Estudio sobre la Ciberseguridad y confianza en los hogares españoles

Oleada Julio – Diciembre 2015

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

ontsi observatorio nacional de las telecomunicaciones y de la SI

Junio 2016

INDICE

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

2. **Medidas de seguridad**
   Definición y clasificación de las medidas de seguridad, Uso de medidas de seguridad en el ordenador del hogar, Frecuencia de actualización y utilización, Medidas de seguridad utilizadas en redes inalámbricas Wi-Fi, Uso de medidas de seguridad dispositivos Android

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

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

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

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

7. **Conclusiones**

8. **Alcance del estudio**

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 3.577 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 50 motores antivirus. Los datos así extraídos se representan en el presente informe con siguiente etiqueta:

Los datos reflejados en **este informe abarcan** el **análisis desde julio hasta diciembre de 2015**.

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. Frecuencia de actualización y utilización
4. Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi
5. Uso de medidas de seguridad en dispositivos Android

Definición y clasificación de las medidas de seguridad

2

Medidas de seguridad[1]

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

Medidas automatizables

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

Medidas no automatizables

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

Medidas proactivas

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

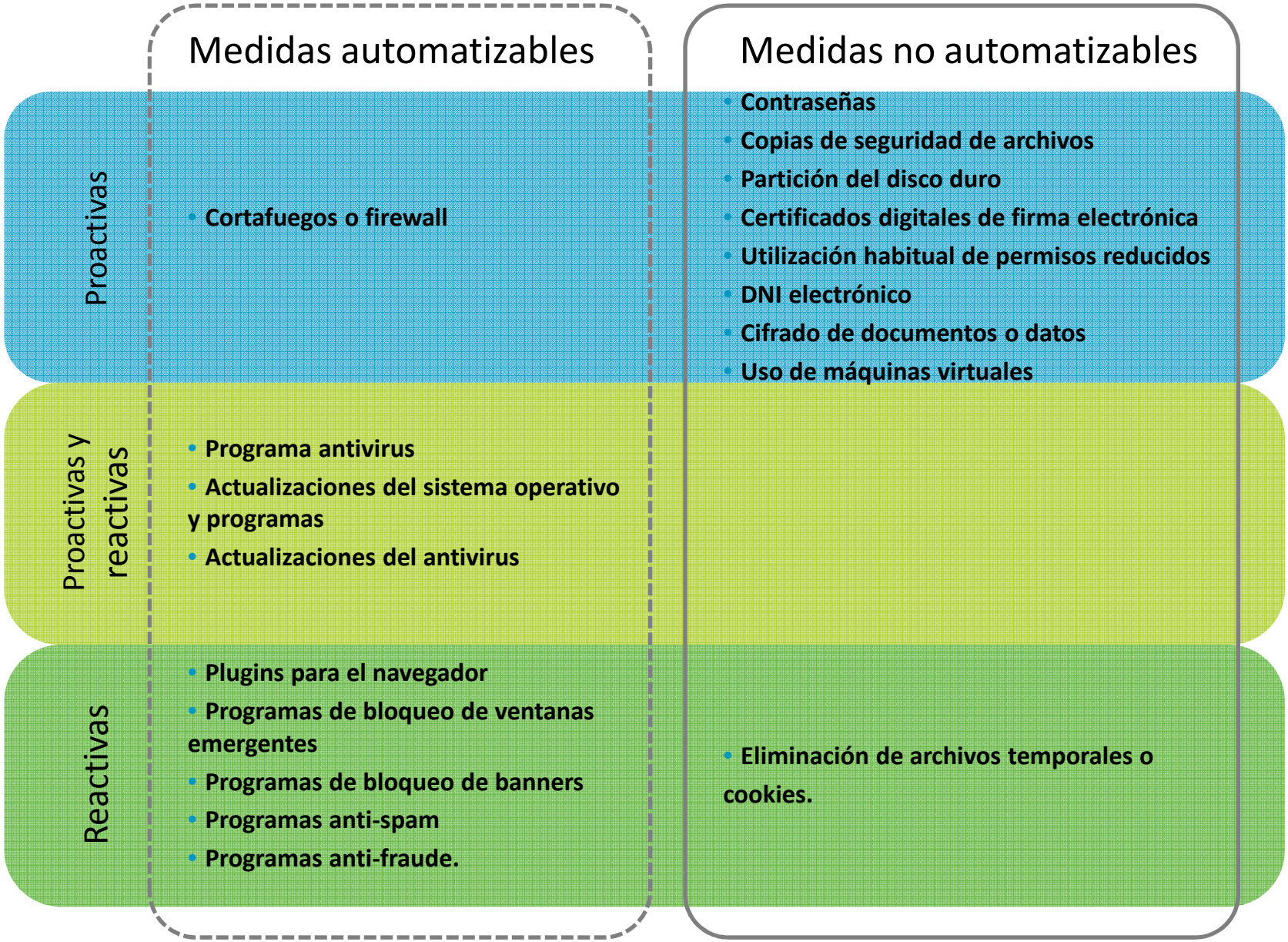
Medidas reactivas

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

Herramientas que te ayudarán a proteger tus dispositivos: https://www.osi.es/herramientas

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

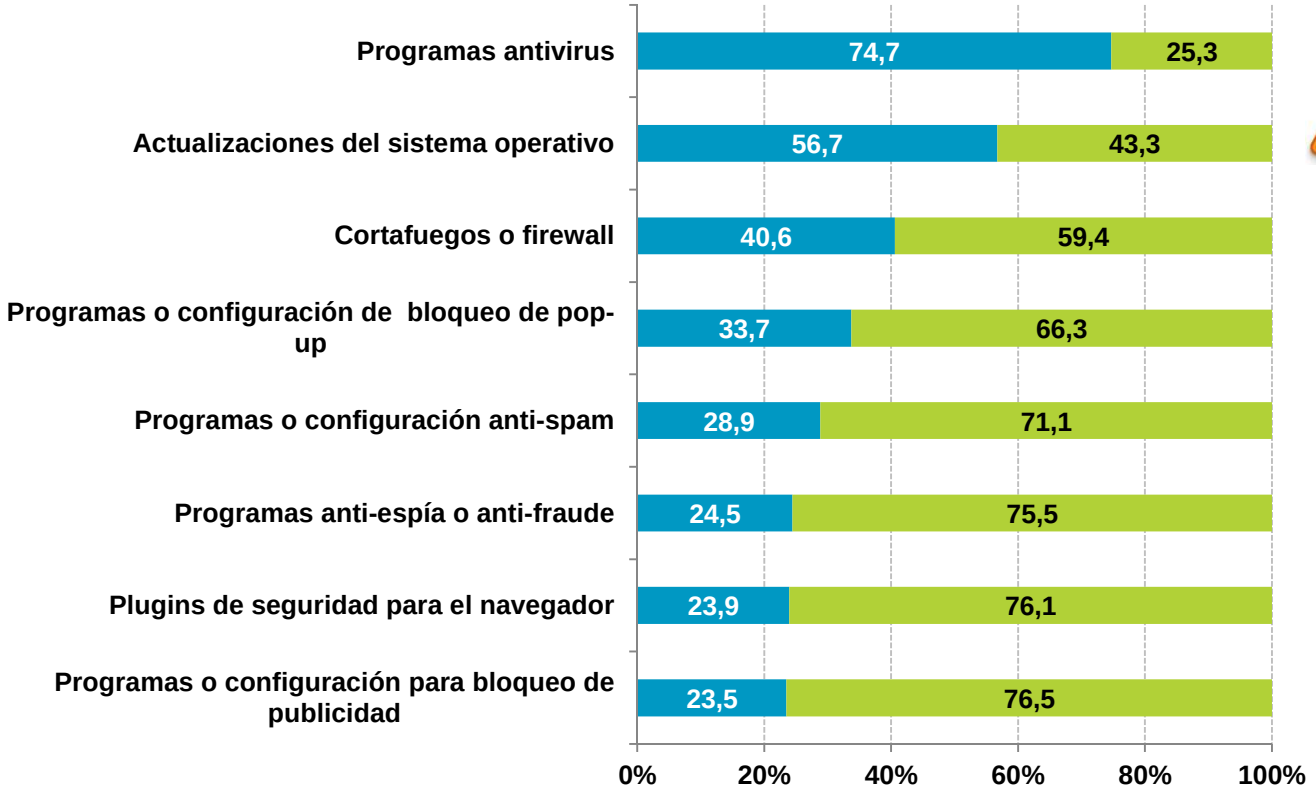
Definición y clasificación de las medidas de seguridad



Uso de medidas de seguridad en el ordenador del hogar

Medidas de seguridad automatizables

Destacan como principales medidas de seguridad automatizables el **software antivirus** (**74,7%**) y las **actualizaciones del sistema operativo** (**56,7%**).



BASE: Usuarios de PC

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

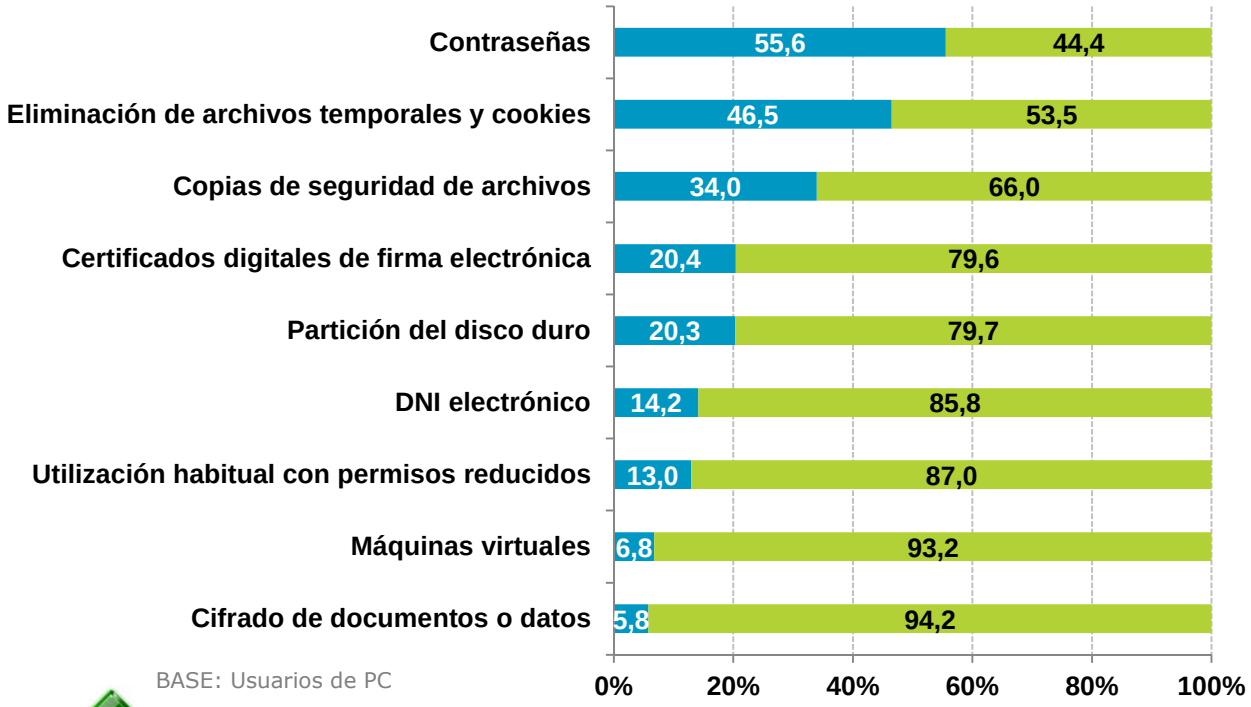
https://www.osi.es/contra-virus

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

Uso de medidas de seguridad en el ordenador del hogar

Medidas de seguridad no automatizables o activas

Más de la mitad de los usuarios declaran utilizar **contraseñas** para proteger su equipo y/o documentos, y el **46,5%** elimina los **archivos temporales y cookies** generados al navegar por Internet.



BASE: Usuarios de PC

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

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

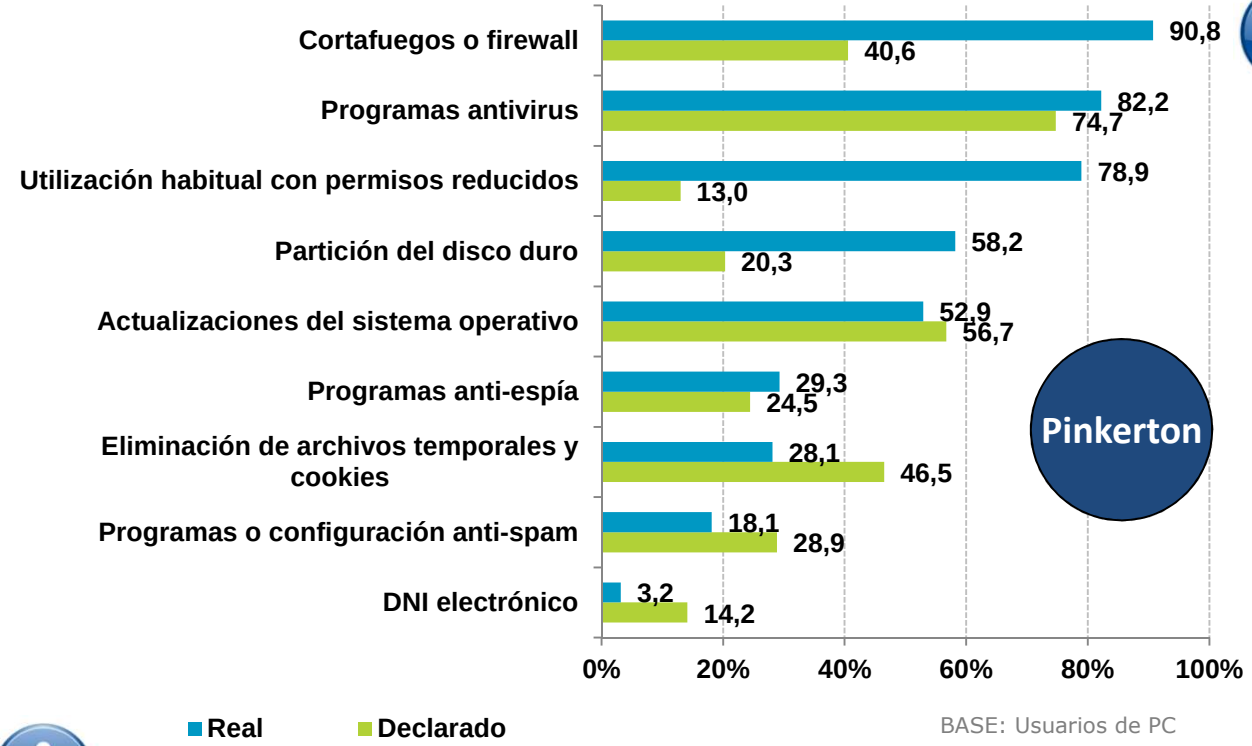
Es muy importante gestionar correctamente las contraseñas y además, realizar copias de seguridad de los datos que queremos salvaguardar. Obtén más información sobre cómo realizar estas tareas:

- ✓ **Contraseñas:** 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

El **13%** de los internautas encuestados declara el uso habitual de un **usuario con permisos reducidos** en el ordenador del hogar. Sin embargo, el dato obtenido con Pinkerton revela que realmente el **78,9%** de los equipos analizados dispone de una cuenta con **permisos limitados**.



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 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.

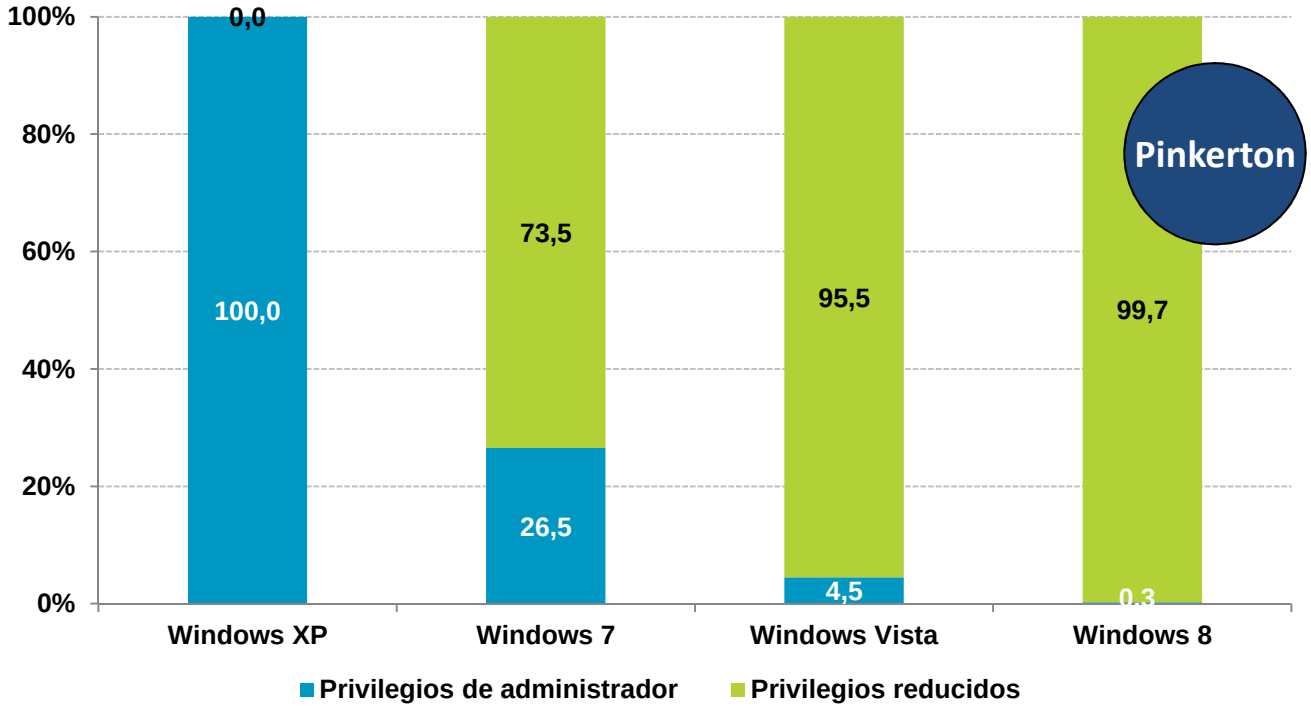
Uso de medidas de seguridad en el ordenador del hogar

Uso real de perfiles según nivel de privilegios 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

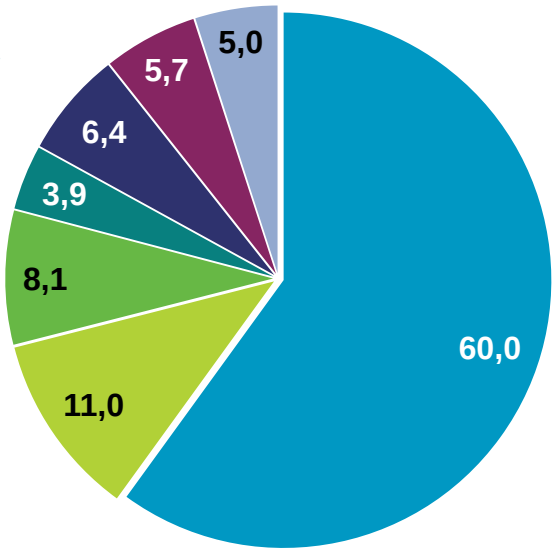


Pueden existir sistemas operativos Windows 10 identificados como otras versiones anteriores. Esto es debido al proceso de actualización llevado a cabo por Microsoft, que permite la instalación de Windows 10 sobre una versión de Windows 7, 8 u 8.1, manteniendo archivos de la antigua versión del sistema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

Frecuencia de actualización y utilización

El **60%** de los usuarios permite que la **frecuencia de actualización** de las herramientas de seguridad sea determinada de forma **automática** por las propias herramientas.

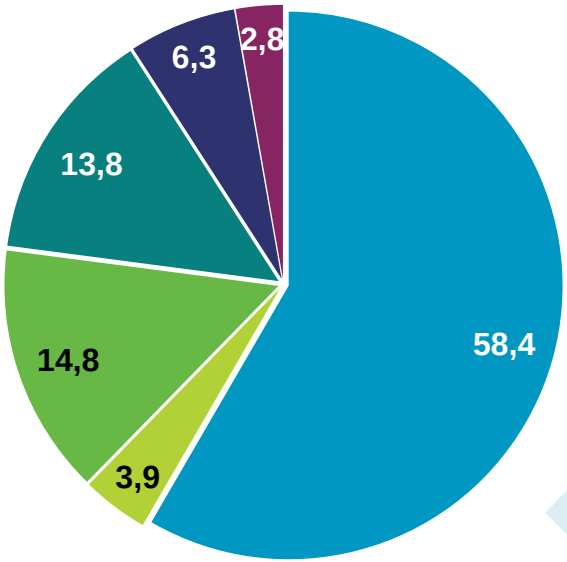
Frecuencia de actualización de herramientas de seguridad



- Mi herramienta lo hace automáticamente
- Varias veces al mes
- Una vez al mes
- Una vez cada tres meses
- Con menor frecuencia
- Nunca
- No lo sé

% individuos

BASE: Total usuarios



- Mi antivirus lo hace automáticamente
- Siempre que me conecto
- Varias veces al año
- Varias veces al mes
- Varias veces a la semana
- Nunca

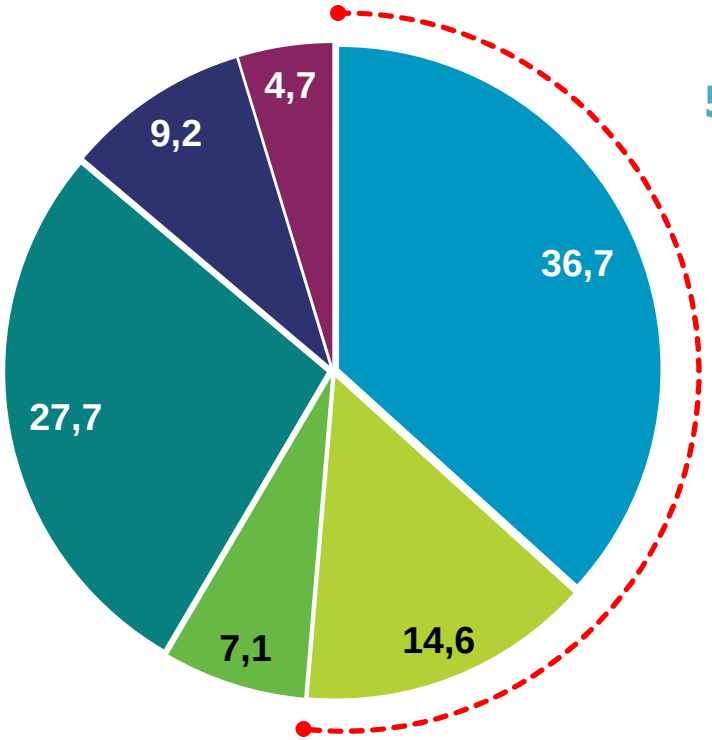
Frecuencia de escaneo con un programa antivirus

BASE: Usuarios que utilizan programas antivirus

Casi un **59% delega** en el programa antivirus la responsabilidad sobre la decisión de la **frecuencia de escaneo** de su equipo para detectar posibles infecciones de malware.

Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi

Un **13,9%** de los usuarios deja su red inalámbrica Wi-Fi **desprotegida** y/o **desconoce** su estado.



% individuos

51,3% usa **WPA** y **WPA2**

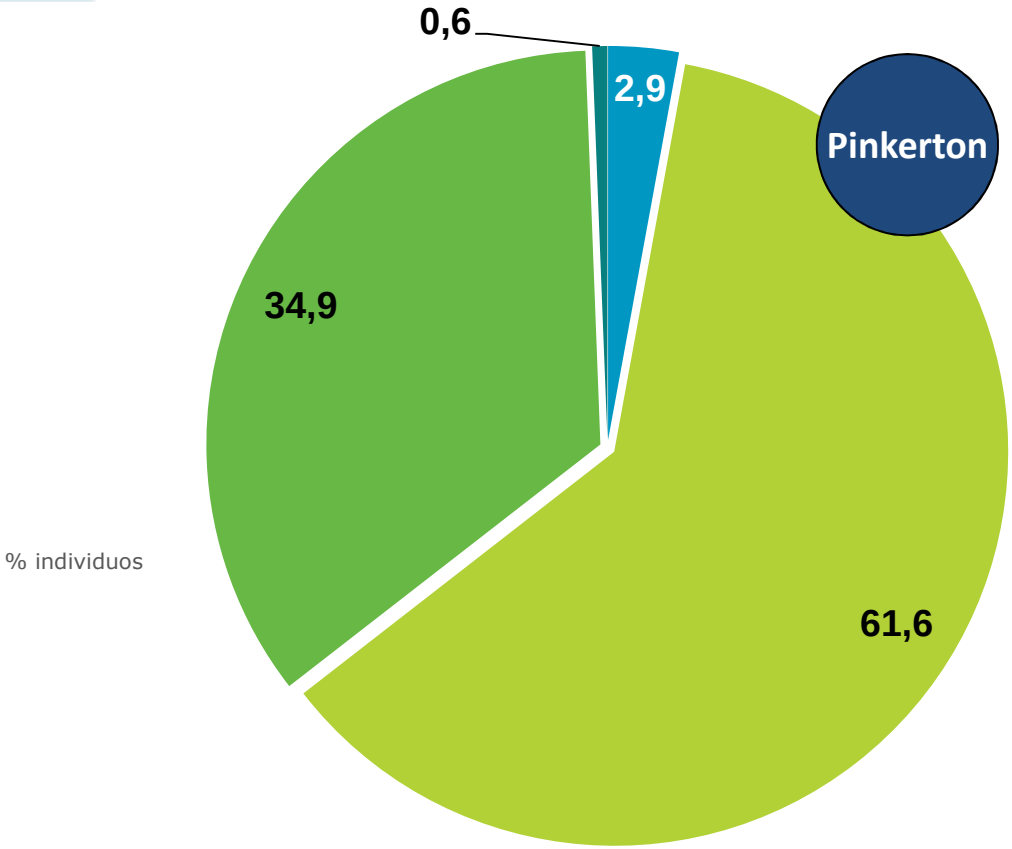
- **Estándar WPA2**
- **Estándar WPA**
- **Estándar WEP**
- **Red protegida, desconoce el sistema**
- **Desconoce si la red está protegida**
- **Red no protegida**

BASE: Usuarios Wi-Fi con conexión propia

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

Versión del sistema operativo en dispositivos Android

La gran mayoría de los smartphones y tablets analizados disponen de alguna versión de Android de la rama 4.x.



% individuos

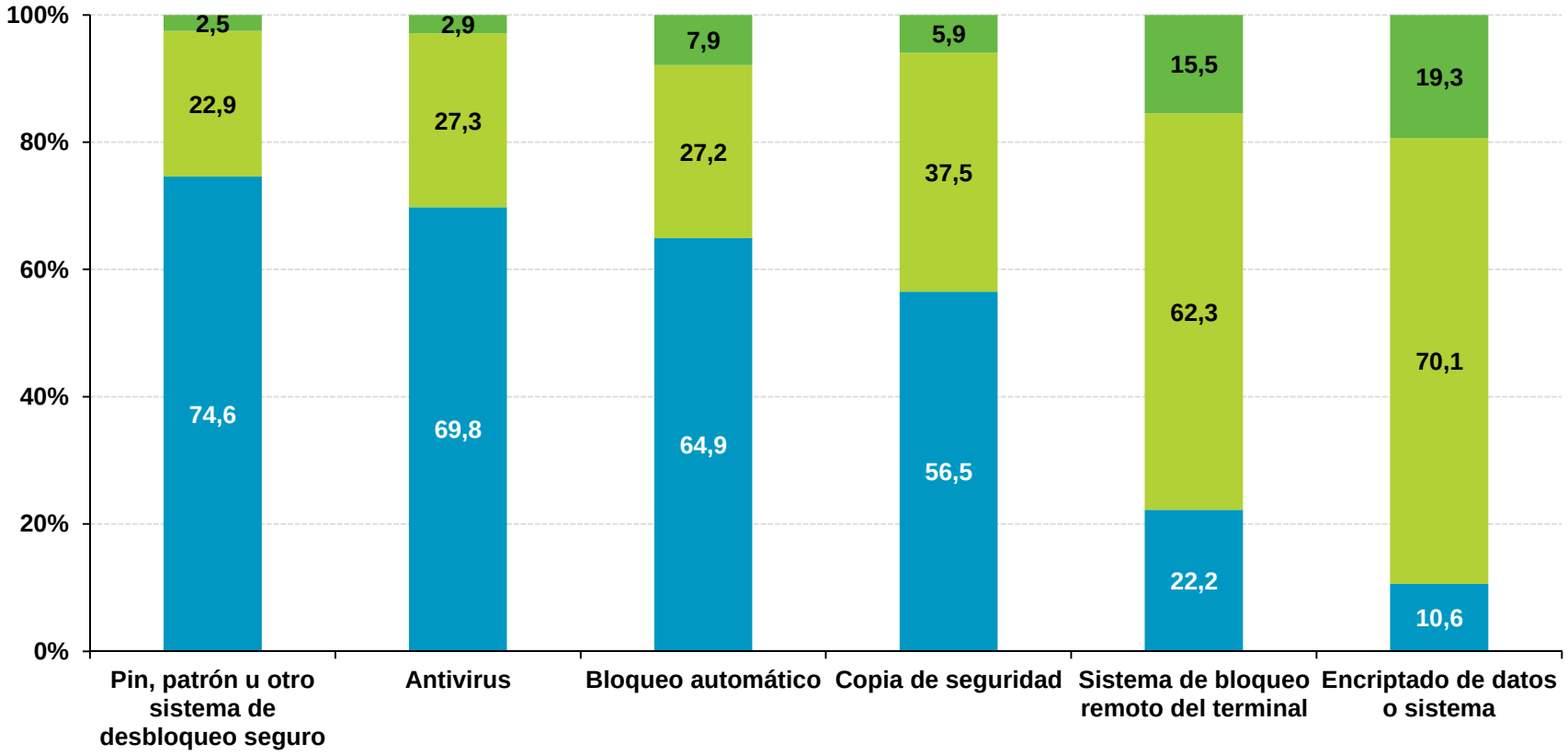
Es muy recomendable mantener el sistema operativo actualizado a la última versión disponible para evitar que el dispositivo sea vulnerable o se vea afectado por problemas y errores conocidos y corregidos en las últimas versiones de Android.

Cabe recordar que la versión de Android de la rama 4.x. ya no está atendida por Google.

BASE: Usuarios que disponen de dispositivo Android

Uso de medidas de seguridad en dispositivos Android

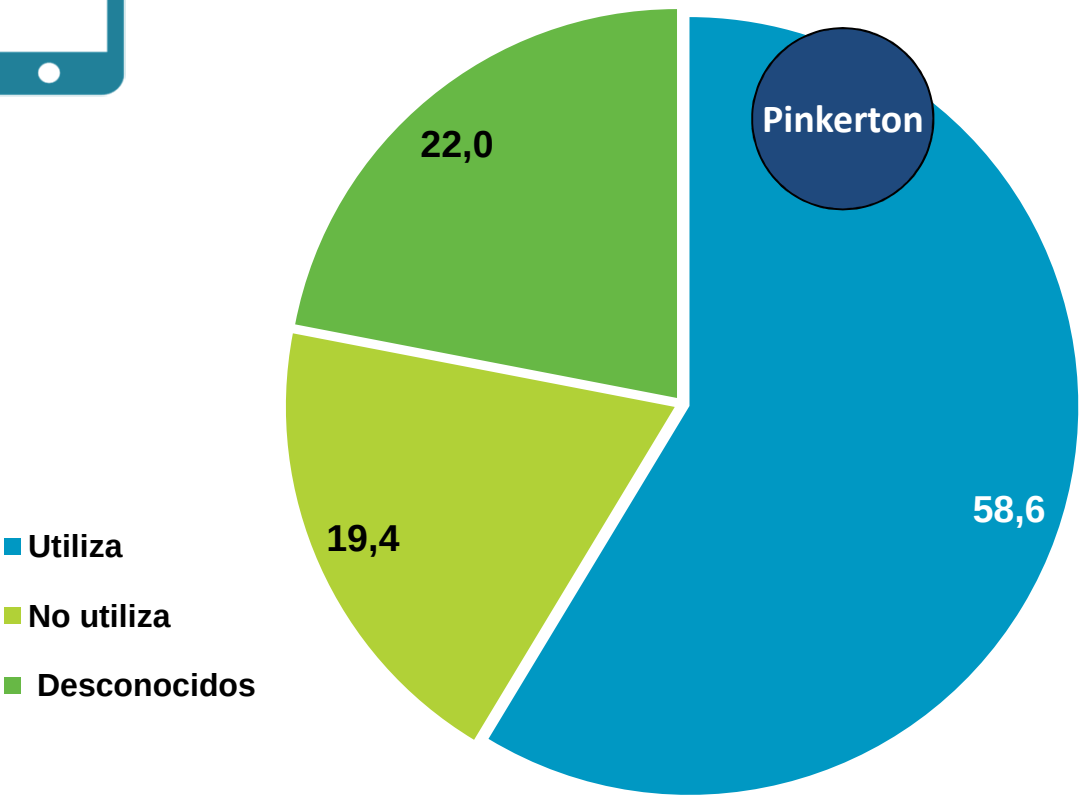
Las principales medidas de seguridad declaradas por los usuarios de dispositivos móviles son el uso de **sistemas de desbloqueo seguro** mediante PIN o patrón (**74,6%**), **software antivirus** (**69,8%**) y **bloqueo automático del dispositivo** tras periodo de inactividad (**64,9%**).



BASE: Usuarios que disponen de dispositivo Android

Uso de medidas de seguridad en dispositivos Android

El **58,6%** utiliza el móvil con privilegios limitados, frente a un **19,4%** que sí tiene privilegios de administrador o mecanismos para obtenerlos.



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

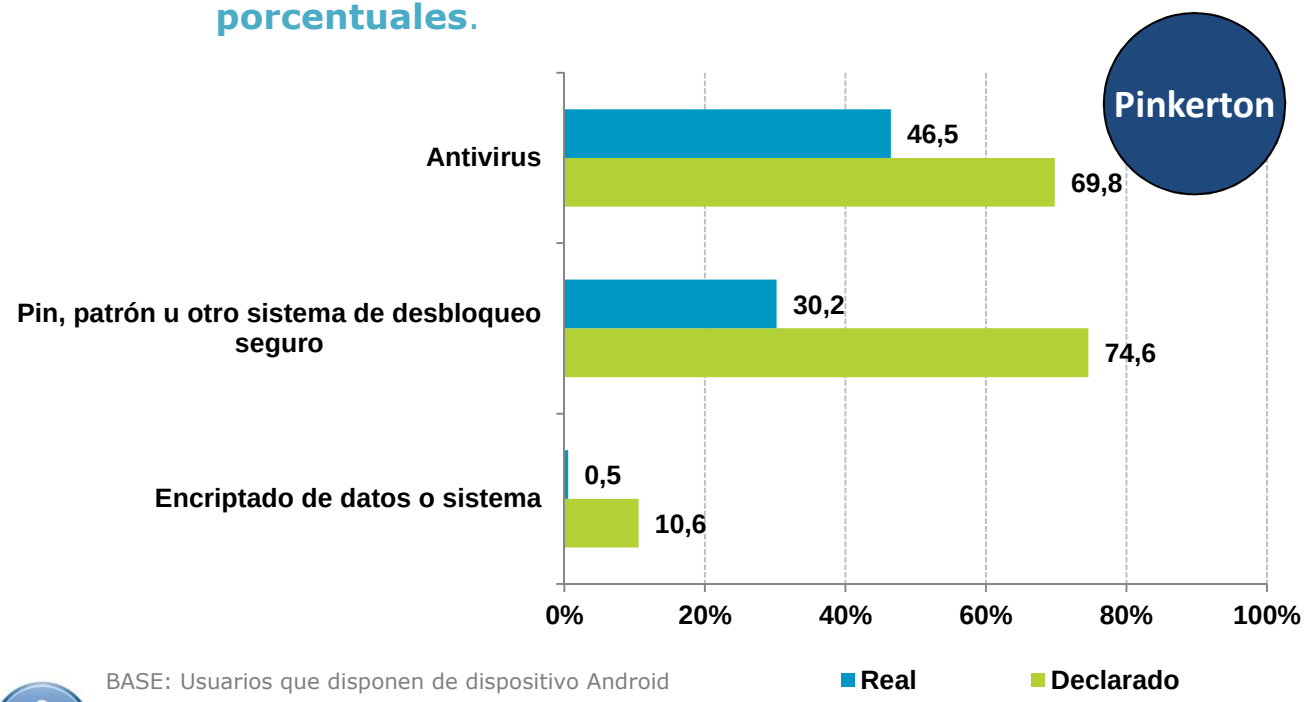
Los privilegios de administrador del dispositivo Android se obtiene mediante métodos indirectos.

Uso de medidas de seguridad en dispositivos Android

Uso de medidas de seguridad declarado vs. real

Casi un **70%** de los internautas encuestados afirma utilizar un programa **antivirus** en su dispositivo móvil, mientras que el dato aportado por **Pinkerton** sitúa la utilización real en **23,3 puntos porcentuales** por debajo.

El **PIN, patrón, u otro sistema seguro de desbloqueo seguro** es la medida **más distanciada entre el uso real y declarado**, siendo superior a **44 puntos porcentuales**.



BASE: Usuarios que disponen de dispositivo Android

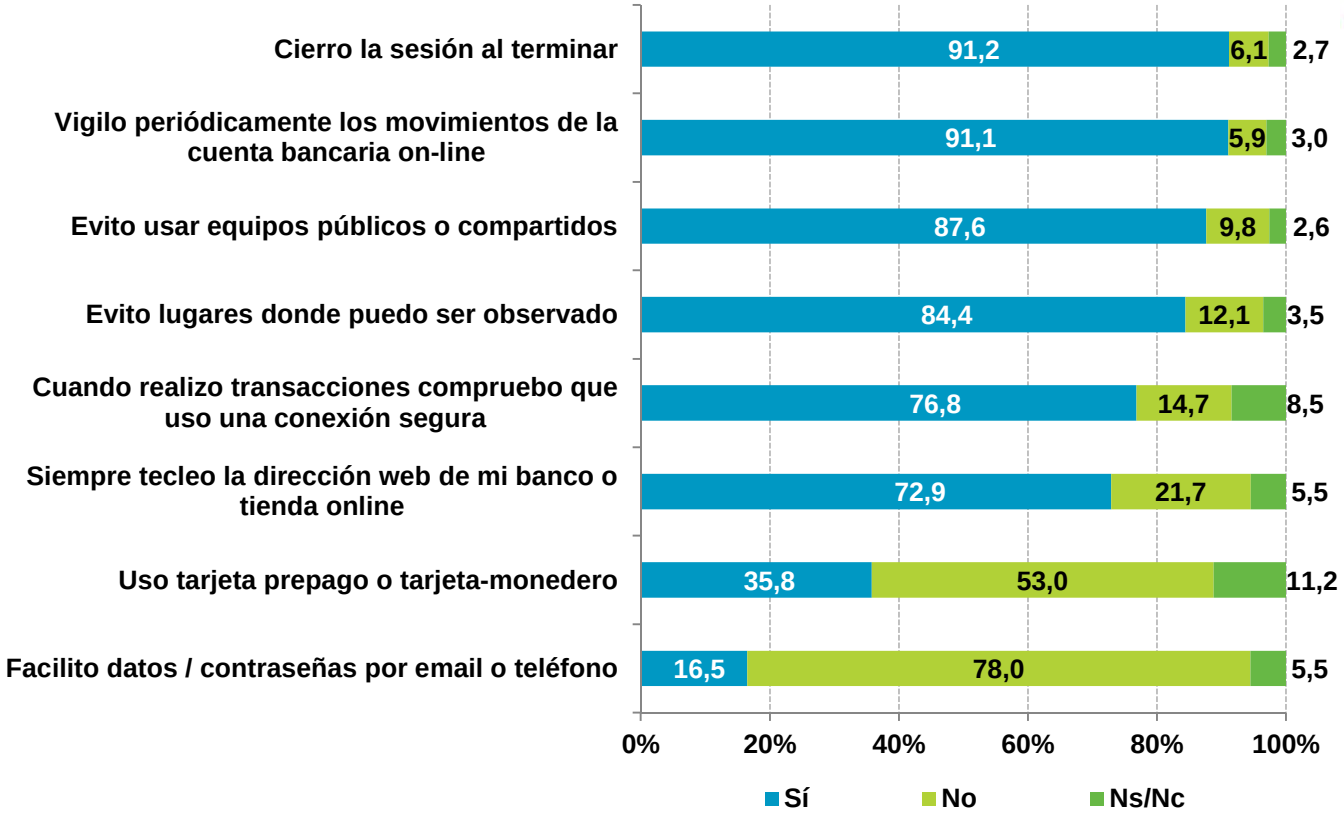
La utilización de un sistema de desbloqueo seguro mediante **patrón, PIN, sistemas biométricos**, etc., permite evitar de manera sencilla los **accesos no autorizados o no deseados** al dispositivo móvil y su contenido, **protegiendo la privacidad del usuario**.

El **encriptado** o **cifrado** de datos o sistema permite almacenar el contenido del dispositivo codificado, de manera que solo se puede acceder a el 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.

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

Banca en línea y comercio electrónico

Los usuarios de los **servicios de banca y comercio a través de Internet** mantienen buenos hábitos de comportamiento en general. Las **tarjetas prepago o monedero**, es el menos utilizado, por un **35,8%** de usuarios de dichos servicios.



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

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

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

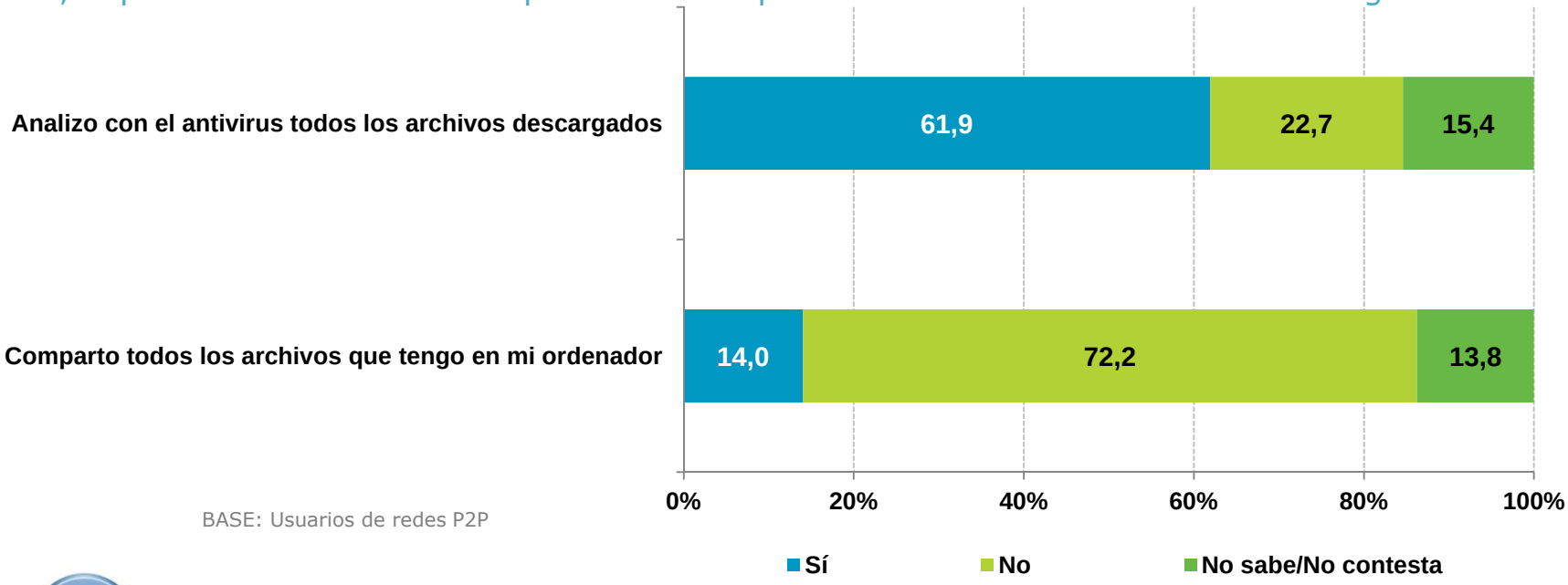
Medidas para protegerte al realizar trámites on-line: https://www.osi.es/pagos-online

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

Redes P2P

El **61,9%** de los panelistas declara **analizar** con el antivirus cualquier fichero descargado a través de redes P2P antes de abrirlo.

Por otro lado, el **14%** declara **compartir todos los ficheros** del equipo informático en las redes P2P, exponiendo su información privada a cualquier usuario de estas redes de descarga.



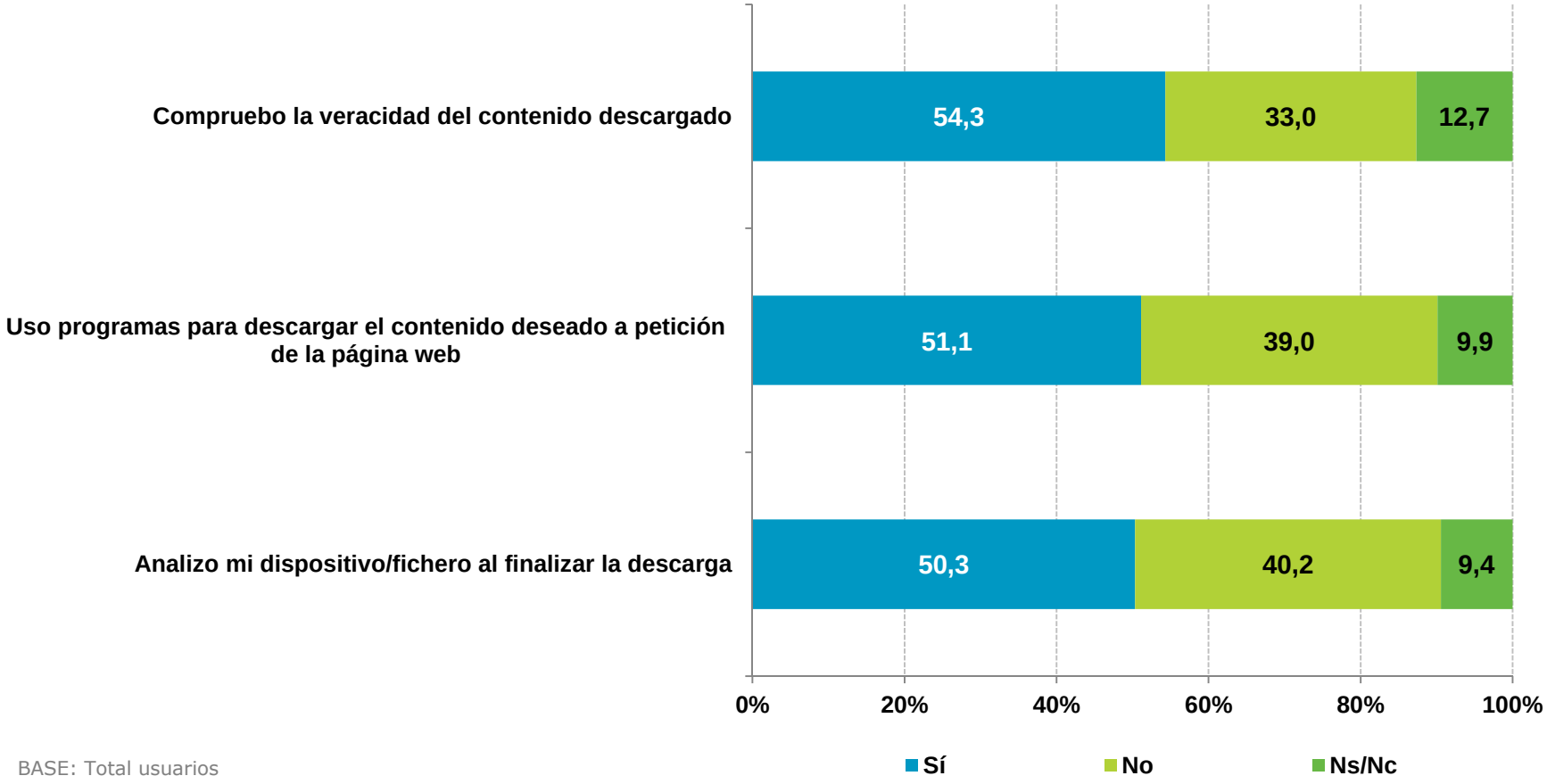
BASE: Usuarios de redes P2P

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.

Descarga directa

El **54,3%** de los panelistas declara **comprobar la veracidad del contenido descargado** (dirección del sitio web, tipo de fichero, hash del fichero, etc.) antes de abrirlo.

Por otro lado, más de la mitad **51,1%** afirma **utilizar programas para descargar el contenido a petición del sitio web**, exponiendo su equipo a infecciones de malware.

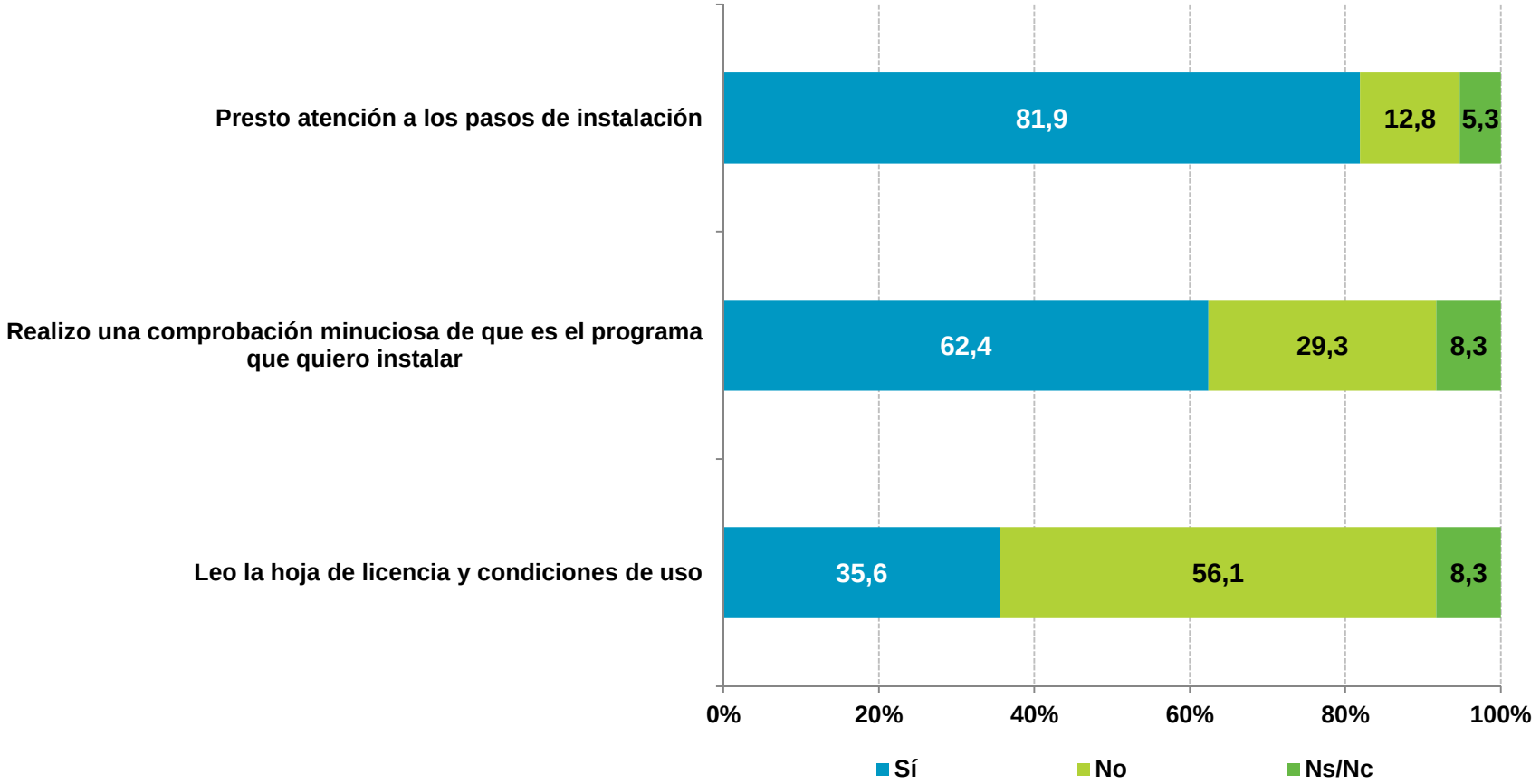


BASE: Total usuarios

Instalación de software descargado

La gran mayoría de los panelistas (**81,9%**) declara **prestar atención a los pasos de instalación del software**.

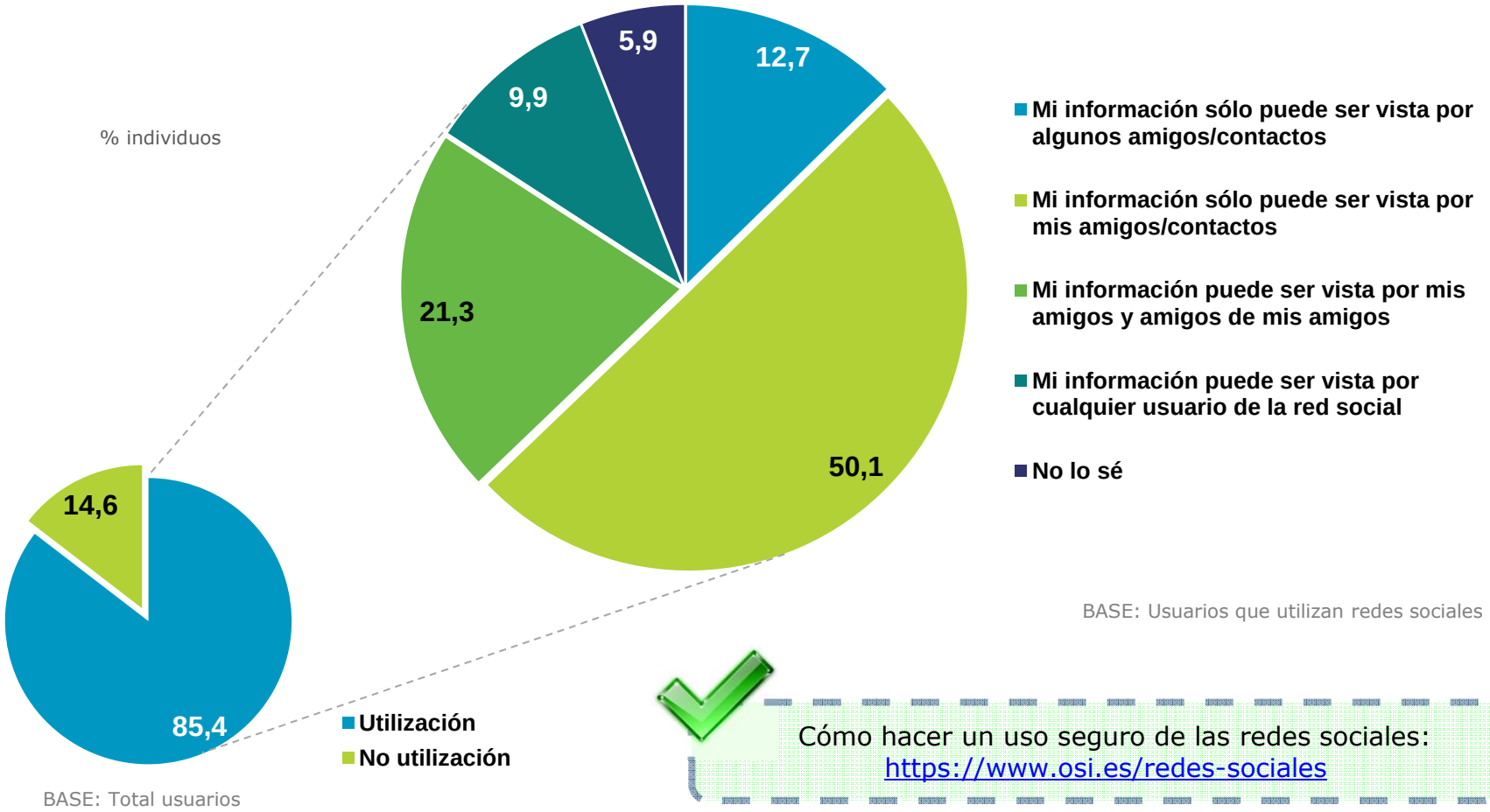
Únicamente 1 de cada 3 usuarios lee la licencias y/o condiciones de uso al instalar un programa.



BASE: Usuarios de PC

Redes sociales

La mitad (**50,1%**) de los usuarios de redes sociales configura su perfil para que solo sea accesible por sus amigos y contactos. Sin embargo el **31,2%** (21,3 + 9,9) **expone los datos** publicados en su perfil a **terceras personas y/o desconocidos**, e incluso un **5,9%** de los consultados declara **desconocer** el nivel de privacidad de su perfil.

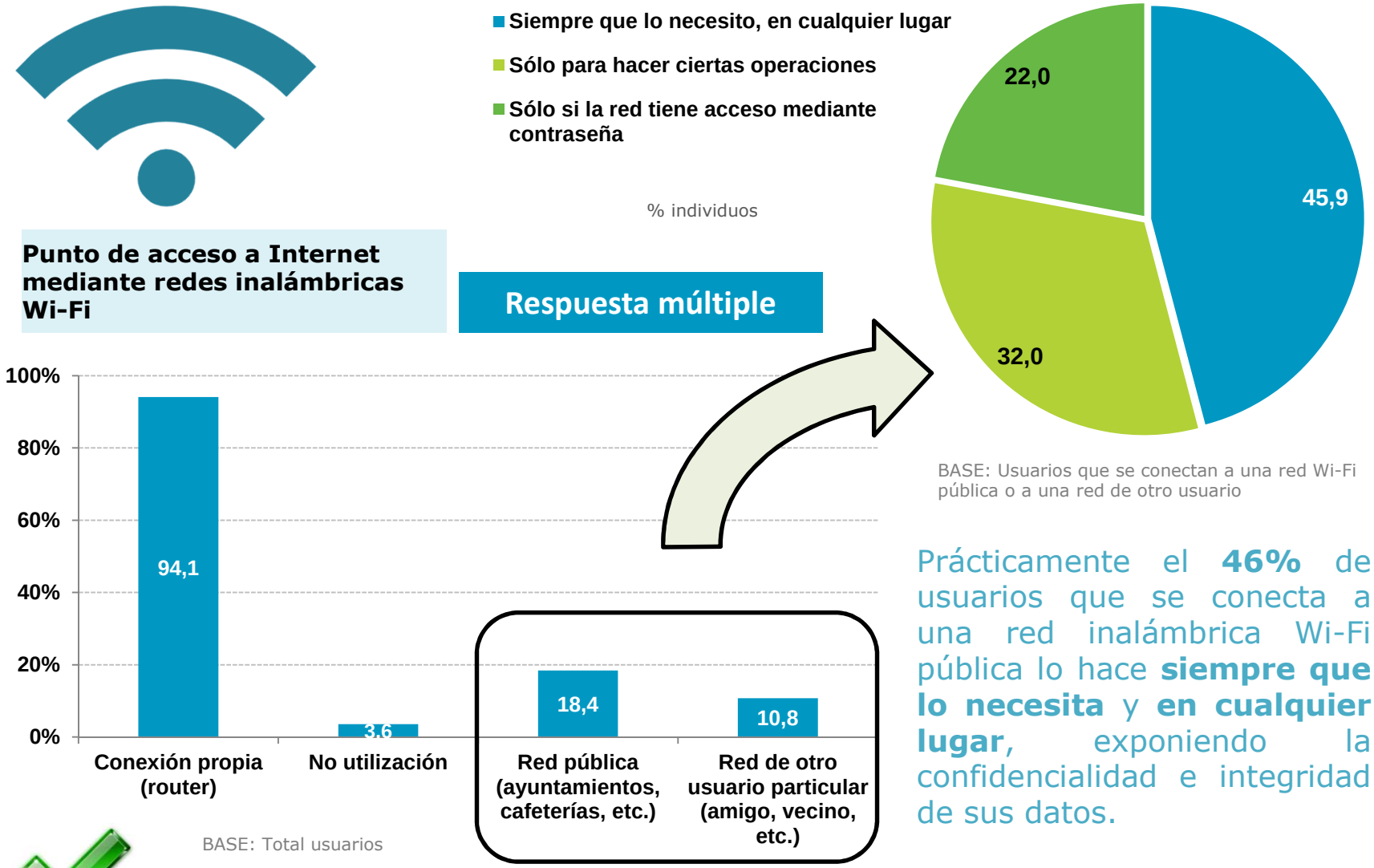


Cómo hacer un uso seguro de las redes sociales:
https://www.osi.es/redes-sociales

Hábitos de uso de las redes inalámbricas Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Respuesta múltiple

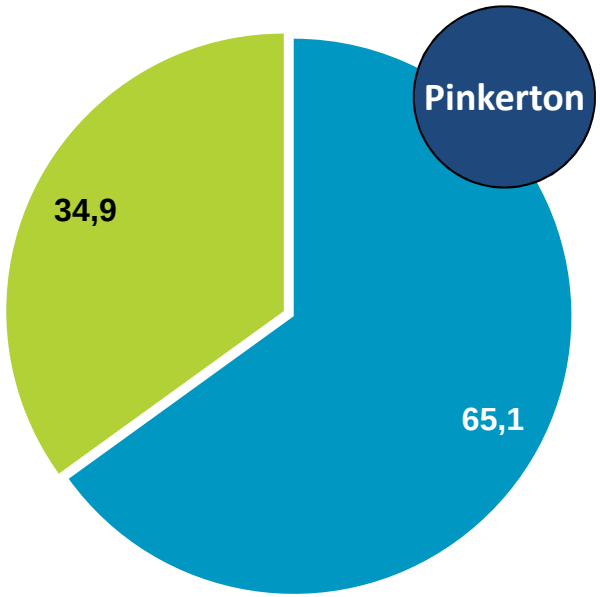


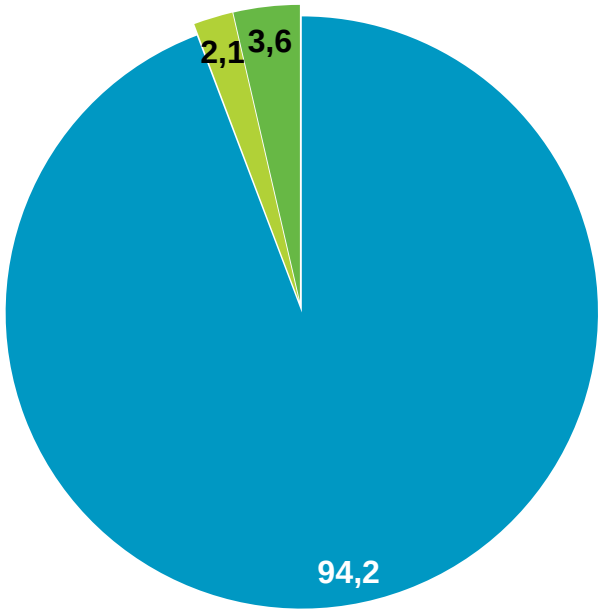
Prácticamente el **46%** de usuarios que se conecta a una red inalámbrica Wi-Fi pública lo hace **siempre que lo necesita** y **en cualquier lugar**, exponiendo la confidencialidad e integridad de sus datos.

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

Hábitos de uso en dispositivos Android

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





% individuos

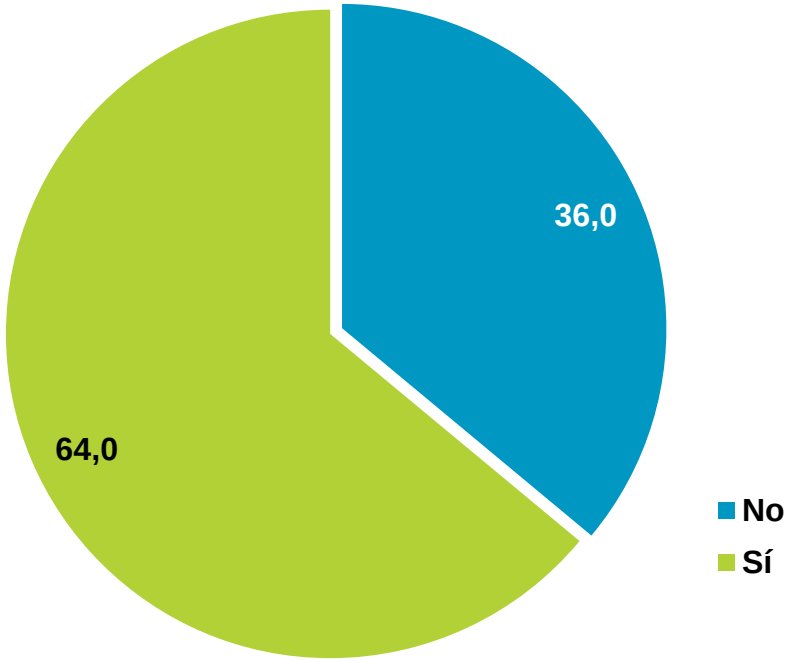
La mayoría (**94%**) de usuarios de smartphones y tablets Android declara realizar descargas de aplicaciones desde los **repositorios oficiales.**

Sin embargo **más de un tercio** (**34,9%**) de los dispositivos Android analizados están configurados para permitir la instalación de aplicaciones desde **fuentes desconocidas**.

BASE: Usuarios que disponen de dispositivo Android

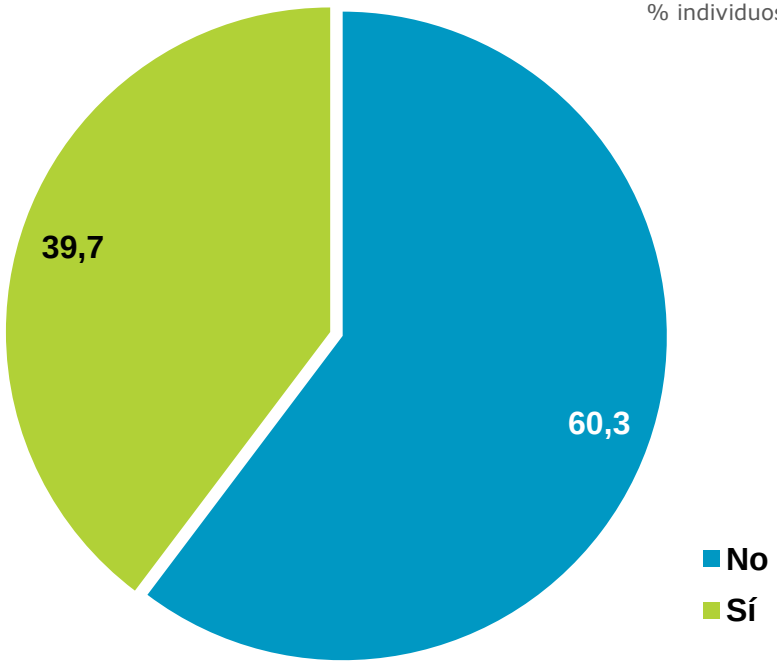
Hábitos de uso en dispositivos Android

Comprobación de permisos al instalar una aplicación



BASE: Usuarios de dispositivos Android que descargan aplicaciones

% individuos



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: Usuarios que disponen de dispositivo Android

Incidentes de seguridad

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

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/

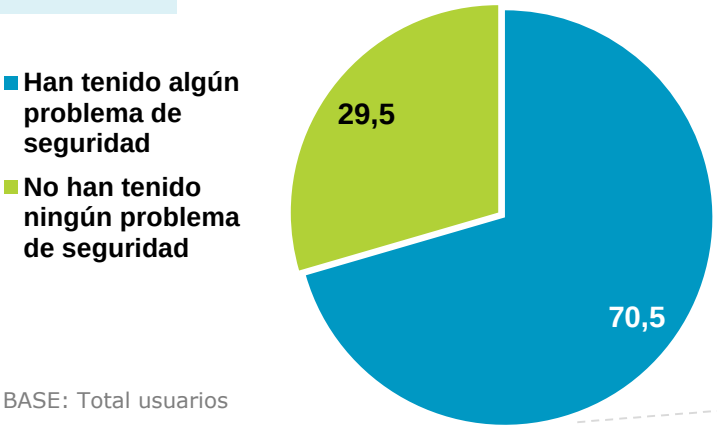
Incidencias de seguridad

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:

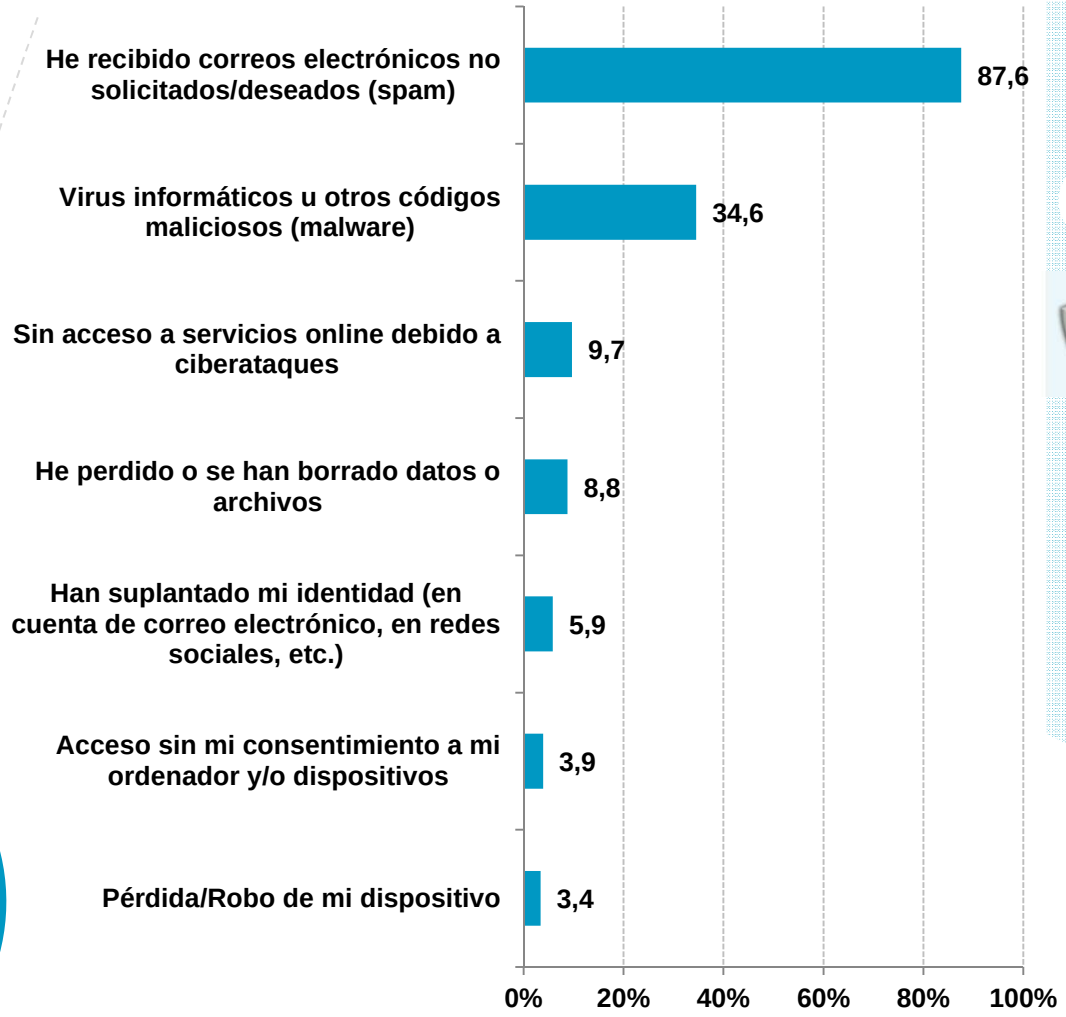
% individuos



BASE: Total usuarios

Incidencias sufridas:

Respuesta múltiple

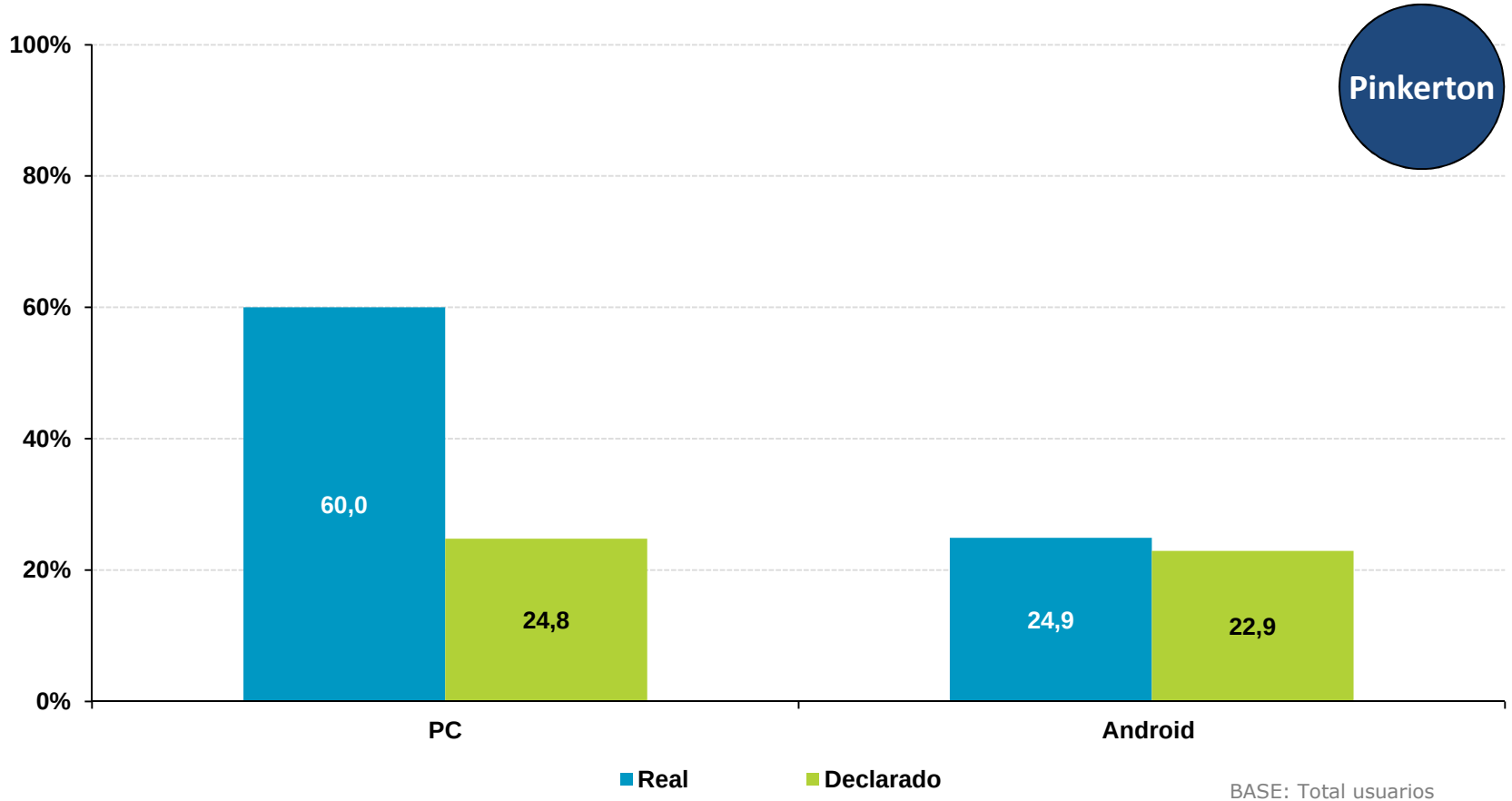


BASE: Usuarios que han sufrido alguna incidencia de seguridad

Evolución de los incidentes por malware

Existe una diferencia superior a **35 puntos porcentuales** entre la percepción de los usuarios con respecto a las infecciones de sus ordenadores personales y las infecciones reales que revela el análisis de Pinkerton.

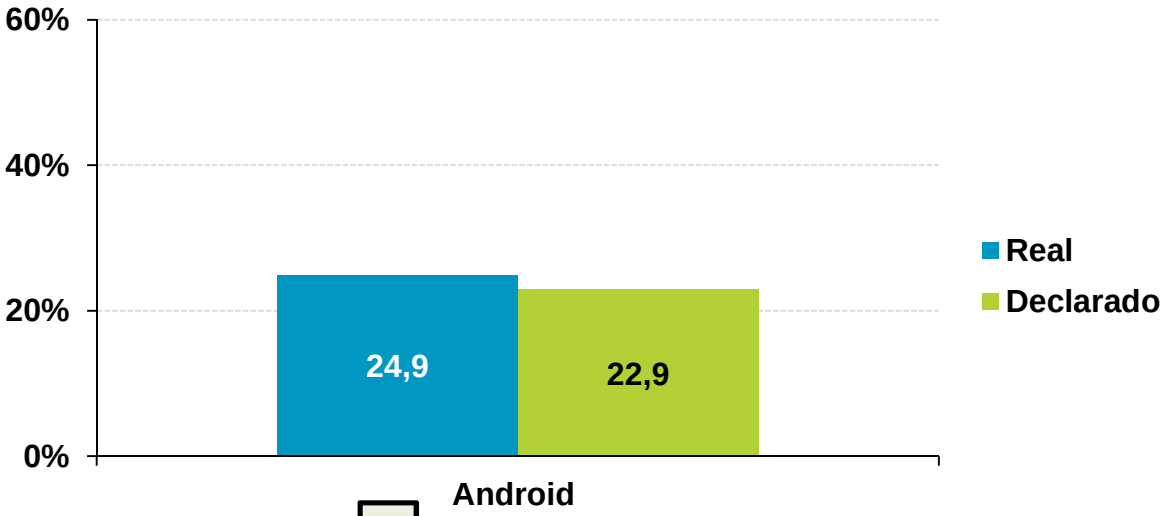
Esta diferencia es menor entre los usuarios de dispositivos Android, apenas hay **2 puntos porcentuales** de diferencia entre las infecciones declaradas y las reales.



BASE: Total usuarios

Incidentes por malware en Android

Aunque los porcentajes entre los que declararon tener malware y los que realmente los tenían son similares, realmente sólo **entre el 4,9% de los dispositivos analizados coincidió la presencia de malware y la percepción del usuario de la infección**.



BASE: Total usuarios

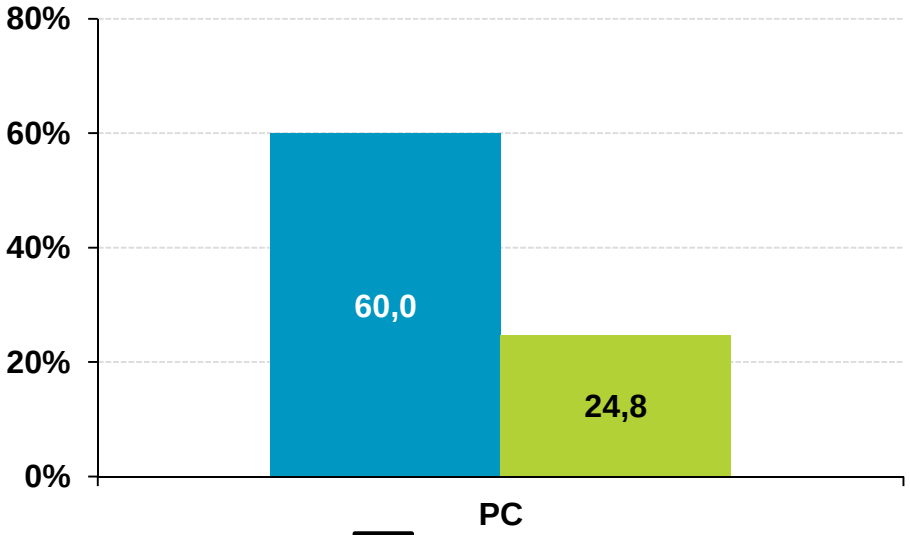
Declararon tener malware	Su Android presentaba malware		
	Sí	No	Total
Sí	4,9	18,2	23,1*
No	20,0	56,9	76,9
Total	24,9	75,1	100,0

BASE: Total usuarios con dispositivo escaneado

*Nota: El 22,9% corresponde a todos los que respondieron en la encuesta tener malware mientras que el 23,1% hace referencia a los usuarios que declararon esto mismo y cuyo dispositivo Android ha sido escaneado

Incidentes por malware en PC

Entre los ordenadores analizados el **15,2% presentaba virus y sus usuarios declararon tenerlos**.



BASE: Total usuarios

Declararon tener malware	Su PC presentaba malware		
	Sí	No	Total
Sí	15,2	8,9	24,1*
No	44,8	31,1	75,9
Total	60,0	40,0	100,0

BASE: Total usuarios con dispositivo escaneado

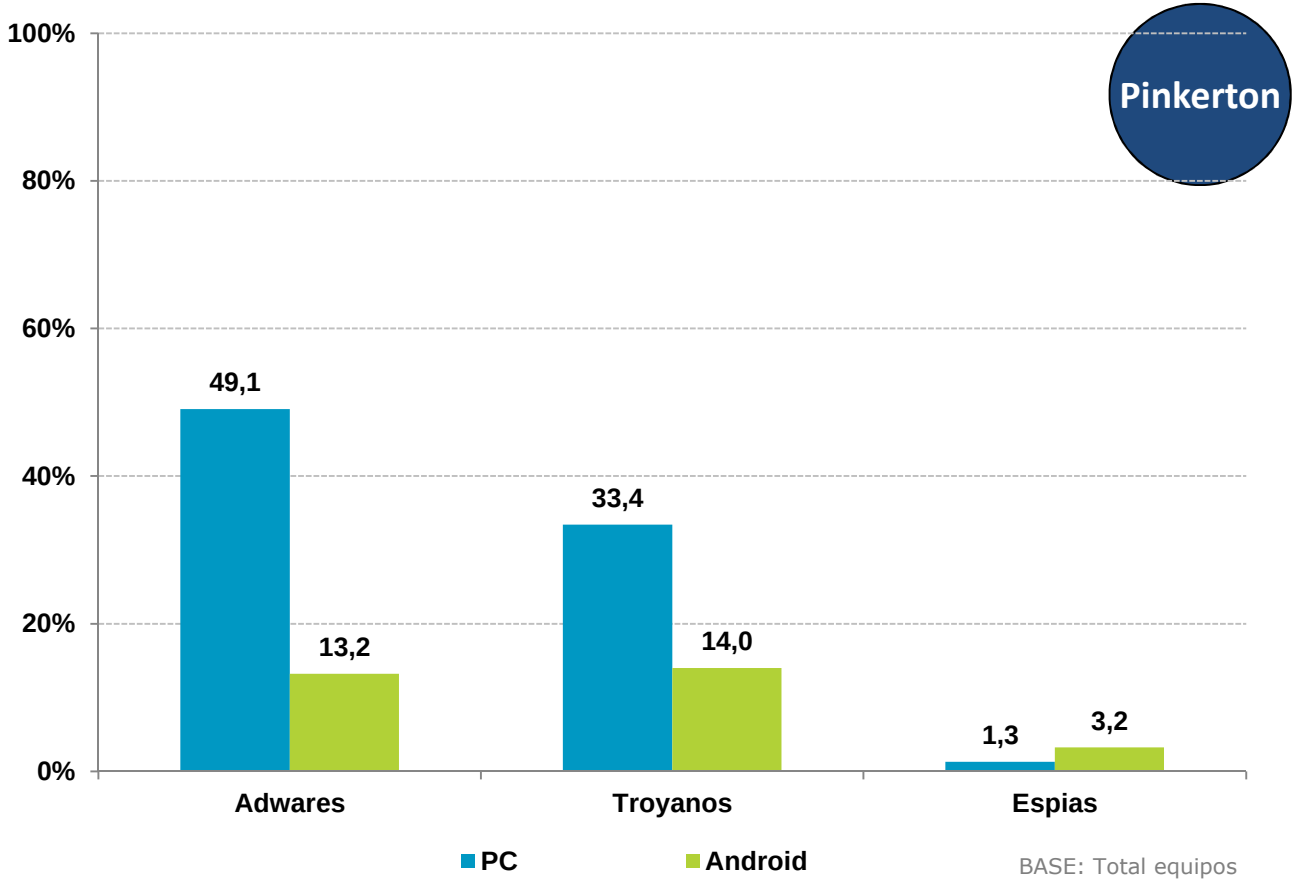
*Nota: El 24,8% corresponde a todos los que respondieron en la encuesta tener malware mientras que el 24,1% hace referencia a los usuarios que declararon esto mismo y cuyo PC ha sido escaneado

Tipología del malware detectado

El malware con mayor presencia en los equipos informáticos es aquel cuyo cometido es lograr un beneficio económico: **troyanos** y **adware publicitarios**.

Los adwares publicitarios se han detectado en el **49,1%** de los ordenadores analizados y el **13,2%** de los dispositivos Android. El nivel de detección de los **troyanos** es algo inferior entre los ordenadores, encontrándose en **un tercio** de estos, y de nivel similar (**14%**) en los dispositivos Android analizados.

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

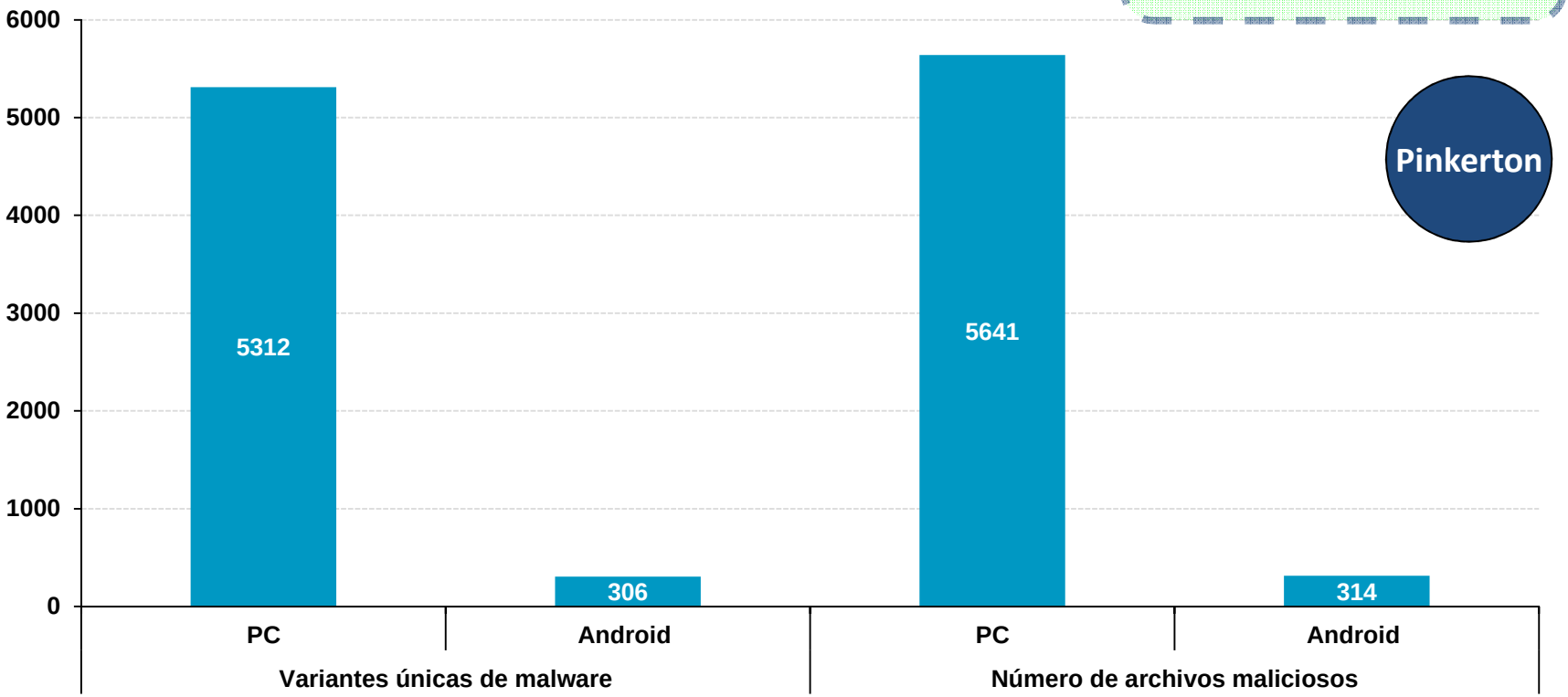
BASE: Total equipos

Diversificación del malware detectado

Número total de archivos maliciosos y variantes únicas detectadas en PC y Android

La gran variedad y personalización de código malicioso se manifiesta en el hecho de que el **94,1%** de los archivos maliciosos detectados en ordenadores personales y el **97,4%** en dispositivos Android son **variantes únicas**.

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



BASE: Total equipos

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.).

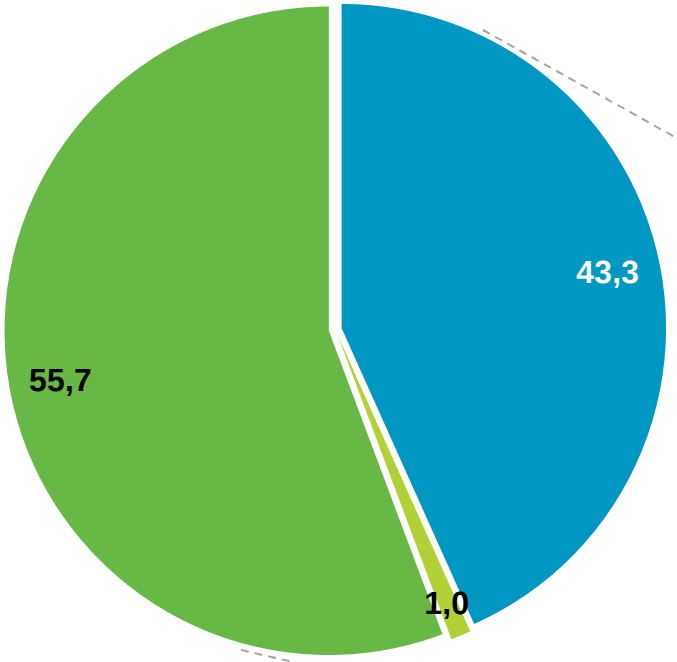
Peligrosidad baja: se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, *hacking tools*, etc.). En la mayoría de los casos son herramientas instaladas por el usuario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

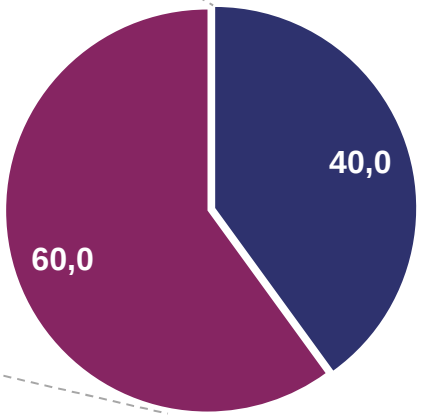
Tres de cada cinco ordenadores de los hogares españoles analizados con Pinkerton se encuentran infectados con al menos una muestra de malware conocida. De estos, un **55,7%** presentan un nivel de **riesgo alto** debido al potencial peligro que suponen los archivos maliciosos encontrados en ellos.



Riesgo bajo
Riesgo medio
Riesgo alto

Pinkerton

BASE: Total ordenadores infectados



No infectados
Infectados

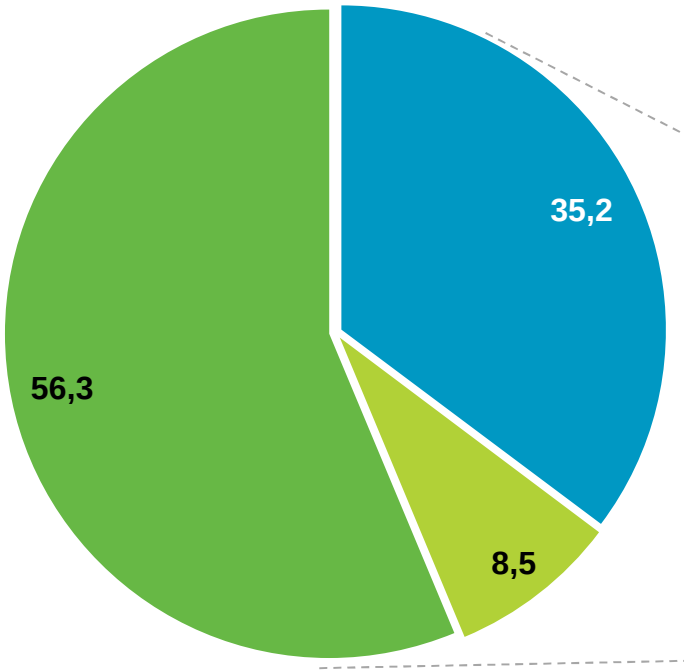
BASE: Total ordenadores

4

Peligrosidad del código malicioso y riesgo del equipo

Dispositivos Android

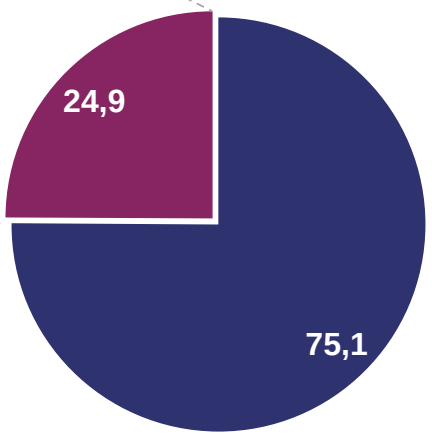
Prácticamente un cuarto de los dispositivos Android analizados con Pinkerton se encuentran infectados con al menos una muestra de malware conocida, de los cuales un **56,3%** presentan un nivel de **riesgo alto**.



BASE: Total dispositivos Android infectados

Pinkerton

Riesgo bajo
Riesgo medio
Riesgo alto



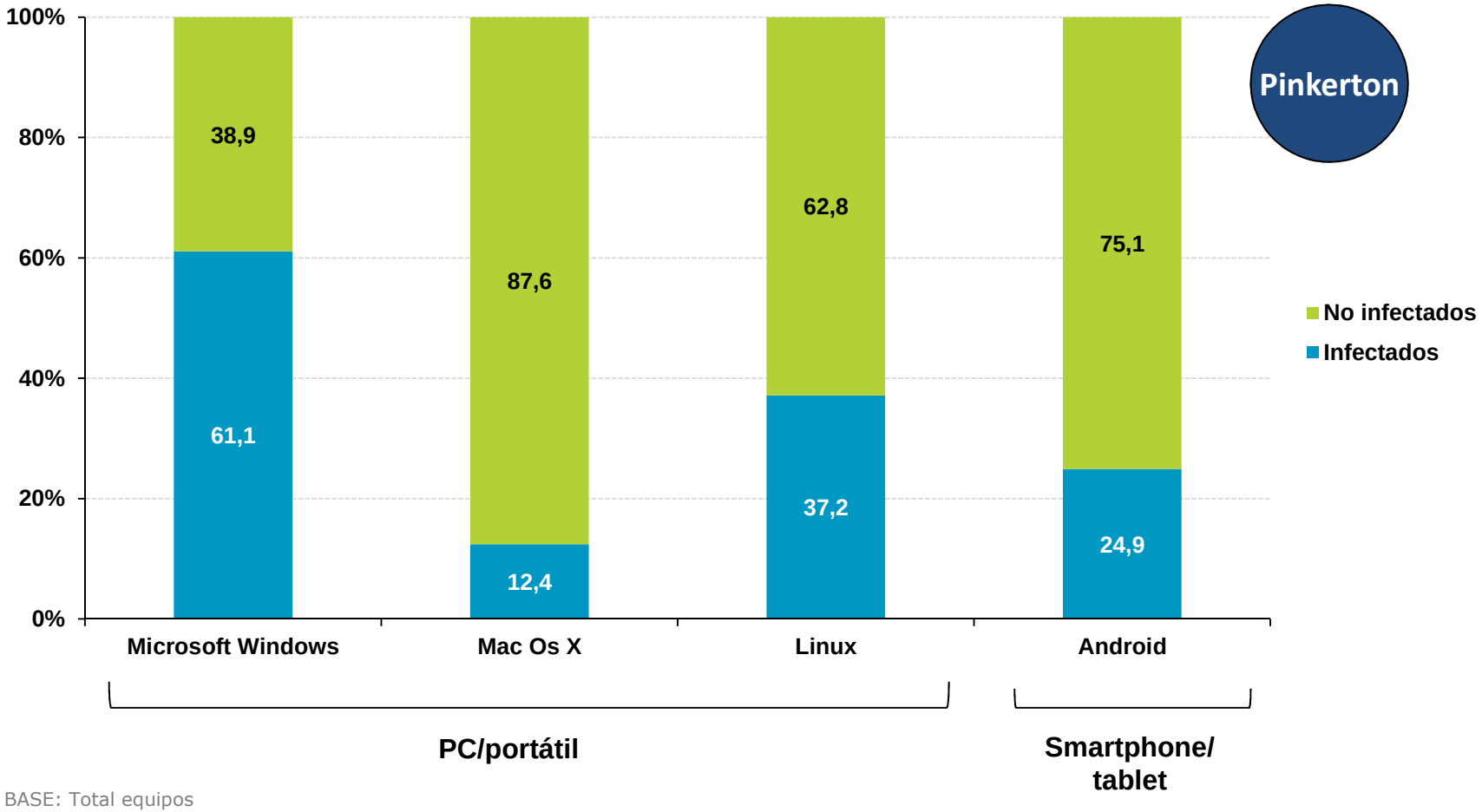
No infectados
Infectados

BASE: Total dispositivos Android

Malware vs. sistema operativo

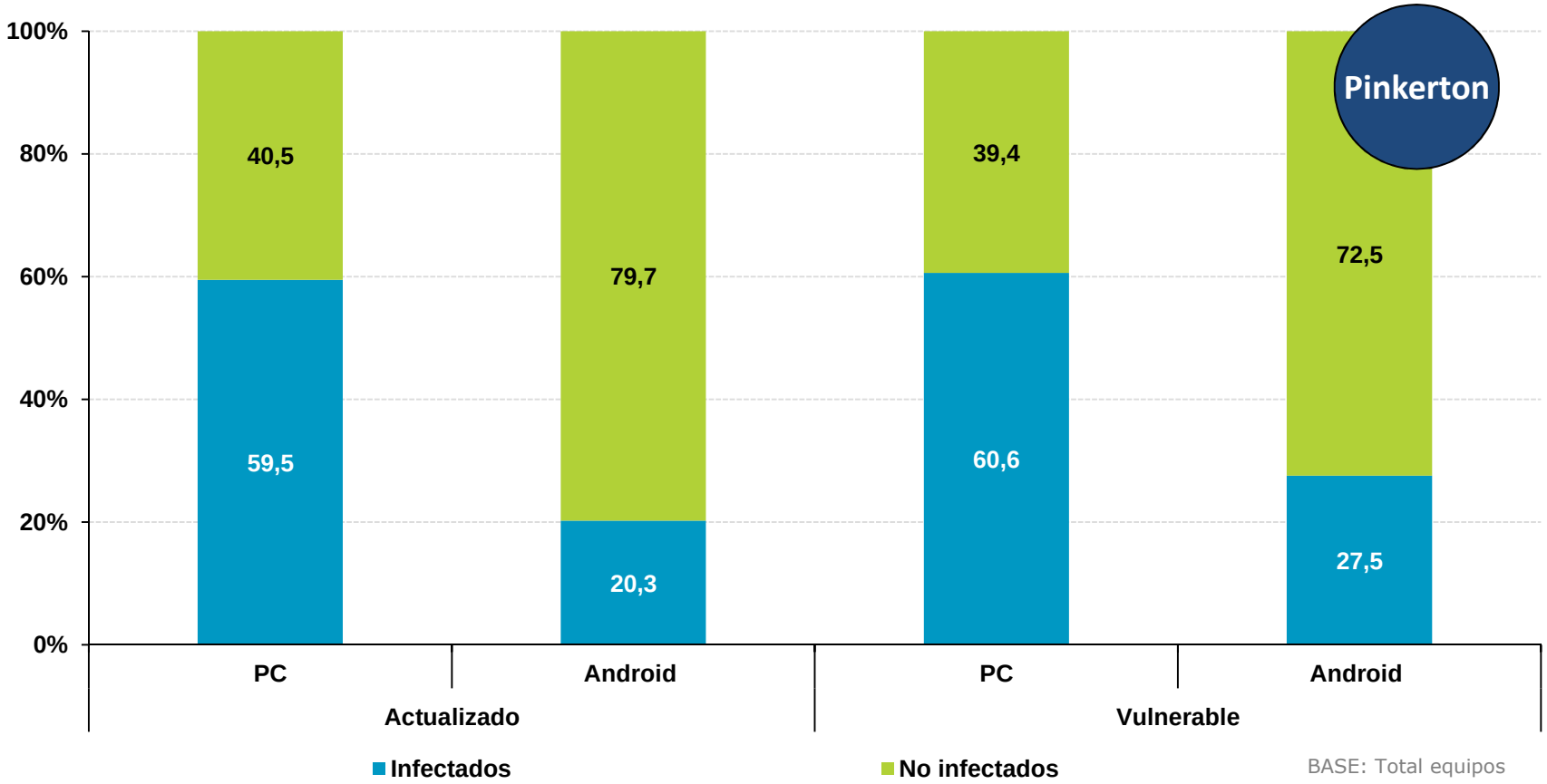
Pinkerton detecta malware en más del **61%** de los equipos basados en **Microsoft Windows.**

Tan solo en uno de cada cuatro (**24,9%**) dispositivos **Android** se detecta algún tipo de malware conocido.



BASE: Total equipos

Malware vs. actualización del sistema



BASE: Total equipos

Atendiendo al estado de actualización de las máquinas analizadas, se puede observar que en los dispositivos Android existe una mayor brecha que en los sistemas de escritorio, superando los **7 puntos porcentuales** de diferencia.

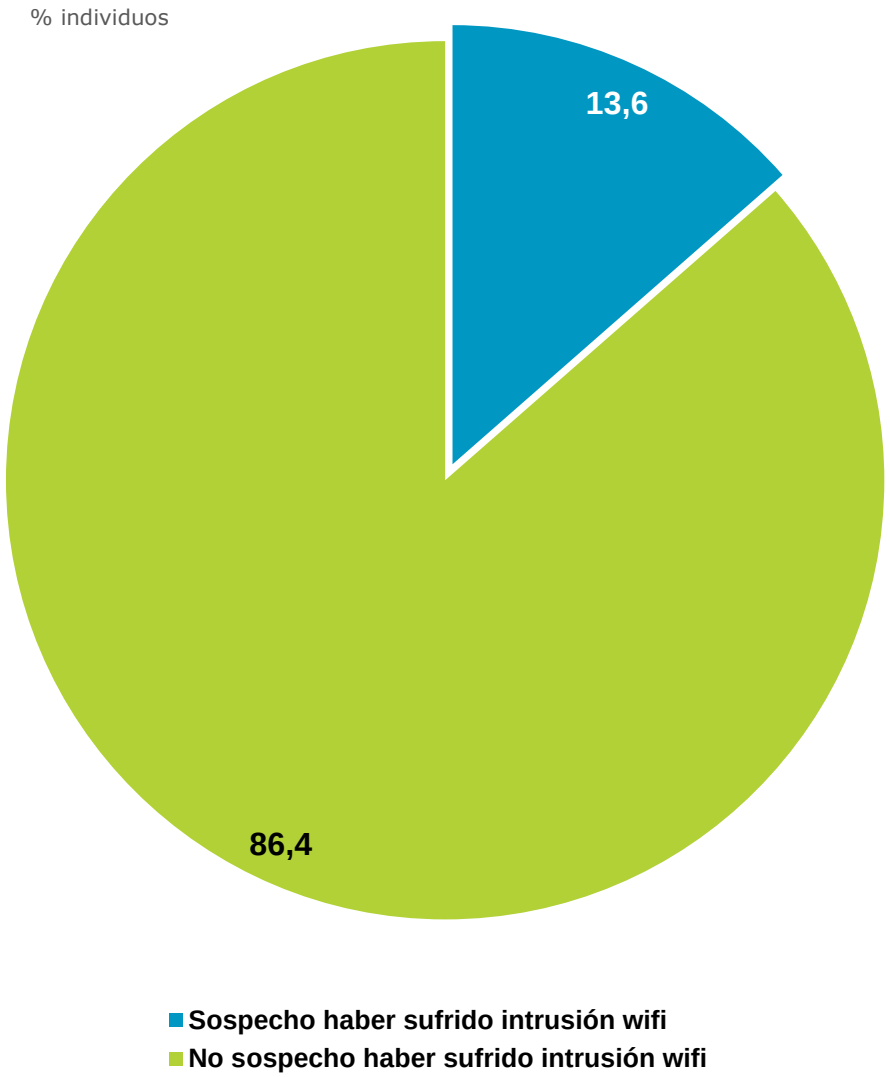
Además existe una mayor penetración de malware en aquellos dispositivos que no se encuentran actualizados, lo que demuestra el aprovechamiento de vulnerabilidades en el proceso de infección.

Incidencias de seguridad en redes inalámbricas Wi-Fi

Un **13,6%** de panelistas *sospechan* que pueden haber sufrido una **intrusión en la red inalámbrica Wi-Fi** de su hogar.

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

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



BASE: Usuarios con conexión Wi-Fi propia

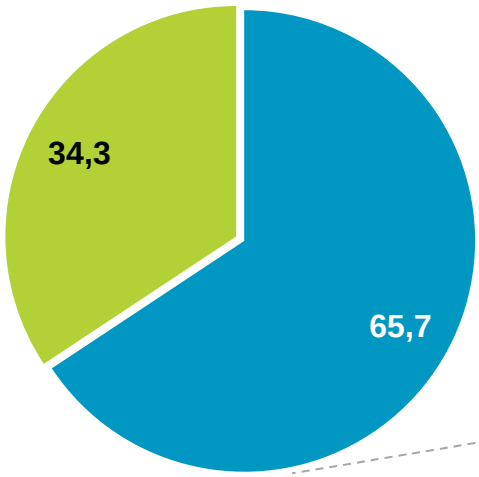
Consecuencias de los incidentes de seguridad y reacción de los usuarios

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

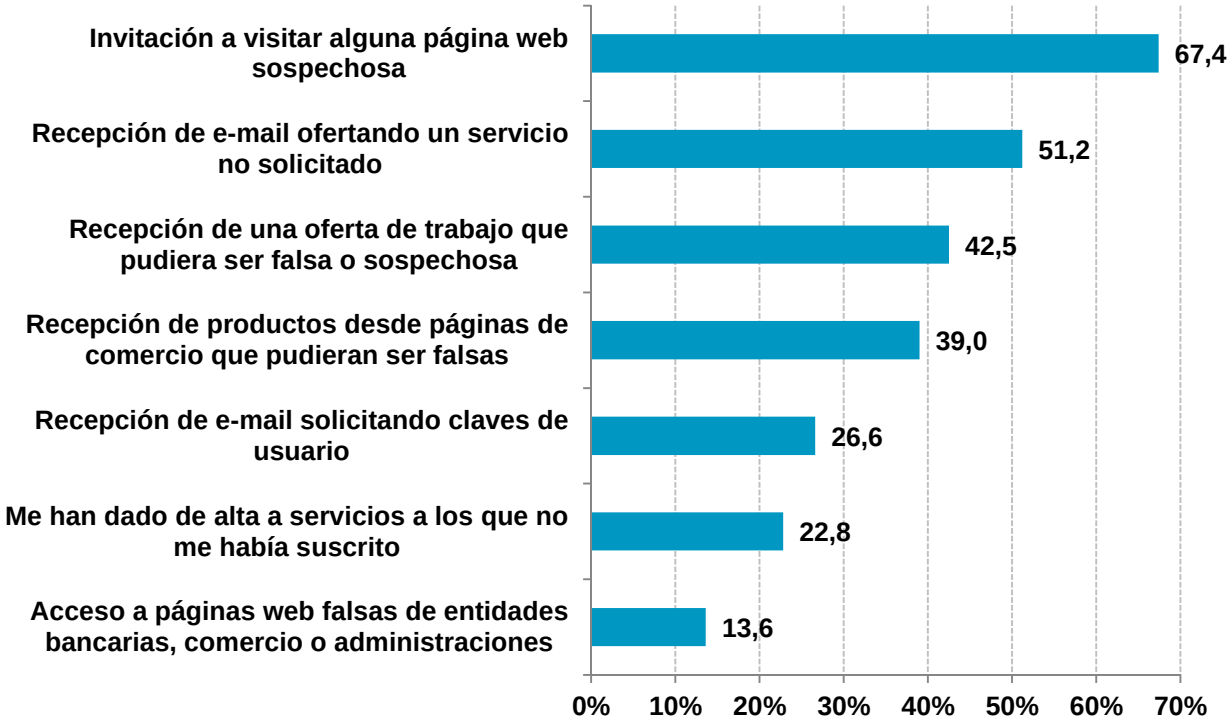
No ha sufrido ninguna situación de fraude

BASE: Total usuarios

Manifestaciones del intento de fraude online:

Respuesta múltiple

% individuos

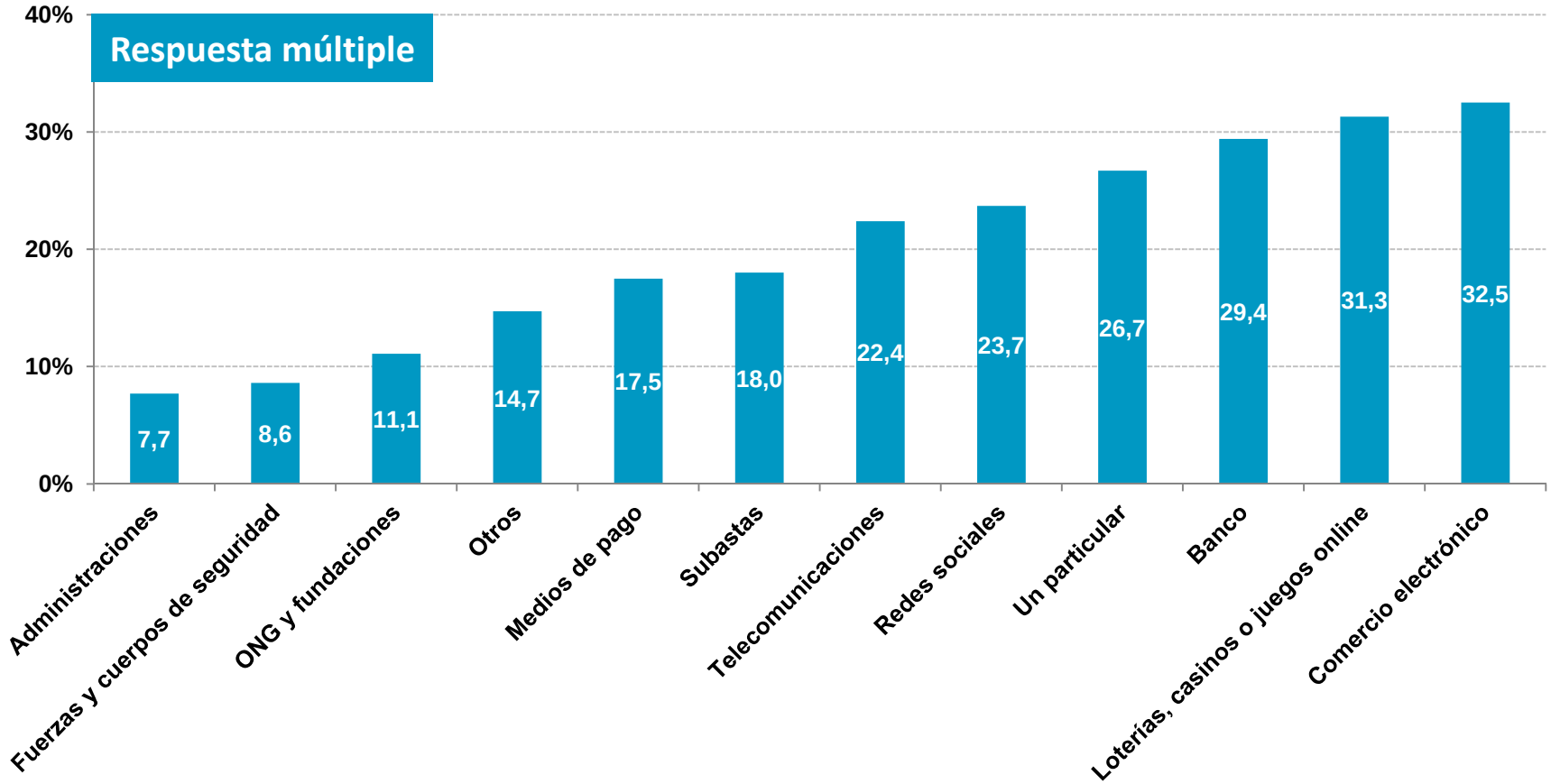


BASE: Usuarios que han sufrido algún intento de fraude

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

Intento de fraude online y manifestaciones

Las **formas adoptadas** más comúnmente por el remitente de la comunicación sospechosa de ser fraudulenta[4], son las imágenes de páginas de **"Comercio electrónico"** (**32,5%**) y **"Loterías, casinos y juegos online"** (**31,3%**).



BASE: Usuarios que han sufrido algún intento de fraude

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

Intento de fraude online y manifestaciones

Manifestación del fraude	Forma adoptada por el remitente de la comunicación[5] (%)											
	Banco	Comercio electrónico	Medios de pago	Redes sociales	Administraciones	Telecomunicaciones	ONG y fundaciones	Subastas	Loterías	Fuerzas y cuerpos de seguridad	Particular	Otros
Recepción de e-mail solicitando claves de usuario	**54,2**	35,1	32,2	33,5	13,5	26,4	15,3	23,8	35,6	15,9	31,2	7,2
Recepción de e-mail ofertando un servicio no solicitado	34,0	**42,5**	20,6	28,4	8,3	31,7	14,4	24,5	41,5	11,1	31,9	12,7
Recepción de e-mail con invitación a visitar alguna página web sospechosa	33,5	**35,6**	20,3	27,5	8,8	24,4	12,7	20,9	35,0	8,8	28,9	14,5
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	35,8	35,2	23,3	29,5	10,6	26,0	14,0	22,1	35,2	11,9	**42,0**	14,4
Recepción de productos desde páginas de comercio que pudieran ser falsas	35,7	43,5	25,0	32,6	10,3	30,2	16,1	28,9	**43,5**	12,4	34,0	10,6
Acceso a páginas web falsas de entidades bancarias, comercio o Administraciones	**53,1**	32,3	33,1	28,4	21,9	30,7	20,5	25,0	39,0	25,4	29,8	7,9
Alta en servicios a los que no se ha suscrito	32,1	**45,1**	26,4	33,3	10,5	37,7	18,2	25,1	40,2	10,5	31,6	14,1

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

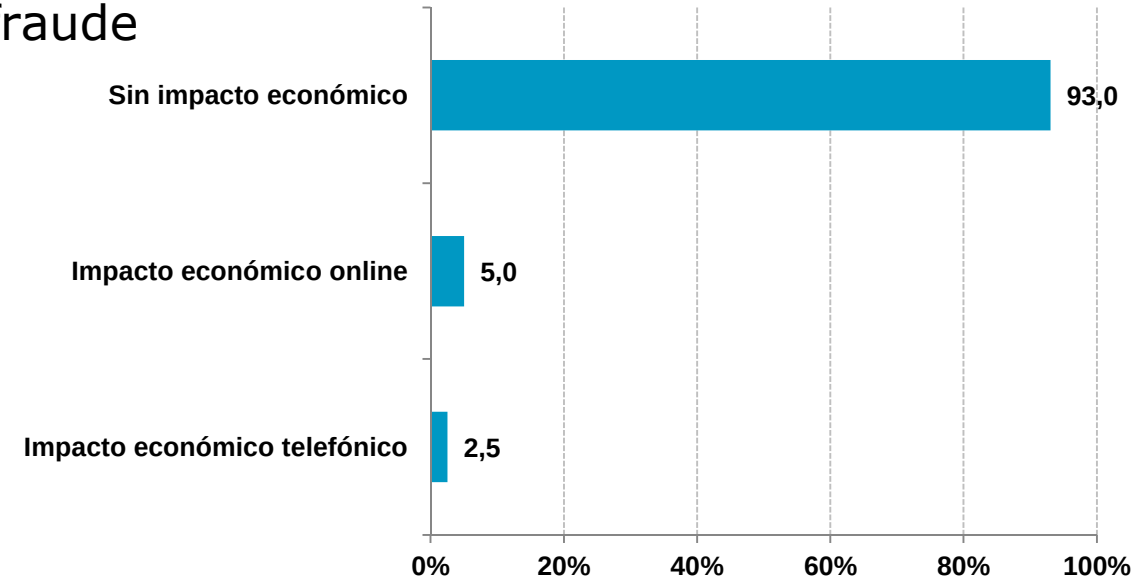
[5] Ver nota al pie número 4

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

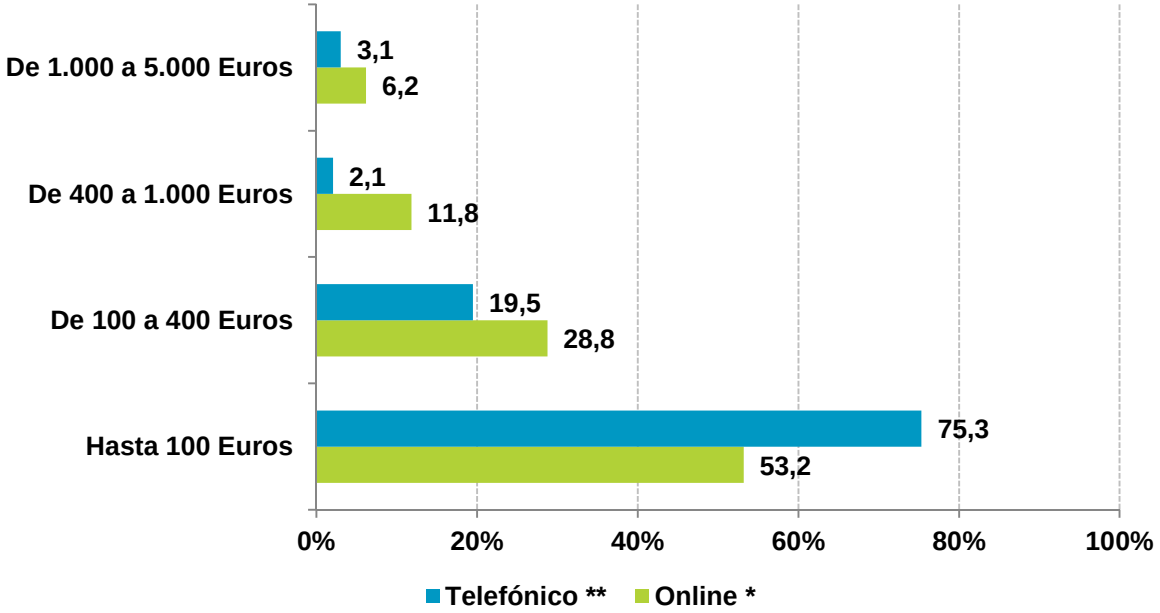
Impacto económico del fraude

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

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



BASE: Usuarios que han sufrido un intento de fraude



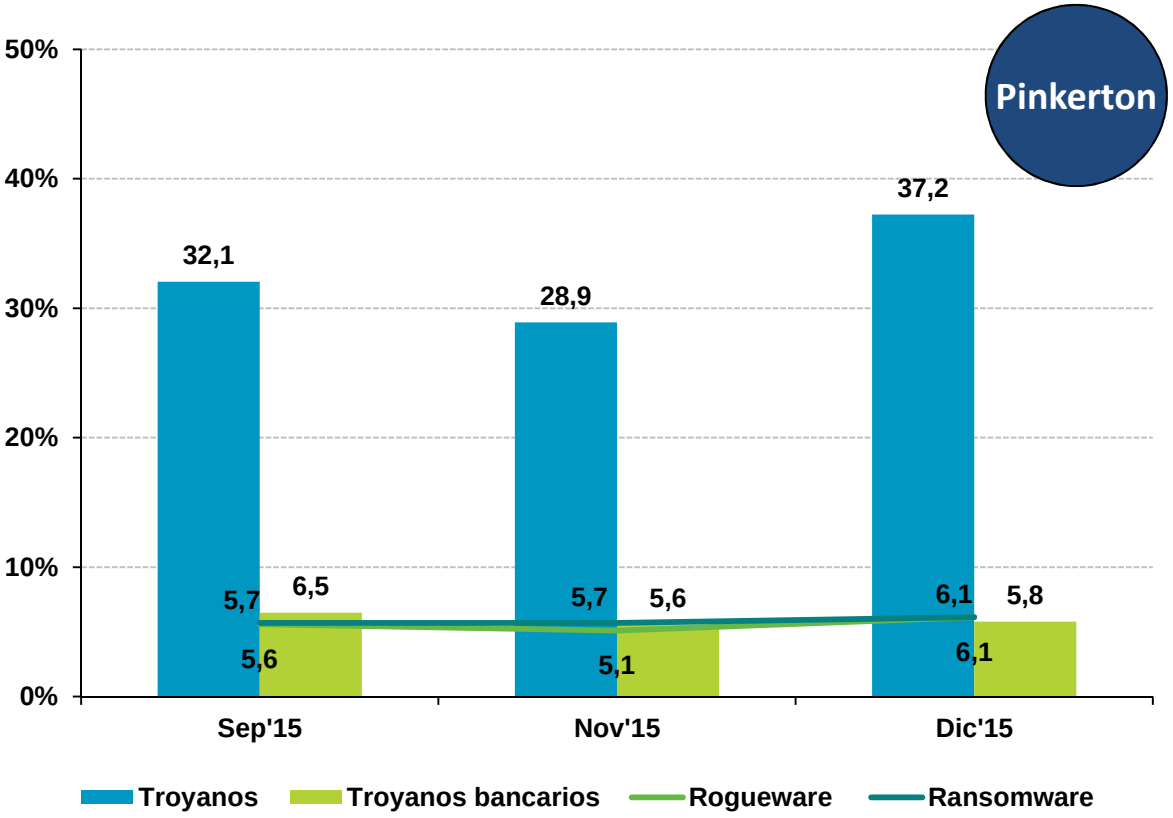
Distribución del impacto económico del fraude

* 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

Los tipos de troyanos **'Ransomware'** y **'Rogueware'** llegan hasta los niveles de los **'Troyanos bancarios'** detectados, encontrándose en torno al **6%** de los ordenadores analizados con **Pinkerton**.



BASE: Total ordenadores

Tipología del malware analizado

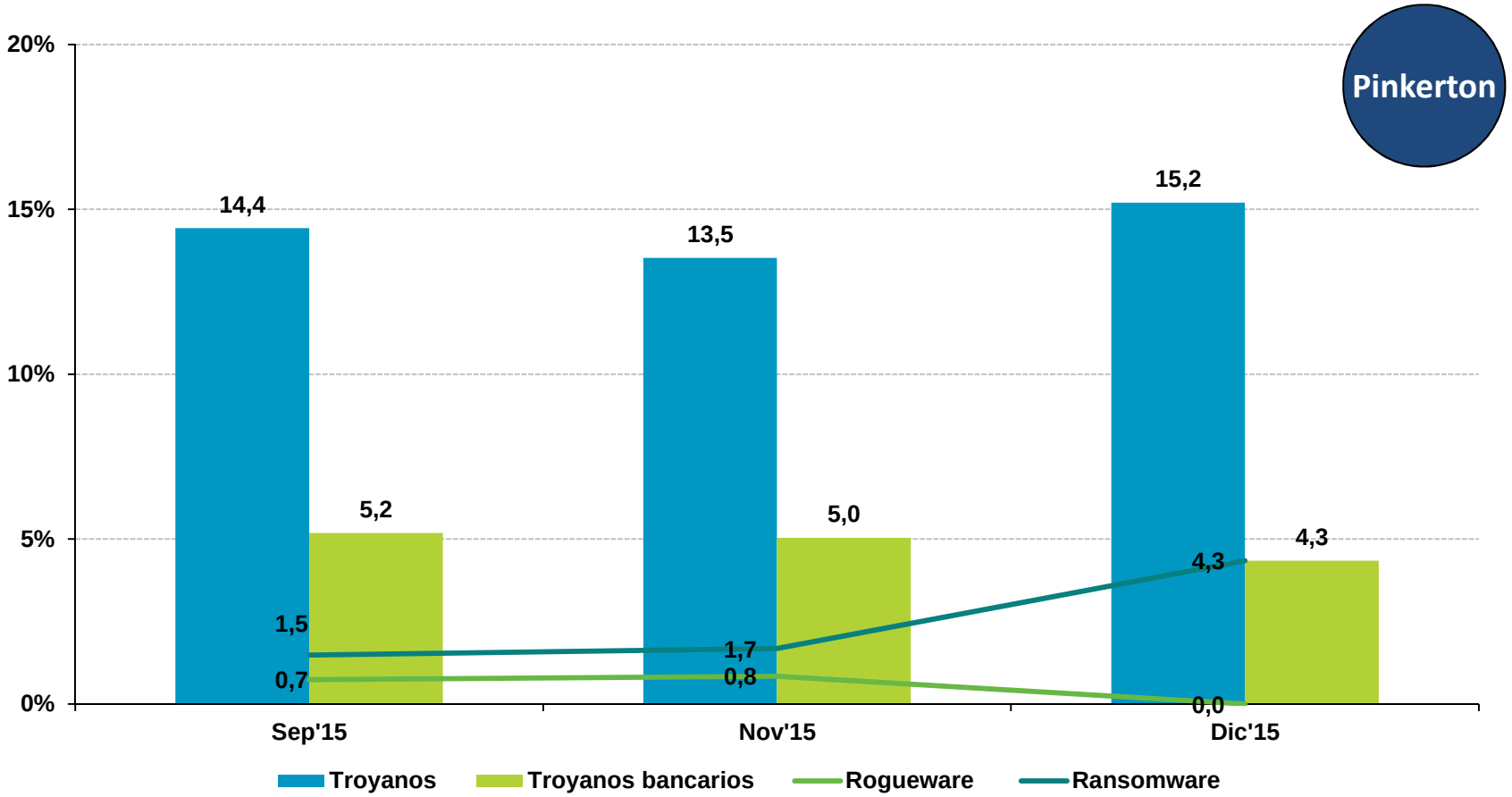
✓ Troyano bancario:
malware que roba información confidencial a los clientes de banca y/o plataformas de pago online.

✓ 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

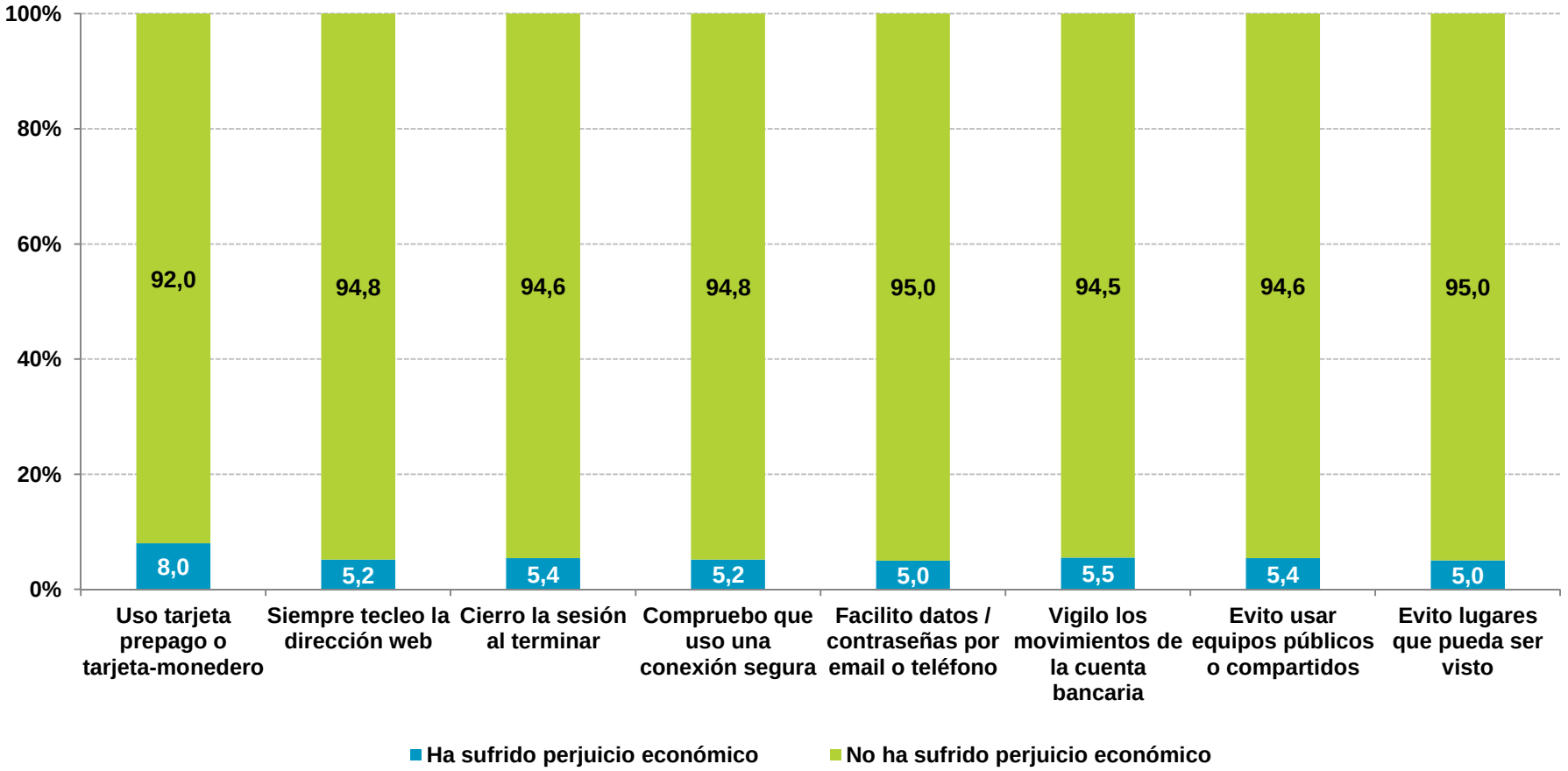
Los **troyanos bancarios** detectados están presentes en un **5%** de los dispositivos Android analizados con **Pinkerton**.



BASE: Usuarios que disponen de dispositivo Android

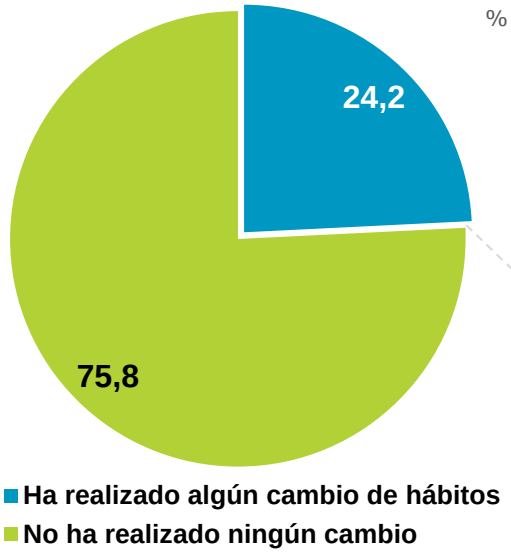
Consumación del intento de fraude según los hábitos prudentes

El uso de hábitos prudentes **minimiza** el riesgo de consumación de un intento de fraude. En todos los caso, un porcentaje menor al **8%** de los usuarios que tienen buenos hábitos sufrieron perjuicio económico como consecuencia de un fraude online o telefónico.



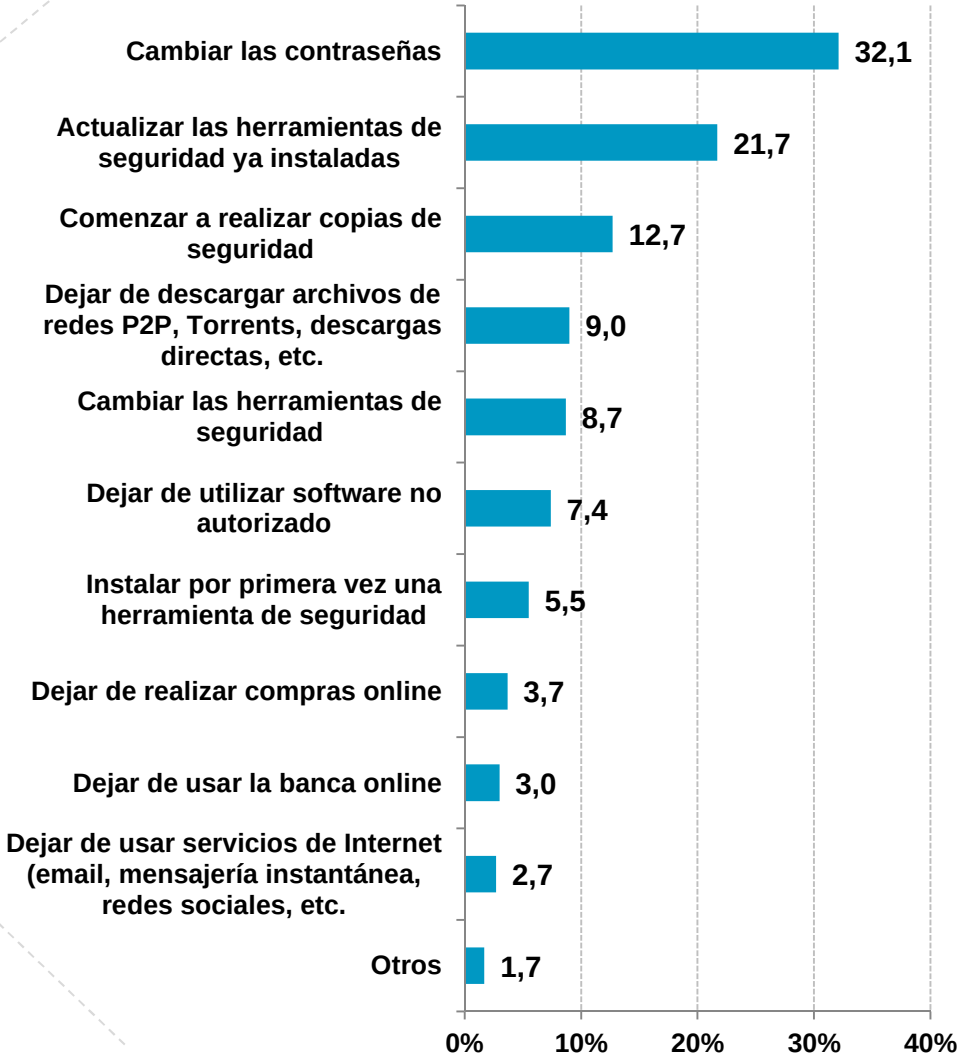
BASE: Usuarios que utilizan banca online

Cambios adoptados tras un incidente de seguridad



BASE: Total usuarios

Cambios realizados: **Respuesta múltiple**



BASE: Usuarios que realizan algún cambio

Cambios adoptados tras un incidente de seguridad

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

Entre aquellos usuarios que han sufrido incidencias de seguridad correspondientes a **suplantación de identidad** destaca el **cambio de contraseñas** como la principal modificación de hábito (**60,4%**).

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	36,8	31,5	17,3	16,3	11,1	8,7
Pérdida de archivos o datos	45,0	31,5	**29,3**	**20,3**	**21,2**	12,6
Servicios inaccesibles debido a ciberataques	41,6	**34,7**	20,4	14,3	**21,2**	10,2
Recepción de spam	29,5	21,1	11,5	7,6	6,6	4,8
Suplantación de identidad	**60,4**	30,9	20,9	23,0	14,9	16,8
Intrusión Wi-Fi	50,0	28,6	20,2	17,3	20,4	**17,2**

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

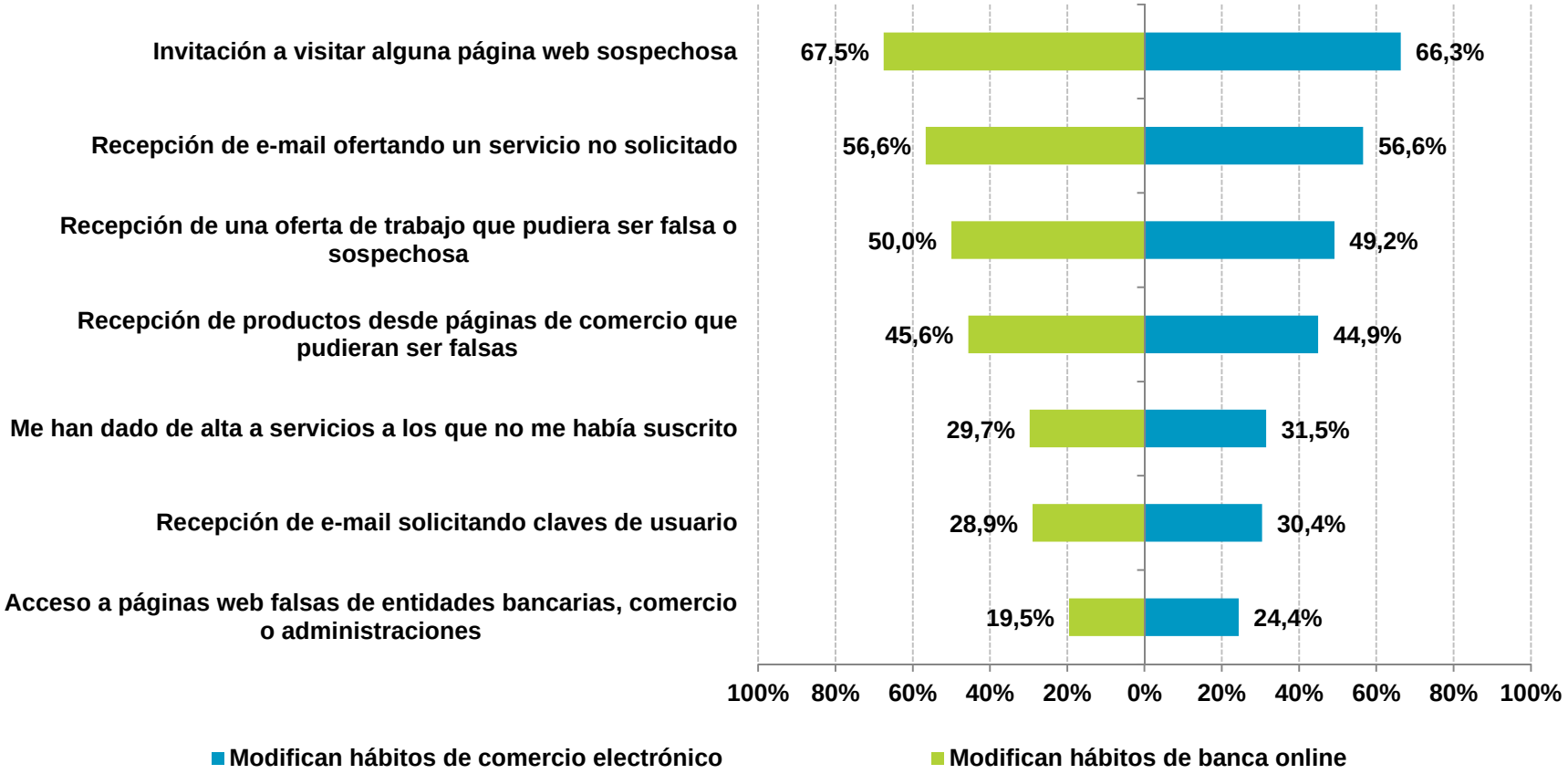
El **22,4%** de los usuarios que han sufrido una **intrusión Wi-Fi** abandonan la banca online.

Incidencia (%)	Cambio en el uso de servicios			
	Abandonar descargas	Abandonar la banca online	Abandonar el comercio electrónico	Dejar de usar servicios de Internet
Malware	13,3	3,9	4,2	2,8
Pérdida de archivos o datos	15,3	12,2	9,5	9,9
Servicios inaccesibles debido a ciberataques	**18,8**	8,6	7,8	12,7
Recepción de spam	8,4	2,1	2,3	1,8
Suplantación de identidad	13,5	11,5	11,4	10,1
Intrusión Wi-Fi	18,2	**22,4**	**13,3**	**16,2**

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

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

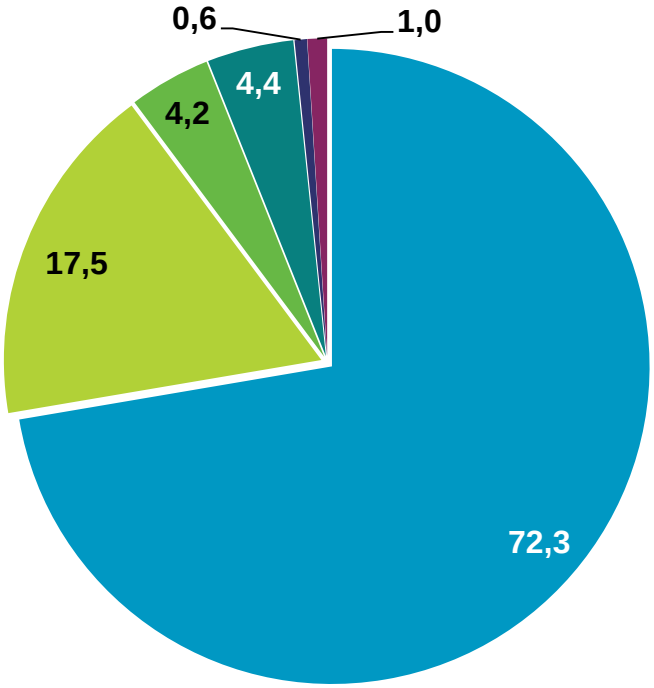
El **67,5%** de usuarios de banca online y **66,3%** de comercio electrónico modifican sus hábitos tras recibir una **invitación a visitar alguna página web sospechosa**.



BASE: Usuarios que han sufrido un intento de fraude

Cambios adoptados tras un incidente de seguridad

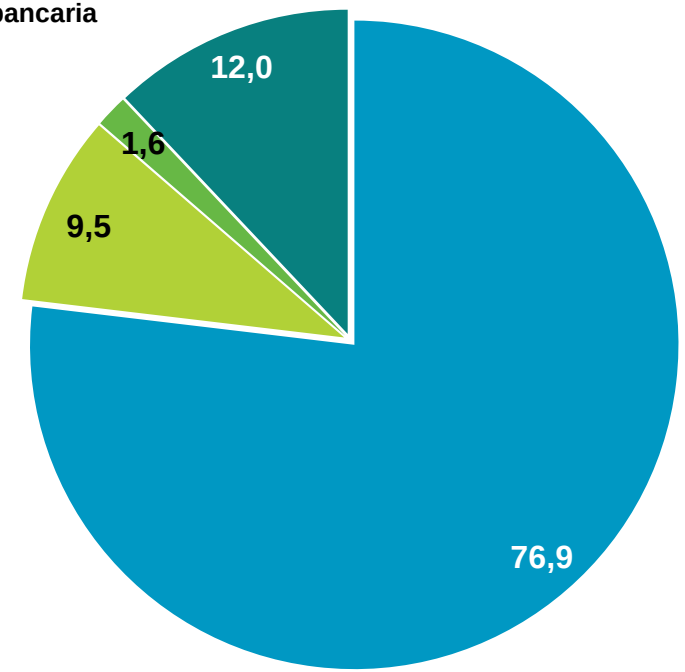
Modificación de hábitos prudentes relacionados con los servicios de banca online y comercio electrónico tras sufrir un intento de fraude



- Sin modificación de hábitos de banca electrónica
- Utilizo las medidas de seguridad de mi entidad
- Limitación de uso de banca electrónica
- Reducción de uso de banca electrónica
- Abandono banca electrónica
- Cambio de entidad bancaria

% individuos

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



- Sin modificación de hábitos de comercio electrónico
- Reducción de uso de comercio electrónico
- Abandono de comercio electrónico
- He modificado la forma de pago

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

Confianza en el ámbito digital en los hogares españoles

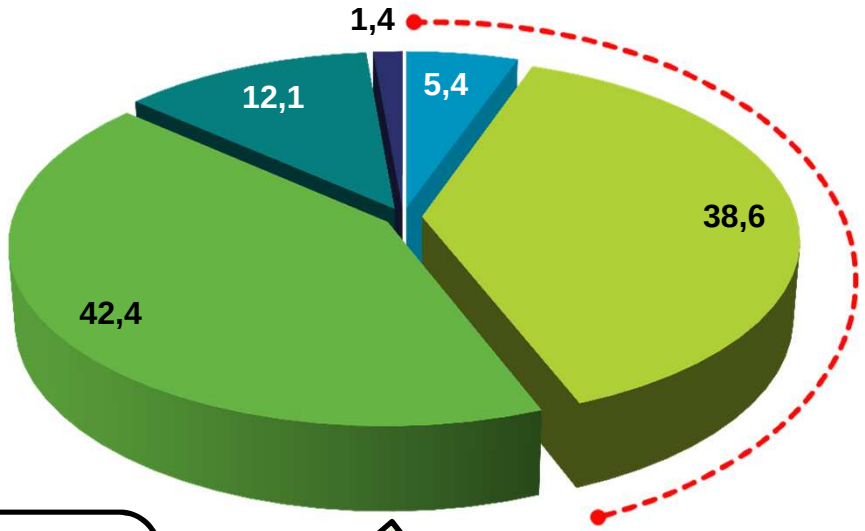
1. e-Confianza y limitaciones en la Sociedad de la Información
2. Percepción de los usuarios sobre la evolución en seguridad
3. Valoración de los peligros de Internet
4. Responsabilidad en la seguridad de Internet

6

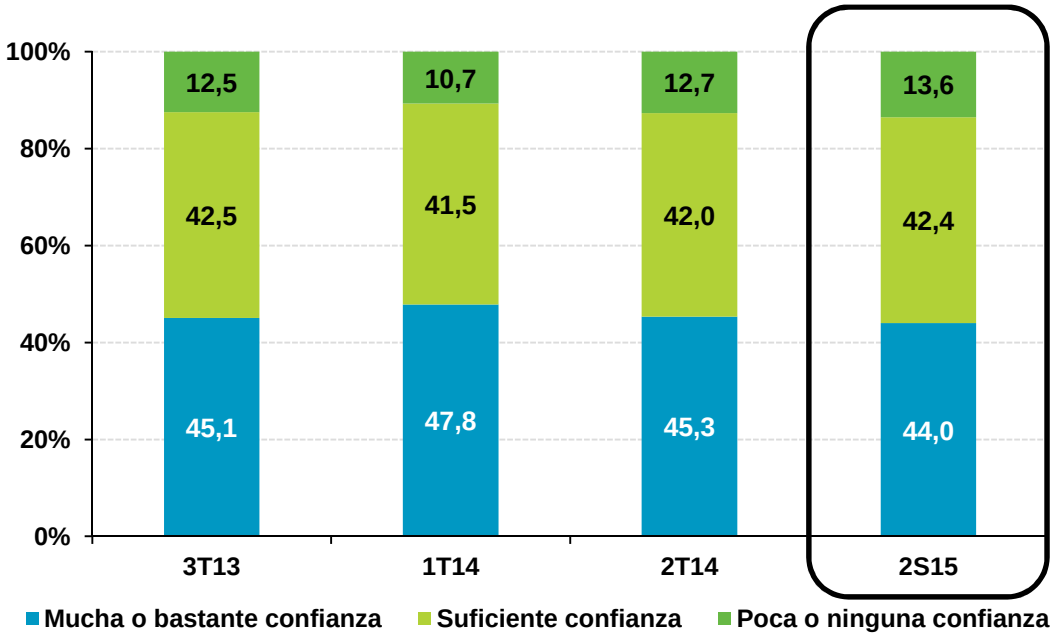
Nivel de confianza en Internet

El **44%** de los usuarios encuestados **confía** bastante o mucho en Internet.

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



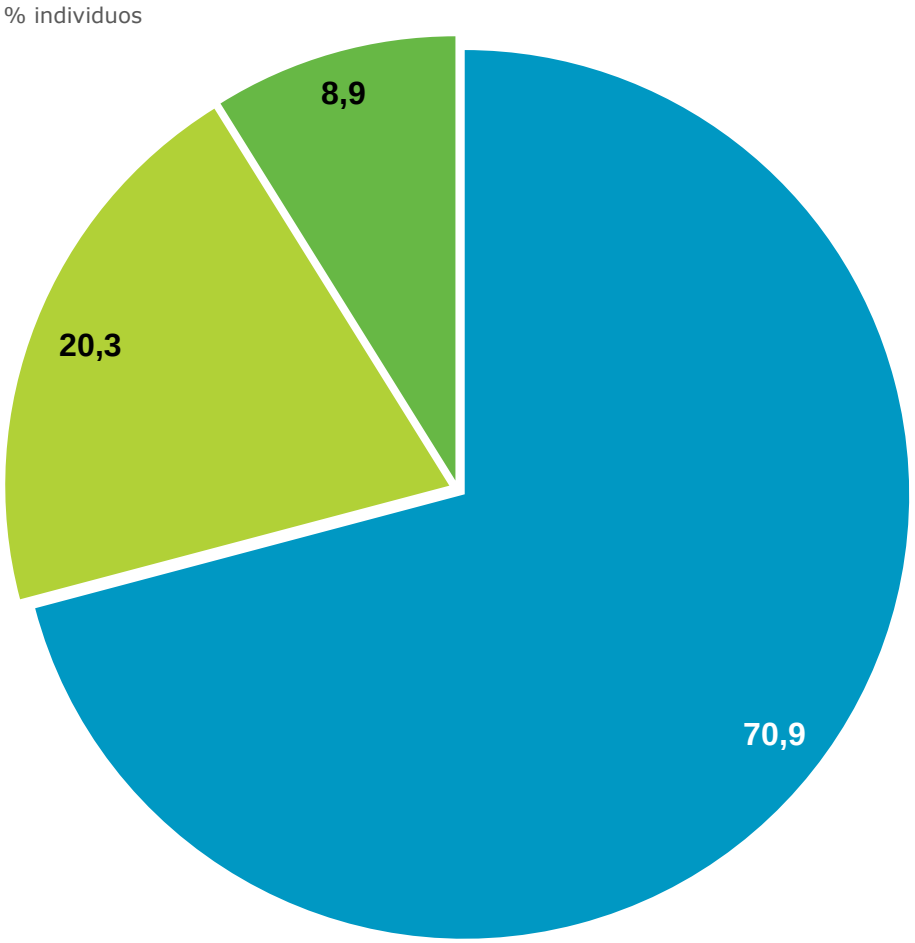
% individuos



BASE: Total usuarios

3T13 corresponde al estudio realizado en el tercer trimestre de 2013. **1T14 y 2T14** a los estudios correspondientes al primer y segundo trimestres de 2014, respectivamente. **2S15**, corresponde al presente estudio, relativo al segundo semestre de 2015.

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

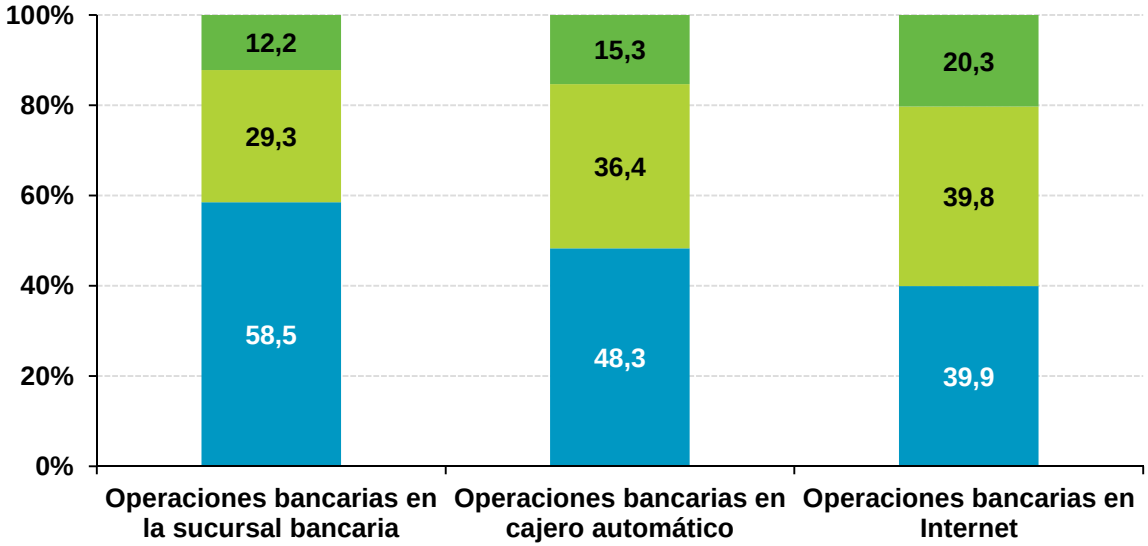


Casi el **71%** de los internautas encuestados opinan que su **equipo informático** o **dispositivo móvil** se encuentra **razonablemente protegido** frente a las potenciales amenazas de Internet.

6

BASE: Total usuarios

Confianza online vs. confianza offline



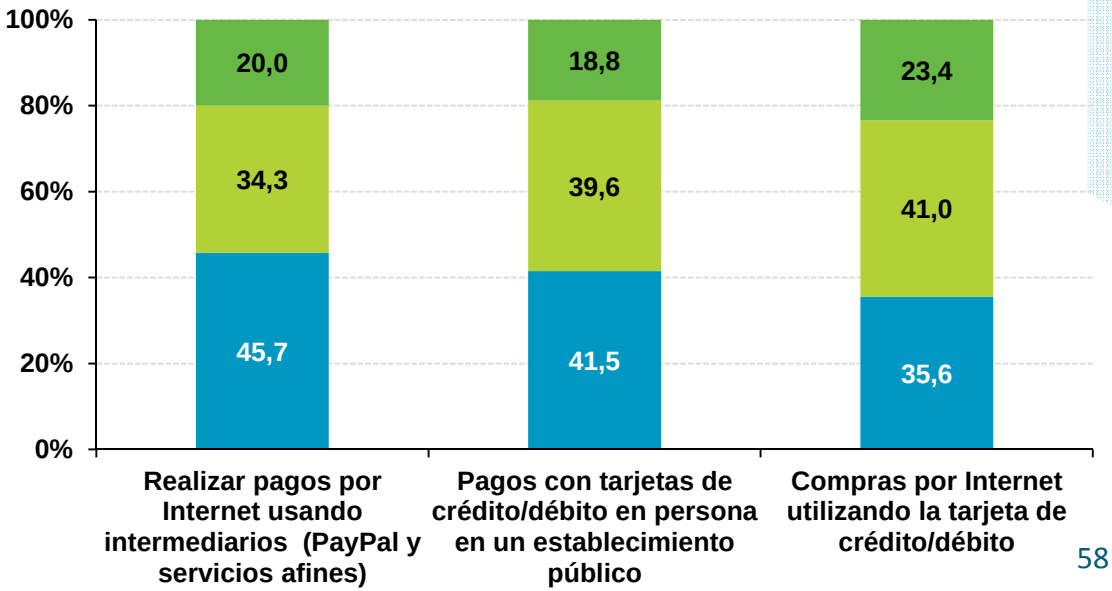
Nivel de confianza en operaciones bancarias

El usuario deposita mayor confianza en el trato con otra persona en la **entidad bancaria** (**58,5%**) que en aquellas **operaciones bancarias** realizadas a través de un **cajero automático** (**48,3%**) o mediante **Internet** (**39,9%**).

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

Nivel de confianza en operaciones de compra-venta

El pago con **tarjeta de crédito/débito** en establecimiento público (**41,5%**) y el uso de intermediarios como **PayPal y servicios afines** (**45,7%**) para realizar pagos a través de Internet son las opciones que mayor confianza aportan al usuario en **operaciones de compra-venta**.



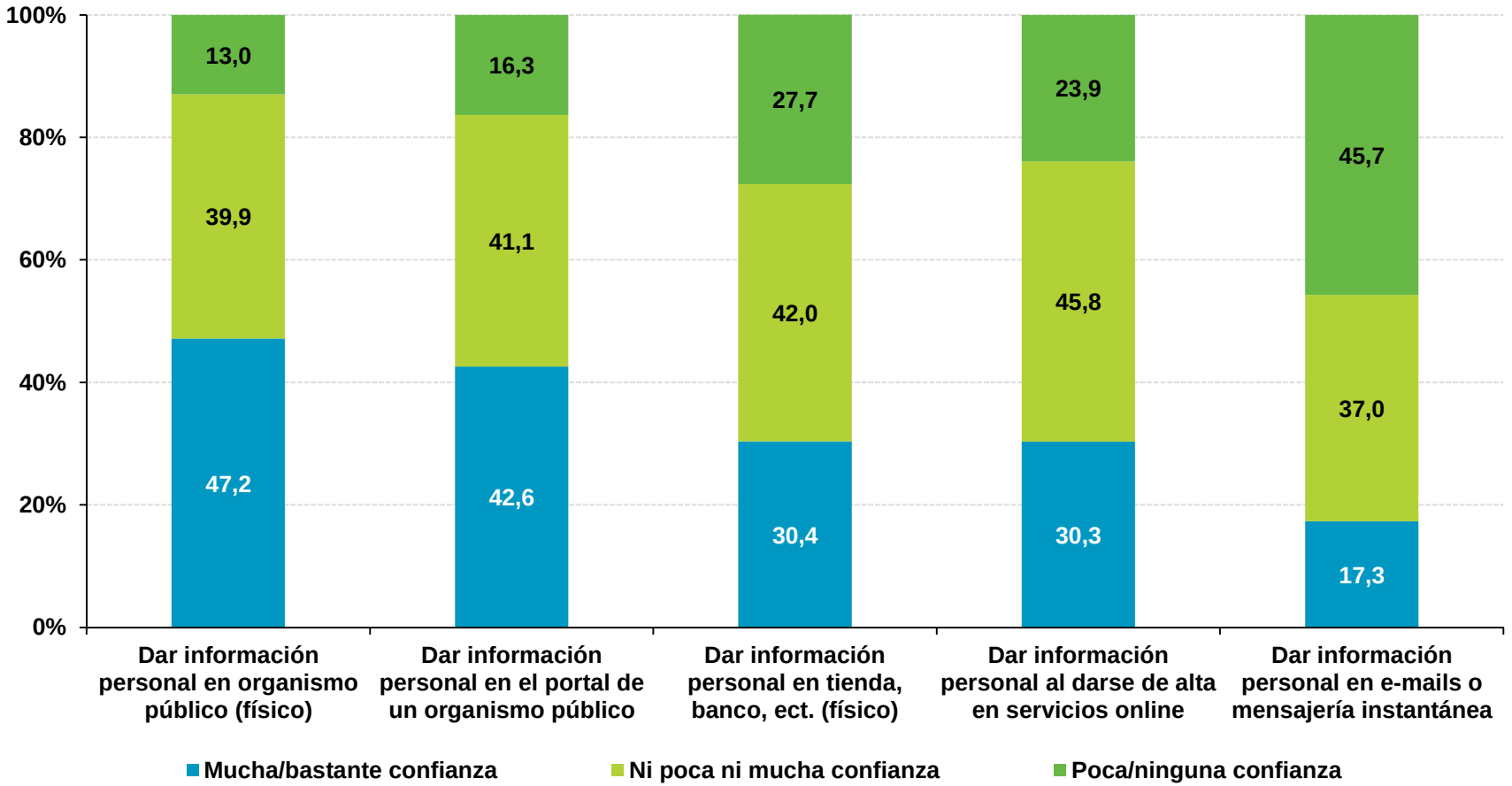
BASE: Total usuarios

% individuos

Confianza online vs. confianza offline

Un **17,3%** de la población afirma tener suficiente confianza para **facilitar información** de carácter personal a través de **correo electrónico, chat o mensajería instantánea**.

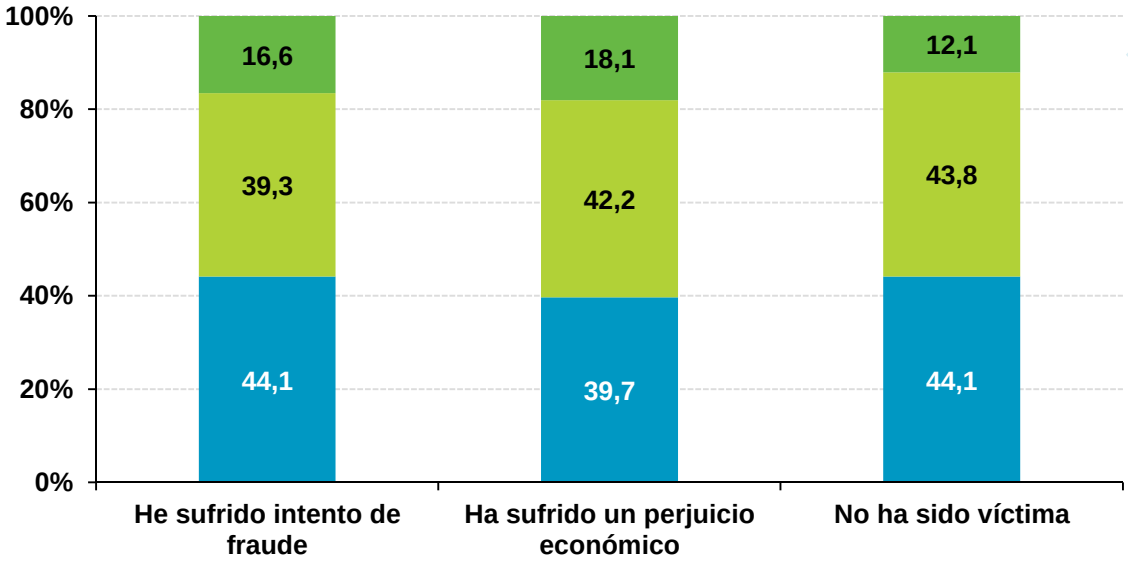
Nivel de confianza en facilitar datos personales



BASE: Total usuarios

% individuos

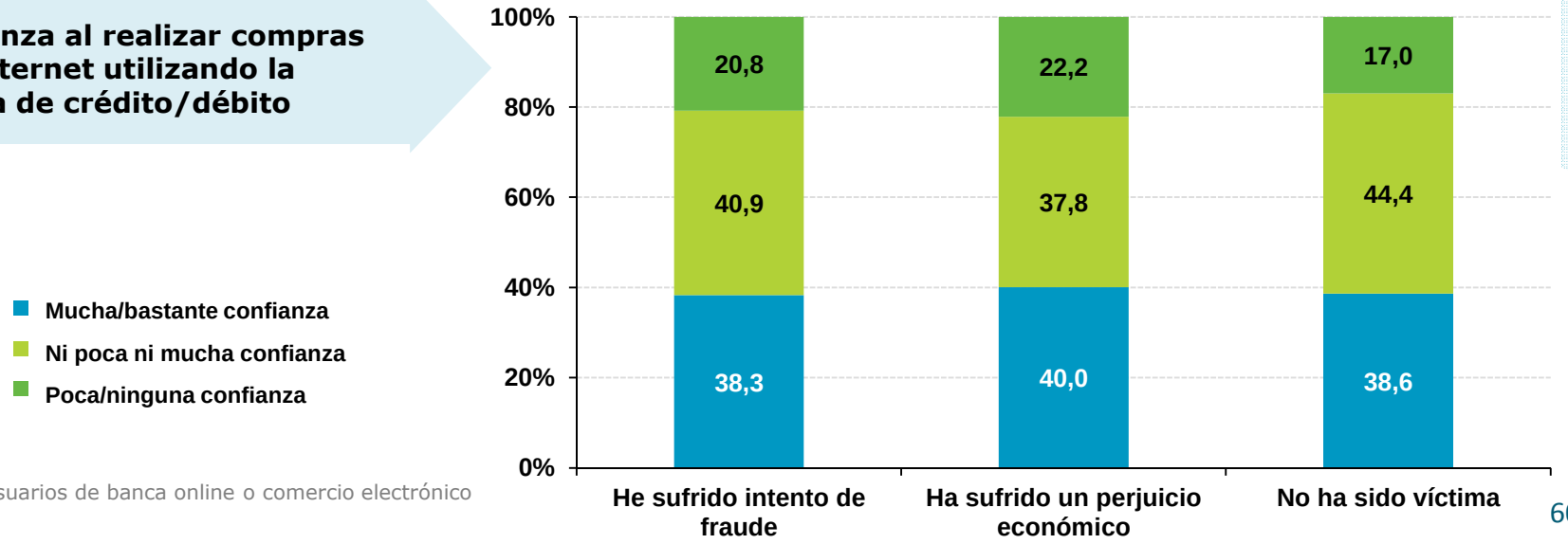
Confianza vs. fraude



Confianza al realizar operaciones bancarias en Internet

% individuos

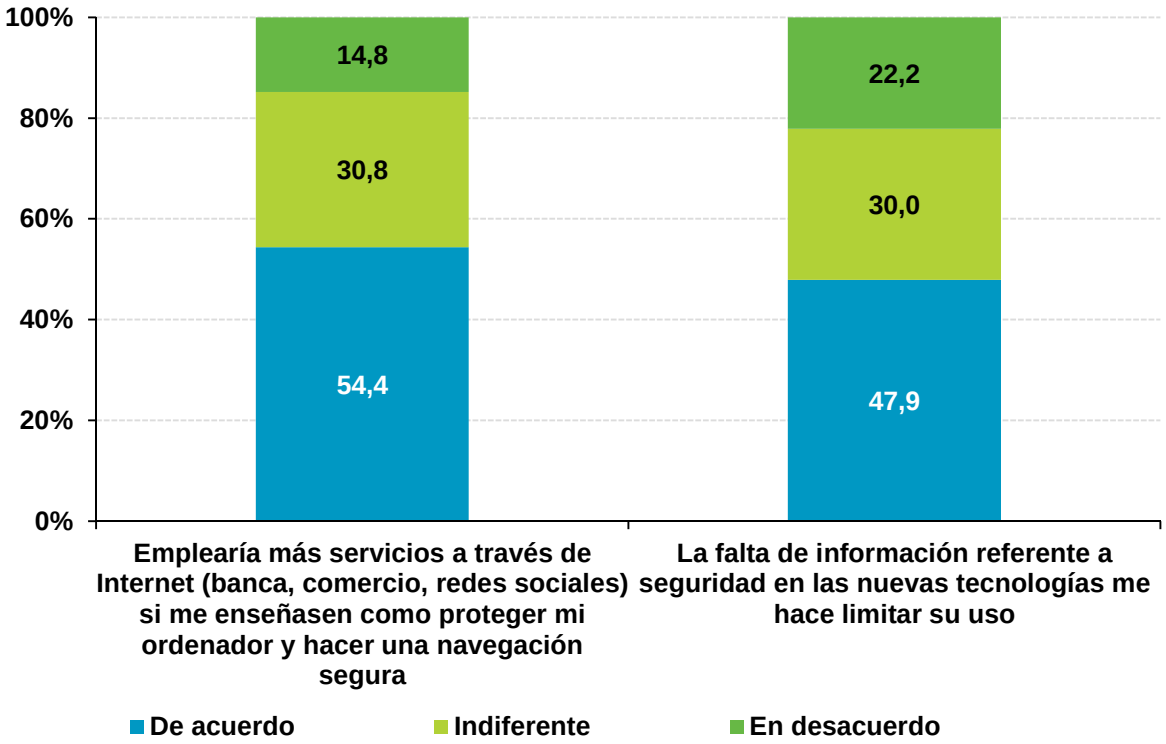
Confianza al realizar compras por Internet utilizando la tarjeta de crédito/débito

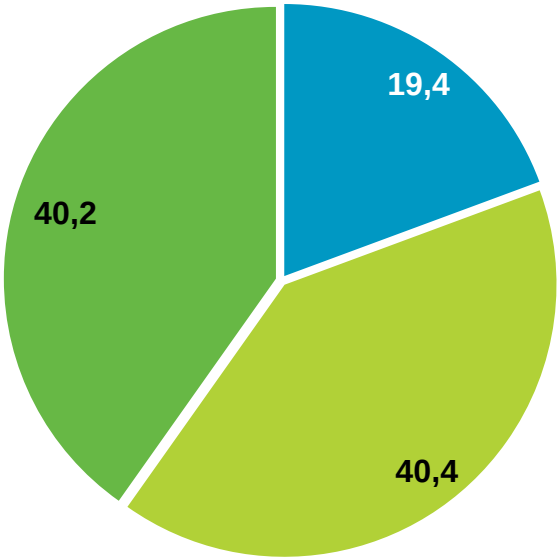


BASE: Usuarios de banca online o comercio electrónico

Limitación a causa de problemas de seguridad

Seguridad como factor limitante en la utilización de nuevos servicios





Limitaciones en el uso de Internet

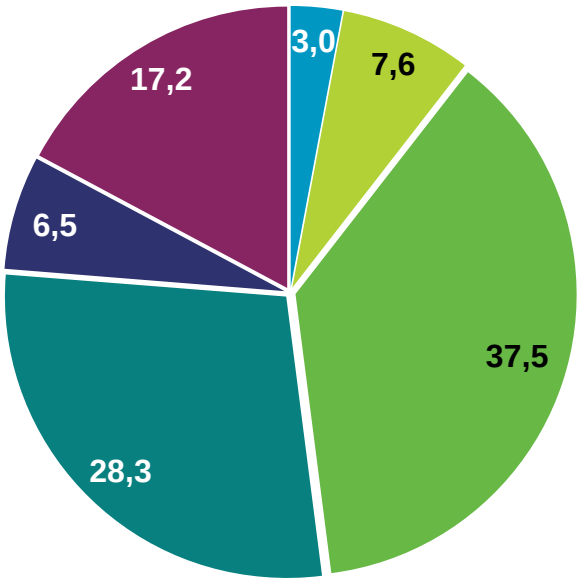
% individuos

6

e-Confianza y limitaciones en la Sociedad de la Información

Razones para no utilizar banca online

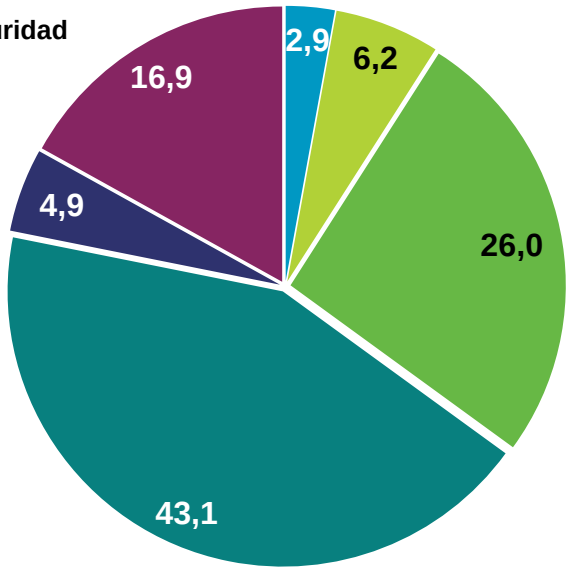
La **falta de confianza y/o seguridad** es el **principal motivo** que alegan los usuarios para no utilizar los servicios de banca online (**37,5%**).



% individuos

- No sé lo que es
- No sé usarlo o me resulta difícil
- No me da confianza, no me da seguridad
- No necesito o no me interesa
- No protege mis datos privados
- Otros

Razones para no utilizar comercio electrónico

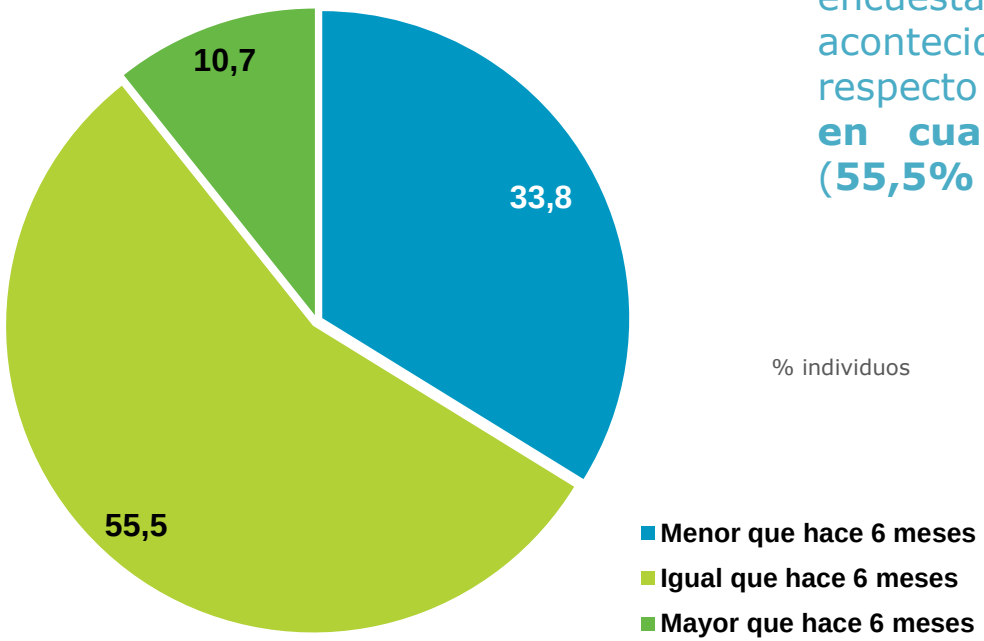


En referencia al comercio electrónico, la **falta de necesidad o interés** en dicho servicio es el principal motivo que causa que el **43,1%** de los usuarios no lo utilicen.

BASE : Usuarios que no utilizan el servicio

Percepción de los usuarios sobre la evolución en seguridad

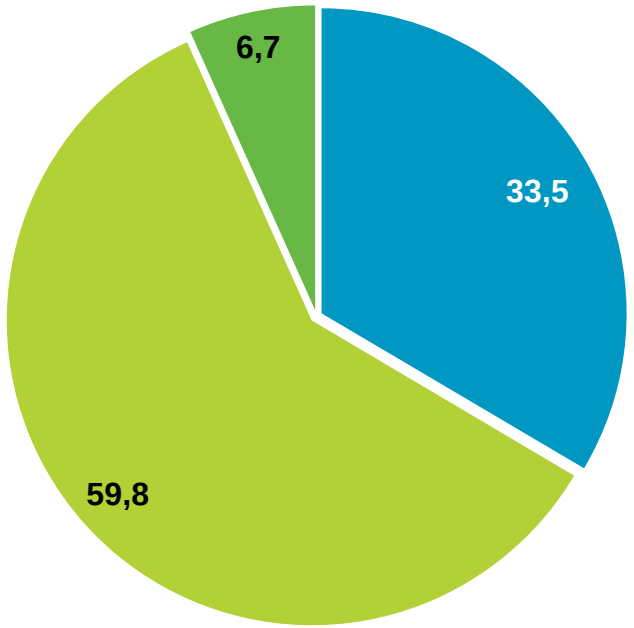
Número de incidencias



Más de la mitad de los usuarios encuestados perciben que las incidencias acontecidas en los últimos 3 meses con respecto a meses anteriores son **similares en cuanto a cantidad y gravedad** (**55,5%** y **59,8%**, respectivamente).

Gravedad de las incidencias

% individuos



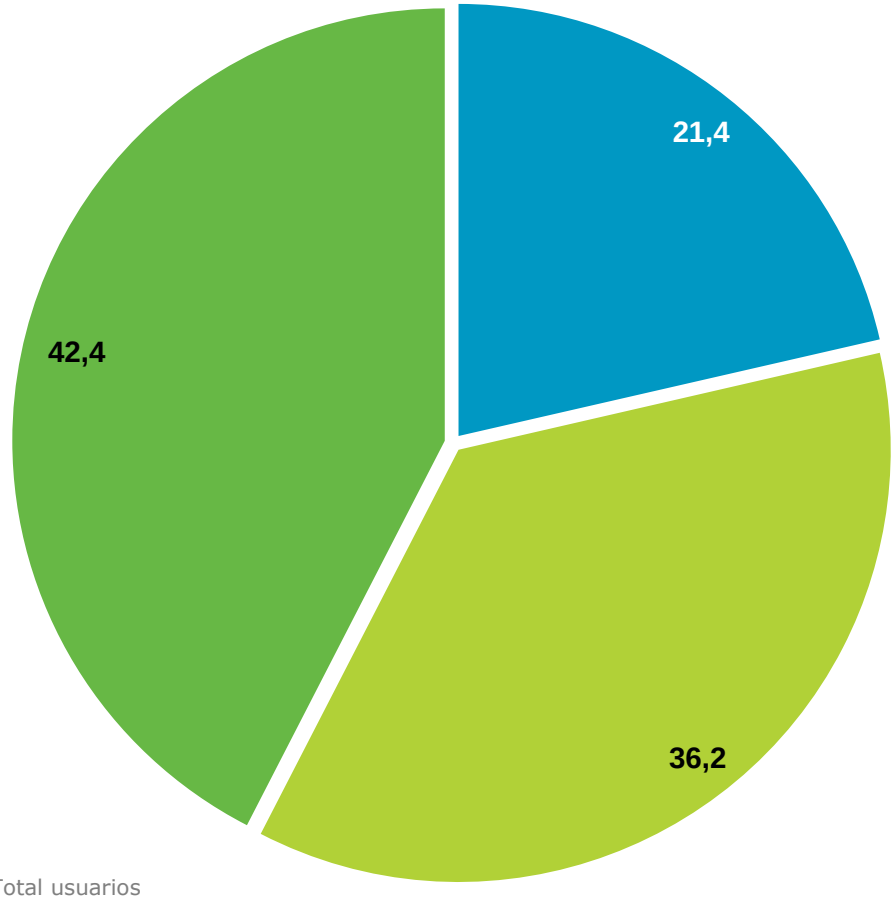
Un tercio percibe un **menor número** de incidencias en los últimos 3 meses y además las considera de **menor gravedad**.

BASE: Total usuarios

Percepción de los usuarios sobre la evolución en seguridad

Percepción de riesgos en Internet

El **robo y uso de información personal** (**42,4%**) sin el consentimiento del usuario y el **perjuicio económico** (**36,2%**) derivado de un fraude son los principales riesgos en Internet percibidos por los internautas.

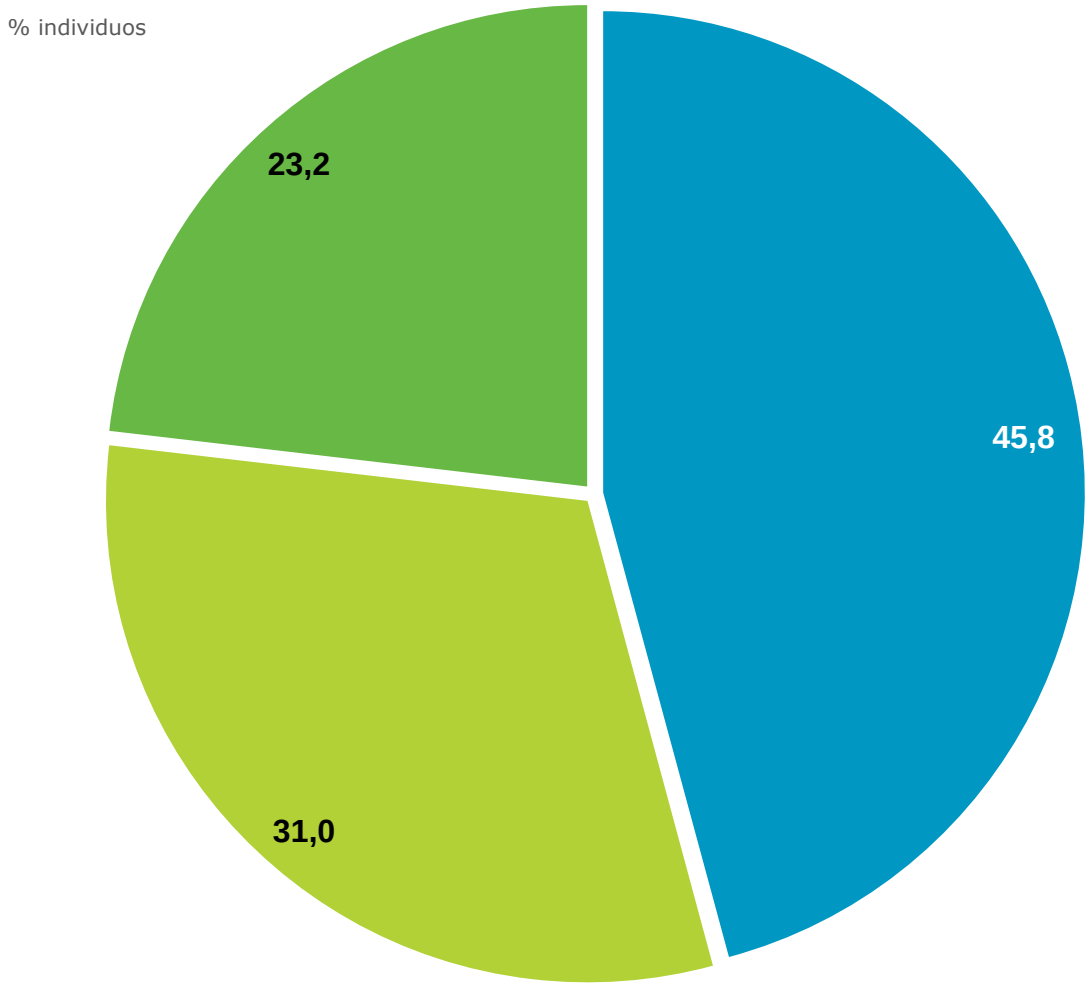


% individuos

- **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

Valoración de Internet cada día como más seguro



Un **45,8%** de los internautas españoles perciben **Internet cada día como más seguro**.

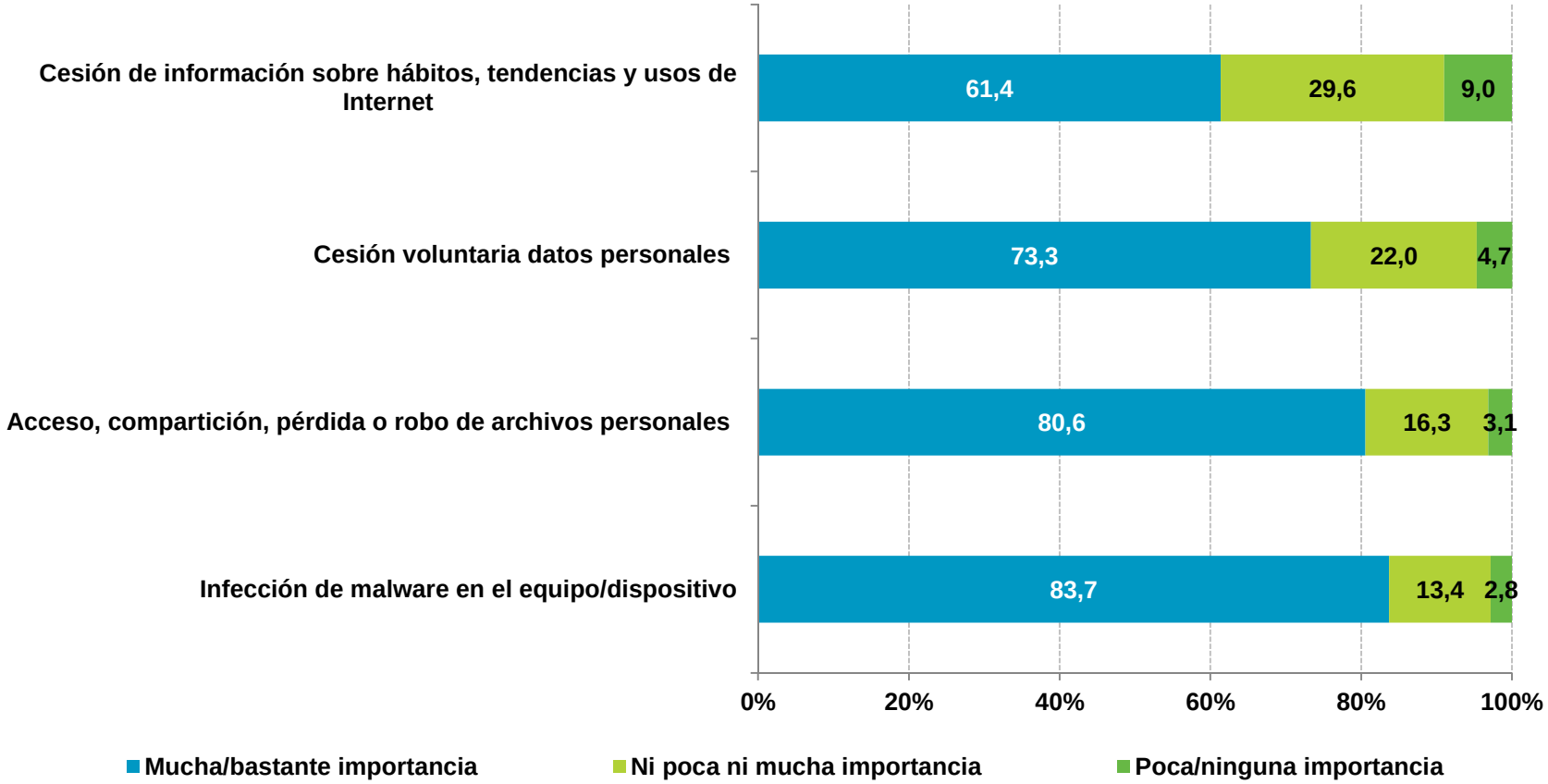
6

BASE: Total usuarios

Valoración de los peligros de Internet

El peligro que los panelistas consideran de mayor importancia es la **infección de malware en su equipo/dispositivo (83,7%)**.

La **cesión de datos personales** (**61,4%**) o **información sobre hábitos, tendencias y usos de Internet** (**61,4%**) son los peligros menos valorados.



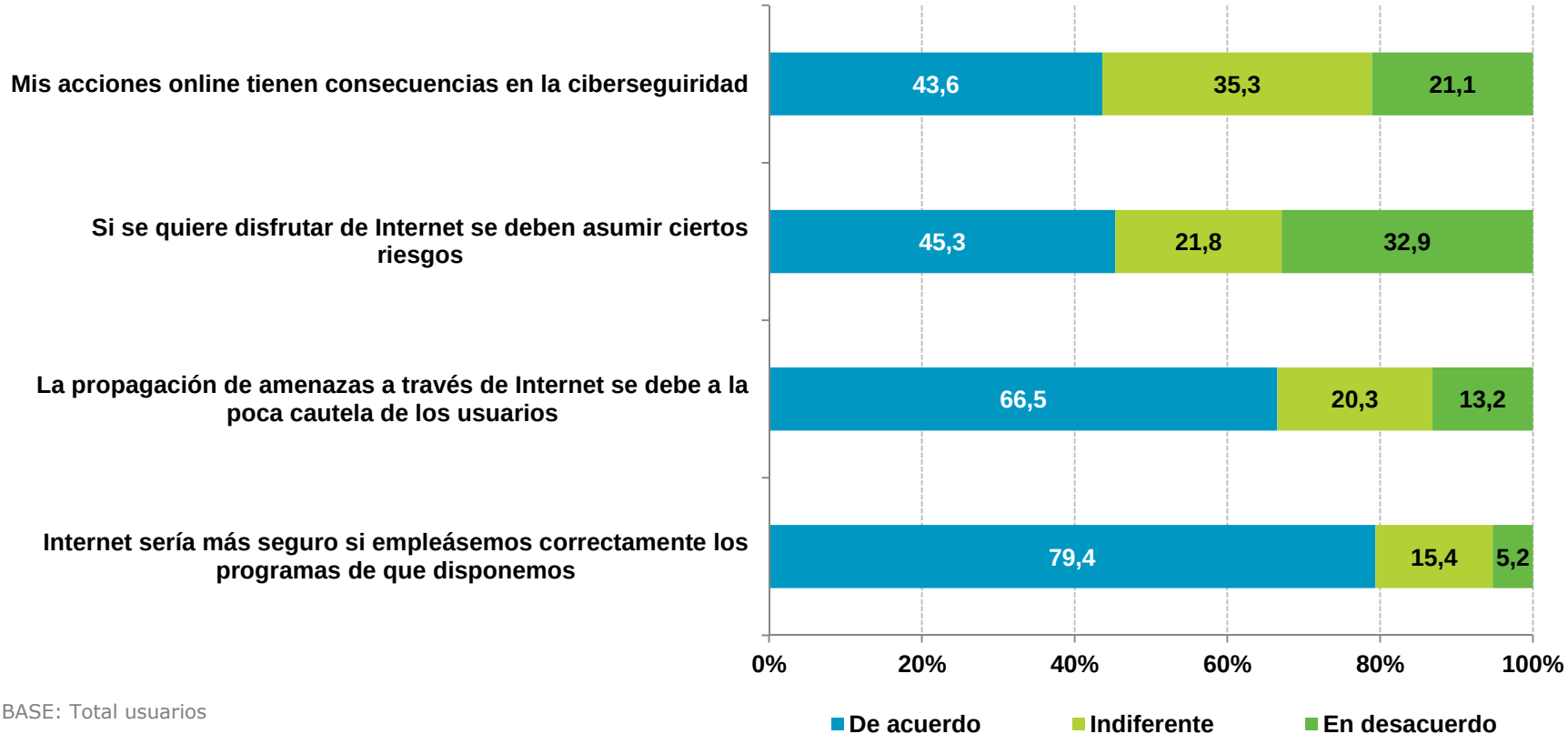
BASE: Total usuarios

Responsabilidad en la seguridad de Internet

Rol del usuario

La gran mayoría de los usuarios (**79,4%**) creen que no se usa adecuadamente el software de que disponen. **Dos tercios** opinan que la propagación de las amenazas se debe a la poca cautela de los propios usuarios.

Alrededor del **45%** de los panelistas declaran que sus acciones tienen consecuencias en la ciberseguridad, y que es necesario asumir ciertos riesgos para disfrutar de Internet.



BASE: Total usuarios

Conclusiones

MEDIDAS DE SEGURIDAD

Las medidas de seguridad con mayor presencia real en los equipos informáticos españoles son los cortafuegos (90,8%) y programas antivirus (82,2%). En el caso de los cortafuegos, el uso declarado se encuentra 50 puntos porcentuales por debajo de la presencia real.

Otra gran diferencia es la que supone el uso real de cuentas con permisos reducidos (78,9%) frente al declarado (13%). Se observa a demás como en las últimas versiones del sistema operativo Microsoft Windows aumenta el uso de cuentas con permisos limitados, hasta llegar al punto de ser inexistentes en Windows 8 y posteriores. Esto se debe a la configuración por defecto de las distintas versiones y a la falta de necesidad real de mayores privilegios para el uso convencional del ordenador del hogar.

Con respecto a los usuarios de dispositivos Android, se observan también importantes brechas entre el uso real y declarado de software antivirus (superior a 23 puntos porcentuales), y sistemas seguros de desbloqueo del dispositivo como por ejemplo PIN, patrón, etc. (superior a 44 puntos porcentuales).

También se revela que **la gran mayoría de los smartphones y tablets analizados disponen de alguna versión de Android de la rama 4.x. la cual se encuentra fuera de soporte** y por lo tanto son dispositivos **potencialmente vulnerables**.

El 13,9% de los usuarios Wi-Fi con conexión propia no protege su red o desconoce si se aplica algún tipo de protección. El porcentaje de personas que no se implican en la protección de su red inalámbrica aumenta casi hasta 50% si se agregan aquellos que utilizan el estándar WEP (7,1%), obsoleto y fácilmente eludible, y los que desconocen la tecnología que usan (27,7%).

Conclusiones

HÁBITOS DE COMPORTAMIENTO EN LA NAVEGACIÓN Y USOS DE INTERNET

En el ámbito de la banca en línea y comercio electrónico, la mayoría de panelistas, siempre en un porcentaje superior al 72,9%, **sigue buenas prácticas**. Solo el uso de tarjetas monedero/prepago es utilizado por un número menor de usuarios (35,8%).

También se demuestran **buenos hábitos en cuanto a las descargas desde Internet** entre los panelistas. El **62% de los usuarios de redes P2P analiza todos los ficheros descargados**, al igual que más de la mitad de los usuarios de descarga directa, y dos tercios de los usuarios afirman comprobar la veracidad de los ficheros descargados antes de abrirlos (sitio de descarga, tipo de fichero, hash, etc.).

Además, la gran mayoría de los panelistas (81,9%) declara prestar atención a los pasos de instalación del software, lo que contribuye a evitar la instalación de programas o aplicaciones adicionales y no deseadas cuya aceptación se incluye muchas veces en dicho proceso.

En referencia al uso de dispositivos Android, la mayoría de los usuarios (94%) presenta un comportamiento seguro al preferir realizar la descarga de aplicaciones principalmente desde repositorios oficiales. Sin embargo **el análisis llevado a cabo con Pinkerton revela que más de un tercio (34,9%) de los dispositivos están configurados para permitir la instalación de aplicaciones desde fuentes desconocidas, con el riesgo que ello conlleva.**

Conclusiones

INCIDENTES DE SEGURIDAD

La incidencia más comúnmente sufrida continúa siendo el spam, afectando a más del 87% de las victimas de algún incidente, mientras que las relacionadas con **virus y malware son declaradas únicamente por un 34,6%** de aquellos usuarios que han sufrido alguna incidencia de seguridad.

Considerando el total de usuarios, **el 24,8% considera haber tenido alguna incidencia de malware**. Sin embargo el impacto real es muy superior al declarado, ya que **Pinkerton detecta un 60% de ordenadores infectados de malware durante el periodo estudiado**. Esta brecha es un indicativo de que el malware se oculta cada vez mejor y pasa desapercibido ante el usuario y los programas antivirus.

Además, se observa que el porcentaje de infecciones aumenta cuanto menos actualizado está el equipo, sobre todo en Android, poniéndose de manifiesto **el aprovechamiento de vulnerabilidades en el proceso de infección**.

A pesar del elevado número de usuarios que potencialmente tiene su red inalámbrica expuesta, únicamente un porcentaje relativamente pequeño (13,6%) sospecha haber sufrido una intrusión en su red.

CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

Dos de cada tres panelistas declaran haber sufrido alguna vez una situación de intento de fraude, presentándose como una invitación a visitar alguna página web sospechosa en el 67,4% de las ocasiones, o un email ofertando un servicio no deseado en el 51,2%. **Las principales formas adoptadas por el remitente de la comunicación fraudulenta es la de comercio electrónico (32,5%) o loterías, casinos y juegos online (31,3%)**.

Los objetivos que el fraude persigue se mueven en cifras monetarias bajas para evitar la consideración de delito según el código penal. Así el 75,3% de los fraudes online y el 53,2% de los telefónicos estafaron menos de 100 euros, y entre 100 y 400 euros en el 19,5% y 28,8% de las ocasiones, respectivamente.

Entre los usuarios que han sufrido alguna incidencia de seguridad, casi un cuarto (24,2%) modifica sus hábitos, siendo el cambio de contraseñas y la actualización de las herramientas ya instaladas las medidas más populares. Las incidencias que en general promueven a los usuarios a cambiar contraseñas son la suplantación de identidad (60,4%) y la intrusión Wi-Fi (50%). El spam, incidencia más extendida, es la que menos motiva a los usuarios a modificar su comportamiento en la Red.

Conclusiones

CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

La confianza que los usurarios depositan en Internet es elevada: un 44% confía mucho o bastante en la Red mientras que solo un 1,4% desconfía totalmente de Internet. Así casi la mitad de los encuestados (45,8%) juzga Internet como cada día más seguro y un 70,9% estima que su ordenador y/o dispositivo Android está razonablemente protegido.

Para operaciones bancarias o de compra-venta, a los usuarios les da más confianza el trato personal que realizar estas acciones a través de la Red. La diferencia más notable –superior a 18 puntos porcentuales– se haya entre aquellos usuarios que confían en realizar operaciones bancarias en la sucursal (58,5%) y los que confían en efectuarlas online (39,9%). La operación que menos confianza genera entre los entrevistados es el pago a través de Internet utilizando la tarjeta de crédito/débito (35,6% de la población). En este ámbito, haber sufrido un intento de fraude o incluso un perjuicio económico no parece influir notablemente en el grado de confianza en los servicios de banca online y comercio electrónico.

El 45,7% de los usuarios tiene poca confianza o ninguna a la hora de facilitar sus datos personales mediante un e-mail o mensajería instantánea. La mayor tasa de confianza se presenta al facilitar datos en un organismo público físico (47,2%), o bien de manera online en portales de organismos públicos (42,6%).

Respecto al papel del propio usuario en la seguridad de Internet, **dos tercios piensan que la propagación de las amenazas a través de la Red se debe a la poca cautela de los usuarios**. Por contra **un 45,3% de los internautas se declara a favor de asumir determinados riesgos para disfrutar plenamente de la experiencia de navegar por Internet**.

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: 3.577 hogares encuestados y de ellos, 1.999 hogares encuestados y equipos/dispositivos Android escaneados (software instalado en 1298 PC's, 552 smartphones y/o 149 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 2015 mediante entrevistas online a partir de un panel de usuarios de Internet.

Error Muestral: Asumiendo criterios de muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5, y para un nivel de confianza del 95,5%, se establecen que al tamaño muestral n=3.577 le corresponde una estimación del error muestral igual a ±1,64%.

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:

Reservados todos los derechos. Se permite su copia y distribución por cualquier medio siempre que se mantenga el reconocimiento de sus autores, no se haga uso comercial de las obras y no se realice ninguna modificación de las mismas

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