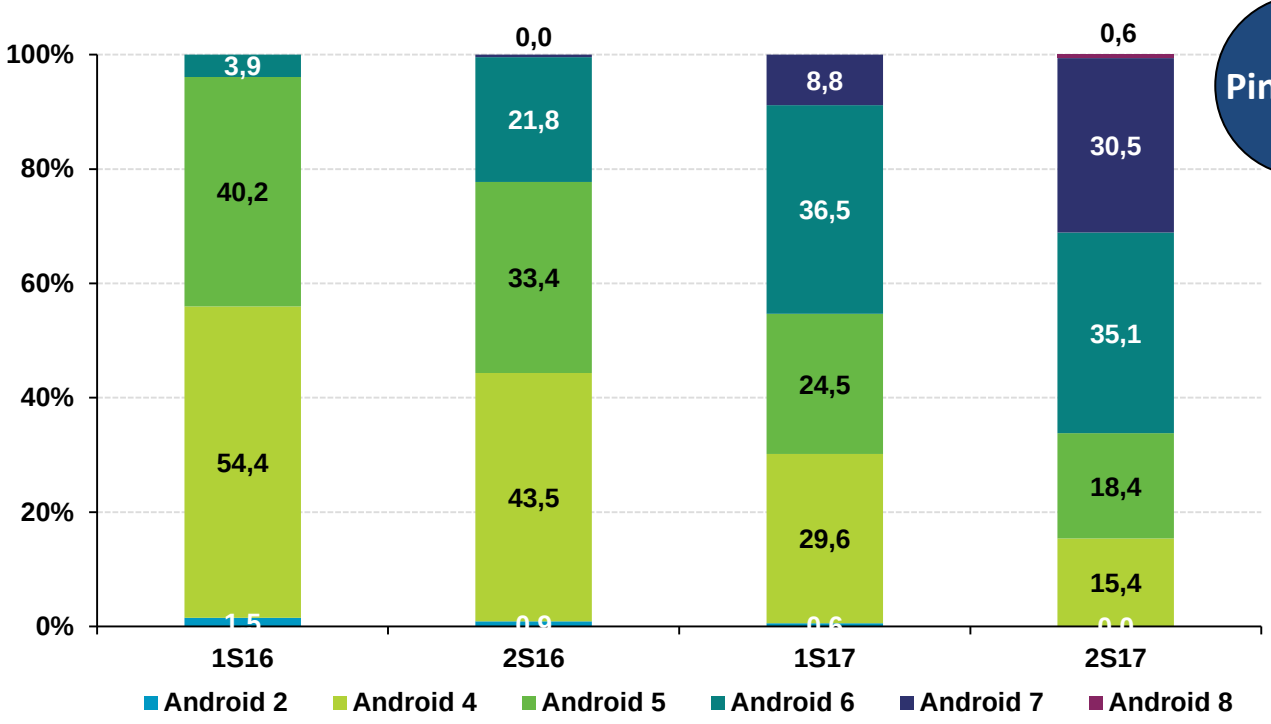
Uso de medidas de seguridad en dispositivos Android

Versión del sistema operativo en dispositivos Android

Android 6 (**35,1%**) y 7 (**30,5%**) se tornan en las versiones mayoritariamente utilizadas en smartphones y tablets. El uso de las versiones 4 y 5 se reduce hasta el **15,4%** y **18,4%** respectivamente.

Pinkerton

% individuos

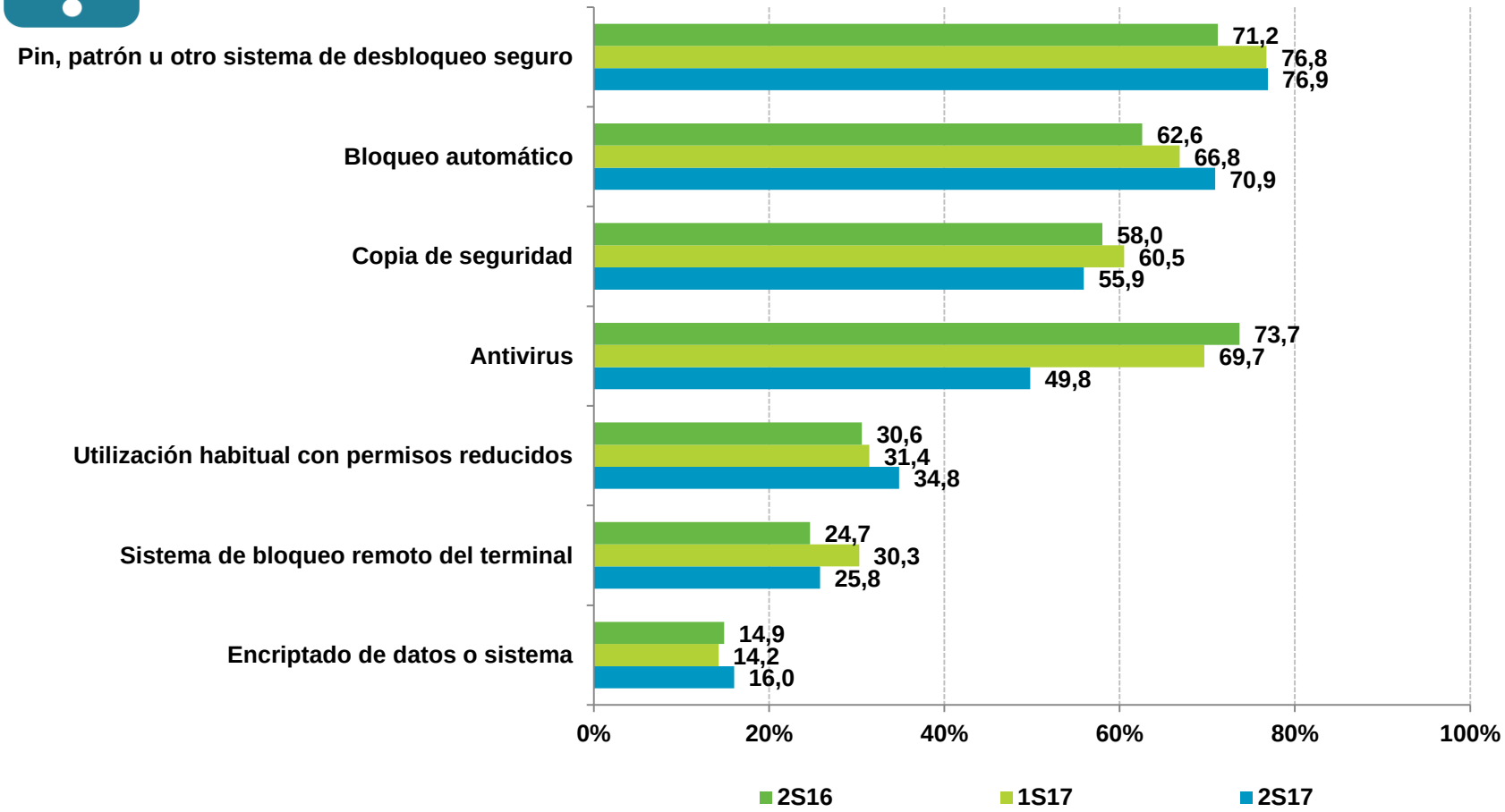


BASE: Usuarios que disponen de dispositivo Android

Es altamente recomendable mantener el sistema operativo actualizado a la última versión disponible para evitar que el dispositivo sea vulnerable o se vea afectado por problemas y errores conocidos y corregidos en las últimas versiones de Android.

Uso de medidas de seguridad en dispositivos Android

El uso de **soluciones antivirus** en dispositivos Android experimenta un importante descenso en este periodo (**-19,9 p.p.**) acelerando la tendencia iniciada en 2016.

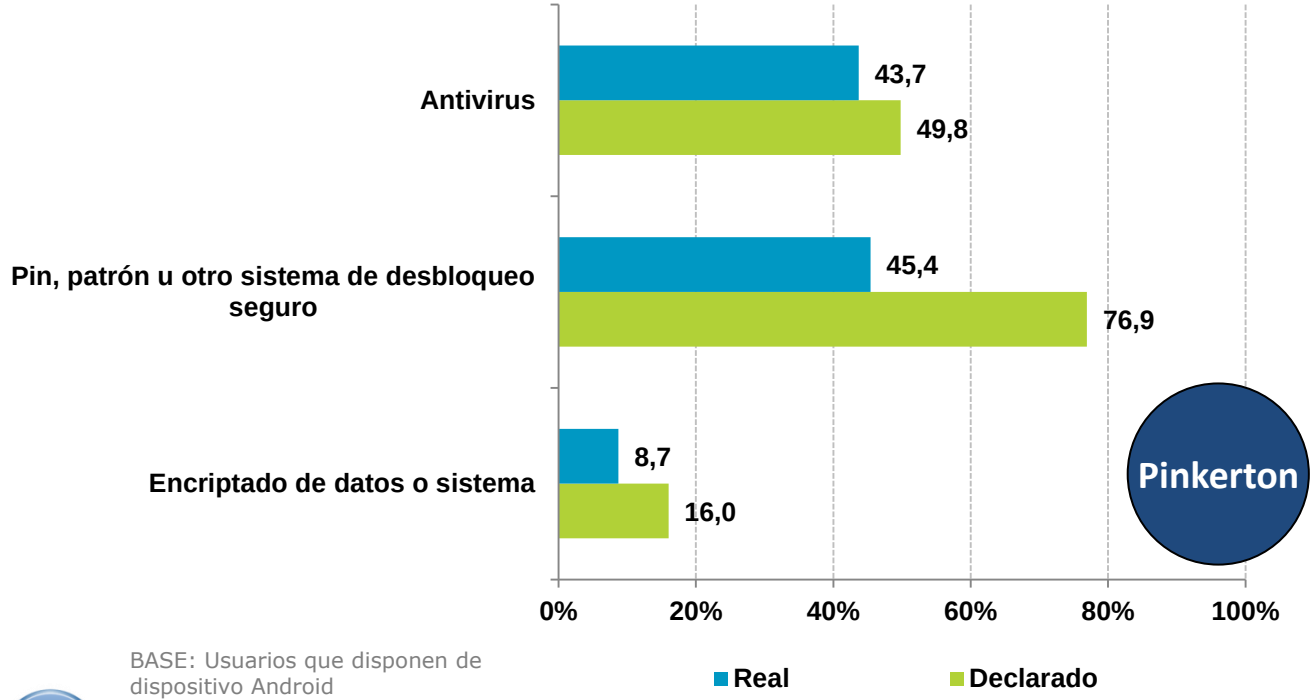


BASE: Usuarios que disponen de dispositivo Android

Uso de medidas de seguridad declarado vs. real

El acusado descenso en las declaraciones de **uso de antivirus** hace que ese valor se aproxime al uso real detectado por Pinkerton, aunque este aún resulta **6,1 p.p.** inferior.

El uso real de **sistemas seguros de desbloqueo (PIN, patrón, etc.)** aumenta hasta el **45,4%** acortando la diferencia con el valor declarado (**+31,5 puntos porcentuales**).



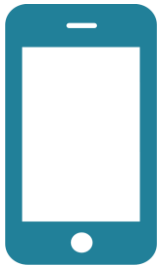
BASE: Usuarios que disponen de dispositivo Android

La utilización de un sistema de desbloqueo seguro mediante **patrón, PIN, sistemas biométricos**, etc., permite evitar de manera sencilla los **accesos no autorizados o no deseados** al dispositivo móvil y su contenido, **protegiendo la privacidad del usuario**.

El **encriptado** o **cifrado** de datos o sistema permite almacenar el contenido del dispositivo codificado, de manera que solo se puede acceder a él si se conoce la clave de cifrado (PIN, patrón, o contraseña) para descodificarlo. Esto permite mantener los datos a salvo en caso de robo o pérdida del dispositivo móvil.

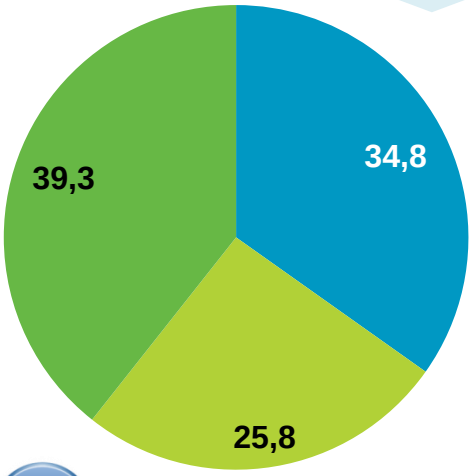
Uso de medidas de seguridad en dispositivos Android

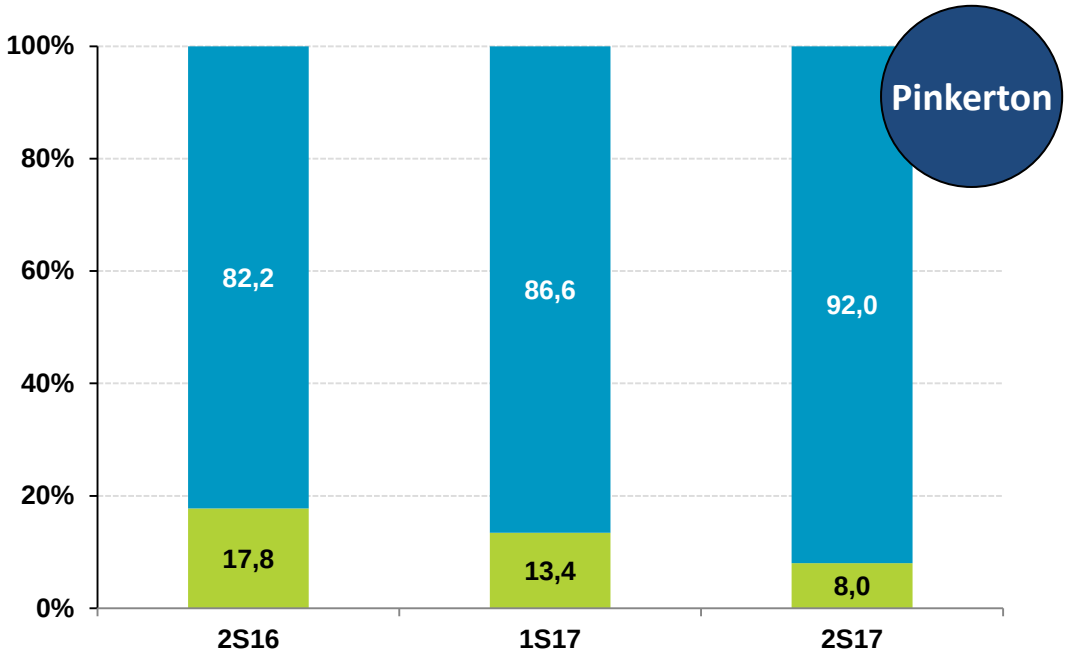
Permisos de Administrador



Dato real

Dato declarado (2S17)





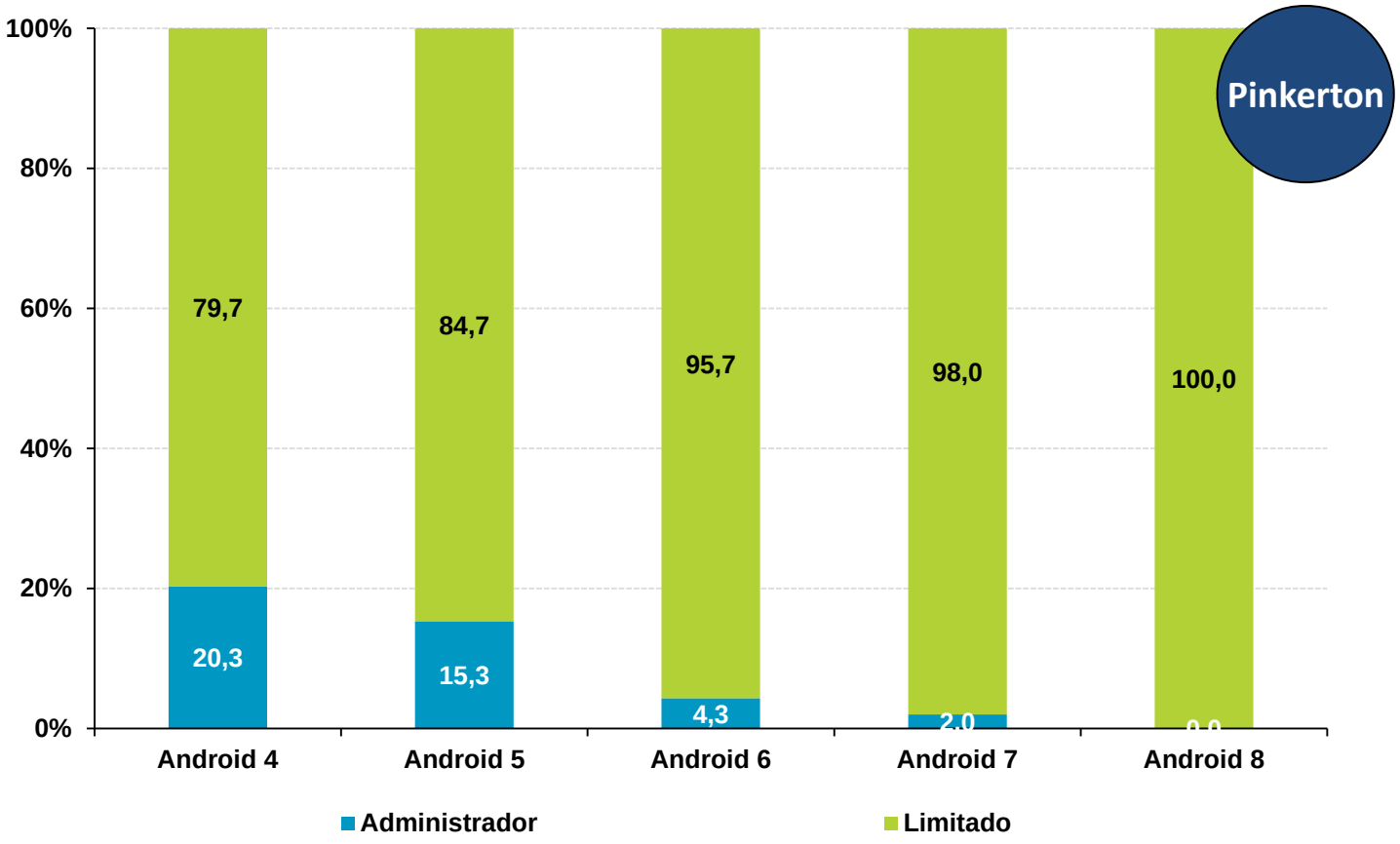
Pinkerton obtiene la información acerca de los privilegios de administrador del dispositivo Android mediante métodos indirectos.

Se conoce como **"rooteo"** o **"rootear"** a la obtención de **privilegios de administrador** (root). Esto permite al usuario **acceder y modificar cualquier aspecto del sistema operativo**. Pero también existen riesgos ya que **el malware puede aprovecharse de esto** logrando un mayor control y/o acceso al dispositivo.

BASE: Usuarios que disponen de dispositivo Android

Uso de medidas de seguridad en dispositivos Android

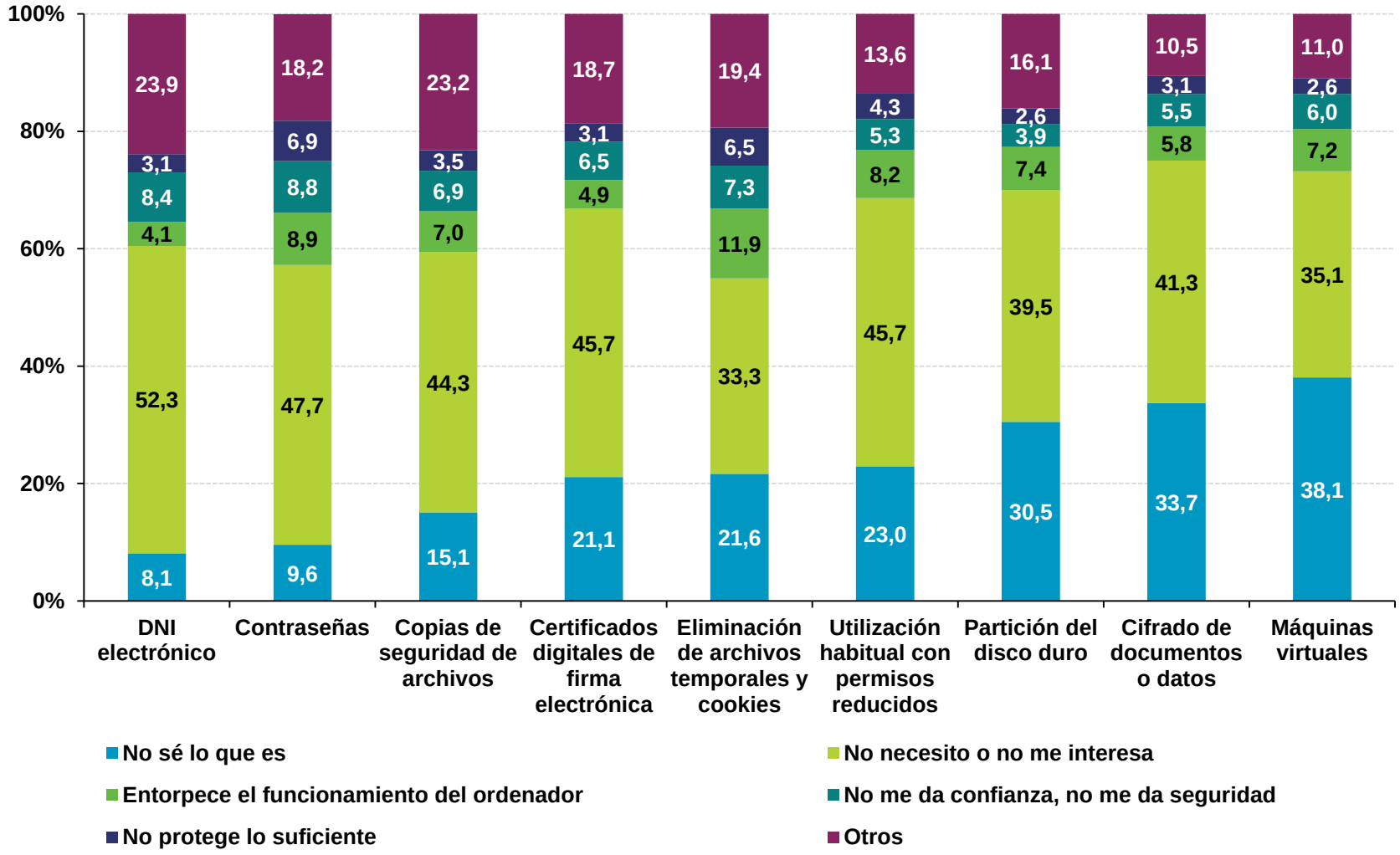
Los usuarios tienden a *'rootear'* los dispositivos que cuentan con las versiones más antiguas de Android (**20,3% en Android 4** y **15,3% en Android 5**)



BASE: Usuarios que disponen de dispositivo Android

Motivos de no utilización de medidas de seguridad

El principal motivo de no utilizar medidas de seguridad no automatizables es la **falta de necesidad** o **no considerarlas de interés**.

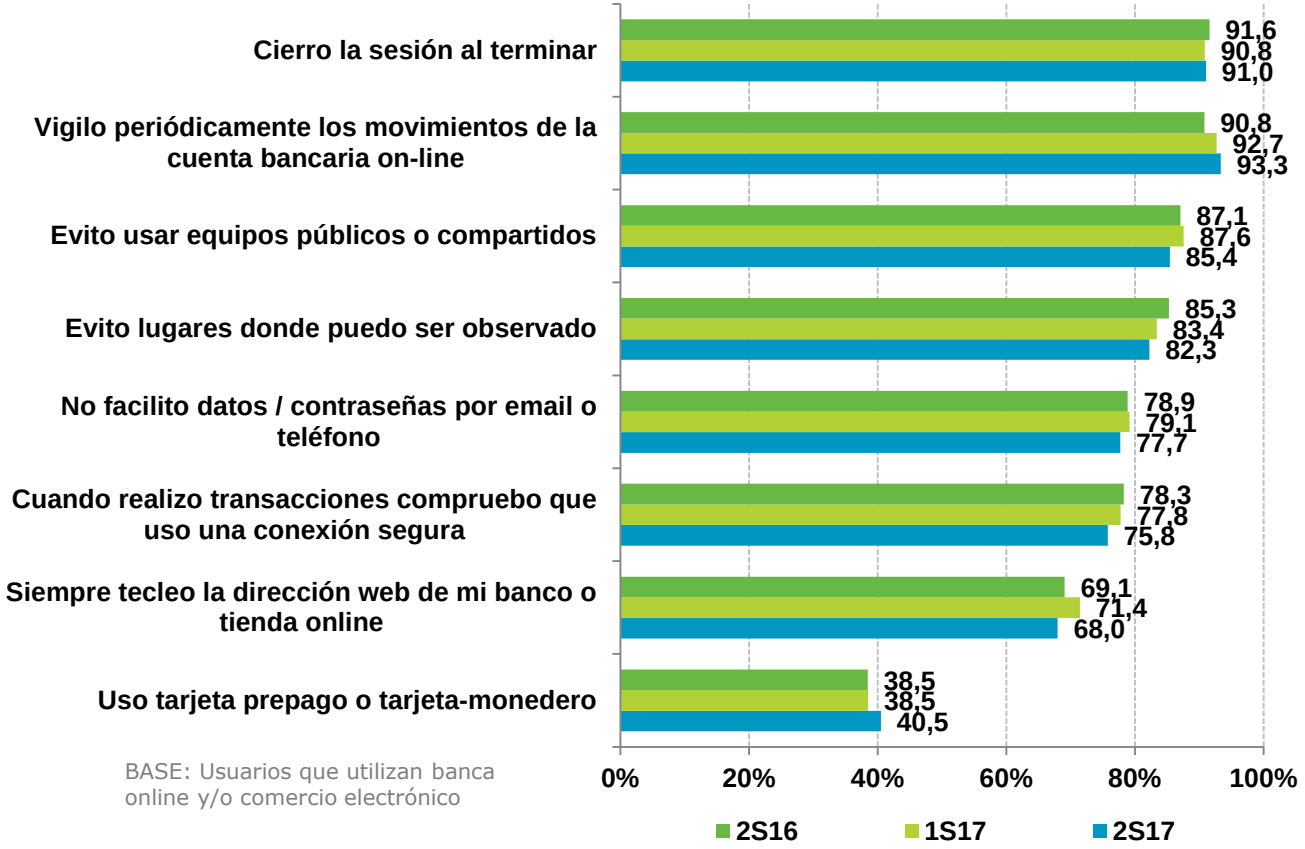


BASE: Usuarios que no utilizan alguna de las medidas de seguridad

Hábitos de comportamiento en la navegación y uso de Internet

1. **Banca en línea y comercio electrónico**
2. **Descargas en Internet**
3. **Alta en servicios en Internet**
4. **Redes sociales**
5. **Hábitos de uso de las redes inalámbricas Wi-Fi**
6. **Hábitos de uso en dispositivos Android**
7. **Adopción consciente de conductas de riesgo**

Banca en línea y comercio electrónico



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.

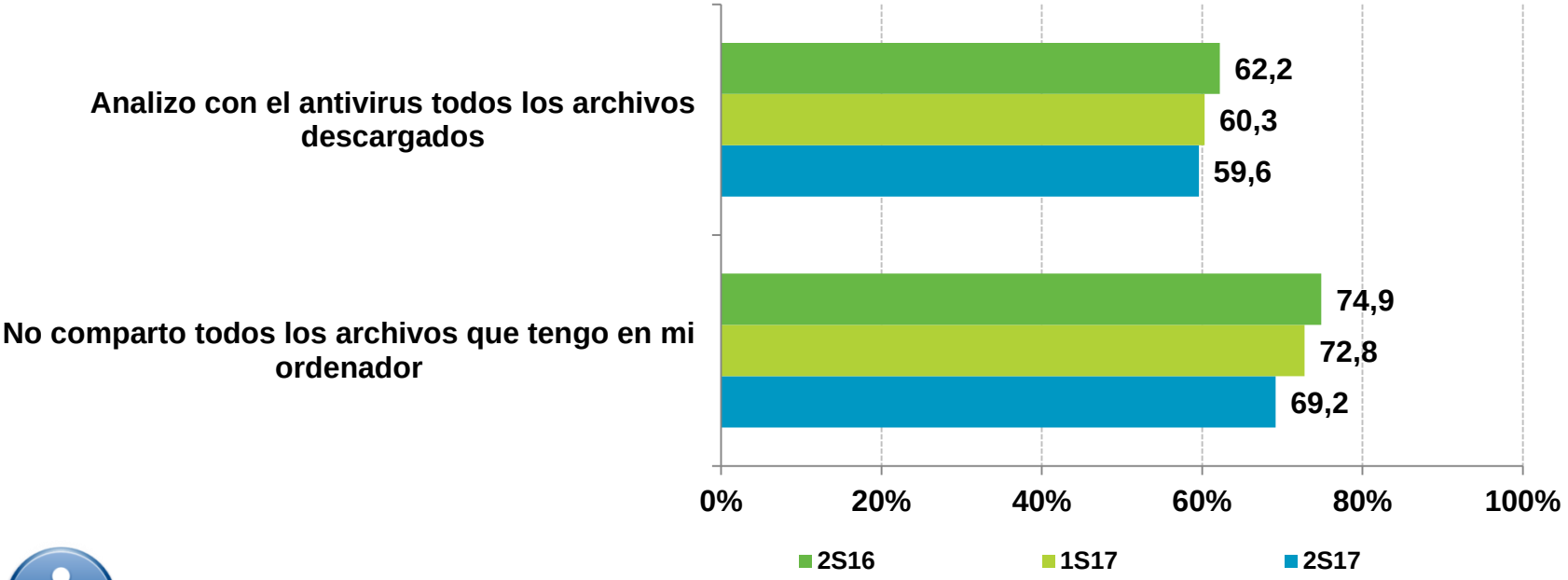
Medidas para protegerte al realizar trámites on-line: https://www.osi.es/pagos-online

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

Guía de compra segura en Internet: https://www.osi.es/sites/default/files/docs/guia_compra_segura_internet_web_vfinal.pdf

Redes P2P

Los buenos hábitos de uso en las redes P2P continúan la tendencia menguante iniciada en 2016: el **análisis con el antivirus de todos los ficheros descargados** alcanza el **59,6%** (**-4,2 p.p.** desde 1S16) y el hecho de **no compartir en las redes P2P todos los archivos del equipo** se sitúa en **69,2%** (**-5,7 p.p.** desde 2S16).

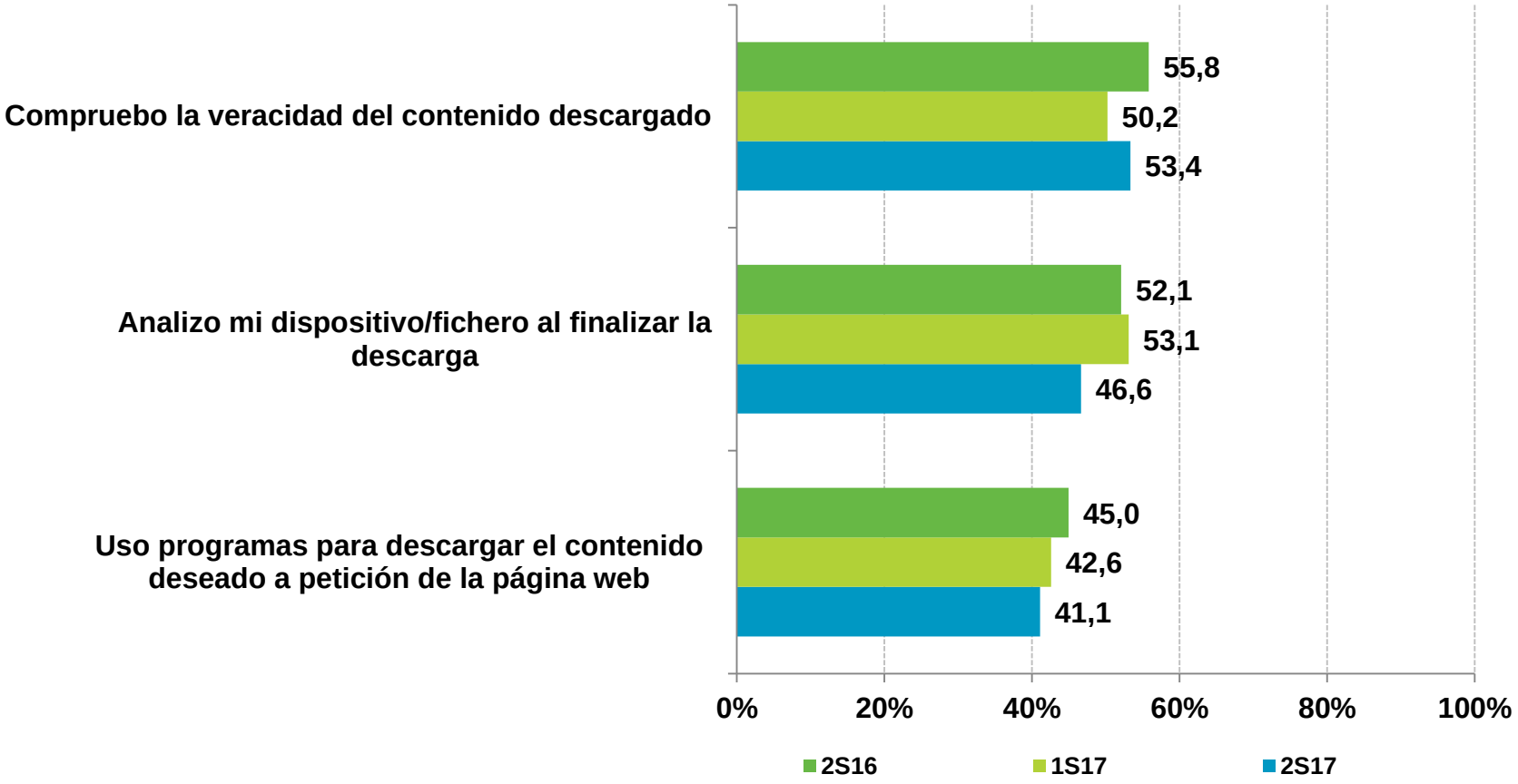


Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de malware. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como por ejemplo novedades de software, cinematográficas, musicales, etc.) logran el objetivo de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

BASE: Usuarios de redes P2P

Descarga directa

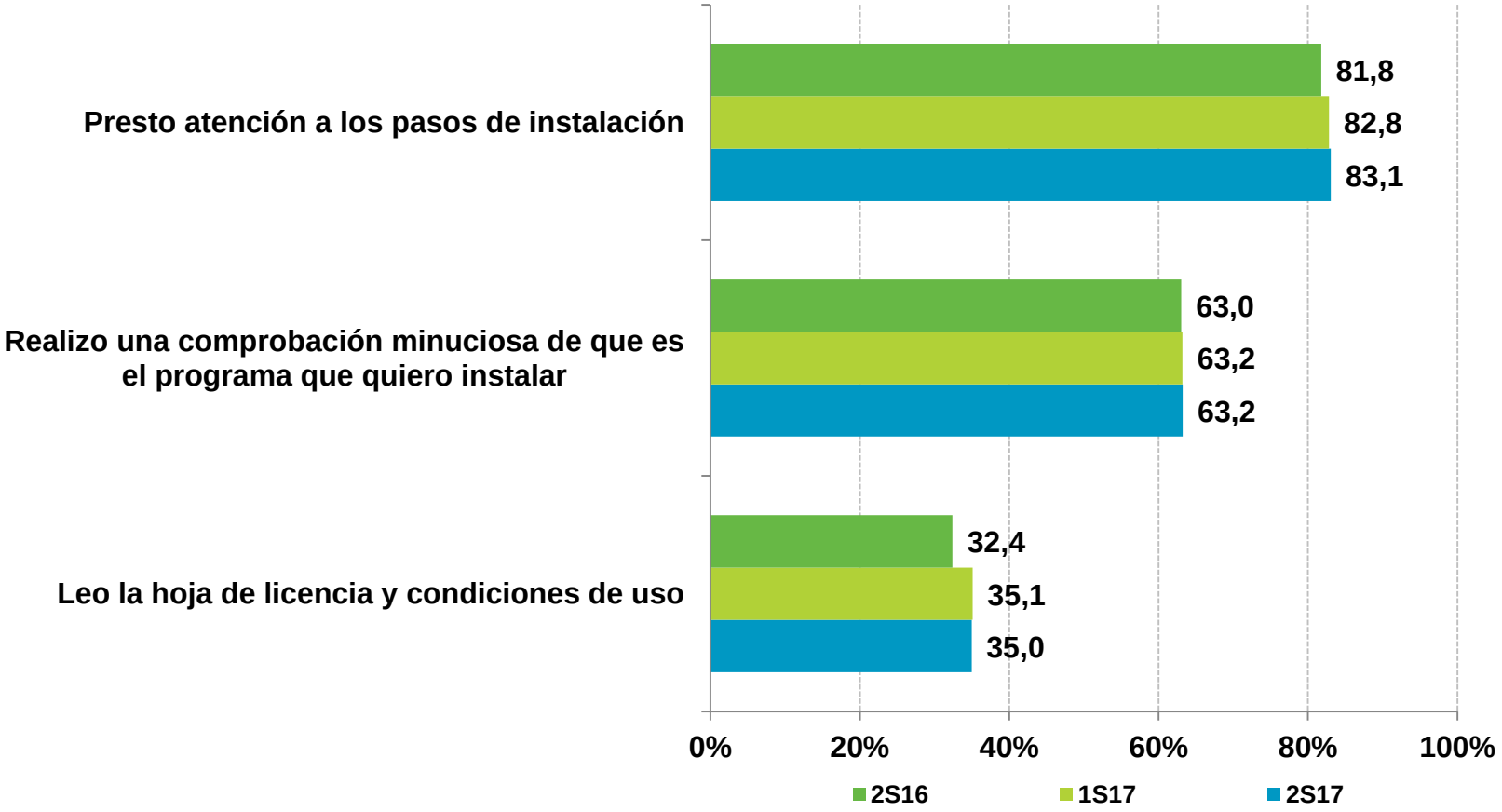
En la **descarga directa** de ficheros, el **46,6%** de internautas afirma **analizar los archivos al finalizar la descarga** (**-6,5 p.p.** respecto al análisis anterior).



BASE: Total usuarios

Instalación de software descargado

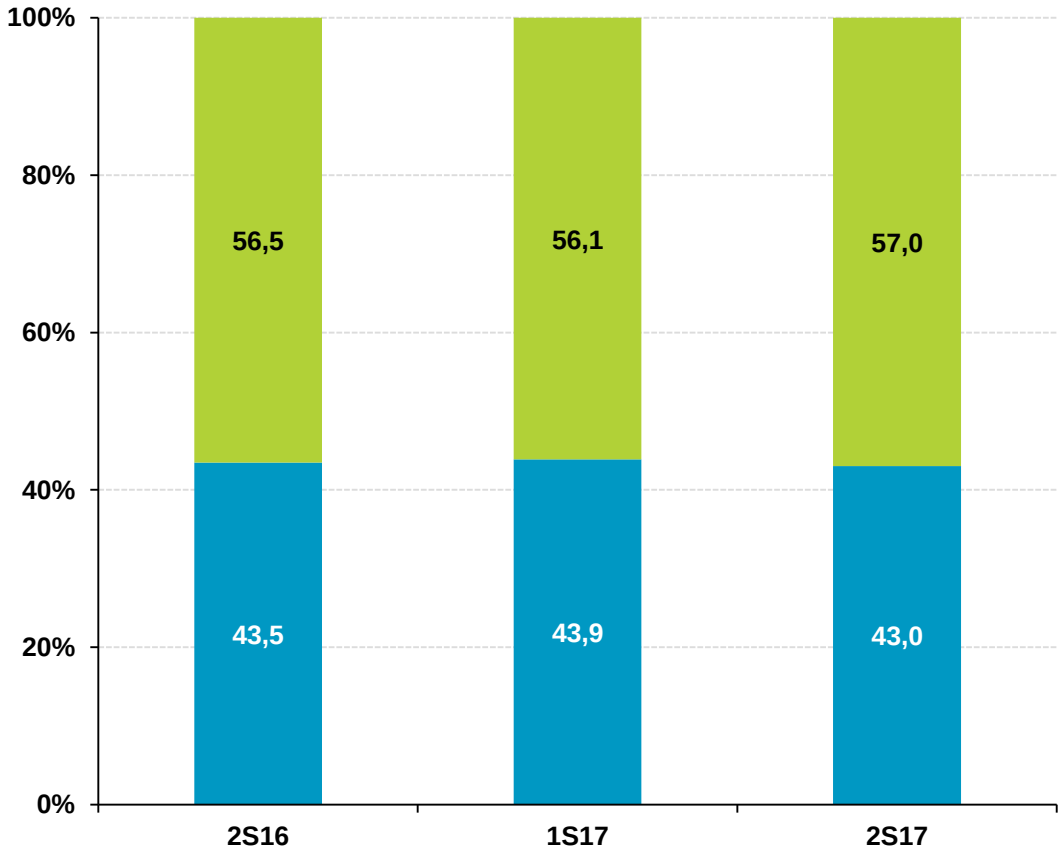
Ocho de cada diez usuarios (**83,1%**) **presta atención a los pasos de instalación** del software descargado desde Internet.



BASE: Usuarios de PC

Alta en servicios en Internet

El **57%** de los internautas españoles afirman **no leer las condiciones e información legal antes de aceptarlas** al registrarse o darse de alta en proveedores de servicio en Internet (redes sociales, comercio electrónico, etc.).

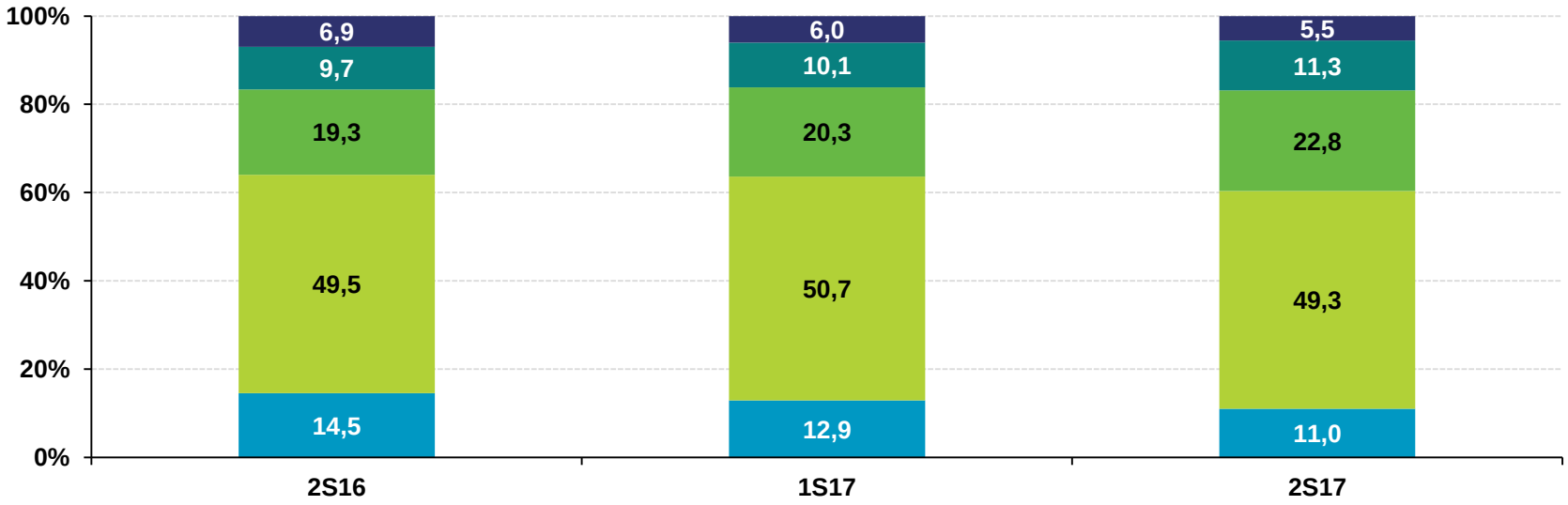


Lectura y aceptación de la información legal al registrarse o darse de alta en proveedores de servicio en Internet (redes sociales, comercio electrónico, etc.)

BASE: Total usuarios

Redes sociales

El **34,1%** (22,8 + 11,3) de los usuarios de redes sociales consultados **expone los datos** publicados en su perfil a **terceras personas y/o desconocidos**, mientras que el **5,5%** declara **desconocer** el nivel de privacidad de su perfil.



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

Cómo hacer un uso seguro de las redes sociales: (Videos tutoriales) https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

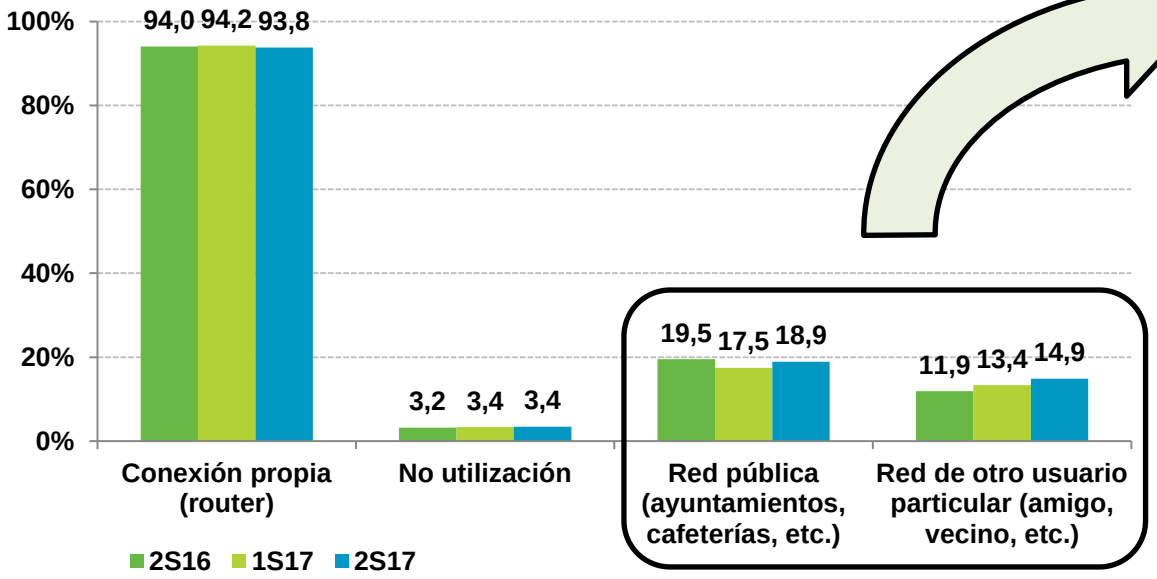
BASE: Usuarios que utilizan redes sociales

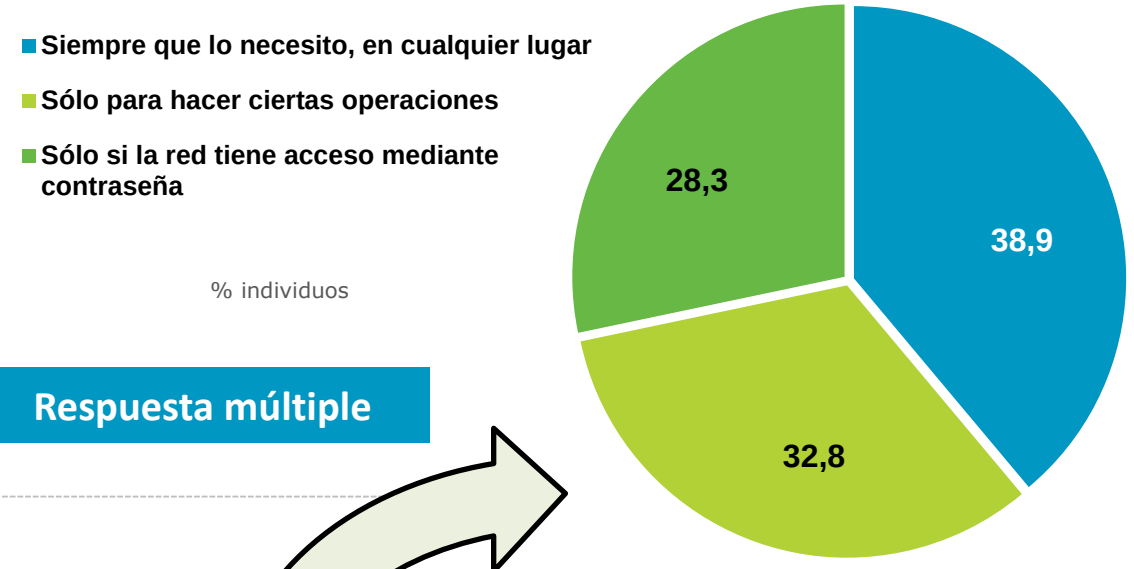
% individuos

Hábitos de uso de las redes inalámbricas Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Respuesta múltiple





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

Un tercio de los internautas se conectan a una red inalámbrica Wi-Fi pública (**18,9%**) o de un particular (**14,9%**) siempre que lo necesitan y en cualquier lugar (**38,9%**).

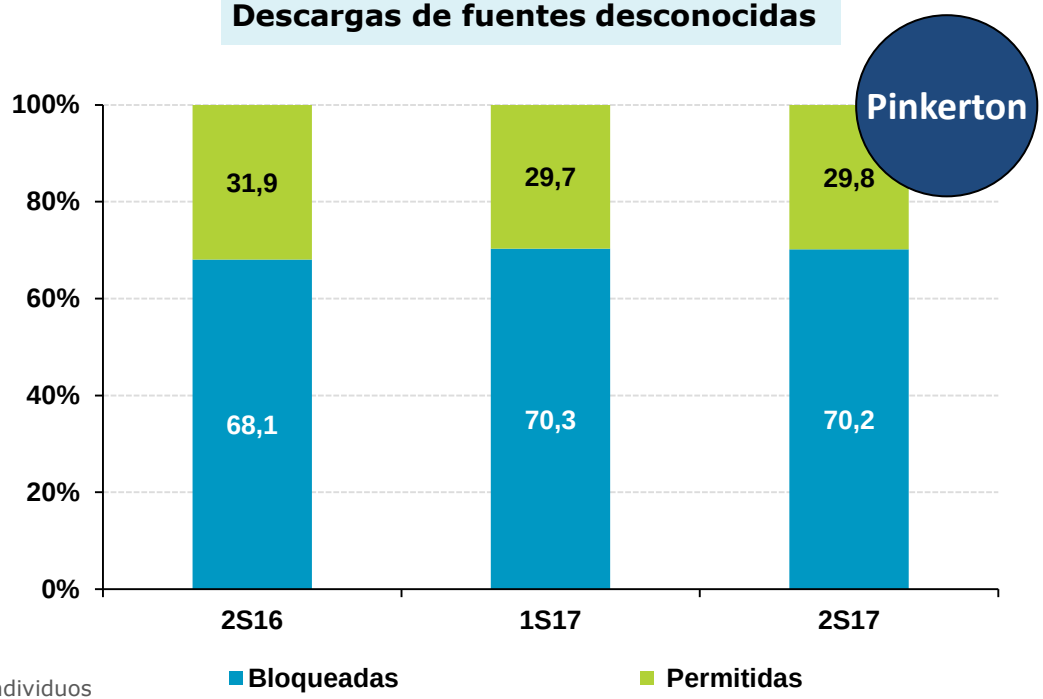
BASE: Total usuarios

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

Hábitos de uso en dispositivos Android

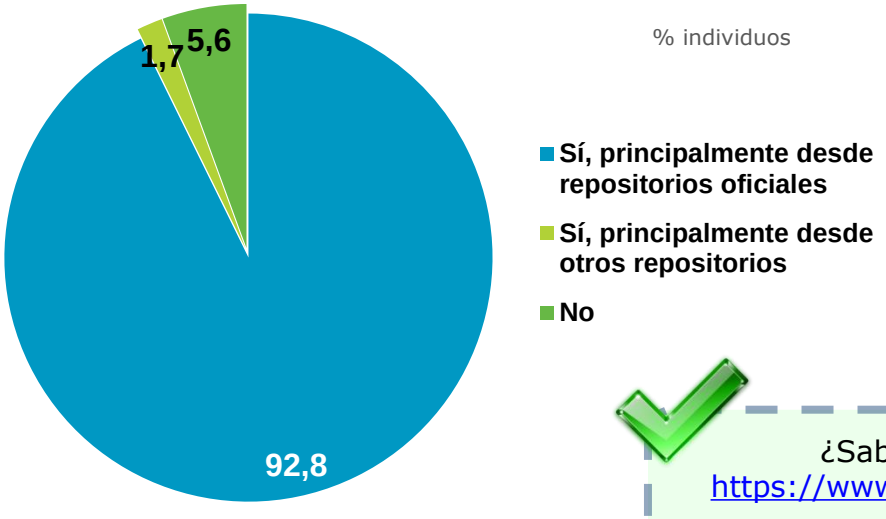
El uso de aplicaciones provenientes de fuentes dudosas puede suponer **problemas de seguridad** y la instalación en el dispositivo móvil de cualquier tipo de **malware**.

Descargas de fuentes desconocidas



% individuos

Descargas de programas o aplicaciones en el móvil



Los usuarios del **29,8%** de los dispositivos Android analizados por Pinkerton han configurado el dispositivo para permitir la instalación de aplicaciones desde **fuentes desconocidas** (la configuración por defecto no lo permite). Sin embargo, apenas el **1,7%** declara realizar instalaciones desde **repositorios no oficiales**.

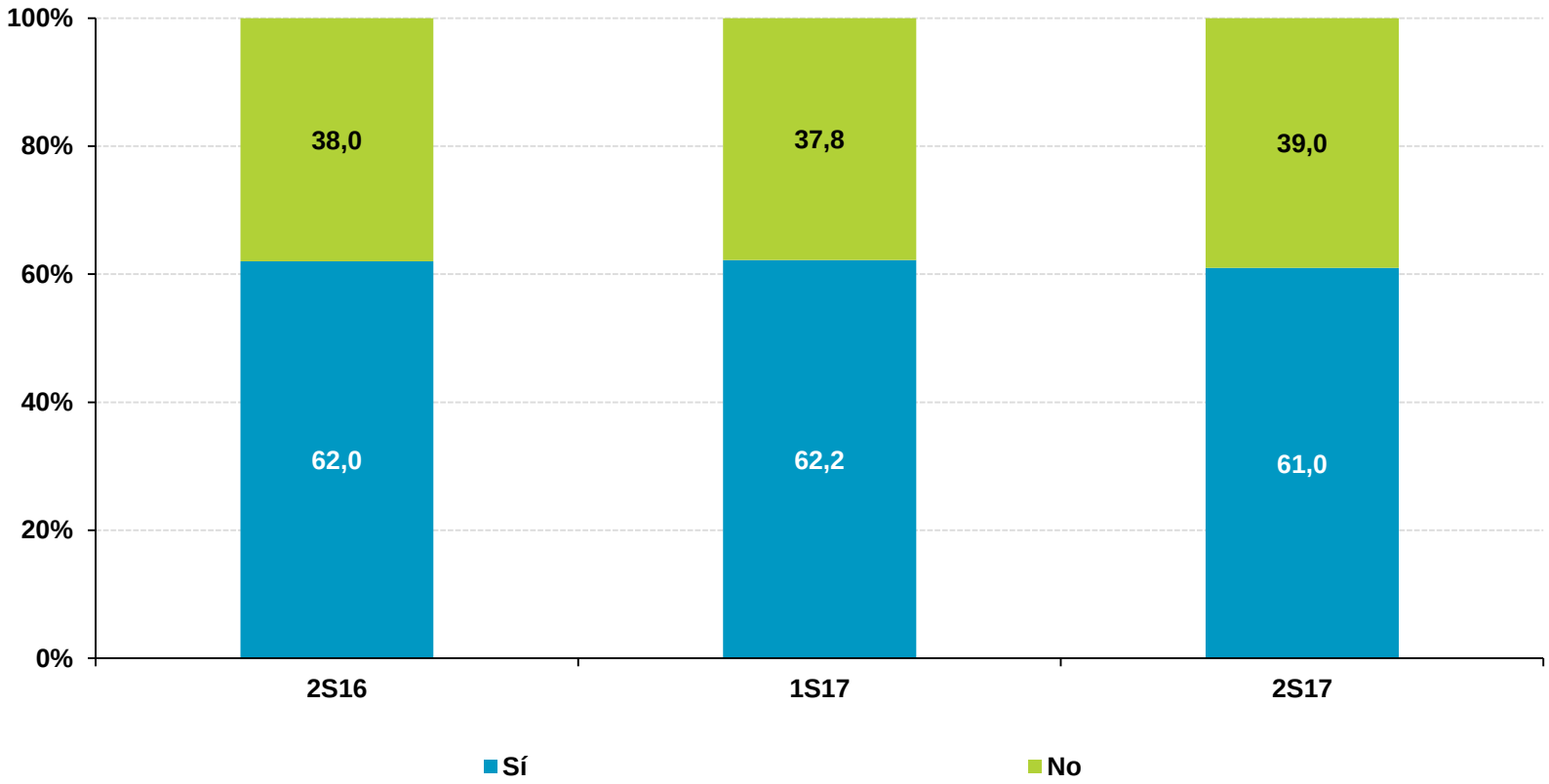
¿Sabes que esta APP puede robar tu información?
https://www.osi.es/es/actualidad/blog/2017/07/05/esta-app-te-puede-robar-toda-tu-informacion

BASE: Usuarios que disponen de dispositivo Android

Hábitos de uso en dispositivos Android

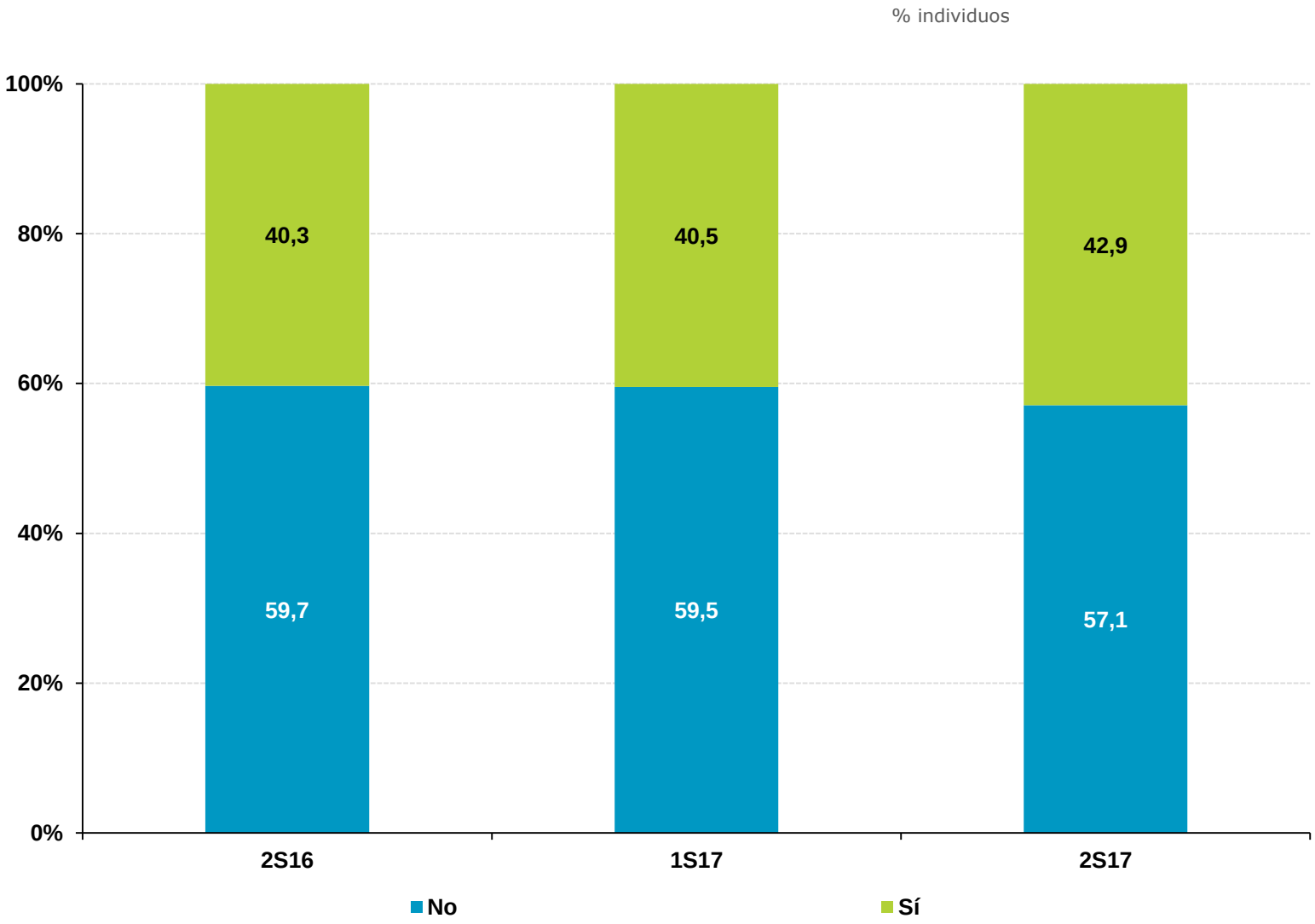
Comprobación de permisos al instalar una aplicación

% individuos



BASE: Usuarios que disponen de dispositivos Android que descargan aplicaciones

Adopción consciente de conductas de riesgo



BASE: Total usuarios

Incidentes de seguridad

Tipos de malware

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un PC/portátil o dispositivo móvil (tablet, smartphone, relojes inteligentes, etc.) 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

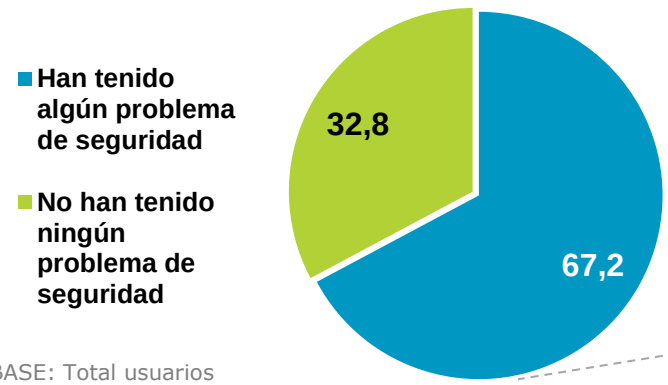
Mas información: https://www.incibe.es/glossary/empresas/diccionario/

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.

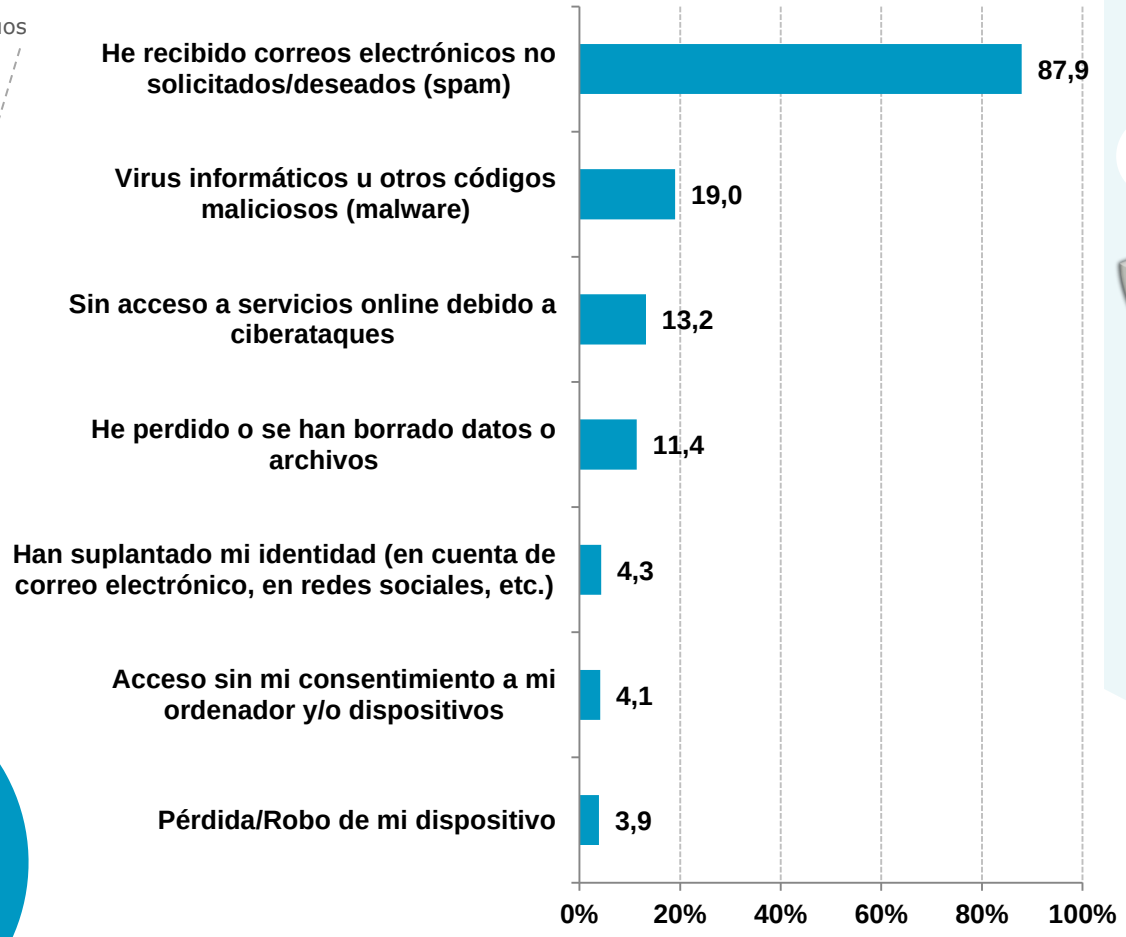
Afectados:



BASE: Total usuarios

Incidencias sufridas:

Respuesta múltiple



BASE: Usuarios que han sufrido alguna incidencia de seguridad

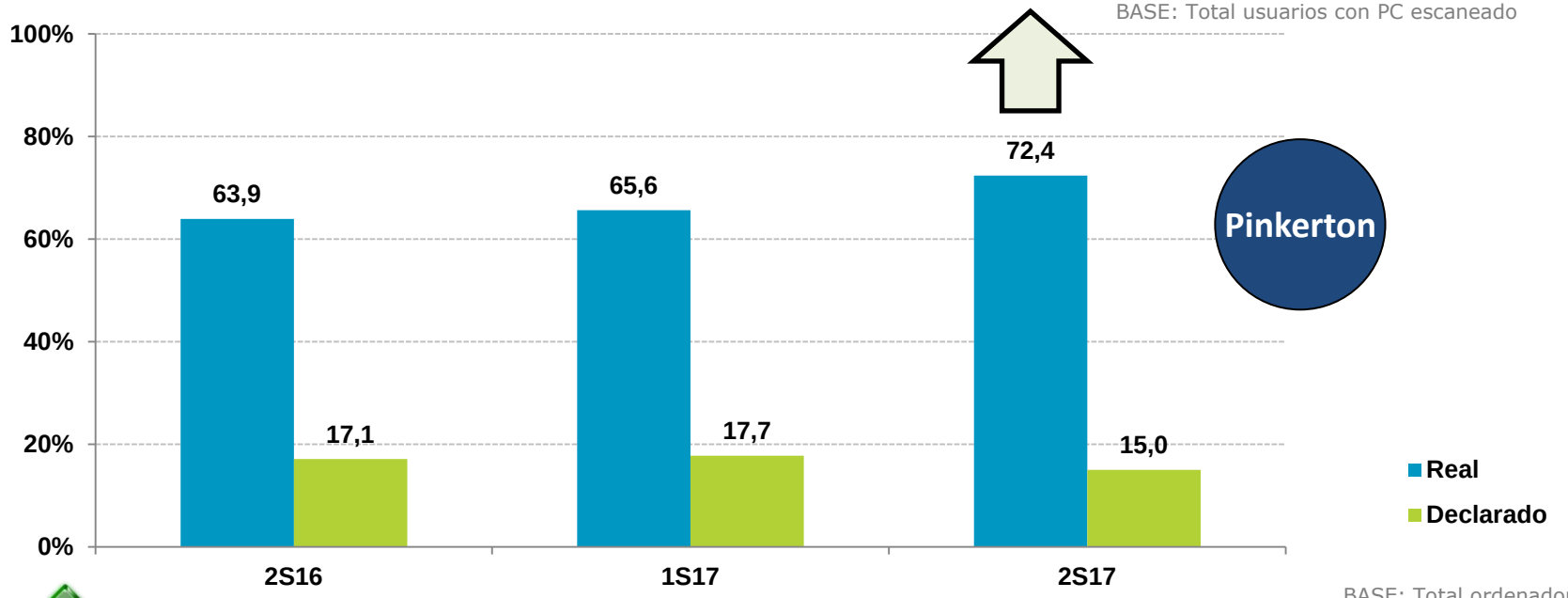
Incidentes por malware

Ordenador del hogar

El **61,7%** de los ordenadores analizados se encuentran **infectados con alguna muestra de malware aunque sus usuarios piensan que no**.

Declararon tener malware en PC	Su PC presentaba malware		
	Sí	No	Total
Sí	10,7	3,2	13,9
No	61,7	24,4	86,1
Total	72,4	27,6	100,0

BASE: Total usuarios con PC escaneado



BASE: Total ordenadores

Aprende los pasos que debes dar para la eliminación de los virus de tu equipo:
https://www.osi.es/es/desinfecta-tu-ordenador

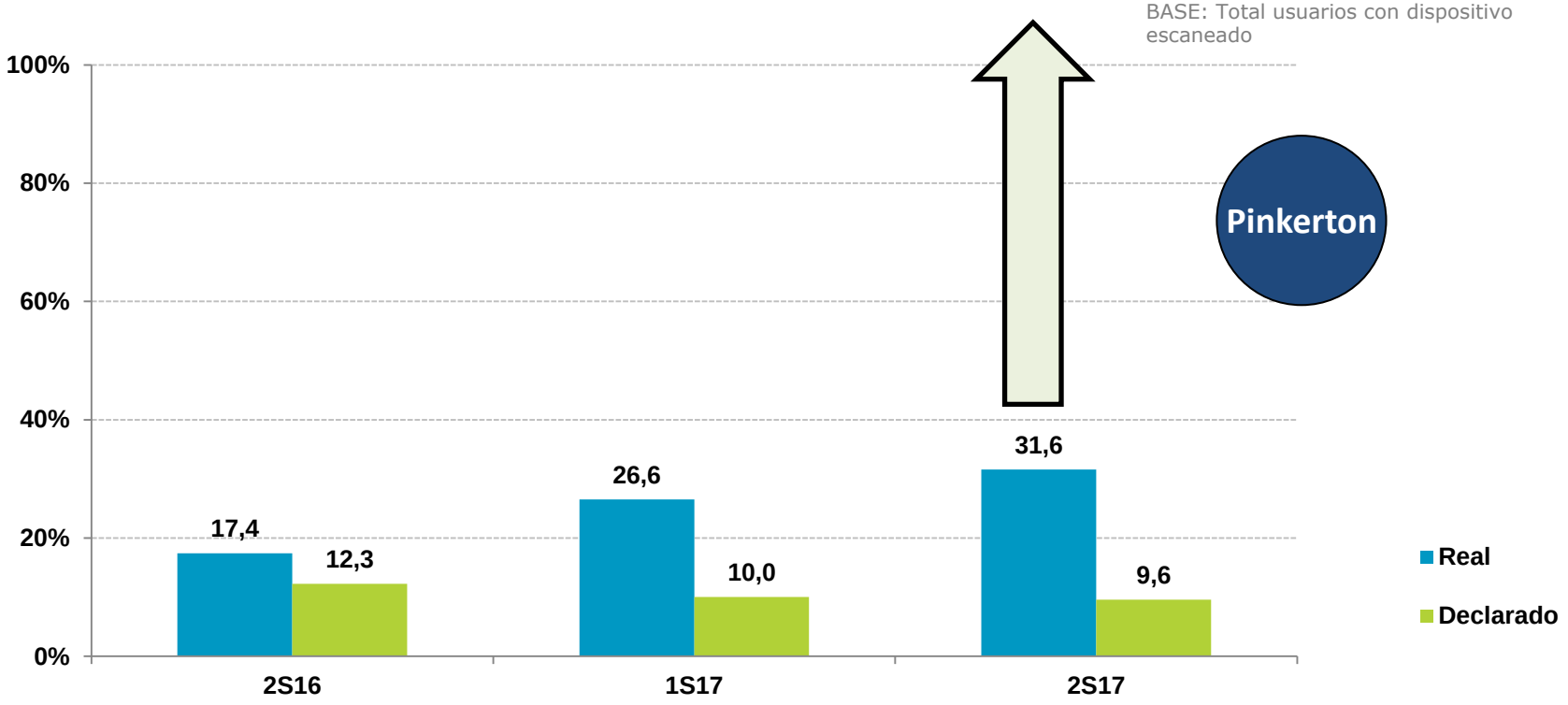
Incidentes por malware

Dispositivos Android

Los usuarios **no percibieron la presencia de malware** en el **28,1%** de los dispositivos Android en los que **Pinkerton encontró infecciones**.

Declararon tener malware en Android	Su Android presentaba malware		
	Sí	No	Total
Sí	3,5	5,1	8,6
No	28,1	63,3	91,4
Total	31,6	68,4	100,0

BASE: Total usuarios con dispositivo escaneado



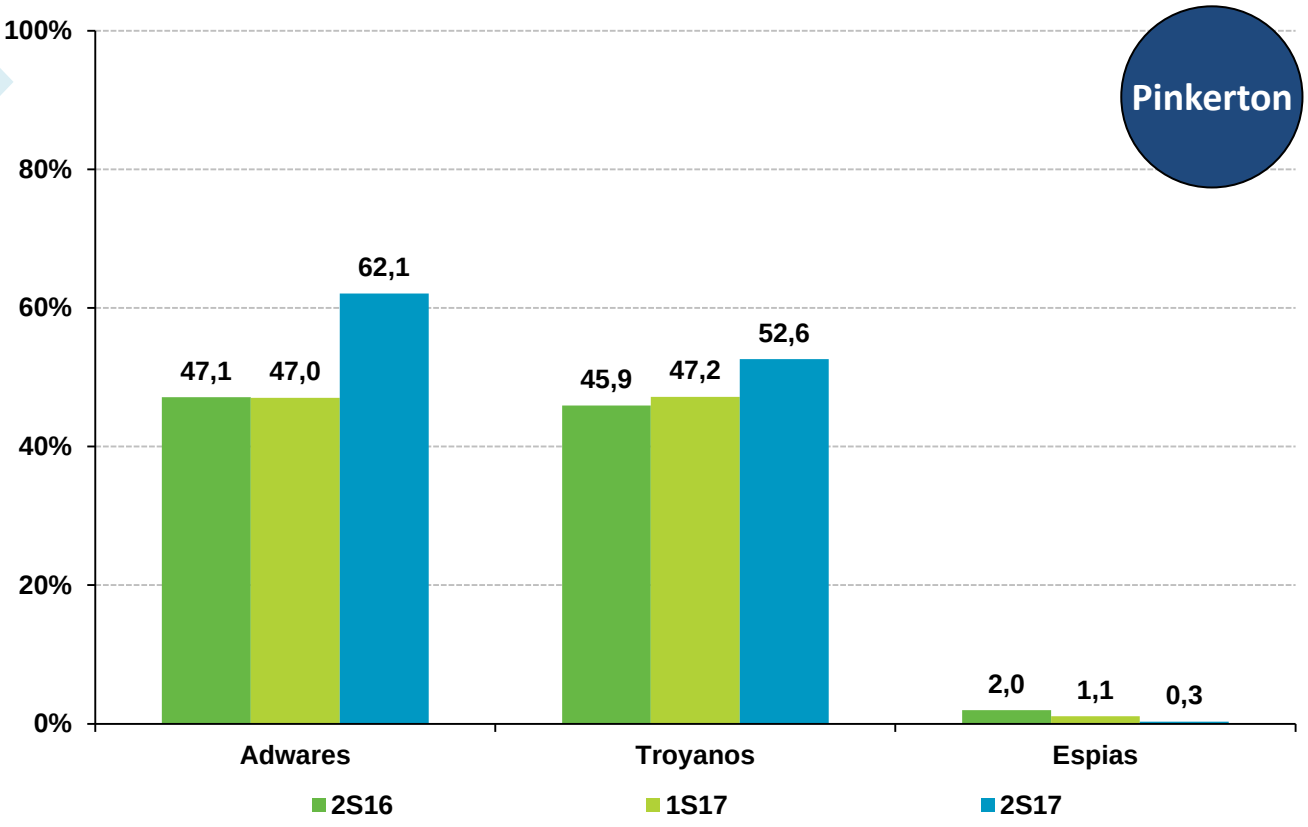
BASE: Usuarios que disponen de dispositivo Android

Tipología del malware detectado en PC

Ordenador del hogar

El **adware publicitario** y los **troyanos** aumentan considerablemente su presencia en los ordenadores españoles: **+15,1 p.p.** y **+5,4 p.p.** respectivamente desde el anterior periodo analizado.

Equipos que alojan malware según tipología



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

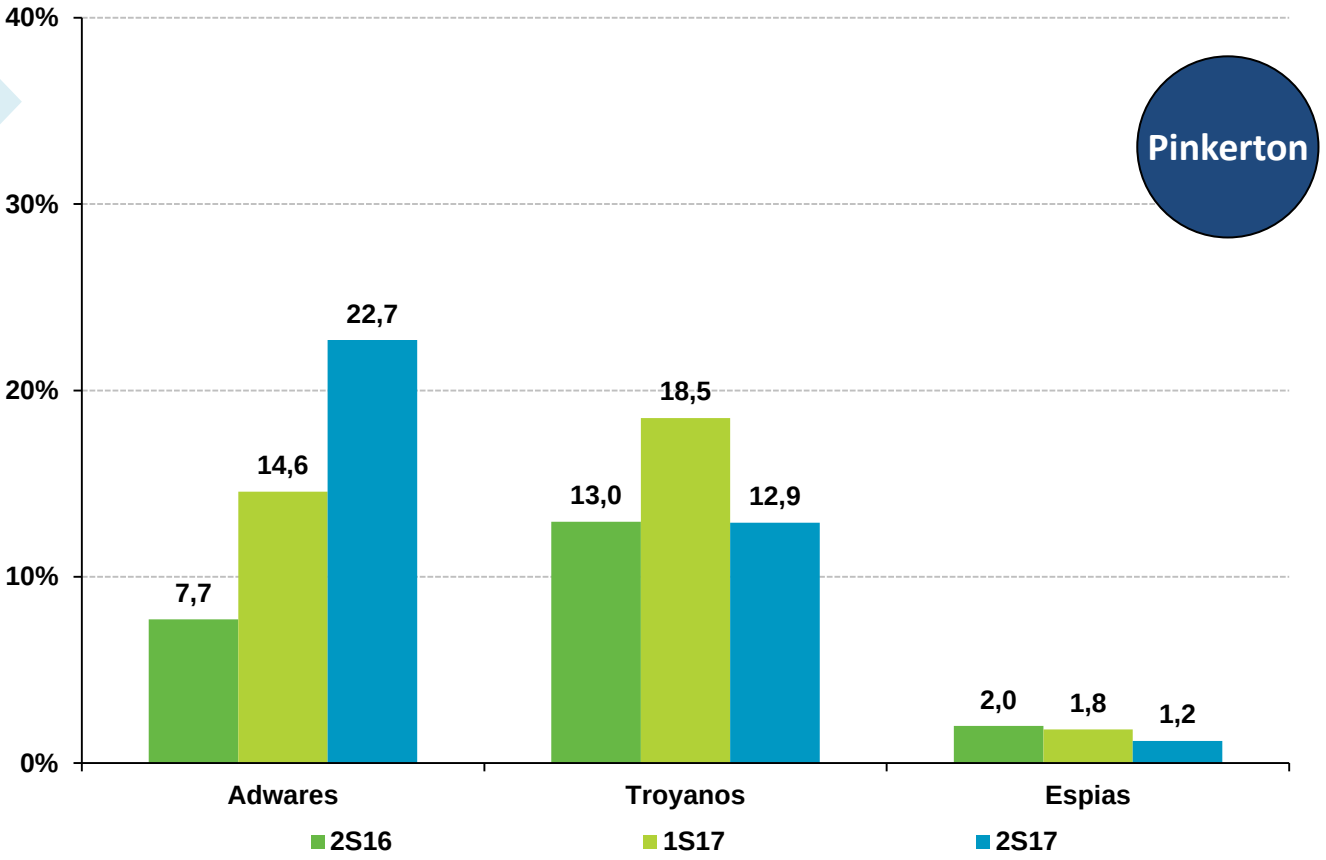
BASE: Total ordenadores

Tipología del malware detectado en android

Dispositivos Android

En los dispositivos Android, el **adware publicitario** también experimenta un crecimiento notable: **+4,6 p.p.** en el último semestre de y **+10,1 p.p.** desde el mismo periodo de 2016.

Equipos que alojan malware según tipología



Pinkerton

4

BASE: Usuarios que disponen de dispositivo Android

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.).

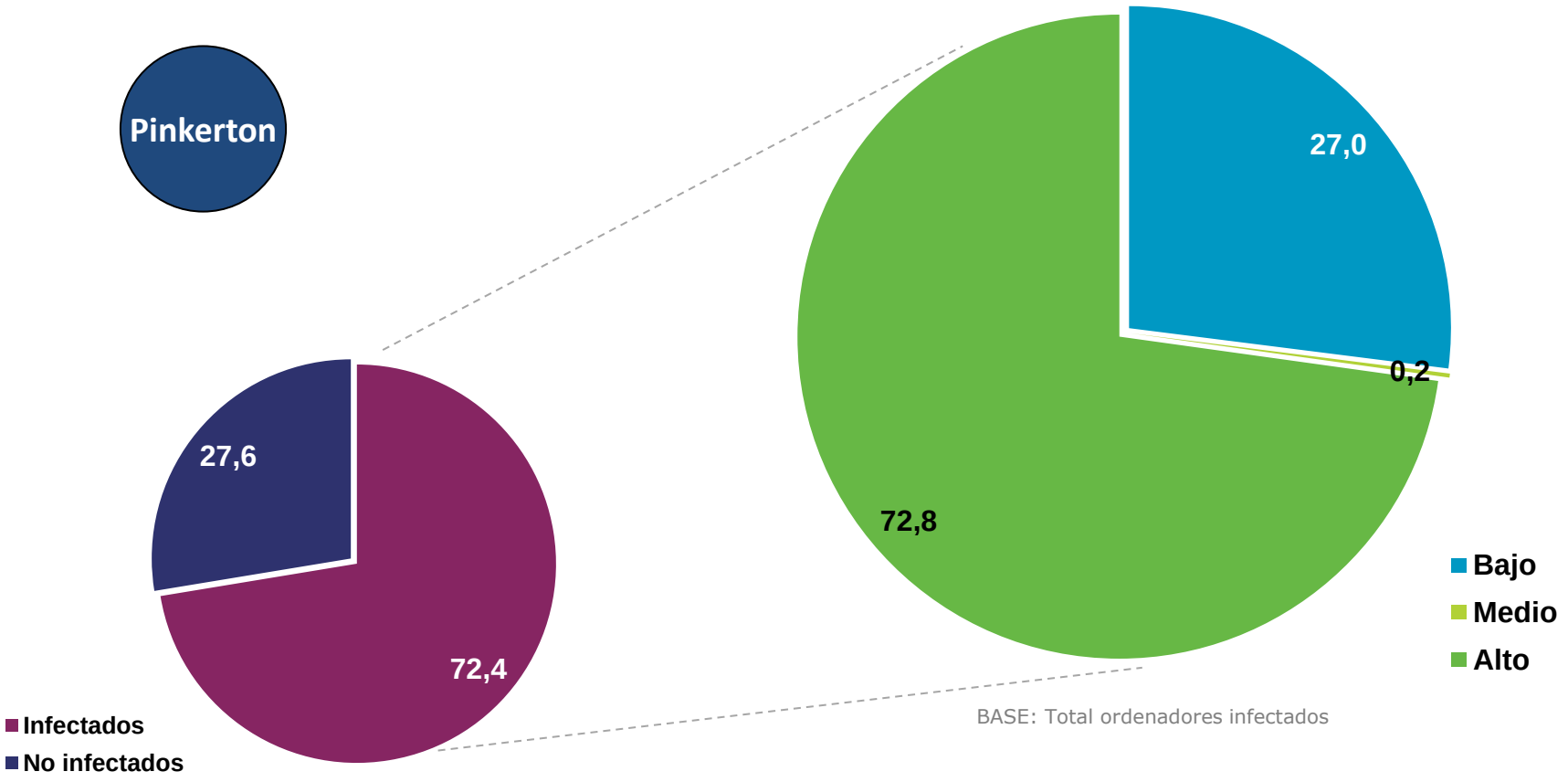
Peligrosidad baja: se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, *hacking tools*, etc.). En la mayoría de los casos son herramientas instaladas por el usuario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

Ordenador del hogar

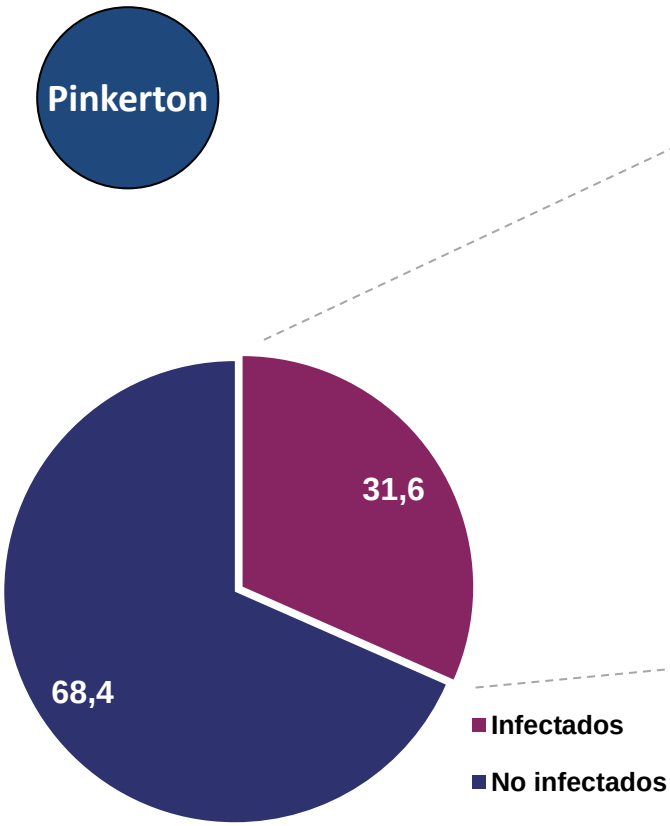
Tres de cada cuatro (**72,4%**) ordenadores de los hogares españoles analizados con Pinkerton se encuentran infectados con al menos una muestra de malware conocida. De estos, la mayoría (**72,8%**) presentan un nivel de **riesgo alto** debido al potencial peligro que suponen los archivos maliciosos encontrados en ellos.



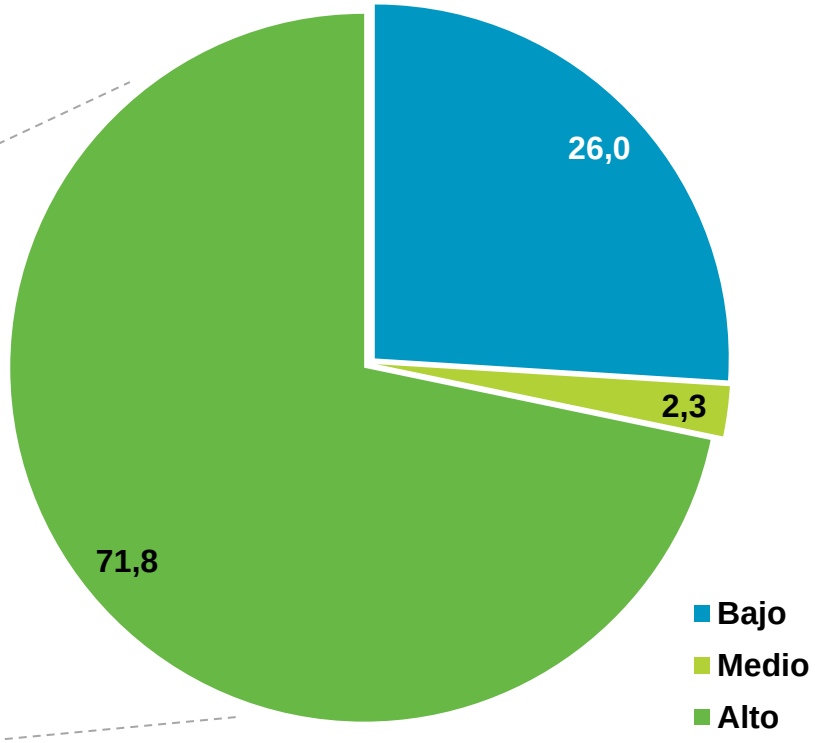
Peligrosidad del código malicioso y riesgo del equipo

Dispositivos Android

Casi un tercio (**31,6%**) de los dispositivos Android analizados con Pinkerton se encuentran infectados con al menos una muestra de malware conocida, de los cuales un **71,8%** presentan un nivel de **riesgo alto**.



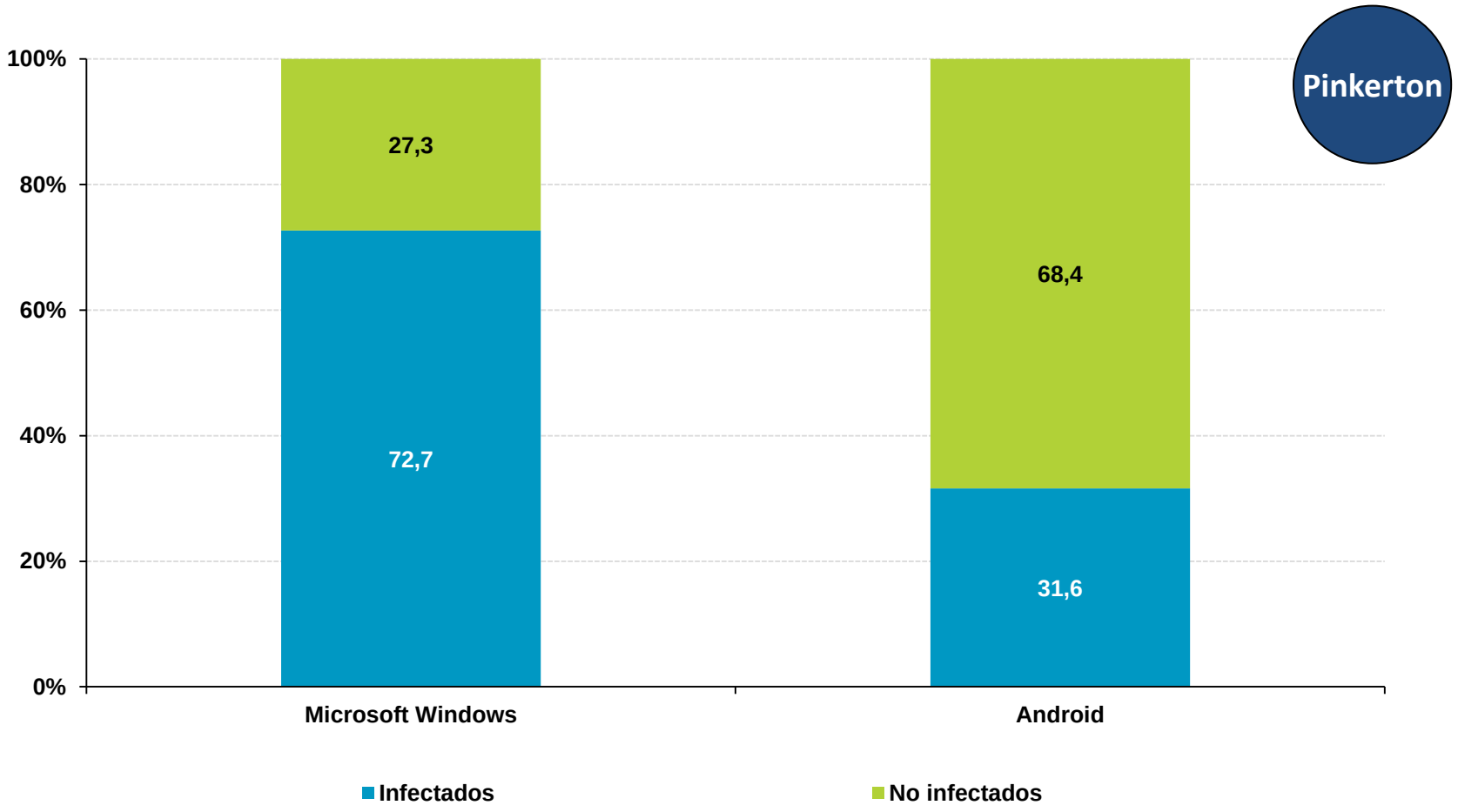
BASE: Usuarios que disponen de dispositivo Android



BASE: Total dispositivos Android infectados

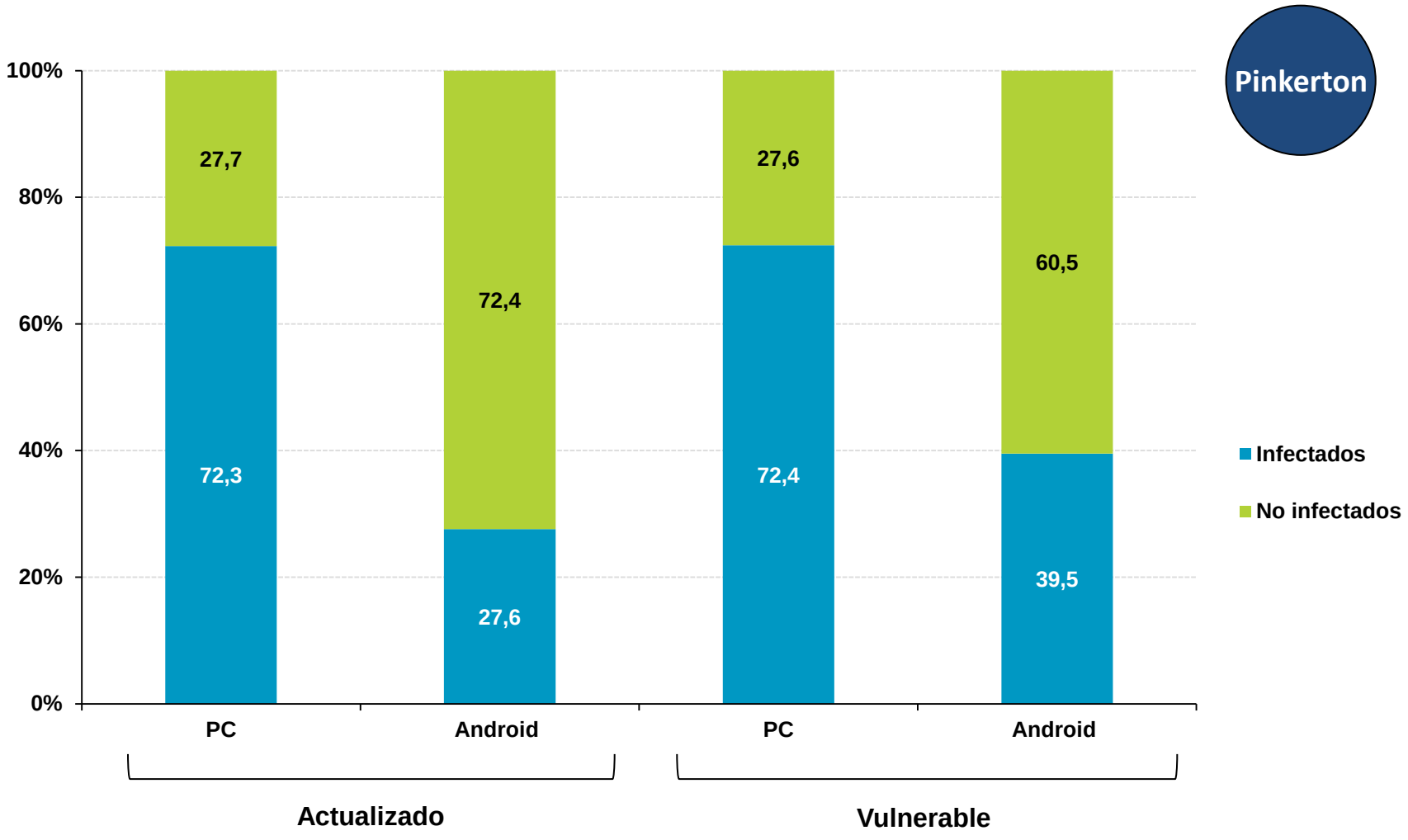
Malware vs. sistema operativo

Según el análisis de Pinkerton, el **72,7%** de los ordenadores del hogar con sistema operativo **Microsoft Windows** y el **31,6%** de los dispositivos **Android** contienen malware conocido.



BASE: Total equipos

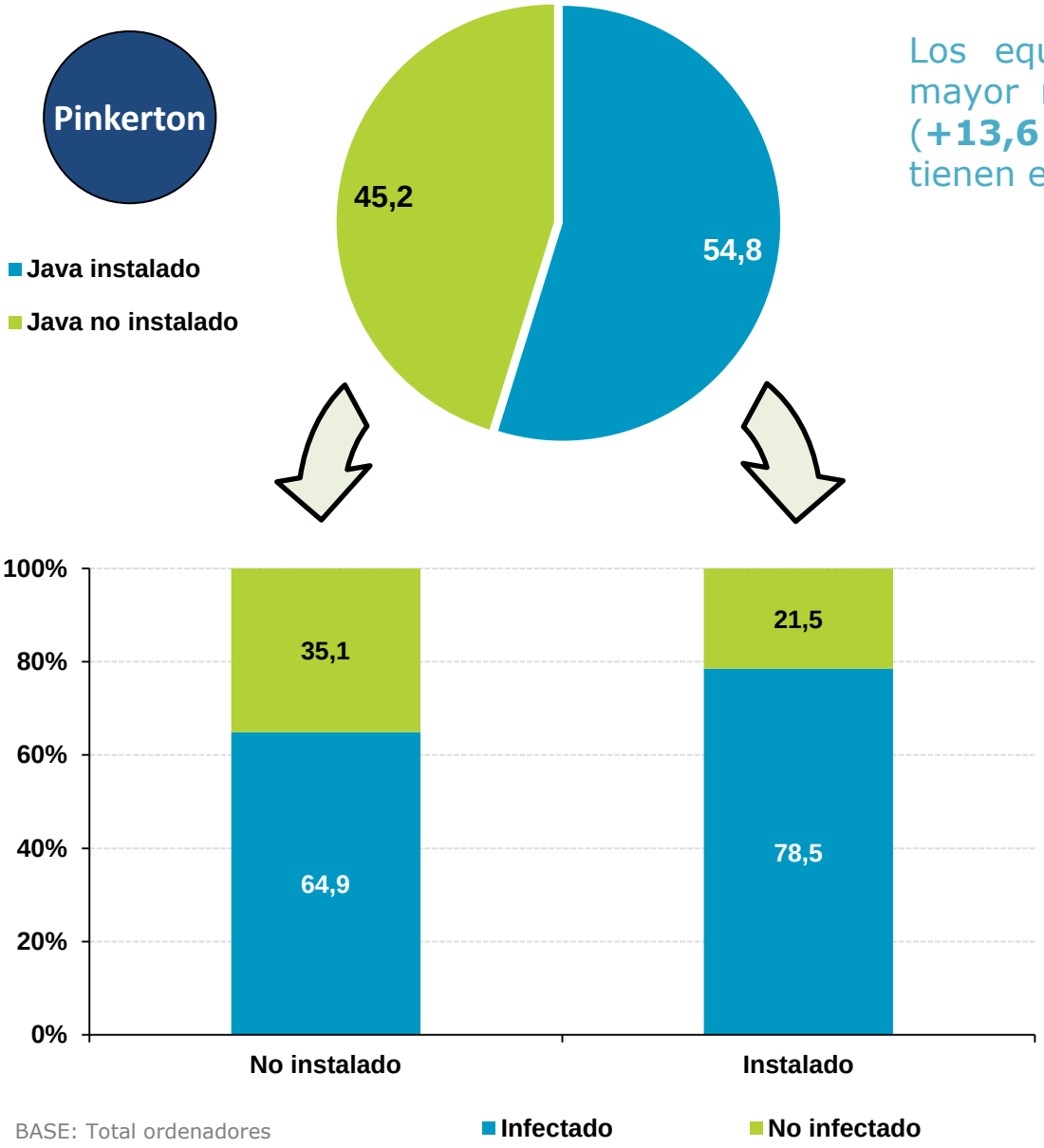
Malware vs. actualización del sistema



Entre los dispositivos Android, los más afectados por el malware son aquellos que no se encuentran actualizados (**+11,9 p.p.**)

BASE: Total equipos

Malware vs. Java en PC



Los equipos con Java presentan un mayor nivel de infección de malware (**+13,6 p.p**) que aquellos que no tienen este entorno instalado.

Alertas de seguridad de Java en julio y octubre de 2017:

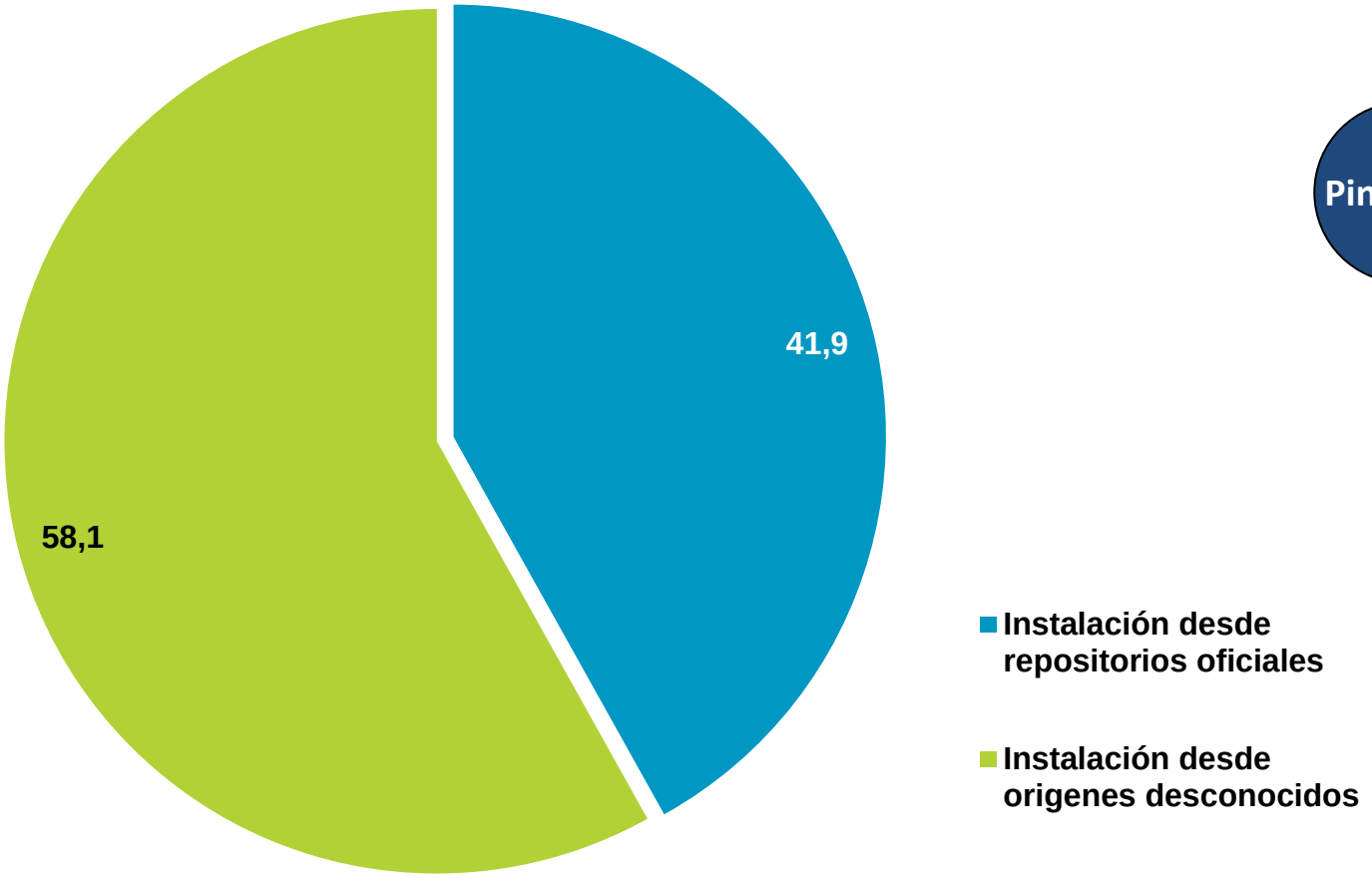
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html#AppendixJAVA

http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html#AppendixJAVA

El aprovechamiento y explotación de vulnerabilidades en Java ha sido, a lo largo de los últimos años, uno de los vectores de entrada más utilizados por el malware para infectar equipos con una versión de este software desactualizada.

Malware vs. orígenes de APPs en Android

Casi 3 de cada 5 (**58,1%**) dispositivos Android que presentan una **infección de malware** disponen de la opción para **permitir la instalación de aplicaciones desde orígenes desconocidos activada**. Dicha opción se encuentra desactivada por defecto.



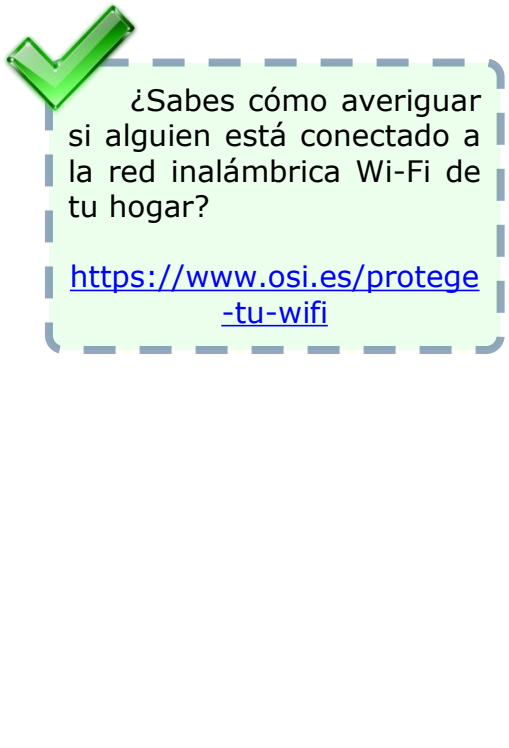
4

Pinkerton

BASE: Usuarios que disponen de dispositivo Android con infección de malware

Incidencias de seguridad en redes inalámbricas Wi-Fi

Aumentan ligeramente hasta el **14,5%** las *sospechas* de **intrusión en la red inalámbrica Wi-Fi** del hogar. Esto supone **+2,2 p.p.** en el último año.



¿Sabes cómo averiguar si alguien está conectado a la red inalámbrica Wi-Fi de tu hogar?

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

BASE: Usuarios con conexión Wi-Fi propia

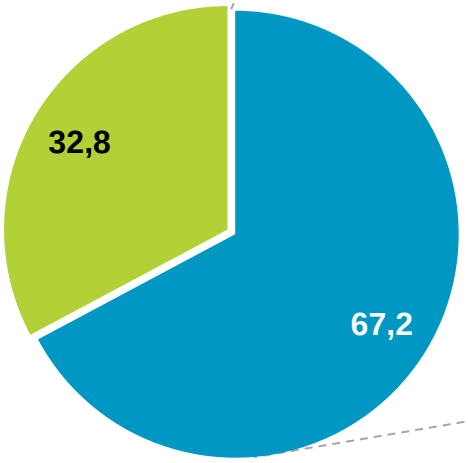
Consecuencias de los incidentes de seguridad y reacción de los usuarios

1. **Intento de fraude online y manifestaciones**
2. **Seguridad y fraude**
3. **Cambios adoptados tras un incidente de seguridad**

5

Intento de fraude online y manifestaciones

Intento de fraude online:

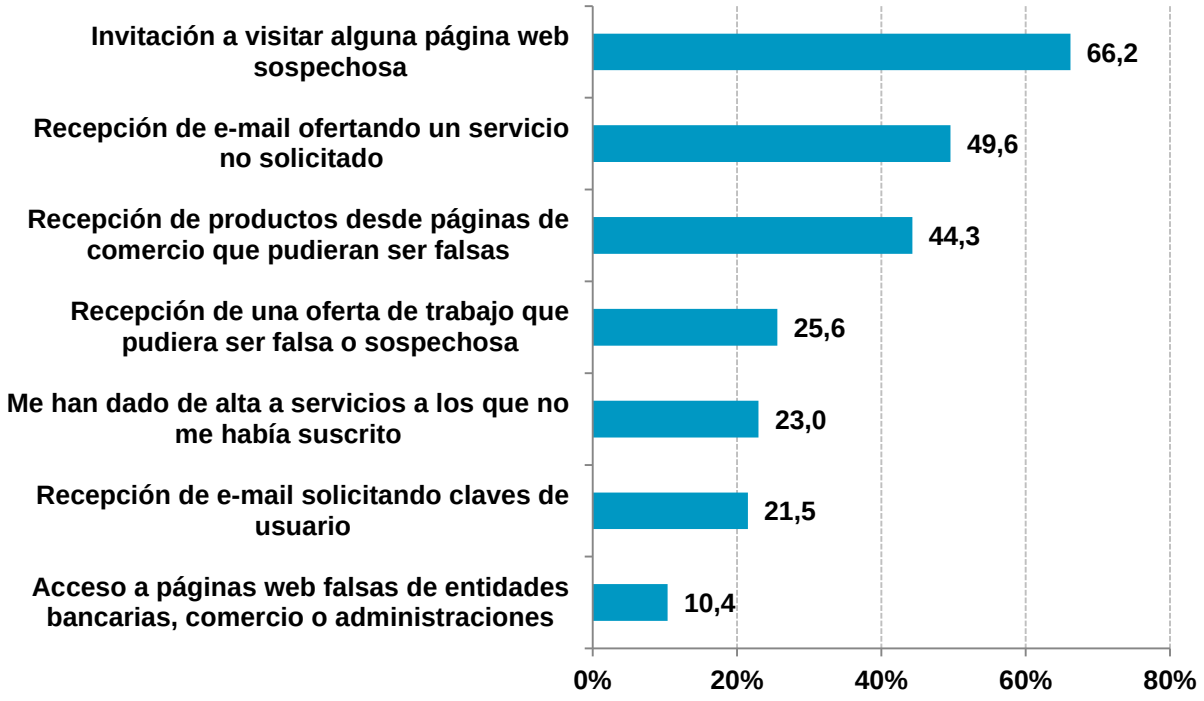


BASE: Total usuarios

Manifestaciones del intento de fraude online:

Respuesta múltiple

% individuos



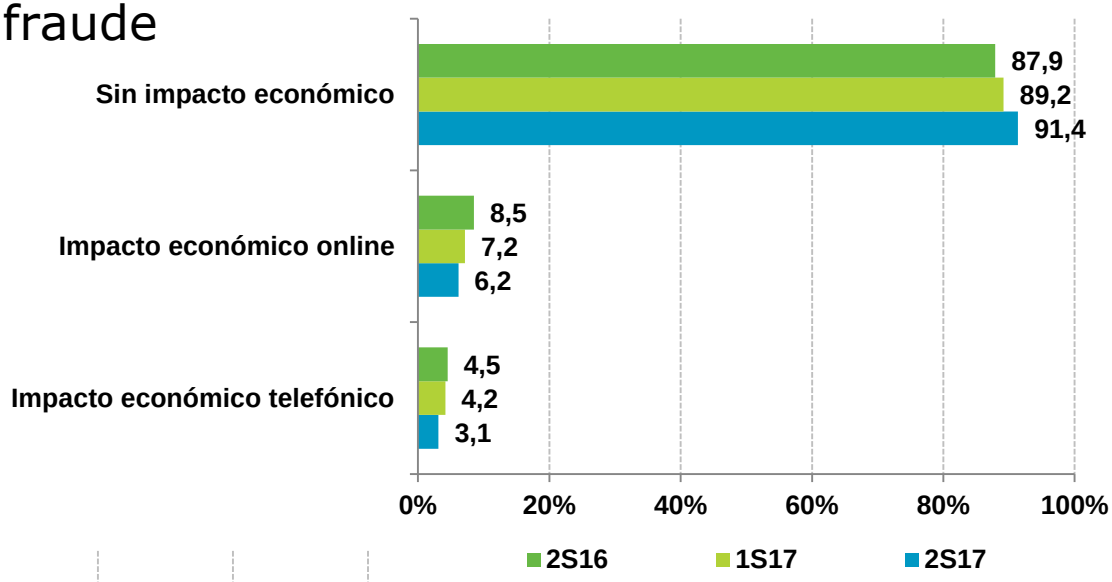
BASE: Usuarios que han sufrido algún intento de fraude

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

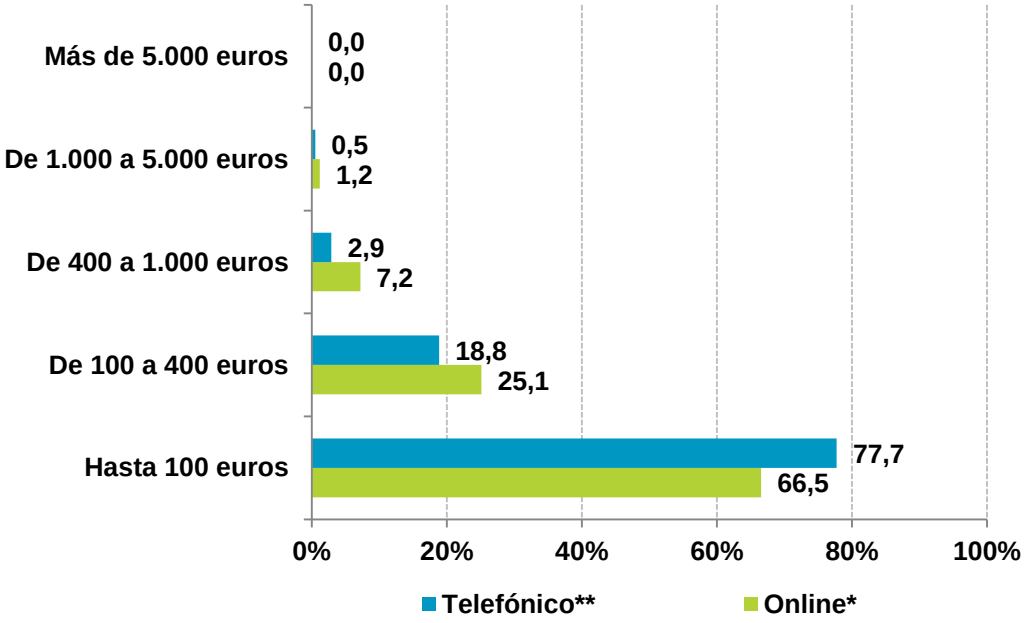
Intento de fraude online y manifestaciones

Impacto económico del fraude

Disminuyen los intentos de fraude que logran causar un **perjuicio económico** para la víctima en el segundo semestre de 2017.



BASE: Usuarios que han sufrido un intento de fraude



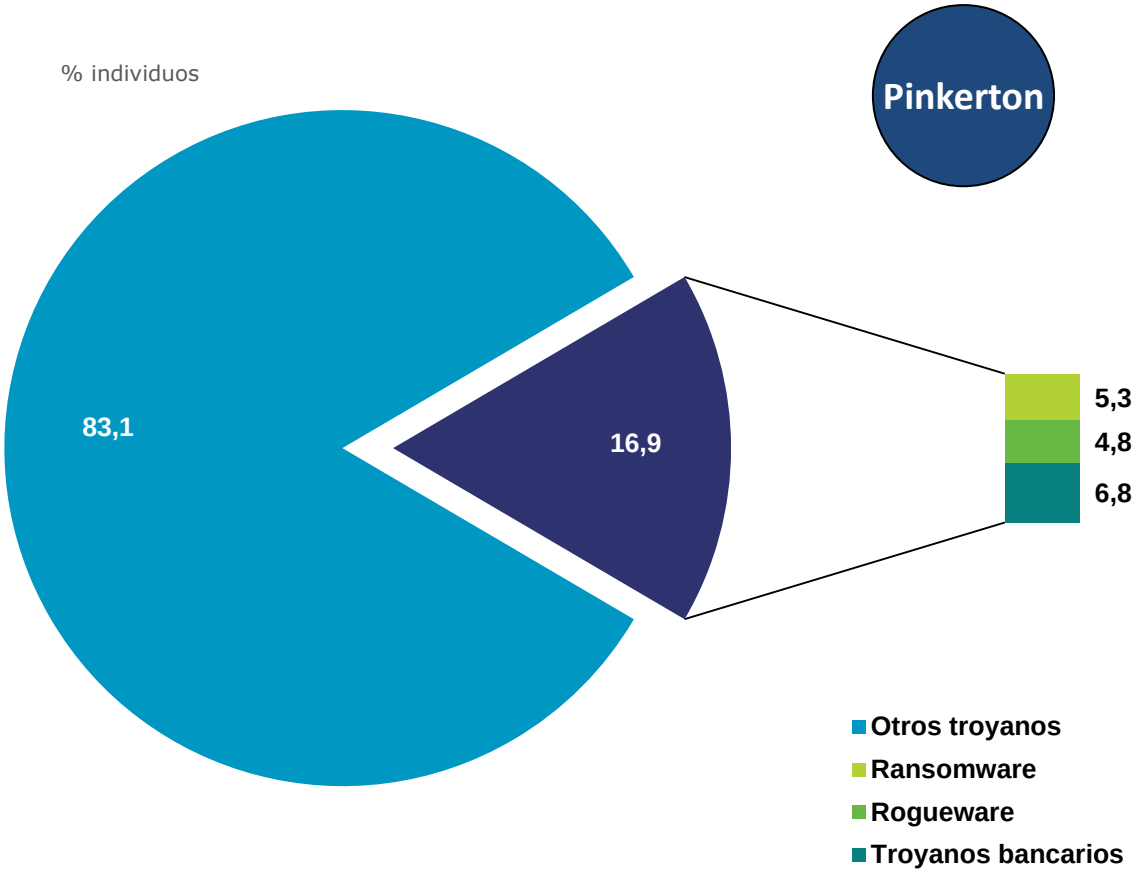
Distribución del impacto económico del fraude

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

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

Fraude y malware en el ordenador

La presencia los ordenadores de los hogares españoles de **troyanos bancarios**, **ransomware** y **rogueware** se sitúa en valores muy similares entre ellos.



BASE: Equipos con troyanos detectados en ordenadores

Tipología del malware analizado

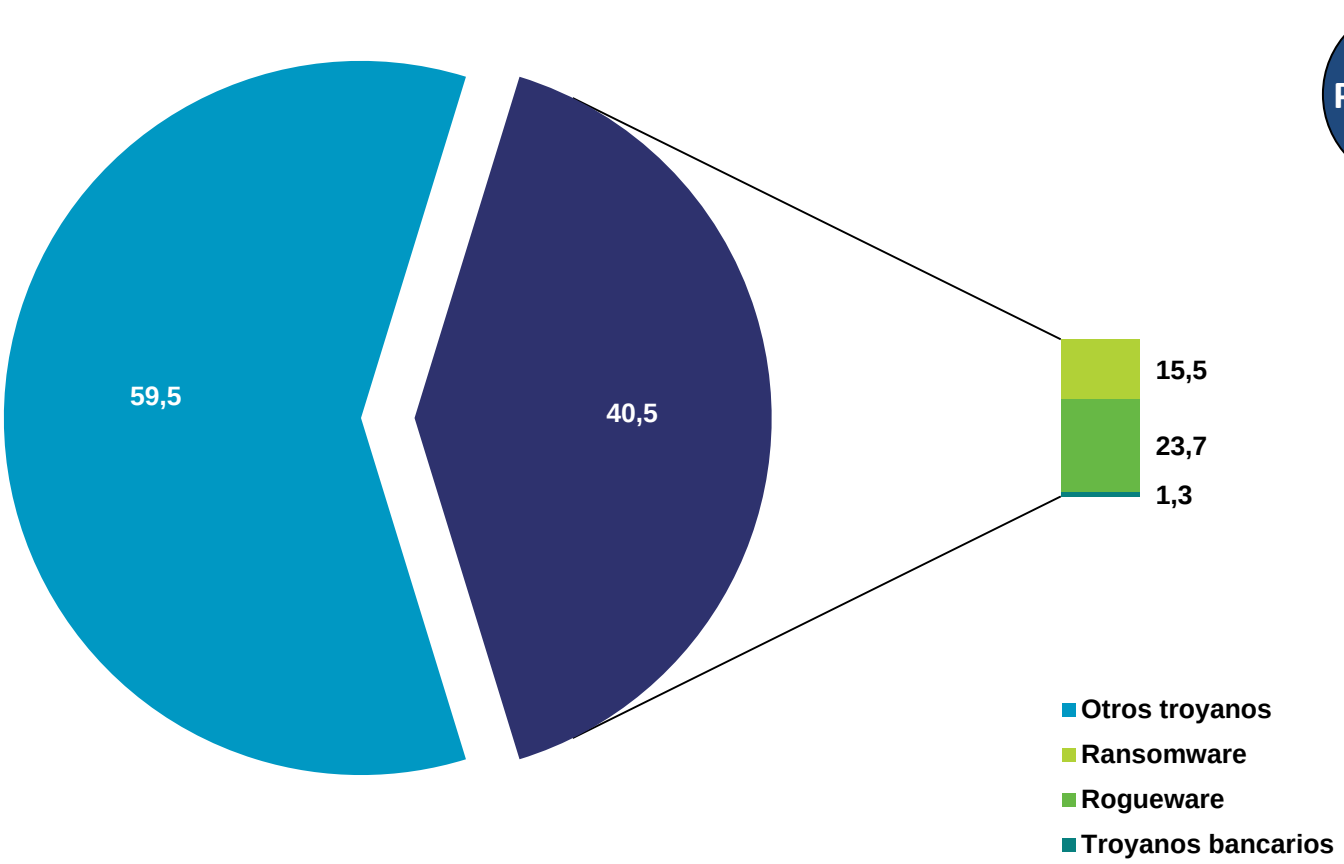
✓ Troyano bancario:
malware que roba información confidencial a los clientes de banca y/o plataformas de pago online.

✓ 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.

Fraude y malware en dispositivos móviles

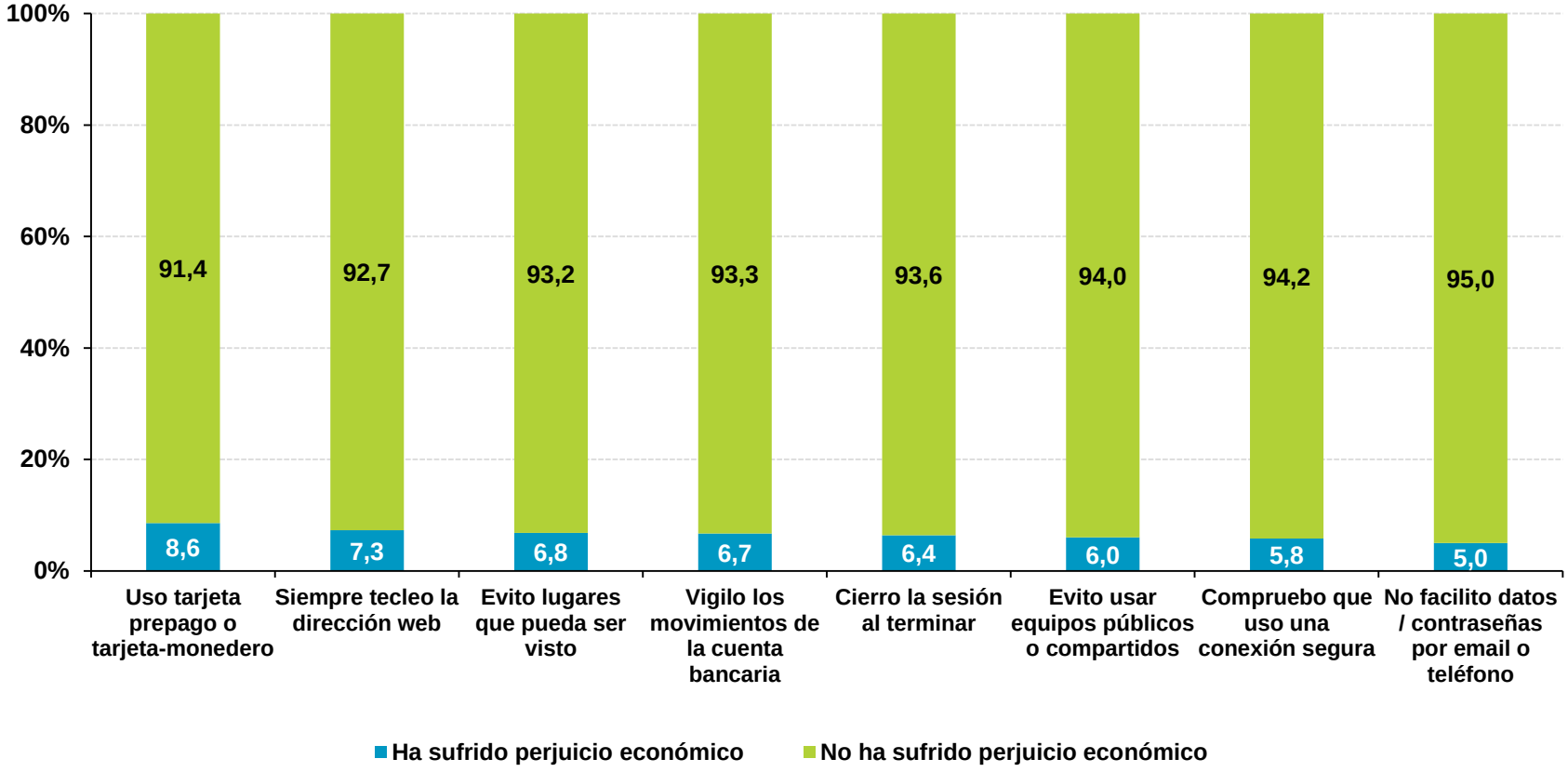
Destaca el **rogueware** como la subcategoría de troyano más detectada en los dispositivos Android**.**



BASE: Equipos con troyanos detectados en dispositivos Android

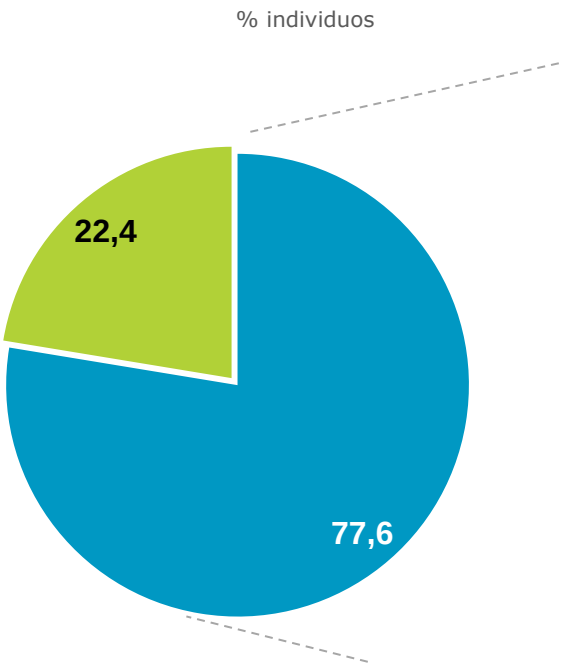
Consumación del intento de fraude según los hábitos prudentes

La utilización de hábitos prudentes conduce a una **minimización** del riesgo de consumación de un intento de fraude. En todos los casos, un porcentaje superior al **91,4%** de los usuarios que tienen buenos hábitos NO sufrieron ningún tipo de perjuicio económico como consecuencia de un intento de fraude.



BASE: Usuarios que utilizan banca online

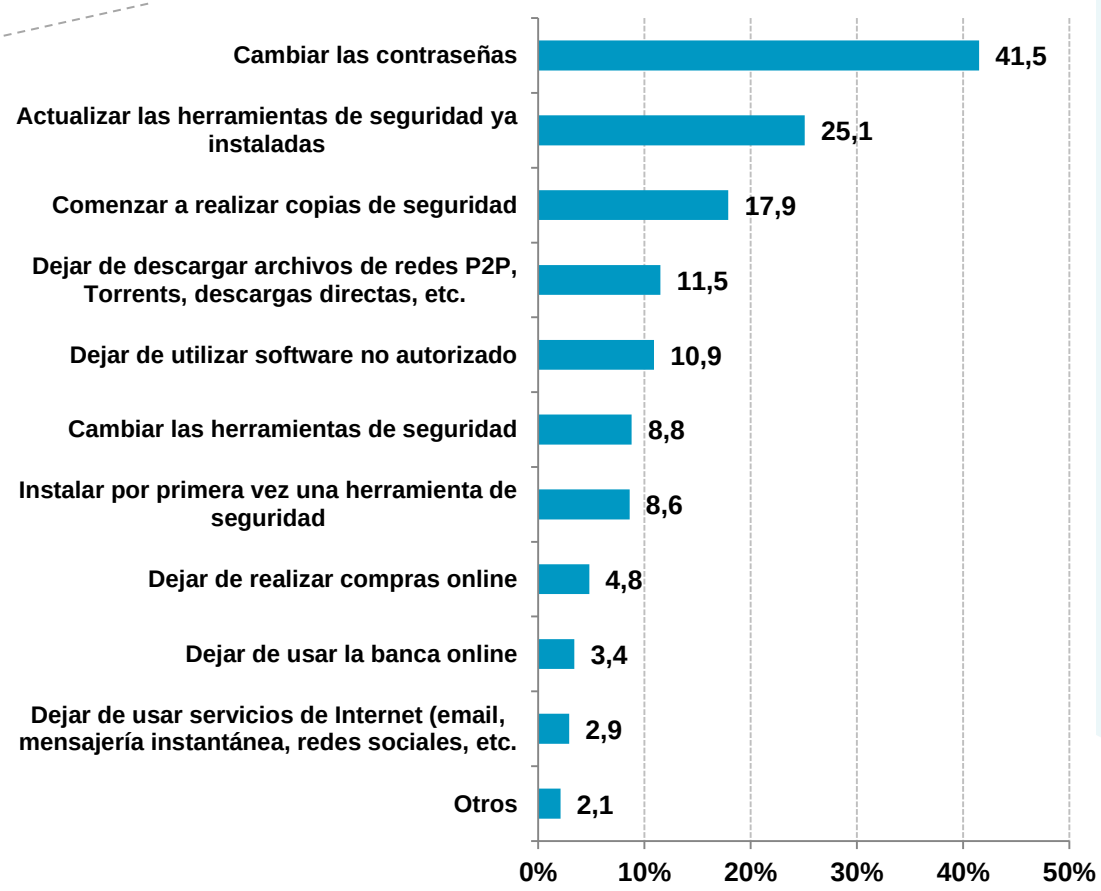
Cambios adoptados tras un incidente de seguridad



BASE: Total usuarios que experimentan alguna incidencia

Cambios realizados:

Respuesta múltiple



BASE: Usuarios que experimentan alguna incidencia y realizan algún cambio

5

No esperes a tener un problema para realizar copias de seguridad:
https://www.osi.es/sites/default/files/docs/copiaseguridad.pdf

Cambios adoptados tras un incidente de seguridad

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

Los usuarios tienden a **modificar sus contraseñas** principalmente a raíz de sufrir una **suplantación de identidad** (**58,6%**), **perder el dispositivo** (**51,3%**), debido a **ciberataques a servicios** que utiliza (**44,8%**) e incidencias relacionadas con **malware** (**42,4%**).

Incidencia (%)	Cambio en los hábitos					
	Cambiar contraseñas	Actualizar herramientas	Realizar copias de seguridad	Cambio de programas de seguridad	Abandonar software no autorizado	Instalar herramientas por 1ª vez
Malware	42,4	**35,4**	22,5	17,9	14,7	12,1
Pérdida de archivos o datos	38,4	32,1	**35,8**	15,3	16	14,9
Recepción de spam	32,1	18,6	13,1	6,2	8,2	4,9
Suplantación de identidad	**58,6**	30,3	22,5	**28,2**	**29,4**	24
Intrusión Wi-Fi	40,8	34,6	19,6	25,6	31,3	32
Pérdida del dispositivo	51,3	34,8	34,2	25,4	24,8	**23,7**
Servicios inaccesibles debido a ciberataques	44,8	29	22,3	16	13	12,7

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

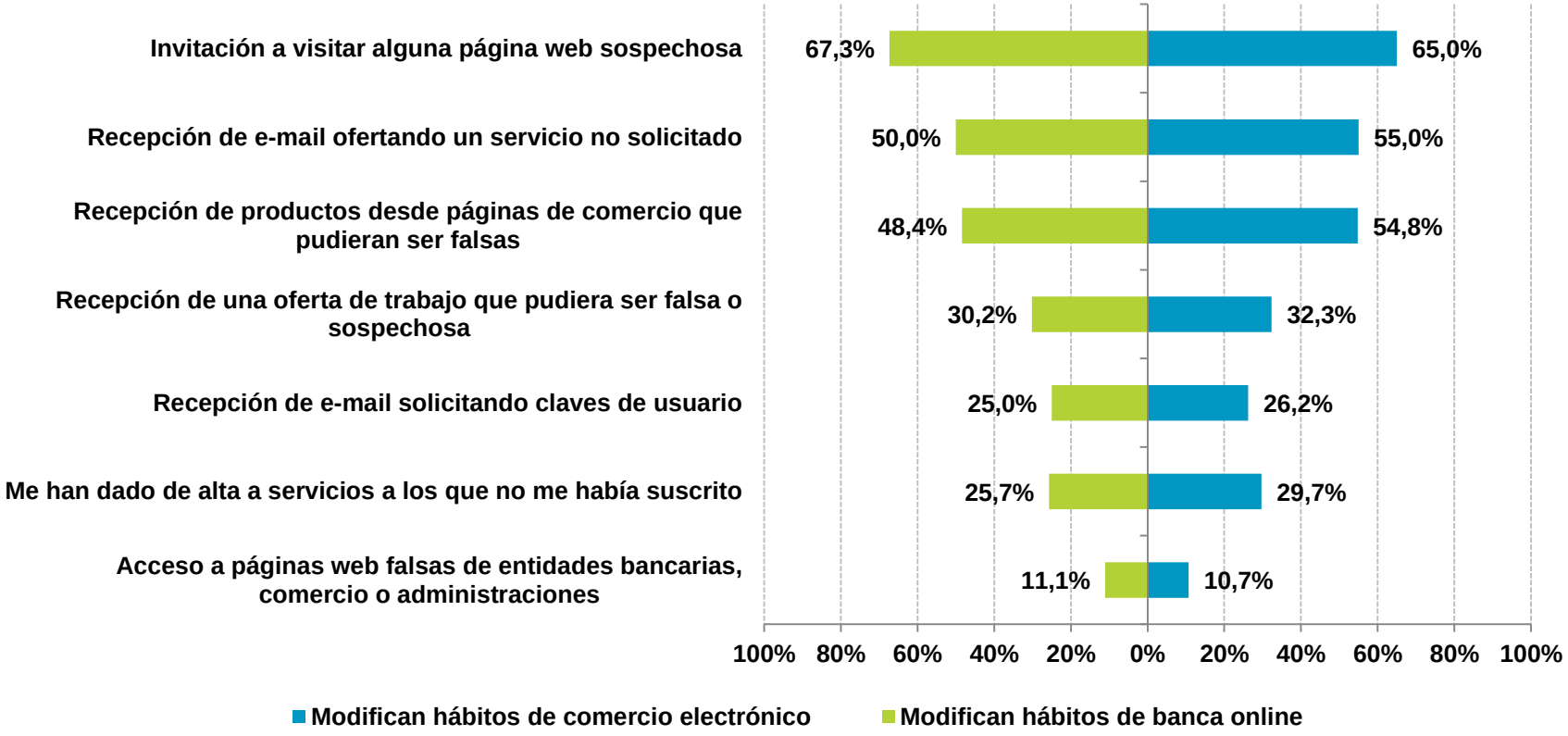
Incidencia (%)	Cambio en el uso de servicios			
	Dejar de usar servicios de Internet	Abandonar la banca online	Abandonar el comercio electrónico	Abandonar descargas
Malware	6	6,6	8,3	15,7
Pérdida de archivos o datos	7,4	8,2	13,3	19,4
Recepción de spam	1,8	2,4	2,9	8,2
Suplantación de identidad	11,6	12,6	19,8	23,7
Intrusión Wi-Fi	**22,1**	**17**	19,9	**28,9**
Pérdida del dispositivo	18	15,9	**22,9**	19,3
Servicios inaccesibles debido a ciberataques	7,5	5,4	6,6	11,5

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

Cambios adoptados tras un incidente de seguridad

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

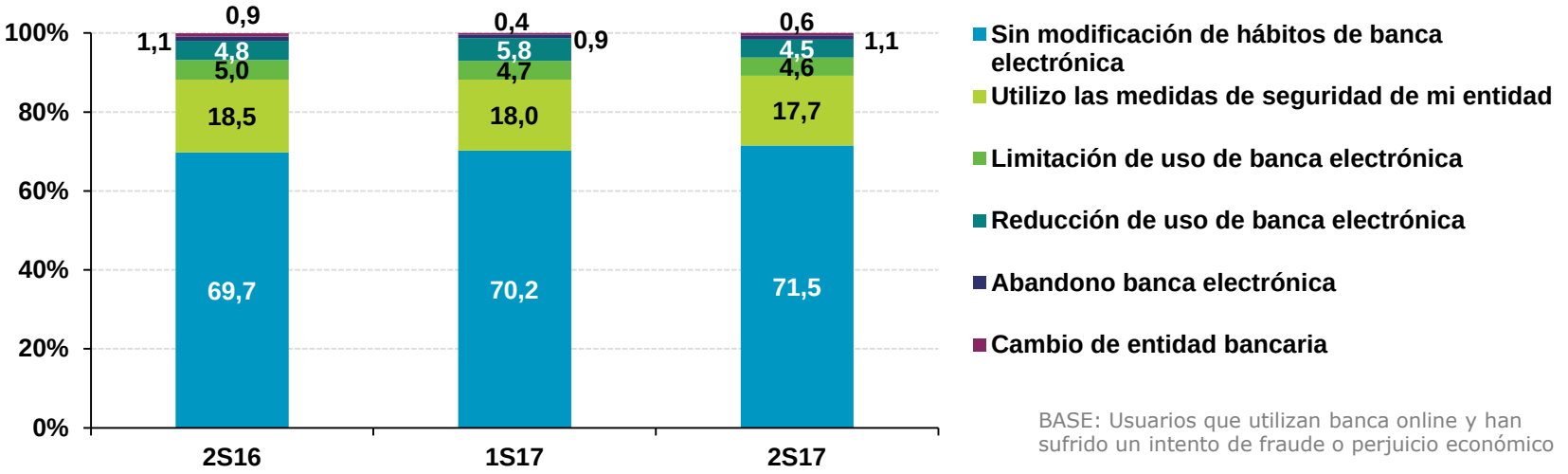
La recepción de una **invitación a visitar alguna página web sospechosa** continua siendo la mayor influencia para la modificación de hábitos del usuario de banca online y comercio electrónico.



BASE: Usuarios que utilizan banca online y/o comercio electrónico y que han sufrido un intento de fraude

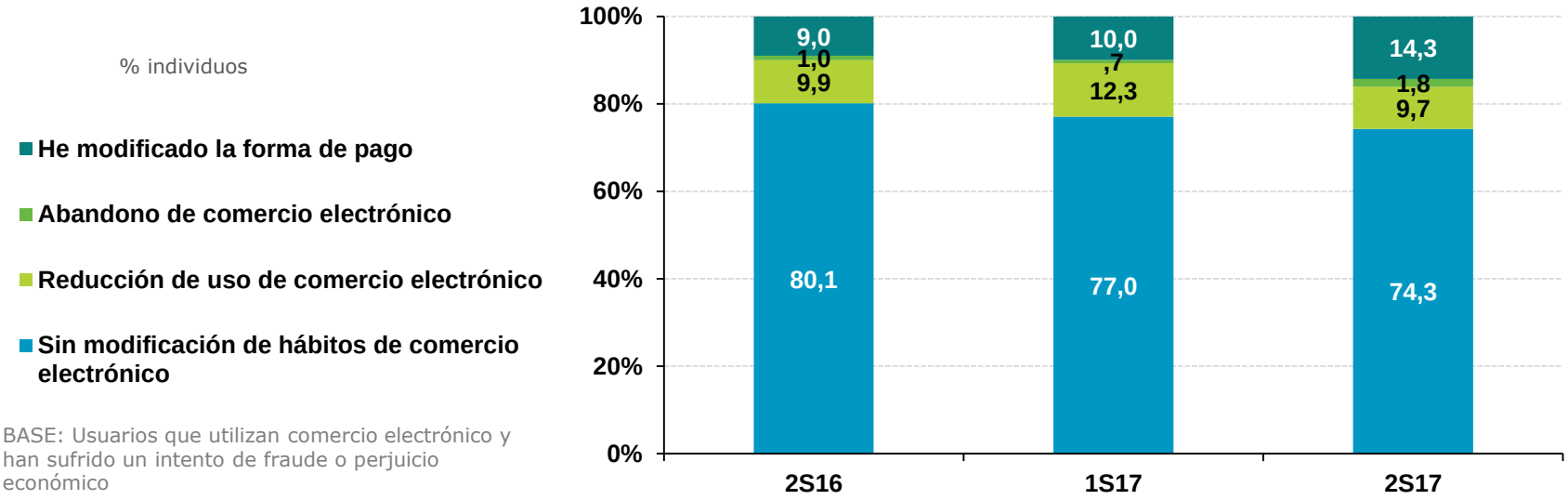
Cambios adoptados tras un incidente de seguridad

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



BASE: Usuarios que utilizan banca online y han sufrido un intento de fraude o perjuicio económico

% individuos



BASE: Usuarios que utilizan comercio electrónico y han sufrido un intento de fraude o perjuicio económico

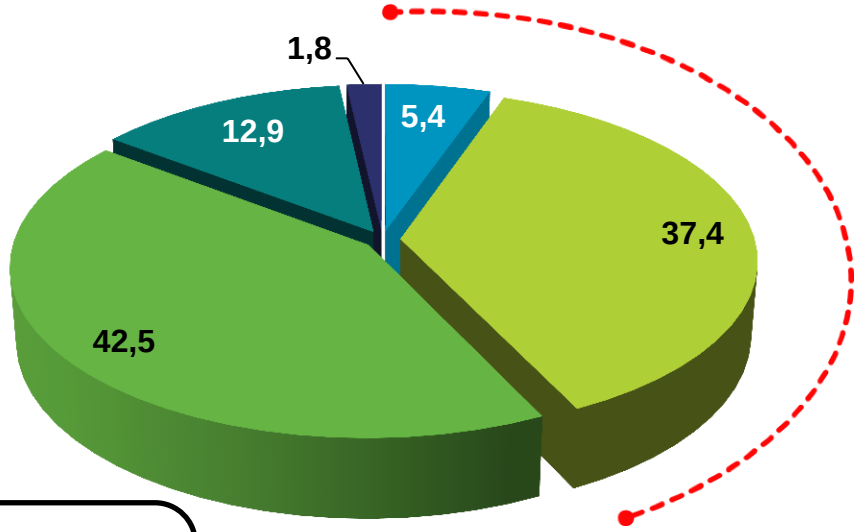
Confianza en el ámbito digital en los hogares españoles

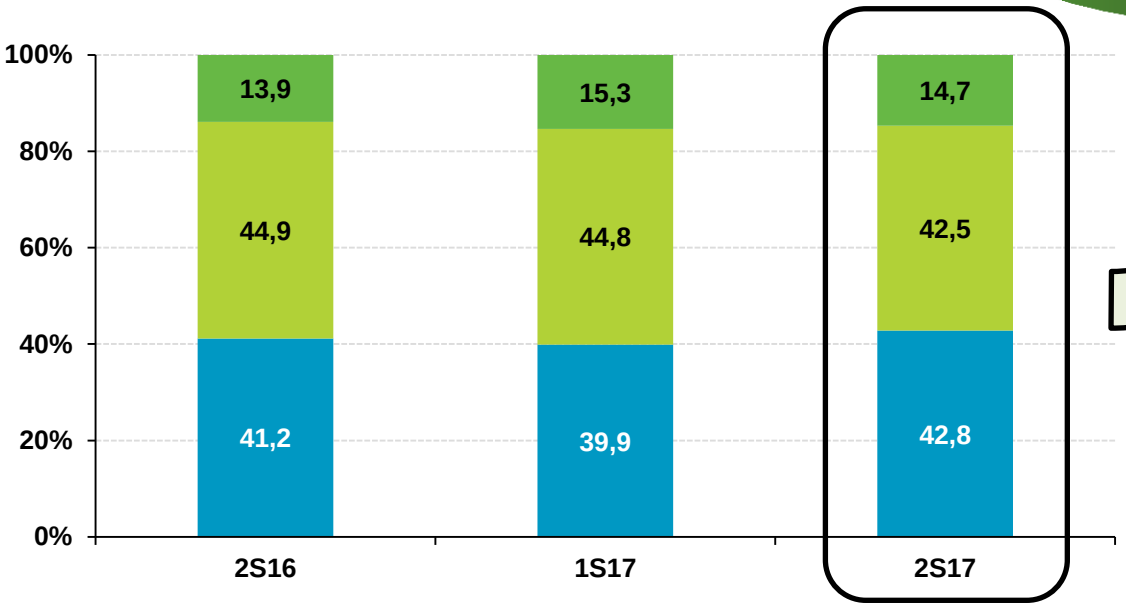
1. **e-Confianza y limitaciones en la Sociedad de la Información**
2. **Percepción de los usuarios sobre la evolución en seguridad**
3. **Valoración de los peligros de Internet**
4. **Responsabilidad en la seguridad de Internet**

6

Nivel de confianza en Internet

Se recuperan casi **3 p.p.** en la confianza depositada por el usuario en la Red, aproximándose a los niveles observados en el último semestre de 2015.



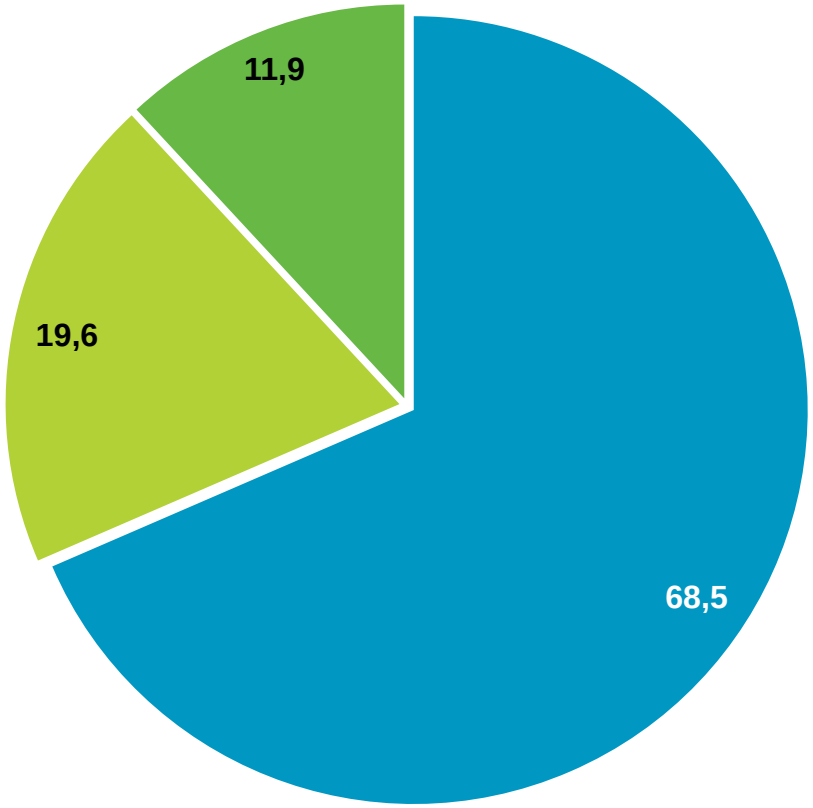


% individuos

BASE: Total usuarios

Valoración del ordenador personal y/o dispositivo móvil como razonablemente protegido

% individuos

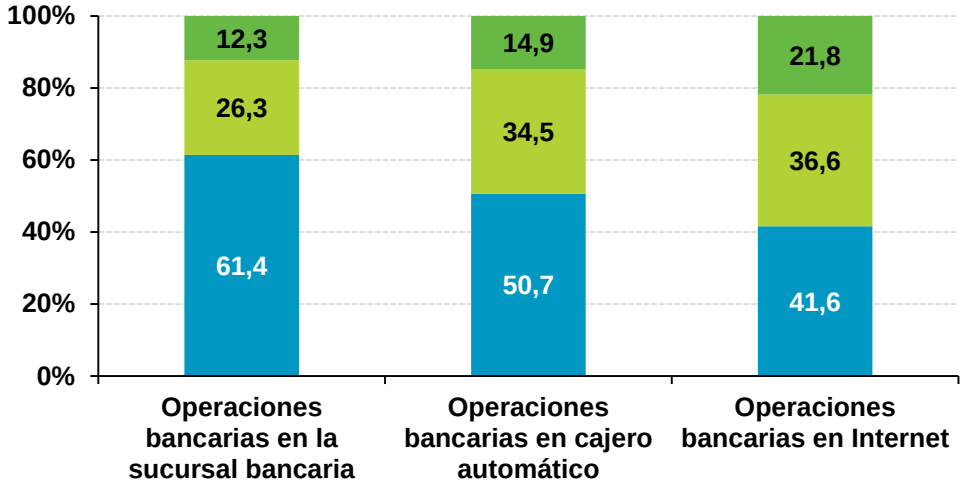


Casi 7 de cada 10 usuarios (**68,5%**) consideran que su equipo (ordenador del hogar y/o dispositivo móvil) se encuentra **razonablemente protegido** frente a las potenciales amenazas de Internet.

6

BASE: Total usuarios

Confianza online vs. confianza offline



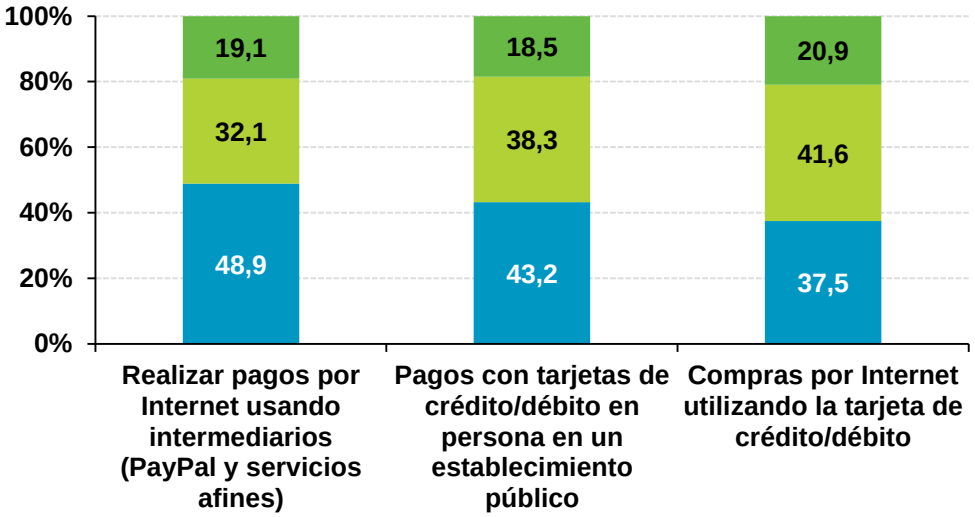
Nivel de confianza en operaciones bancarias

% individuos

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

Nivel de confianza en operaciones de compra-venta

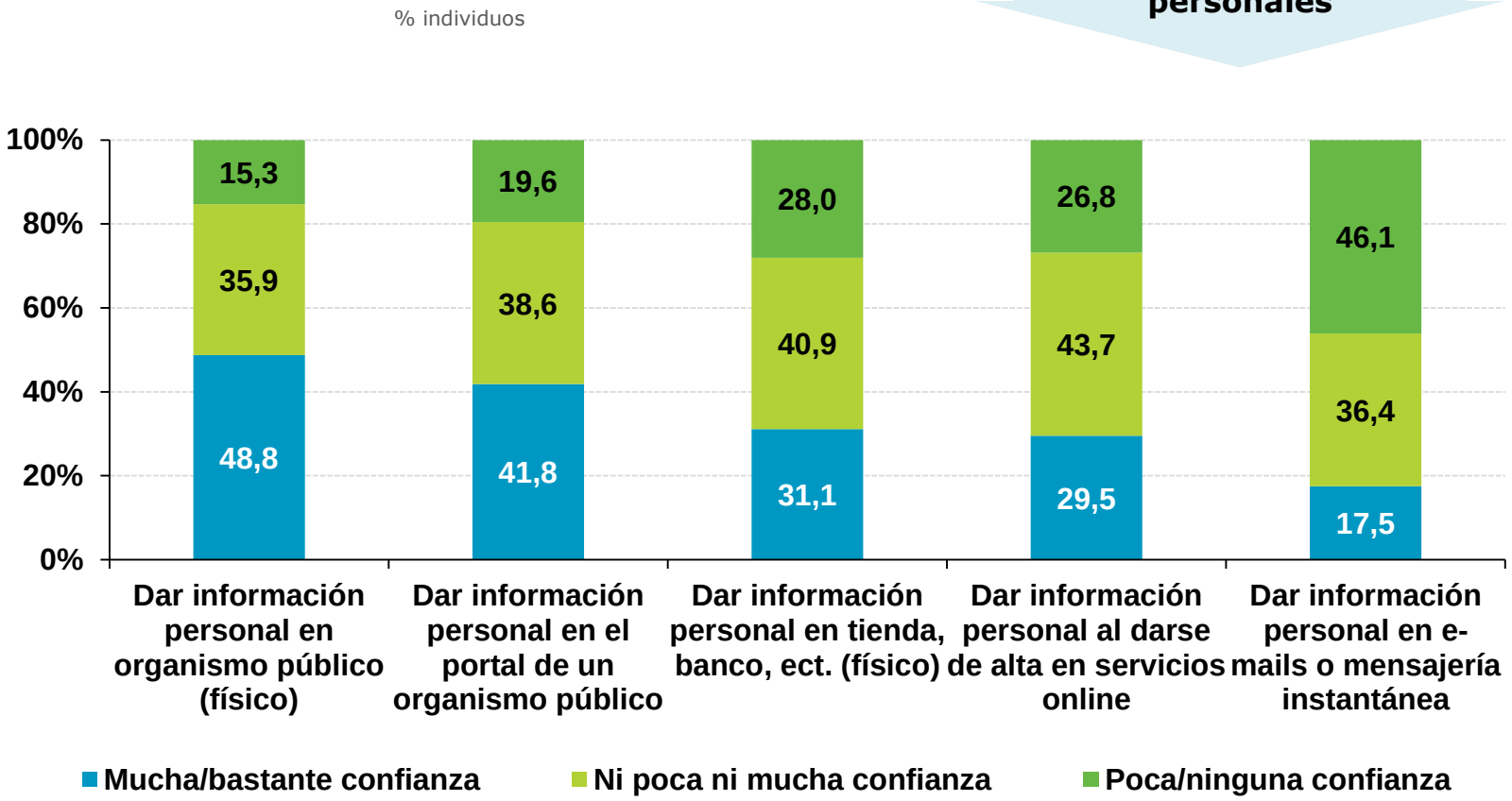
Realizar pagos en Internet usando un intermediario como Paypal reporta una mayor confianza (**+5,7 p.p.**) al usuario que pagar con tarjeta en persona en un establecimiento público.



BASE: Total usuarios

Confianza online vs. confianza offline

Nivel de confianza en facilitar datos personales

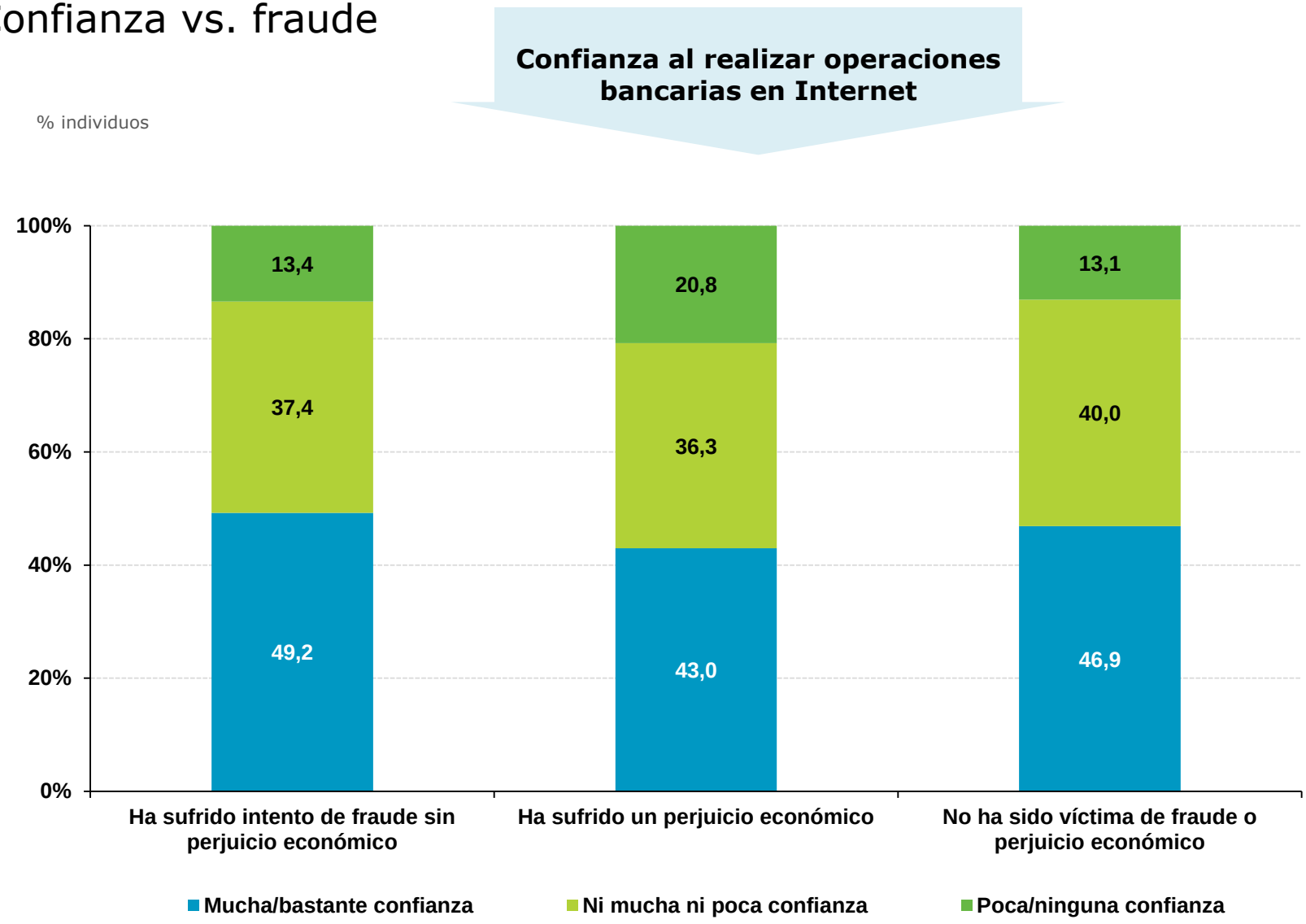


¿Tengo obligación de dar mis datos cuando me los piden?

https://www.osi.es/sites/default/files/docs/datospersonales.pdf

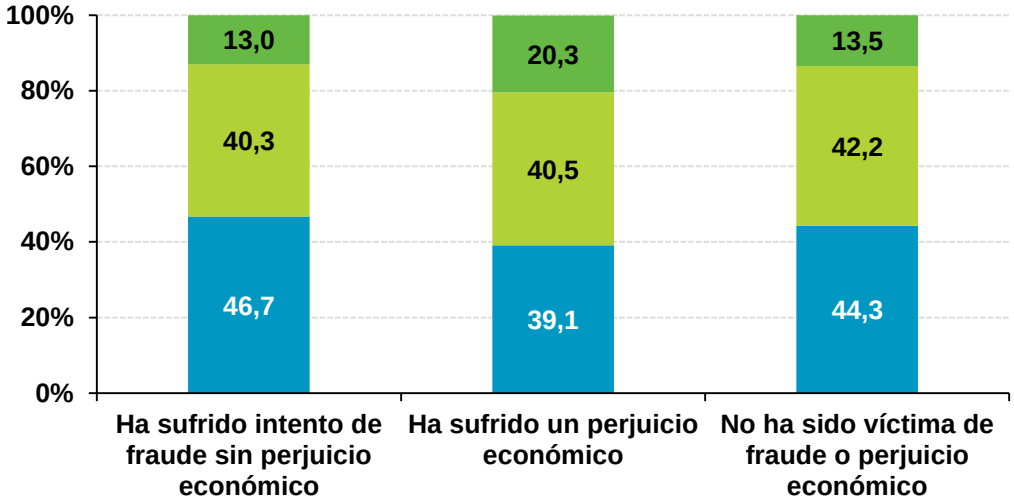
BASE: Total usuarios

Confianza vs. fraude



BASE: Usuarios que utilizan banca online

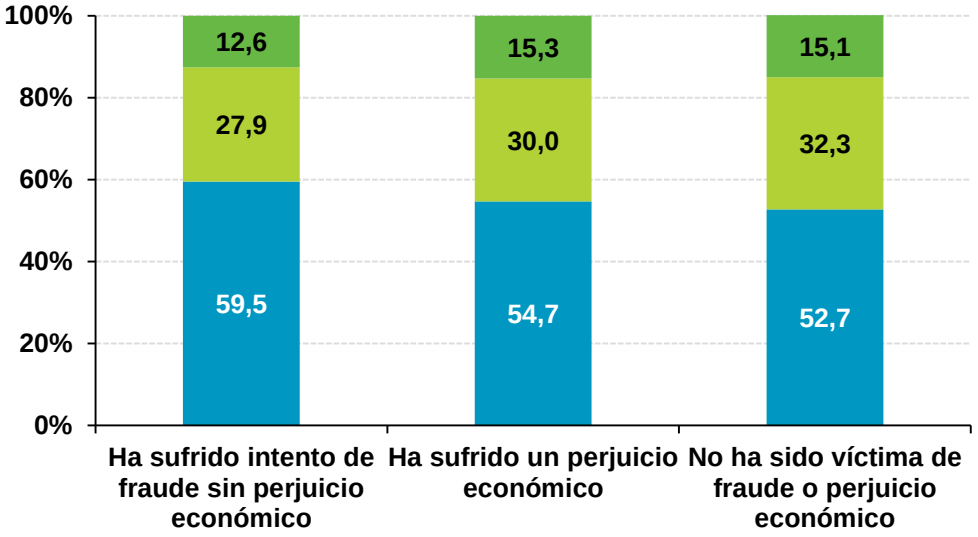
Confianza vs. fraude



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

% individuos

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

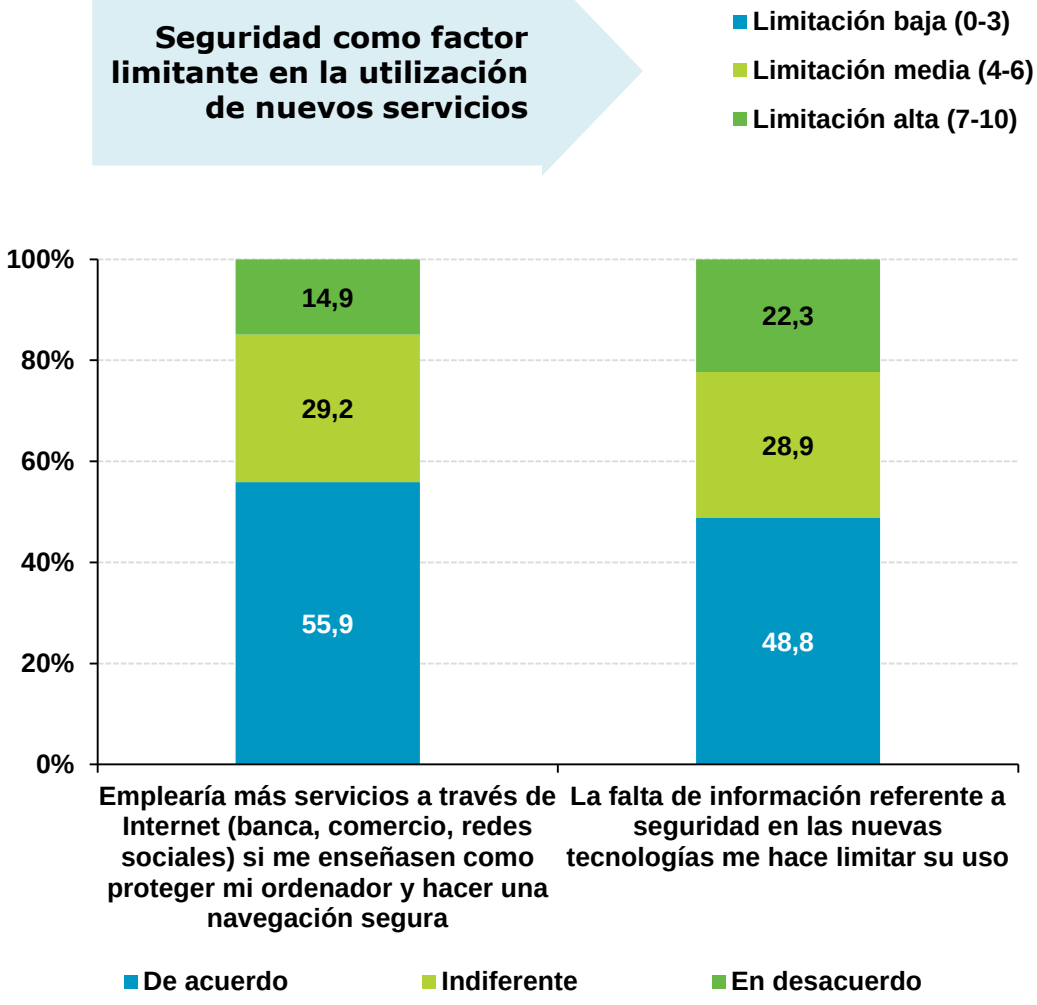


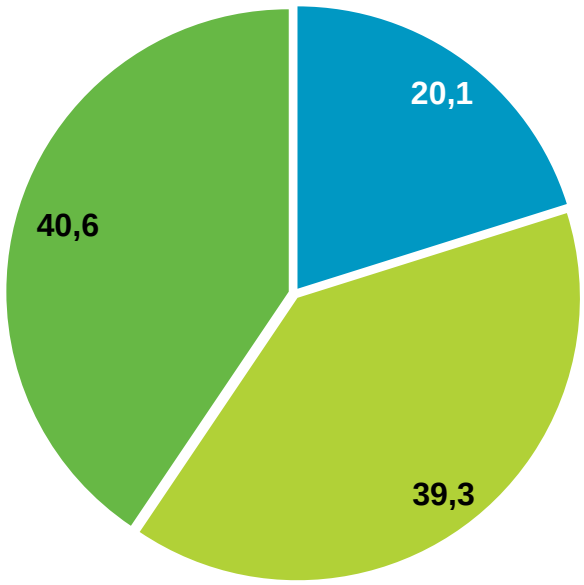
Mucha/bastante confianza
Ni poca ni mucha confianza
Poca/ninguna confianza

BASE: Usuarios que utilizan comercio electrónico

Limitación a causa de problemas de seguridad

Seguridad como factor limitante en la utilización de nuevos servicios





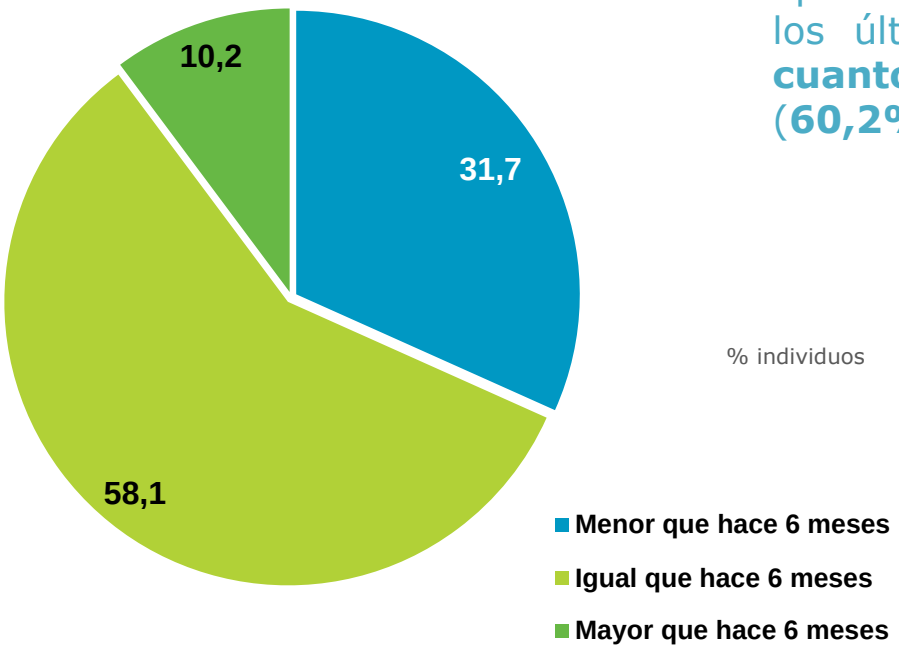
% individuos

Limitaciones en el uso de Internet

6

Percepción de los usuarios sobre la evolución en seguridad

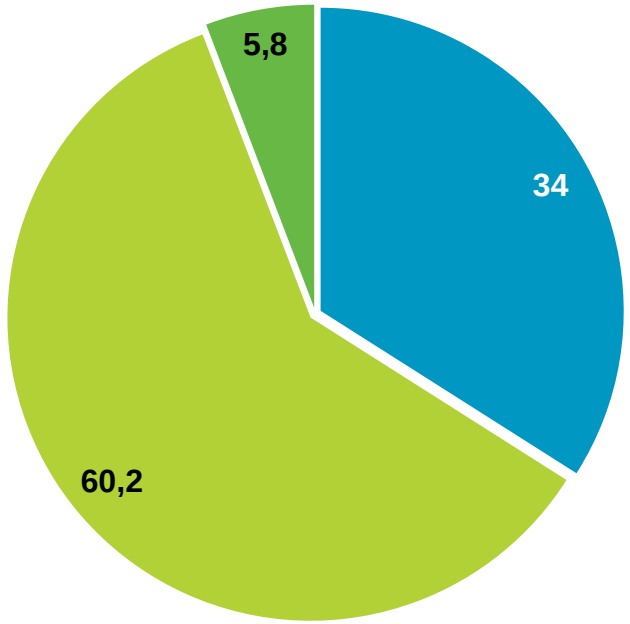
Número de incidencias



Casi 2 de cada 3 usuarios encuestados opinan que las incidencias acontecidas en los últimos 6 meses son **similares en cuanto a cantidad** (**58,1%**) y **gravedad** (**60,2%**) respecto al semestre anterior.

Gravedad de las incidencias

% individuos

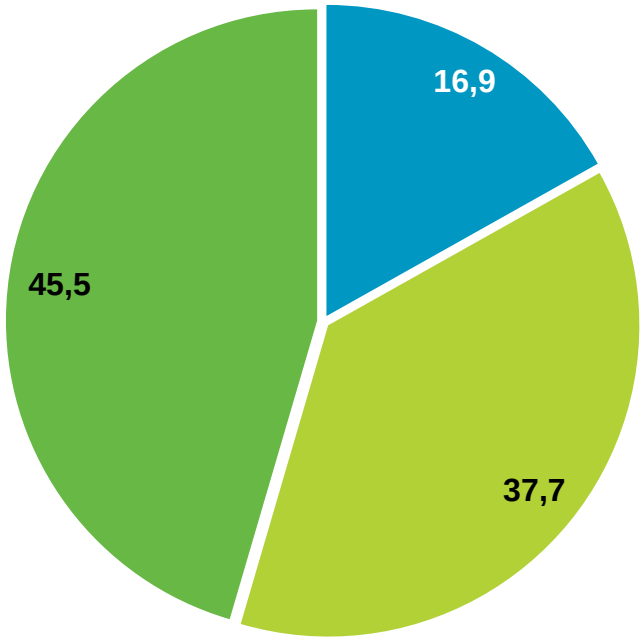


Un tercio percibe un **menor número** de incidencias en los últimos 6 meses (**31,7%**) y además las considera de **menor gravedad** (**34,0%**).

BASE: Total usuarios

Percepción de riesgos en Internet

Los usuarios perciben el **robo y uso de información personal** (**45,5%**) como el principal riesgo en Internet.



% individuos

¿Sabes como cuidar tu privacidad en Internet y tus datos en la nube?

✓ **Privacidad:** https://www.osi.es/es/tu-informacion-personal

✓ **Datos en la nube:** https://www.osi.es/es/tu-informacion-en-la-nube

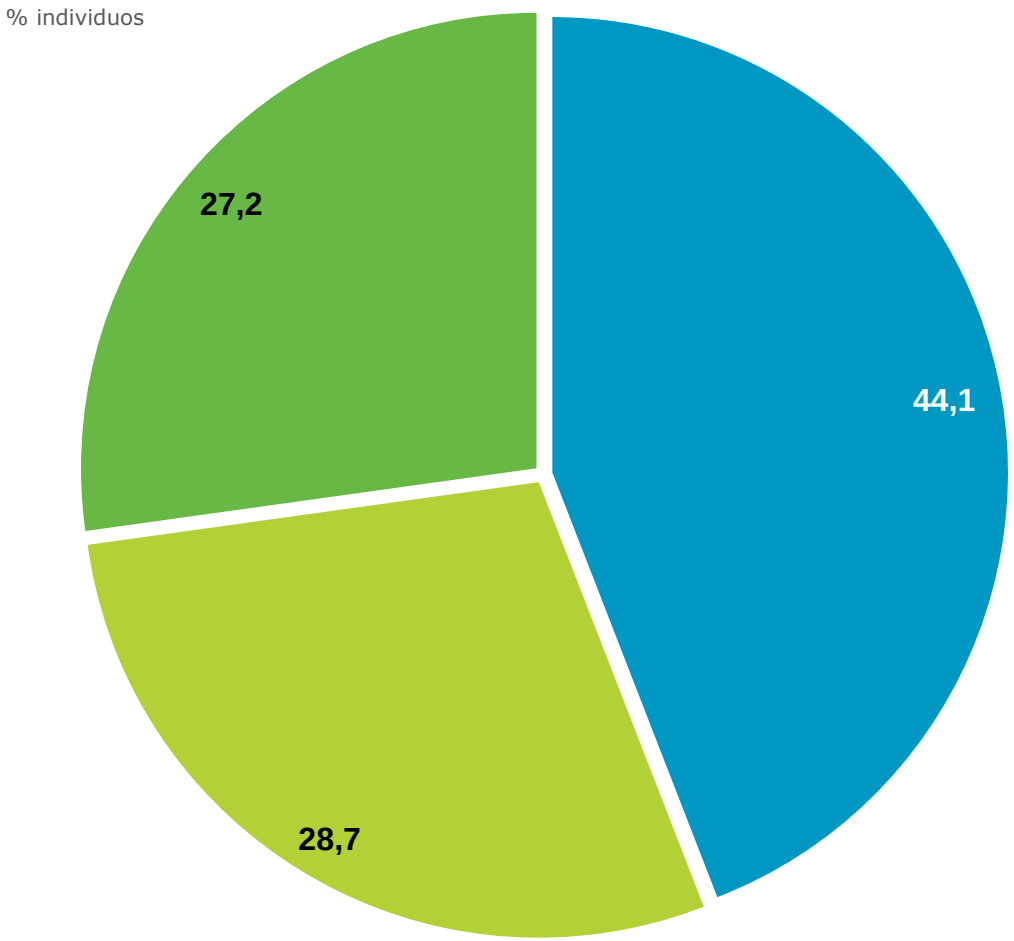
6

- **Daños en los componentes del ordenador (hardware) o en los programas que utilizan (software)**
- **Perjuicio económico: fraude en cuentas bancarias online, tarjetas de crédito, compras**
- **Privacidad: robo o uso sin mi consentimiento de información de carácter personal (fotografías, nombre, dirección)**

BASE: Total usuarios

Percepción de los usuarios sobre la evolución en seguridad

Valoración de Internet cada día como más seguro

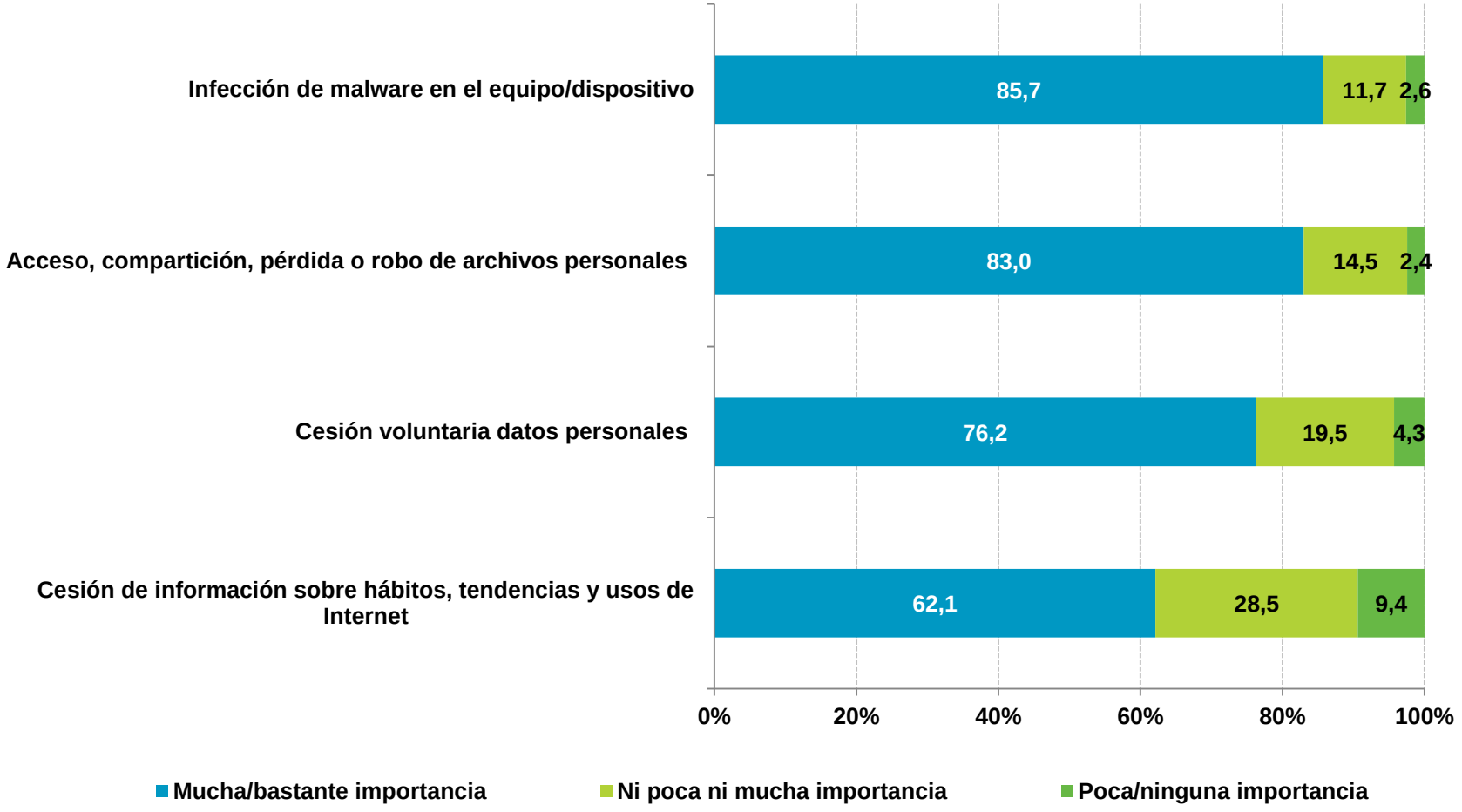


Internet es valorado como cada día más seguro por el **44,1%** de los internautas españoles.

BASE: Total usuarios

Valoración de los peligros de Internet

Los peligros más valorados por los panelistas son la **infección de malware en su equipo/dispositivo** (**85,7%**) y el **acceso, compartición, pérdidas o robo de archivos personales** (**83,0%**).

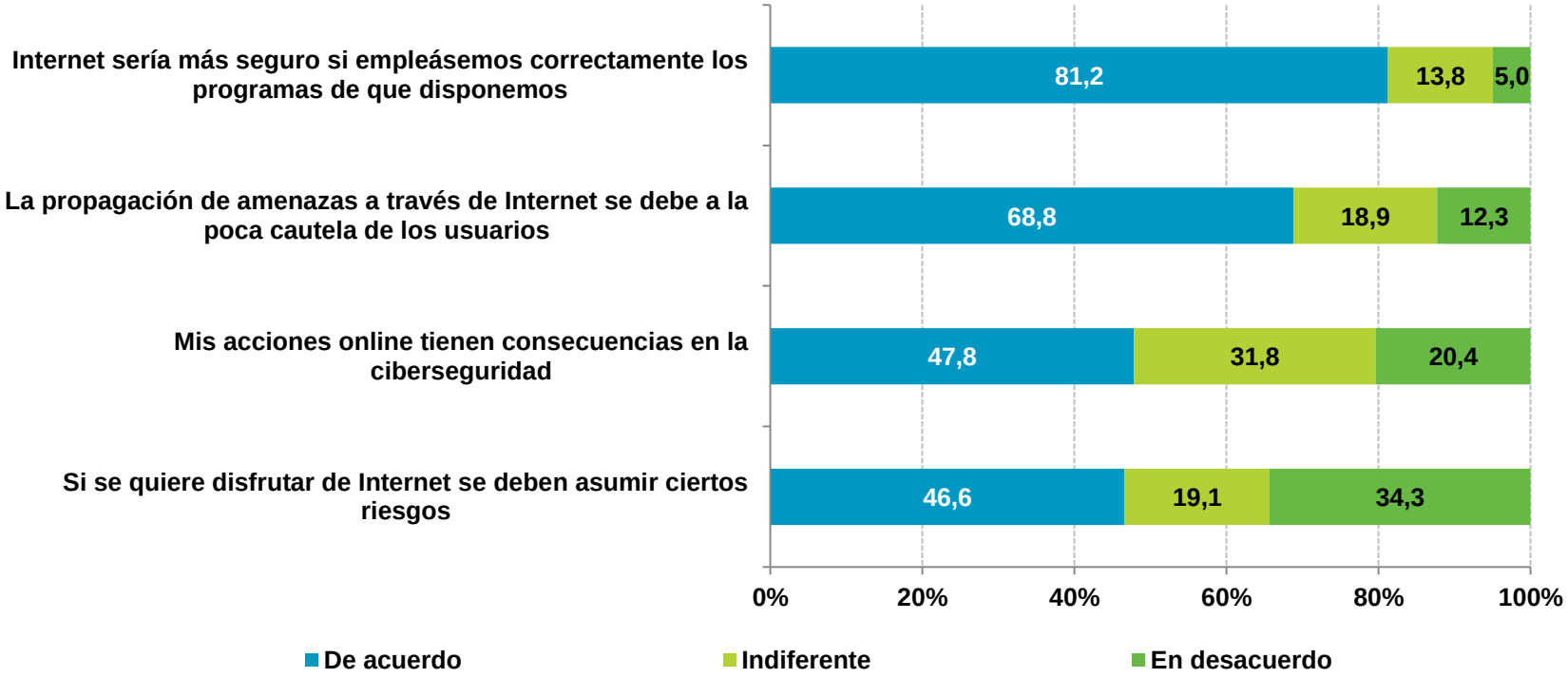


BASE: Total usuarios

Rol del usuario

Los internautas opinan que **la propagación de las amenazas se debe a la poca cautela de los propios usuarios** (**68,8%**) y que **sus acciones tienen consecuencias en la ciberseguridad** (**47,8%**).

Por otro lado, el **46,6%** considera **necesario asumir ciertos riesgos para disfrutar de Internet**.



BASE: Total usuarios

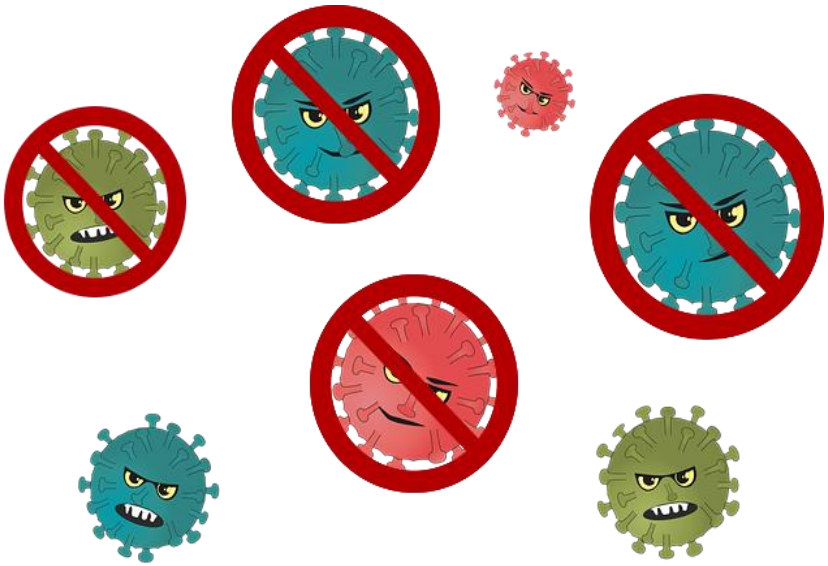
Conclusiones

Conclusiones

Conclusiones

En el segundo semestre de 2017 nos encontramos con un escenario donde las aguas empiezan a volver a su cauce tras el maremoto de noticias causado por el *malware*, o más concretamente el *ransonware* (*'Wannacry'*, *'NotPetya'*, *'exPetr'*) y ante tal situación la e-confianza del usuario comienza a recuperarse (42,8%), Internet sigue siendo considerado como cada día más seguro (44,1%), los equipos se consideran razonablemente protegidos (68,5%) y se relaja el hábito de realización de copias de seguridad (55,9%, -4,6 p.p. con respecto al primer semestre del año), e incluso entre aquellos que comienzan a hacer *backups* tras un incidente de seguridad (-2,6 p.p.). Pero, aunque no copen las portadas en los medios de comunicación, los desarrolladores de *malware* y sus creaciones no descansan.

Una gran parte del *software* malicioso resulta novedoso e innovador de forma que pueda eludir las detecciones de las soluciones antivirus basadas en firmas (hasta un 47% del *malware* detectado en el segundo trimestre de 2017 [1]), o se va transformando continuamente para adaptarse (como el *adware 'Stantinko'*, que ha logrado pasar desapercibido durante 5 años [2]). Sin embargo estos datos no deben interpretarse como que los antivirus no son necesarios o efectivos, sino que ponen de manifiesto la importancia de mantener actualizado tanto el motor como las firmas.



[1] https://www.watchguard.com/wgrd-resource-center/security-report

[2] https://www.welivesecurity.com/wp-content/uploads/2017/07/Stantinko.pdf

Conclusiones

Nos encontramos con que el uso real de soluciones antivirus por parte de los internautas españoles es más relajado que el uso declarado (-4,6 p.p. en ordenadores y -6,1 p.p. en dispositivos Android) junto a un mínimo histórico en las incidencias declaradas relacionadas con *malware* (19%) que podría estar causando una falsa sensación de seguridad. Queda patente la delicadeza de este tema al contrastar el estado real de los equipos con las opiniones de sus usuarios: el 61,7% de los usuarios de ordenadores y el 28,1% de dispositivos Android, no se percatan de las infecciones existentes en sus equipos. Además, 7 de cada 10 de estos equipos se encuentran en riesgo alto debido a la tipología de *malware*.

Los usuarios analizan todos los ficheros descargados desde redes P2P (59,6%), descarga directa (46,6%), e instala aplicaciones Android principalmente desde repositorios oficiales (92,8%) para evitar incidencias de seguridad. Pero los desarrolladores de *malware* sacan provecho de vulnerabilidades tanto en el *software* o el sistema operativo, como Android (+11,9 p.p. de infecciones en dispositivos no actualizados), *Java* [3] (+13,6 p.p. de infecciones en ordenadores que lo tienen instalado), o *Adobe Flash* [4], como en protocolos de comunicaciones como Bluetooth[5], así como también de sistemas online utilizados por los usuarios como *LinkedIn Messenger* [6] y *Facebook Messenger* [7].

[3] https://www.ca.com/ar/company/newsroom/press-releases/2017/88-percent-of-java-apps-susceptible-to-widespread-attacks-from-known-security-defects-according-to-new-research-from-ca-veracode.html

[4] https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

[5] https://blog.fortinet.com/2017/09/14/blueborne-may-affect-billions-of-bluetooth-devices

[6] https://blog.checkpoint.com/2017/08/18/malware-hiding-resume-vulnerability-linkedin-messenger-allowed-malicious-file-transfer/

[7] https://www.kaspersky.es/blog/facebook-messenger-malware/14287/

Conclusiones

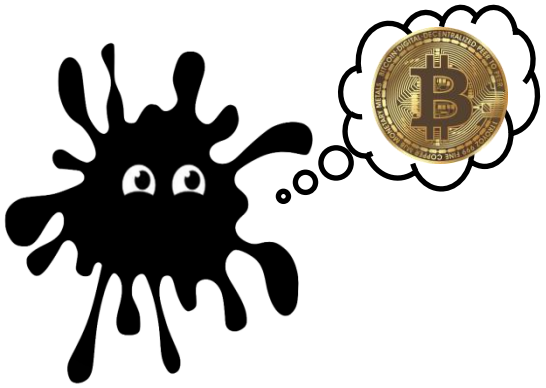
Otro de los objetivos del *malware* es la creación de *botnets*, que son grupos de ordenadores y dispositivos comprometidos -llamados *bots* o *zombies*- controlados remotamente para realizar ataques *DDoS*, hacer *SPAM*, etc. En este sentido España es el quinto país europeo con más equipos formando parte de estas redes, destacando la ciudad de Madrid en número de los mismos [8].

Durante este segundo semestre de 2017, concretamente en Agosto, se descubrió la mayor *spambot* hasta la fecha [9]: *'Onliner'* utilizaba hasta 711 millones de cuentas de correo electrónico con sus correspondientes credenciales para enviar *SPAM* y distribuir sitios fraudulentos de *phishing* y *malware* (como el *troyano* bancario *'Ursnif'*). Los emails utilizados provenían en su mayoría de filtraciones de bases de datos como las de *LinkedIn* y *Badoo*, poniendo de manifiesto la importancia de cambiar las contraseñas de acceso a servicios online con cierta periodicidad. (actualmente sólo el 33,2% de los usuarios españoles lo hace cuando tiene constancia de una incidencia de seguridad).

[8] https://uk.norton.com/tools/bots/index.html#madrid

[9] http://www.zdnet.com/article/onliner-spambot-largest-ever-malware-campaign-millions/

Conclusiones



Bien conocido es el hecho de que una de las principales motivaciones que mueve a los desarrolladores de *malware* redunda en el beneficio económico que sus códigos les pueden reportar (*adware*, troyanos bancarios, *ransomware*, etc.). El hecho de que durante los últimos meses de 2017 se haya experimentado un gran crecimiento en el valor del *Bitcoin*, ha propiciado que las criptomonedas se sitúen en el punto de mira de estos ya que podrían resultar en una importante fuente de ingresos.

Así se han divisado muestras que con el objetivo de robar criptodivisas y sus *wallets* (monederos digitales) [10][11], crear *botnets* (de servidores, ordenadores personales y dispositivos móviles, etc.) [12][13][14] para utilizar la capacidad de procesamiento en pos de la minería, insertar *script* en sitios web [15] para aprovechar los recursos de las máquinas usadas por los visitantes, etc.

Por regla general, las infecciones con objeto de minar son difíciles de detectar dado que el *malware* –de tipo *dropper*– descarga, tras una infección exitosa, un cliente de minado que de por sí no es malicioso y podría ser instalado legítimamente por el propio usuario del equipo. Esto implica que aunque la infección sea detectada y eliminada, el *software* de minado permanezca instalado y reportando beneficios a los cibercriminales. Hecho que ofrece un aliciente adicional a los desarrolladores de código malicioso.

[10] https://www.welivesecurity.com/la-es/2013/12/16/bitcoins-valiosa-robusta-pero-facil-extraviar-robar/

[11] https://www.kaspersky.es/blog/cryptoshuffler-bitcoin-stealer/14701/

[12] https://securelist.com/miners-on-the-rise/81706/

[13] https://www.welivesecurity.com/la-es/2017/09/29/malware-que-mina-monero/

[14] https://www.kaspersky.es/blog/loapi-trojan/15024/

[15] https://www.pandasecurity.com/spain/mediacenter/malware/webs-apps-malware-criptomonedas/

Conclusiones

Por otra parte, existen hogares españoles que mantienen una configuración de red inalámbrica con una protección que la hace vulnerable: uso de protocolo *WEP* que está obsoleto (4,9%) y sin ningún tipo de protección (4,9%). Incluso queda demostrada la indiferencia de los usuarios en este sentido en vistas del 13,2% que desconoce si su red Wi-Fi se encuentra o no protegida y del 27,1% que piensa que sí lo está aunque desconoce el sistema utilizado; en ambos casos cabe presuponer que se utiliza la configuración por defecto establecida por el proveedor del servicio, que podrían ser vulnerables. A pesar de esto, únicamente el 14,5% sospecha haber sufrido una intrusión en su red.

Pero tampoco *WPA2/WPA* se libra de ser atacable: se han descubierto múltiples vulnerabilidades en el propio diseño [16][17] que deja en riesgo a todos los dispositivos que hacen uso de este sistema ante un ataque que ha recibido el nombre de *KRACK* (*Key Reinstallation Attack*), poniendo de manifiesto -una vez más- la importancia de las actualizaciones de seguridad.

Mientras tanto, 1 de cada 3 usuarios se conectan a una red inalámbrica Wi-Fi pública (18,9%) o de un particular ajeno (14,9%), poniendo en un posible riesgo su información personal, datos bancarios, credenciales de cuentas de correo electrónico, etc. a pesar de que el 53% no sabe diferenciar entre una red Wi-Fi pública segura o insegura [18].

[16] http://papers.mathyvanhoef.com/ccs2017.pdf

[17] https://www.itproportal.com/news/millions-of-android-phones-put-at-risk-by-mobile-wiffi-security-flaw/

[18] https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf

Conclusiones

Se deriva de las declaraciones de los usuarios que el 91,4% no ha sufrido perjuicio económico ocasionado por un fraude online gracias a los buenos hábitos de uso. Como contrapunto, las infecciones de *malware* aumentan (+6,8 p.p. en ordenadores del hogar y +5 p.p. en Android). En relación con este crecimiento se detectan comportamientos de riesgo. Así, casi el 30% de los dispositivos Android han sido configurados para permitir la instalación de aplicaciones desde fuentes desconocidas (lo que implica una diferencia de 16,2 p.p. en infecciones reales con respecto a aquellos que no las permiten) y el 39% no comprueba los permisos de las *APPs* durante el proceso de instalación. En esta situación resulta inquietante la baja aceptación por parte de los internautas de medidas de seguridad básicas como puede ser la protección proporcionada por el antivirus (69% en PC y 43,7% en Android).

Considerando además que casi el 88% de las incidencias percibidas por los usuarios españoles están relacionadas con el *SPAM* y que, aunque casi la totalidad de los usuarios afirman ser capaces de detectar un correo de *phishing* [19], el 56% continúa haciendo *click* en los enlaces procedentes de remitentes desconocidos (vía email, redes sociales, chats) [20] debido a la curiosidad aun siendo conscientes de los riesgos, resulta preocupante que un 46,6% considere necesario asumir riesgos para disfrutar de Internet y el 42,9% los asuma de forma consciente.

Como se mencionaba anteriormente, el usuario puede estar siendo víctima de una sensación de seguridad aparente que le engatusa y deriva en una relajación de hábitos prudentes dejando expuestos su equipo, contenido, datos, etc. en la Red de Redes.

[19] https://nordvpn.com/blog/national-privacy-test-do-internet-users-recognize-phishing-emails/

[20] https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/

Alcance del estudio

Alcance del estudio

Alcance del estudio

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

Los datos extraídos de la encuesta, realizada con una periodicidad semestral, 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: 3.695 hogares encuestados y equipos/dispositivos Android escaneados (software instalado en 1.489 PCs y 1.924 smartphones y 282 tablets Android).

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 julio y diciembre de 2017 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 95,0%, se establecen que al tamaño muestral n=3.695 le corresponde una estimación del error muestral igual a ±1,61%.

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

Dirección: Alberto Urueña López
Equipo técnico:
Raquel Castro García-Muñoz
Santiago Cadenas Villaverde
Jose Antonio Seco Arnegas

Agradecer la colaboración en la realización de este estudio a:

Asimismo se quiere también agradecer la colaboración de:

ISSN 2386-3684
DOI: 10.30923/2386-3684-27

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