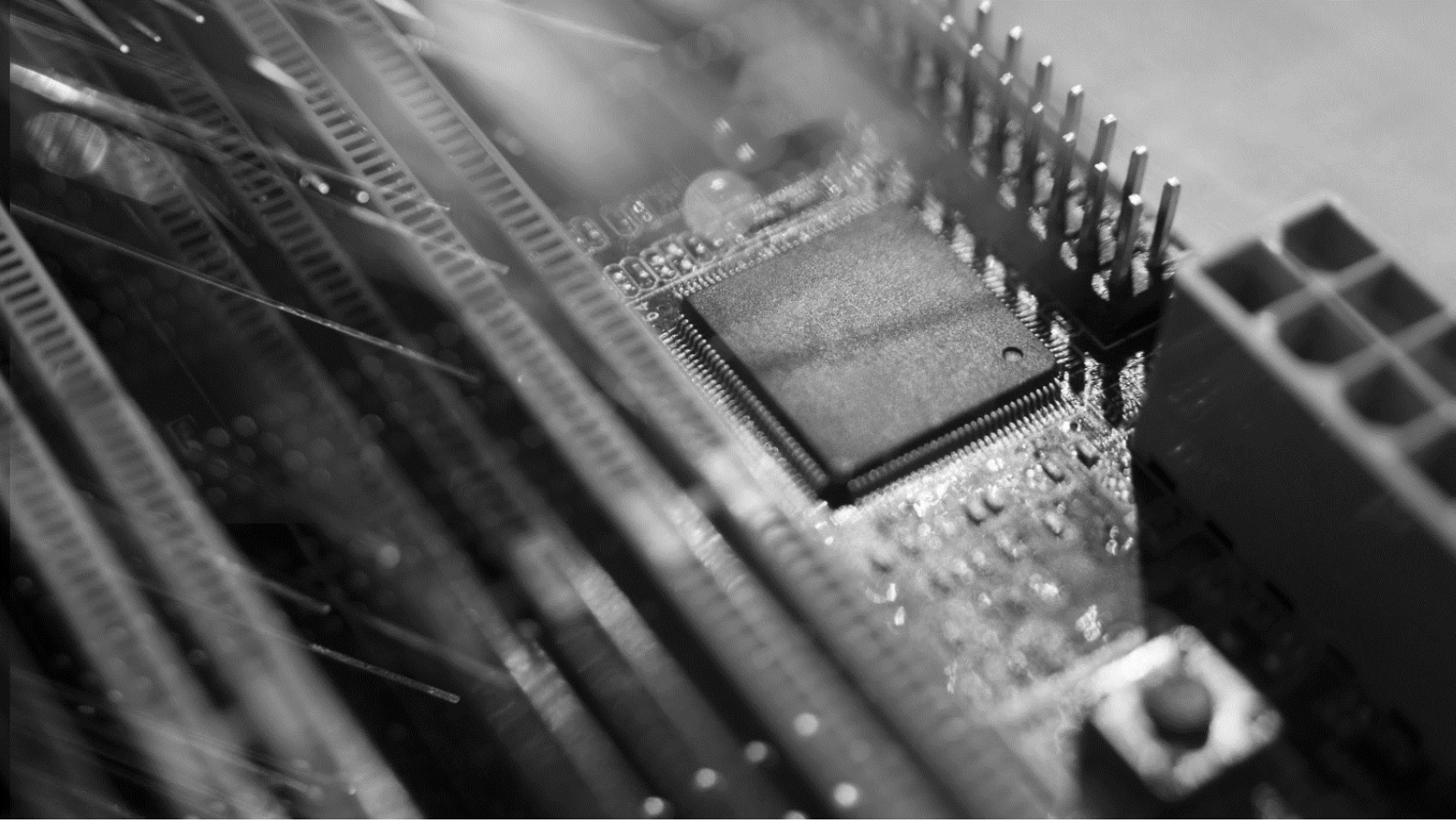


# ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

## Oleada Enero – Junio 2019

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA
ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

# ÍNDICE



# 1. ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

Red.es en colaboración con Hispasec Sistemas y GFK realiza un estudio para analizar la adopción de medidas de seguridad y evaluar las incidencias de situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que los hogares españoles depositan en el uso de las nuevas tecnologías de la información.

El objetivo de este estudio es el análisis del estado de los hogares españoles a través de indicadores de seguridad basados en la percepción de los usuarios sobre la misma, así como el nivel de confianza de éstos respecto a la seguridad y su evolución, haciendo un contraste comparativo con el nivel real de seguridad que mantienen tanto los equipos informáticos como los dispositivos Android. Se pretende impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe tiene como finalidad, entre otras, informar del comportamiento y utilización segura y privada de las nuevas tecnologías, además de servir como apoyo para solucionar incidencias por parte de los usuarios y la adopción de medidas por parte de la Administración.

El estudio se realiza a través de dos vías: el análisis de seguridad real de los equipos informáticos y dispositivos Android, mediante el escaneo con la herramienta Pinkerton y el análisis de las declaraciones aportadas por los internautas encuestados.

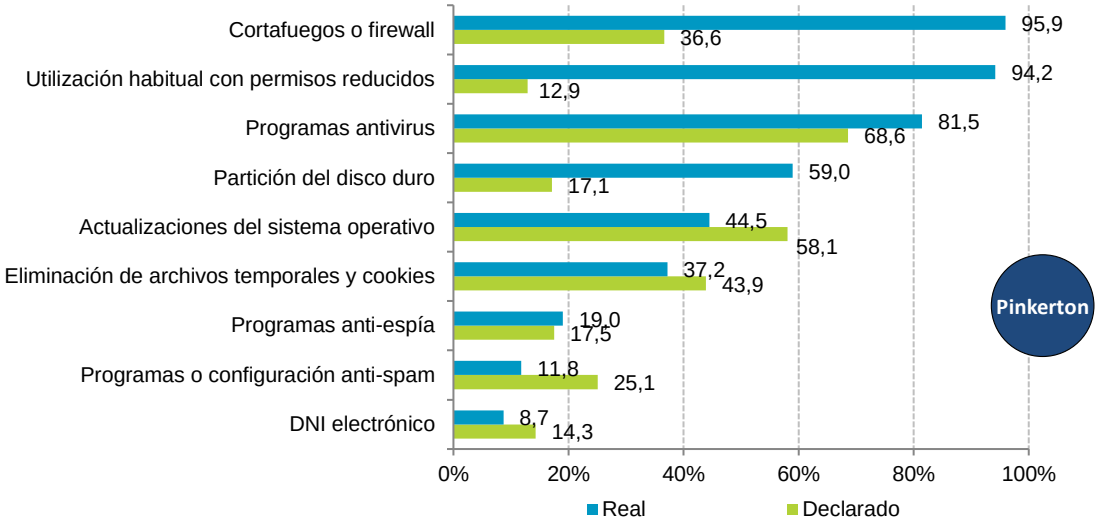
Los datos declarados son obtenidos de las encuestas online realizadas a los hogares que han conformado la muestra del estudio, mientras que para los datos reales se utiliza el software Pinkerton. Este software analiza los sistemas de PCs y dispositivos Android recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas, a la vez que detecta la presencia de *malware* en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 50 motores antivirus.

## 1.1 Medidas de seguridad

Resulta fundamental para la seguridad de la información conocer las medidas de seguridad disponibles a tal efecto, tanto las de tipo activo, que debe ejecutar directamente el usuario para que surtan efecto, como las de tipo pasivo, que no precisan de la acción directa del mismo.

A partir de las declaraciones de los usuarios españoles que participan en el estudio y de los datos recopilados mediante el análisis de sus equipos con la herramienta Pinkerton (ordenadores del hogar y dispositivos móviles), se han obtenido los siguientes resultados respecto a las medidas de seguridad, tanto activas como pasivas disponibles.

**FIGURA 1. USO DECLARADO VS. REAL DE MEDIDAS DE SEGURIDAD EN EL ORDENADOR DEL HOGAR (%)**




*Base: usuarios de PC*
*Fuente: Panel hogares, ONTSI*

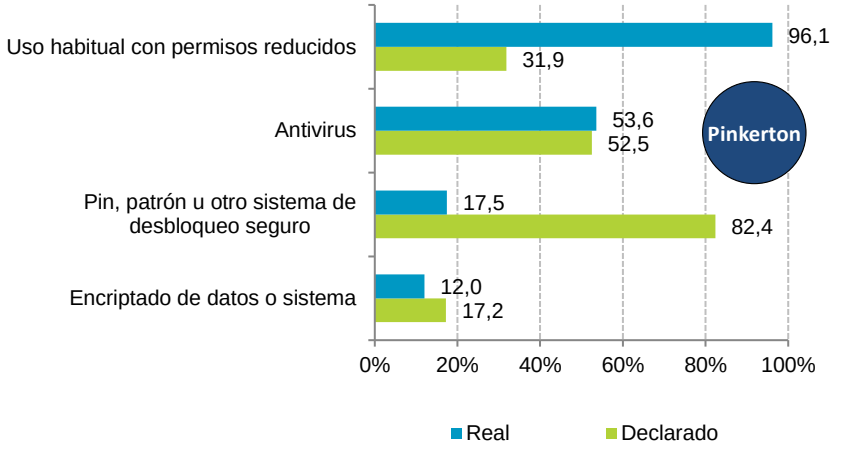
El uso de cortafuegos y el empleo de usuarios con permisos reducidos son, con diferencia, las medidas de seguridad más ampliamente utilizadas, apreciándose un ligero incremento en las mismas con respecto al semestre anterior, y situándose su uso real entorno al 95%. El uso de programas antivirus sigue siendo una medida bastante popular, situándose en el 81,5%, seguida del empleo de diferentes particiones del disco duro, con un 59,0% de uso real.

El uso del DNI electrónico no parece aumentar su popularidad permaneciendo por debajo del 10%, lo que la convierte en la medida de seguridad menos utilizada por los internautas españoles.

No obstante, los resultados obtenidos de los análisis tomados con Pinkerton en los ordenadores del hogar continúan arrojando grandes diferencias con respecto a las declaraciones de los usuarios. Dado que las diferencias más notables se aprecian en el uso de cortafuegos (59,3 p.p.), el empleo habitual del equipo con permisos reducidos (81,3 p.p.) y en el uso particionado del disco duro (41,9 p.p.), es de suponer que estas discrepancias se pueden deber probablemente al desconocimiento del usuario medio sobre la existencia de las mismas en su equipo.

La mayoría de los sistemas operativos actuales suelen incorporar un cortafuegos de serie, crean por defecto una cuenta con permisos limitados, y en aquellos casos en los que el SO viene preinstalado, suelen tener una partición oculta de recuperación, además que las últimas versiones de los sistemas operativos de Microsoft crean una partición de arranque de poca capacidad que también resulta invisible al usuario. De modo que si el usuario no es consciente de todo esto, al encender su ordenador se encontrará con un usuario con permisos reducidos, el cortafuego permanecerá activado, y trabajará sobre la partición de sistema y datos sin percatarse de ello.

**FIGURA 2. USO DECLARADO VS. REAL DE MEDIDAS DE SEGURIDAD EN DISPOSITIVOS ANDROID (%)**




*Base: usuarios de dispositivos Android*
*Fuente: Panel hogares, ONTSI*

La medida de seguridad más empleada en los dispositivos móviles es el uso habitual con permisos reducidos (96,1%), seguida a bastante distancia del antivirus (53,6%). Por otro lado, el cifrado de datos o del sistema apenas es utilizado (12,0%); y el uso de un sistema de desbloqueo seguro a pesar de que muchos usuarios declaran usarlo (82,4%), la herramienta Pinkerton registra que tan solo el 17,5% de los usuarios emplea realmente dicha medida de seguridad.

Se observa que tanto en el uso de antivirus como del cifrado de datos, la información recogida por Pinkerton y la declarada por los usuarios no difiere en exceso.

No obstante, en el caso del uso habitual con permisos reducidos, la herramienta Pinkerton demuestra que es empleada por muchos más usuarios de los que declaran usarla (64,2 p.p.). Esta discrepancia podría deberse a que la mayoría de los usuarios no son conscientes de que la configuración por defecto del sistema Android consiste en la creación de un usuario con privilegios limitados, de modo que para modificar esta condición y trabajar con un usuario administrador (root), es necesario manipular el terminal mediante un proceso software no trivial que puede suponer la pérdida de la garantía del fabricante al modificar sustancialmente el producto, o conllevar un riesgo para el terminal.

Respecto al uso de un sistema de desbloqueo seguro, se observa que una gran parte de los usuarios declara su empleo (82,4%), mientras que Pinkerton solo registra un reducido 17,5%. Esta diferencia (64,9 p.p.) parece que se debe a que la mayoría de los usuarios no es consciente de en qué consiste este sistema. Por lo que podrían responder afirmativamente a esta pregunta cuando en realidad lo que tienen activado en su terminal es el bloqueo automático de pantalla para evitar pulsaciones no deseadas, o un sistema de desbloqueo que no precise del uso de un código pin, un patrón de desbloqueo o una clave basada en sistemas biométricos que únicamente son conocidos por el usuario, pudiendo ser desactivado por cualquier persona simplemente pulsando el botón de encendido o desplazando la pantalla hacia un lateral.

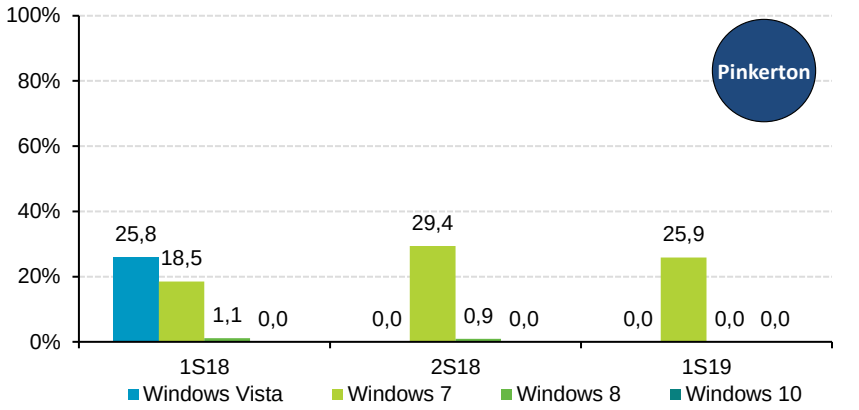
**USO HABITUAL CON PRIVILEGIOS REDUCIDOS EN WINDOWS (DATO REAL)[1]**

**100,0%**
CON PERMISOS REDUCIDOS EN WINDOWS 10

**100,0%**
CON PERMISOS REDUCIDOS EN WINDOWS 8

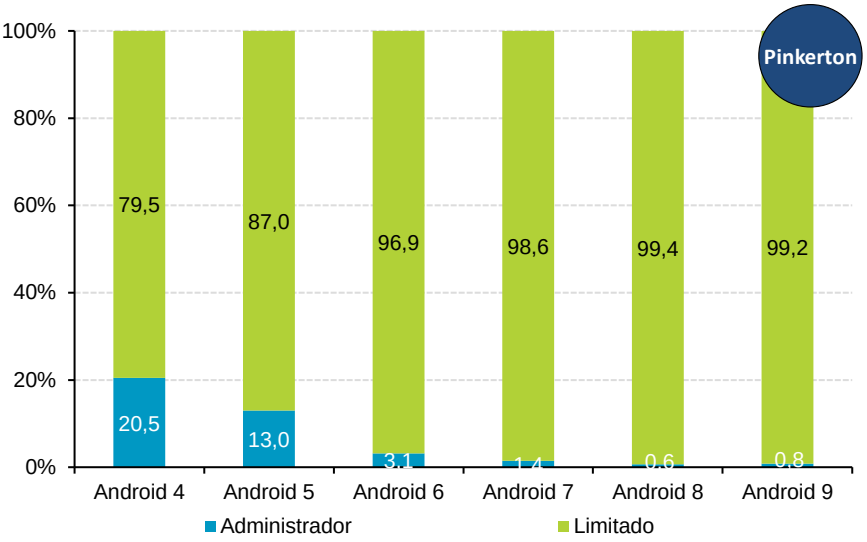
**74,1%**
CON PERMISOS REDUCIDOS EN WINDOWS 7

**FIGURA 3. EVOLUCIÓN DEL USO REAL DE PERFILES DE ADMINISTRADOR EN SISTEMAS OPERATIVOS MICROSOFT WINDOWS (%)[1]**




*Base: usuarios de Microsoft Windows*
*Fuente: Panel hogares, ONTSI*

**FIGURA 4. USO REAL DE PERFILES DE ADMINISTRADOR EN DISPOSITIVOS ANDROID (%)**




*Base: usuarios de dispositivos Android*
*Fuente: Panel hogares, ONTSI*

**USO HABITUAL CON PRIVILEGIOS REDUCIDOS EN ANDROID (DATO REAL)**

**99,2%**
CON PERMISOS REDUCIDOS EN ANDROID 9

**99,4%**
CON PERMISOS REDUCIDOS EN ANDROID 8

**98,6%**
CON PERMISOS REDUCIDOS EN ANDROID 7

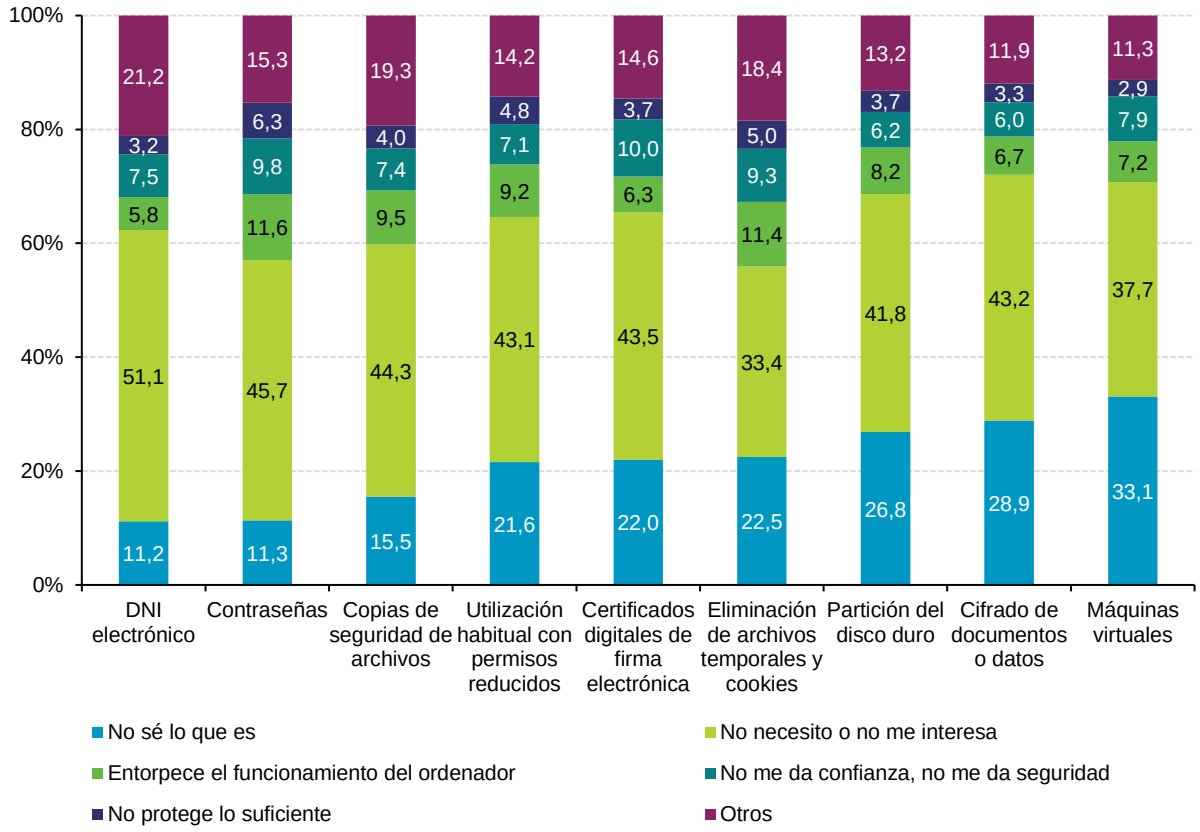
Se observa que el uso del perfil de administrador en sistemas Windows se limita a la versión Windows 7 (25,9%), siendo prácticamente nulo en el resto de versiones. En las últimas versiones de los sistemas operativos de Microsoft (Windows 8 y Windows 10), se trata de un hábito potenciado por el hecho de que se crea por defecto una cuenta con permisos reducidos.

En los dispositivos Android se observa un decremento importante en el uso de usuarios con privilegios de administrador conforme se trata de una versión de Android más reciente, siendo su uso inferior al 2% en las versiones Android 7 a Android 9. Mientras que en la versión Android 4 se observa que un 20,5% de los usuarios emplea habitualmente el terminal con privilegios de administrador, y en la versión Android 5 este porcentaje disminuye a un 13,0%.

[1] Desde el segundo semestre de 2018 hasta la actualidad, el uso del sistema operativo Microsoft Windows Vista ha sido meramente testimonial entre los panelistas por lo que los datos relativos a este no deben considerarse.

Posiblemente esta tendencia se deba a que para poder usar aplicaciones actuales en versiones del sistema operativo que ya han dejado de recibir soporte y actualizaciones por parte del fabricante, el usuario se ve forzado a modificar el sistema para elevar privilegios y poder instalar por otra vía los programas nuevos y actualizaciones.

**FIGURA 5. MOTIVOS DE NO UTILIZACIÓN DE MEDIDAS DE SEGURIDAD (%)**




*Base: usuarios que no utilizan alguna de las medidas de seguridad*
*Fuente: Panel hogares, ONTSI*

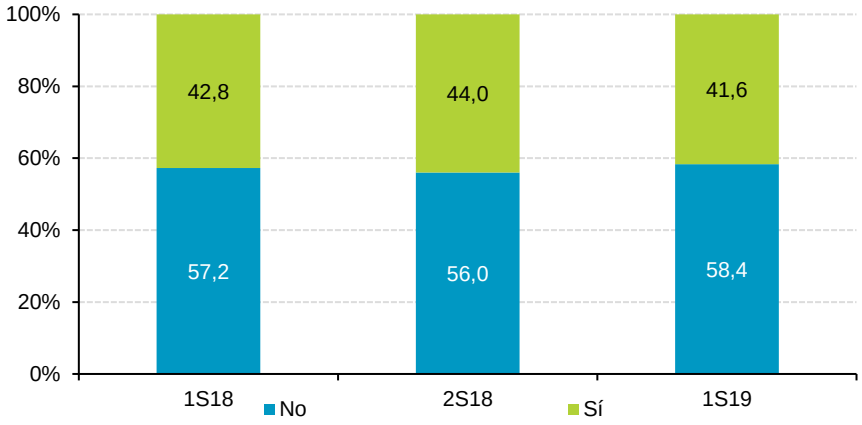
Según declaraciones de los usuarios, el principal motivo de no utilizar medidas de seguridad es el hecho de no considerarlas necesarias o de interés (entre 33,4% y 51,1% según la medida). La menos interesante para los internautas es el uso del DNI electrónico (51,1%), seguida del uso de contraseñas (45,7%).

En el caso de medidas que el usuario declara no emplear porque no las conoce, las más desconocidas son las máquinas virtuales (33,1%), el cifrado de documentos (28,9%) y las particiones del disco duro (26,8%).

## 1.2 Hábitos de comportamiento en la navegación y usos de Internet

Este semestre se aprecia un descenso en el porcentaje de usuarios que declara que adopta conductas de riesgo de forma consciente (-2,4 p.p.), por lo que la toma de consciencia sobre la importancia de los hábitos de uso seguro de Internet para prevenir incidencias empieza a aumentar, recuperándose del receso sufrido en los anteriores semestres.

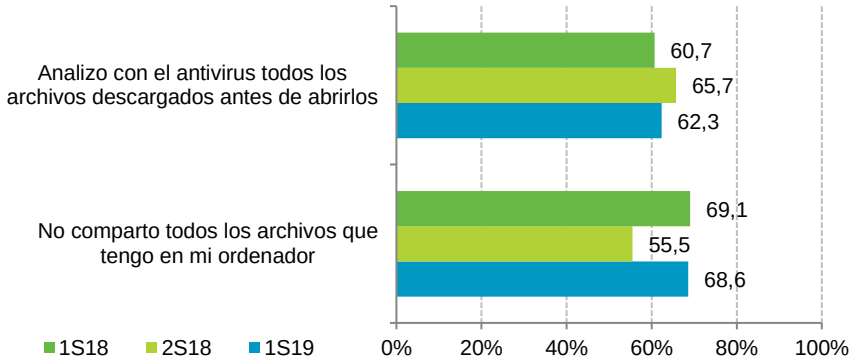
**FIGURA 6. EVOLUCIÓN DE LA ADOPCIÓN CONSCIENTE DE CONDUCTAS DE RIESGO (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

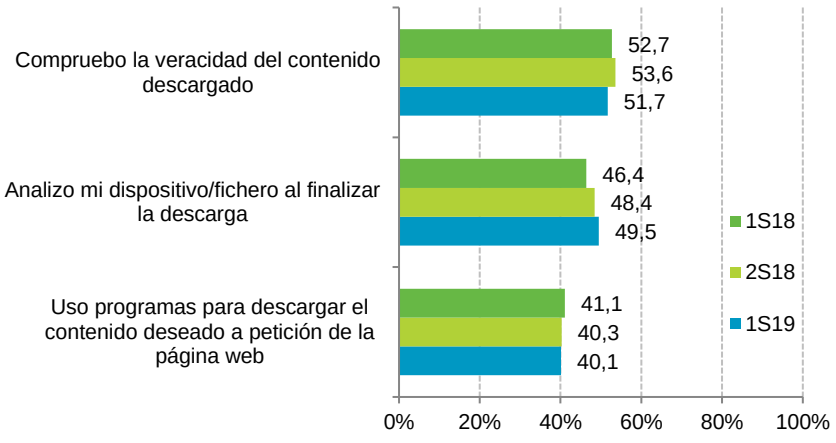
Durante el último semestre se aprecia un ligero aumento en el uso de medidas de seguridad asociado a una mayor consciencia sobre la necesidad de usar Internet de manera responsable y con los debidos hábitos recomendables de comportamiento y uso. No obstante, el crecimiento observado en el empleo de medidas de seguridad y en el número de usuarios que declara no adoptar conductas de riesgo de forma consciente sigue siendo moderado.

**FIGURA 7. DESCARGAS EN REDES P2P (%)**




*Base: usuarios de redes P2P*
*Fuente: Panel hogares, ONTSI*

**FIGURA 8. DESCARGAS EN INTERNET (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

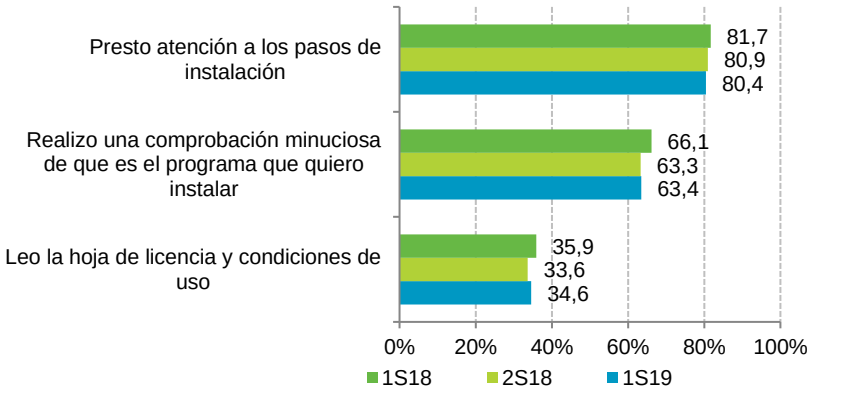
Analizando los datos obtenidos respecto a la gestión de descargas en redes P2P y las directas desde Internet se observa un ligero descenso en la asunción de hábitos prudentes, que salvo en el caso de la revisión con un antivirus de los archivos descargados (-3,4 p.p.), no se pueden considerar disminuciones significativas respecto a los datos obtenidos en el anterior semestre.

El cambio más significativo en cuanto a las conductas de seguridad tomadas respecto a las descargas de archivos se aprecia en la configuración de las carpetas compartidas en descargas en redes P2P, donde un 68,6% de los usuarios declara no compartir todos los archivos de su ordenador (+13,1 p.p.), por lo que se retorna a valores similares a los observados a principios de 2018 tras la repentina bajada sufrida durante el último semestre de dicho año.

Pese al significativo aumento de usuarios que restringen las carpetas compartidas en redes P2P, los resultados de los hábitos prudentes en este tipo de acciones pueden considerarse preocupantes debido a que aproximadamente la mitad de los usuarios no parece prestar la debida atención a los riesgos de seguridad que suponen los archivos descargados de Internet (ya sea por descarga directa o por redes P2P). Al no tratarse de archivos avalados por ninguna organización, son susceptibles de contener *malware*, estar corruptos (ser inutilizables o suponer un riesgo en la estabilidad del sistema), o incluso presentar contenidos distintos de los esperados o no deseado (no recomendables para menores).

Además, los sitios de descargas gratuitas suelen recurrir a métodos para obtener beneficios como el uso de botones falsos de descargas adicionales o la adición de adware u otro tipo de software no deseado, entre otras prácticas.

**FIGURA 9. INSTALACIÓN DE PROGRAMAS EN EL ORDENADOR DEL HOGAR (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Un alto porcentaje de los usuarios encuestados manifiestan prestar atención a los pasos de instalación, aunque como se puede observar, dicho porcentaje sigue mostrando tendencia a disminuir en comparación a semestres anteriores. Esta aparente confianza que poco a poco se va manifestando entre los usuarios puede deberse a la aparición de *markets* oficiales para los ordenadores (como Microsoft Store en Windows, Mac App Store para macOS, y los repositorios oficiales de cada distribución de Linux), en los que las aplicaciones ofertadas pasan unos estrictos controles de calidad y se presuponen libres de amenazas.

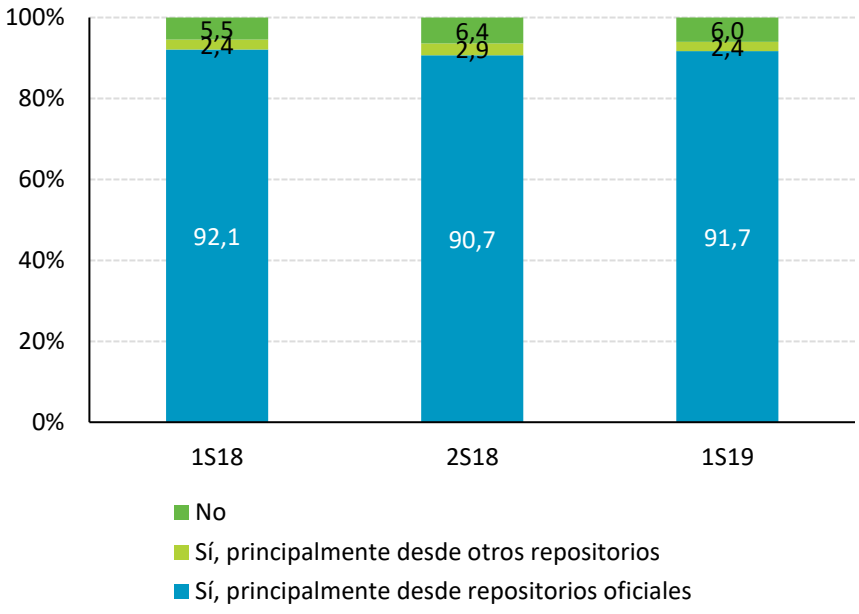
En cuanto a las comprobaciones minuciosas realizadas antes de instalar un programa determinado, el porcentaje con respecto al semestre anterior se ha mantenido estable, lo cual puede resultar preocupante si se compara con la caída de casi 3 p.p. con respecto al primer semestre de 2018, ya que esto demuestra, aparentemente, un exceso de confianza por parte de los usuarios en una época en la cual los ataques informáticos de todo tipo van en aumento.

Esta disminución en las comprobaciones también puede venir dada por la desidia del usuario al llevar a cabo un proceso de instalación que para quien carece de conocimientos básicos o medios sobre informática puede resultar tedioso. Esto también está relacionado con la lectura de la hoja de licencia y condiciones de uso que suele ser presentada con todo software que se instala en los ordenadores, algo que pocos usuarios, sobre todo domésticos, suelen hacer.

No obstante es reseñable el hecho de que, con respecto al segundo semestre de 2018, este porcentaje ha aumentado 1 p.p., algo que apunta a una toma de conciencia entre los usuarios, quienes parecen preocuparse más por saber qué tipo de condiciones están aceptando al instalar y utilizar un programa.

Cuando se descargan aplicaciones gratuitas es común encontrar durante los pasos de instalación solicitudes de instalación de aplicaciones de terceros que vienen preseleccionadas por defecto. Por ello, si no se presta la suficiente atención se puede acabar instalando software no deseado e incluso adware publicitario.

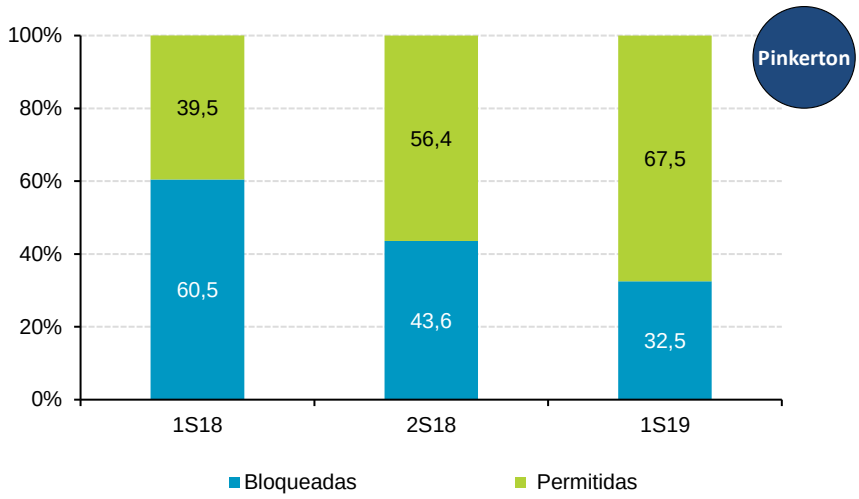
**FIGURA 10. EVOLUCIÓN DE LA DESCARGA DE APLICACIONES EN DISPOSITIVOS ANDROID (%)**




*Base: usuarios de dispositivos Android*
*Fuente: Panel hogares, ONTSI*

Según las declaraciones de los usuarios de dispositivos Android el 91,7% realiza la descarga de *apps* principalmente desde repositorios/ *markets* oficiales, lo cual puede responder más a la integración con el sistema y facilidad de uso que a cuestiones de seguridad.

**FIGURA 11. EVOLUCIÓN DEL ESTADO DE LAS FUENTES DESCONOCIDAS (%)**




*Base: usuarios de dispositivos Android*
*Fuente: Panel hogares, ONTSI*

Los datos reales recogidos por Pinkerton revelan que los usuarios están asumiendo cada vez más riesgos a la hora de instalar aplicaciones en sus dispositivos Android y han modificado la configuración por defecto para permitir la instalación de aplicaciones mediante fuentes desconocidas. Desde 2017 se ha experimentado una tendencia al alza de este permiso, que se traduce en un incremento de 28 p.p. llegándose, durante el primer semestre de 2019, a invertir los valores obtenidos en estudios anteriores (2015-2016).

Instalar aplicaciones móviles procedentes de *markets* no oficiales supone asumir un alto riesgo para la seguridad de los dispositivos ya que estos repositorios no cuentan con medidas de análisis y detección de aplicaciones fraudulentas en sus almacenes, así como tampoco se controla la procedencia de las mismas. El principal reclamo para el usuario suele ser encontrar contenido de pago de forma gratuita.

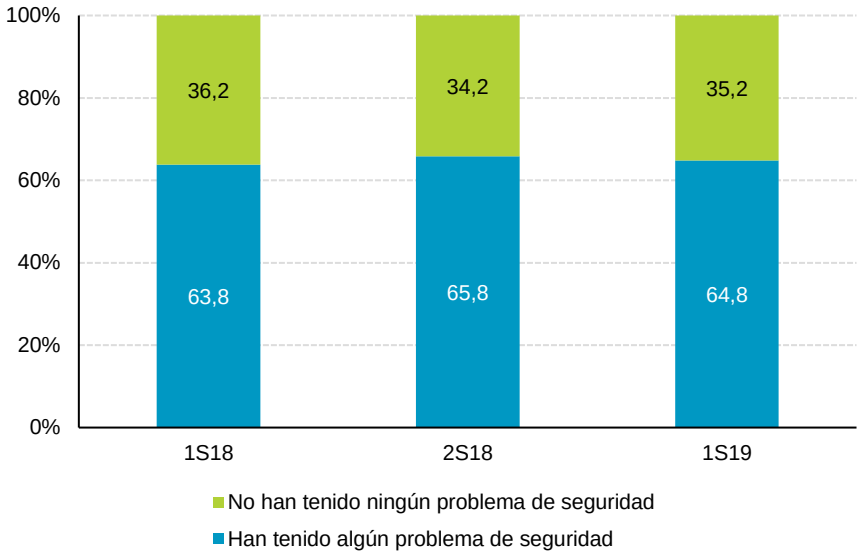
Es importante mencionar la existencia de *droppers –malware* cuya función es descargar otros códigos maliciosos para instalarlos en el sistema infectado– que suponen un riesgo adicional para todos aquellos dispositivos en los que la opción de permitir la instalación de aplicaciones desde fuentes desconocidas ha sido activada.

## 1.3 Incidentes de seguridad

Las amenazas se encuentran en continua evolución y tratan de evadir las posibles barreras tanto a nivel de usuario como de sistema o incluso antivirus lo que convierte en imposible tener métodos infalibles que eviten incidentes de seguridad. Esto significa que la utilización de las diferentes medidas de seguridad y la práctica de hábitos prudentes reducen el riesgo de que las incidencias de seguridad ocurran, pero este siempre estará presente.

En este apartado se analizan los incidentes de seguridad sufridos por los encuestados en el periodo comprendido entre enero y junio de 2019.

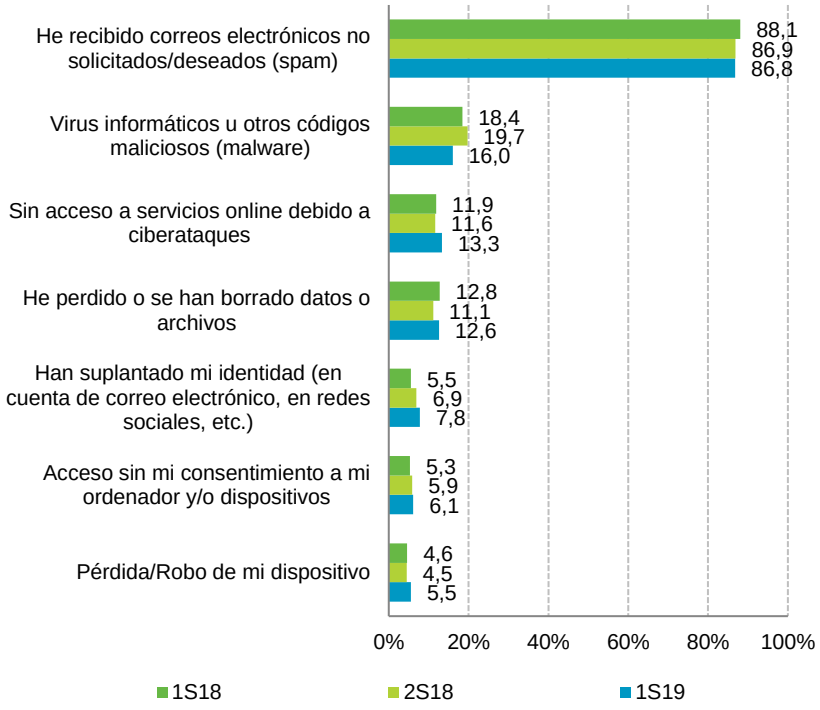
**FIGURA 12. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Se aprecia una disminución de 1 p.p. del total de usuarios que reportan algún problema relativo a la seguridad este semestre. Se aprecia que uno de cada tres usuarios (35,2%) declara que no ha tenido ningún problema de seguridad, o no es consciente de ello, frente a casi dos tercios de afectados. Este dato puede correlarse con la adopción consciente de conductas de riesgo (**FIGURA 6**) mostrándose una estrecha relación entre ambos.

**FIGURA 13. EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)**




*Base: usuarios que han sufrido alguna incidencia de seguridad*
*Fuente: Panel hogares, ONTSI*

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

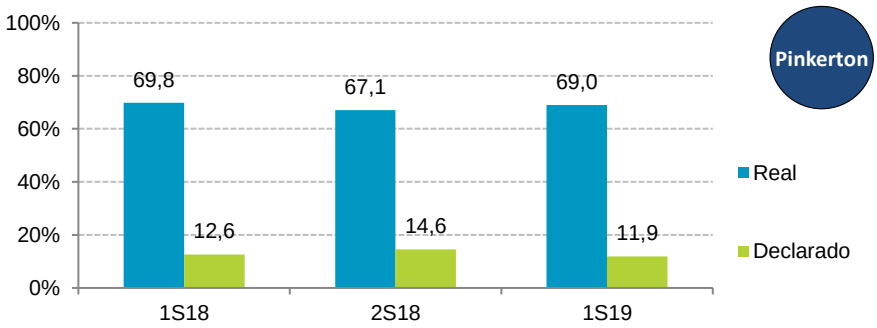
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras muchas tipologías.

Como es de esperar las campañas de SPAM encabezan la lista con un 86,8 % de declaraciones, un valor muy por encima del resto de incidencias. No se observan cambios significativos con respecto a la oleada anterior pero sí una disminución de 1,3 p.p desde el año pasado.

Los usuarios consideran que el *malware* ha disminuido significativamente, notándose una disminución en las respuestas afirmativas de -3,7 p.p, desde la pasada oleada. Siendo esta la única de las opciones que tiene una notable mejoría frente a las demás.

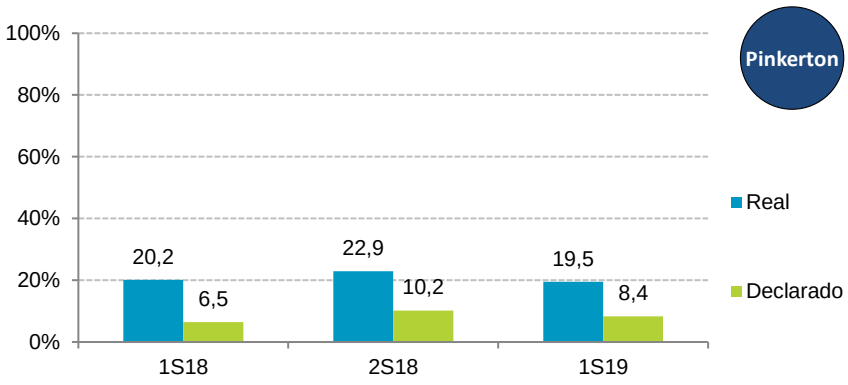
En las siguientes figuras se realizará un análisis más detallado sobre el *malware* con objeto de determinar si la percepción del usuario en lo referente a ese tipo de incidencias se asemeja a la realidad, o se trata de una amenaza oculta que continúa pasando desapercibida para la mayoría de internautas.

**FIGURA 14. EVOLUCIÓN DE LAS INCIDENCIAS DE MALWARE (DECLARADO VS. REAL) EN EL ORDENADOR DEL HOGAR (%)**




*Base: usuarios de PC*
*Fuente: Panel hogares, ONTSI*

**FIGURA 15. EVOLUCIÓN DE LAS INCIDENCIAS DE MALWARE (DECLARADO VS. REAL) EN DISPOSITIVOS ANDROID (%)**




*Base: usuarios de dispositivos Android*
*Fuente: Panel hogares, ONTSI*

**ORDENADORES QUE ALOJAN MALWARE (DATO REAL VS. PERCEPCIÓN)**

**69,0%**
**DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE**

**11,9%**
**DE LOS USUARIOS PERCIBEN MALWARE EN SUS ORDENADORES PERSONALES**

Como viene siendo habitual, los datos reales arrojados por Pinkerton muestran unos resultados muy dispares con respecto a las incidencias reportadas por los usuarios relacionadas con *malware*.

La situación es realmente preocupante ya que el 69% de los ordenadores del hogar alberga algún tipo de *malware*. Sin embargo el punto positivo es que esta cifra sigue siendo menor que la observada en el segundo semestre de 2017 y primero de 2018.

**DISPOSITIVOS ANDROID QUE ALOJAN MALWARE (DATO REAL VS. PERCEPCIÓN)**

**19,5%**
DE LOS DISPOSITIVOS ANDROID ESCANEADOS CON PINKERTON ALOJAN MALWARE

**8,4%**
DE LOS USUARIOS PERCIBEN MALWARE EN SUS DISPOSITIVOS ANDROID

La brecha existente entre la realidad y lo declarado por los usuarios sigue siendo uno de los puntos más preocupantes del estudio, más aún si cabe si se observa que las declaraciones al respecto han seguido una tendencia a la baja desde el año 2016 (**FIGURA 13** y **FIGURA 14**).

En el caso de los dispositivos Android han disminuido tanto las detecciones de *malware* de forma consciente por los usuarios (-1,8 p.p) como las detecciones reales recogidas por Pinkerton (-3,4 p.p).

**TABLA 1. INCIDENCIAS DE MALWARE EN EL ORDENADOR DEL HOGAR (%)**

Pinkerton

| Declararon tener malware en PC | Su PC presentaba malware | | |
|---|---|---|---|
| | Sí | No | Total |
| Sí | 8,1 | 2,3 | 10,4 |
| No | 60,9 | 28,7 | 89,6 |
| Total | 69,1 | 30,9 | 100 |

*Base: usuarios con PC escaneado*
*Fuente: Panel hogares, ONTSI*

**TABLA 2. INCIDENCIAS DE MALWARE EN DISPOSITIVOS ANDROID (%)**

Pinkerton

| Declararon tener malware en Android | Su Android presentaba malware | | |
|---|---|---|---|
| | Sí | No | Total |
| Sí | 1,2 | 5,2 | 6,4 |
| No | 18,4 | 75,2 | 93,6 |
| Total | 19,6 | 80,4 | 100 |

*Base: usuarios con dispositivo Android escaneado*
*Fuente: Panel hogares, ONTSI*

En las **TABLA 1** y **TABLA 2**, se han comparado las declaraciones de los usuarios con los datos reales de cada dispositivo escaneado para analizar la brecha existente entre los datos recogidos. Esta práctica nos permitirá descartar conclusiones erróneas que puedan ser consecuencia de posibles fallos en los dispositivos que no son causa de malware sino de configuraciones mal efectuadas.

Se puede observar que una pequeña parte de los usuarios era consciente de la infección de sus ordenadores (8,1%) y dispositivos (1,2%) y además no habían tomado medidas para solventar dicha situación -por desconocimiento sobre cómo hacerlo, por estar a la espera de recibir soporte técnico, o incluso por no darle la suficiente importancia a este tipo de incidencias- al menos hasta el momento del análisis realizado por Pinkerton.

Por otro lado se encuentran aquellos usuarios que habiendo detectado una infección de malware supieron reaccionar y desinfectar su equipo, o que ante un comportamiento extraño del equipo sospecharon de un virus como el causante. Este grupo está

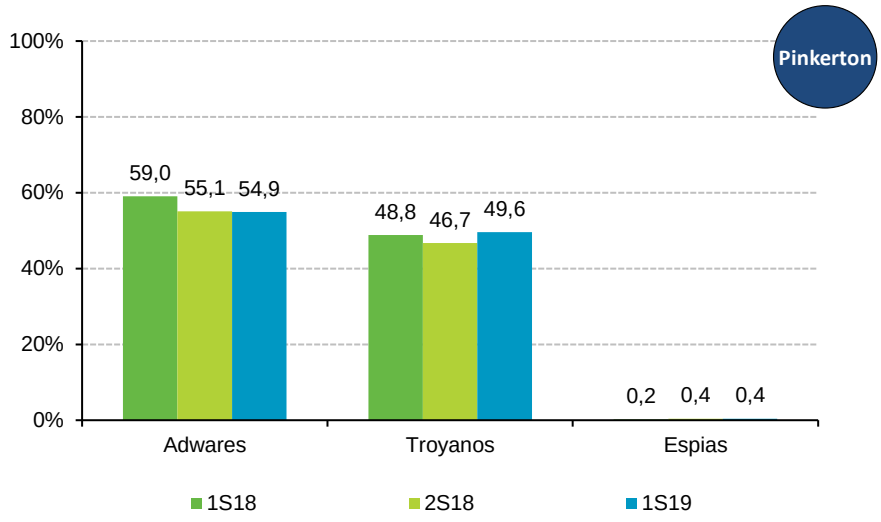
formado por los usuarios que afirmaron que su PC (2,3%) o dispositivo Android (5,2%) tenía malware, mientras que Pinkerton no encontró rastro de ninguna amenaza de este tipo.

Pese a las mejoras recogidas, el dato más destacable sigue siendo el de aquellos que declaran no haber sufrido ningún incidente de seguridad relacionado con *malware* aunque los análisis realizados por Pinkerton indican que los equipos estaban comprometidos. En esta situación se encuentran el 60,9% de los ordenadores del hogar y el 18,4% de los teléfonos Android analizados con Pinkerton. A este respecto, la situación actual es bastante preocupante, no únicamente por las infecciones sino por la falta de percepción de los usuarios.

La única mejora real con respecto a la oleada anterior se puede apreciar en los usuarios de Android que declaran no tener malware pero su dispositivo sí presenta algún tipo de infección, habiendo bajado la muestra en -3 p.p.

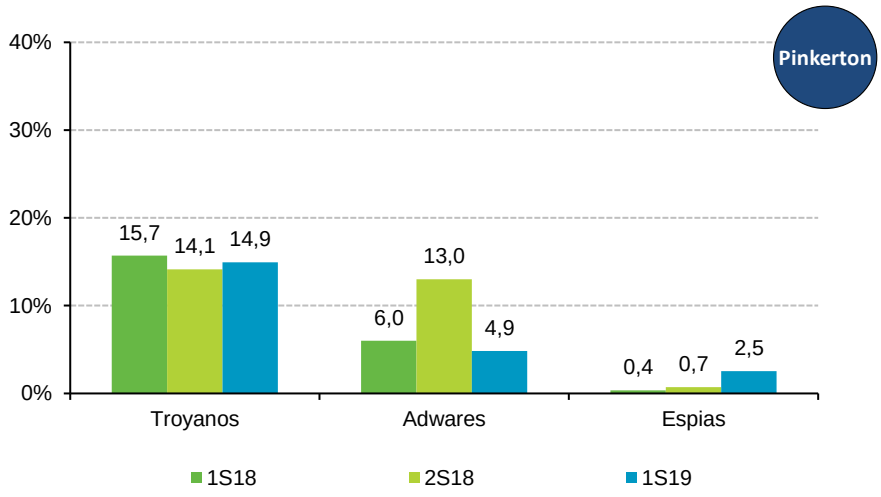
**FIGURA 16. EVOLUCIÓN DEL MALWARE EN EL ORDENADOR DEL HOGAR (%)**

Los ordenadores del hogar se encuentran afectados principalmente por *adware* y troyanos




*Base: Total ordenadores*
*Fuente: Panel hogares, ONTSI*

**FIGURA 17. EVOLUCIÓN DEL MALWARE EN DISPOSITIVOS ANDROID (%)**




*Base: Total dispositivos Android*
*Fuente: Panel hogares, ONTSI*

Existen dos estrategias diferentes que utilizan los atacantes a la hora de diseñar el *malware* e infectar a la víctima para conseguir sus objetivos.

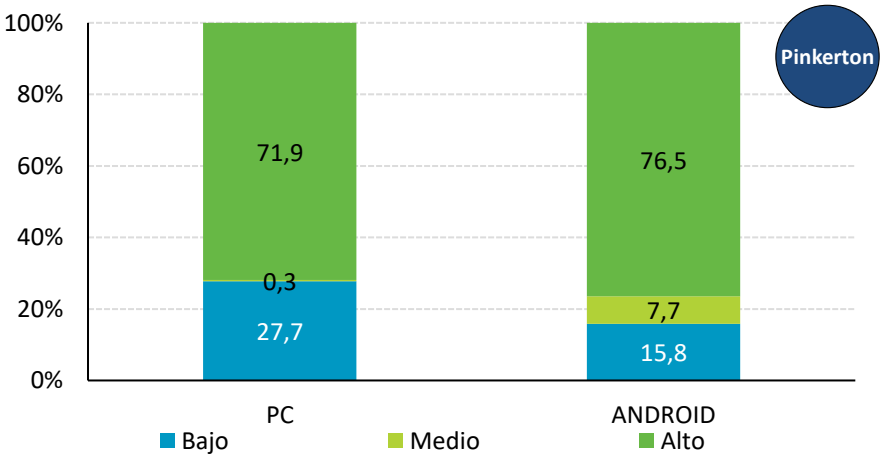
Una de ellas consiste en incluir el contenido malicioso a simple vista en el PC o dispositivo Android del usuario para conseguir ingresos a partir de anuncios que se muestran en el dispositivo sin autorización (Adware publicitario), la implementación de barras de complementos en el navegador, o de forma más agresiva, pidiendo un rescate a cambio de los archivos cifrados del dispositivo (ransomware). La otra, por el contrario, utiliza tácticas para lograr que el *malware* pase desapercibido ante soluciones antivirus e incluso del usuario del sistema, de manera que llegue a conseguir aquello para lo que ha sido diseñado, ya sea la obtención de credenciales bancarias, cuentas de email, o cualquier información con la que se pueda obtener un beneficio económico.

Se observa como la presencia de código malicioso en el PC se incrementa respecto a los meses anteriores en el caso de los troyanos (+2,9 p.p) siendo este el valor más alto respecto a las dos oleadas anteriores. En el caso de los programas espías, el cómputo de usuarios infectados apenas llega al 0,4% por lo que es casi inexistente. En el caso del *adware* publicitario, que sigue siendo el preferido de los atacantes, prácticamente se mantiene el número de infecciones con respecto a la oleada anterior.

En lo referente a *malware* en dispositivos Android, estos son diferentes en tanto que existe una presencia mayor de troyanos que de *adware*, aunque el total de malware es mucho menor en Android frente a PCs. A pesar del aumento que hubo en las campañas de Adware en la oleada anterior, su nivel de incidencia vuelve a descender quedando por debajo de los resultados del primer semestre de 2018 (-1,1 p.p.). Este hecho podría estar relacionado con la renovación del parque de dispositivos fomentada en las campañas navideñas.

El 71,9% de los ordenadores y el 76,5% de los dispositivos Android infectados con *malware* se encuentran en un nivel de riesgo alto

**FIGURA 18. NIVEL DE RIESGO EN EL ORDENADOR DEL HOGAR Y EN DISPOSITIVOS ANDROID (%)**




*Base: PCs y dispositivos Android que alojan malware*
*Fuente: Panel hogares, ONTSI*

Tras haber analizado el nivel de peligrosidad de las diferentes tipologías de *malware* encontrado por Pinkerton se ha estimado que el 71,9% de los ordenadores y el 76,5% de los dispositivos Android se encuentran ante niveles de riesgo altos que, muestran una subida de +2,9 p.p en PC.

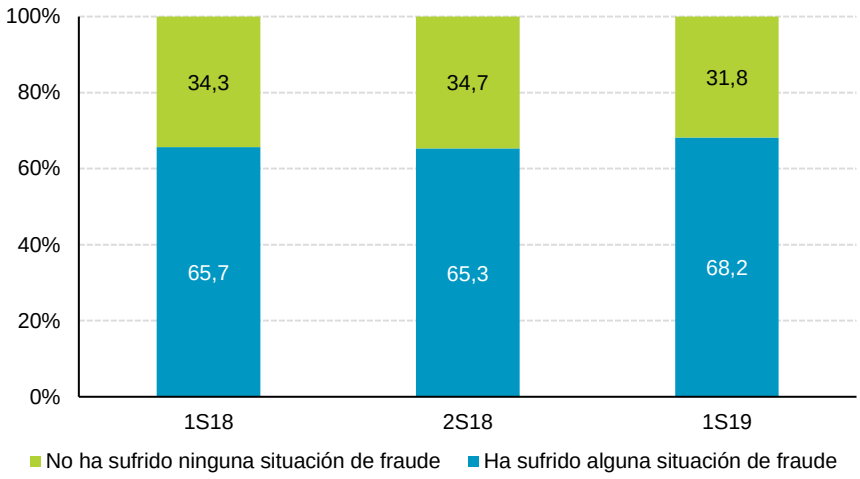
Estos datos elevan aun más si cabe la preocupación del panorama actual debido a la amenaza velada que supone el *malware* (**FIGURA 13**, **TABLA 1** y **TABLA 2**).

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

Cuando se sufren las consecuencias de una incidencia es habitual que los usuarios quieran aprender a prevenir esas situaciones para que no se vuelvan a repetir. Por lo que podría traducirse en un cambio de hábitos y la adquisición de otros más prudentes a la hora de navegar por Internet, así como en el incremento de las medidas de seguridad utilizadas.

En este apartado se analizarán estas reacciones de los usuarios ante los incidentes de seguridad experimentados.

**FIGURA 19. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)**



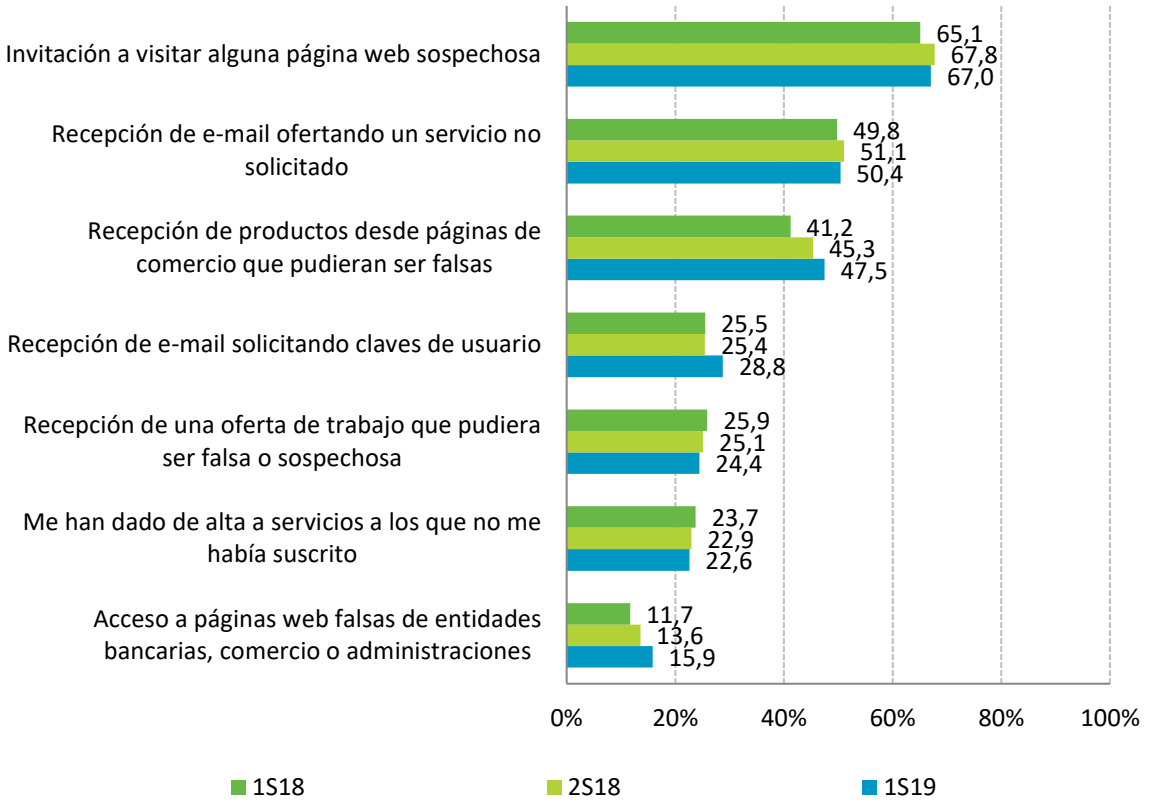

*Base: Total usuarios*
*Fuente: Panel hogares, ONTSI*

Más de dos tercios de los internautas (68,2%) declaran haberse visto expuestos a alguna situación de fraude –consumado o no– durante el primer semestre de 2019. Mostrando un incremento de 2,9 p.p con respecto a la pasada edición.

Se debe tener en cuenta que la alta incidencia de este tipo de delitos llevados a cabo en Internet no se debe solo a la falta de precaución o conocimiento por parte del usuario, sino que también los métodos de fraude van evolucionando continuamente tanto en su parte técnica como en las estrategias de ingeniería social empleadas (que se basan en explotar la falta de conocimiento del usuario y su confianza e interés), por lo que resulta difícil adoptar medidas de protección y concienciación frente a todos y cada uno de estos métodos fraudulentos.

Los intentos de fraude pueden presentarse de muy diversas formas ante el usuario para lograr su cometido y que éstos se conviertan en víctimas. En la siguiente gráfica se analizan las principales formas en las que se manifiestan los intentos de fraude según la percepción de los internautas españoles.

**FIGURA 20. EVOLUCIÓN DE LA MANIFESTACIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)**




*Base: Usuarios que han sufrido un intento de fraude*
*Fuente: Panel hogares, ONTSI*

Las invitaciones a visitar páginas web sospechosas (67%) y la recepción de e-mails ofertando servicios no solicitados (50,4%) continúan liderando el ranking como las principales formas en que los intentos de fraude se manifiestan.

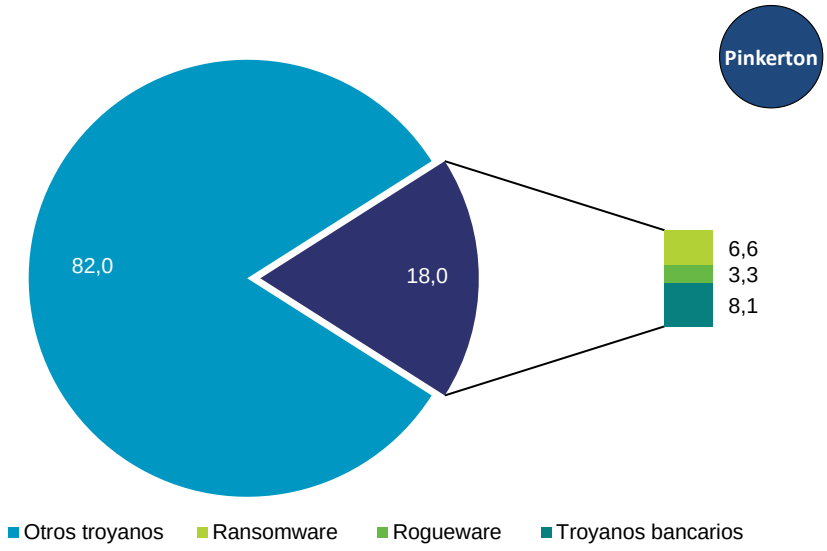
Cabe destacar también la tendencia al alza expuesta por la recepción de productos desde páginas de comercio electrónico que pudieran ser falsas (+2,2 p.p.), el acceso a páginas web falsas de entidades bancarias, comercio o Administraciones (+2,3 p.p), y la recepción de e-mails solicitando claves de usuario (+3,4 p.p).

El envío de *spam* supone una de las vías principales de difusión de los intentos de fraude (**FIGURA 13**), aunque también pueden llegar a los usuarios a través de publicaciones o mensajes en redes sociales y mensajes SMS. A este respecto, cabe la posibilidad de que muchos de los intentos de fraude puedan verse frustrados debido a las medidas de seguridad que incorporan tanto los servicios de correo electrónico como las propias redes sociales. Esto explicaría que el phishing -páginas web falsas de entidades bancarias o comercios electrónicos para obtener los credenciales de los usuarios- ocupen la última posición de la lista. Aunque también podría ser una amenaza que pasa desapercibida para el usuario debido a que copia perfectamente la imagen del sitio web oficial al que intenta suplantar

También resulta común que los fraudes online se presenten ante el usuario simulando ser encuestas o concursos legítimos que, suplantando a alguna entidad o marca popular, ofrecen premios, cupones descuento, cheques regalo o cualquier otro tipo de gancho para lograr que un usuario incauto proporcione

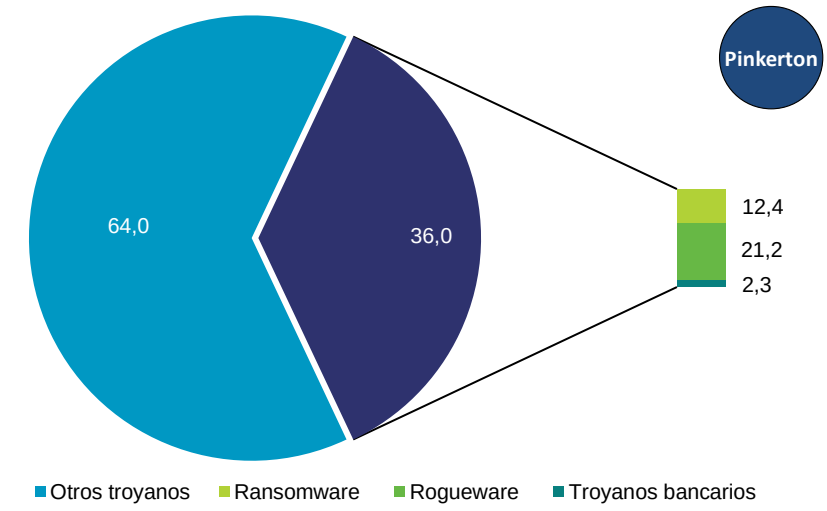
información personal y, sin percatarse, acepte recibir promociones, servicios no solicitados (50,4%) y publicidad no deseada (nuevamente *SPAM*), el alta en servicios de *SMS Premium* (22,6%), instalar algún tipo de programa o aplicación no segura –y potencialmente maliciosa–, etc.

**FIGURA 21. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN EL ORDENADOR DEL HOGAR (%)**




*Base: Equipos con troyanos detectados en PC*
*Fuente: Panel hogares, ONTSI*

**FIGURA 22. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN DISPOSITIVOS ANDROID (%)**




*Base: Equipos con troyanos detectados en dispositivos Android*
*Fuente: Panel hogares, ONTSI*

**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 solicita al usuario el pago de una cantidad monetaria como rescate (*ransom* en inglés).

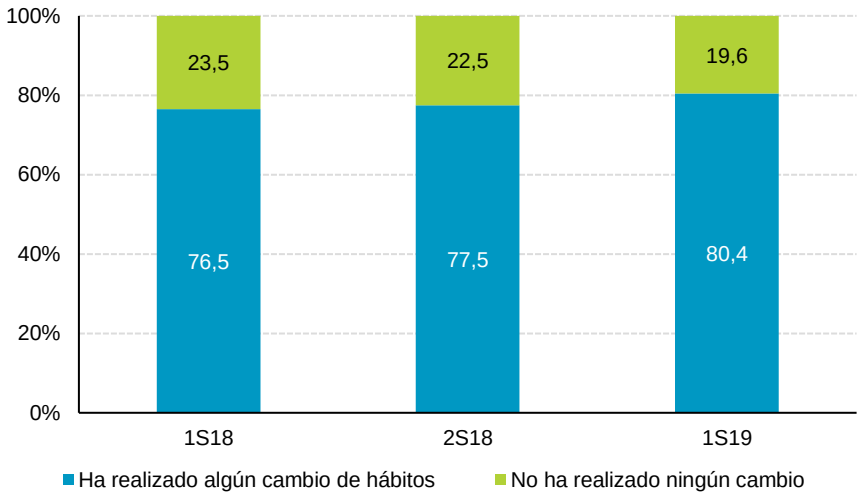
En los ordenadores del hogar despuntan los troyanos de tipo bancario. Este enfoque de los desarrolladores de malware puede deberse a la tendencia de antaño de utilizar el PC para realizar las compras online, administrar las cuentas bancarias, y otros usos relacionados con la economía, aunque los dispositivos móviles están desplazando al PC en estos ámbitos también. Además los ordenadores suelen ser compartidos por los diferentes miembros del hogar, siendo habitual el uso del mismo usuario para todos -a veces incluso una cuenta de administrador- en lugar de la creación de diferentes perfiles para cada uno de los usuarios. Esto se puede

considerar un hábito bastante peligroso debido a la potencial asunción de riesgos que cada usuario asume en momentos determinados y con el desconocimiento del resto, derivando en que estos tampoco tomen precauciones durante la utilización del equipo.

En los dispositivos Android destacan claramente las infecciones provocadas por el *rogueware* (21,2%). Este tipo de *malware* trata de engañar a la víctima informando o simulando la detección de una falsa infección en su dispositivo para incitarles a instalar otras aplicaciones maliciosas.

**FIGURA 23. EVOLUCIÓN DE LAS REACCIONES ADOPTADAS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%)**

Cuatro de cada cinco internautas españoles modifica sus hábitos prudentes tras experimentar una incidencia de seguridad



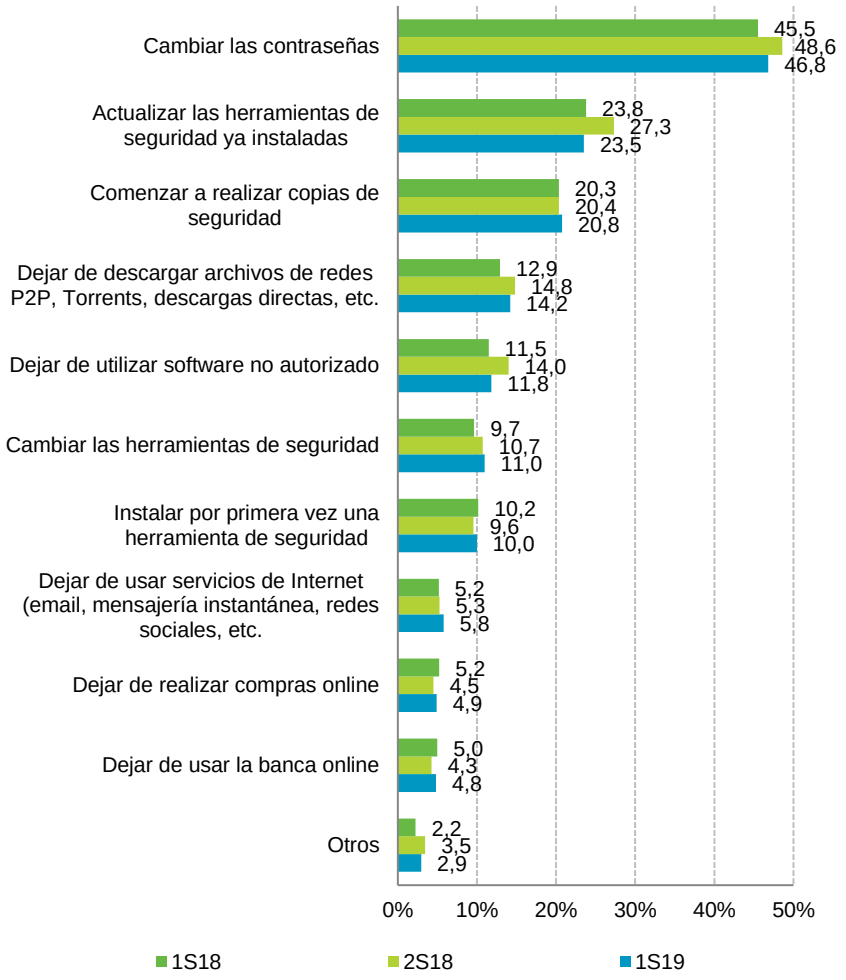

*Base: Usuarios que han sufrido un incidente de seguridad*
*Fuente: Panel hogares, ONTSI*

Durante este primer semestre de 2019 se continúa observando una tendencia al alza por parte del usuario a modificar sus hábitos prudentes y uso de medidas de seguridad tras sufrir un incidente de seguridad. Los valores vuelven a incrementarse y muestran una tendencia positiva por parte de los usuarios para modificar sus hábitos prudentes (+2,9 p.p. por encima de 2S18).

No obstante, a pesar del aspecto positivo del incremento en el porcentaje de personas que optan por modificar sus hábitos al hacer uso de Internet, se debería poner el foco de atención en la consecución de un objetivo que trate de lograr que los usuarios se decidan por implementar prácticas para prevenir la ocurrencia de los mismos.

En este primer semestre de 2019 se ha registrado una pequeña caída en el cambio de contraseñas (-1,8 p.p) que, aunque no es algo significativamente notable, puede deberse a que en la pasada oleada se reportaron numerosos casos de *leaks* (o fugas de información) que aparecieron en distintos medios de comunicación con el consecuente incremento del número de usuarios que actualizaron sus contraseñas, y en este pequeño período de tiempo, los usuarios no han considerado que fuese imprescindible una nueva modificación. No obstante, es conveniente recordar que se recomienda cambiar la contraseña de forma periódica –se haya experimentado algún incidente de seguridad o no– y no utilizar la misma para diferentes servicios.

**FIGURA 24. EVOLUCIÓN DE LOS CAMBIOS DE HÁBITOS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%)**




*Base: Usuarios que realizan algún cambio de hábitos tras sufrir un incidente de seguridad*
*Fuente: Panel hogares, ONTSI*

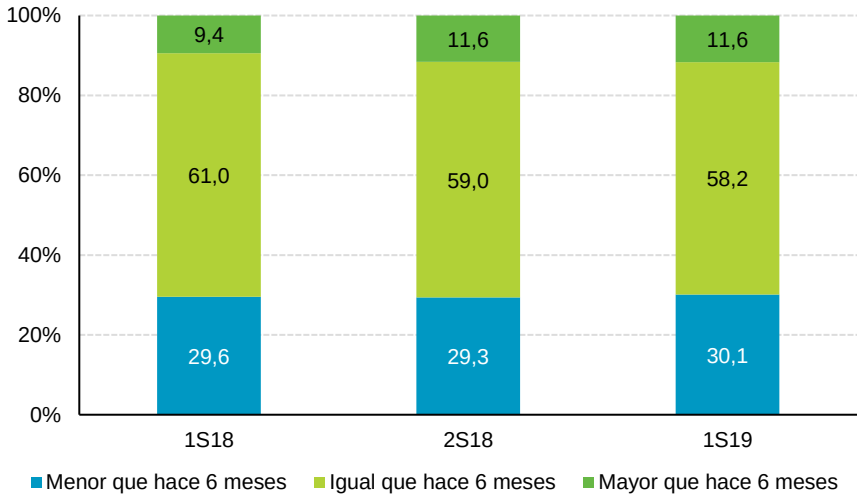
En segundo lugar se haya la actualización de las herramientas de seguridad instaladas en los dispositivos (23,5%), un aspecto muy importante a tener en cuenta para mantener los equipos y dispositivos libres de amenazas ya que no cesa la evolución de estas últimas. A pesar de su importancia, se ha registrado una marcada bajada en la actualización de dichas herramienta, algo que puede llevar a generar nuevas brechas de seguridad.

En cuanto a la realización de copias de seguridad, esta se mantiene estable (20,8%), aunque parece que poco a poco va aumentando. No obstante, pese a que se recomienda encarecidamente el realizar copias de seguridad con frecuencia para prevenir la pérdida de datos, en caso de un incidente se seguridad, apenas uno de cada cinco usuarios declara empezar a realizarlas tras haber sufrido un incidente, alcanzando el 44,3% de los encuestados aquellos que siguen considerándola una práctica innecesaria (**FIGURA 5**).

## 1.5 Confianza en el ámbito digital en los hogares españoles

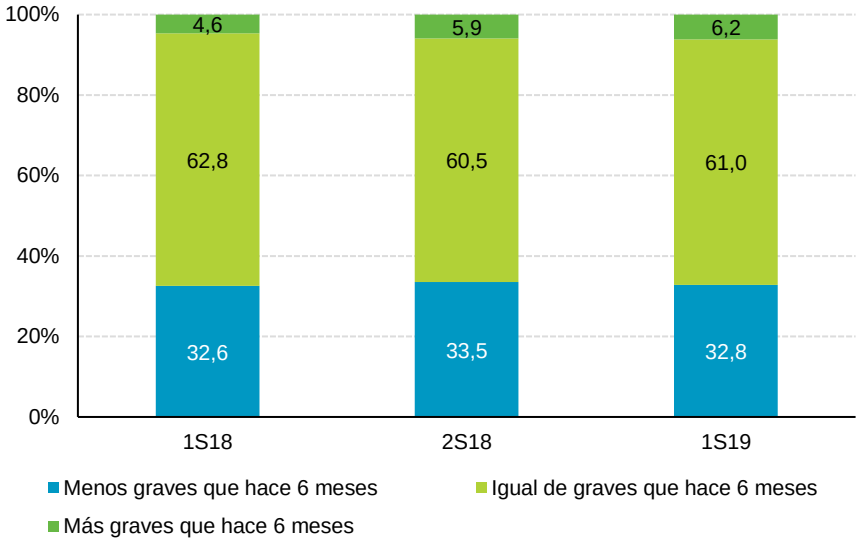
Para finalizar el estudio se realiza un análisis de la opinión y valoración de los usuarios acerca de los riesgos y peligros que se encuentran en Internet, sus consideraciones acerca de la responsabilidad propia en cuanto a la seguridad, y la confianza que tienen en la Red de Redes.

**FIGURA 25. EVOLUCIÓN DE LA PERCEPCIÓN DE LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

**FIGURA 26. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%)**

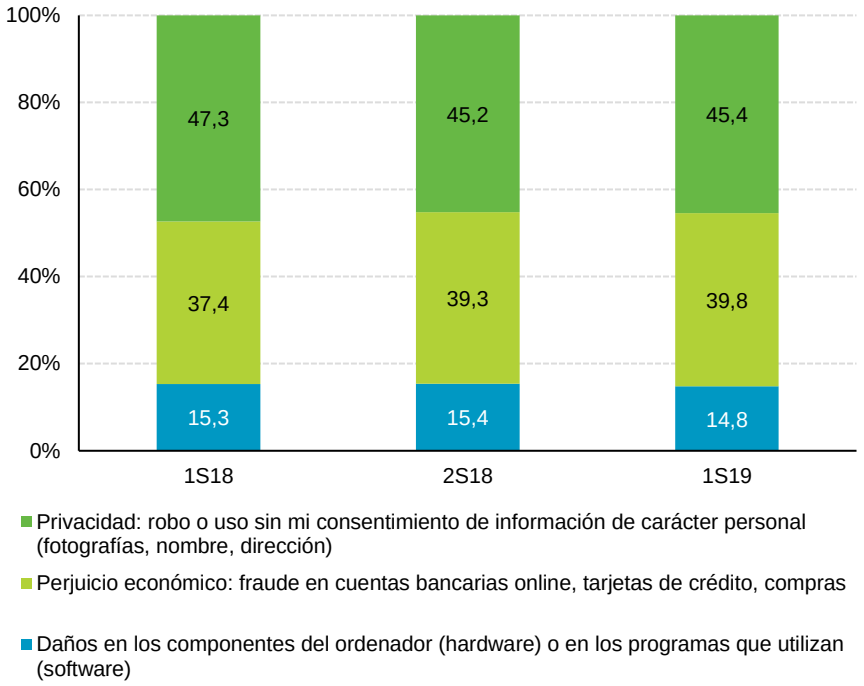



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Los valores se mantienen prácticamente estables con respecto a las pasadas entregas, significando esto que los usuarios encuestados perciben que el número de incidencias y la gravedad de las mismas es similar. Apenas un 11,6% de los usuarios encuestados considera que el número de incidencias ha aumentado y el 6,2% que son de mayor gravedad.

Sin embargo, esto no constituye un dato positivo si se cruza con los datos del estado real de los equipos en relación al *malware* (**FIGURA 14** y **FIGURA 15**), el nivel de riesgo en que se encuentran los mismos (**FIGURA 18**), y la falta de percepción del usuario en este tipo de incidencias (**TABLA 1** y **TABLA 2**).

**FIGURA 27. EVOLUCIÓN DE LA PERCEPCIÓN DE RIESGOS EN INTERNET (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

A la hora de navegar por Internet el principal riesgo continúa siendo, según la percepción de los usuarios, el robo o el uso de información personal sin consentimiento de la persona, seguido del temor a sufrir un perjuicio económico derivado de un fraude relacionado con la banca en línea, las tarjetas de crédito, las compras online, etc.

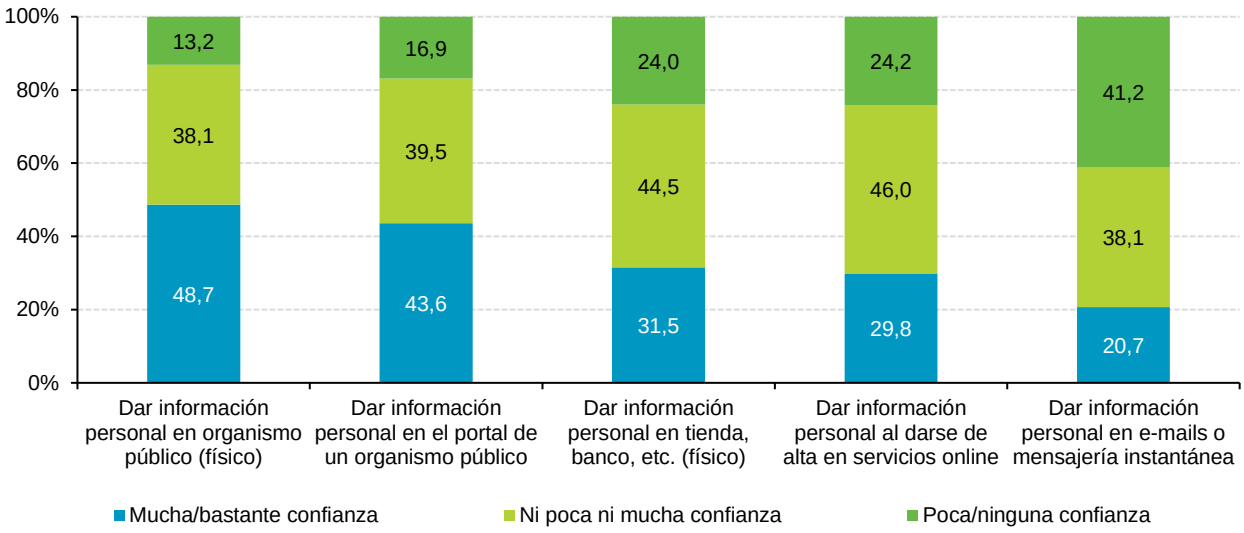
La percepción de riesgos en Internet se ha mantenido prácticamente constante en el último año.

A continuación se analiza la confianza que inspira al usuario el hecho de facilitar datos personales en diferentes situaciones.

A pesar de los numerosos esfuerzos por parte de los atacantes para intentar robar los datos de los usuarios se observa que un 41,2% de los internautas españoles desconfían ante solicitudes de información personal o privada a través del correo electrónico o mensajería instantánea. Sin embargo este rechazo disminuye hasta un 24,2% en el caso de que dicha información se solicite durante el registro o alta de un servicio online.

En el otro extremo, destaca el alto nivel de confianza que el usuario deposita sobre la entrega de documentación a organismos públicos vía telemática (43,6%) o de manera física (48,7%). Además, esta diferencia entre la confianza de hacerlo de manera online o física se está viendo reducida debido a la comodidad y ahorro de tiempo que puede suponer al usuario con respecto a pedir una cita y personarse en la sede del organismo para entregar o recoger documentación física.

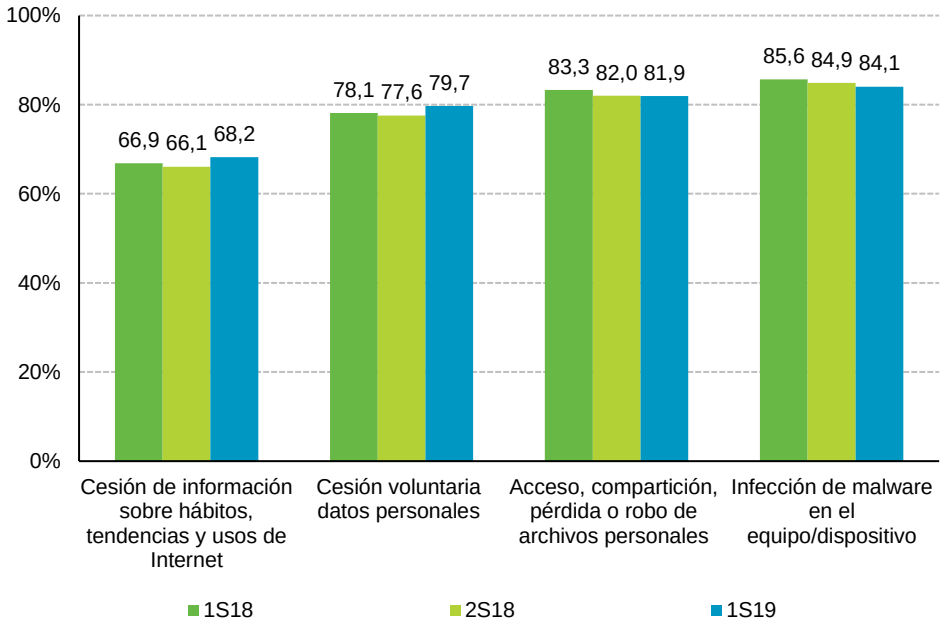
**FIGURA 28. NIVEL DE CONFIANZA EN FACILITAR DATOS PERSONALES (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

En cuanto a los peligros de Internet, los usuarios españoles otorgan una mayor valoración que en estudios anteriores a la cesión de información sobre hábitos, tendencias y usos de Internet y a la cesión voluntaria de datos personales (+2,1 p.p. en ambos casos). Por lo que podría considerarse que aumenta la preocupación por el uso que se le podría dar a dichos datos y por la posibilidad del robo de los mismos a consecuencia de un ataque cibernético a la institución. Por otro lado, el riesgo de infección de *malware* sigue siendo la principal preocupación de los internautas, aunque comparando los datos con los últimos semestres, se aprecia un ligero descenso en el número de usuarios que valoran este tipo de riesgos (-0,8 p.p.).

**FIGURA 29. EVOLUCIÓN DE LA VALORACIÓN DE LOS PELIGROS DE INTERNET (%)**

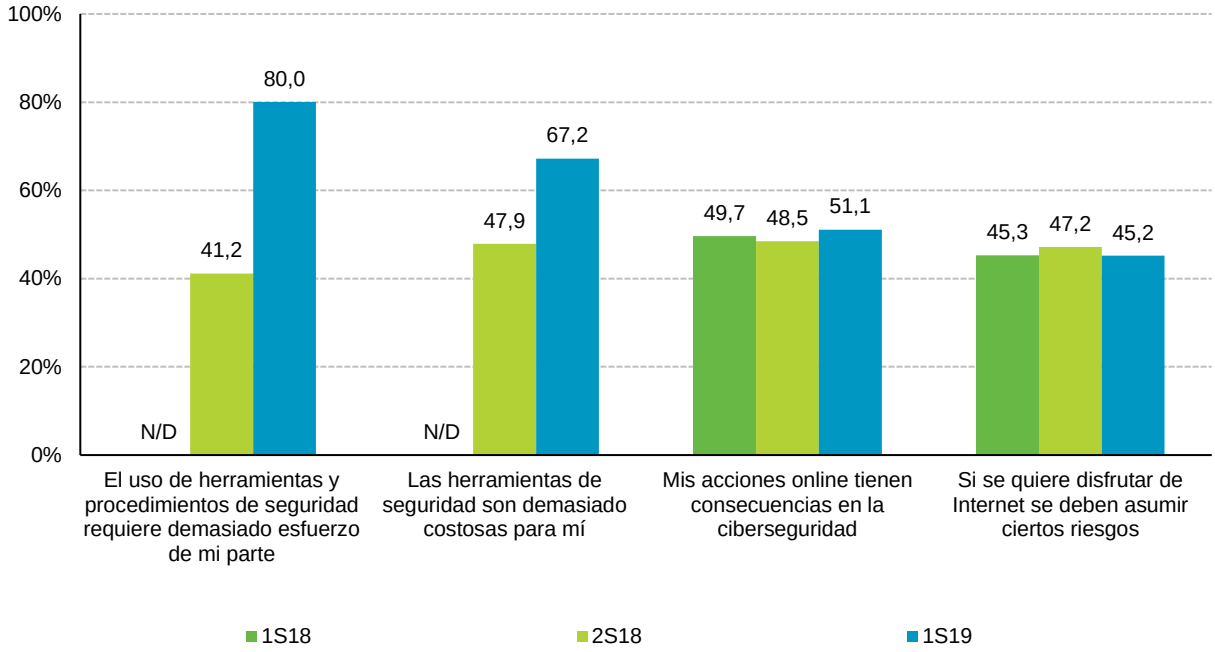



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Dado que en general la valoración de los usuarios sobre los distintos peligros de Internet planteados en el estudio ronda el 80% en la mayoría de ellos, presentando aproximadamente 10 p.p. menos el peligro de la cesión de información sobre hábitos, tendencias y usos de Internet, que es el menos valorado, se puede considerar que la concienciación general es alta.

Una parte significativa de los usuarios es consciente de los riesgos que asumen al usar Internet y de las repercusiones que tiene el uso de las medidas de seguridad para prevenirlos.

**FIGURA 30. EVOLUCIÓN DE LA RESPONSABILIDAD EN LA SEGURIDAD DE INTERNET (%)**



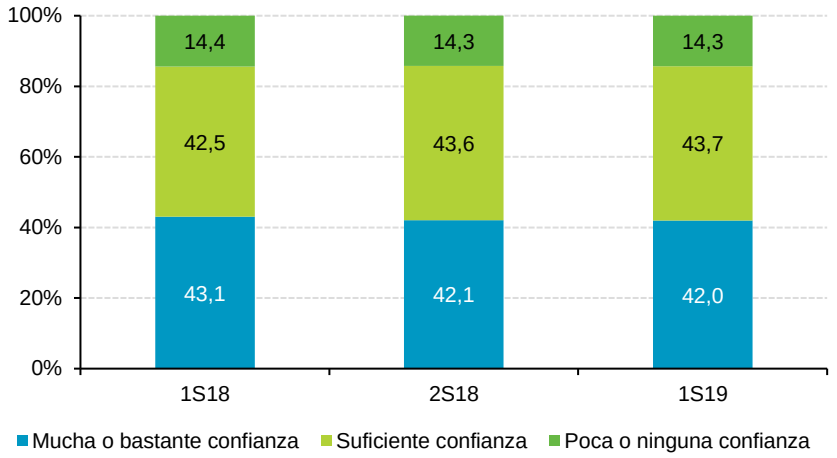

*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

El 51,1% de los encuestados manifiestan ser conscientes de que las acciones llevadas a cabo en la red tienen repercusiones en la ciberseguridad, un ligero incremento que nos hace pensar en la adquisición de buenos hábitos que se comentó en la **FIGURA 24**. El 45,2% de ellos considera que debe asumir cierto grado de riesgo si quiere disfrutar de Internet, valor que, frente al semestre anterior, ha bajado en 2 p.p.

También se observan grandes cambios en la percepción de los usuarios en cuanto al coste de las herramientas de seguridad (el 67,2% consideran que son demasiado costosas) y la dificultad de su utilización (cuatro de cada cinco consideran que requieren de demasiado esfuerzo de su parte). Se trata, sin embargo, de una idea preconcebida errónea ya que existen multitud de herramientas de seguridad gratuitas, que no suponen hacer ningún desembolso económico y ofrecen una buena protección. Además muchas herramientas suelen incorporar un asistente (o *wizard*) que proporciona información o incluso un proceso guiado para la correcta instalación y configuración.

Estos datos, en conjunción con los referentes a los motivos de no utilizar medidas de seguridad –no considerarlas necesarias o de interés, y no conocerlas– (**FIGURA 5**) presentan un panorama poco halagüeño que se ve, además, potenciado por el nivel de riesgo en que se encuentran los equipos de los usuarios (**FIGURA 18**).

**FIGURA 31. EVOLUCIÓN DEL NIVEL DE CONFIANZA EN INTERNET (%)**




*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Se observa que, desde el primer semestre del año 2018 hasta el primer semestre del año 2019 la confianza que se deposita en Internet ha decrecido en -1,1 p.p. Este dato no resulta negativo pero se debe analizar junto a los datos anteriormente expuestos, ratificando las conclusiones a las que se llegó en las figuras 14 y 15: al aumentar la percepción de los usuarios también se ha generado más desconfianza.

Tanto la valoración de los riesgos de la Red por parte del usuario como la concienciación acerca de ellos son parámetros que se muestran favorables a la ciberseguridad. Sin embargo, también existen flaquezas importantes como el saber reconocer estas amenazas cuando se presentan ante el internauta.

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

Se quiere agradecer su colaboración en la relación de este estudio a:

HISPASEC GfK

Asimismo, se quiere también agradecer la colaboración de:

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



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

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