# Estudio sobre la ciberseguridad y confianza del ciudadano en la RED

ABRIL 2020

Oleada julio - diciembre 2019

Colección Ciberseguridad y Confianza

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

# ÍNDICE

1. MEDIDAS DE SEGURIDAD

2. HÁBITOS DE COMPORTAMIENTO EN LA NAVEGACIÓN Y USOS DE INTERNET

3. INCIDENTES DE SEGURIDAD

4. CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

5. CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

6. CONCLUSIONES

ANÁLISIS DE URGENCIA: LA CIBERSEGURIDAD DURANTE LA CRISIS DEL CORONAVIRUS

# ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA DEL CIUDADANO EN LA RED

Red.es en colaboración con Hispasec Sistemas y GFK realiza semestralmente 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. Este resumen ejecutivo corresponde al estudio realizado en el segundo semestre de 2019.

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 estos 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 PC's 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.

Finalmente, se incluye un análisis de urgencia sobre la ciberseguridad en la crisis del coronavirus al final del informe.

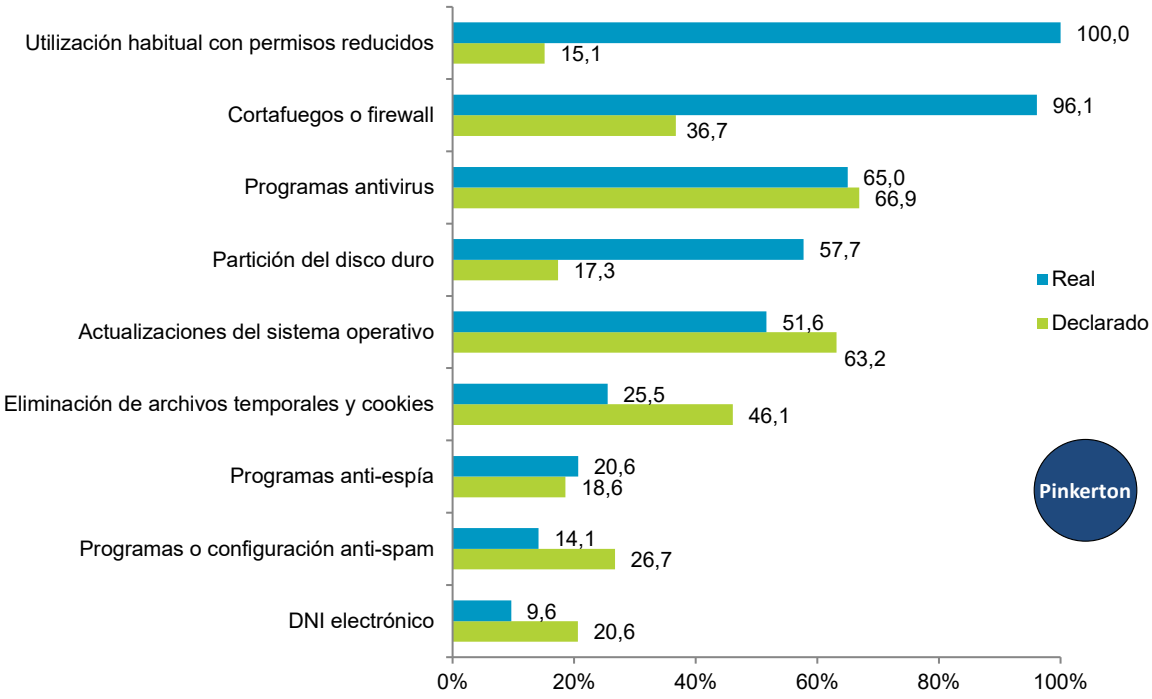
## 1. Medidas de seguridad

La interacción entre usuario y dispositivo es una de las fases más delicadas de la seguridad de la información. En la actualidad, las personas usuarias disponen de muchas herramientas para controlar y proteger sus móviles, ordenadores y otros equipos de incidencias de seguridad y ataques de terceros. No obstante, si no se emplean adecuadamente y se llevan a cabo las acciones necesarias, estas herramientas dejan de tener el efecto de protección deseado.

En este apartado se analizan las medidas de seguridad utilizadas por los panelistas españoles durante el segundo semestre de 2019.

Los datos que se muestran a continuación se han obtenido a partir de las declaraciones de aquellas personas de nacionalidad española que han participado en las encuestas y de la información recopilada mediante el análisis real de sus sistemas (ordenadores del hogar y dispositivos móviles) por la herramienta Pinkerton.

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




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

Se encuentran discrepancias significativas al comparar el uso real de las herramientas de seguridad en los ordenadores del hogar con las declaraciones realizadas por los usuarios. En algunos casos, como en las actualizaciones del sistema operativo, esta discrepancia no es muy notoria (11,6 p.p.), mientras que en otros, como en el uso habitual con permisos reducidos (84,9 p.p.), la utilización de cortafuegos o firewall (59,4 p.p.) o el particionado del disco duro (40,4 p.p.), la diferencia es considerable.

Estas discrepancias más acusadas se pueden deber al desconocimiento del usuario acerca de la existencia de las mismas en sus equipos y, al disponer de una mayor tasa de uso real, puede considerarse como un aspecto positivo. Sin embargo, el hecho de desconocer que se encuentran disponibles implica que su capacidad de protección podría no estar siendo aprovechada: por ejemplo, usando una adecuada configuración del cortafuegos o una correcta separación entre los datos de usuario y los del sistema operativo mediante el particionado del disco duro.

Durante esta oleada ha coincidido que la utilización habitual de una cuenta de usuario con permisos reducidos ha sido completa por parte de todos los equipos analizados.

Esto es debido al uso cada vez mayor de sistemas operativos como Windows 8 y Windows 10, en los que por defecto se aplica este tipo de cuentas de usuario, y la inminente finalización del soporte para Windows 7 por parte de Microsoft (acontecida el 14 de enero de 2020). De este modo, cuando una acción requiere un mayor nivel de privilegios, el sistema solicita las credenciales para elevar los mismos de manera puntual.

En cualquier caso, los datos obtenidos revelan que las medidas de seguridad más populares en equipos del hogar continúan siendo la limitación de permisos a los usuarios habituales y el uso de programas antivirus (66,9%).

Entre las medidas con menor implantación en los hogares españoles nos encontramos el uso del DNI electrónico (20,6%) y el uso de programas anti-espías (18,6%) y anti-spam (26,7%).

También hay que resaltar que el hábito de eliminar los archivos temporales y cookies se sitúa en torno a una cuarta parte de los internautas. Además existe una parte considerable de los usuarios (20,6 p.p.) que declara haber adoptado esta medida, aunque los datos obtenidos por Pinkerton indican que no coinciden los datos declarados y reales.

En los dispositivos móviles, como podemos ver en la gráfica siguiente, puede observarse una tendencia similar. Los panelistas parecen no ser conscientes de que el sistema diferencia entre el usuario habitual (con permisos limitados) y el administrador (o root), por la propia seguridad del dispositivo.

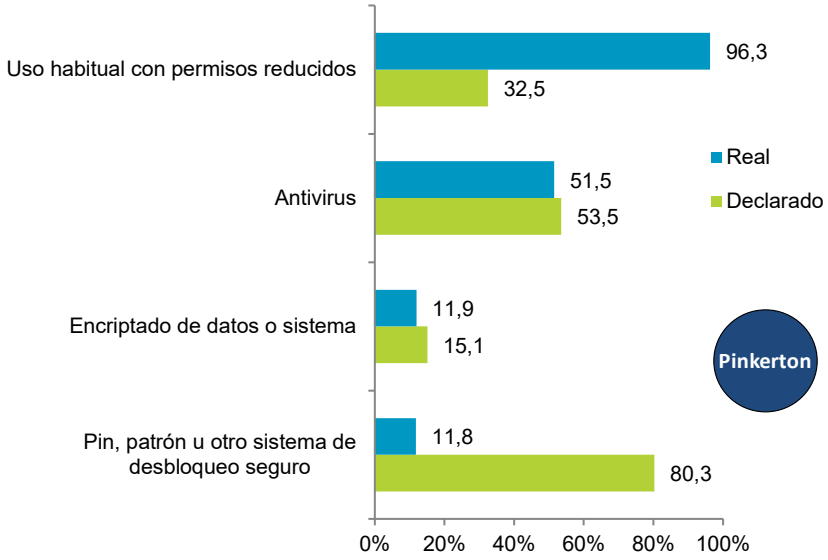
Además, para obtener elevados privilegios en el sistema operativo Android, es necesario realizar un proceso y una serie de cambios que requieren de unos conocimientos técnicos que no suele tener el usuario promedio.

Como vienen siendo habitual, muchas de las declaraciones sugieren el uso de un sistema de desbloqueo seguro (80,3%), mientras que los datos reales muestran que únicamente el 11,8% dispone de un pin, patrón o alguna otra medida similar de seguridad como pudiera ser la huella digital u otro factor biométrico.

Esta discrepancia de 68,5 p.p. entre los datos declarados y los reales demuestra que muchos usuarios identifican erróneamente el mecanismo simple de desbloqueo (por ejemplo mediante un deslizamiento o pulsación) que cualquiera puede realizar, con el mecanismo seguro que requiere de un factor que únicamente el usuario conoce, impidiendo de esta manera, el accedo a terceras personas no autorizadas.

También puede deberse a que se esté confundiendo la funcionalidad del bloqueo automático de la pantalla del terminal (usada principalmente para evitar pulsaciones no deseadas) con la de desbloqueo del dispositivo (cuya finalidad es la de evitar accesos no autorizados).

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




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

A diferencia del ámbito del ordenador personal, en los dispositivos móviles no es común la utilización de aplicaciones antivirus. Sin embargo, parece que cada vez un mayor porcentaje de usuarios de Android es consciente del peligro al que se expone por no usar esta medida de seguridad en sus dispositivos. En esta oleada la proporción de usuarios que ha optado por instalar un antivirus en su terminal supera ligeramente la mitad (53,5%). Además, como el sistema operativo Android no incluye este tipo de software por defecto y es el usuario el que debe instalar una aplicación antivirus, el dato real y el declarado prácticamente coinciden.

La medida de seguridad menos popular entre los usuarios de Android continúa siendo la encriptación de datos o del sistema. Los posibles motivos de que apenas se supere el 10% de terminales con esta medida implementada pueden ser tanto el desconocimiento sobre la medida en sí, como la posible pérdida de rendimiento del dispositivo, mucho más notoria en aquellos terminales de gama media-baja.

Por otro lado, el uso de perfiles de administrador en dispositivos Android parece estar íntimamente relacionado con la antigüedad del dispositivo. Mientras que en aquellos terminales que disponen de alguna de las últimas versiones disponibles la mayoría de los usuarios suelen operarlos con los permisos que por defecto establece el sistema, en las versiones de Android 4 y 5 se observa que hasta un cuarto de los dispositivos (en la versión 4, en la versión 5 en torno al 20%) ha sido modificado para elevar sus privilegios.

Este comportamiento podría responder a la necesidad de modificar aquellos dispositivos que han dejado de tener soporte oficial por parte del fabricante para continuar disfrutando de novedades y actualizaciones gracias a módulos libres creados por la comunidad de desarrolladores, aplicaciones que precisan de algún requisito especial, o para modificar de alguna manera el rendimiento o incluso la apariencia del terminal.

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

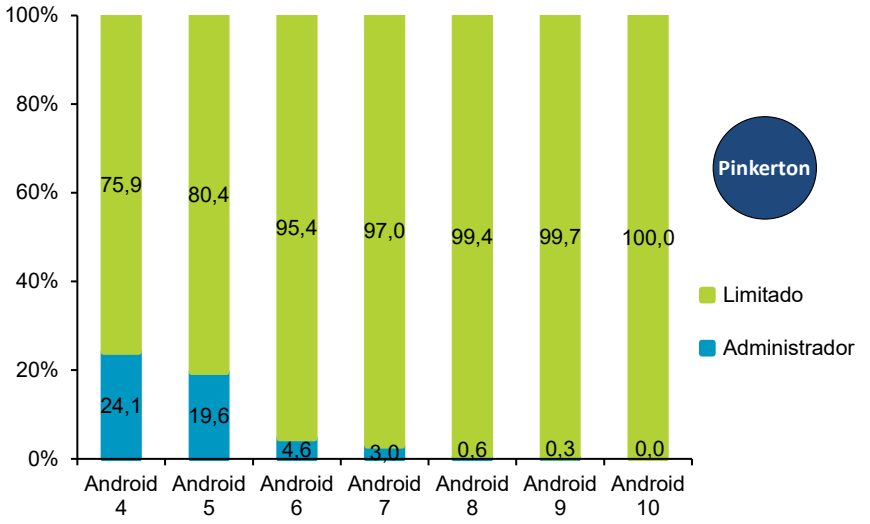
**100%**
**CON PERMISOS REDUCIDOS EN ANDROID 10**

**99,7%**
**CON PERMISOS REDUCIDOS EN ANDROID 9**

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

**97%**
**CON PERMISOS REDUCIDOS EN ANDROID 7**

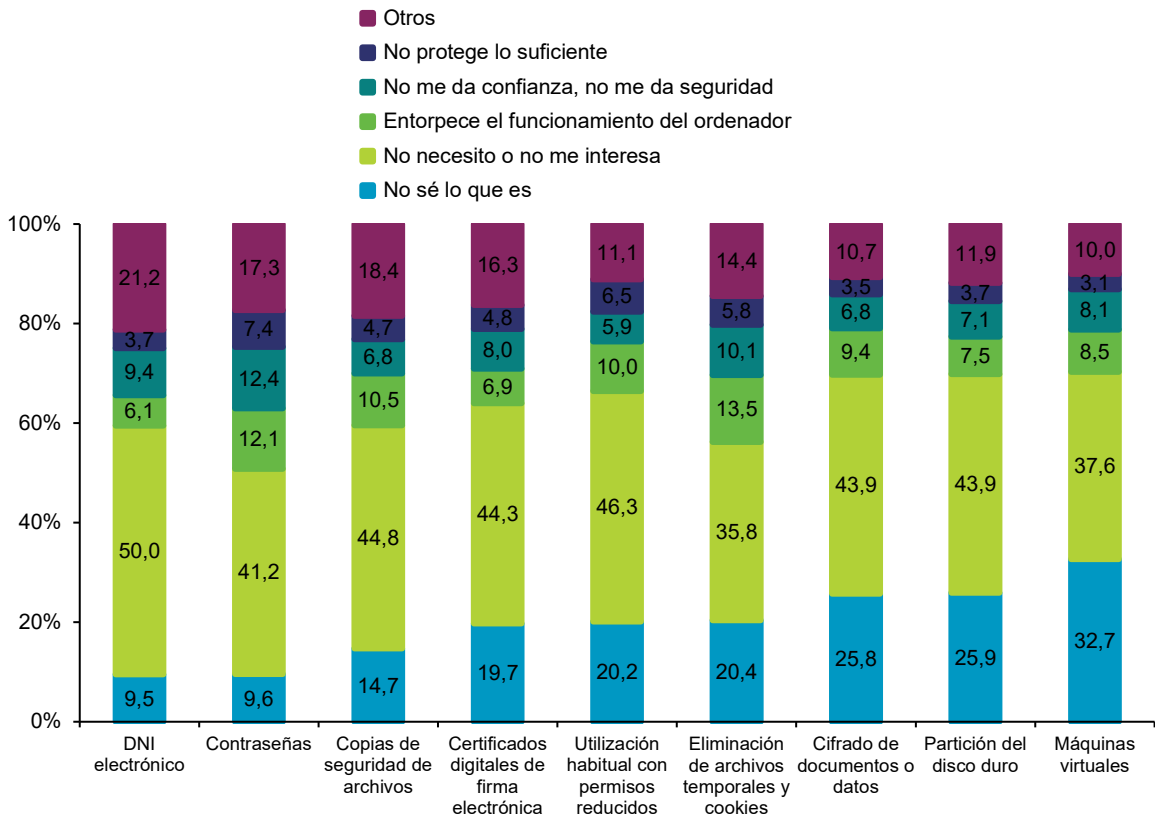
**FIGURA 3. USO REAL DE PERFILES DE ADMINISTRADOR EN DISPOSITIVOS ANDROID (%)**




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

También se debe considerar que los dispositivos más recientes suelen cubrir las necesidades del usuario, cuestión que las versiones anteriores, posiblemente, no hagan debido a haberse quedado obsoletas. Y por último, destacar que para obtener permiso de administrador es necesario realizar acciones no triviales en el dispositivo que podría ponerlo en riesgo y perder la garantía. Por lo que, una vez pasado el periodo de garantía, es más factible que el usuario opte por manipular el dispositivo.

**FIGURA 4. MOTIVOS DE NO UTILIZACIÓN DE MEDIDAS DE SEGURIDAD (%)**




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

Respecto a las causas alegadas por los internautas españoles para no utilizar determinadas medidas de seguridad, cabe destacar que entre un 36% y un 50% opinan que no las necesitan. Aunque, como se verá más adelante (**FIGURA 11**), los datos revelan que casi un 60% de los panelistas han tenido algún problema de seguridad en el último semestre de 2019.

Como en oleadas anteriores, las medidas menos populares debido a que los usuarios desconocen su funcionamiento son: el uso de máquinas virtuales (32,7%), el particionado del disco duro (25,9%) y el cifrado de documentos o datos (25,8%). Por otro lado, las medidas de seguridad consideradas menos necesarias o carentes de interés por parte de los usuarios son: el DNI electrónico (50%), el empleo de usuarios con permisos reducidos (46,3%) y las copias de seguridad (44,8%).

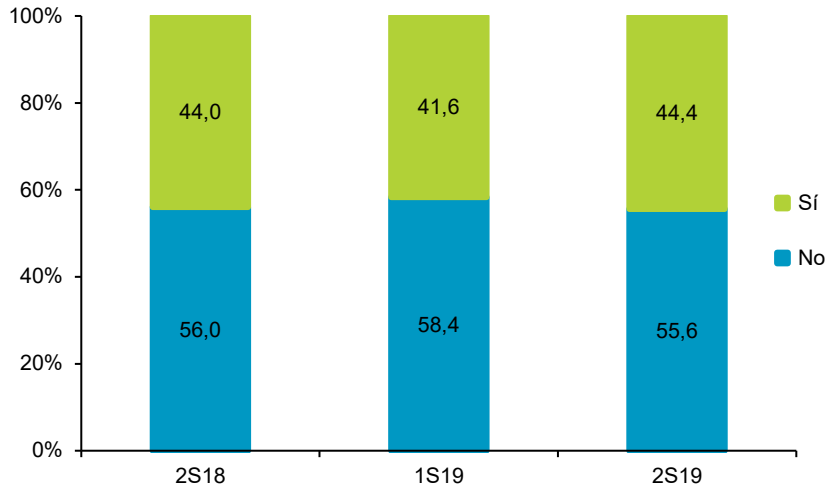
A pesar de ello, , el uso de certificados digitales o el DNI electrónico son medidas de seguridad que permiten acceder a aplicaciones y documentos con un alto nivel de seguridad; mientras que la realización de copias de seguridad con frecuencia reduce significativamente el riesgo de perder datos y recuperarse con facilidad de ciertos ataques de malware como el ransomware.

## 2. Hábitos de comportamiento en la navegación y usos de Internet

Los hábitos de comportamiento del usuario a la hora de navegar por Internet y utilizar su equipo, suponen una parte tan importante en la seguridad como las medidas y herramientas analizadas en el apartado anterior. Por tanto resulta de interés comprobar cuales de los principales hábitos prudentes son utilizados por los usuarios españoles.

Durante este semestre se ha apreciado un ligero aumento en el porcentaje de usuarios que declaran que adoptan conductas de riesgo de forma consciente (+2,8 p.p.), alcanzándose de nuevo un porcentaje similar al observado en el segundo semestre de 2018.

**FIGURA 5. EVOLUCIÓN DE LA ADOPCIÓN CONSCIENTE DE CONDUCTAS DE RIESGO (%)**

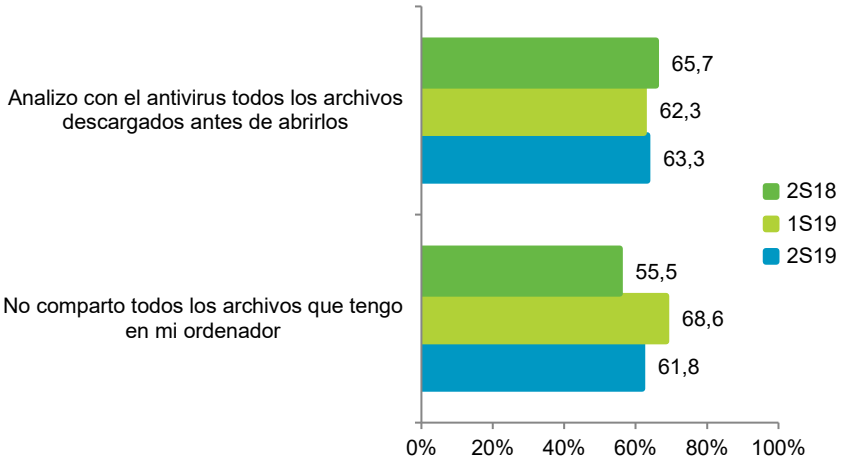



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Casi uno de cada dos usuarios realiza, aunque sea de manera puntual, algún tipo de conducta de riesgo cuando navega o usa Internet. Es importante destacar que, para que se produzca una incidencia de seguridad, únicamente es necesario realizar alguna acción de riesgo puntual: por ejemplo, deshabilitar el software antivirus para poder realizar con éxito una descarga de dudosa procedencia que dicho programa ha bloqueado o eliminado por haber detectado alguna amenaza.

A continuación se analiza la interacción del usuario con respecto a la descarga a través de redes P2P y la descarga de archivos.

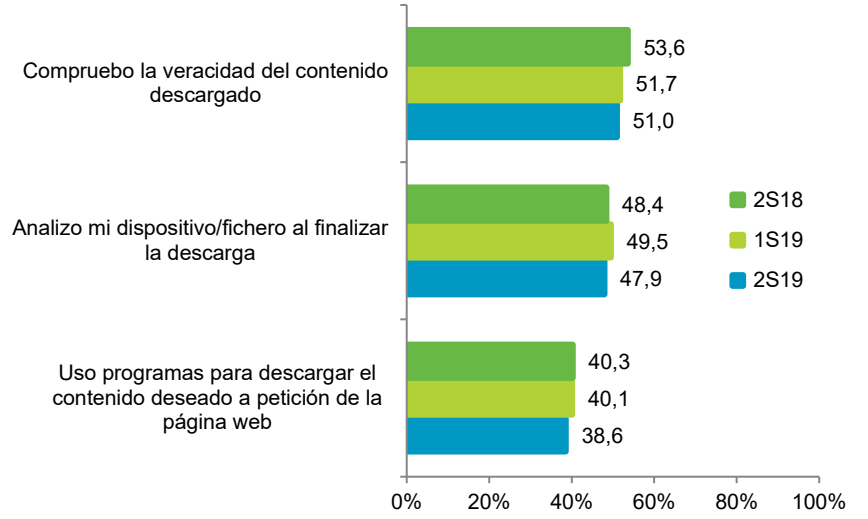
**FIGURA 6. DESCARGAS EN REDES P2P (%)**




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

La proporción de panelistas que analiza los archivos descargados en redes P2P con antivirus se mantiene en torno a los dos tercios (63,3%) y algo menos aquellos que restringen los archivos compartidos (61,8%). Sin embargo, cabe destacar la reducción acontecida durante el periodo analizado para este último dato (-6,8 p.p.), que se traduce en que casi dos de cada cinco usuarios exponen todo el contenido de su equipo en las redes P2P.

**FIGURA 7. DESCARGAS EN INTERNET (%)**




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

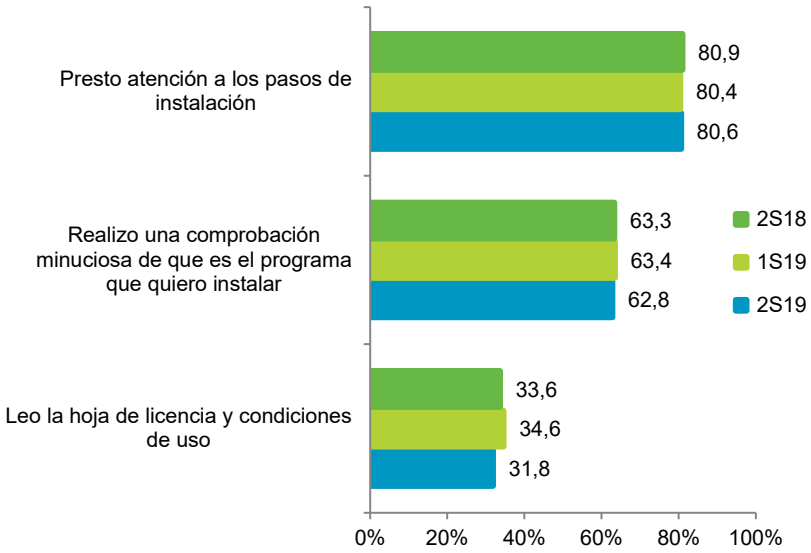
Por otro lado, los usuarios que realizan descargas en Internet demuestran ser menos cuidadosos, situándose en torno a la mitad aquellos que comprueban si el contenido descargado coincide con el buscado (51%) o que analiza el equipo o los archivos una vez finalizada la descarga (47,9%). Independientemente del análisis de los ficheros descargados, siempre es recomendable comprobar también la autenticidad de los archivos con algún tipo de *hash* (o resumen), para contrastarlo con la información disponible en la web oficial desde la que se han bajado.

A pesar de que el 65% de panelistas tiene un antivirus instalado en su ordenador del hogar con sistema Windows (**FIGURA 1**), menos del 50% se preocupa por analizar los archivos descargados, pese a que es una práctica bastante común distribuir malware mediante esta vía.

En general, se aprecia un ligero descenso en el volumen de usuarios que adopta prácticas seguras en las descargas directas semestre a semestre.

En las siguientes dos gráficas se muestran los datos referentes a los pasos realizados al instalar programas en el ordenador del hogar y las descargas de aplicaciones en dispositivos Android, teniendo en cuenta su origen (tienda oficial u origen desconocido). En este caso, no se observan grandes cambios en los hábitos de los internautas españoles en los últimos semestres.

**FIGURA 8. INSTALACIÓN DE PROGRAMAS EN EL ORDENADOR DEL HOGAR (%)**




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

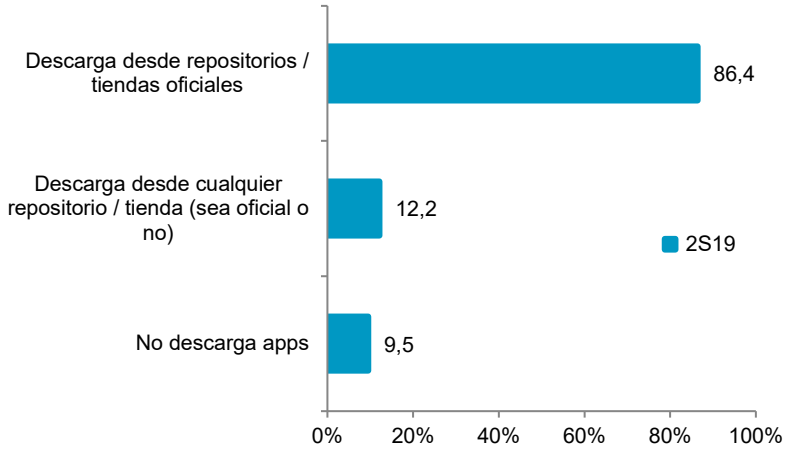
Resulta interesante ver como los resultados correspondientes a los hábitos prudentes relacionados con la instalación de programas se han mantenido prácticamente constantes durante las últimas oleadas. El 80% de los panelistas siguen declarando prestar atención a los pasos de instalación. Este hábito tan simple adquiere una mayor importancia debido a que durante la instalación de determinados programas o versiones gratuitas o de prueba de los mismos se solicita, y aparece marcada por defecto su aceptación, la opción de instalar software de terceros a modo de financiación.

De forma que al no prestar la debida atención, se instalará software no deseado en el sistema.

Por el contrario, casi dos tercios (62,8%) declaran realizar una comprobación minuciosa para asegurarse de que el programa que se está instalando es realmente el deseado.

La parte negativa la representa el 68,2% de los usuarios no se preocupa de leer la hoja de licencia y las condiciones de uso del software que está instalando: algo menos de un tercio tiene este hábito prudente.

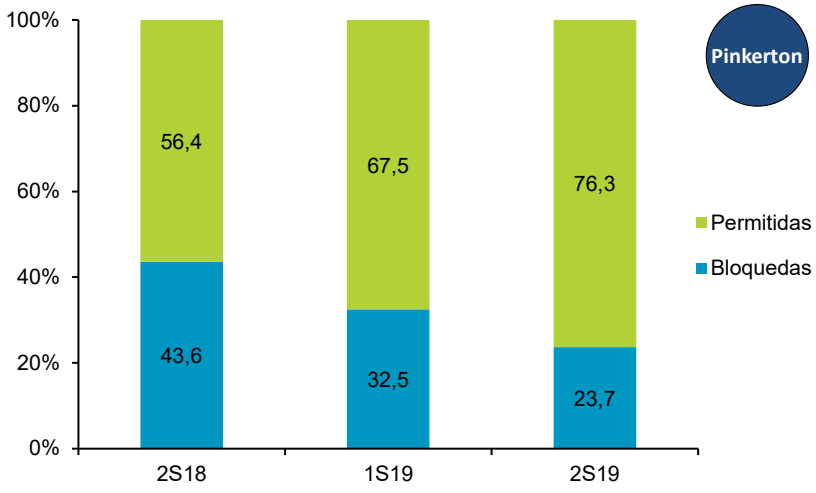
**FIGURA 9. DESCARGA DE APLICACIONES EN DISPOSITIVOS ANDROID (%)**




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

En cuanto a los dispositivos Android, la mayoría opta por utilizar los repositorios oficiales (86,4%) a la hora de descargar *apps*, aunque un 12,2% también opta por markets no oficiales. El elevado uso de los repositorios oficiales podría responder, más que a cuestiones de seguridad, al hecho de que estos se encuentran integrados en los dispositivos, resultando más cómodo y sencillo para el usuario utilizarlos que buscar otras fuentes alternativas.

**FIGURA 10. EVOLUCIÓN DEL ESTADO DE LAS FUENTES DESCONOCIDAS (%)**




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

Y sin embargo, a pesar de las anteriores declaraciones (**FIGURA 9**), más de las tres cuartas partes de los dispositivos Android tienen habilitada la opción para permitir la instalación de aplicaciones desde fuentes desconocidas. Es necesario mencionar que, por defecto, dicha opción viene desactivada en el sistema Android debiendo el usuario modificarla. Este dato muestra una tendencia al alza bastante importante, habiendo pasado de unos valores del 56,4% en el segundo semestre de 2018 a un 76,3% en el periodo actual.

Llevar a cabo instalaciones de aplicaciones desde tiendas o repositorios no oficiales supone un riesgo para el dispositivo y la integridad de otras aplicaciones. En dichos repositorios o tiendas, por lo general, no se controla la procedencia de las aplicaciones que en ellas se almacenan, en ocasiones, no se realizan análisis para comprobar la existencia de malware, e incluso puede no ser posible comprobar el certificado con el que se ha firmado la aplicación, al contrario que en los markets oficiales.

Una aplicación descargada desde un sitio no oficial, podría incluir algún tipo de malware, como los droppers, que se encargan de descargar otros códigos maliciosos en el sistema infectado, o bankbots, que manipulan aplicaciones bancarias instaladas en el sistema realizando una suplantación de la pantalla de inicio del banco y en ocasiones de la tarjeta de coordenadas en el momento en el que el usuario abre la aplicación.

# 3. Incidentes de seguridad

La utilización de las diferentes medidas de seguridad y la práctica de hábitos prudentes adquieren un papel de gran importancia al reducir significativamente el riesgo de que las amenazas de seguridad se tornen en incidencias reales. Sin embargo, no existe un método que resulte infalible y, además, dichas amenazas se encuentran en continua evolución en su afán de tratar de eludir las posibles barreras tanto a nivel de usuario como de sistema, e incluso, pasar desapercibidas ante los diferentes programas de seguridad.

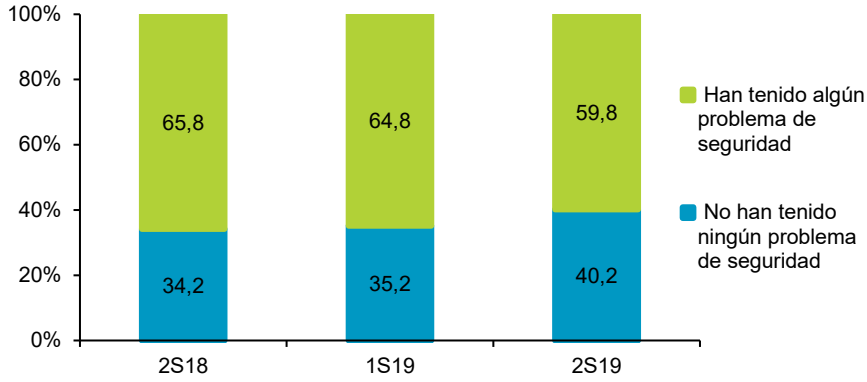
En este apartado se analizan los incidentes de seguridad sufridos por los panelistas en el periodo comprendido entre junio y diciembre de 2019.

En esta última oleada se ha visto reducido el número de usuarios que han informado de algún problema de seguridad (-5 p.p.), manteniéndose una tendencia a la baja. No obstante, el porcentaje de usuarios que ha sufrido algún tipo de incidente de seguridad sigue siendo próximo a los dos tercios (59,8%).

Este elevado número de incidencias podría verse explicado por la falta de hábitos prudentes en el uso de la Red que se desprende de las declaraciones observadas en los apartados anteriores.

Muchos de los usuarios que no utilizan herramientas de seguridad (hasta el 50%) consideran que no son necesarias (**FIGURA 4**) y la mayoría de los usuarios de PC continúa sin darle importancia a herramientas de seguridad para equipos de sobremesa como los programas anti-espía (79,4%) o los programas anti-spam (85,9%) y casi la mitad de ellos (48,4%) no mantiene actualizados sus equipos (**FIGURA 1**).

**FIGURA 11. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)**

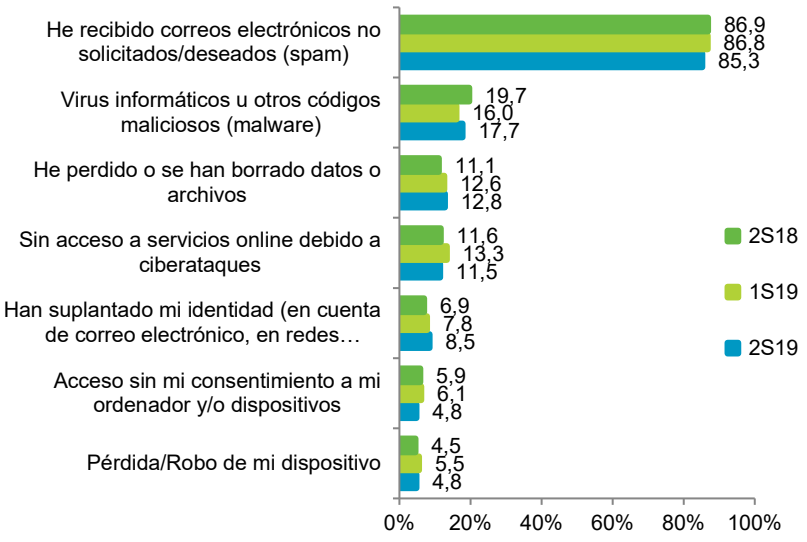



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

En el caso de los terminales móviles (**FIGURA 2**), no suelen instalar soluciones antivirus casi la mitad de los usuarios (48,5%) y una gran mayoría (88,2%) no emplea sistemas de desbloqueo seguros como código pin, patrones o medidas biométricas, conformándose con la versión básica que solo requiere el desplazamiento del dedo sobre la pantalla, permitiendo que cualquier persona pueda desbloquear el terminal y hacer uso del mismo.

Además de no usar las herramientas de seguridad oportunas, muchos usuarios (44,4%) asumen conscientemente conductas de riesgo en el uso de Internet (**FIGURA 5**) porque consideran que es necesario para poder sacar mayor partido a su uso. Como se ha visto anteriormente (**FIGURA 6**), prácticamente solo un tercio de los usuarios de redes P2P se preocupa de analizar los archivos descargados con un antivirus y restringe los archivos que comparte. Respecto a las descargas directas de Internet (**FIGURA 7**), el porcentaje de usuarios que adopta hábitos seguros aumenta hasta prácticamente la mitad, verificando la autenticidad de los archivos descargados mediante herramientas como los hashes (51%) o analizando los archivos descargados con antivirus (47,9%).

**FIGURA 12. 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.

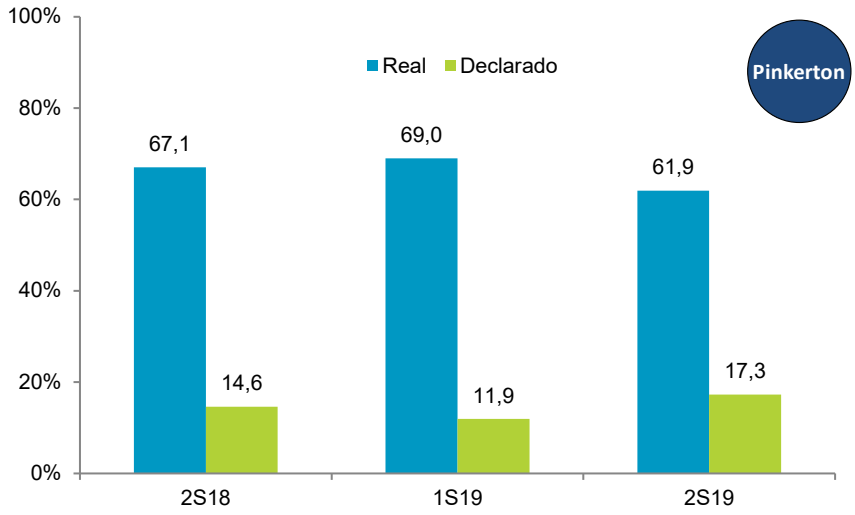
Comúnmente se conocen como virus, aunque en realidad se trata de un término mucho más amplio que engloba otras muchas tipologías.

En esta ocasión se observa un ligero aumento en el reporte de incidencias con malware (+1,7 p.p.) sobre la oleada anterior, manteniéndose como el segundo tipo de incidencia más habitual, aunque continúa por debajo del resultado obtenido a finales de 2018. El resto de clases de incidencia no presenta grandes variaciones, o muestran pequeños descensos, como en el caso de la pérdida de acceso a Internet debido a ciberataques (-1,8 p.p.), o el acceso sin consentimiento al ordenador o dispositivo móvil (-1,3 p.p.).

El tipo de ataque más frecuente, y con una gran diferencia con respecto a los demás, es la recepción de correos electrónicos no solicitados que, a pesar de tener la cifra más baja respecto a oleadas anteriores, sigue siendo considerablemente elevada (85,3%). Actualmente las campañas de correo no deseado (spam) son uno de los principales vectores de ataque para la difusión de malware o las campañas de phishing (robo de credenciales bancarias), por poner algunos ejemplos.

Otra clase de ataque que está cobrando cada vez mayor relevancia es la suplantación de identidad en redes sociales o correo electrónico, que continúa creciendo progresivamente a un ritmo lento pero constante semestre tras semestre. Cada día hay más vulneración en la custodia de datos en empresas debido a incidentes de seguridad, donde el objetivo de los atacantes suelen ser principalmente listados de usuarios y contraseñas. Estos datos podrían ser aprovechados para suplantar identidades, realizar campañas de spam, o incluso, lograr acceso a otros servicios relacionados con los usuarios afectados debido a que en bastantes ocasiones se utiliza la misma contraseña en servicios diferentes con el peligro que esto conlleva.

**FIGURA 13. EVOLUCIÓN DE LAS INCIDENCIAS DE MALWARE (DECLARADO VS. REAL) EN EL ORDENADOR DEL HOGAR (%)**




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

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

**61,9%**
**DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE**

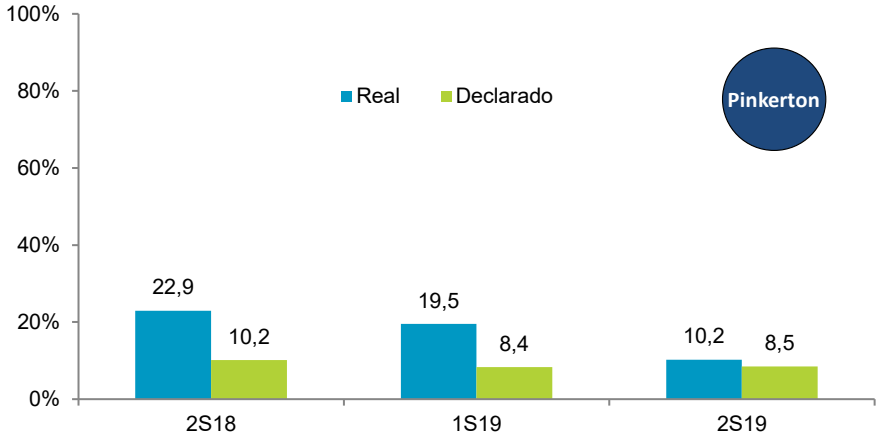
**17,3%**
**DE LOS USUARIOS PERCIBEN MALWARE EN SUS ORDENADORES PERSONALES**

Se aprecia un ligero descenso (-7,1 p.p.) en la detección de software malicioso respecto al primer semestre del año 2019 y, aunque los usuarios continúan declarando un porcentaje mucho menor de infecciones, la brecha entre el malware declarado y el detectado por Pinkerton se reduce considerablemente, pasando de 57,1 p.p. a 44,6 p.p. a lo largo del año 2019.

Parece que los internautas españoles empiezan a ser más conscientes de las infecciones de malware sufridas. Aunque la situación continúa mostrándose preocupante puesto que el hecho de no ser consciente de una infección implica que no se tomarán las medidas necesarias para mitigarla.

Las empresas de soluciones antivirus están constantemente actualizando sus sistemas de detección de amenazas desarrollando técnicas nuevas que puedan servir tanto para las familias de malware ya conocidas, como para que las de nuevo desarrollo puedan ser también rápidamente neutralizadas. Es por ello que el uso de este tipo de software es básico para proteger un equipo o dispositivo móvil frente a este tipo de incidencias.

**FIGURA 14. EVOLUCIÓN DE LAS INCIDENCIAS DE MALWARE (DECLARADO VS. REAL) EN DISPOSITIVOS ANDROID (%)**




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

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

**10,2%**
**DE LOS DISPOSITIVOS ANDROID ESCANEADOS CON PINKERTON ALOJAN MALWARE**

**8,5%**
**DE LOS USUARIOS PERCIBEN MALWARE EN SUS DISPOSITIVOS ANDROID**

Los reportes de malware detectado en dispositivos Android continúan disminuyendo cada semestre, reduciéndose notablemente la diferencia entre las infecciones detectadas por el usuario y las identificadas por Pinkerton, que ha pasado a ser inferior a 2 p.p. durante el último semestre de 2019 frente a los cerca de 13 p.p. que se reportaron hace un año.

Comparando los resultados de infecciones en equipos del hogar y en terminales Android, destaca la poca presencia de malware que podemos encontrar en estos últimos respecto a los ordenadores del hogar. A pesar de que la mayoría de las personas dispone actualmente de teléfonos inteligentes, no se registran tantas infecciones. Posiblemente esto se deba a que la gran mayoría de los usuarios (86,4%) descarga aplicaciones a través de repositorios oficiales (**FIGURA 9**), que suelen verificar la seguridad de las mismas.

Sin embargo, siguen apareciendo dispositivos infectados debido a prácticas poco seguras como la activación de las fuentes desconocidas y la instalación de aplicaciones de dudosa procedencia o sospechosas (**FIGURA 10**). No obstante, el porcentaje de dispositivos Android infectados continúa descendiendo cada semestre, bajando del 22,9% identificado a finales de 2018 hasta los 10,2% de finales de 2019.

En las siguientes tablas se contrasta las incidencias de malware detectado en equipos de sobremesa y Android respecto a las incidencias reportadas por los panelistas.

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

Pinkerton

| Declaran tener malware en PC | Su PC presenta malware | | |
|---|---|---|---|
| | Sí | No | Total |
| Sí | 9,9 | 5 | 14,9 |
| No | 52,1 | 33 | 85,1 |
| Total | 62 | 38 | 100 |

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

Resulta importante resaltar que el 52,1% de usuarios desconocen estar infectados por algún tipo de malware. Como aspecto positivo, cabe destacar que más de un tercio de los panelistas parecen tener un mayor conocimiento del estado de su sistema, identificando correctamente cuándo no sufren ninguna infección o cuándo están realmente infectados.

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

Pinkerton

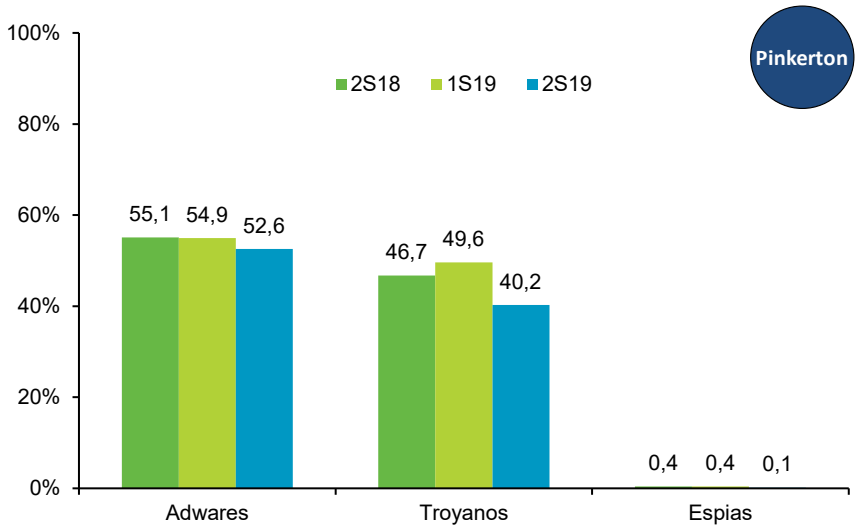
| Declaran tener malware en el dispositivo Android | Su dispositivo Android presenta mal | | |
|---|---|---|---|
| | Sí | No | Total |
| Sí | 0,7 | 5,9 | 6,6 |
| No | 9,5 | 83,9 | 93,4 |
| Total | 10,2 | 89,8 | 100 |

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

Los datos cotejados en la **Tabla 2** corresponden a las incidencias de malware detectadas y declaradas en dispositivos Android. Como se puede ver, gracias al funcionamiento interno del sistema operativo y a los canales oficiales de descargas, aparte de que el porcentaje de infecciones era significativamente menor que en equipos de sobremesa (**FIGURA 13** y **FIGURA 14**), los usuarios que no se percatan de que su terminal está infectado es inferior al 10%, mientras que el porcentaje de usuarios que son conscientes del estado real de infección de su dispositivo prácticamente supone el 85%.

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

**FIGURA 15. EVOLUCIÓN DEL MALWARE EN EL ORDENADOR DEL HOGAR (%)**

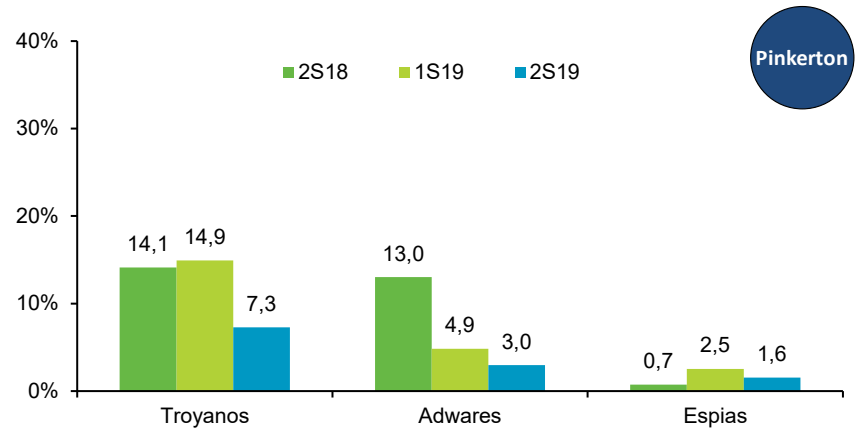



*Base: Total ordenadores*
*Fuente: Panel hogares, ONTSI*

Los datos mostrados revelan una notable bajada en la presencia de troyanos en el ordenador del hogar. Por otro lado, el software espía sigue teniendo una incidencia muy baja, de tan solo un 0,1% en esta oleada y el 0,4% en las pasadas. En este último caso, el motivo puede ser que este tipo de malware suele ser más sofisticado y las infecciones están enfocadas a objetivos muy concretos, mientras que el adware y los troyanos podrían obtener beneficios prácticamente de cualquier sistema infectado.

Asimismo, se observa que el adware, software cuya finalidad es el despliegue de anuncios, sufre una disminución de 2,3 p.p., mientras que los troyanos acusan una bajada más significativa, de 9,4 p.p.

**FIGURA 16. EVOLUCIÓN DEL MALWARE EN DISPOSITIVOS ANDROID (%)**




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

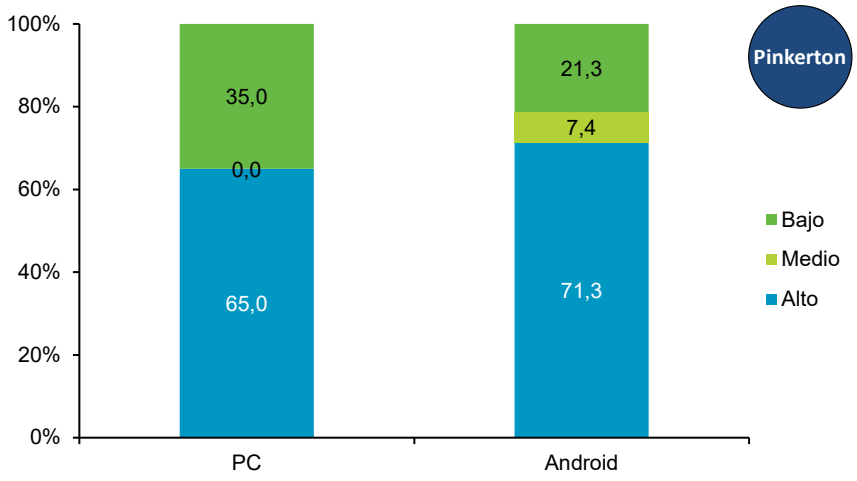
Al igual que se ha observado en el ordenador del hogar, también en los dipositivos Android ha disminuido la presencia de malware. Especialmente importante ha sido el descenso de las incidencias de troyanos, que se han reducido a la mitad respecto al semestre

anterior. El objetivo más habitual de los troyanos en dispositivos móviles suele ser la obtención de acceso a cuentas bancarias o contenido sensible con el que poder chantajear a los usuarios para que paguen una determinada cantidad, generalmente en bitcoins o en alguna moneda electrónica para evitar el rastreo del pago.

Tanto el adware como el malware espía también se reducen, presentando una incidencia del 3% y 1,6%, respectivamente.

El 65% de los ordenadores y el 71,3% de los dispositivos Android infectados con *malware* se encuentran en un nivel de riesgo alto

**FIGURA 17. NIVEL DE RIESGO EN EL ORDENADOR DEL HOGAR Y EN DISPOSITIVOS ANDROID (%)**




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

El nivel de riesgo reflejado demuestra que en el caso de ordenadores del hogar hay un mayor porcentaje (35%) de infecciones de riesgo bajo que en los dispositivos Android. Esto se puede deber principalmente a que el objetivo de las infecciones en Android está encaminada a recopilar las credenciales bancarias de los usuarios.

A pesar de todo, la perspectiva es preocupante, debido a que se aprecia un nivel de riesgo alto en un porcentaje de equipos infectados muy elevado, llegando al 65% en los PC y subiendo por encima del 70% en los dispositivos Android.

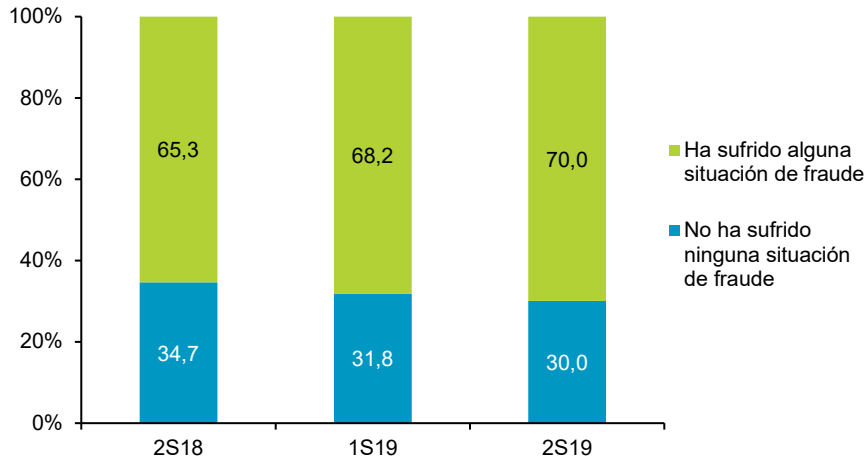
## 4. Consecuencias de los incidentes de seguridad y reacción de los usuarios

Una vez sufrido un incidente de seguridad, las víctimas suelen tratar de evitar que se repita modificando sus hábitos prudentes y las medidas de seguridad utilizadas (o comenzando a utilizarlas), buscando información en Internet, recibiendo formación o contratando a empresas dedicadas a la seguridad entre otras reacciones.

Todo esto conlleva un cambio de actitud frente al mundo de la seguridad en Internet, que va adquiriendo mayor importancia con el paso de los años.

En el siguiente apartado se analizan las reacciones experimentadas por los usuarios después de haber padecido un incidente de seguridad.

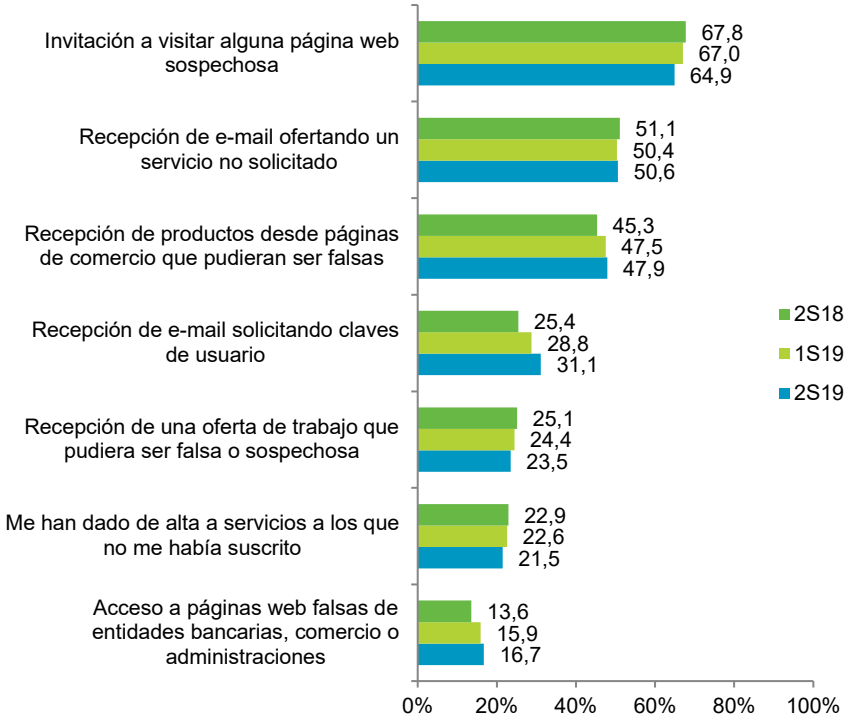
**FIGURA 18. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)**




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

Con el aumento de los ciberataques se está incrementado poco a poco el porcentaje de intentos de fraude sufridos cada año. Se puede apreciar que, a pesar de haber descrito anteriormente un descenso en el número de detecciones de software malicioso, en esta oleada los intentos de fraude siguen aumentando ligeramente, alcanzando el 70%.

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

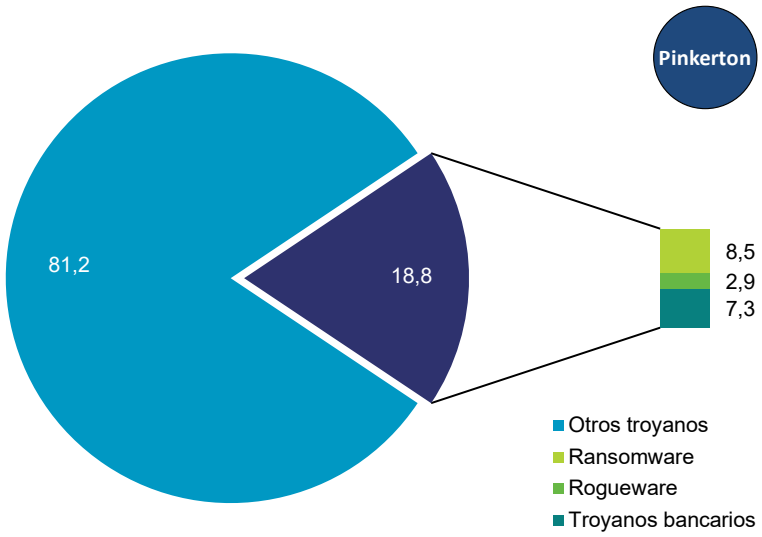



*Base: Usuarios que han sufrido un intento de fraude*
*Fuente: Panel hogares, ONTSI*

Las manifestaciones de los intentos de fraude no distan demasiado de las oleadas pasadas, siendo la subida más representativa de 2,3 p.p. en la recepción de correos solicitando claves de usuario.

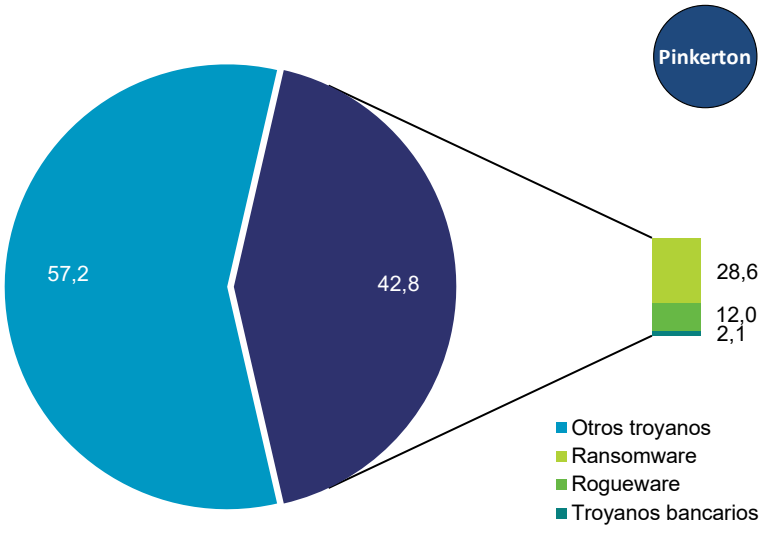
También sigue una tendencia al alza el phishing o acceso a páginas web falsas de entidades bancarias, comercio electrónico o administraciones, aumentando 3,1 p.p. en el último año (y 6,3 p.p. desde la segunda mitad de 2017).

**FIGURA 20. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN EL ORDENADOR DEL HOGAR (%)**




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

**FIGURA 21. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN DISPOSITIVOS ANDROID (%)**




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

Se analizan los datos más interesantes del nuevo paradigma de la ciberseguridad, ya que los ataques por ransomware y troyano bancarios se han convertido en unas de las amenazas más rentables y frecuentes dirigidas por los cibercriminales.

**Tipología del malware analizado**

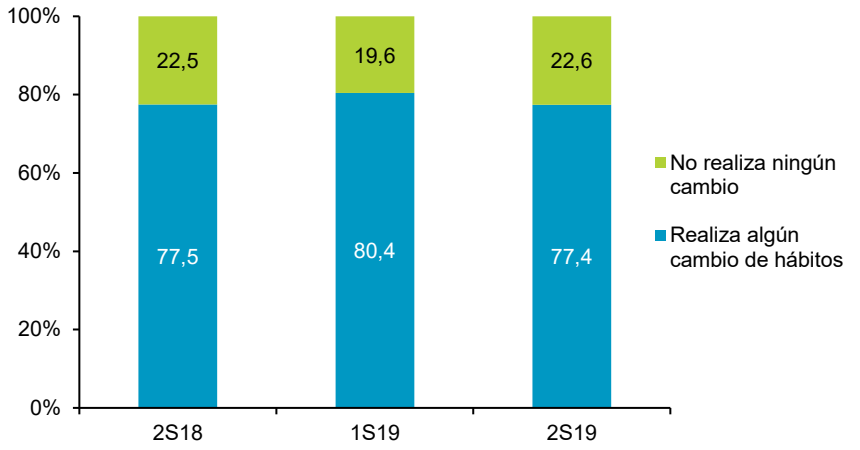
- Troyano bancario: *malware* que roba información confidencial a los clientes de banca y/o plataformas de pago online.
- *Rogueware* o rogue: *malware* que hace creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto 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).

Por norma general, el ransomware se incluye dentro de algún troyano, como una herramienta que desplegará el atacante una vez haya recopilado los datos de interés. Esto hace que a través del ransomware se consigan maximizar las ganancias llevando a cabo el cifrado de archivos en los dispositivos infectados para después pedir un rescate por los mismos.

Aun así, resulta interesante destacar la diferencia de porcentaje que se ha detectado en los ordenadores del hogar, 8,5%, frente al 28,6% en dispositivos Android. Los 20,1 p.p. de diferencia dejan entrever la importancia que le dan los cibercriminales a los datos de los dispositivos móviles y el valor que éstos pueden tener tanto personal como empresarialmente.

**FIGURA 22. EVOLUCIÓN DE LAS REACCIONES ADOPTADAS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%)**

Más de tres de cada cuatro 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*

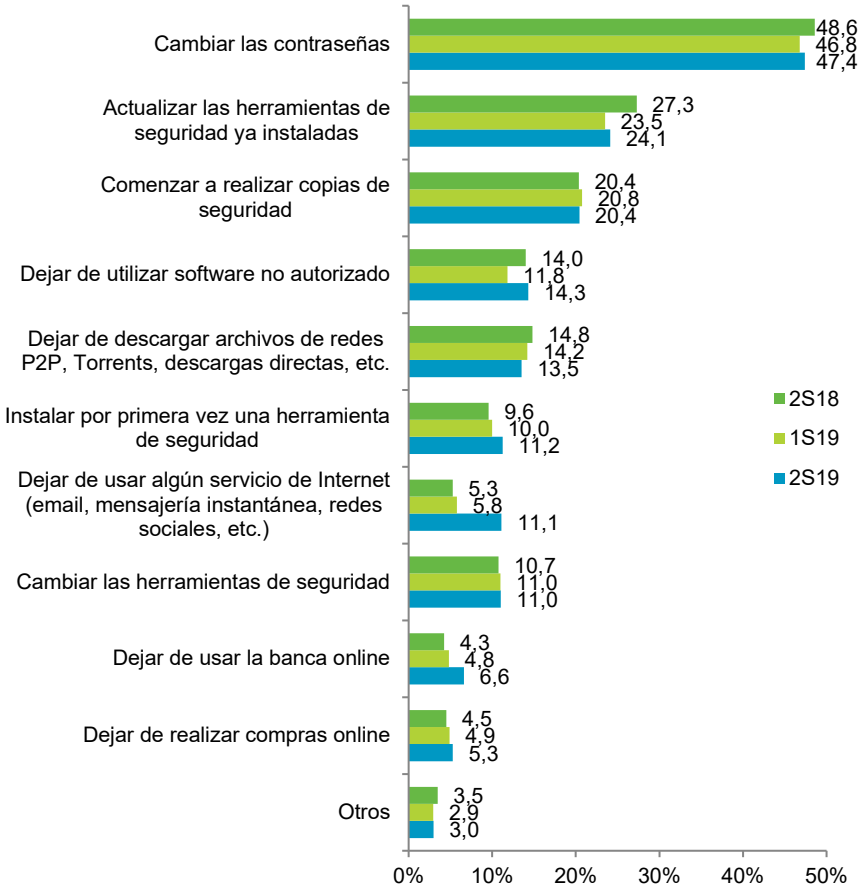
Se percibe un ligero decremento en la adopción de cambios en los hábitos de uso tras sufrir un incidente de seguridad, volviendo a valores similares a los observados durante el segundo semestre de 2018.

Aun así, la diferencia entre los usuarios que adoptan nuevas medidas de seguridad frente a los que no sigue siendo muy significativa dejando unos valores esperanzadores: tres de cada cuatro internautas realiza algún cambio de hábitos tras sufrir una incidencia de seguridad.

El cambio más popular adoptado por los usuarios tras sufrir un incidente de seguridad es la modificación de sus contraseñas (47,4%), habiendo aumentado en 0,6 p.p. desde la pasada oleada. A esta le sigue la actualización de las herramientas de seguridad ya instaladas (24,1%) y la adquisición de nuevos hábitos en la realización de copias de seguridad (20,4%).

Un dato relevante es la caída del software no autorizado, habiendo aumentado su desuso en 2,5 p.p. y superando el valor obtenido en el periodo de 2018 correspondiente a este mismo semestre. La subida más significativa de esta oleada es dejar de usar algún servicio de Internet, que aumenta en 5,3 p.p. Esto puede deberse a la gran variedad de servicios similares existentes y que, en el momento que el usuario tiene una mala experiencia en el uso de alguno de ellos puede optar por una alternativa que le ofrezca más seguridad.

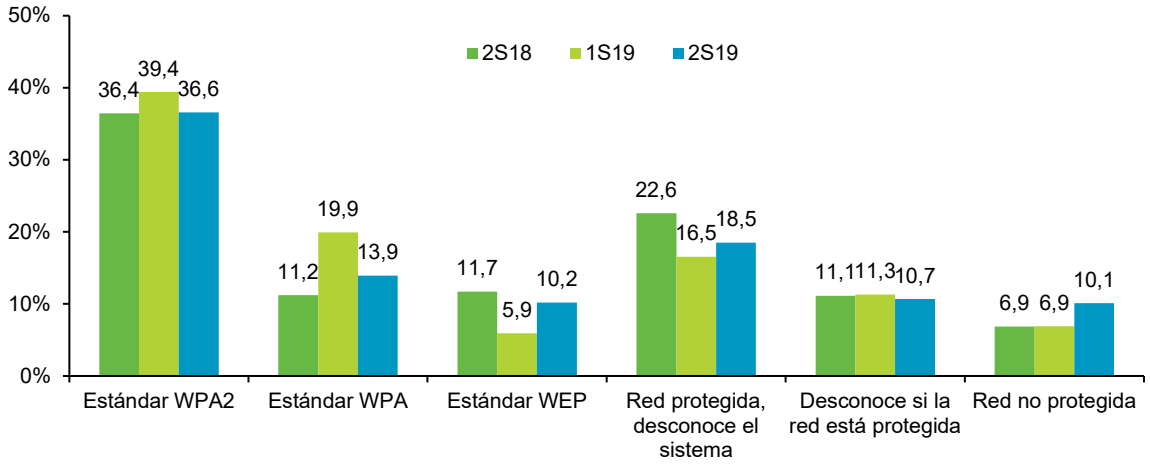
**FIGURA 23. EVOLUCIÓN DE LOS CAMBIOS DE HÁBITOS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%)**




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

Para finalizar, destacar que los usuarios parecen satisfechos con las herramientas de seguridad de que disponen y, únicamente, el 11% se plantea cambiarlas a pesar de haber experimentado un incidente de seguridad.

**FIGURA 24. EVOLUCIÓN DEL SISTEMA DE PROTECCIÓN DE LA RED INALÁMBRICA UTILIZADO POR USUARIOS QUE SOSPECHAN HABER SUFRIDO UNA INTRUSIÓN WI-FI (%)**



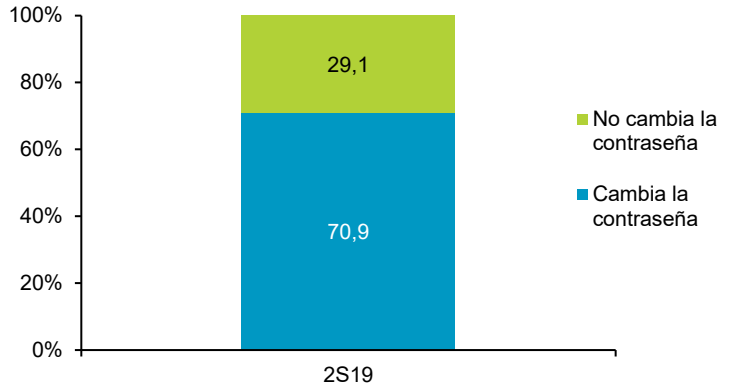

*Base: Usuarios con conexión Wi-Fi propia que sospechan haber sufrido una intrusión en su red*
*Fuente: Panel hogares, ONTSI*

Casi un tercio de los internautas españoles que sospecha haber sufrido una intrusión en su red Wi-Fi, continúa sin usar un sistema de protección, desconoce su estado, o utiliza el estándar WEP (obsoleto)

Resulta notable la gran cantidad de usuarios que pese a sospechar que su red ha sido vulnerada, continúan usando protocolos de seguridad desaconsejados debido a resultar vulnerables (WEP, 10,2%), que continúan desconociendo el tipo de protocolo utilizado (18,5%), si la red está o no protegida (10,7%), o que incluso mantiene una red sin protección (10,1%).

También es importante destacar que el hecho de que el mayor porcentaje de usuarios que sospecha haber sufrido alguna intrusión en su red inalámbrica del hogar se corresponda con aquellos que utilizan el estándar WPA2, no se debe a que éste protocolo sea más inseguro que otro sino que responde a su mayor tasa de uso. Es realidad WPA2 es el estándar más seguro actualmente y, por tanto, el recomendado.

**FIGURA 25. MODIFICACIÓN DE LA CONTRASEÑA DE LA RED INALÁMBRICA TRAS SOSPECHAR DE UNA INTRUSIÓN WI-FI (%)**




*Base: Usuarios con conexión Wi-Fi propia que sospechan haber sufrido intrusión en su red*
*Fuente: Panel hogares, ONTSI*

Como norma general es recomendable cambiar la contraseña de la red Wi-Fi y no utilizar la que configurada por defecto. Esta recomendación se torna en imprescindible si se ha sufrido una intrusión en la red del hogar, o se sospecha de ella.

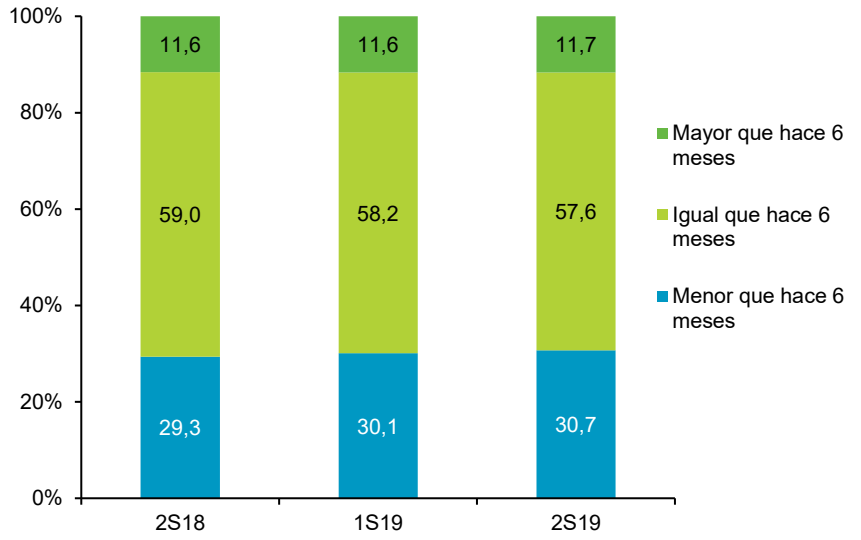
Sin embargo se observa que un 29,1% de usuarios no toma esta acción y mantienen la misma contraseña de acceso, permitiendo que su red inalámbrica permanezca comprometida. Esto puede deberse a que desconocen el procedimiento a seguir para cambiar la contraseña o porque no son ellos mismos quienes administran la red Wi-Fi.

Es necesario recordar que el hecho de acceder a la red del hogar podría suponer también el acceso a las carpetas y recursos compartidos en dicha red, como documentos privados o cualquier dispositivo conectado a la misma.

## 5. Confianza en el ámbito digital en los hogares españoles

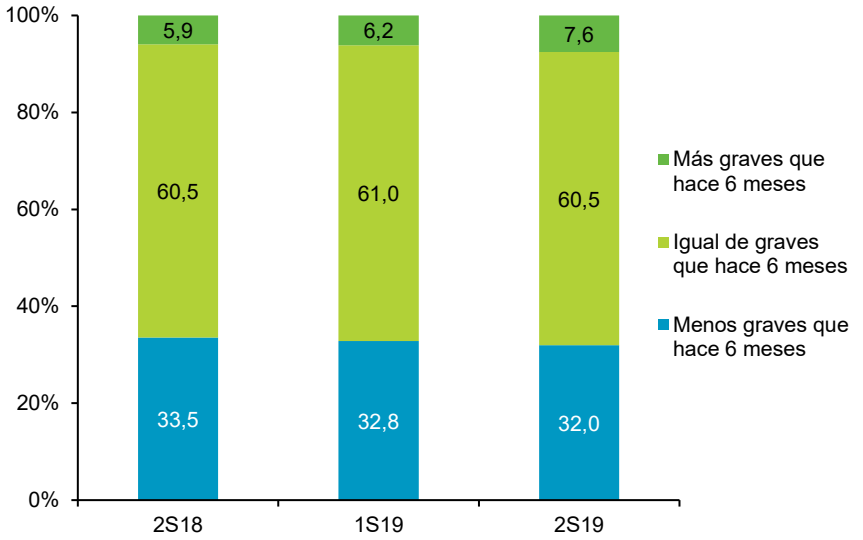
En este último apartado se han recogido las valoraciones propias de los usuarios en cuanto a los riesgos que se corren al navegar por el mundo digital, la responsabilidad que conlleva estar conectado a la Red, y la confianza depositada en Internet.

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




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

**FIGURA 27. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%)**

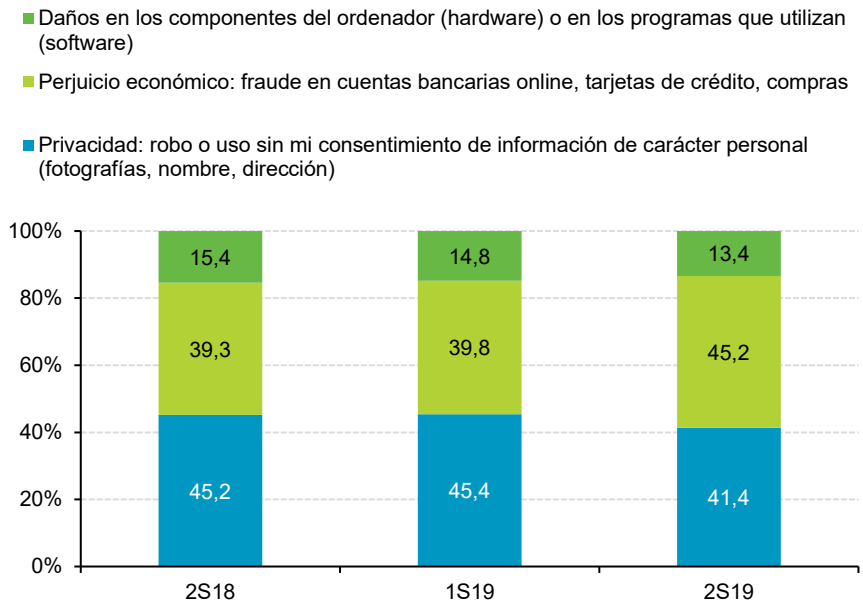



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

La percepción de los usuarios en cuanto a la cantidad y gravedad de incidencias de seguridad acontecidas en los últimos 6 meses se mantiene constante.

La mayoría consideran que el número de incidencias y su gravedad no se han visto modificados en ese periodo (57,6% y 60,5% respectivamente).

**FIGURA 28. EVOLUCIÓN DE LA PERCEPCIÓN DE RIESGOS EN INTERNET (%)**



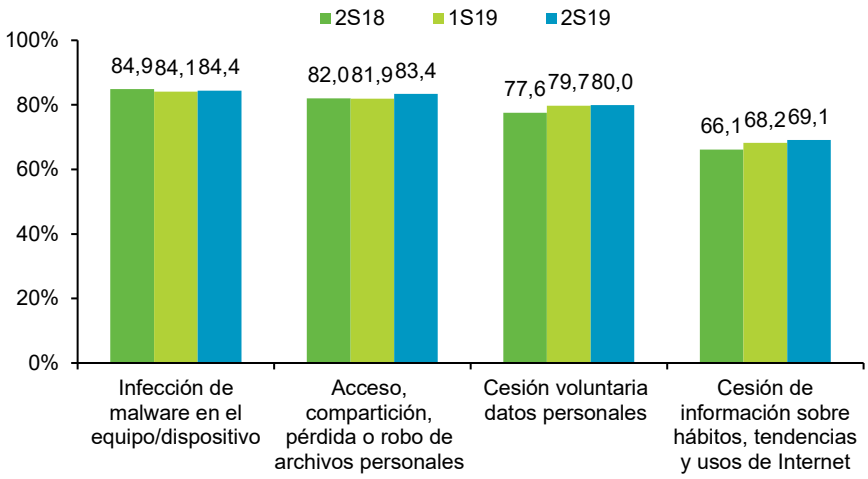

*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

Durante este periodo se observa como el perjuicio económico se presenta como el principal riesgo percibido por los usuarios (45,2%) arrebatando este puesto al riesgo de pérdida de privacidad (41,4%).

Este aumento de preocupación ante el perjuicio económico se encuentran en consonancia con otros datos observados anteriormente como la cantidad de equipos infectados por malware del tipo troyanos (**FIGURA 15** y **FIGURA 16**) y las situaciones de fraude sufridas (**FIGURA 18**).

También cabe recordar que los datos personales y la pérdida de privacidad, aunque han bajado en el ranking de la percepción de los panelistas, continúa siendo una información muy demandada y cotizada ya que pueden ser usados por parte de los atacantes para su beneficio propio, o incluso ser vendidos en mercados negros.

**FIGURA 29. EVOLUCIÓN DE LA VALORACIÓN DE LOS PELIGROS DE INTERNET -BASTANTE O MUY IMPORTANTE- (%)**



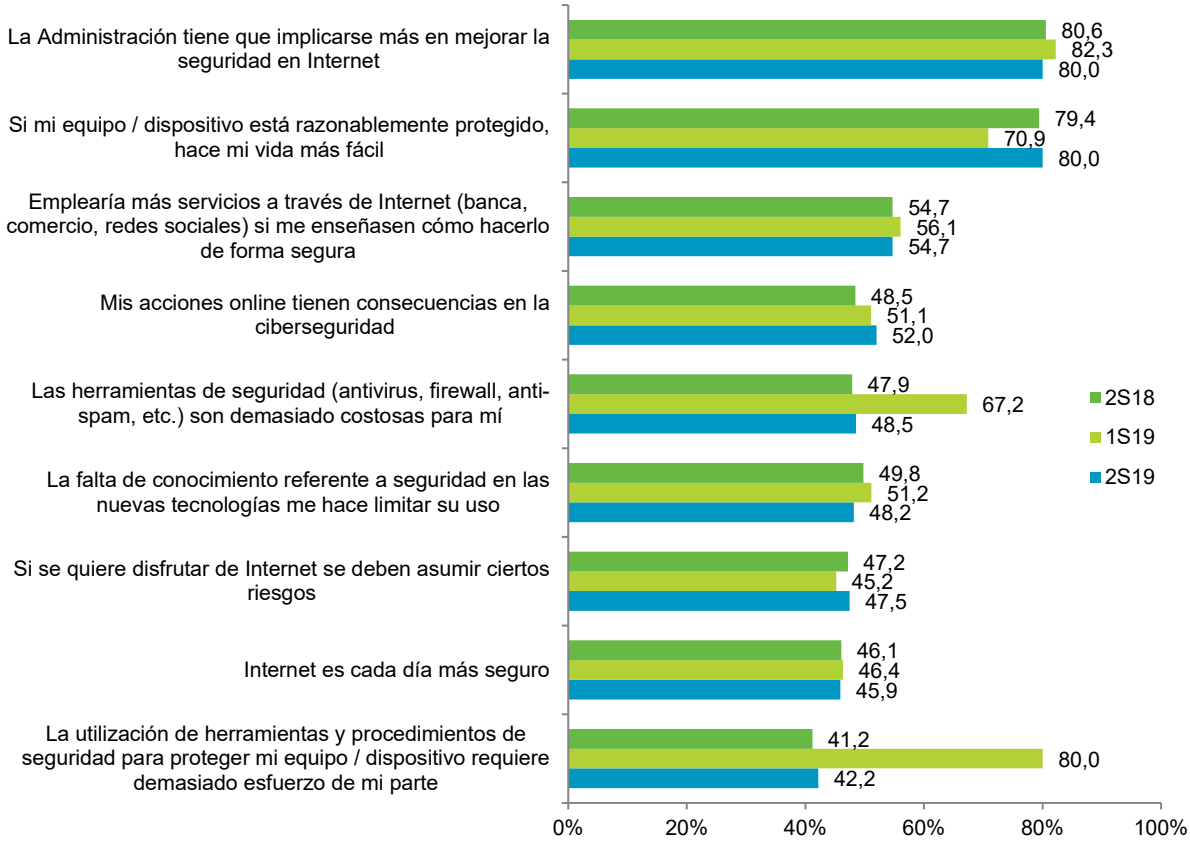

*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

La valoración de la gravedad de todas las amenazas a las que los usuarios pueden quedar expuestos ha aumentado ligeramente frente a pasadas oleadas.

Más de ocho de cada diez usuarios considera que la infección de malware o el acceso, compartición, pérdida o robo de archivos personales, o la cesión voluntaria de datos personales, son los mayores peligros a los que se puede enfrentar alguien que use Internet.

Tal y como se comentaba anteriormente, se debe prestar una especial atención a la cesión voluntaria de datos personales, y de información sobre hábitos, tendencias y usos de Internet debido a que, aunque el propio usuario no lo valore adecuadamente, este tipo de información resulta de gran interés para terceras personas y empresas.

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

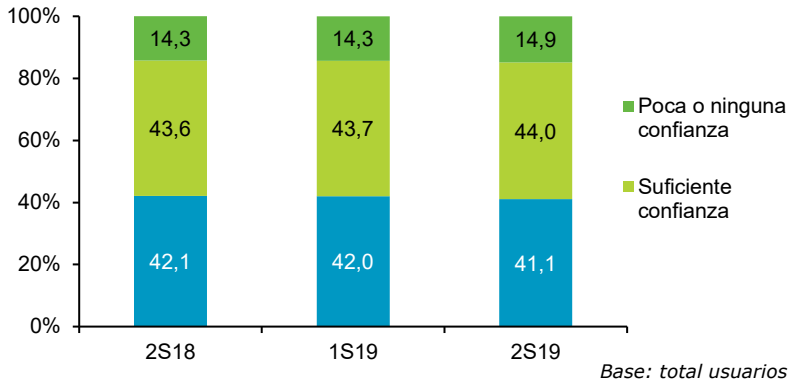



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

La concienciación del usuario sobre las repercusiones de sus acciones sobre la seguridad continúa aumentando (+0,9 p.p.), lo que contribuye a la adquisición de hábitos más prudentes a la hora de usar Internet.

Además, ocho de cada diez usuarios opinan que si su equipo está mejor protegido, le evita preocupaciones, y el 45,9% de los usuarios piensa que Internet es cada día más seguro. Sin embargo, un 47,5% declaran que hay que asumir ciertos riesgos si se quiere disfrutar de la experiencia de navegar por Internet.

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




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

La total confianza en Internet entre los panelistas sigue experimentando la misma tendencia a la baja ya observada durante las últimas oleadas, situando en el 41,1% a aquellos que declaran mucha o bastante confianza.

Sin embargo, a pesar de esta tendencia decreciente, no se ha alcanzado el mínimo histórico a que se llegó durante el primer semestre de 2017, momento en el que la alta confianza cayó hasta el 39,9% de las declaraciones.

Tan solo el 14,9% de los usuarios presentan una confianza baja o inexistente en Internet.

## 6. Conclusiones

Durante el periodo comprendido entre los meses de julio a diciembre de 2019 han continuado apareciendo brechas de seguridad en grandes compañías dejando al descubierto los datos personales de millones de usuarios, como en el caso de las redes sociales o de aplicaciones en la nube. Entre las filtraciones que han recibido más atención por parte de la prensa especializada se podrían destacar, por ejemplo, la concerniente a una base de datos que contenía información privada de usuarios de Facebook y que no se encontraba adecuadamente protegida, dejando expuestos los datos personales (identificador de los usuarios y sus números de teléfono entre otros) de más de 400 millones de usuarios de esta famosa red social[1].

Otro ejemplo de filtración masiva de datos se produjo en la empresa de domótica Wyze en el mes de diciembre[2]. En esta ocasión, los datos expuestos incluían desde correos electrónicos hasta datos de la red inalámbrica Wi-Fi utilizada por los dispositivos de domótica e, incluso, datos biométricos.

Ante este tipo de noticias resulta comprensible la preocupación de cerca del 80% de los usuarios españoles ante la pérdida de

[1] https://www.silicon.co.uk/security/cyberwar/database-facebook-phone-numbers-284467

[2] https://forums.wyzecam.com/t/updated-02-13-20-data-leak-12-26-2019/79046

privacidad de sus datos. No obstante, algunos internautas se prestan a facilitar sus datos personales al darse de alta en servicios de Internet (30,3%), a través de correo electrónico (21,5%), no configuran adecuadamente sus perfiles en redes sociales permitiendo que su información sea accesible por cualquier otro usuario de la red social (15,4%), por amigos de amigos (23,4%), o incluso desconocen el estado de la privacidad de su perfil (5,4%), y no leen los términos de servicio y condiciones de uso (68,2%) en los que se puede especificar el uso que se hará de los datos recopilados por el servicio o programa.

Por otra parte, los usuarios siguen sin prestar la debida atención al uso de contraseñas robustas, reutilizan la misma contraseña para varios servicios online, y no las modifican periódicamente o como mínimo cuando se ha sufrido algún incidente de seguridad (únicamente el 47,7% declara tomar esta medida). A este respecto, un estudio anual[3] de las contraseñas utilizadas por los usuarios, continua detectando el uso de contraseñas triviales, y fácilmente recuperables mediante ataques por diccionario o fuerza bruta.

Las formas más comunes de que un ciberdelincuente se pueda hacer con las contraseñas de los usuarios incautos son las campañas de spam por correo electrónico (sufrido por más del 85% de los internautas españoles mientras que tan solo el 14,1% utiliza alguna herramienta específica para combatirlo) y el malware (por ejemplo los keyloggers). A través del correo no deseado se presentan diferentes argucias, como simular provenir de una entidad de confianza para el usuario (banca, comercio, administraciones, etc.), proponer concursos, ofrecer premios, solventar alguna incidencia de carácter urgente para tratar de engañar al usuario y obtener sus credenciales o información personal.

Ante esta situación, resulta obvio comprender la importancia de utilizar una contraseña única para cada servicio en lugar de reutilizarlas, puesto que si una de ella es robada o comprometida (ya sea mediante engaños al usuario, a través de una filtración por parte de la empresa que ofrece el servicio, o por vulnerabilidades en los programas o aplicaciones[4]) automáticamente estaría permitiendo acceso a todos los demás servicios; llegándose al extremo de poder acceder al correo electrónico del usuario y desde el mismo poder solicitar la recuperación o restauración de los credenciales de acceso de todos aquellos servicios en los que se haya registrado utilizando dicha cuenta de correo.

En este punto es importante recordar algunas de las recomendaciones para componer una contraseña segura como combinar mayúsculas, minúsculas, números y símbolos, y utilizar una longitud adecuada para lograr fortaleza ante ataques de fuerza bruta. Ante todo evitar el uso de palabras simples que aparezcan en el diccionario (de cualquier idioma), nombres propios, nombres de mascotas, fechas (de cumpleaños, aniversarios, etc.), y patrón es de teclado (como por ejemplo 'qwertyuiop' o '1qaz2wsx'). Dado que la contraseña resultante supone una 'cadena de caracteres sin sentido' que es prácticamente imposible de recordar (y que se debe

[3] https://www.teamsid.com/1-50-worst-passwords-2019/

[4] https://privacy.twitter.com/en/blog/2019/twitter-for-android-security-issue

usar una diferente para cada servicio), resulta adecuado el uso programas gestores de contraseñas para facilitar esta labor. Además este tipo de software suele permitir la generación automática de contraseñas aleatorias y evaluar su robustez.

Otro de los principales riesgos que se perciben en Internet es el perjuicio económico (45,2%), que también resulta comprensible puesto que el 70% de internautas declara haber sufrido algún tipo de situación de fraude durante los últimos seis meses de 2019.

Afortunadamente, los desarrolladores de navegadores web cada vez se implican más en la lucha contra el fraude[5], incluyendo mecanismos de bloqueo de páginas falsas, de detección de intentos de robo de información mientras se navega, e incluso para el bloqueo de descargas identificadas como peligrosas.

Sin embargo, el 44,4% de los usuarios españoles continúa adoptando conscientemente conductas de riesgo en su uso habitual de Internet, pese a que el 59,8% continúa declarando que han sufrido algún tipo de incidencia durante el último semestre.

La infección de malware ocupa el primer lugar entre los peligros al navegar por Internet más valorados (según el 84,4% de los cibernautas) y, sin embargo, el uso real de soluciones antivirus solamente tiene presencia en el 65% de los ordenadores y el 51,5% de los dispositivos Android, menos del 50% de usuarios se preocupa por analizar los archivos descargados y tan solo el 62,8% se asegura de haber descargado realmente el contenido que buscaba.

No sorprende, por tanto, que se detecte una gran cantidad de equipos infectados, sobre todo entre los ordenadores del hogar (61,9%). Aunque el dato más preocupante es que el 52,1% de los usuarios que sufren algún tipo de infección de malware, lo desconoce totalmente a pesar de que entre los tipos de infección más comunes se encuentran los adwares (52,6%) un tipo de malware que no trata de ocultarse ante el usuario ya que su finalidad es mostrar anuncios y publicidad no deseada.

También es importante recordar que, en muchas ocasiones, las infecciones son facilitadas por hecho de no aplicarse a tiempo los debidos parches de seguridad que solucionan vulnerabilidades conocidas del software[6], siendo poco más de la mitad (51,6%) aquellos usuarios que aplican realmente estas actualizaciones.

Tal vez, el problema se encuentra en que el usuario tiene la percepción general de que los incidentes de seguridad acontecidos siguen siendo más o menos igual de frecuentes y de una gravedad similar a lo largo del tiempo, lo cual redunda en que no se aprecie un cambio significativo en las conductas de uso de la Red ni en las medidas de seguridad tomadas. Pero en realidad las amenazas que acechan en la Red de Redes se encuentran en continua evolución con el objetivo de pasar desapercibidas y lograr sus objetivos. Y, ante esto, la mejor solución es la prevención.

[5] https://www.theverge.com/2019/12/10/21004434/google-chrome-79-password-protections-security-stolen-password-data-features

[6] https://www.techrepublic.com/resource-library/whitepapers/costs-and-consequences-of-gaps-in-vulnerability-response/

# ANÁLISIS DE URGENCIA: La ciberseguridad durante la crisis del coronavirus

Actualmente se está viviendo una situación de crisis internacional debida a la pandemia causada por un nuevo virus altamente infeccioso que rápidamente se ha propagado por los cinco continentes. Ante tales circunstancias ha surgido la necesidad de la toma de medidas extraordinarias que incluyen el confinamiento y aislamiento social con el objetivo de reducir las probabilidades de contagio entre la población y la consecuente saturación de los sistemas sanitarios de cada país. El siguiente análisis destaca los riesgos de seguridad que se están produciendo y apunta algunos consejos que permitan mitigar la situación.

La digitalización en tiempo récord de empresas y ciudadanos ha permitido una cierta continuidad en el plano laboral, en aquellos casos que ha sido posible, en el plano doméstico, para mantenerse informados y en contacto con otras personas, así como herramienta de ocio y en el aspecto educativo ayudando a mantener la actividad en colegios y universidades. Esto ha tenido un impacto importante en la situación laboral de miles de trabajadores que se han visto imposibilitados de realizar sus labores, cabe recordar que el teletrabajo es una opción tan solo al alcance de determinados puestos de trabajo o sectores de actividad. De tal forma que las empresas, sobre todo las que ofrecen servicios en línea, se han visto igualmente obligadas a tomar determinadas medidas con el objetivo de hacer frente a la situación.

El aumento sin precedentes de la demanda en los servicios en línea de ocio queda patente en los récords registrados por algunas plataformas como Steam, que a mediados de marzo superó los 20 millones de usuarios conectados simultáneamente,y posteriormente volvería a superar dicho récord sobrepasando los 23,5 millones de usuarios conectados. Otras empresas que ofrecen servicios en línea relacionados con el ocio han aprovechado para ofrecer acceso gratuito a su contenido premium o de pago con el objetivo de amenizar la situación y combatir la monotonía y, a la vez, hacer promoción de dichos servicios y contenidos. Así nos encontramos desde páginas de ocio para adultos, hasta canales de emisión en continuo (streaming) infantiles colaborando para hacer la situación de aislamiento más llevadera.

Sin embargo, todo este aumento de uso de la red también tiene sus consecuencias. Y muchas empresas proveedoras de contenidos relacionados con el ocio se han visto en la tesitura de reducir el ancho de banda consumido por sus servicios (por ejemplo, Netflix, Youtube, Prime Video, Disney+, Playstation Networks o Xbox Live Gold) con el objetivo de preservar la calidad y estabilidad de las conexiones durante los picos más altos de tráfico y evitar la saturación de las redes, priorizando de esta manera el tráfico relacionado con el teletrabajo y la consecuente dependencia del acceso a Internet.

A tales efectos, incluso empresas desarrolladoras de software (entre ellas Microsoft y Google) han tomado la decisión de minimizar o pausar el despliegue de actualizaciones no críticas (por ejemplo aquellas opcionales, que agregan nuevas funcionalidades, o las que no son de seguridad) con el objetivo de mantener versiones estables que no afecten a la productividad de los usuarios

que precisan trabajar con estas herramientas.

Afloran también iniciativas como el llamamiento social para hacer uso de la computación distribuida para agilizar las investigaciones sobre el coronavirus utilizando la potencia de los ordenadores del hogar, llegando a convertirse actualmente en uno de los proyectos de este tipo de mayor envergadura en el planeta y alcanzando un rendimiento de 98.7 PetaFlops. El objetivo común es colaborar en la ejecución de simulaciones de la estructura molecular del virus para intentar desarrollar terapias efectivas contra la infección lo antes posible.

Bajo esta situación también resulta factible presuponer que los cibercriminales se encuentran en el mismo estado de confinamiento, con un mayor tiempo disponible para dedicar a actividades fraudulentas e incluso con la necesidad de potenciar sus ataques en caso de que su situación laboral se haya visto negativamente afectada.

Frente a estas medidas y actuaciones expuestas para mejorar la situación actual del ciudadano y la colaboración para buscar soluciones al problema, surge la otra cara de la moneda: los atacantes aprovechan el desconcierto, la desinformación, el distanciamiento social, la saturación a la que se están viendo sometidas las autoridades, e incluso los miedos y esperanzas de los ciudadanos ante la actual situación sin precedentes que se está viviendo para crear cebos y sacar el máximo provecho, creándose un escenario positivo para el fraude online, phishing, malware, ingeniería social, etc.

Se ha detectado el registro de más de 51 mil (más de 30 mil durante las dos últimas semanas de marzo) nombres de dominio que contienen alguna palabra clave relacionada con la pandemia, como "coronavirus", "corona-virus", "covid19" o "covid-19", muchos de los cuales han sido creados únicamente con fines fraudulentos.

Actualmente se están registrando una media de 2600 ataques diarios (con picos de hasta 5 mil) con relación a esta crisis mundial, cifra que continúa incrementándose día a día. Destacan las campañas de suplantación de entidades conocidas y confiables para el usuario como la Organización Mundial de la Salud, instituciones sanitarias o administraciones públicas para enviar correos electrónicos que contienen información falsa sobre el virus para lograr la atención del receptor, como por ejemplo, datos acerca del número de afectados, mapas de la situación, descubrimiento de vacunas o remedios, venta de material sanitario, recomendaciones para prevenir el virus, instrucciones para detectarlo, ayudas gubernamentales o de empresas para paliar las necesidades del ciudadano , etc. Como ocurre con este tipo de ataques, al abrir el documento adjunto al correo, al descargarlo desde el enlace que se provee en el correo o accediendo a un sitio web malicioso, el equipo o dispositivo del usuario resulta infectado con algún tipo de malware, o se torna en víctima de un phishing o fraude en el que su información personal, privada e incluso bancaria puede quedar expuesta.

Pero no se debe perder de vista que las campañas habituales de phishing y fraudes continúan estando muy presentes. De hecho, el

envío masivo de correos electrónicos suplantando a comercios en línea, empresas de logística, e incluso servicios técnicos de proveedores que solicitan un pago para liberar un envío, paquete o pedido que ha sido retenido por cualquier causa ficticia es otra manera de aprovechar el panorama actual y el incremento de las compras a través de Internet debido al confinamiento. Al aumentar el número de estas transacciones, la probabilidad de que un usuario haya realizado una compra en línea -motivado por el miedo y peligro de contagio al acceder a su comercio habitual- en una pequeña ventana temporal previa a la recepción de este tipo de estafas se incrementa, y por tanto las expectativas son de una mayor tasa de éxito.

Igualmente la distribución de falsas encuestas o promociones utilizando la imagen de algún comercio o marca reconocida incitando al usuario a cumplimentar sus datos bajo la falsa promesa de recibir cupones de decenas o centenas de euros, se encuentra en auge en las redes sociales. En realidad el único beneficiado, como en todos los fraudes, es quien lo realiza y en este caso es típico utilizar los datos recopilados para dar de alta al usuario en servicios de SMS Premium, y además, enviarle posteriormente spam.

También ha aumentado el número de estafas telefónicas, bien en forma de ataque de ingeniería social para recopilar información privada bajo la excusa de dar soporte al ciudadano; bien como campaña de ayuda humanitaria para los más desfavorecidos o afectados por la pandemia a través del envío de un mensaje SMS a un determinado número cuyos beneficios, por supuesto, irán a parar al bolsillo del ciberdelincuente.

Otra nueva tendencia que se está percibiendo es la creación de apps maliciosas que pretenden hacer creer al usuario que sirven para realizar un seguimiento sobre la evolución de las infecciones de covid-19, ocultando su intención real de instalar malware. Como por ejemplo, el llamado CovidLock, un ransomware que bloquea el dispositivo y solicita un rescate en bitcoins.

Estas aplicaciones no se encuentran en los repositorios oficiales de aplicaciones sino que son descargadas desde sitios controlados por los desarrolladores de malware o markets alternativos con un lexo o nulo control de calidad y seguridad. Es por ello que resulta altamente recomendable no instalar en el dispositivo apps desconocidas desde markets no oficiales, o de confianza, para no exponerse a este tipo de riesgos en auge.

Paralelamente a la especulación que está sufriendo este tipo de productos, surgen también tiendas digitales falsas para vender material sanitario como mascarillas, guantes, desinfectante, remedios "mágicos" e incluso productos de higiene personal y papel higiénico.

La víctima, que no pone precio a su salud ni a la de sus allegados, se arriesga en el mejor de los casos a recibir un placebo o un producto de baja calidad, pero también corre el riesgo de recibir productos que no han superado las debidas medidas de seguridad y podrían ser incluso peligrosos para la salud.

Pero no son únicamente los usuarios los que se encuentran en

riesgo, los cibercriminales no hacen excepciones, y su afán de lucro se muestra por encima de cualquier sentimiento de humanidad o compasión para con sus semejantes. Así pues, se lanzan ataques de ransomware como NetWalker y Ryuk contra instituciones hospitalarias en el peor momento posible, con la intención de forzar el pago del rescate para liberar el sistema informático de los mismos sin tener en consideración las vidas que pueda haber en juego.

Inclusive la necesidad de teletrabajar abre nuevas posibilidades a los atacantes, debido entre otras cosas a la celeridad con la que se han tenido que implementar los sistemas de teletrabajo. El riesgo al que se enfrentan las empresas ha aumentado, que podrían ver comprometida la integridad de sus cuentas corporativas y la confidencialidad de la información, al verse relajadas las medidas de seguridad y hábitos prudentes por parte del empleado al realizar las labores habituales desde la comodidad del hogar y encontrarse en un entorno más vulnerable. Además, muchos trabajadores se han visto obligados a modificar su forma de trabajo sin haber tenido tiempo de recibir la debida formación, tanto para el desempeño de sus labores como en ciberseguridad.

**Consejos para mitigar los riesgos de seguridad**

Frente a estas perspectivas se deben tomar una serie de medidas:

- El uso exclusivo del equipamiento de la empresa u organización, cuando esto sea posible.
- Uso de contraseñas para iniciar sesión y desbloquear el equipo, un usuario con nivel de privilegios adecuado
- Utilización de software antivirus y firewall
- Evitar la instalación de programas o aplicaciones ajenas al entorno laboral en equipos corporativos,
- Cifrado de los dispositivos de almacenamiento para evitar el acceso a la información en caso de robo o pérdida
- Implantar medidas para localizar el dispositivo y realizar un borrado remoto de la información
- Utilizar en la medida de lo posible conexiones fiables y cifrar las comunicaciones y conexiones a recursos de la empresa, forzando el uso de doble factor de autenticación para acceder a recursos fuera de la red corporativa, cerrar las conexiones al finalizar la jornada y limpiar los archivos temporales, cookies e historial del navegador.
- Además se debe tener presente que el tiempo de respuesta ante una incidencia física que afecte al equipamiento puede ser indeterminado debido al aislamiento y la dificultad para prestar la asistencia técnica necesaria.

A tales efectos se recomienda mantener un escritorio limpio y libre de líquidos que pudieran derramarse y afectar al equipo de trabajo. Ante esta situación en la que no se controlan muchos factores de seguridad, es de importancia vital el uso de copias de seguridad periódicas para preservar la información vital de la empresa en el caso de que se produzca cualquier incidente de seguridad.

De forma general y en base al panorama actual es necesario extremar las precauciones. Ante la necesidad de información se recomienda acudir siempre a fuentes fiables y contrastadas, e ignorar la información recibida vía email, redes sociales, o procedente de cualquier fuente desconocida y no solicitada.

Ante cualquier petición o solicitud recibida, se recomienda mantener la calma, analizar y reflexionar sobre lo que se insta a hacer antes de actuar o tomar decisiones precipitadas. La prudencia, la desconfianza, y un buen conjunto de herramientas de seguridad, se tornan en estos momentos en unos aliados claves e indispensables para capear el temporal de ciberataques.

Y se debe tener presente que, al contrario que en el mundo físico, en la Red de Redes no existe el aislamiento y todos estamos interconectados por lo que las incidencias de seguridad e infecciones de malware siempre son posibles.

El informe del *"Estudio sobre la Ciberseguridad y Confianza del ciudadano en la Red"* 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