Estudio sobre la Ciberseguridad y confianza en los hogares españoles

Oleada Julio – Diciembre 2018

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

ontsi observatorio nacional de las telecomunicaciones y de la SI

red.es

Abril 2019

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 3.824 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 2018**.

Presentación

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:

- **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).
- **1S18**, estudio realizado en el primer semestre de 2018 (enero - junio).
- **2S18**, estudio realizado en el segundo semestre de 2018 (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

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

[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.

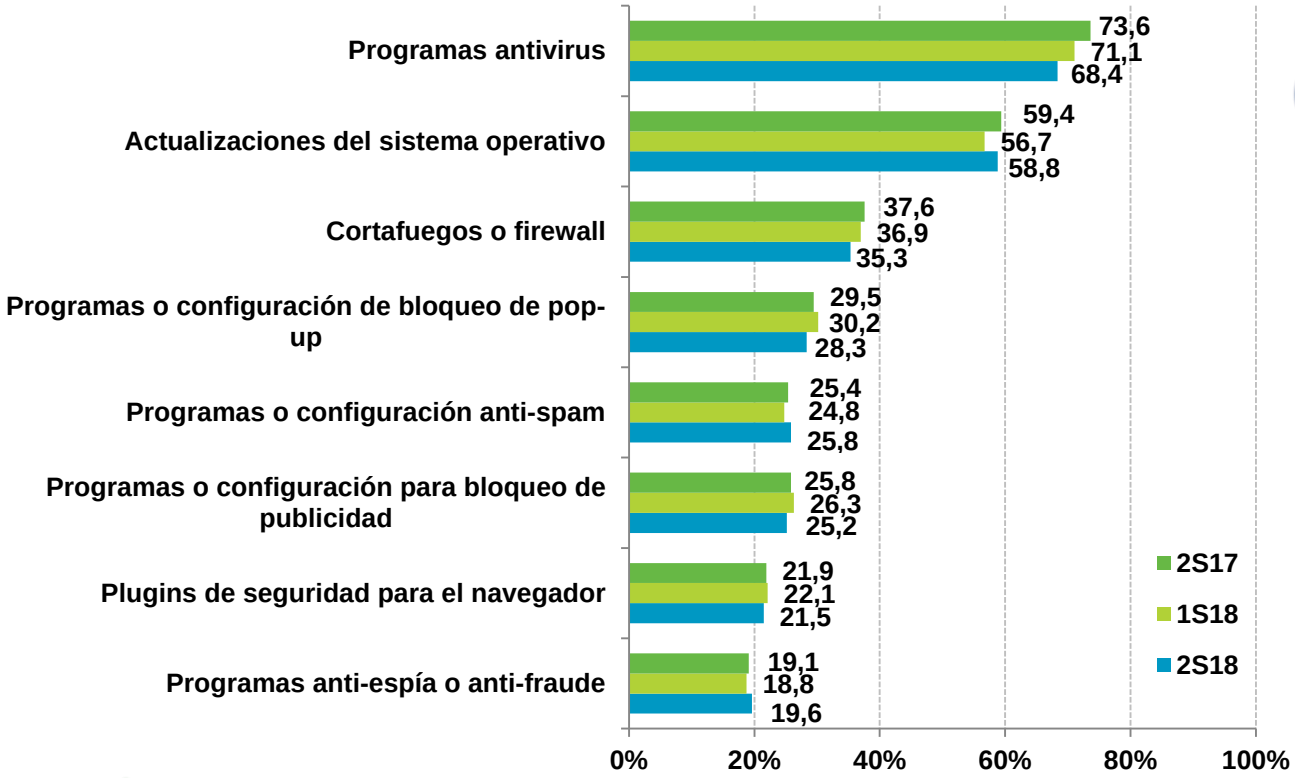
Definición y clasificación de las medidas de seguridad

	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

Uso de medidas de seguridad en el ordenador del hogar

Medidas de seguridad automatizables

El uso de **programas antivirus** mantiene una tendencia a la baja (**-2,7 p.p.**) mientras que las **actualizaciones del SO** se recuperan (**+2,1 p.p.**) de la bajada sufrida el semestre anterior.



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

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

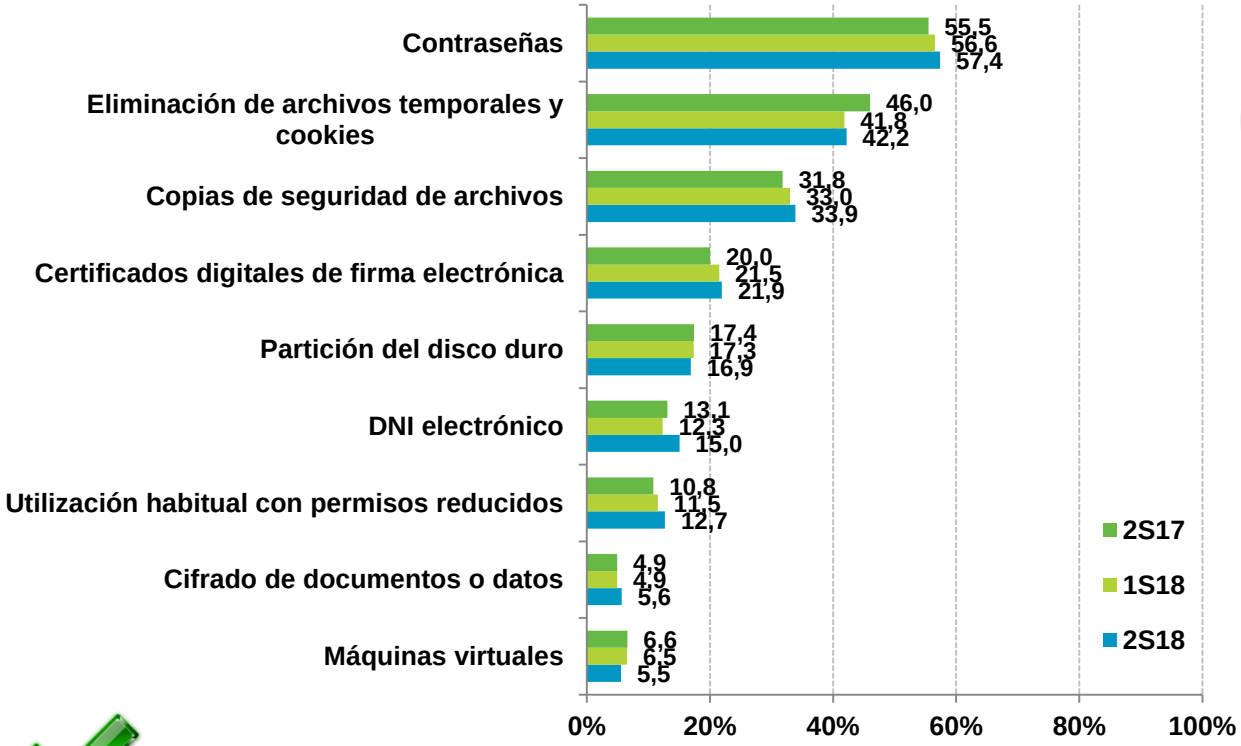
BASE: Usuarios de PC

¿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

Las medidas de seguridad activas tienden a continuar creciendo, salvo el uso de **máquinas virtuales** y de **particiones del disco duro**.



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.

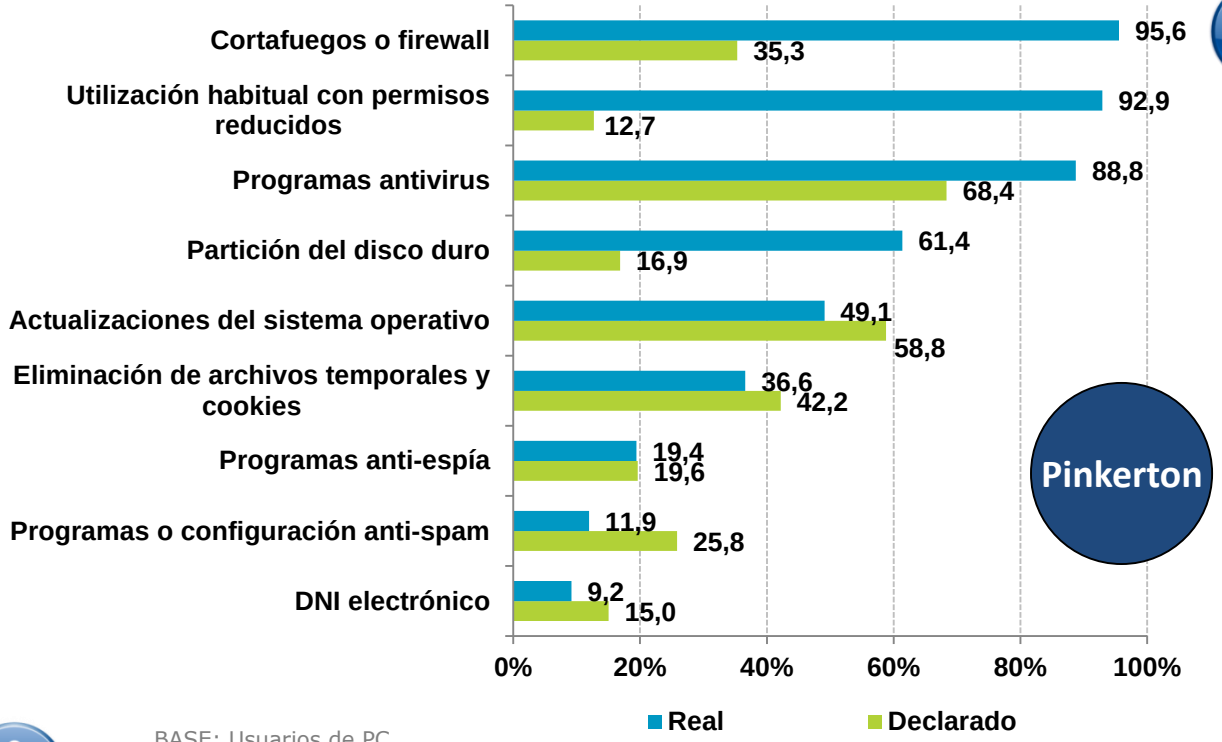
BASE: Usuarios de PC

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 declarado vs. real

Las grandes diferencias entre datos declarados y reales mostrados en la **utilización habitual de permisos reducidos (80,2 p.p.), cortafuegos o firewall (60,3 p.p.), partición del disco duro (44,5 p.p.)** sugieren que el usuario medio no es consciente de su uso.



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

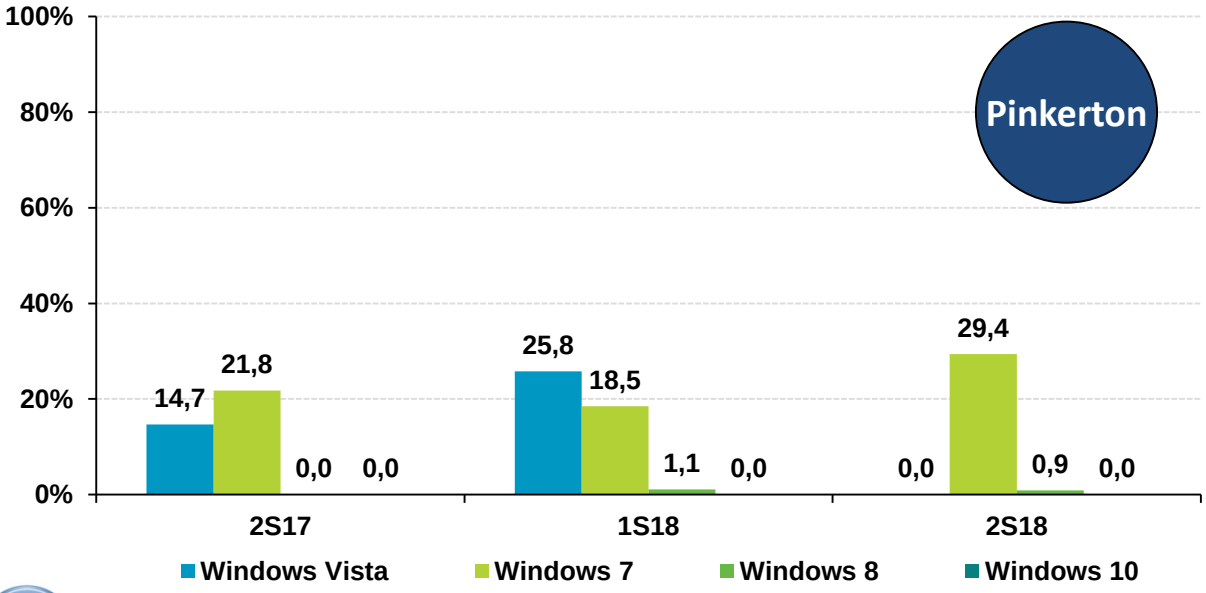
Para la obtención del dato real se utiliza el software **Pinkerton** desarrollado por Hispasec Sistemas, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 50 motores antivirus. **Pinkerton** se instala en los equipos y los analiza, detectando el malware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

2

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



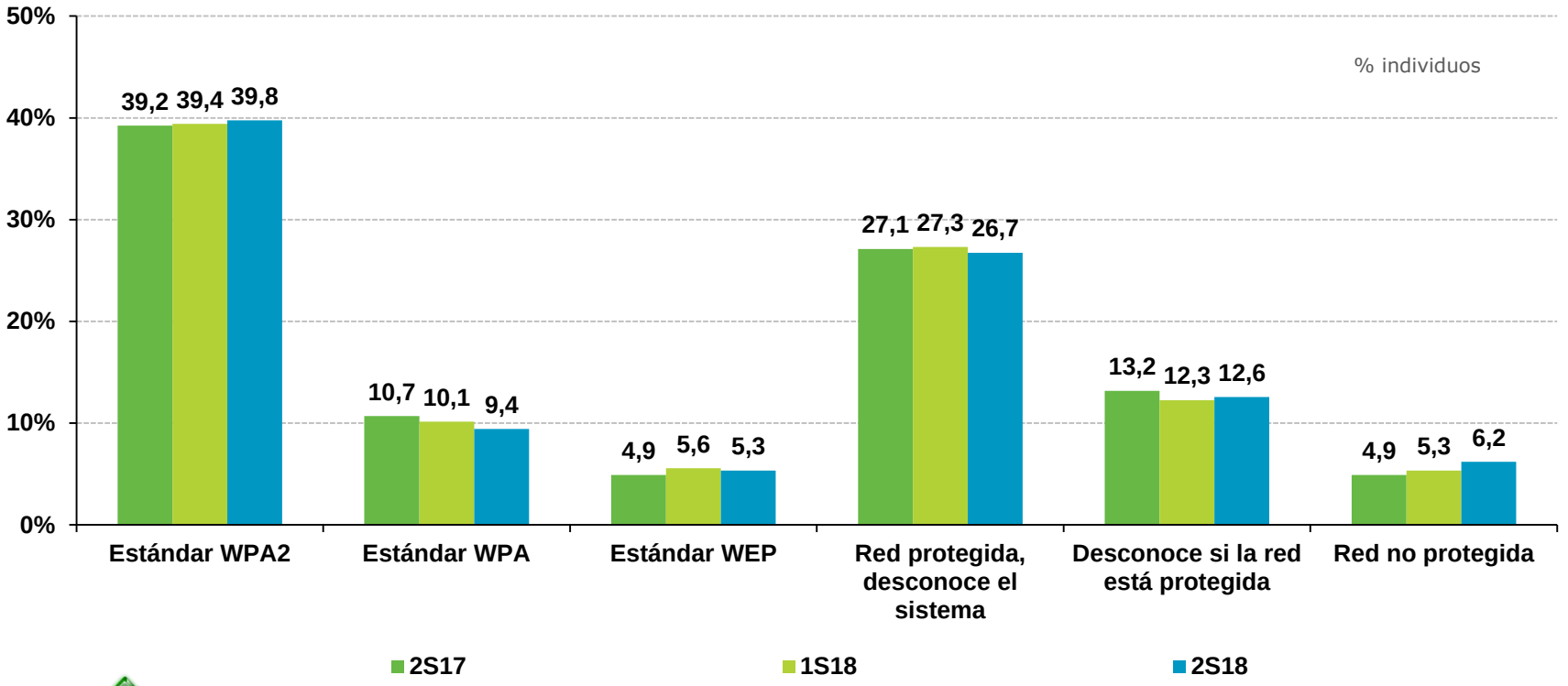
La diferencia entre el nivel de privilegios usado en las distintas versiones de Windows se debe a la configuración por defecto aplicada a la cuenta de usuario.

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.

Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi

Se sigue manteniendo la cuota de uso de los **estándares WPA/WPA2** en el hogar por parte de casi la mitad de los usuarios (9,4 + 39,8). También se observa un ligero incremento en el porcentaje de **redes no protegidas** (+0,9 p. p.)



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

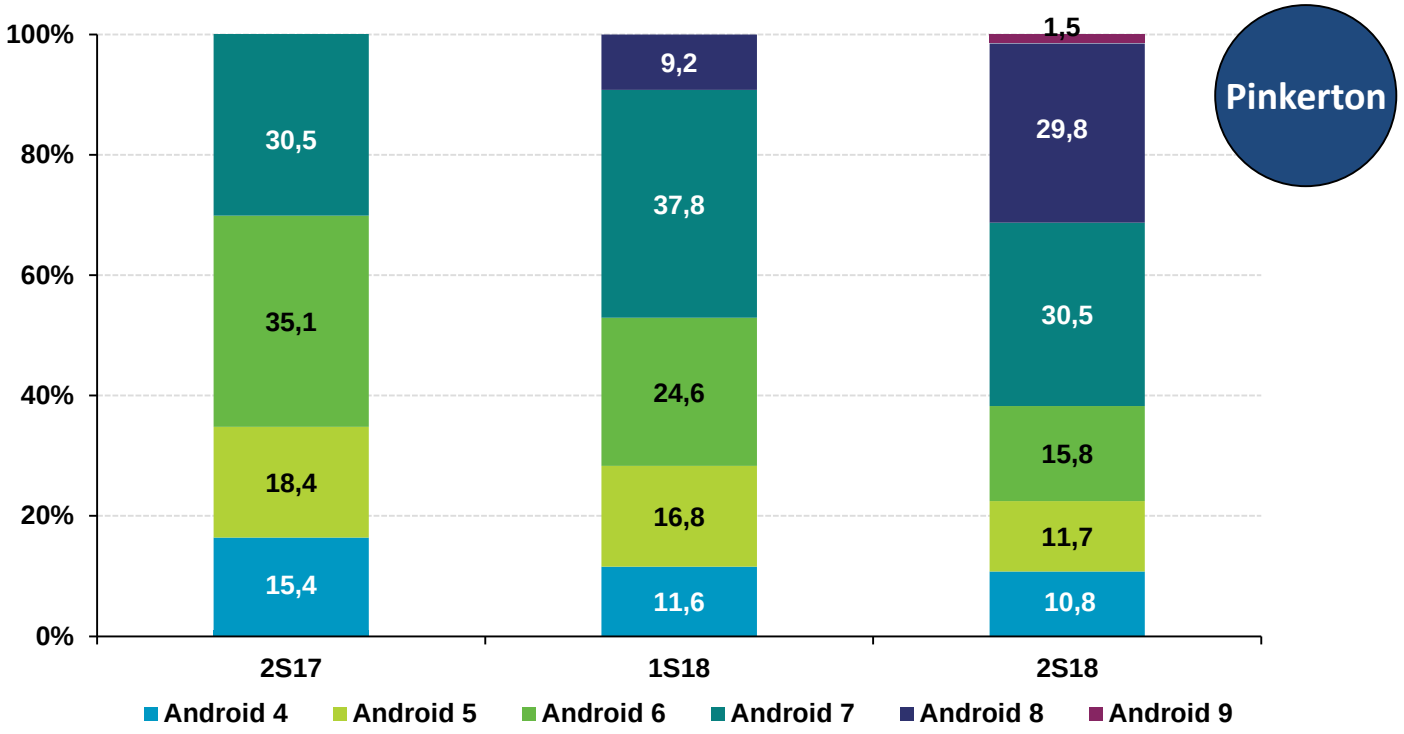
BASE: Usuarios Wi-Fi con conexión propia

Uso de medidas de seguridad en dispositivos Android

Versión del sistema operativo en dispositivos Android

El uso de la versión Android 8 se incrementa hasta casi el 30% de la cuota de mercado, prácticamente igualando a Android 7. Las versiones anteriores continúan bajando en uso.

% individuos

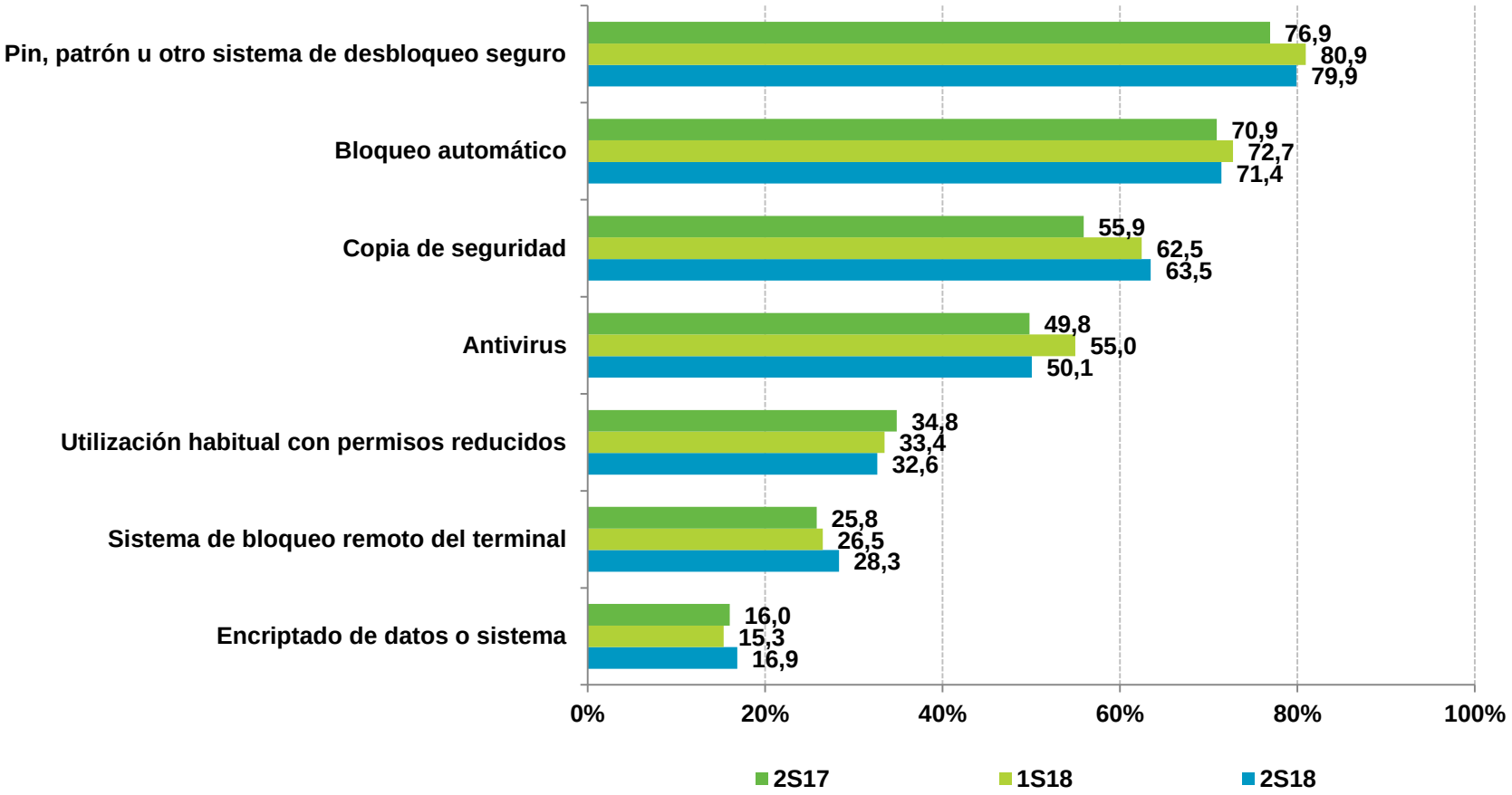


BASE: Usuarios que disponen de dispositivo Android

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 del **sistema de bloqueo remoto** (**+1,8 p.p.**), el **encriptado de datos o sistema** (**+1,6 p.p.**) y **copias de seguridad** (**+1 p.p.**) muestran un ligero ascenso, aunque el uso de **sistemas de desbloqueo seguro** (**79,9%**) y **bloqueo automático** (**71,4%**) continúan siendo las medidas mayoritarias con diferencia según los usuarios.

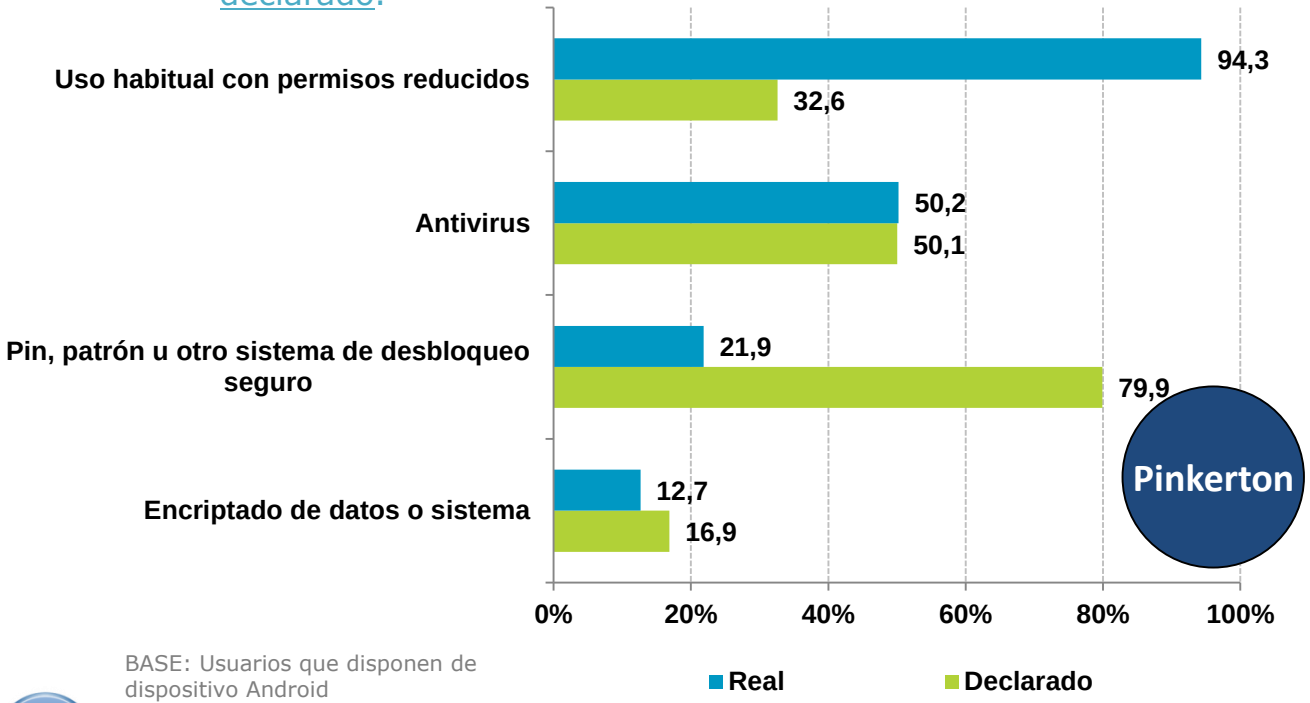


BASE: Usuarios que disponen de dispositivo Android

Uso de medidas de seguridad declarado vs. real

El uso real de **software antivirus** mantiene su cuota del **50%**, coincidiendo con los datos recogidos en las encuestas.

Sin embargo, el uso real de **sistemas seguros de desbloqueo (PIN, patrón, etc.)** desciende hasta el **21,9%** resultando en una diferencia de **-58 p. p.** con respecto al valor declarado.



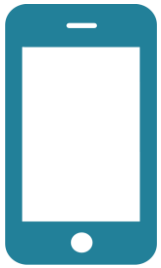
BASE: Usuarios que disponen de dispositivo Android

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.

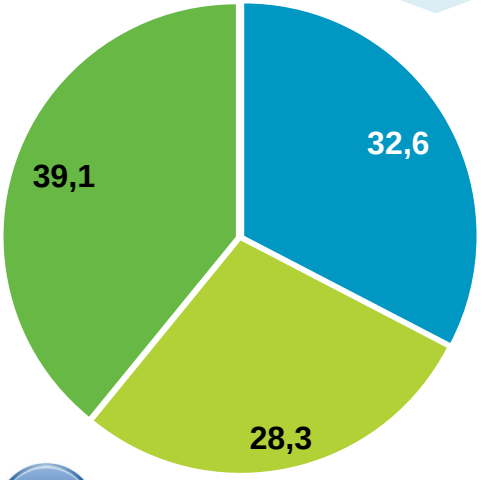
Uso de medidas de seguridad en dispositivos Android

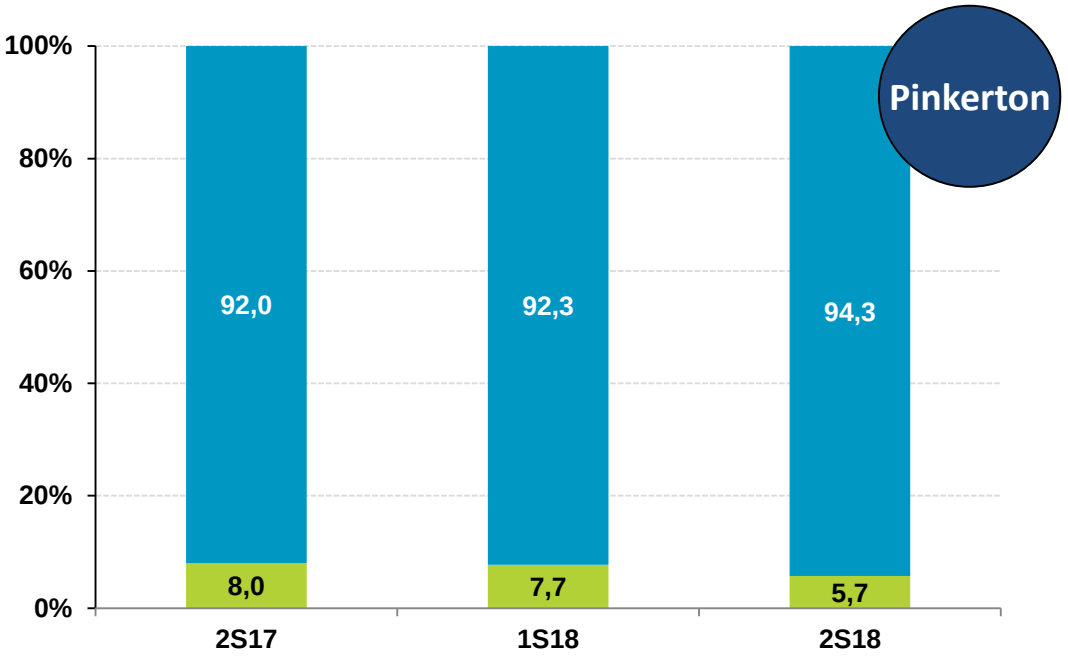
Permisos de Administrador



Dato real

Dato declarado (2S18)





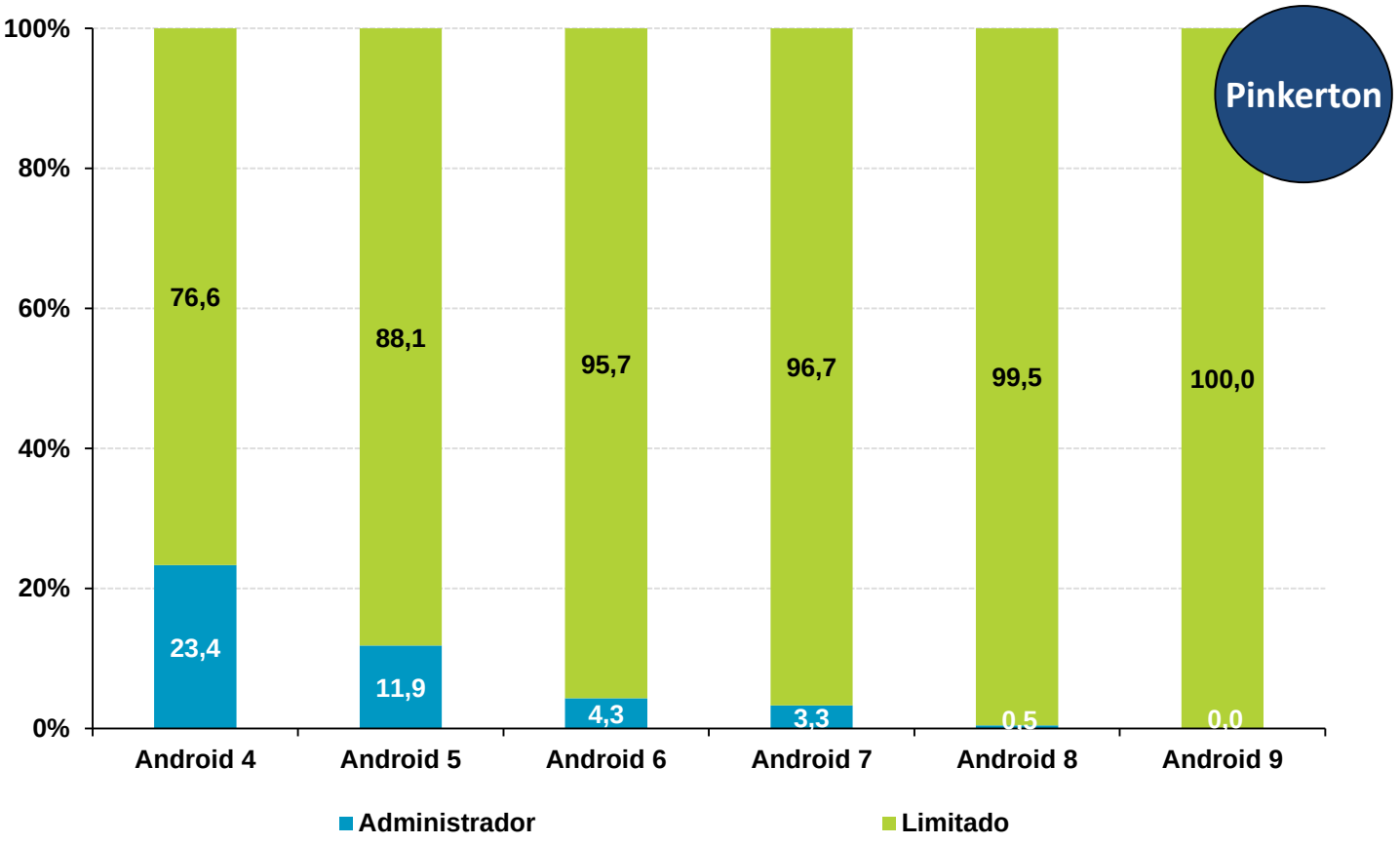
Pinkerton obtiene la información acerca de los privilegios de administrador del dispositivo Android mediante métodos indirectos.

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

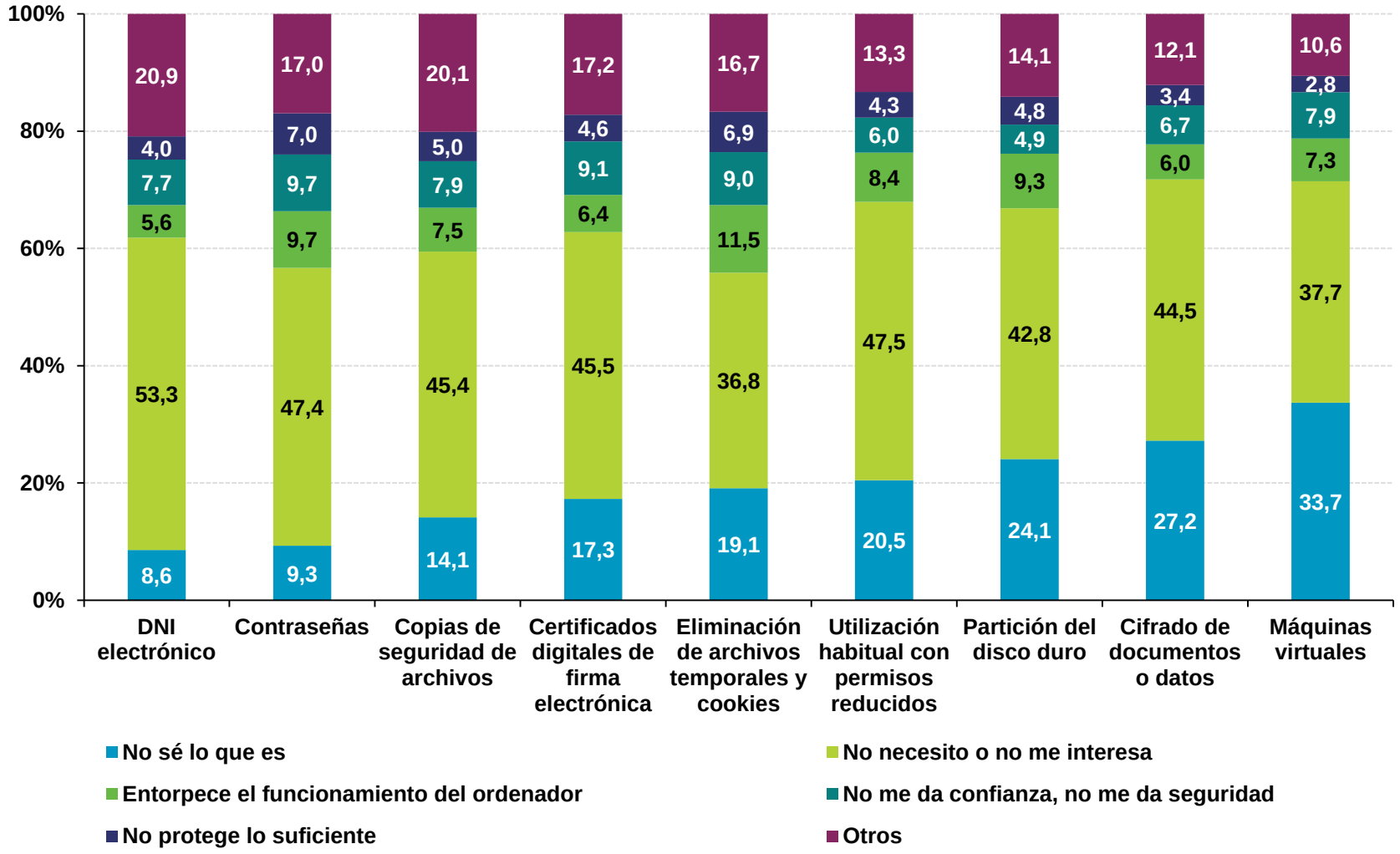
Se mantiene la tendencia de que los dispositivos estén *'rooteados'* en las versiones más antiguas de Android.



BASE: Usuarios que disponen de dispositivo Android

Motivos de no utilización de medidas de seguridad

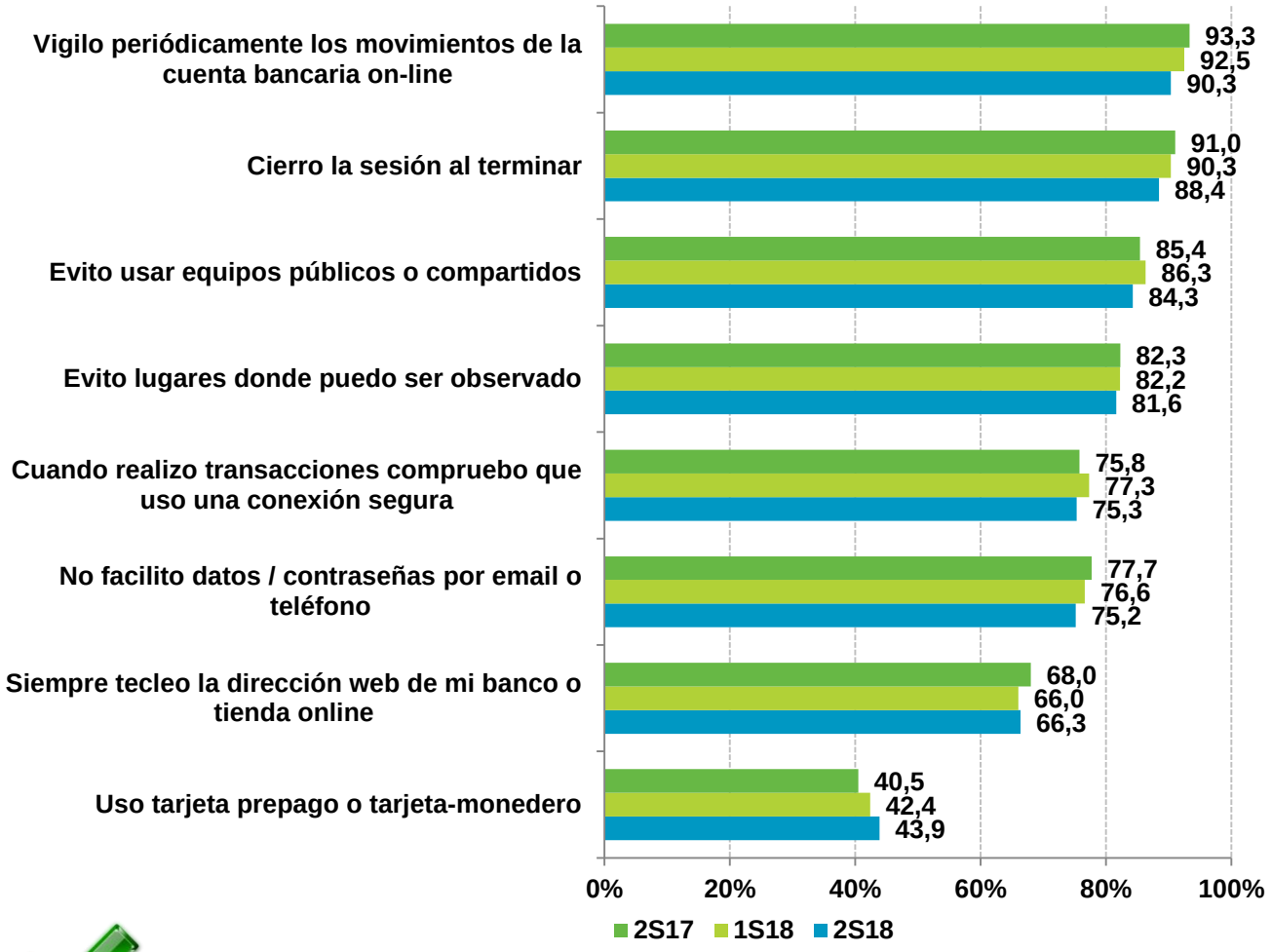
El principal motivo alegado para no utilizar medidas de seguridad no automatizables es principalmente la **falta de necesidad o interés** y el **desconocimiento de la medida**.



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

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



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.

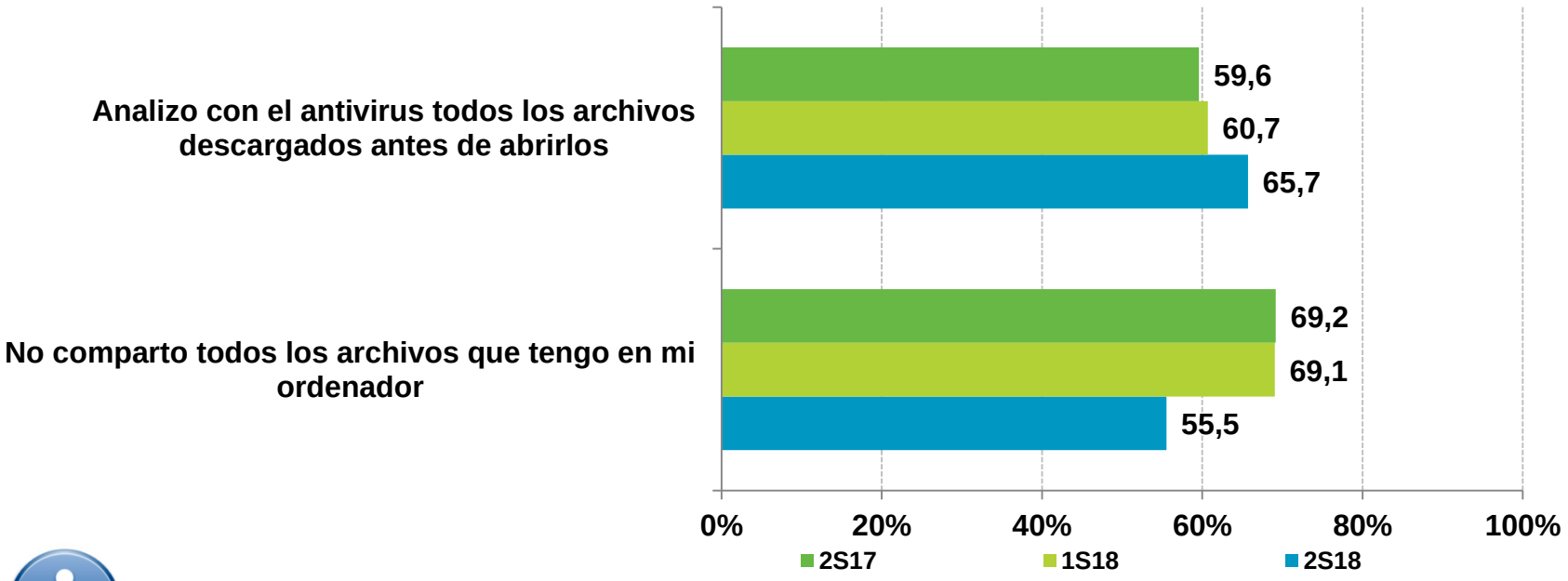
BASE: Usuarios que utilizan banca online y/o comercio electrónico

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

Redes P2P

Se presenta una disminución significativa a la hora de establecer un directorio de **archivos compartidos a través de las redes P2P** (**-13,6 p.p.**), mientras que el uso de **antivirus para analizar todos los ficheros descargados antes de abrirlos** ha aumentado en **5 p.p.**.

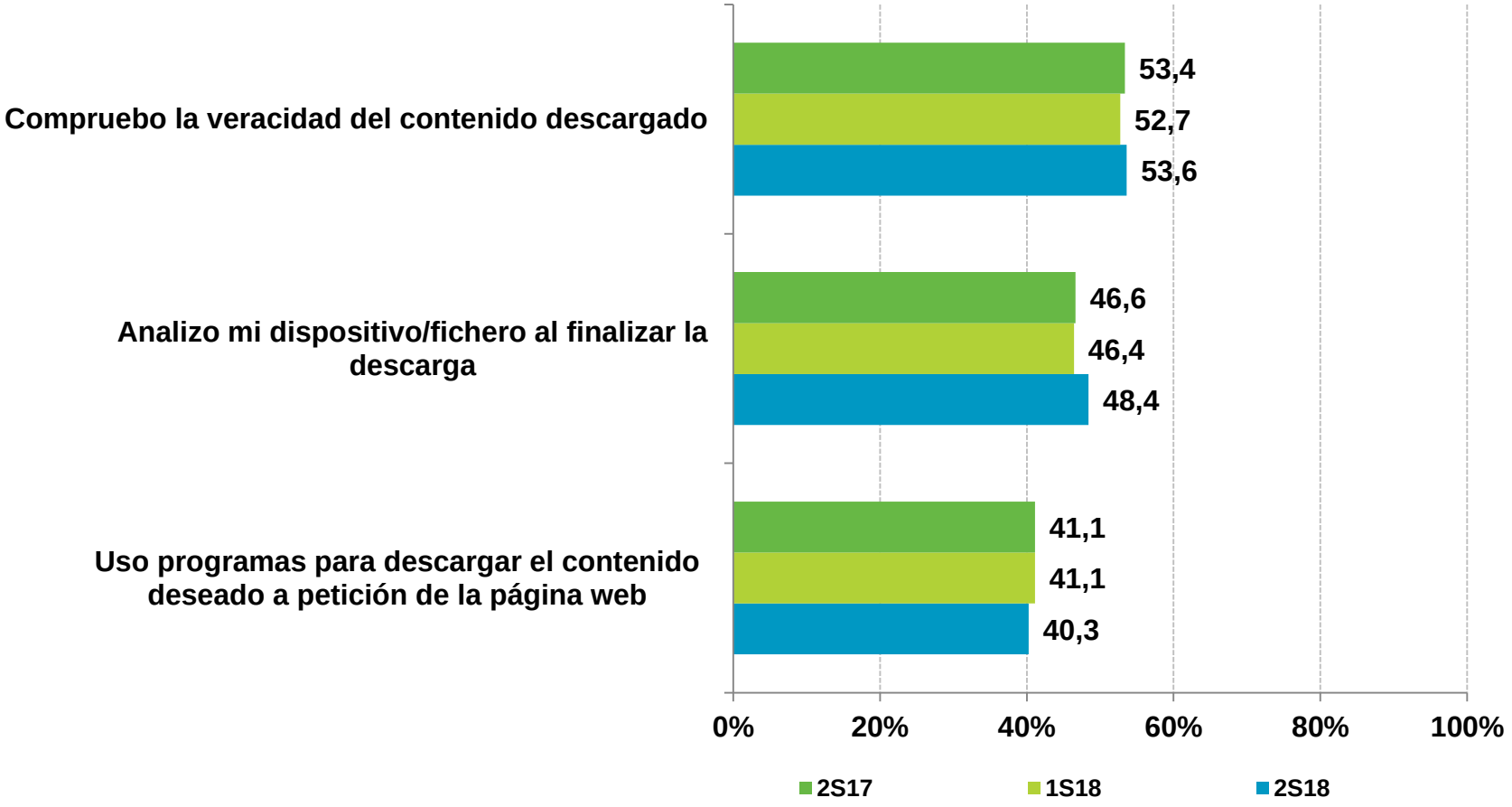


Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de malware. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como por ejemplo novedades de software, cinematográficas, musicales, etc.) logran el objetivo de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

BASE: Usuarios de redes P2P

Descarga directa

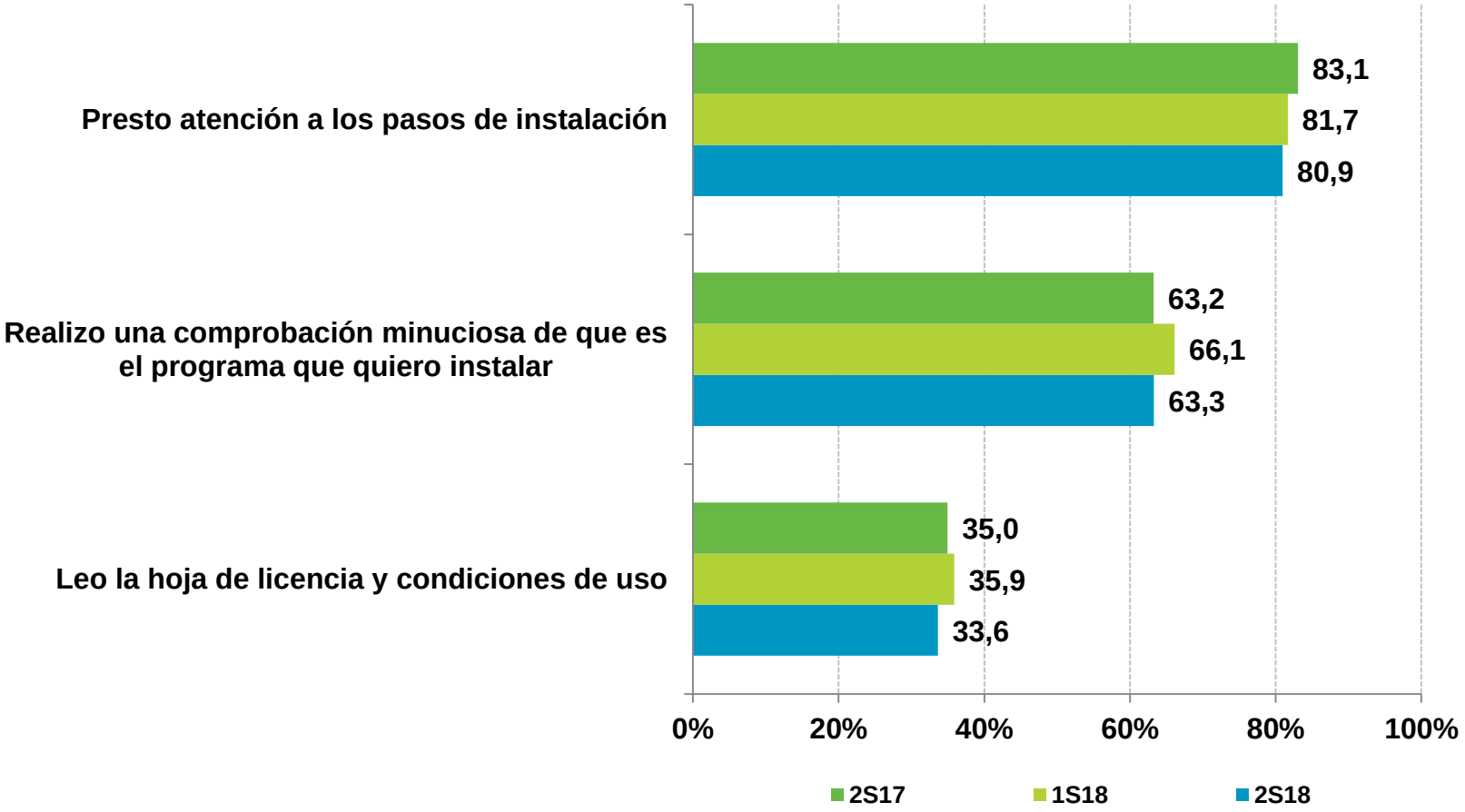
Los hábitos referentes a la **descarga directa** de ficheros parecen mantenerse en consonancia con respecto a los estudios de semestres anteriores, con un aumento de **2 p.p.** en el **análisis de los ficheros descargados**.



BASE: Total usuarios

Instalación de software descargado

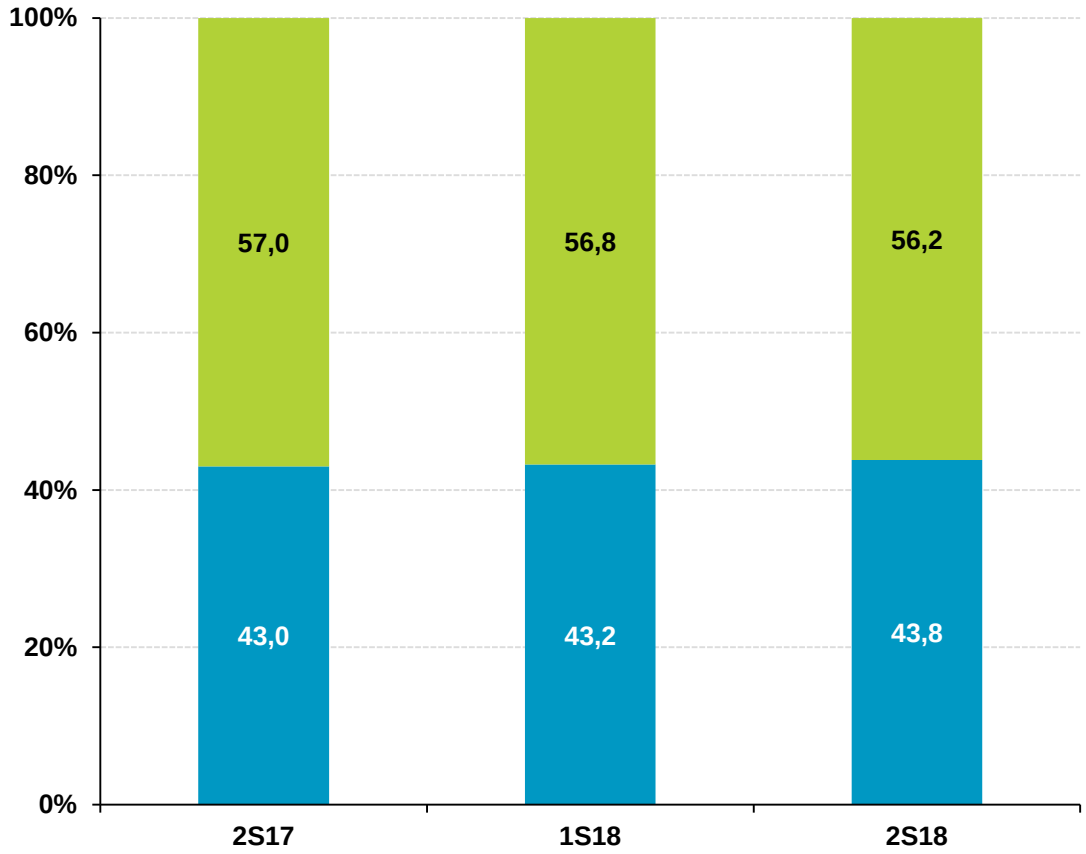
Se mantienen la tendencia de que aproximadamente ocho de cada diez usuarios (**80,9%**) **presta atención a los pasos de instalación** del software descargado desde Internet y seis de cada diez (**63,3%**) **comprueba que se trata del programa que se desea instalar**.



BASE: Usuarios de PC

Alta en servicios en Internet

Más de la mitad (**56,2%**) de los internautas españoles continúa afirmando **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.).

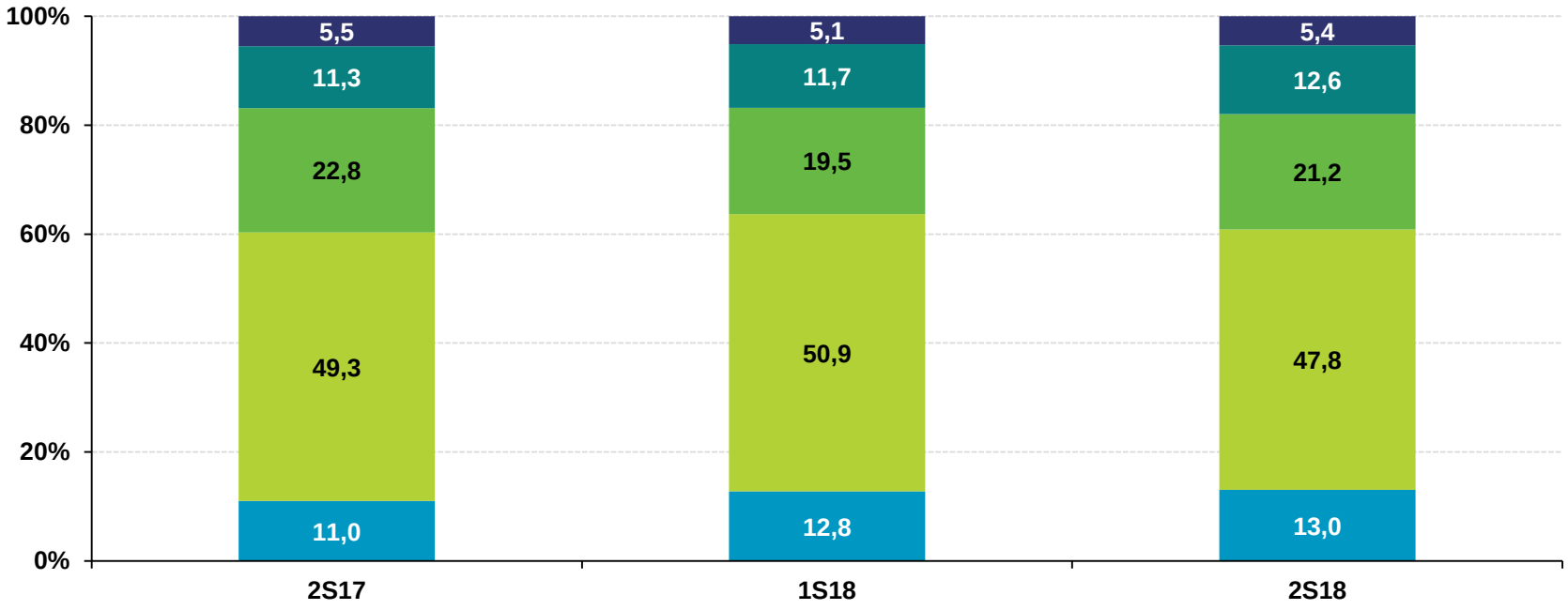


Lectura y aceptación de la información legal al registrarse o darse de alta en proveedores de servicio en Internet (redes sociales, comercio electrónico, etc.)

BASE: Total usuarios

Redes sociales

El **33,8%** (21,2 + 12,6) de los usuarios de redes sociales consultados **expone los datos** publicados en su perfil a **terceras personas y/o desconocidos**. Adicionalmente, el **5,4%** declara **desconocer** el nivel de privacidad de su perfil en redes sociales.



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

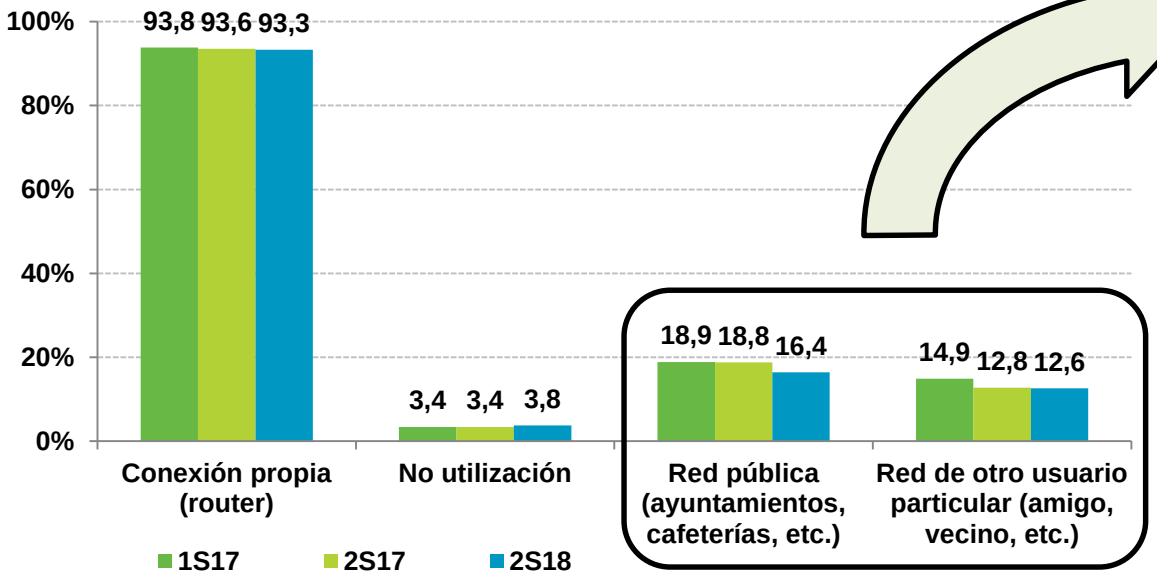
BASE: Usuarios que utilizan redes sociales

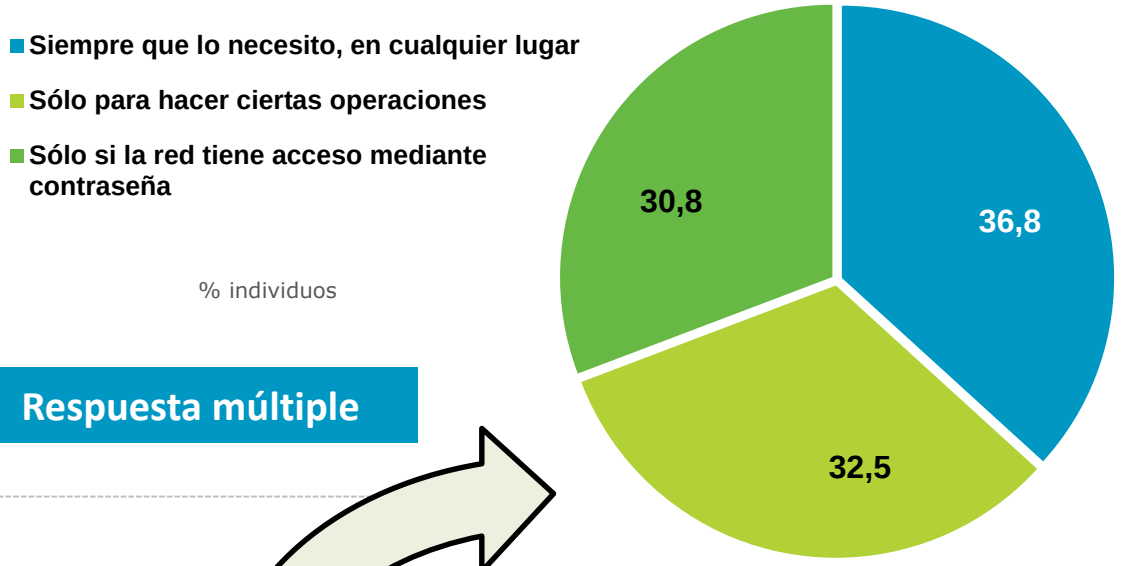
% individuos

Hábitos de uso de las redes inalámbricas Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Respuesta múltiple





% individuos

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

Aún con una ligera disminución, **un 29%** de los internautas continúan conectándose redes inalámbricas Wi-Fi públicas (**16,4%**) o de particulares (**12,6%**) cuando lo necesitan y en cualquier lugar (**36,8%**).

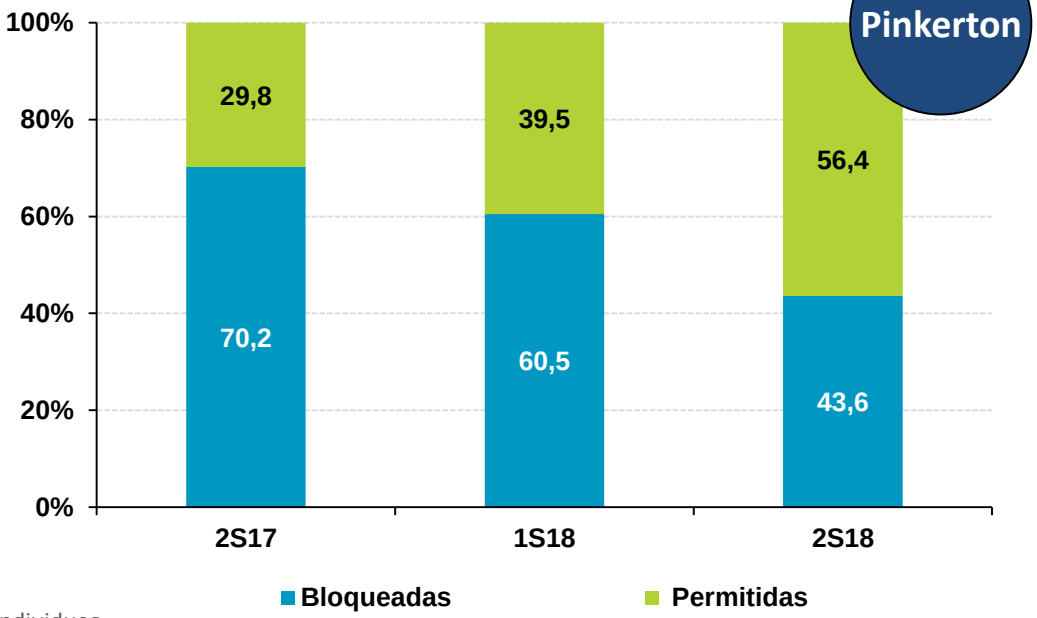
BASE: Total usuarios

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

Hábitos de uso en dispositivos Android

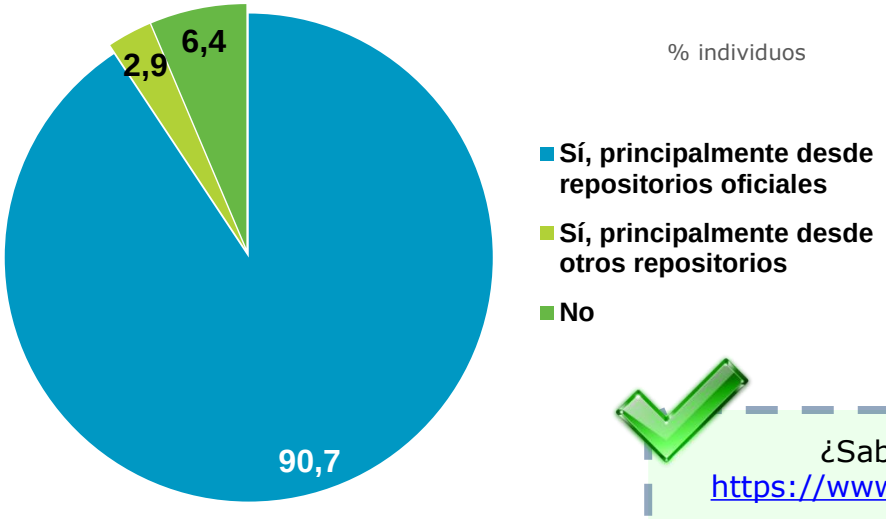
El uso de aplicaciones provenientes de fuentes dudosas puede suponer **problemas de seguridad** y la instalación en el dispositivo móvil de cualquier tipo de **malware**.

Descargas de fuentes desconocidas



% individuos

Descargas de programas o aplicaciones en el móvil



La tendencia de **la activación de uso de repositorios no oficiales** ha aumentado significativamente durante el último semestre (**+16.9%**) según muestran los datos recogidos con Pinkerton. Aun así, más del **90%** de los usuarios declaran **instalar aplicaciones principalmente desde repositorios oficiales**.

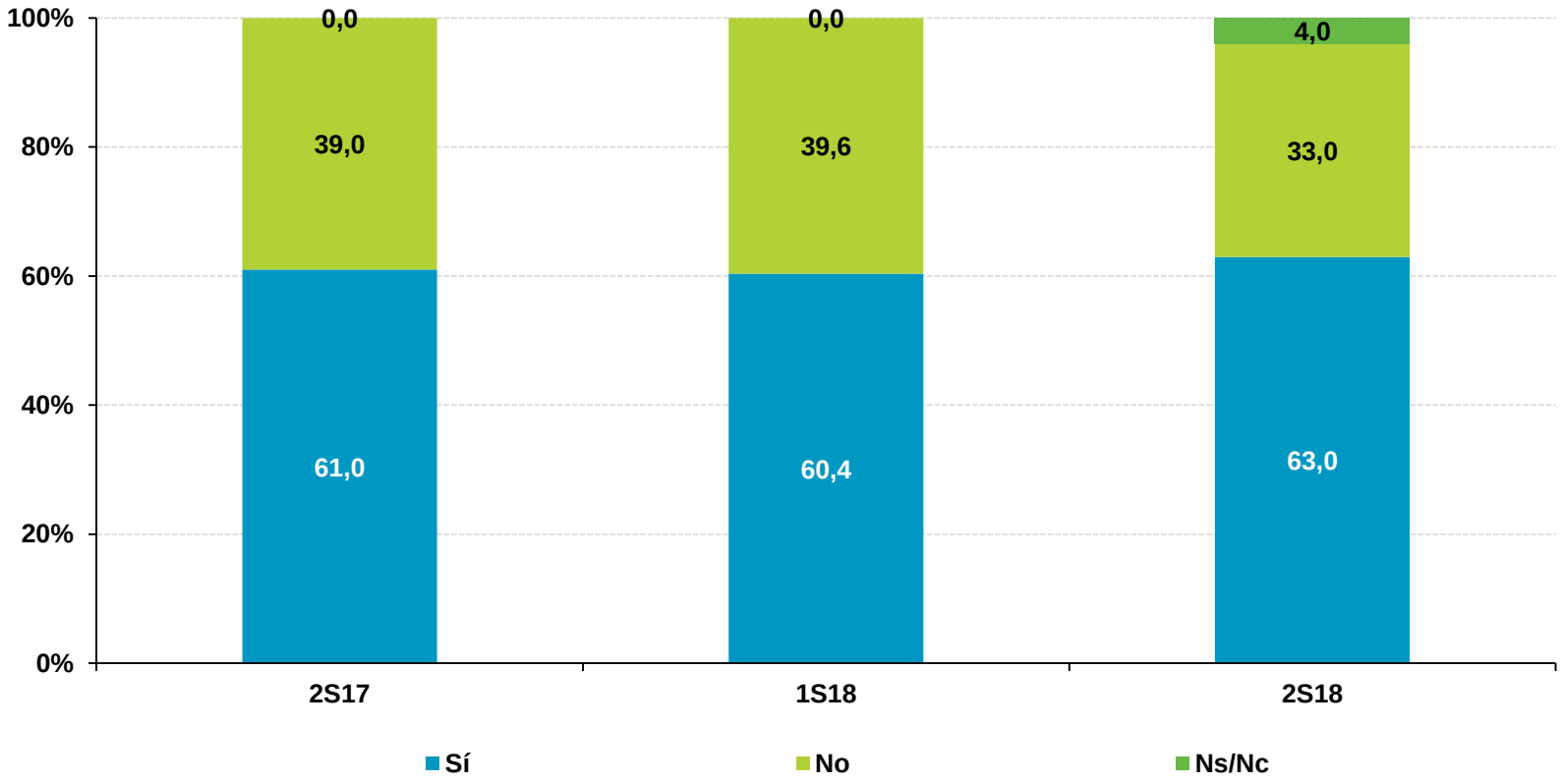
¿Sabes que esta APP puede robar tu información?
https://www.osi.es/es/actualidad/blog/2017/07/05/esta-app-te-puede-robar-toda-tu-informacion

BASE: Usuarios que disponen de dispositivo Android

Hábitos de uso en dispositivos Android

Comprobación de permisos al instalar una aplicación

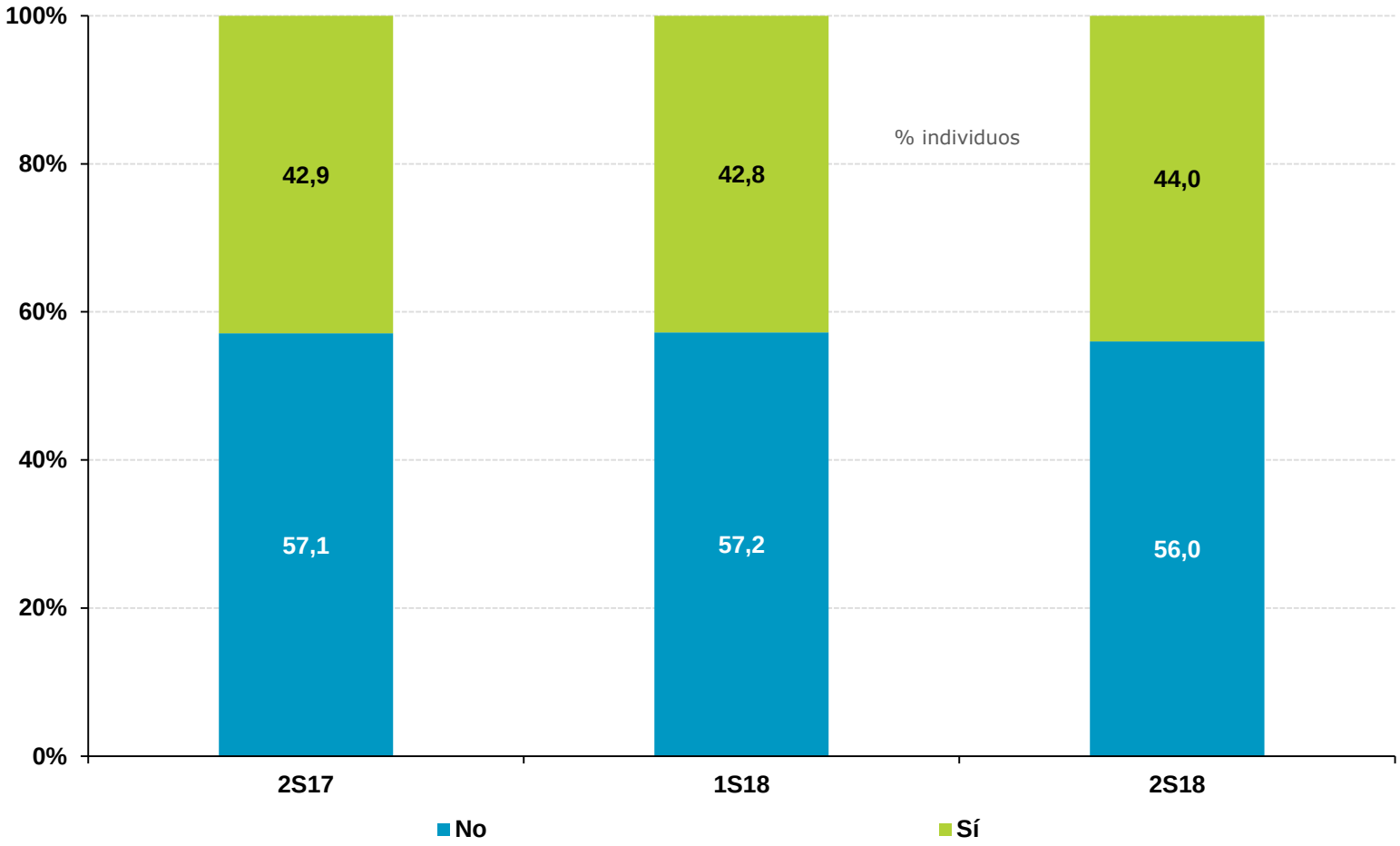
% individuos



BASE: Usuarios que disponen de dispositivos Android y descargan aplicaciones

Adopción consciente de conductas de riesgo

La **adopción consciente de conductas de riesgo** por parte del usuario presenta un ligero aumento respecto al estudio anterior (**+1,2 p.p.**).



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

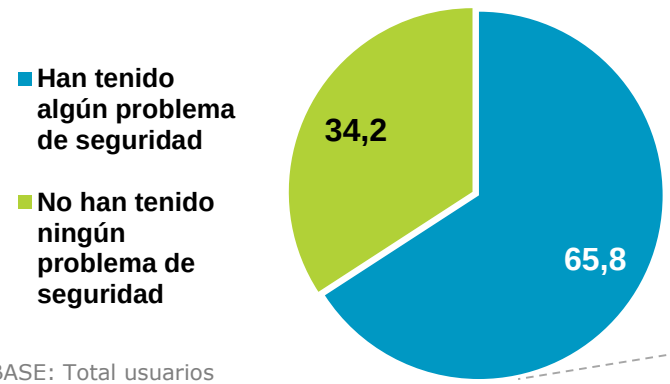
Mas información: https://www.incibe.es/glossary/empresas/diccionario/

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.

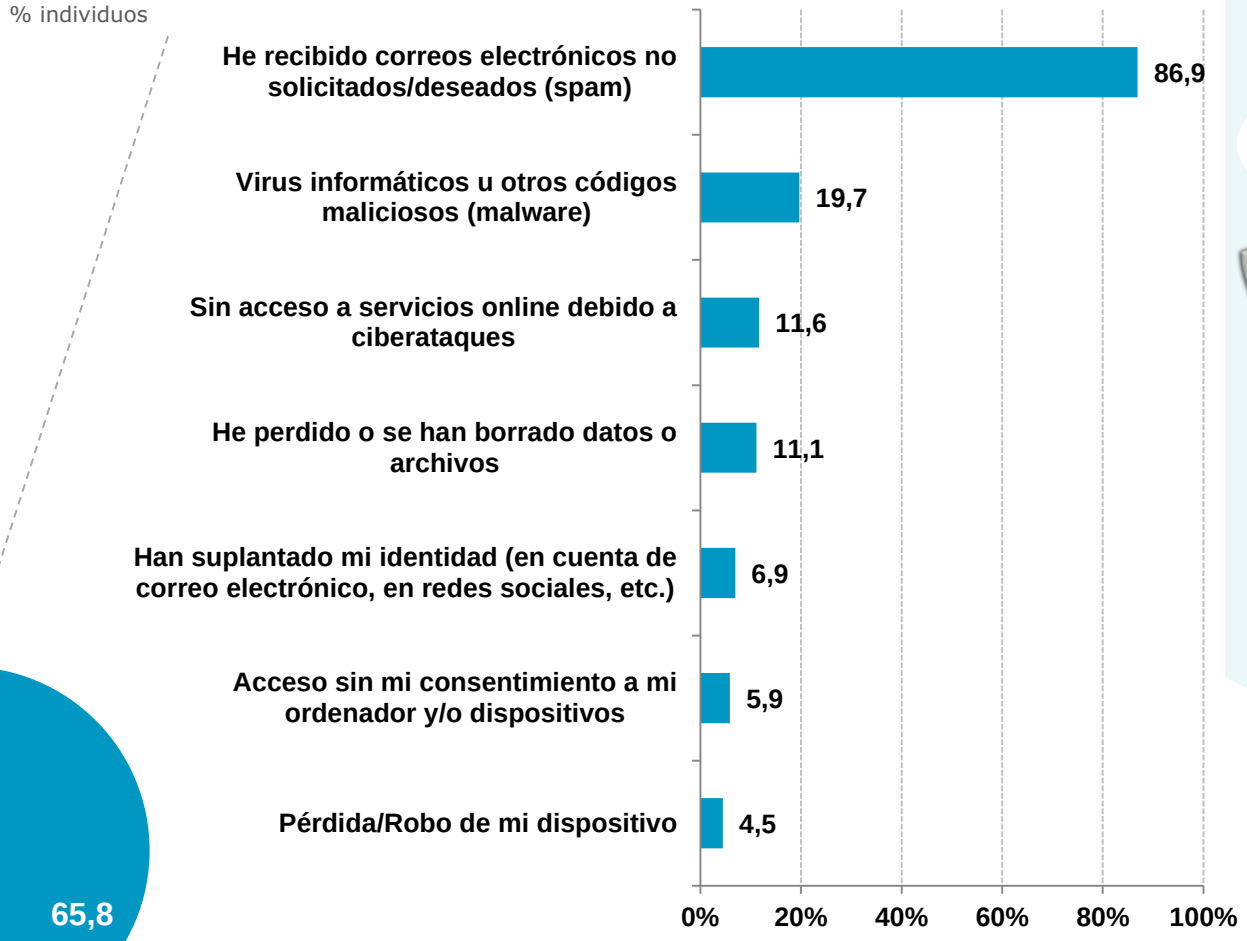
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras tipologías.

Afectados:



BASE: Total usuarios

Incidencias sufridas: **Respuesta múltiple**



BASE: Usuarios que han sufrido alguna incidencia de seguridad

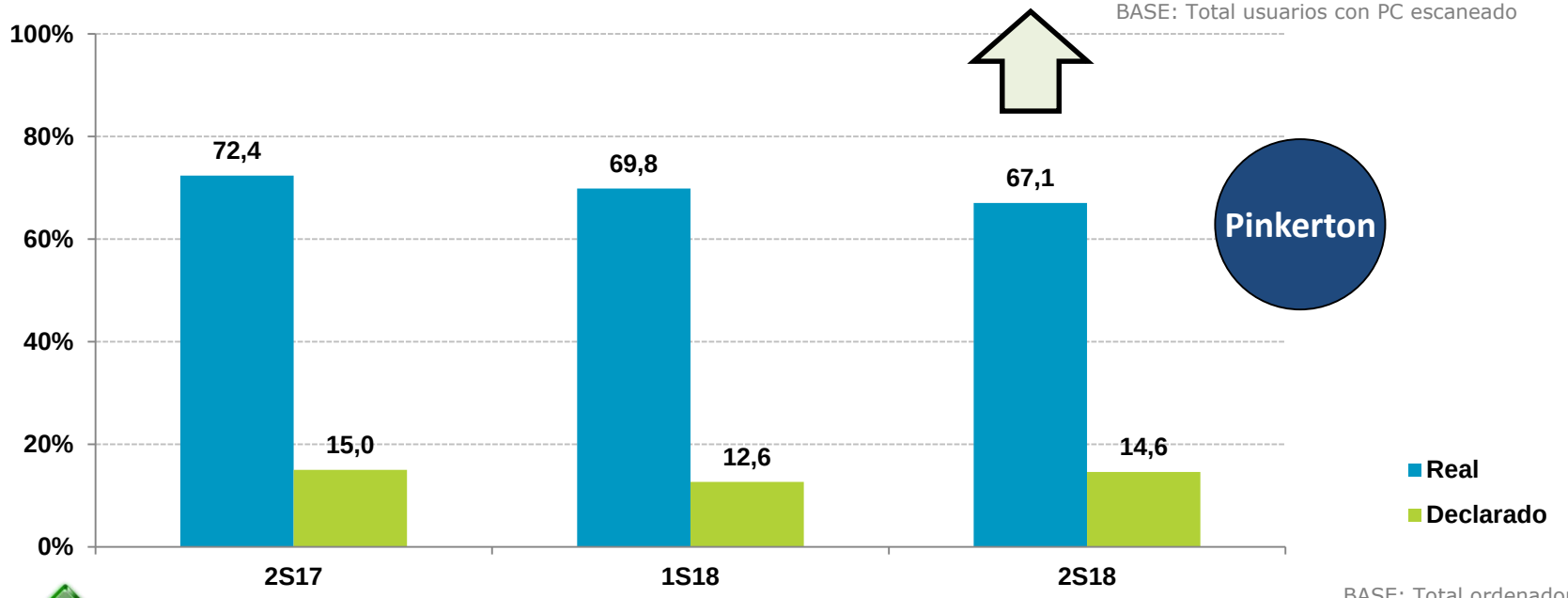
Incidentes por malware

Ordenador del hogar

El **59,2%** 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	7,9	5,6	13,5
No	59,2	27,4	86,5
Total	67,1	32,9	100

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

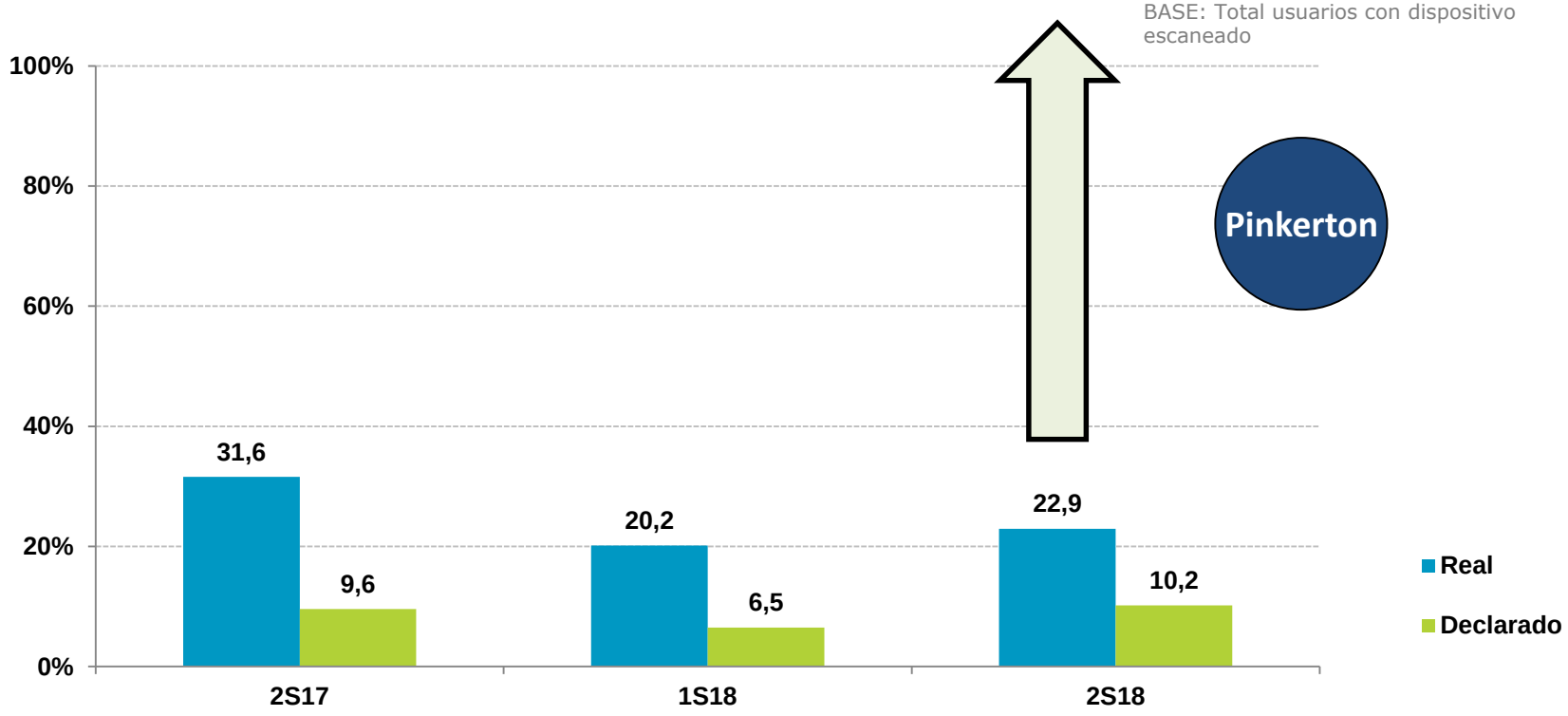
Incidentes por malware

Dispositivos Android

Los usuarios **no percibieron la presencia de malware** en el **21,4%** de los dispositivos Android en los que **Pinkerton encontró infecciones**.

Declararon tener malware en Android	Su Android presentaba malware		
	Sí	No	Total
Sí	1,5	7,9	9,4
No	21,4	69,2	90,6
Total	22,9	77,1	100

BASE: Total usuarios con dispositivo escaneado



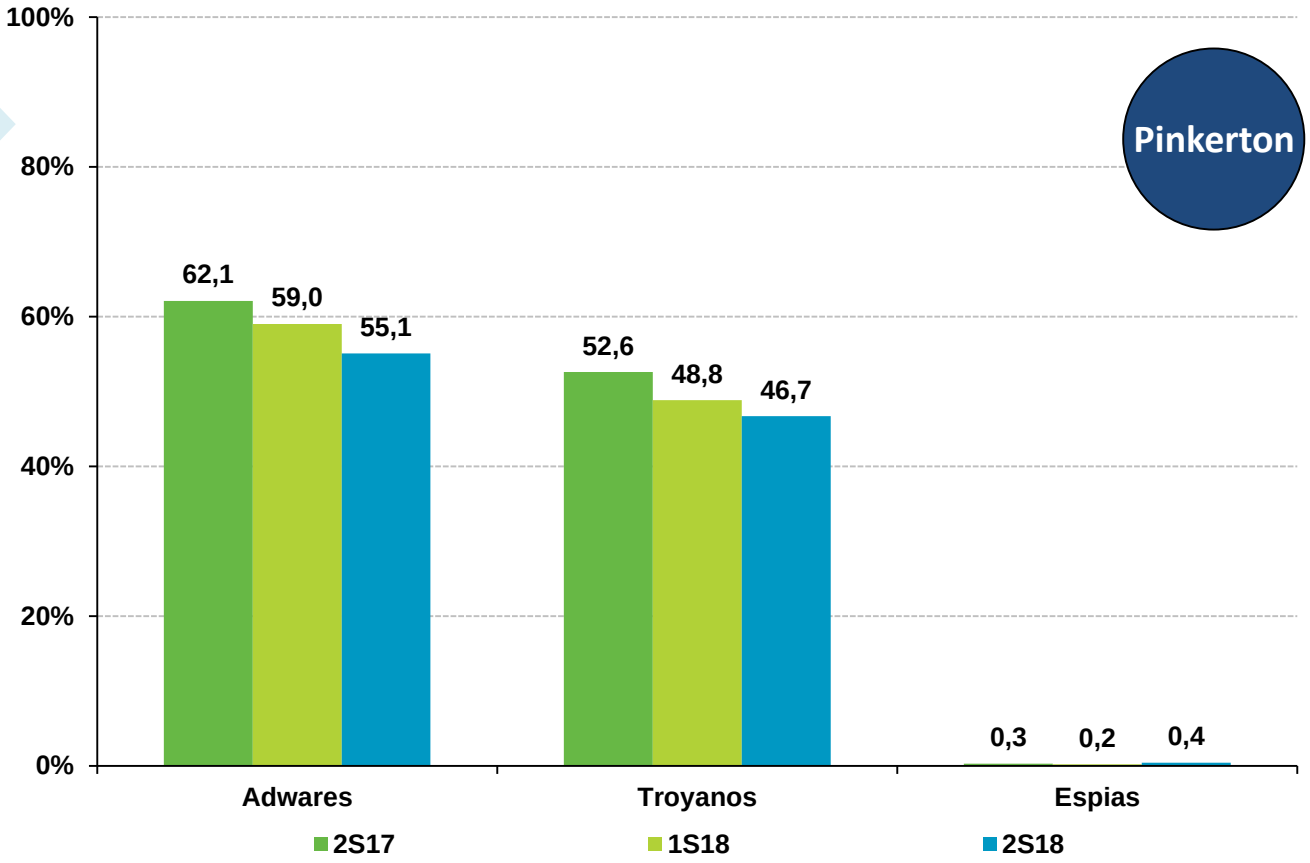
BASE: Total dispositivos Android

Tipología del malware detectado en PC

Ordenador del hogar

El **adware publicitario** y los **troyanos** reducen su presencia en los ordenadores españoles con respecto al semestre anterior: **-3,9 p.p.** y **-2,1 p.p.** respectivamente.

Equipos que alojan malware según tipología



Pinkerton

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

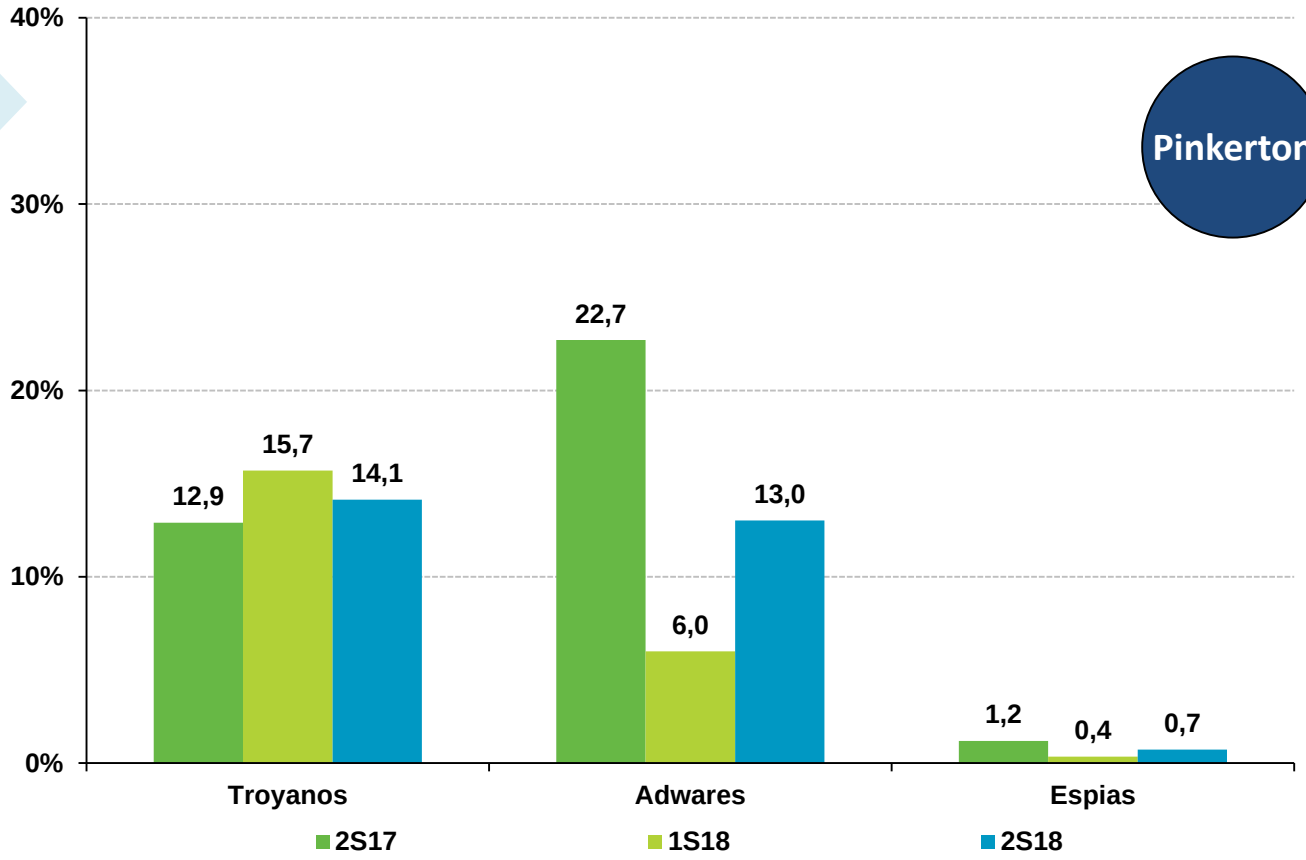
BASE: Total ordenadores

Tipología del malware detectado en android

Dispositivos Android

En los dispositivos Android, mientras que en el último semestre las infecciones de **troyanos** se reducen en **1,6 p.p.**, el **adware publicitario** experimenta un repunte de **7 p.p.**

Equipos que alojan malware según tipología



Pinkerton

4

BASE: Total dispositivos 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.

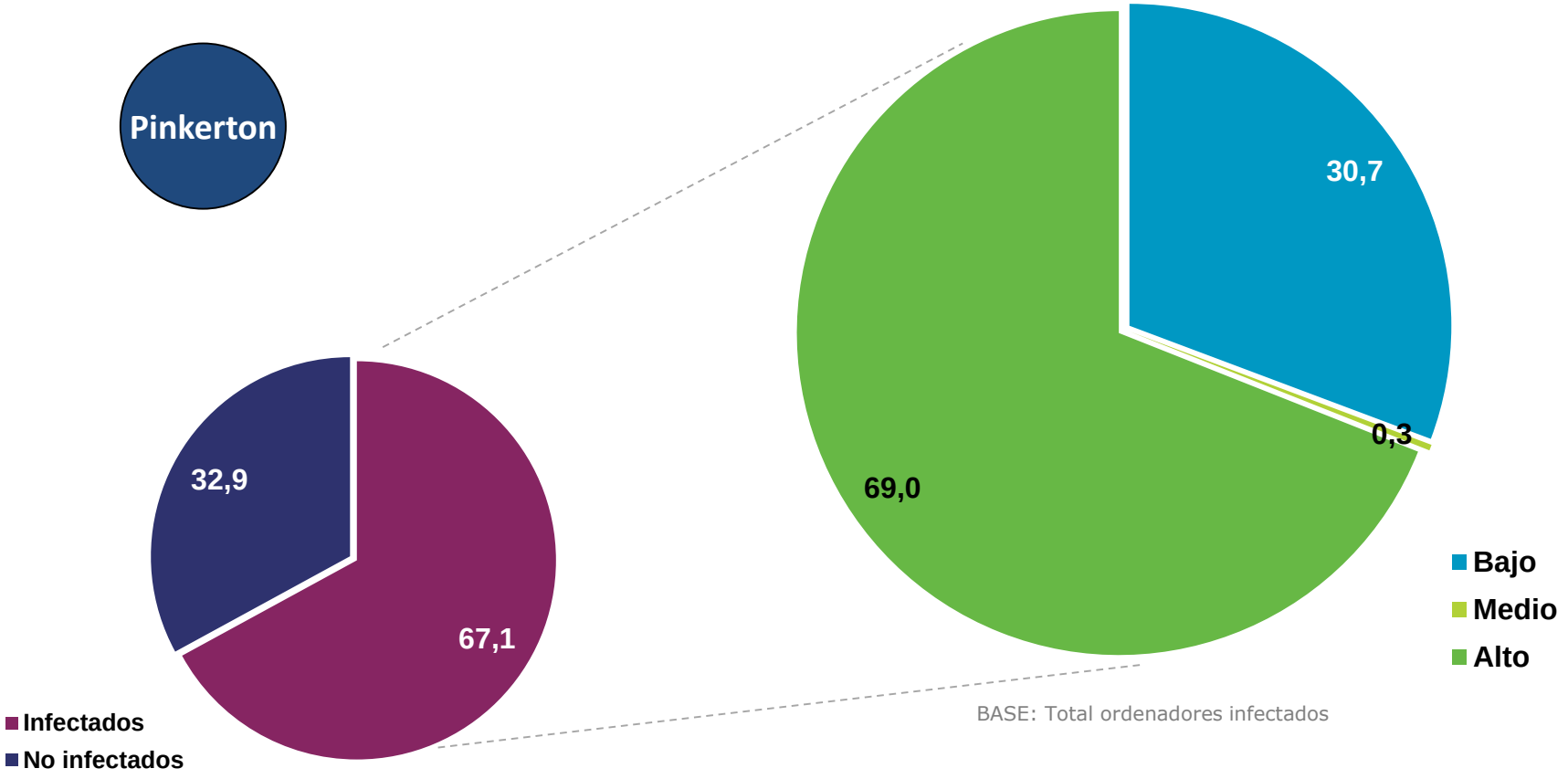
Peligrosidad media: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema: no perjudican de forma notoria su rendimiento; abren ventanas no deseadas al navegar; incrustan publicidad en páginas web legítimas que realmente no contienen publicidad; o facilitan la captura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

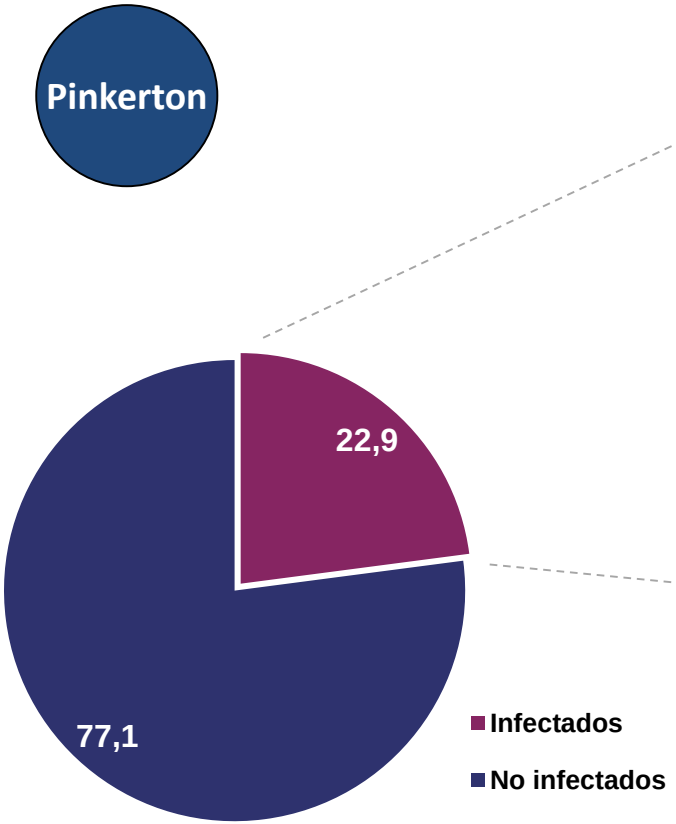
Ordenador del hogar

Dos tercios (**67,1%**) de los ordenadores de los hogares españoles analizados con Pinkerton se encuentran infectados con al menos una muestra de malware conocida. De estos, el **69%** presentan un nivel de **riesgo alto** debido al potencial peligro que suponen los archivos maliciosos encontrados en ellos.

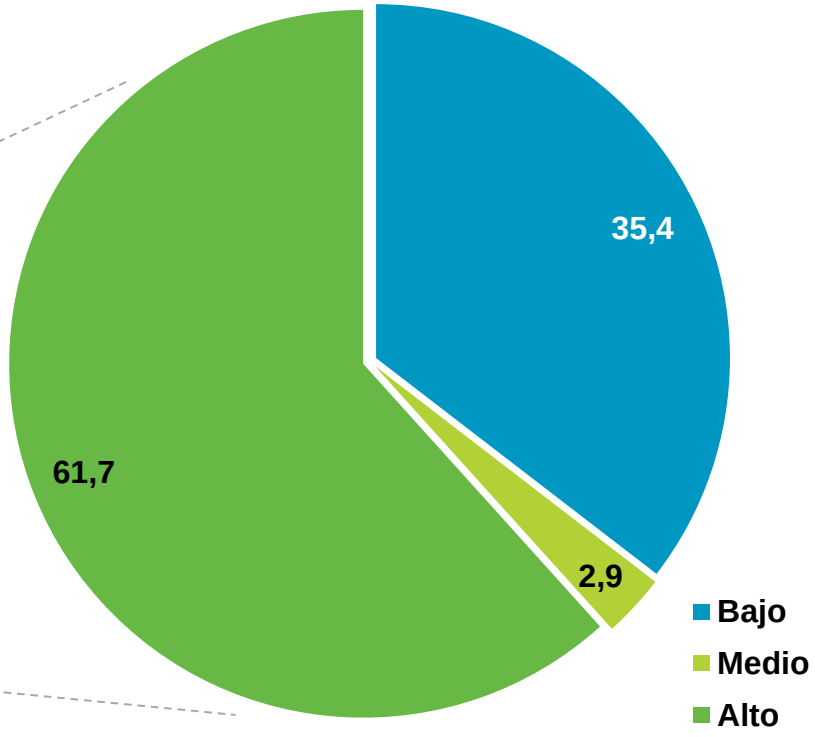


Dispositivos Android

El **22,9%** de los dispositivos Android analizados con Pinkerton se encuentran infectados con al menos una muestra de malware conocida, de los cuales la mayoría (un **61,7%)** presentan un nivel de **riesgo alto**.



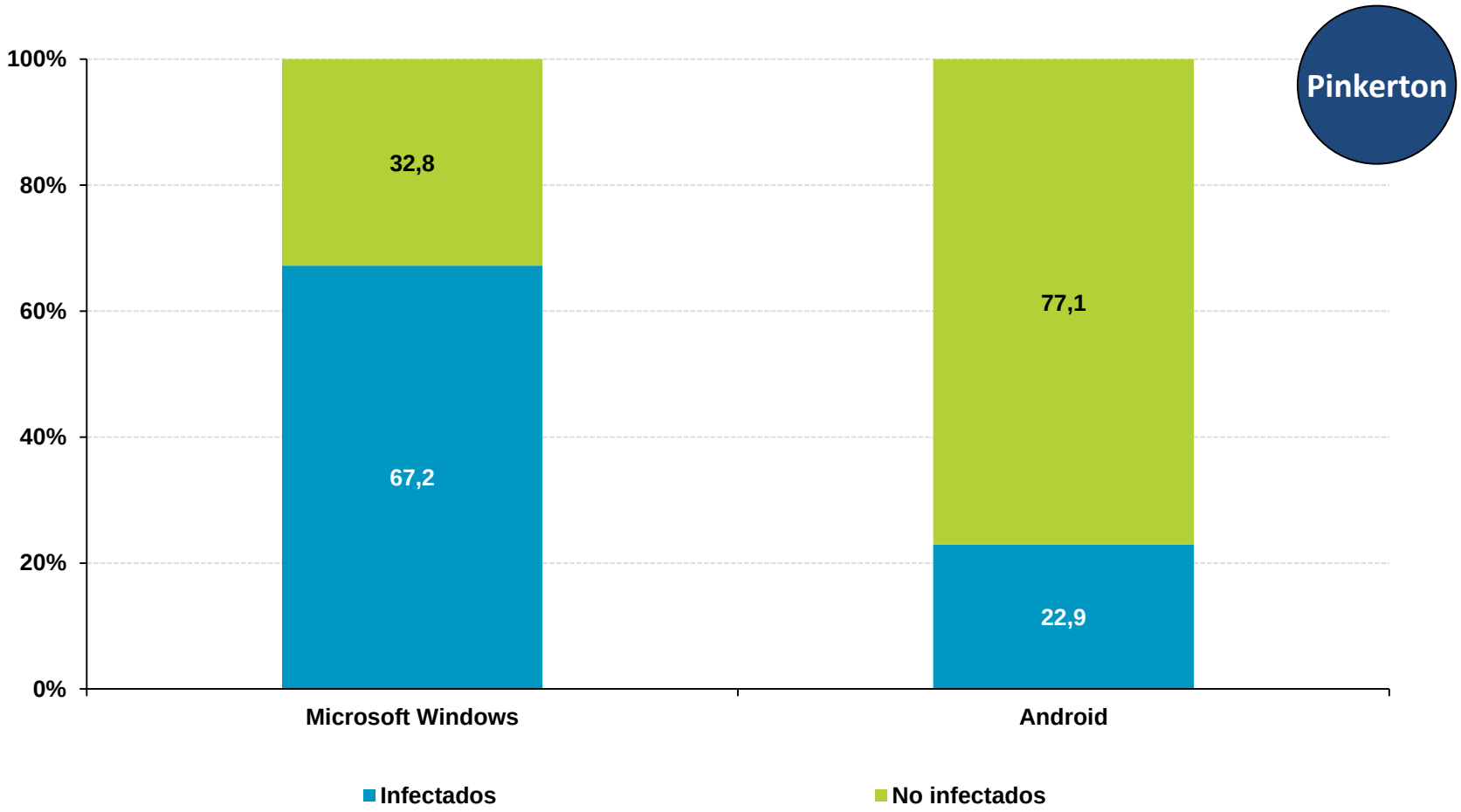
BASE: Total dispositivos Android



BASE: Total dispositivos Android infectados

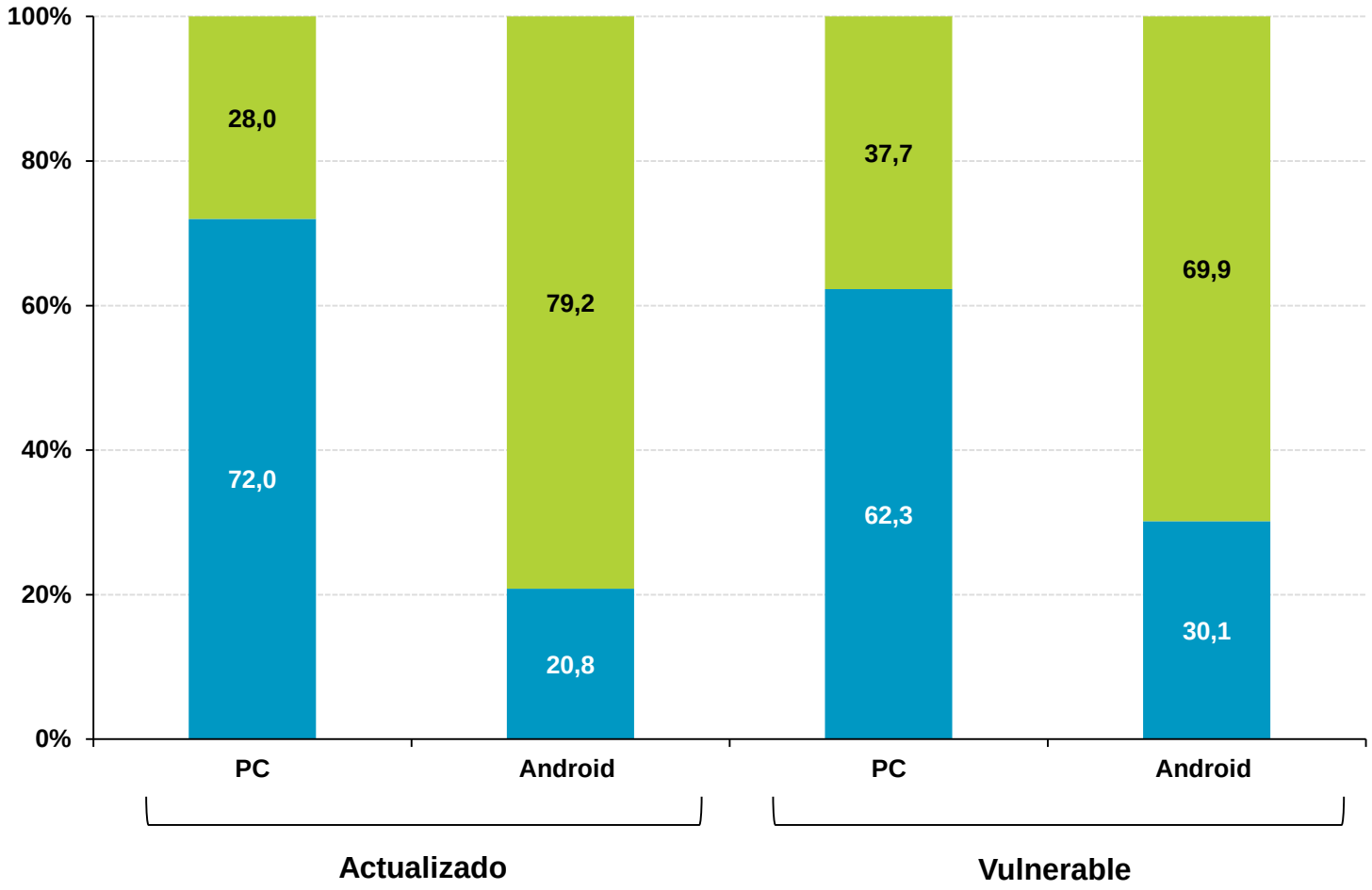
Malware vs. sistema operativo

Según el análisis de Pinkerton, el **67,2%** de los ordenadores del hogar con alguna versión del sistema operativo **Microsoft Windows** y el **22,9%** de los dispositivos **Android** contienen malware conocido.



BASE: Total equipos

Malware vs. actualización del sistema



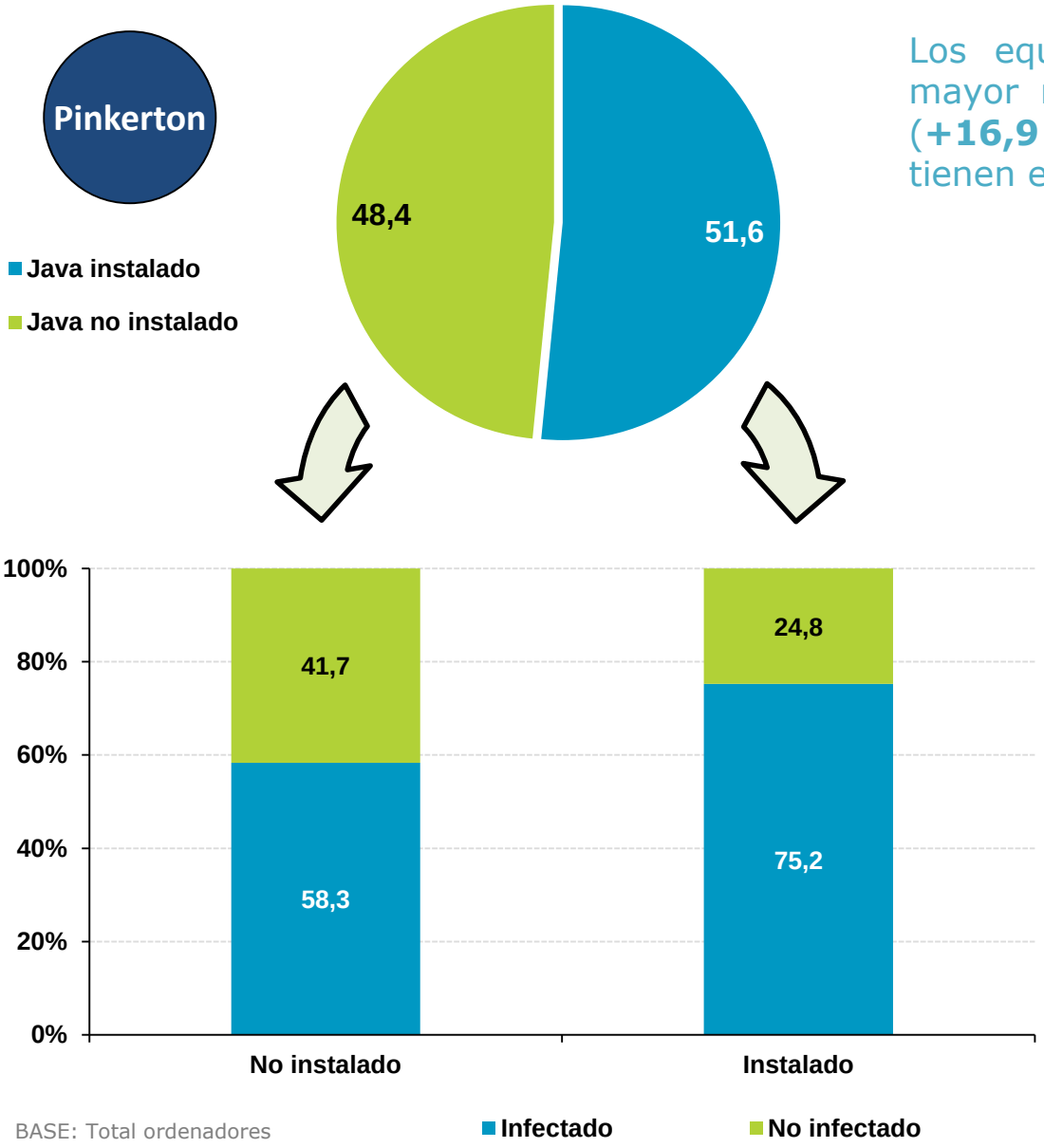
Pinkerton

4

Los dispositivos Android no actualizados son los más afectados por el malware (**+9,3 p.p.**). En el caso de los ordenadores, los desarrolladores de código malicioso se centran en las últimas versiones del sistema operativo Windows (**+9,7 p.p.**).

BASE: Total equipos

Malware vs. Java en PC



BASE: Total ordenadores

Los equipos con Java presentan un mayor nivel de infección de malware (**+16,9 p.p.**) que aquellos que no tienen este entorno instalado.

Alertas de seguridad de Java en julio y octubre de 2018:

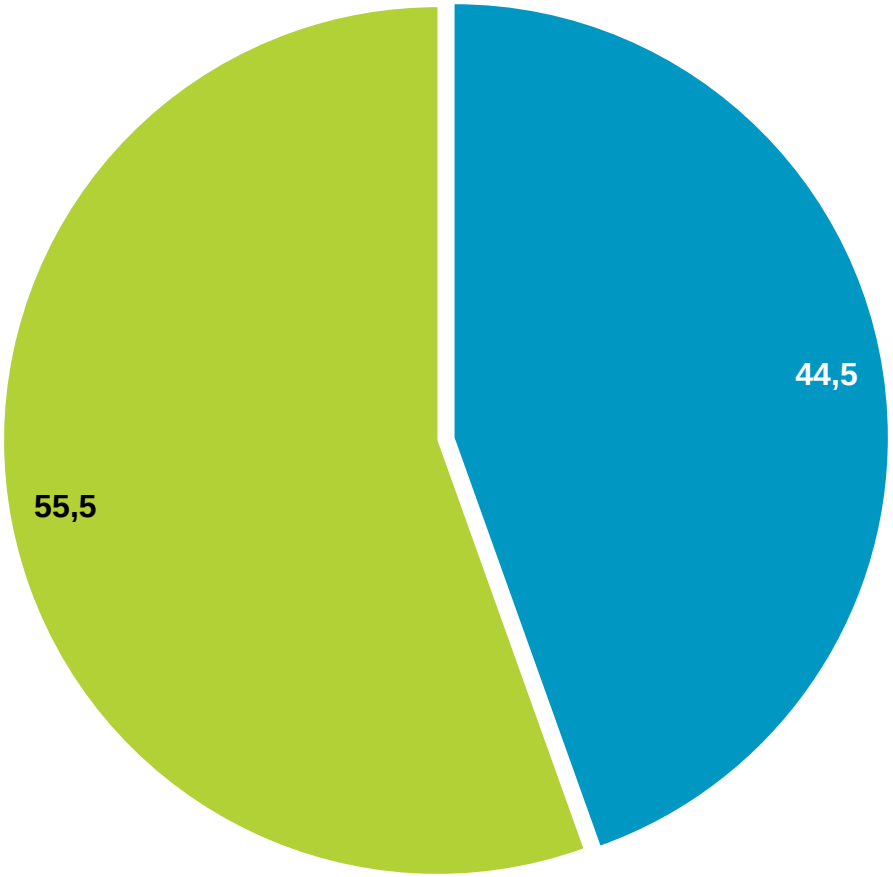
https://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html#AppendixJAVA

https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.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

El **55,5%** de los dispositivos Android que presentan una **infección de malware** tienen **activada** la opción para **permitir la instalación de aplicaciones desde orígenes desconocidos**. Dicha opción se encuentra desactivada por defecto.



Pinkerton

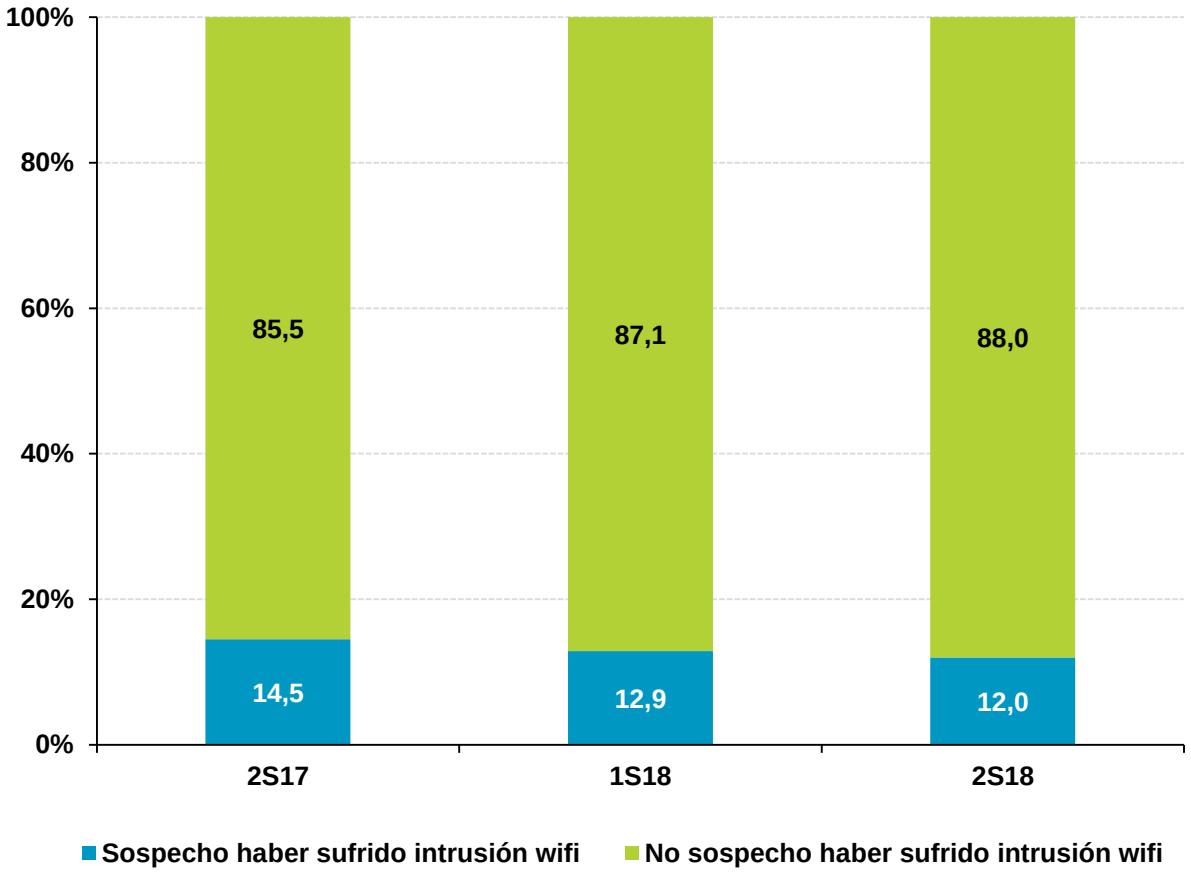
4

BASE: Total dispositivos Android infectados

Incidencias de seguridad en redes inalámbricas Wi-Fi

El **12%** de usuarios ***sospecha*** **haber sufrido una intrusión en la red inalámbrica Wi-Fi** del hogar.

% individuos



¿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

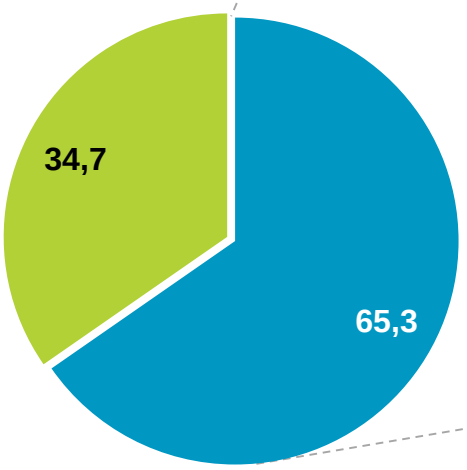
Consecuencias de los incidentes de seguridad y reacción de los usuarios

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:



Ha sufrido alguna situación de fraude

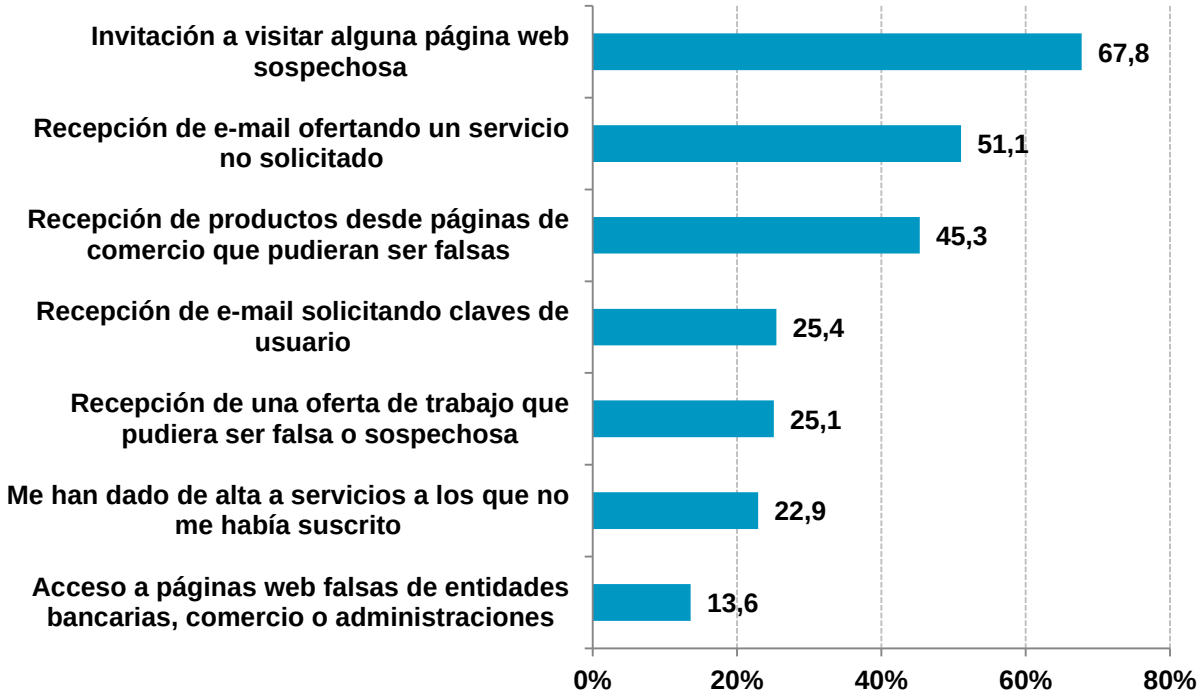
No ha sufrido ninguna situación de fraude

BASE: Total usuarios

Manifestaciones del intento de fraude online:

Respuesta múltiple

% individuos

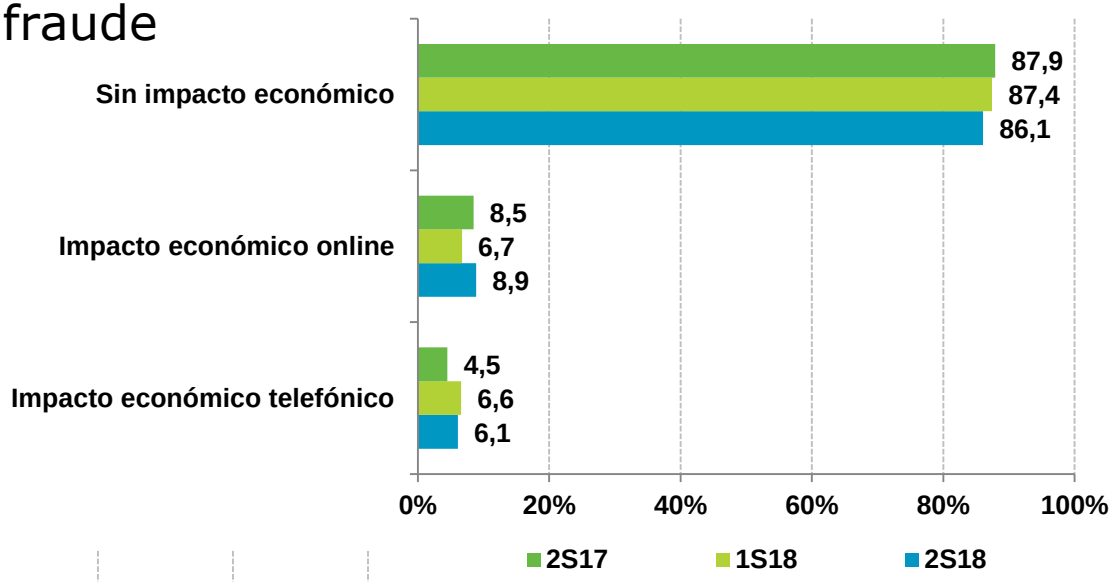


BASE: Usuarios que han sufrido algún intento de fraude

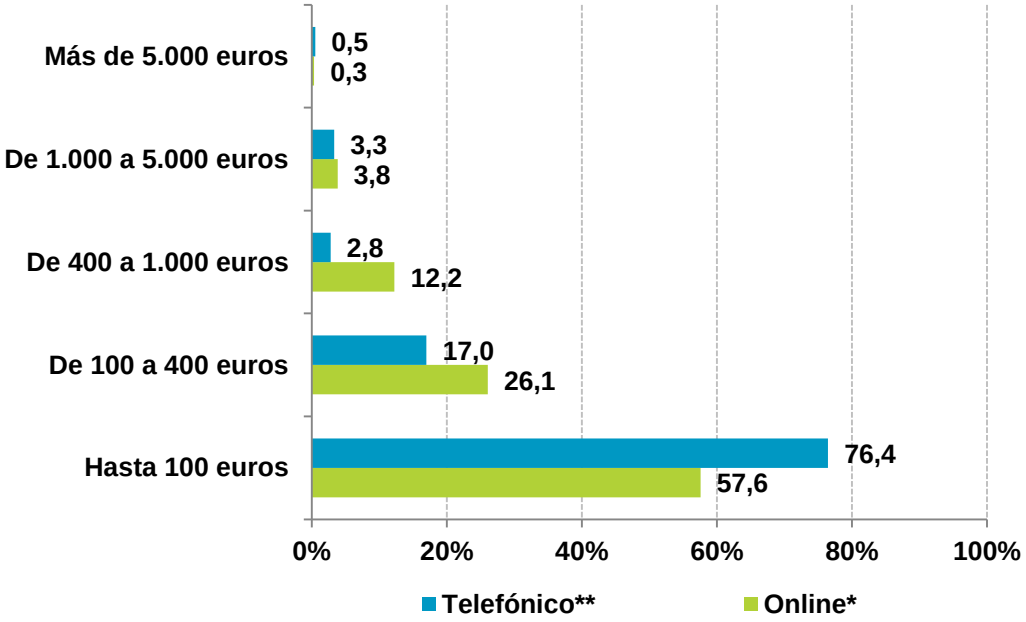
Conoce más en profundidad el fraude online: https://www.osi.es/fraude-online

Impacto económico del fraude

Los intentos de fraude online que logran causar un **perjuicio económico** para la víctima se han aumentado ligeramente (**+1,3 p.p.**) durante el segundo semestre de 2018.



BASE: Usuarios que han sufrido un intento de fraude



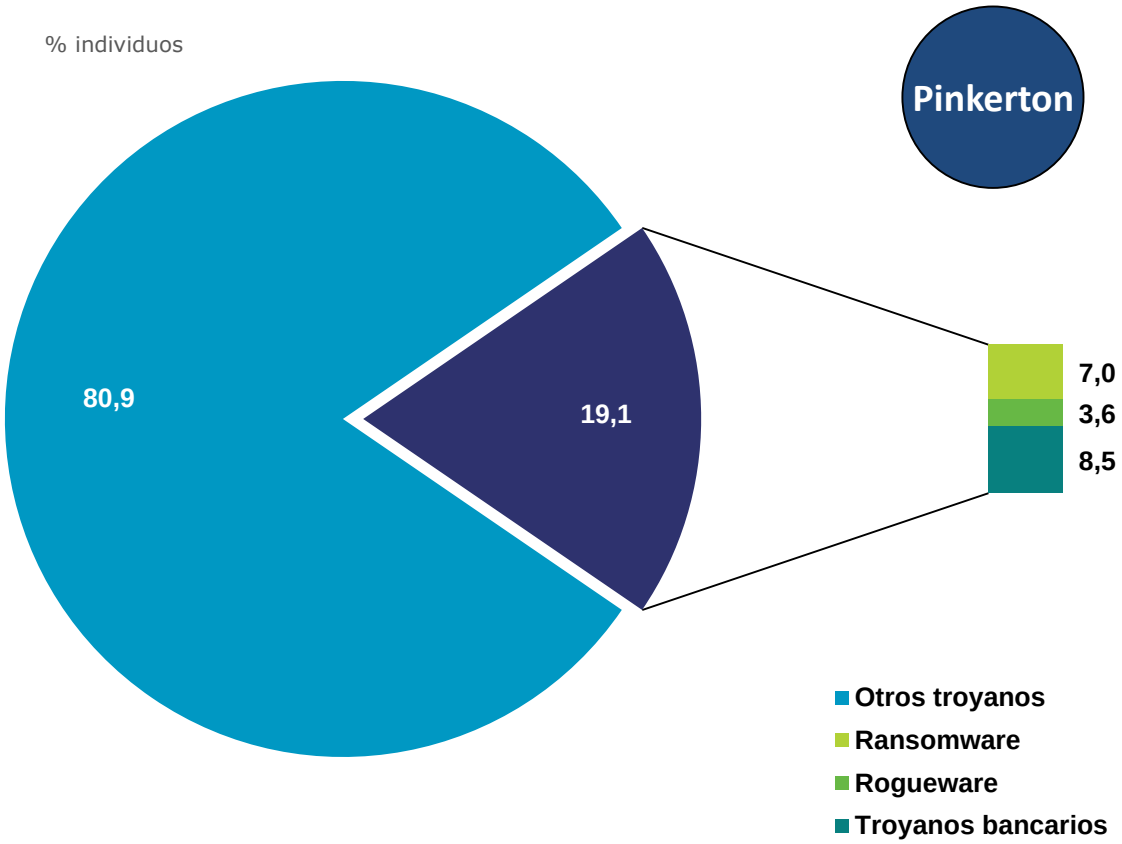
Distribución del impacto económico del fraude

* 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 de **troyanos bancarios** y **ransomware** en los ordenadores de los hogares españoles se sitúa en torno al 7 - 8%.



BASE: Equipos con troyanos detectados en ordenadores

Tipología del malware analizado

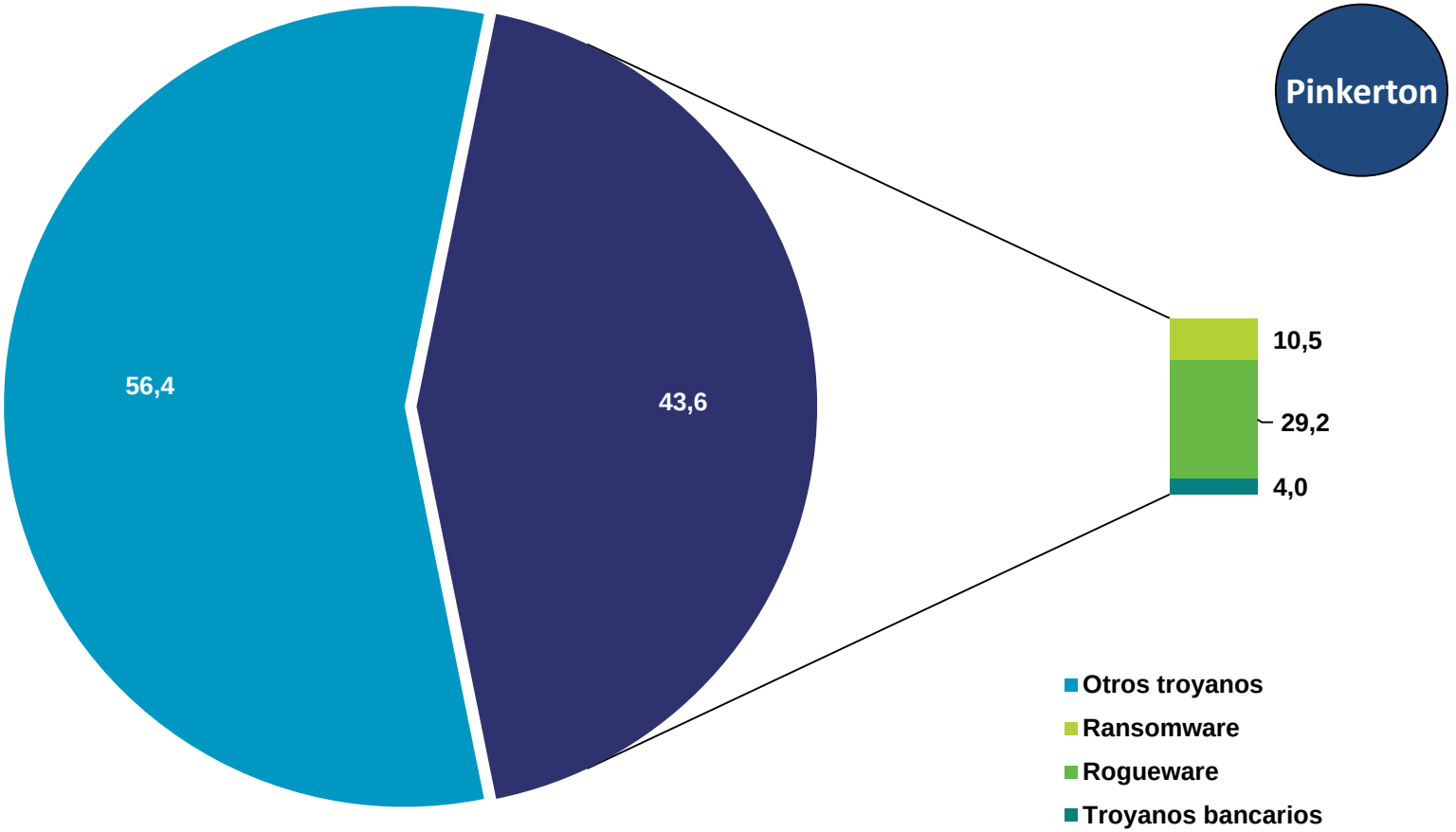
✓ Troyano bancario:
malware que roba información confidencial a los clientes de banca y/o plataformas de pago online.

✓ 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

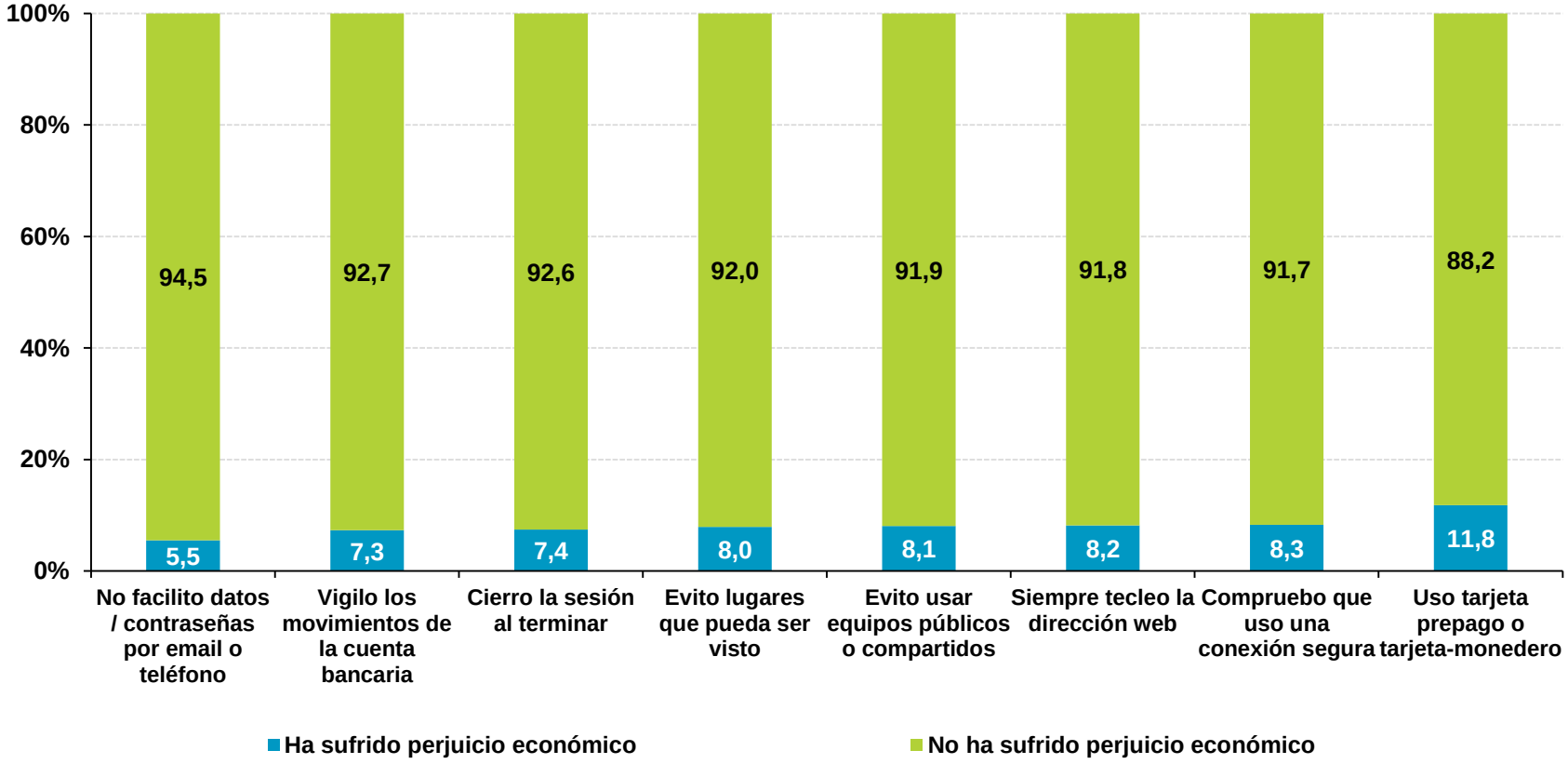
Destaca el **rogueware** como la subcategoría de troyano más detectada en los dispositivos Android**.**



BASE: Equipos con troyanos detectados en dispositivos Android

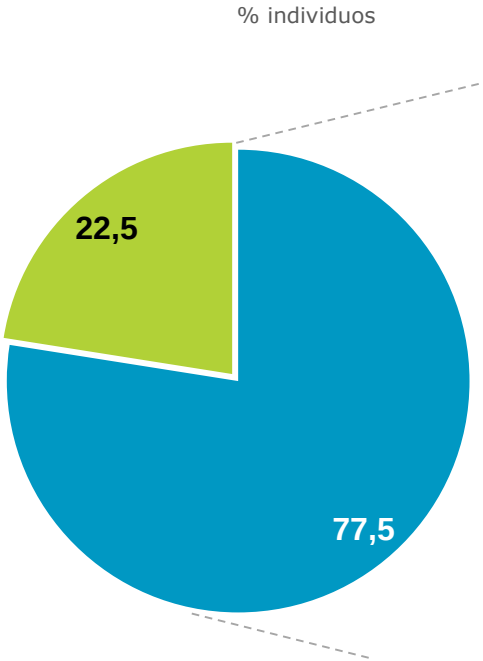
Consumación del intento de fraude según los hábitos prudentes

Los hábitos prudentes en la nevegación por Internet y uso del equipo informático o dispositivo móvil se traduce en una **minimización** del riesgo de consumación de un intento de fraude. En todos los casos, un porcentaje superior al **88,2%** de los usuarios con buenos hábitos NO sufrieron perjuicio económico derivado de un intento de fraude.



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

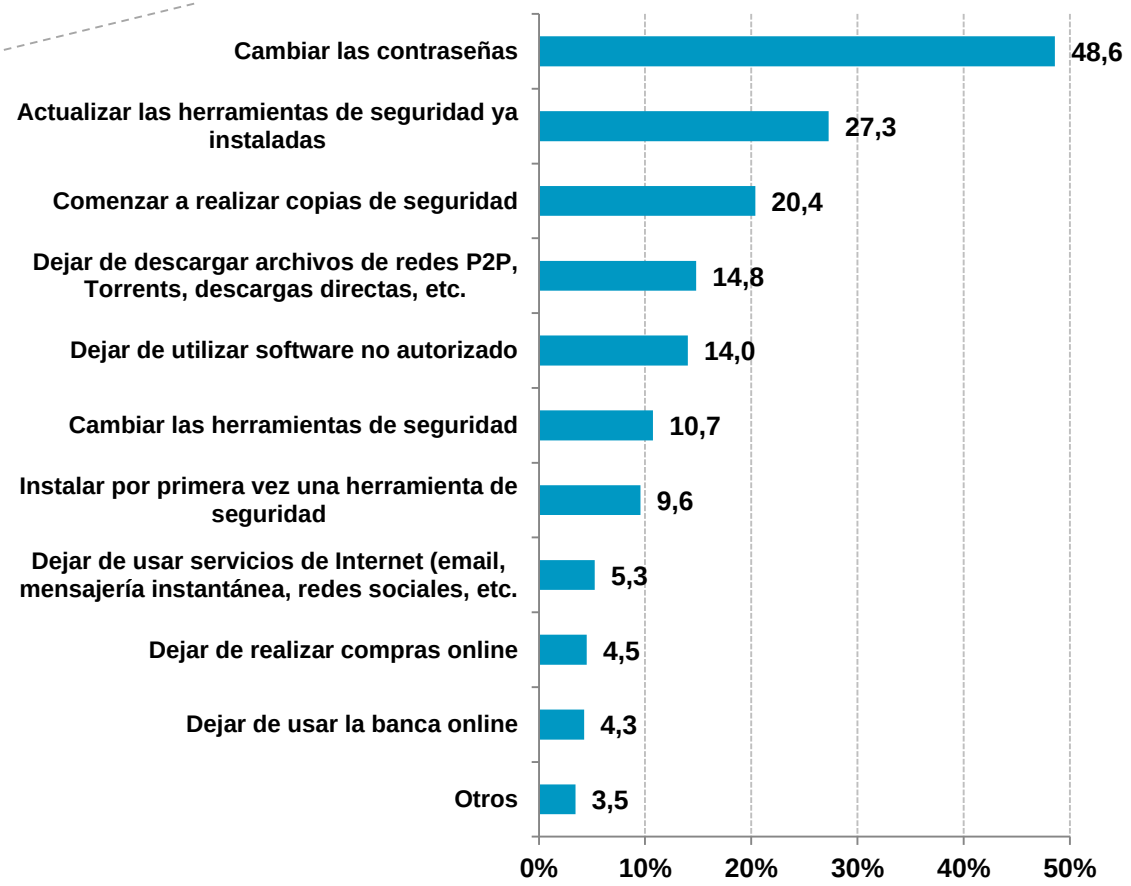
Cambios adoptados tras un incidente de seguridad



BASE: 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

La **suplantación de identidad** es la incidencia de mayor impacto sobre el cambio en los diferentes hábitos de los usuarios (entre un **20,7%** y un **50,2%**).

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	45,9	33,0	22,6	13,4	22,0	12,9
Pérdida de archivos o datos	43,4	27,9	26,3	17,5	21,2	15,6
Recepción de spam	38,3	21,2	15,5	7,7	10,0	6,5
Suplantación de identidad	**50,2**	30,5	**27,7**	**20,7**	**28,6**	**23,1**
Intrusión Wi-Fi	37,2	28,3	26,5	20,1	20,8	20,4
Pérdida del dispositivo	43,3	20,9	23,1	17,1	21,4	17,6
Servicios inaccesibles debido a ciberataques	44,4	**35,1**	24,2	16,3	19,9	17,5

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

Cambios adoptados tras un incidente de seguridad

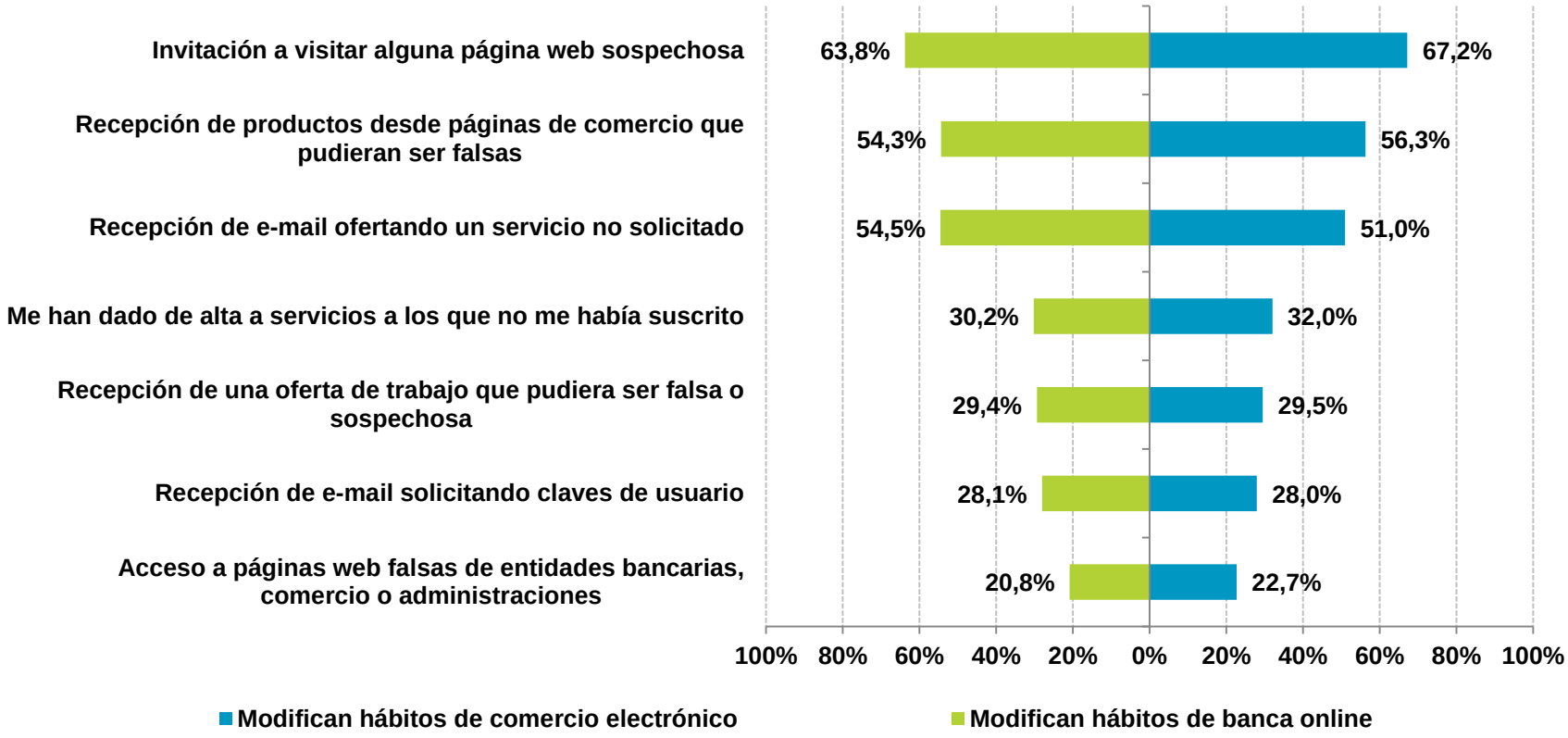
Cambios en el uso de servicios de Internet según el tipo de incidencia

Incidencia (%)	Dejar de usar servicios de Internet	Abandonar la banca online	Abandonar el comercio electrónico	Abandonar descargas
Malware	8,4	7,6	5,3	19,4
Pérdida de archivos o datos	13,4	9,8	9,7	19,2
Recepción de spam	2,8	2,4	2,6	10,2
Suplantación de identidad	12,5	13,5	14,8	20,3
Intrusión Wi-Fi	**23,0**	16,4	**17,8**	24,9
Pérdida del dispositivo	22,7	**22,3**	10,7	**35,6**
Servicios inaccesibles debido a ciberataques	9,0	9,3	9,5	18,9

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

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

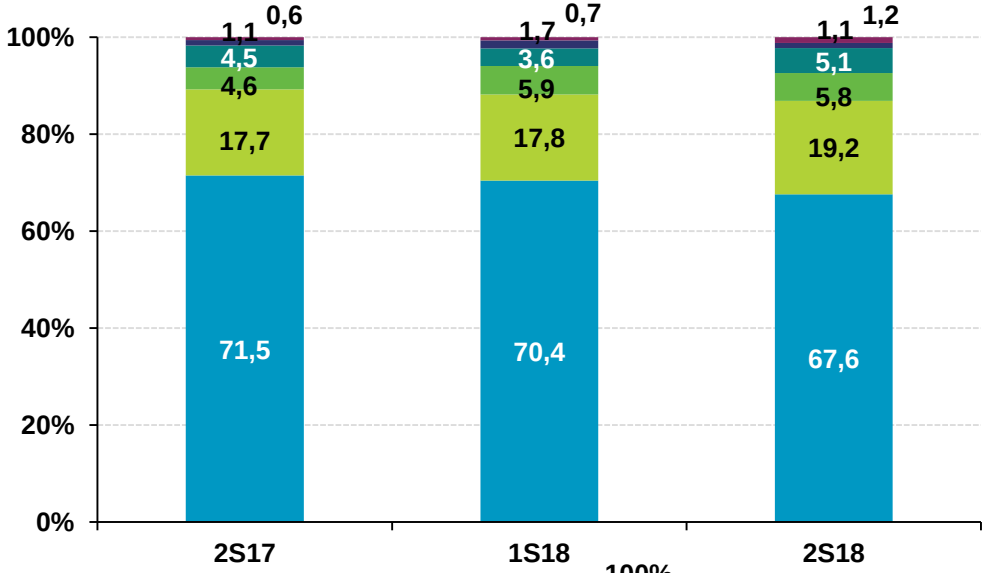
La recepción de una **invitación a visitar alguna página web sospechosa** continúa siendo la mayor influencia para los usuarios en cuanto a la modificación de sus hábitos prudentes en el uso de banca online (**63,8%**) y comercio electrónico (**67,2%**).



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

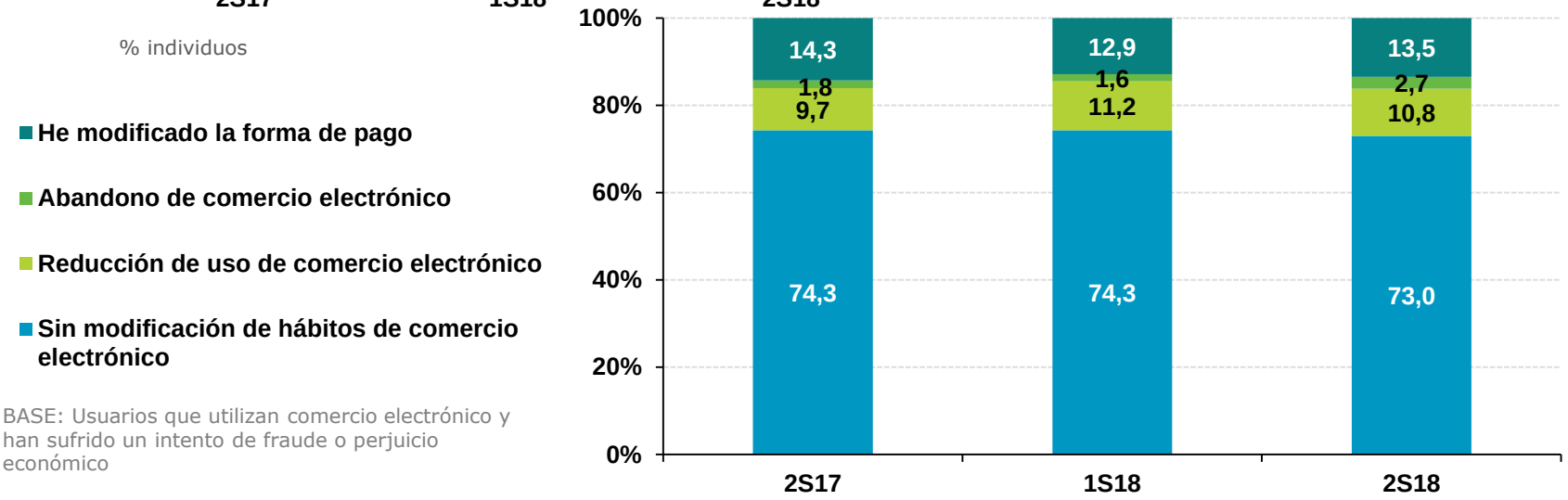
Cambios adoptados tras un incidente de seguridad

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



% individuos

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



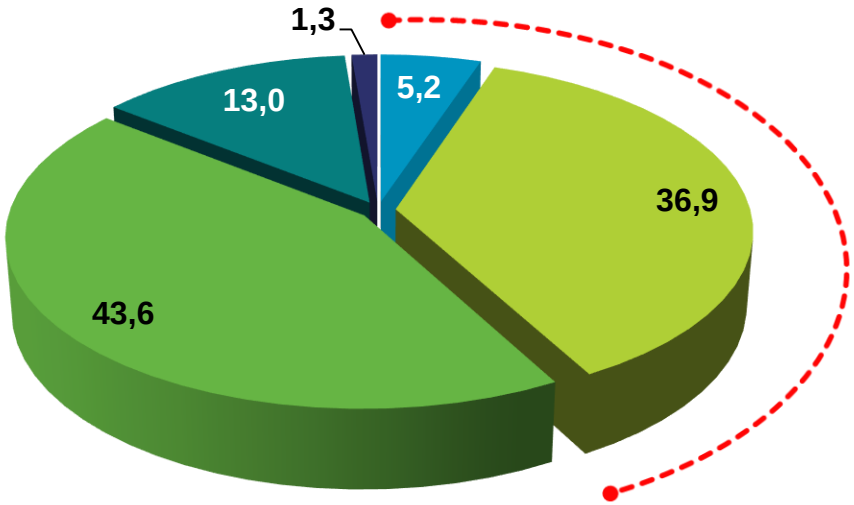
BASE: Usuarios que utilizan comercio electrónico y han sufrido un intento de fraude o perjuicio económico

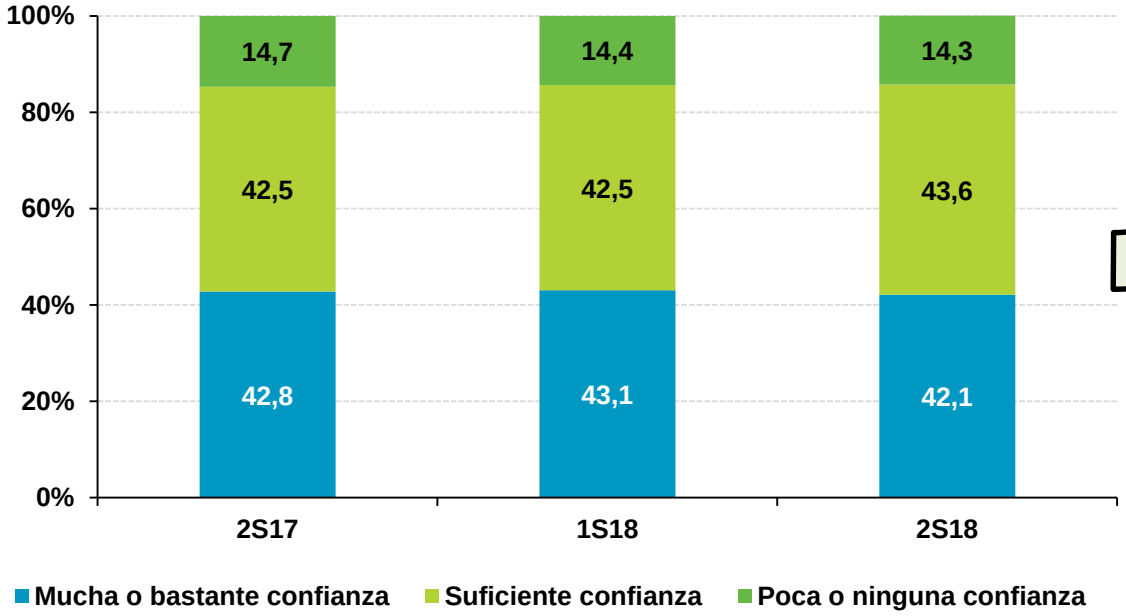
Confianza en el ámbito digital en los hogares españoles

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

Nivel de confianza en Internet

El volumen de usuarios con **poca o ninguna confianza** se **mantiene** constante, mientras que los usuarios con **mucha o bastante confianza decrece** en **-1,1 p.p**.



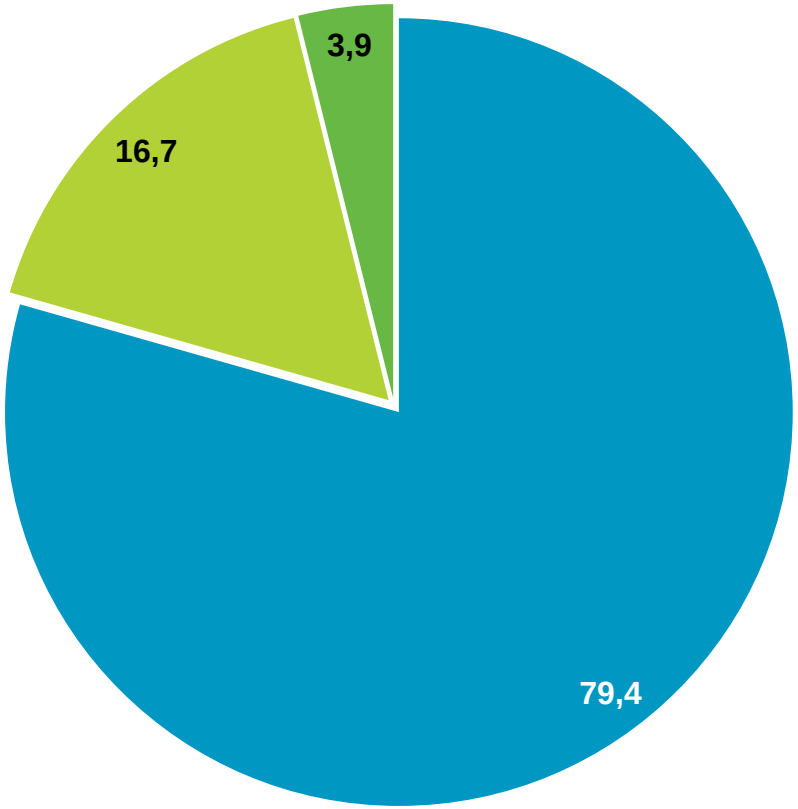


% individuos

BASE: Total usuarios

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

% individuos

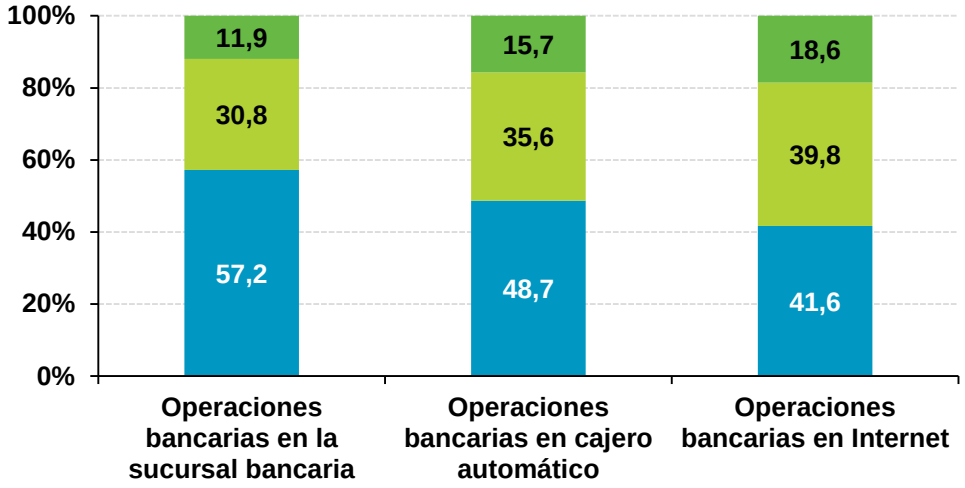


Casi 8 de cada 10 usuarios considera que su ordenador personal o dispositivo móvil se encuentra **razonablemente protegido** contra las amenazas de la Red.

6

BASE: Total usuarios

Confianza online vs. confianza offline



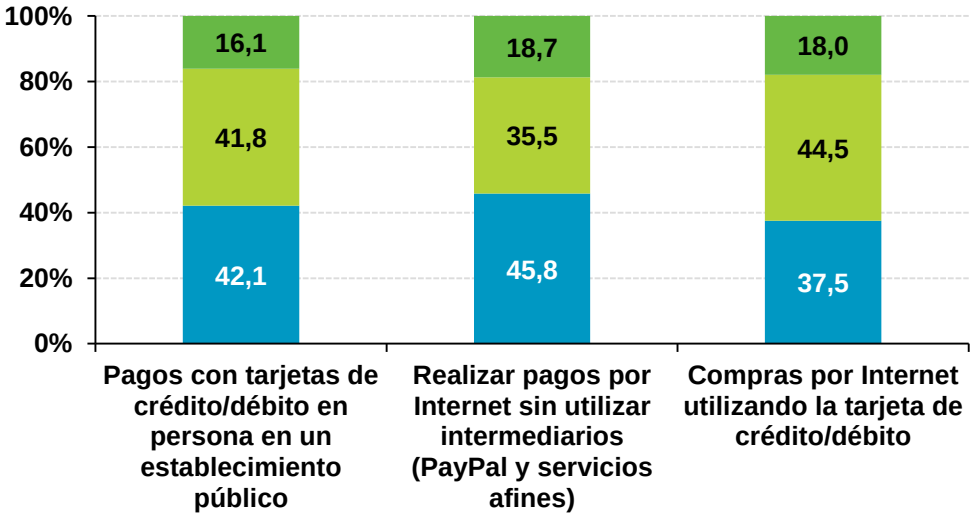
Nivel de confianza en operaciones bancarias

% individuos

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

Nivel de confianza en operaciones de compra-venta

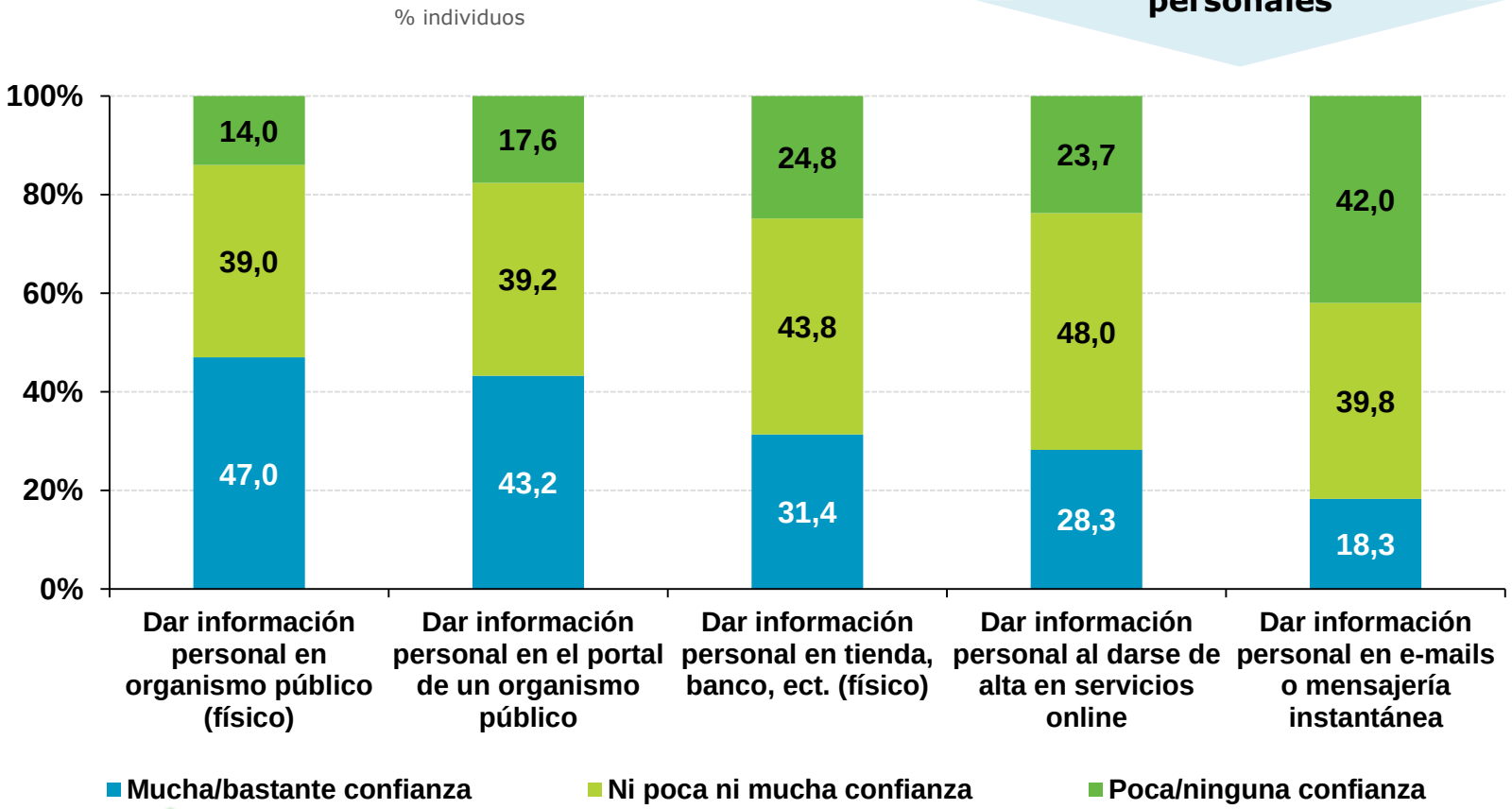
Realizar pagos en Internet usando un intermediario como Paypal aporta una mayor confianza (**+8,3 p.p.**) al usuario que hacer uso de la tarjeta de crédito/débito online.



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?

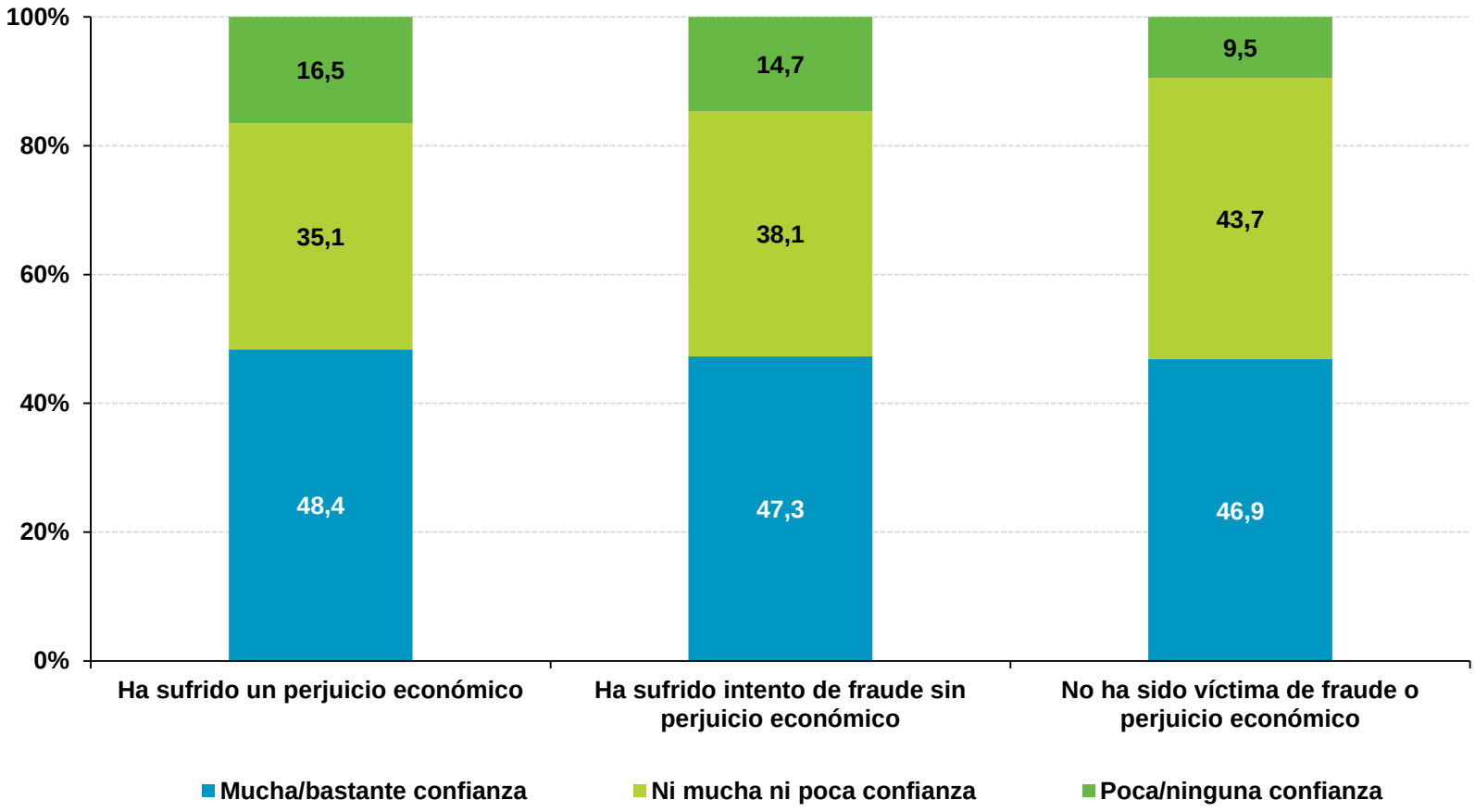
https://www.osi.es/sites/default/files/docs/datospersonales.pdf

BASE: Total usuarios

Confianza vs. fraude

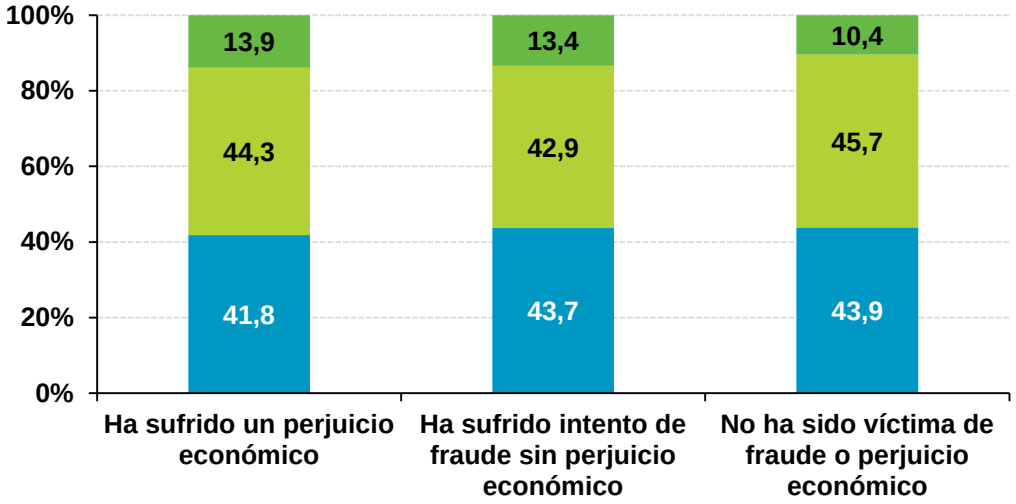
Confianza al realizar operaciones bancarias en Internet

% individuos



BASE: Usuarios que utilizan banca online

Confianza vs. fraude

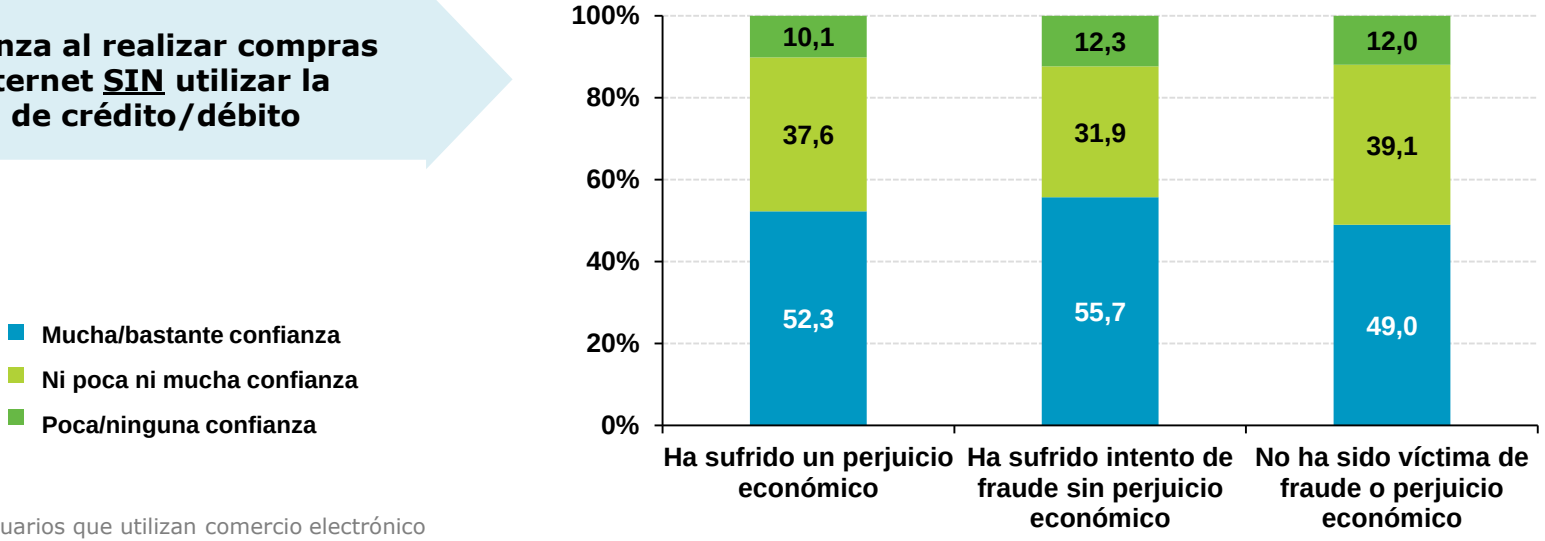


Confianza al realizar compras por Internet utilizando la tarjeta de crédito/débito

% individuos

6

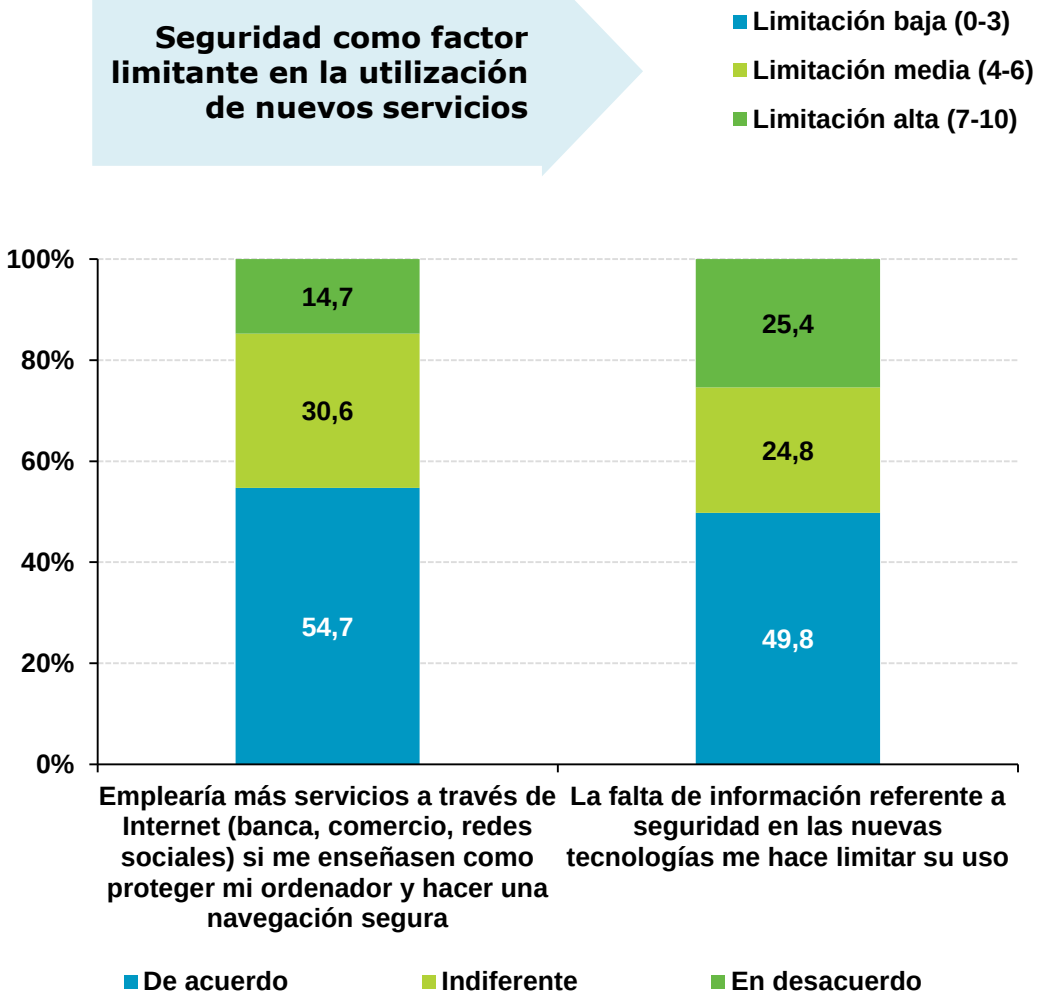
Confianza al realizar compras por Internet SIN utilizar la tarjeta de crédito/débito

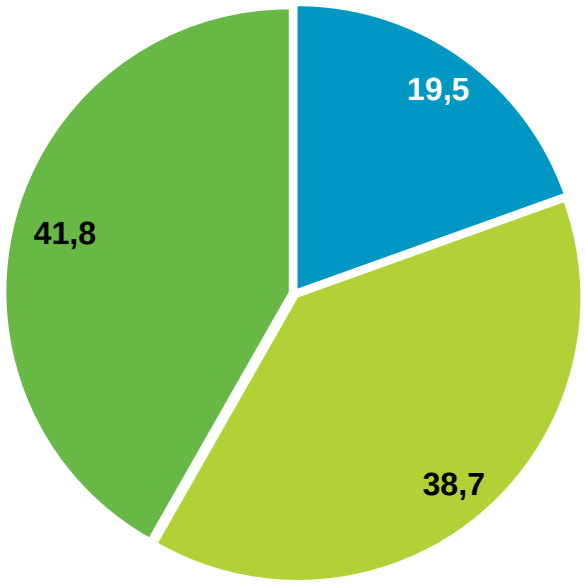


BASE: Usuarios que utilizan comercio electrónico

Limitación a causa de problemas de seguridad

Seguridad como factor limitante en la utilización de nuevos servicios





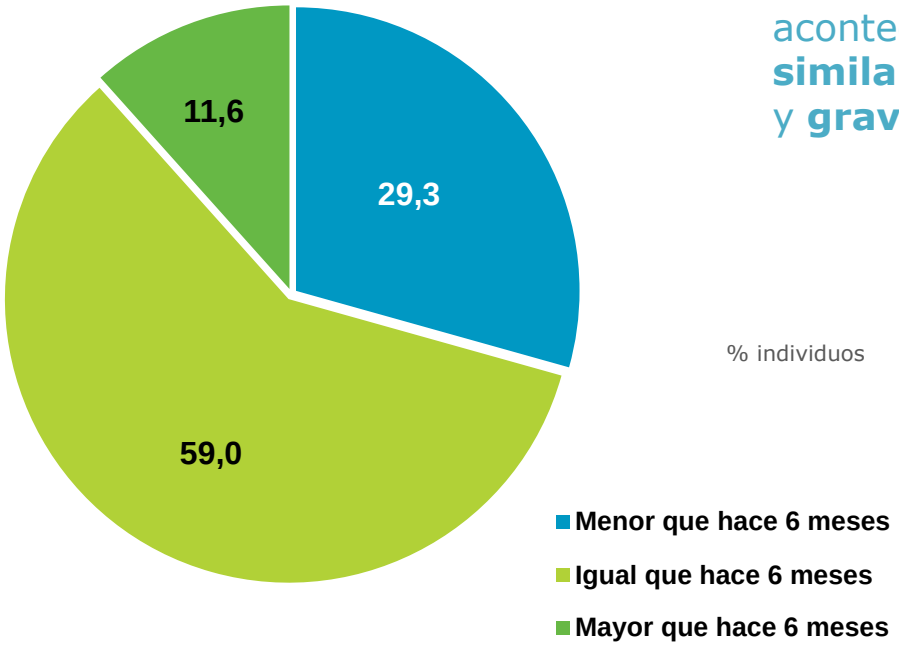
% individuos

Limitaciones en el uso de Internet

6

Percepción de los usuarios sobre la evolución en seguridad

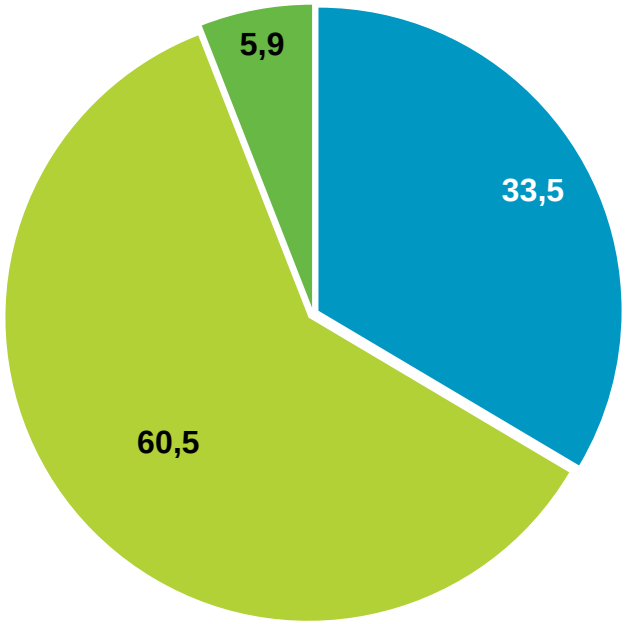
Número de incidencias



Más de la mitad de los usuarios encuestados opinan que las incidencias acontecidas en los últimos 6 meses son **similares en cuanto a cantidad** (**59%**) y **gravedad** (**60,5%**).

Gravedad de las incidencias

% individuos

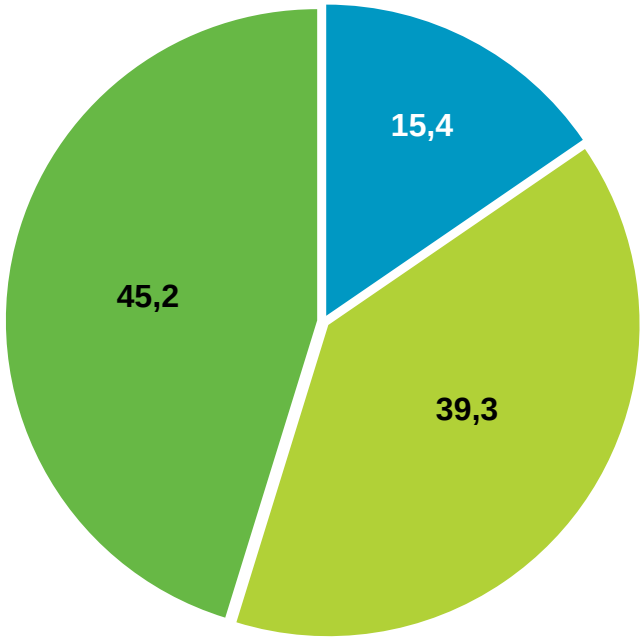


Casi **un tercio** percibe una **menor cantidad** de incidencias en los últimos 6 meses (**29,3%**) y también las considera de **menor gravedad** (**33,5%**).

BASE: Total usuarios

Percepción de riesgos en Internet

La percepción de riesgos en Internet sigue siendo liderada por el **robo y uso de información personal** (**45,2%**).



% individuos

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

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

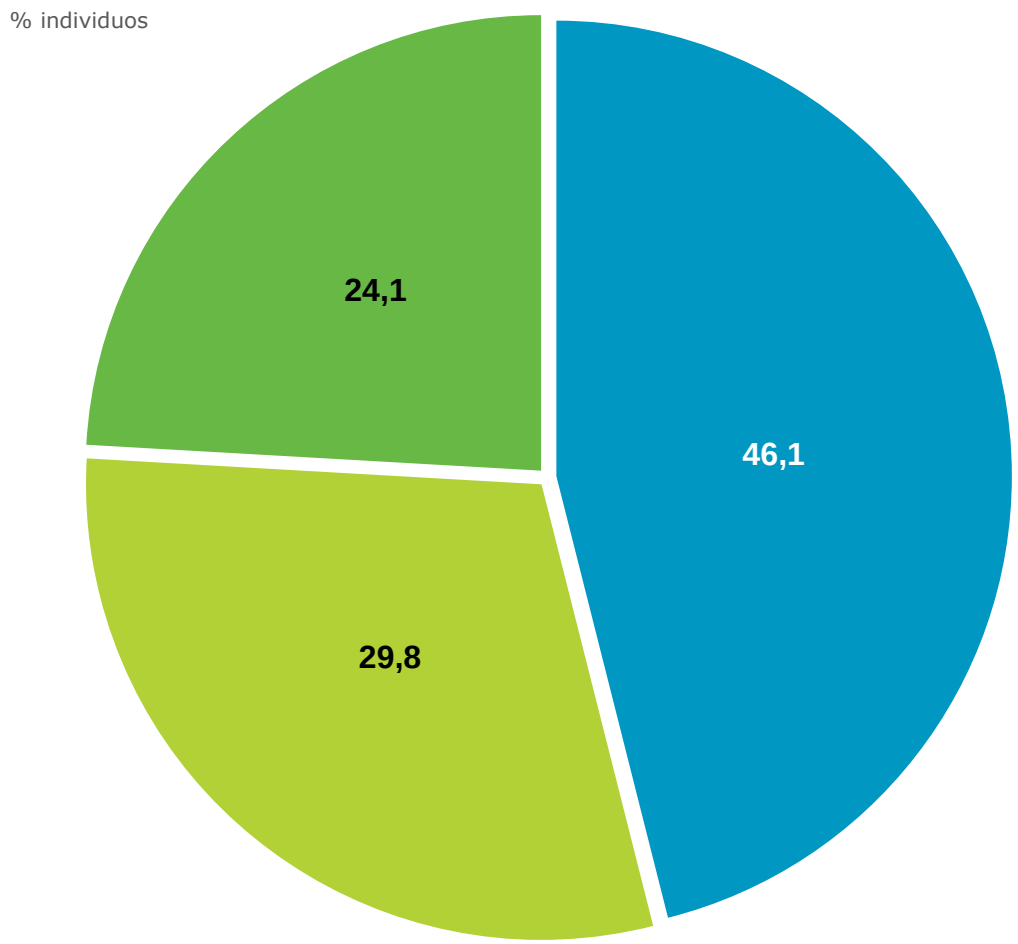
✓ **Datos en la nube:** https://www.osi.es/es/tu-informacion-en-la-nube

- **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



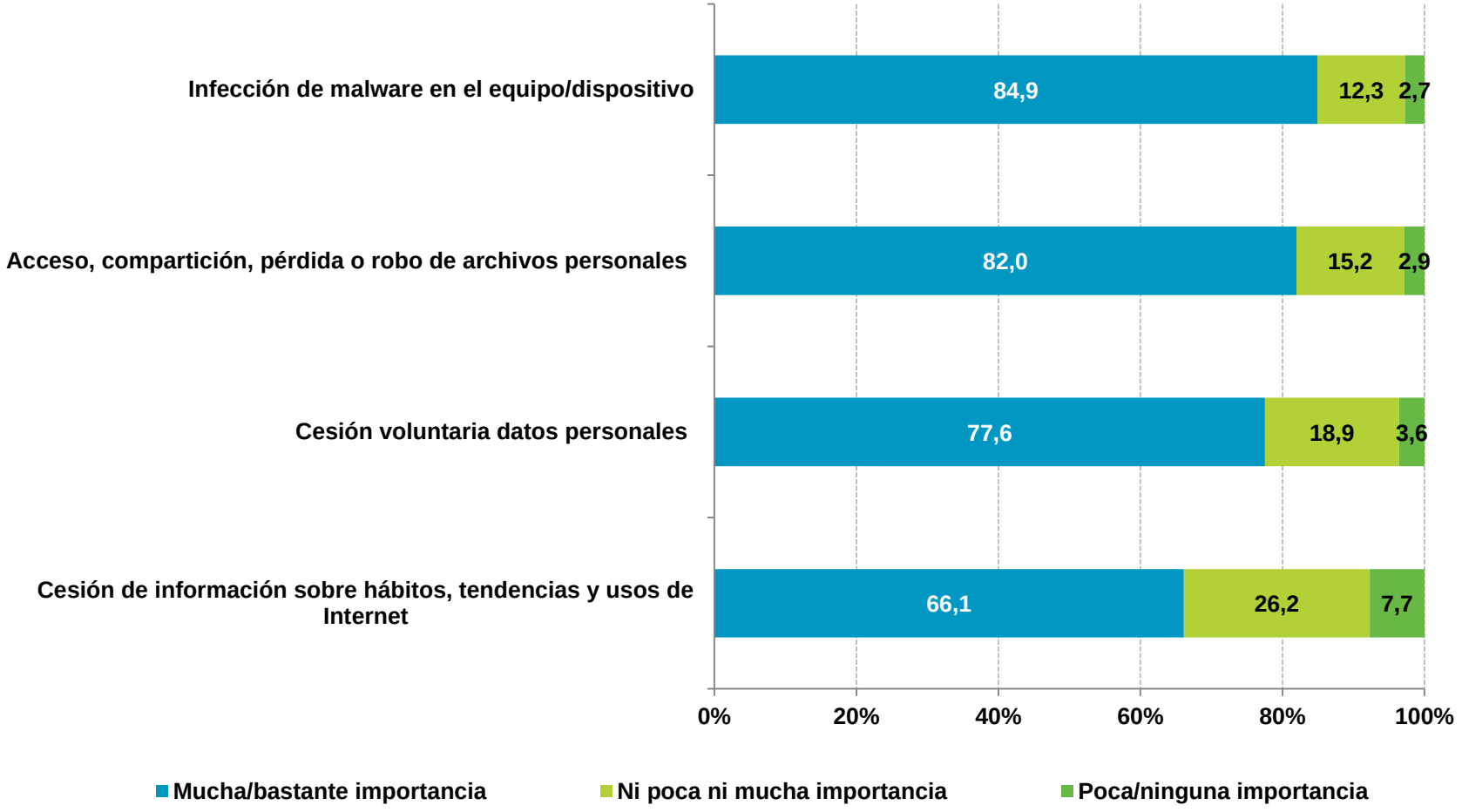
El **46,1%** de los internautas españoles opina que la red Internet es cada día más segura.

6

BASE: Total usuarios

Valoración de los peligros de Internet

Los peligros más valorados por los panelistas siguen siendo la **infección de malware en su equipo/dispositivo** (**84,9%**) y el **acceso, compartición, pérdidas o robo de archivos personales** (**82%**).

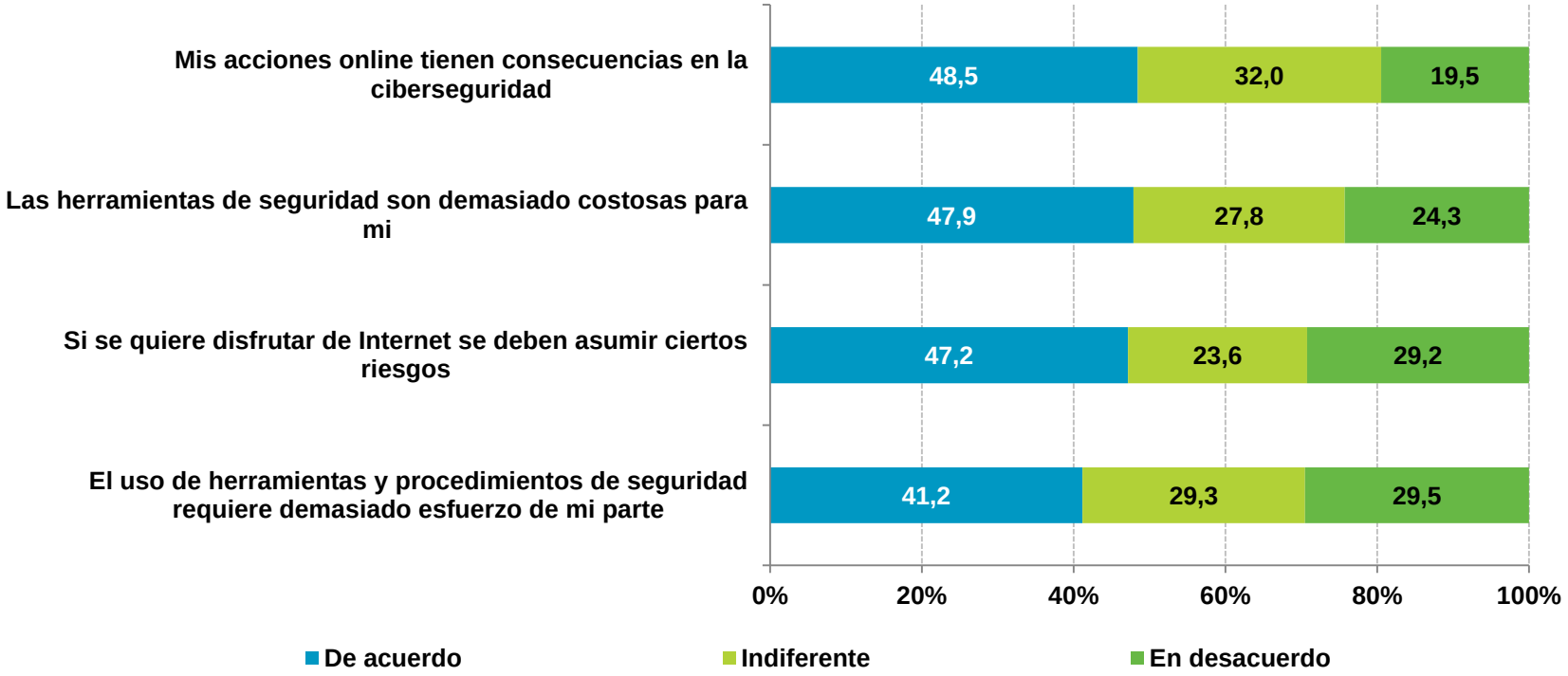


BASE: Total usuarios

Rol del usuario

Los internautas opinan que **sus acciones tienen consecuencias en la ciberseguridad** (**48,5%**).

Por otro lado, casi la mitad considera **necesario asumir ciertos riesgos para disfrutar de Internet** (**47,2%**), que **las herramientas de seguridad son demasiado costosas** (**47,9%**) o que tanto **el uso de herramientas como procedimientos de seguridad requieren demasiado esfuerzo** (**41,2%**)



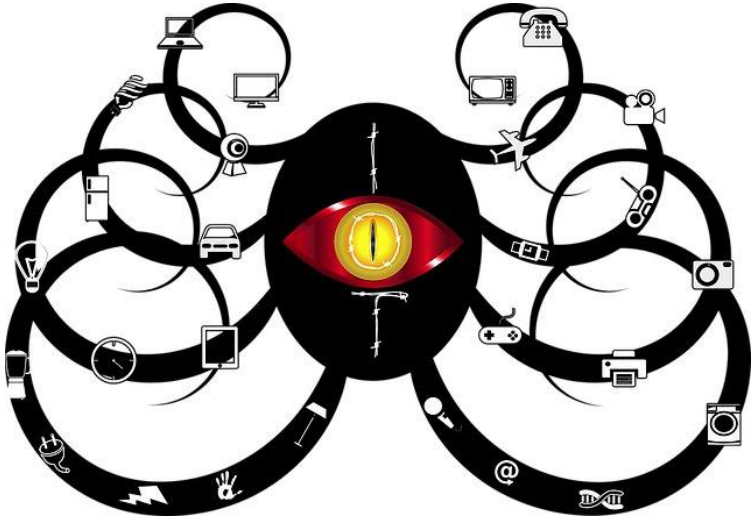
BASE: Total usuarios

Conclusiones

Conclusiones

Durante el 2018 se ha batido el récord de vulnerabilidades en programas y aplicaciones (*software*) detectadas, suponiendo un aumento del 9% con respecto al año anterior y alcanzando un promedio de 46 nuevas vulnerabilidades identificadas al día [1]. No obstante, el 41,2% de hogares españoles declara no actualizar periódicamente sus ordenadores, aumentando hasta el 50,9% el número real de equipos desactualizados, y por tanto, más vulnerables a ataques. En muchos casos, en torno al 60%, no se usan las medidas de seguridad recomendables por desconocimiento de las mismas o por falta de interés al considerar mínima la reducción del riesgo en potencia con respecto a no implementarlas.

Los productos *IoT* (*Internet of Things*) son cada vez más numerosos y el volumen de productos con capacidad de conexión a Internet que se regalan en Navidad sigue aumentando, como *smartphones*, *tablets,* videoconsolas y otros juguetes y dispositivos electrónicos con conectividad a la Red [2]. Sin embargo, los usuarios no suelen ser plenamente conscientes de los riesgos que pueden entrañar y las medidas de seguridad necesarias [3] que se deberían tomar para evitarlos. Además, los atacantes han sabido aprovechar sus vulnerabilidades como una nueva vía de acceso a las redes locales [4].



[1] https://globbsecurity.com/2018-bate-record-en-ciberataques-44093

[2] https://www.laverdad.es/tecnologia/juguetes-conectados-espias-20181218190319-ntrc.html

[3] https://www.blog.andaluciaesdigital.es/juguetes-conectados-normas-de-seguridad/

[4] https://www.itdigitalsecurity.es/actualidad/2018/12/encontrados-importantes-fallos-en-los-principales-protocolos-de-iot

Conclusiones

Teniendo en cuenta la gran cantidad de vulnerabilidades detectadas a lo largo del año que afectan a los dispositivos de conexión de red, la importancia de aplicar las actualizaciones de seguridad disponibles tanto del sistema operativo, programas y aplicaciones instaladas, como del firmware de los dispositivos, así como configurar éstos adecuadamente y evitar mantener las credenciales establecidas por defecto por el fabricante son cada vez más acuciantes. No obstante, no se aprecian cambios significativos en los hábitos de protección de redes en los hogares españoles, manteniéndose la pauta de desinterés y desconocimiento sobre las medidas de protección que proporcionan los routers; llegando a la coyuntura de que actualmente 5 de cada 6 routers son inseguros [5].

El estándar WPA2 continúa siendo el más popular (39,8%), a pesar de que sigue presentando riesgos de seguridad que hacen necesario tomar medidas adicionales [6]. También sigue habiendo un porcentaje significativo de usuarios que consideran que su red está protegida a pesar de desconocer el sistema usado (26,7%). Por otro lado, el porcentaje de usuarios que desconoce si su red está protegida (12,6%) y el de los que admite que no lo está en absoluto (6,2%) han aumentado ligeramente durante el último semestre de 2018. Posiblemente la mayoría de los internautas mantienen la configuración por defecto que establece el fabricante del router o el proveedor del servicio de Internet, lo cual también constituye un importante riesgo [7].

7

[5] https://www.itdigitalsecurity.es/vulnerabilidades/2018/10/5-de-cada-6-routers-son-inseguros

[6] https://www.redeszone.net/2018/10/03/proteger-routers-nuevas-vulnerabilidades-wpa2/

[7] https://omicrono.elespanol.com/2018/12/contrasena-de-la-red-wifi-en-routers-orange/

Conclusiones

A pesar de todo, el porcentaje de usuarios que sospecha que su red del hogar ha sido comprometida y se ha producido una intrusión continúa disminuyendo, situándose durante este semestre en el 12%. Sin embargo, teniendo en cuenta las escasas medidas de seguridad tomadas (6,2%), el porcentaje relativamente elevado de usuarios que desconoce si su red está convenientemente protegida (12,6%) o con qué sistema (26,7%), y el aumento del número de vulnerabilidades y malware dirigido contra routers y dispositivos IoT, no se puede asegurar si este decrecimiento se debe realmente a una disminución del número de intrusiones o a que los usuarios sean menos conscientes de su situación real.

Respecto a los hábitos de uso de redes inalámbricas Wi-Fi externas y/o ajenas, se aprecia como 3 de cada 10 usuarios se conecta a redes públicas (16,4%) o de otro usuario particular (12,6%), y casi un 37% no duda en hacerlo en cualquier lugar siempre que lo necesite sin preocuparse de si esa red es segura o de si los datos que circulen a través de ella podrían verse comprometidos.

[8] https://news.sophos.com/es-es/2018/11/16/botnet-atrapa-100-000-routers-debido-a-una-antigua-vulnerabilidad/

[9] https://www.redeszone.net/2018/09/21/vulnerabilidad-routers-wifi/

Conclusiones

Entre los ciberataques más importantes de este año destacan los dirigidos contra las redes sociales *Facebook* (cerca de 50 millones de cuentas vulneradas) [10] y *Twitter* (no informaron del número de cuentas vulneradas) [11]. En ambos casos las vulnerabilidades que aprovecharon los atacantes estaban relacionadas con el método utilizado para gestionar los datos de acceso por parte de cada una de la red social afectada.

En el caso de *Facebook* el problema fue debido a una vulnerabilidad en el código que se encargaba de implementar la función *"Ver como"* del perfil, que permitía a un atacante suplantar la identidad del dueño de la cuenta mediante el *'token'* de acceso. Por su parte, el fallo de seguridad en el caso de *Twitter* se debió al método en que se almacenaba la contraseña del usuario en forma cifrada dentro de la red social.

A pesar de estas brechas de seguridad, el hábito de cambiar periódicamente las contraseñas de acceso y el empleo de contraseñas diferentes para cada servicio online utilizado podría haber reducido significativamente el riesgo. No obstante, solo el 57,4% de los encuestados afirma utilizar debidamente las contraseñas y menos del 50% afirma que cambia sus contraseñas incluso después de haber sufrido algún tipo de incidencia.

[10] https://www.abc.es/tecnologia/redes/abci-facebook-primer-gran-hackeo-facebook-50-millones-cuentas-estan-riesgo-201809281909_noticia.html

[11] https://as.com/betech/2018/05/03/portada/1525384572_237897.html

Conclusiones

Si bien 2017 fue el año de '*WannaCry'*, este 2018 se podría decir que ha sido el año del *malware* '*Coinhive'* [12][13]. Aunque se ha dado a llamar de igual manera al *malware* que lo utiliza, 'Coinhive' es una herramienta para minar criptomonedas ideada como alternativa a la publicidad con el objetivo de monetizar sitios web fácilmente a través de la aplicación de un código *JavaScript* en el código fuente del sitio en cuestión. Sin embargo los desarrolladores de *malware*, siempre en busca de nuevos métodos para obtener beneficios de los usuarios infectados, han tardado poco en aplicar esta herramienta a sus creaciones.

Los ciberdelincuentes también han sacado provecho de esta herramienta aplicándola a los sitios web con vulnerabilidades (siendo aquellos con mayor número de visitantes –como los sitios web de visualización de contenidos en *streaming* o compartición de ficheros– los preferidos), aprovechando así la capacidad de procesamiento del equipo del internauta que visita una de estas páginas sin que éste se dé cuenta. Se estima que puede llegar a emplear hasta el 65% de la capacidad del equipo mientras el usuario navega por Internet.

[12] https://blog.malwarebytes.com/threat-analysis/2018/07/obfuscated-coinhive-shortlink-reveals-larger-mining-operation/

[13] https://www.forbes.com/sites/donnafuscaldo/2018/12/28/crypto-mining-malware-grew-4000-this-year/#5f27fdec224c

Conclusiones

En cualquier caso, este año el *malware* de criptominado ha superado ampliamente al *ransomware* [14], llegando a estimarse incluso en un aumento del 4000%. Nuevos malware como *'PowerGhost'* [15] o *'Rakhni'* [16] han empezado a actuar este año junto con el conocido *'Coinhive'*.

Respecto a los ordenadores del hogar, pese a que el 67,1% de los equipos que participaban en la encuesta presentaban algún tipo de malware, el 86,5% de los usuarios declararon no estar infectados.

Por lo tanto, hay un gran número de usuarios que no es consciente del riesgo real que supone su uso de Internet. Un 29,3% de los encuestados considera que el número de incidencias en Internet ha disminuido y un 33,5% opina que los incidentes son menos graves [17].

Este año también se ha descubierto el primer *rootkit* de UEFI, *'LoJax'* [18], que supone una grave amenaza debido a que es difícil de detectar y es capaz de continuar infectando la máquina a pesar de la reinstalación del sistema operativo o incluso del reemplazo del disco duro, a menos que se realice una reinstalación del *firmware*.

[14] https://es.cointelegraph.com/news/cryptojacking-overtakes-ransomware-as-top-malware-in-some-countries

[15] https://latam.kaspersky.com/blog/powerghost-nuevo-minero-de-criptomonedas-apunta-a-redes-corporativas-de-america-latina/13206/

[16] https://www.kaspersky.es/blog/rakhni-miner-cryptor/16418/

[17] https://www.kaspersky.es/blog/risky-websites-42/16736/

[18] https://www.welivesecurity.com/la-es/2018/09/27/lojax-primer-rootkit-uefi-en-uso-cortesia-grupo-sednit/

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: 3.824 hogares encuestados y equipos/dispositivos Android escaneados (software instalado en 2.157 PCs y 1.855 smartphones y 255 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 2018 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=3.824 le corresponde una estimación del error muestral igual a ±1,58%.

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: 10.30923/2386-3684-29

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

Tel.: 91 212 76 20 / 25
Twitter: @ONTSI
www.red.es