ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

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

ÍNDICE

ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

Red.es en colaboración con Hispasec Sistemas y GFK realizan 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 (smartphone y tableta).

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 su remediación por parte de los usuarios y 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.

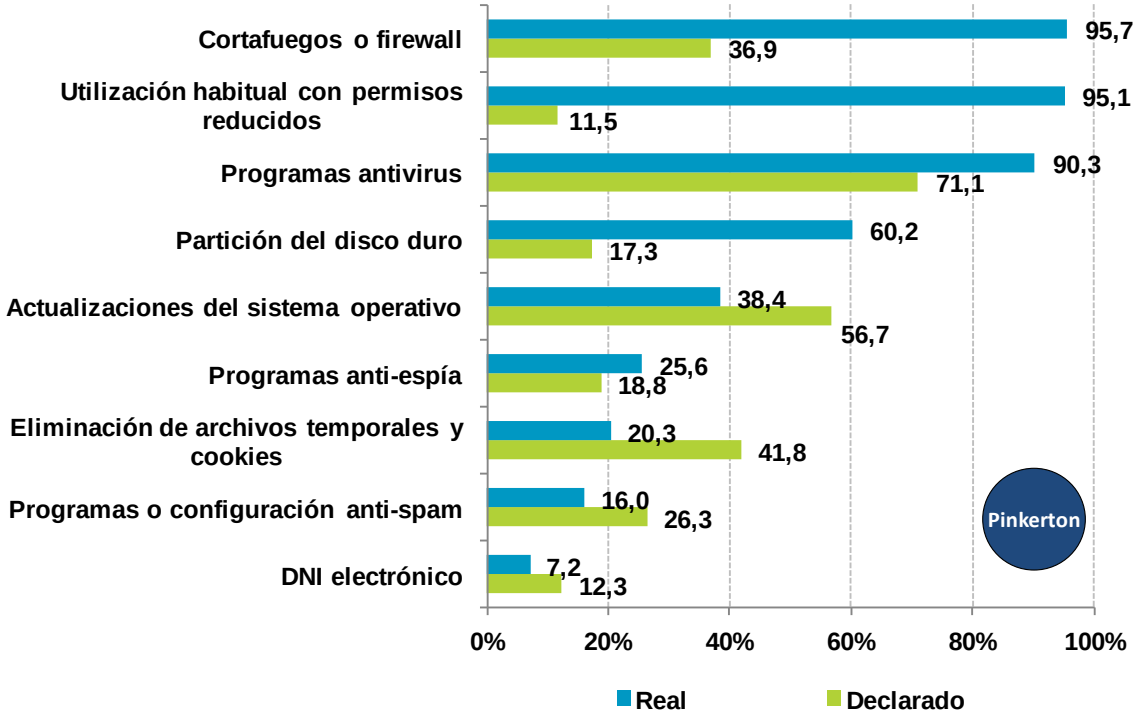
Los datos declarados son obtenidos de las encuestas online realizadas a los hogares que han conformado la muestra del estudio, mientras que para los datos reales se utiliza el software Pinkerton. Este software analiza los sistemas recogiendo datos del sistema operativo, su estado de actualización y las 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. Medidas de seguridad

La presencia de medidas de seguridad en los equipos (ordenadores del hogar y dispositivos Android) se erige en uno de los pilares básicos de la seguridad de la información.

A continuación, se presentan los datos procedentes de las declaraciones de los usuarios españoles y los recopilados mediante el análisis real de sus sistemas (ordenadores del hogar y dispositivos móviles) con la herramienta Pinkerton en cuanto a las medidas de seguridad utilizadas.

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



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

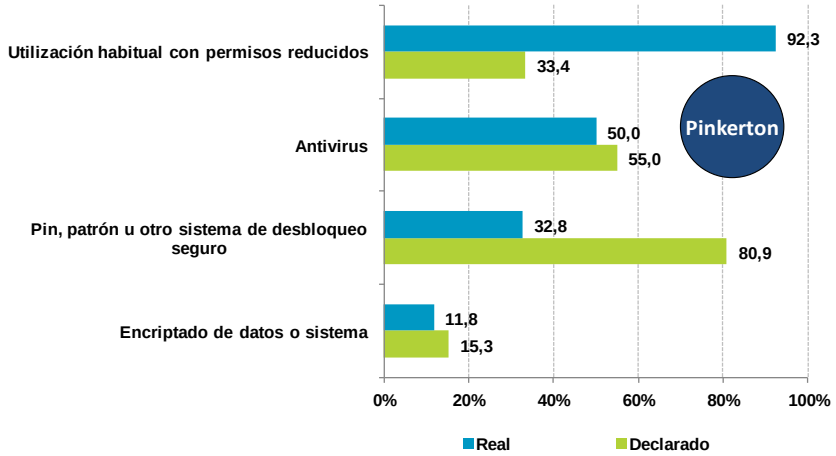
Entre las declaraciones aportadas por los internautas españoles con respecto a sus ordenadores domésticos del hogar y los datos reales recopilados con Pinkerton existen importantes discordancias. Las mayores brechas se encuentran en la utilización habitual con permisos reducidos (+83,6 p.p. de uso real), en el uso de cortafuegos o firewall (+58,8 p.p. de uso real), y en la existencia de particiones en el disco duro (+42,9 p.p. de uso real).

La mayoría de los sistemas operativos de hoy en día, suelen definir cuentas de usuario y cuentas de administrador. La utilización normal en el día a día se realiza con una cuenta de usuario con bajos privilegios y, en caso de realizar alguna acción que así lo requiera, el sistema solicitará credenciales de administrador del sistema o confirmación para la realización de dicha tarea. Esta sería la principal causa por la que los usuarios domésticos no perciben estar utilizando una cuenta con privilegios limitados.

La incongruencia en el uso de software cortafuegos o firewall puede deberse a que hoy en día muchos usuarios utilizan suites de seguridad que incluyen varias herramientas y sin embargo los usuarios identifican dichas suites como la herramienta más conocida del conjunto: el antivirus.

De forma similar ocurre con las particiones del disco duro: tanto en sistemas pre-instalados como durante el proceso de instalación, gran parte de los sistemas operativos actuales crean más de una partición de manera transparente para el usuario. Éstas suelen ser utilizadas para tareas de diagnóstico o recuperación del sistema y suelen permanecer ocultas al usuario, explicando así la discordancia en los datos registrados.

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



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

En cuanto a los dispositivos Android, la mayor desigualdad se encuentra también en la utilización habitual con permisos reducidos (no 'root'), con un 92,3% de uso real, mientras que únicamente un tercio (33,4%) de los usuarios son conscientes de este hecho. Los datos de ambos sistemas ponen de manifiesto la falta de necesidad real de altos privilegios en el uso diario tanto del ordenador como del dispositivo Android.

Además, en estos últimos, lograr permisos de 'root' implica realizar un proceso que puede no estar al alcance de todos los usuarios y que puede conllevar la anulación de la garantía por parte del fabricante al haberse manipulado el dispositivo.

Otra gran brecha entre la realidad y las opiniones de los usuarios se observa en los sistemas de desbloqueo seguro del dispositivo: el 80,9% de las declaraciones afirman su utilización, mientras que el valor obtenido por Pinkerton revela que únicamente el 32,8% tienen un sistema de desbloqueo seguro en sus dispositivos.

En este punto hay que matizar la diferencia entre un sistema de desbloqueo seguro y otro que no lo es. El primero requiere de una contraseña, clave numérica o PIN, patrón de forma, implican un sensor basado en algún parámetro biométrico, etc.; es decir de un elemento que únicamente el usuario conoce o dispone para desbloquear y acceder al dispositivo.

Los sistemas de desbloqueos no seguros son usados simplemente para evitar pulsaciones no deseadas mientras el dispositivo no está en uso activo, y no requieren nada más que, por ejemplo, un movimiento deslizante.

Obviamente esto supone un alto riesgo para la privacidad, ya que cualquier persona con acceso físico al dispositivo (descuido, pérdida, robo, etc.) podría acceder tanto a la información contenida en el dispositivo como a la almacenada online dado que es habitual que las aplicaciones se encuentren con la sesión de usuario ya iniciada.

El uso real de software antivirus en Android se sitúa en la mitad (50%). Estos valores, a pesar de experimentar un aumento desde análisis anteriores, continúan manteniéndose en unos niveles de riesgo. El software antivirus es una medida básica de seguridad que cobra una especial importancia en un escenario donde el dispositivo móvil tiende a sustituir al ordenador del hogar, la banca en línea y las compras online se tornan en tareas cotidianas, y el malware para Android se encuentra en pleno auge.

USO HABITUAL CON PRIVILEGIOS REDUCIDOS EN WINDOWS (DATO REAL)

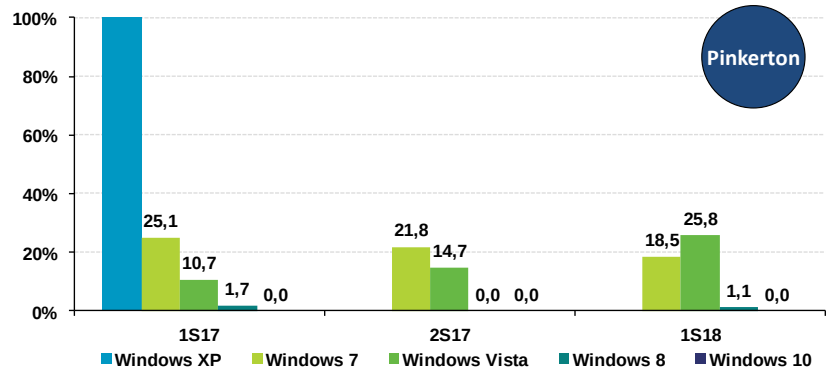
100%
CON PERMISOS REDUCIDOS EN WINDOWS 10

98,9%
CON PERMISOS REDUCIDOS EN WINDOWS 8

81,5%
CON PERMISOS REDUCIDOS EN WINDOWS 7

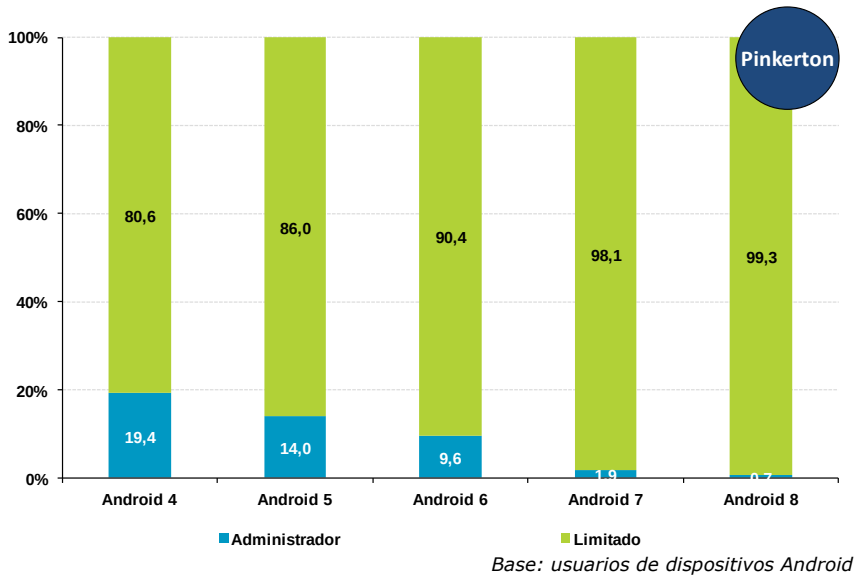
74,2%
CON PERMISOS REDUCIDOS EN WINDOWS VISTA

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

Los sistemas operativos de Microsoft y Android establecen por defecto permisos reducidos para los usuarios. Es habitual en los sistemas de escritorio que exista adicionalmente una cuenta de administrador de forma que se solicitan las credenciales para elevar privilegios en el momento que sea necesario (por ejemplo, para instalar alguna actualización). Por otra parte, en Android es

[1]Los análisis realizados a partir del segundo semestre de 2017 (2S17), dejan de contemplar el sistema operativo Microsoft Windows XP al tratarse de un sistema operativo obsoleto y sin soporte oficial desde Abril de 2014.

USO HABITUAL CON PRIVILEGIOS REDUCIDOS EN ANDROID (DATO REAL)

99,3%
CON PERMISOS REDUCIDOS EN ANDROID 8

98,1%
CON PERMISOS REDUCIDOS EN ANDROID 7

90,4%
CON PERMISOS REDUCIDOS EN ANDROID 6

86,0%
CON PERMISOS REDUCIDOS EN ANDROID 5

80,6%
CON PERMISOS REDUCIDOS EN ANDROID 4

necesario realizar determinadas acciones para obtener permisos 'root' que podrían derivar en la anulación de la garantía del dispositivo. Se observa cómo en las últimas versiones de los sistemas operativos de Microsoft, Windows 8 y Windows 10, prácticamente la totalidad de usuarios cuentan con permisos reducidos (98,9% y 100% respectivamente), mientras que en sistemas más antiguos se experimenta un repunte de usuarios con altos privilegios (algo más de 1 de cada 4 usuarios de Windows Vista).

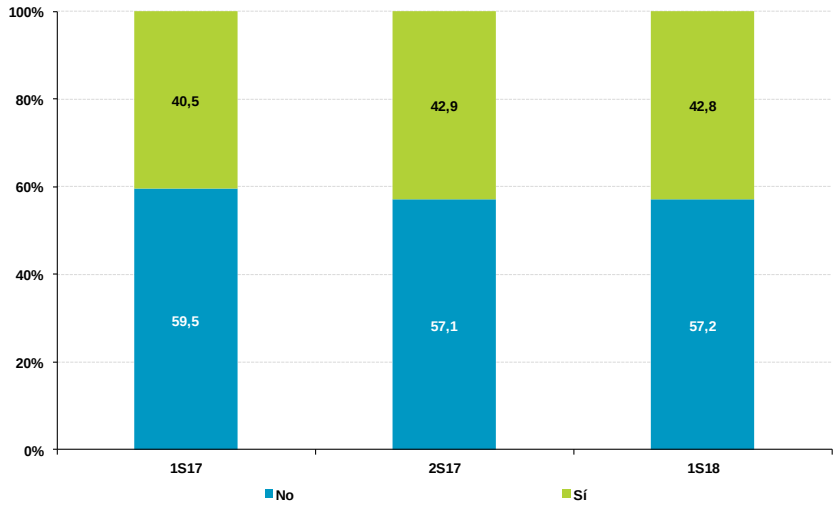
Paralelamente, en los dispositivos Android también se observa la influencia de la versión del dispositivo y su antigüedad en el nivel de privilegios o 'rooteo' del dispositivo. Prácticamente todos los usuarios con dispositivos recientes –aquellos que cuentan con la versión 7 u 8 de Android– lo mantienen sin *'rootear'* (98,1% 99,3% respectivamente). Por otro lado, casi el 20% de los dispositivos con la versión 4 han experimentado el proceso para obtener permisos de 'root'.

Esta clara tendencia a modificar los dispositivos más antiguos responde a dos circunstancias principalmente: en primer lugar, finalización del periodo de garantía del dispositivo, y en segundo el cese del soporte oficial por parte del fabricante. En este escenario el propio usuario se ve impulsado a buscar alternativas para continuar actualizando el sistema operativo Android tanto para poder disfrutar de las novedades presentes en versiones más recientes como para aplicar actualizaciones de seguridad.

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

El comportamiento y los hábitos de seguridad adoptados por los usuarios españoles cuando acceden a Internet aportan claros indicativos de los niveles de precaución tomados para intentar evitar las amenazas y peligros que depara la Red de Redes.

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

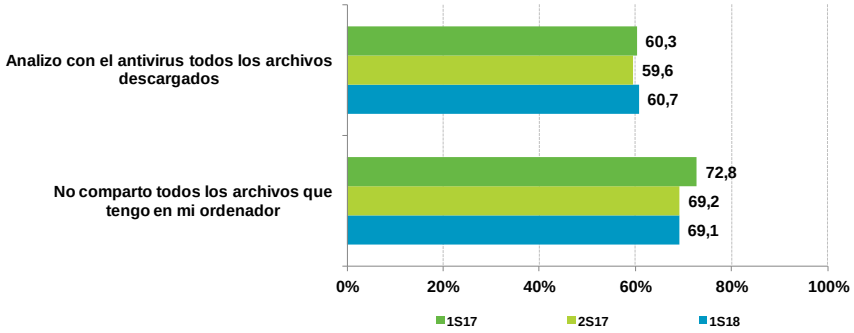


Base: total usuarios
Fuente: Panel hogares, ONTSI

Durante los primeros meses de 2018 los niveles de adopción de conductas de riesgo de manera consciente por parte del usuario se mantiene constante con respecto al semestre anterior: casi un 43% de los internautas manifiestan realizar acciones de riesgo. Dichas conductas de riesgo, aun asumidas de manera consciente y de forma puntual, podrían ser la antesala de la ocurrencia de incidencias de seguridad.

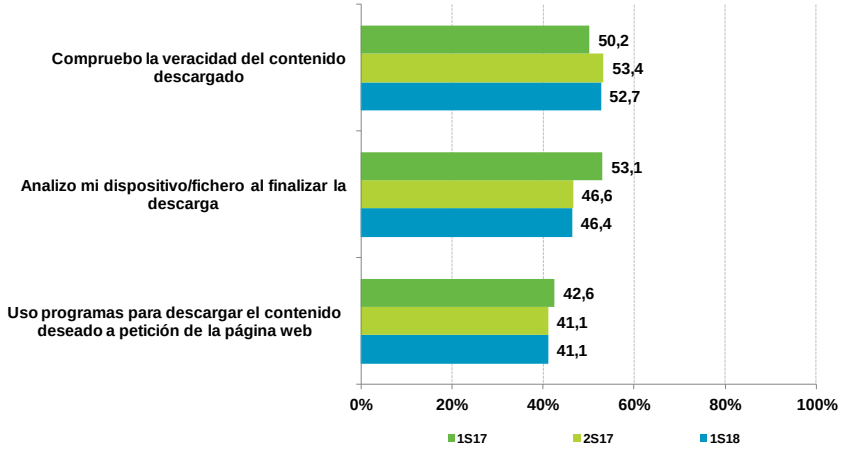
Es necesario analizar los hábitos prudentes relacionados con la navegación, descargas desde Internet e instalación de programas y aplicaciones para determinar si también los usuarios adoptan riesgos en estas acciones.

FIGURA 6. DESCARGAS EN REDES P2P (%)



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

FIGURA 7. DESCARGAS EN INTERNET (%)



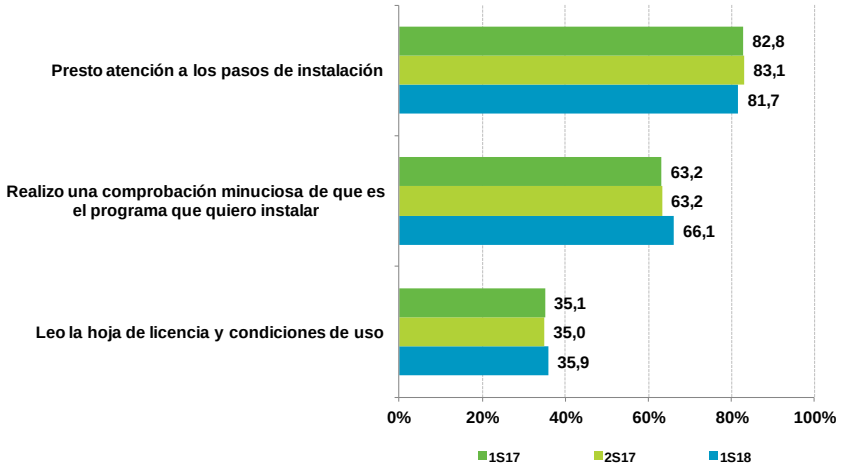
Base: total usuarios
Fuente: Panel hogares, ONTSI

Los ficheros descargados de Internet, tanto por descarga directa como a través de redes P2P, conllevan el potencial riesgo de ocultar *malware* (bajo la forma de algún tipo de fichero, documento, programa, aplicación, contenido gratuito, etc. que resulte de interés para el usuario) destinado a infectar los equipos informáticos y dispositivos móviles de los usuarios. De igual manera existen sitios de descarga que, utilizando como reclamo el ofrecimiento gratuito de contenido de pago o sujeto a derechos, bombardean al usuario con publicidad, *malware* o descargas fraudulentas a través de falsos botones de descarga o solicitando la instalación de alguna falsa aplicación propia para descargar el contenido, incluso se aprovechan de los recursos del ordenador del hogar o dispositivo móvil para minar criptodivisas.

Se observa en las declaraciones de los internautas que existe un 39,3% de usuarios de redes P2P que no analizan con el software antivirus los ficheros descargados, a pesar de que un 90,3% de los ordenadores del hogar –usualmente más utilizado para descargas online que los dispositivos móviles por cuestiones de espacio de almacenamiento, planes de datos, etc.– cuentan con este software de seguridad (**FIGURA 1**).

Cuando se trata de descarga directa, dicho porcentaje aumenta hasta el 53,6% de los usuarios que ponen en riesgo sus equipos al no analizar el contenido descargado. Se podría excusar este comportamiento al pensar que las descargas se realizan desde sitios oficiales, de confianza o repositorios privados; sin embargo, estos también podrían verse comprometidos, por lo que siempre es recomendable el análisis de todos los ficheros descargados desde la Red.

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



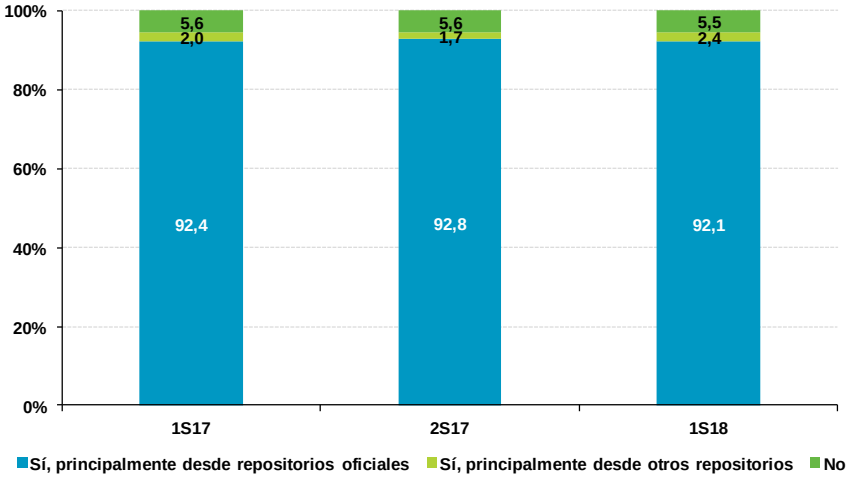
Base: total usuarios
Fuente: Panel hogares, ONTSI

Los hábitos prudentes relacionados con el proceso de instalación de programas en el ordenador del hogar demuestran un aumento (+2,9 p.p.) en la comprobación minuciosa que realiza el usuario para asegurarse de que se trata del programa deseado, y en la lectura de la hoja de licencia y condiciones de uso (hasta el 35,9%) del *software* a instalar.

Por otro lado, el buen hábito de prestar atención a los pasos de instalación se reduce en -1,4 p.p. con respecto al periodo anterior. A pesar de ello se mantiene en un alto porcentaje de usuarios que declaran realizarlo de esta manera: el 81,7%.

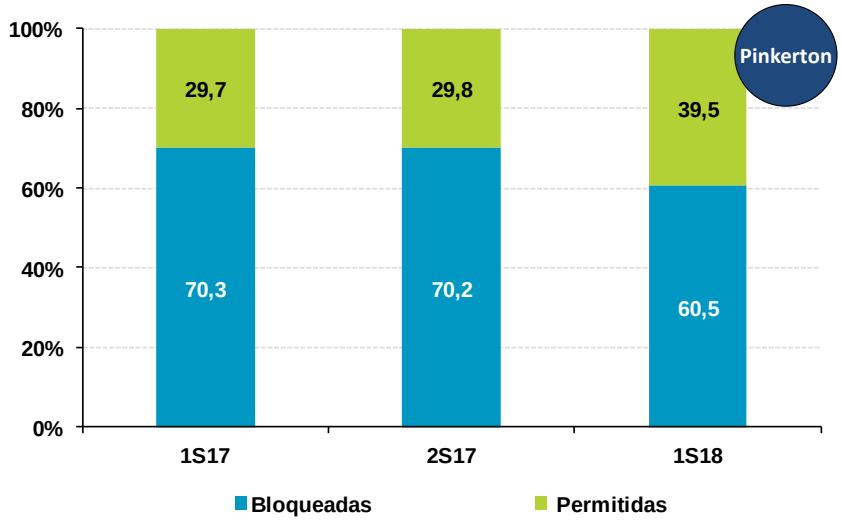
Muchas aplicaciones gratuitas (*freeware* y *shareware,* sobre todo) incluyen la instalación de algún software adicional de sus *sponsors* y solicitan permiso en los pasos de instalación (normalmente viene marcada por defecto su aceptación). Por ello, si un usuario doméstico no presta la suficiente atención puede acabar instalando *adware* o incluso *malware* en su equipo.

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



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

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



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

Según las declaraciones de los usuarios de dispositivos Android el 92,1% 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.

Así el dato real recopilado por Pinkerton revela un incremento de casi 10 p.p. (hasta el 39,5%) de dispositivos Android en los que los usuarios han modificado la configuración por defecto para permitir la instalación de aplicaciones desde fuentes desconocidas.

Llevar a cabo la instalación de aplicaciones móviles procedentes de *markets* alternativos supone un alto riesgo para la seguridad de los dispositivos móviles ya que estos sitios no disponen de medidas de análisis y detección de aplicaciones falsas o maliciosas en sus almacenes, así como tampoco controlan la procedencia de las mismas. Al contrario, el principal interés de estos *markets*

suele ser recopilar y ofrecer el mayor número de *apps* posible sin importar su procedencia, e incluso de manera gratuita como reclamo para atraer a los usuarios.

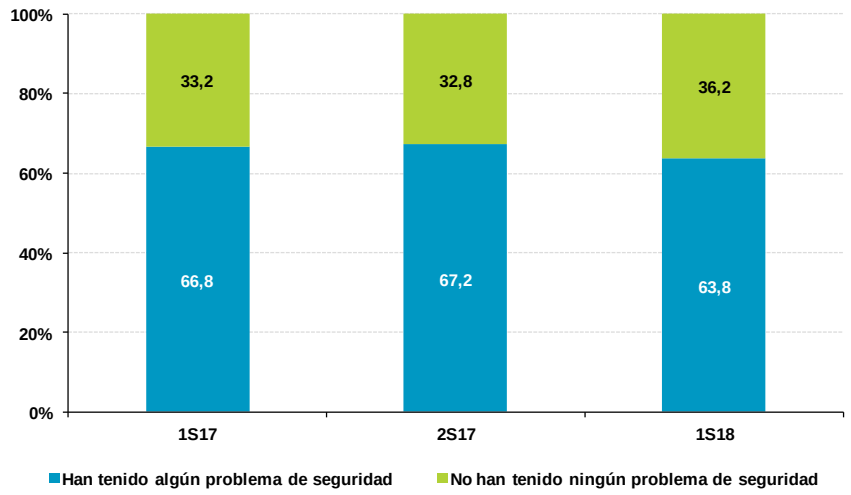
La existencia de *droppers* –*malware* cuya función es descargar otros códigos maliciosos para instalarlos en el sistema infectado– suponen un riesgo adicional para todos aquellos dispositivos en los que la opción de permitir la instalación de aplicaciones desde fuentes desconocidas ha sido activada.

3. Incidentes de seguridad

Aunque los sistemas de seguridad se encuentran en constante evolución en pos de mejorar sus capacidades de protección y prevención de amenazas, estos no son infalibles ni resultan insuperables –dado que las citadas amenazas también se encuentran en constante evolución para contrarrestar a los diferentes sistemas de seguridad y evitar ser detectadas–. También se debe considerar que la efectividad de los sistemas de seguridad dependen en última instancia del usuario: su configuración, actualización, uso adecuado y responsable, etc.

Esto significa que, incluso utilizando las diferentes medidas de seguridad y teniendo buenos hábitos prudentes, el riesgo de que las incidencias de seguridad acontezcan se reducirá, pero siempre estará presente.

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



Base: total usuarios
Fuente: Panel hogares, ONTSI

Se aprecia un decremento (-3,4 p.p.) en la evolución de los problemas de seguridad declarados por los panelistas durante este semestre, regresando a valores similares a los observados en el segundo semestre de 2016.

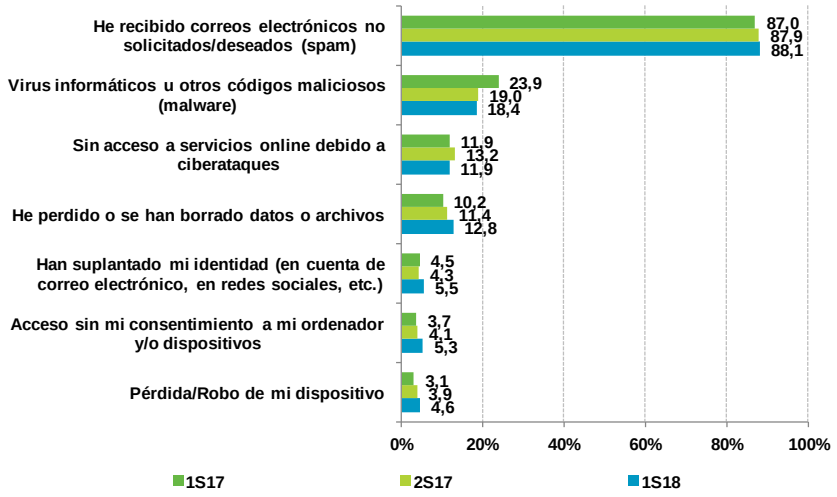
A pesar de que las conductas de riesgo asumidas por los internautas se mantienen constantes, el comportamiento y los hábitos de seguridad adoptados por los usuarios españoles cuando acceden a Internet aportan claros indicativos de los niveles de precaución tomados para intentar evitar las amenazas y peligros que depara la Red de Redes.

El comportamiento y los hábitos de seguridad adoptados por los usuarios españoles cuando acceden a Internet aportan claros indicativos de los niveles de precaución tomados para intentar evitar las amenazas y peligros que depara la Red de Redes.

FIGURA 5

En la siguiente gráfica se desglosan las incidencias de seguridad percibidas por los panelistas. Como viene siendo habitual y es de esperar las campañas de *spam*, con el objetivo de que el usuario las visualice, ocupan un primer lugar (88,1% de las declaraciones) muy diferenciado y destacado del resto de incidencias (casi 70 p.p. con respecto a la siguiente incidencia de seguridad de la clasificación).

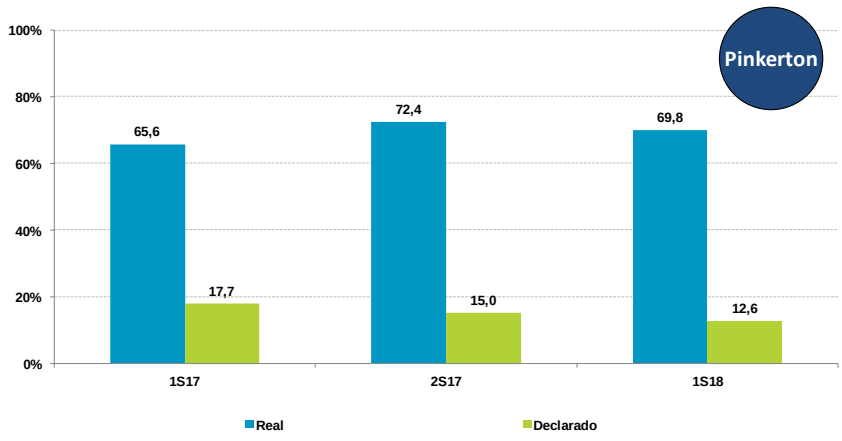
FIGURA 12. EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



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

Continúa siendo sorprendente la evolución de las declaraciones acerca de las incidencias de virus y *malware.* La tendencia a la baja continua en este primer semestre de 2018 y, aunque el decremento es pequeño (-0,6 p.p.), constituye un nuevo mínimo histórico del 18,4%.

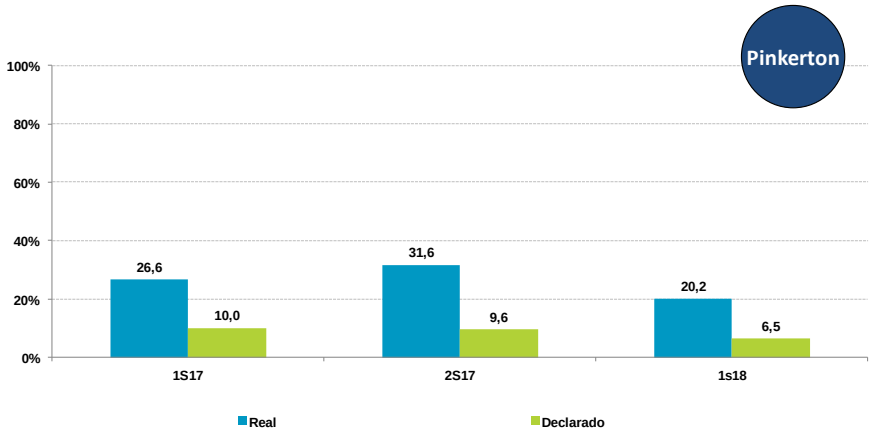
FIGURA 13. EVOLUCIÓN DE LAS INCIDENCIAS DE MALWARE (DECLARADO VS. REAL) EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

A su vez, se observa un continuado crecimiento en las respuestas relativas a la pérdida o borrado de datos y/o archivos. Este hecho podría deberse a fallos en el sistema, descuido del usuario, o incluso estar relacionado con los ataques de *cryptomalware* o *ransomware* que se producen tanto en empresas como en usuarios domésticos y cuyas infecciones siguen representando un grave problema en la actualidad –a pesar de que la tendencia del *malware* parece inclinarse hacia el minado de criptomonedas.

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) ORDENADORES QUE ALOJAN MALWARE

(DATO REAL VS. PERCEPCIÓN)

La realidad hallada en los equipos del hogar y dispositivos Android tras el análisis de Pinkerton muestra unos resultados muy diferentes con respecto a las incidencias relacionadas con virus y *malware*.

Los datos reales ponen de manifiesto una delicada situación en la que casi el 70% de los ordenadores del hogar y el 20,2% de los dispositivos Android sufren de alguna infección de *malware*. Sin embargo, únicamente el 12,6% de los usuarios de PC (-57,2 p.p.) y el 6,5% en Android (-13,7 p.p.) declara haber percibido una incidencia de seguridad de este tipo. Esto supone uno de los puntos más preocupantes del estudio.

20,2%
DE LOS DISPOSITIVOS ANDROID ESCANEADOS CON PINKERTON ALOJAN MALWARE

6,5%
DE LOS USUARIOS PERCIBEN MALWARE EN SUS DISPOSITIVOS ANDROID

69,8%
DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE

En el caso de los dispositivos Android, estas infecciones pueden ser debidas al uso de *markets* no oficiales y a falta de control de las *apps* publicadas en ellos. Las aplicaciones en dichos repositorios pueden –y con frecuencia así es– contener código malicioso cuyo objetivo puede ser desde mostrar anuncios y publicidad no deseada (*adware*) hasta troyanizar el dispositivo para incorporarlo a una *botnet*.

La siguiente pareja de tablas confrontan las declaraciones de cada usuario con el estado real de su propio equipo o dispositivo, buscando profundizar en la realidad de dicha discrepancia en los datos. Esto nos permitirá descartar posibles conclusiones incorrectas derivadas de estas situaciones: como aquellos usuarios que han percibido una incidencia de *malware* en su equipo o dispositivo y han sido capaces de realizar la desinfección antes de que el análisis de Pinkerton tuviese lugar, o aquellos que sospechan de un virus como causante de alguna anomalía cuando no es así.

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

Declararon tener malware en PC	Su PC presentaba malware		
	Sí	No	Total
Sí	10,2	3,2	13,3
No	59,6	27,0	86,7
Total	69,8	30,2	100,0

Base: usuarios de PC
Fuente: Panel hogares, ONTSI

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

Declararon tener malware en Android	Su Android presentaba malware		
	Sí	No	Total
Sí	1,3	5,6	6,9
No	18,9	74,2	93,1
Total	20,2	79,8	100,0

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

Estos nuevos datos manifiestan la existencia de un 10,2% de usuarios en PC y 1,3% en Android que han percibido la existencia de *malware* en sus equipos, pero no han procedido, o bien, no han tenido éxito en su eliminación. Así como un 3,2% de los ordenadores y 5,6% de los dispositivos Android cuyos usuarios presuntamente supieron hacer frente a la incidencia de *malware* y solucionarla de forma que Pinkerton no ha detectado ningún rastro de código malicioso en ellos.

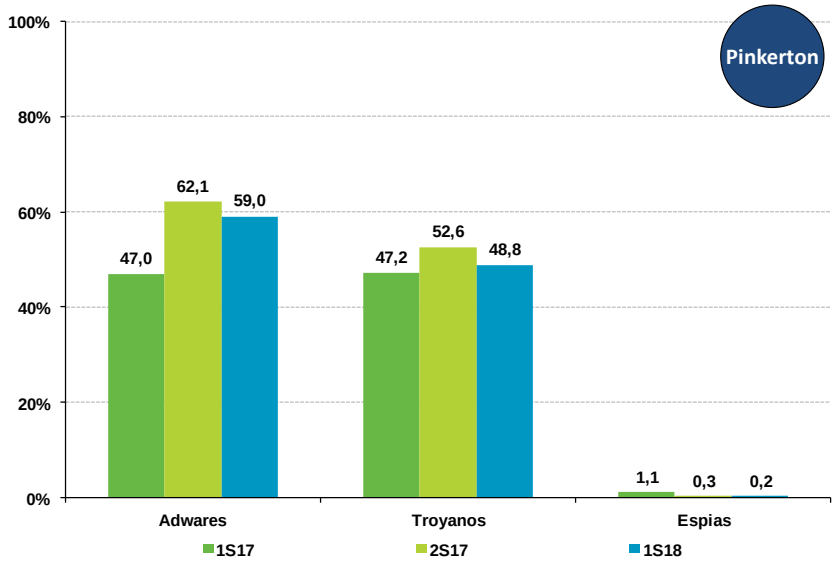
Sin embargo, el dato más destacable es el de aquellos usuarios que declaran no haber sufrido incidencias de seguridad relacionadas con *malware* mientras sus equipos realmente se encuentran comprometidos a causa de la infección de alguna muestra de *malware*. En esta situación se encuentran en el 59,6% de los ordenadores y el 18,9% de los dispositivos Android analizados por Pinkerton.

Esta enorme brecha en el caso de los PCs españoles podría intentar disculparse en base al argumento de que el ordenador del hogar es, habitualmente, utilizado por varios miembros de la unidad familiar, siendo más complejo proteger el equipo frente a, por ejemplo, las acciones de riesgo asumidas por cada uno de ellos y desconocidas para el resto de usuarios del mismo equipo.

En cualquier caso, se trata de una realidad bastante preocupante, no únicamente por las infecciones en sí mismas sino por la falta de percepción del usuario para con este tipo de incidencias de seguridad ya que para poder resolver un problema de infección de un virus informático o *malware* es primordial saber que éste ha acontecido.

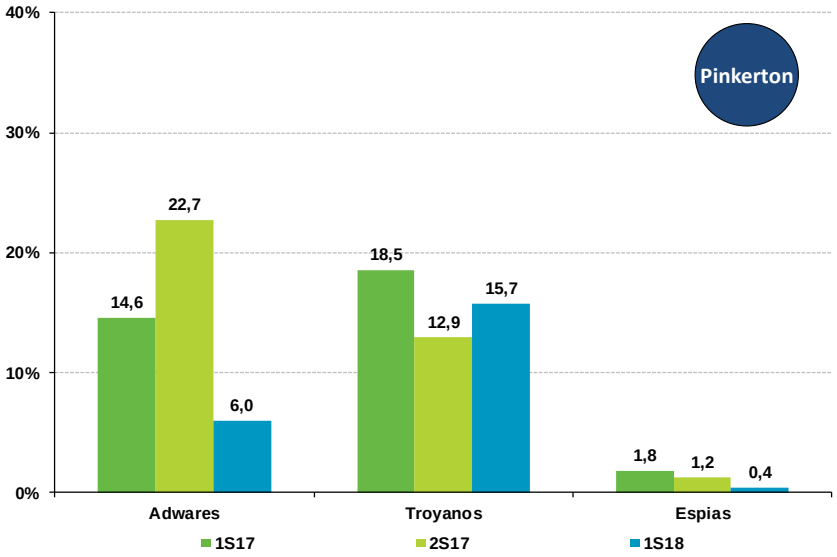
Los ordenadores del hogar se encuentran afectados principalmente por troyanos y *adware*

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



Base: Total ordenadores
Fuente: Panel hogares, ONTSI

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



Base: Total dispositivos Android
Fuente: Panel hogares, ONTSI

Existen dos vertientes diferenciadas en el modelo de financiación por el que se decantan los desarrolladores de código malicioso. Una de ellas consiste en presentarse abiertamente ante el usuario sin ninguna intención de ocultarse: estos son los que persiguen obtener ingresos mediante anuncios mostrados al usuario (*adware publicitario*), la instalación de barras o complementos en el navegador, o incluso solicitar un rescate tras el secuestro del equipo o su contenido (*ransomware*). La segunda tiene un *modus operandi* completamente opuesto: intentar pasar desapercibido tanto ante las soluciones antivirus como para los propios usuarios con el objetivo de mantenerse ocultos en el sistema hasta lograr su objetivo; entre ellos se encuentran *troyanos*, *spyware, o* software que mina criptomonedas sin consentimiento del usuario.

Se puede comprobar mediante el análisis de la tipología del *malware* detectado por Pinkerton que el *adware* publicitario se erige como el principal tipo en los ordenadores del hogar (59%) mientras que en los dispositivos Android son más frecuentes los troyanos (15,7%).

El hecho de que la principal tipología encontrada en los equipos pertenezca al grupo de los que se presentan abiertamente ante el usuario, debería implicar un mayor número de declaraciones al respecto. Sin embargo, se observa que las declaraciones siguen una tendencia a la baja (**FIGURA 13** y **FIGURA 14**) en cada periodo del estudio realizado.

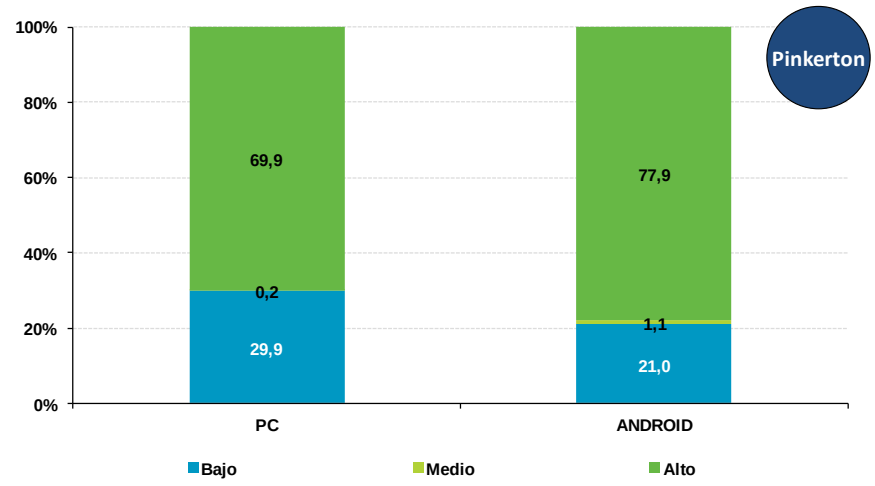
Podría considerarse que el bombardeo constante de anuncios desde la Red recibido por el internauta, resulte una influencia suficiente como para no considerar esos anuncios como el producto de una infección de malware. Además, muchas *apps* para dispositivos Android son gratuitas –o tienen una versión gratuita– y se financian gracias a la inclusión de publicidad, lo cual podría habituar al usuario a la presencia de anuncios e inferir en su percepción.

Por otro lado, resulta evidente, e incluso lógica, la falta de percepción de los usuarios en cuanto a las infecciones debidas a troyanos, espías y otros tipos de malware, cuya actividad se realiza de manera subrepticia, es decir, ocultándose para lograr sus objetivos.

En cualquier caso, la cantidad de muestras de malware encontradas en los equipos analizados durante este último periodo puede considerarse un punto positivo ya que ha existido un decremento en casi todas las tipologías: -3,1 p.p. y -16,7 p.p. en *adware* en ordenadores del hogar y dispositivos Android respectivamente, -3,8 p.p. y +2,8 p.p. en los troyanos en PC y Android respectivamente, y de 0,8 p.p. en *spyware* en los dispositivos Android (esta tipología en los ordenadores permanece constante).

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

Casi el 70% de los ordenadores y el 78% de los dispositivos Android infectados con *malware* se encuentran en un nivel de riesgo alto.



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

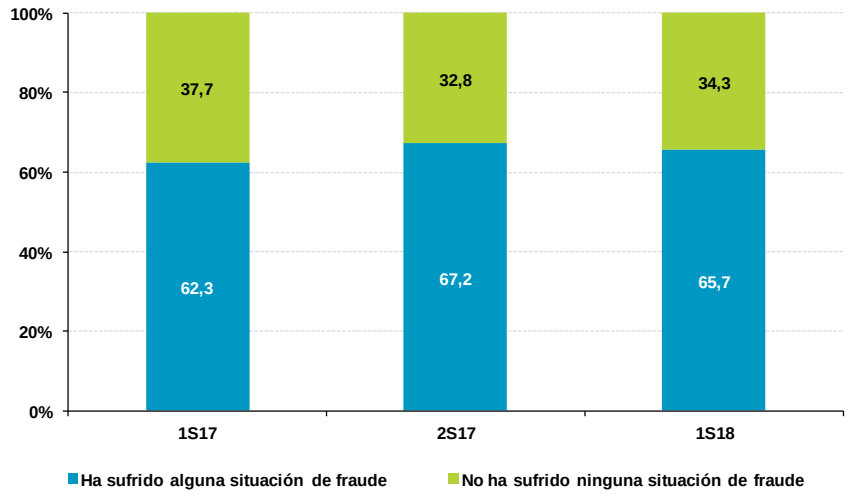
Según el nivel de peligrosidad estimado para las diferentes tipologías de malware detectado en los equipos analizados por Pinkerton, se observa que el nivel de riesgo es alto para el 69,9% de los PCs y para el 77,9% de los dispositivos Android.

Estos nuevos datos, en conjunto con los anteriores acerca de la brecha entre la percepción del usuario y la realidad de sus equipos, y sobre la adopción consciente de conductas de riesgo por parte de casi el 43% de internautas (**FIGURA 5**) ponen de manifiesto un panorama poco halagüeño: se incrementa la probabilidad de que los incidentes de seguridad relacionados con *malware* logren sus objetivos y tengan consecuencias negativas para los usuarios, tales como robo de información, impacto económico, pérdida de datos, etc.

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

A raíz de un incidente de seguridad, el usuario sufre unas determinadas consecuencias. A causa de ello, es habitual que el usuario experimente una reacción con el objetivo de evitar que dichas incidencias –y sobre todo sus consecuencias– puedan volver a repetirse o incluso prevenir otras nuevas incidencias de seguridad. Tales reacciones se pueden traducir en la modificación de los hábitos prudentes utilizados al navegar por Internet y las medidas de seguridad existentes en el equipo.

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

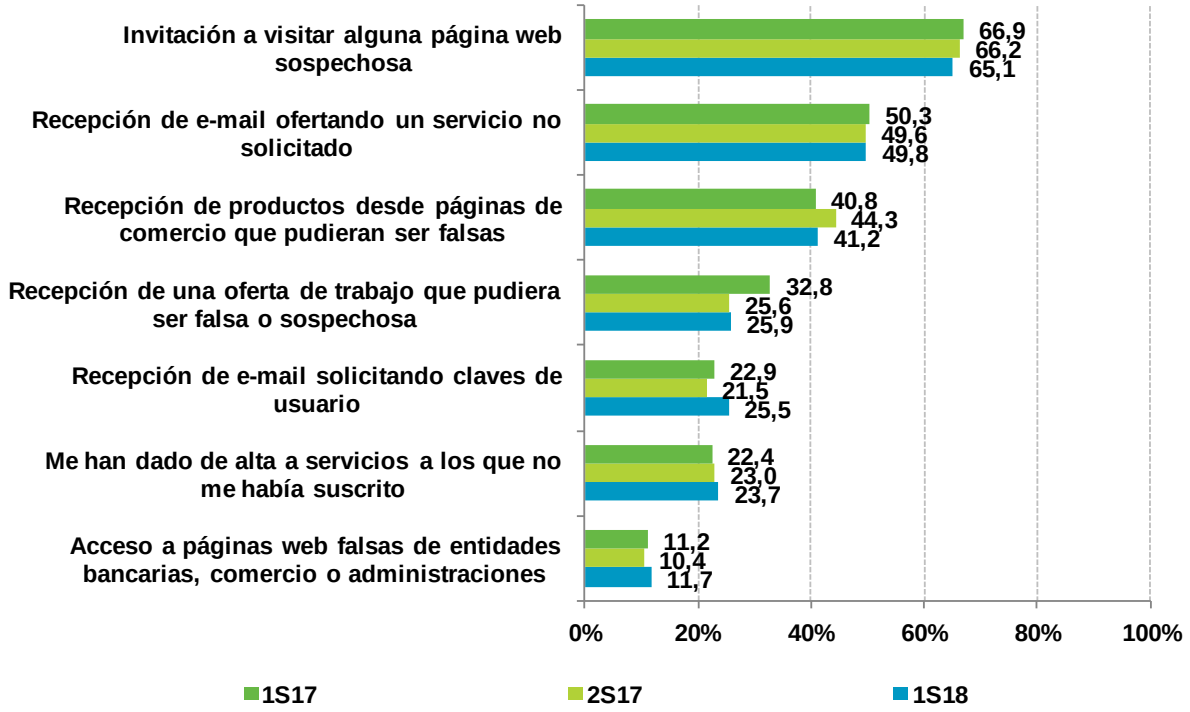


Base: Total usuarios
Fuente: Panel hogares, ONTSI

Prácticamente dos tercios de los internautas (65,7%) declaran haberse visto expuestos a alguna situación de fraude –consumado o no– durante los meses comprendidos entre enero y junio de 2018.

Estos intentos de fraude se presentan de muy diversas formas para intentar engañar al usuario. En la siguiente gráfica se analiza la frecuencia en que cada uno de los tipos son percibidos por el usuario.

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

Aunque experimentan una bajada de 1,1 p.p. las invitaciones a visitar alguna página web sospechosa (65,1%) continúan constituyendo el tipo de manifestación del fraude más frecuentemente acontecido. La recepción de e-mails ofertando servicios no solicitados (49,8%) es la segunda forma más común.

Prácticamente todos estos tipos de fraude online son enviados al usuario a través de correo electrónico no solicitado o *spam* (**FIGURA 12**), o de las redes sociales. Es decir, muchos de los intentos de fraude podrían no llegar al usuario final gracias a las medidas *anti-spam* que los proveedores de este tipo de servicio implementan, e incluso aquellas configuraciones o programas que el usuario tiene en su equipo (**FIGURA 1**).

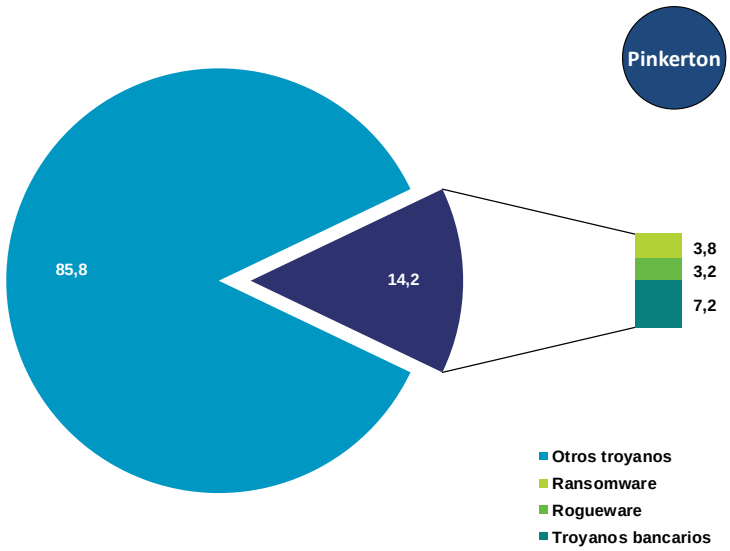
Asimismo, las páginas web falsas de entidades bancarias, comercio electrónico y/o administraciones se verían bloqueadas al contener enlaces de *phishing*, lo que podría explicar que se encuentren en el último lugar de la lista con tan solo el 11,7% de usuarios que han percibido alguna de estas manifestaciones de fraude.

También resulta habitual que los fraudes online se presenten ante el usuario simulando ser inocuas encuestas o concursos que, suplantando la identidad de alguna entidad o marca bien conocida, 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 (49,8%) y publicidad no deseada (nuevamente *spam*), el alta en servicios de *SMS Premium* (23,7%), instalar algún tipo de programa o aplicación no segura –y potencialmente maliciosa–, etc.

Tipología del malware analizado

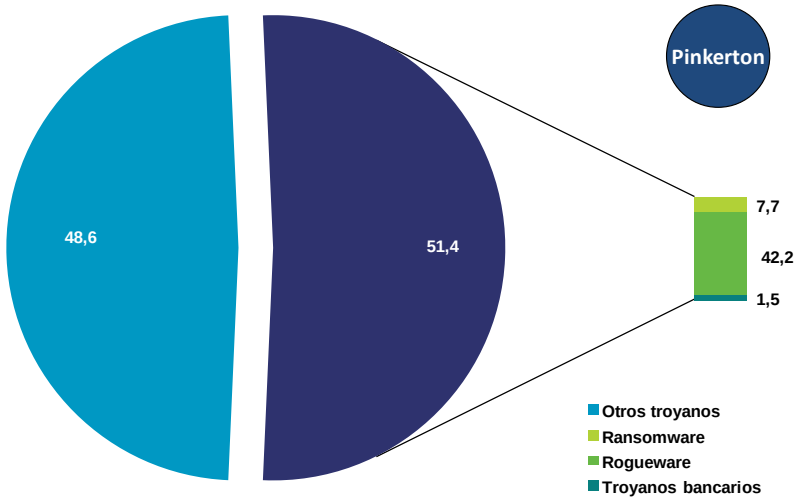
- Troyano bancario: *malware* que roba información confidencial a los clientes de banca y/o plataformas de pago online.
- *Rogueware* o rogue: *malware* que hace creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto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

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



Base: Total troyanos detectados en PC
Fuente: Panel hogares, ONTSI

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

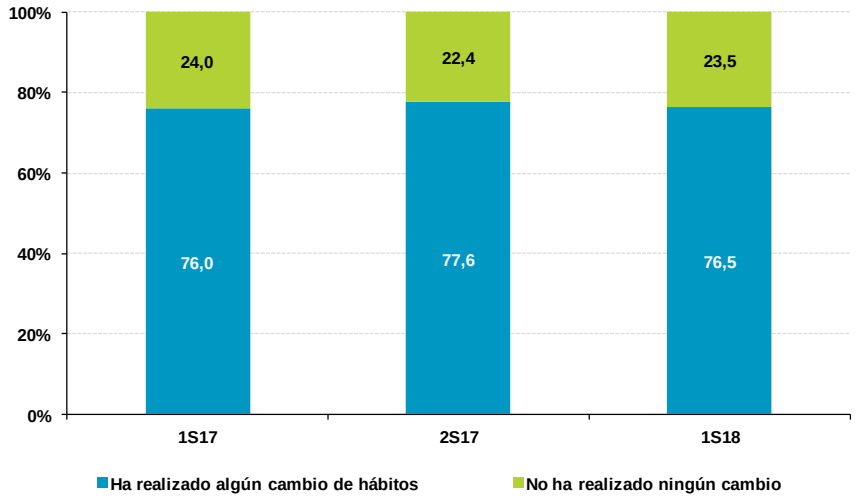


Base: Total troyanos detectados en dispositivos Android
Fuente: Panel hogares, ONTSI

Mientras que en los ordenadores se observan unos niveles bastante similares entre las muestras de troyanos bancarios (7,2%), *ransomware* (3,8%) y *rogueware* (3,2%), en los dispositivos Android se destacan claramente las infecciones provocadas por el *rogueware* (42,2%).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.

Más de tres cuartos de los internautas españoles modifica sus hábitos después de sufrir una incidencia de seguridad.

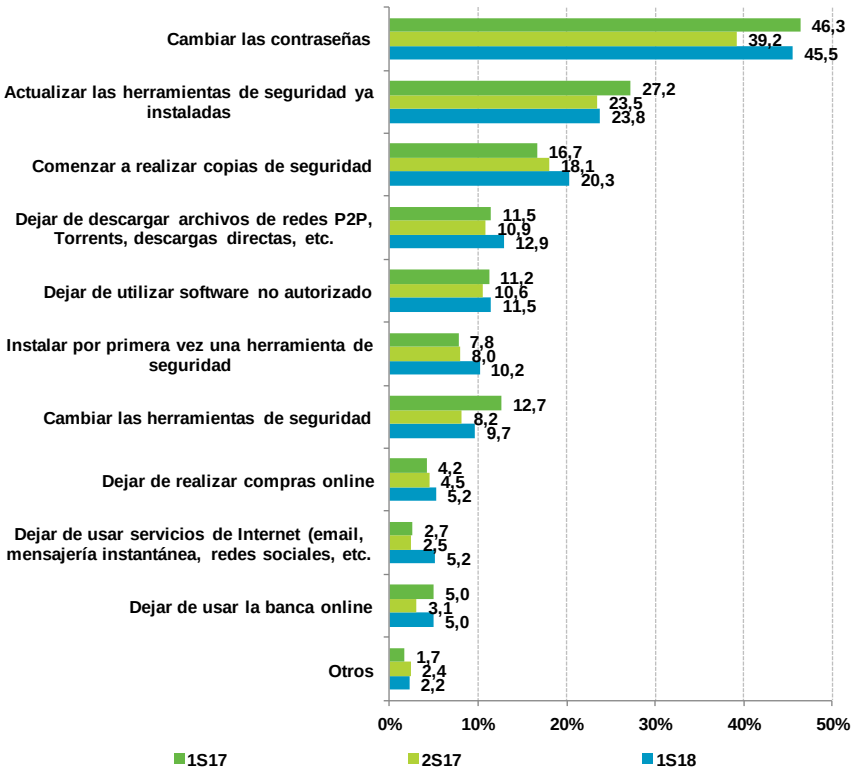
FIGURA 22. EVOLUCIÓN DE LAS REACCIONES ADOPTADAS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%)



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

Durante este primer semestre de 2018 se observa una nueva oscilación en la tendencia del usuario a modificar sus hábitos prudentes y uso de medidas de seguridad tras sufrir un incidente de seguridad. Aquellos que declaran haber realizado algún cambio se reducen en 1,1 p.p. quedando en un valor de 76,5%.

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

Se registra un importante incremento en cuanto a la modificación de contraseñas (+6,3 p.p. con respecto periodo anterior, y regresando a valores similares a los observados un año atrás). Este cambio es beneficioso ya que es recomendable modificar las contraseñas de forma periódica –se haya experimentado algún incidente de seguridad o no– y no utilizar la misma para diferentes servicios.

Otro cambio positivo ha resultado en el hábito de realización de copias de seguridad o *backups* (hasta el 20,3%) tras sufrir un incidente de seguridad.

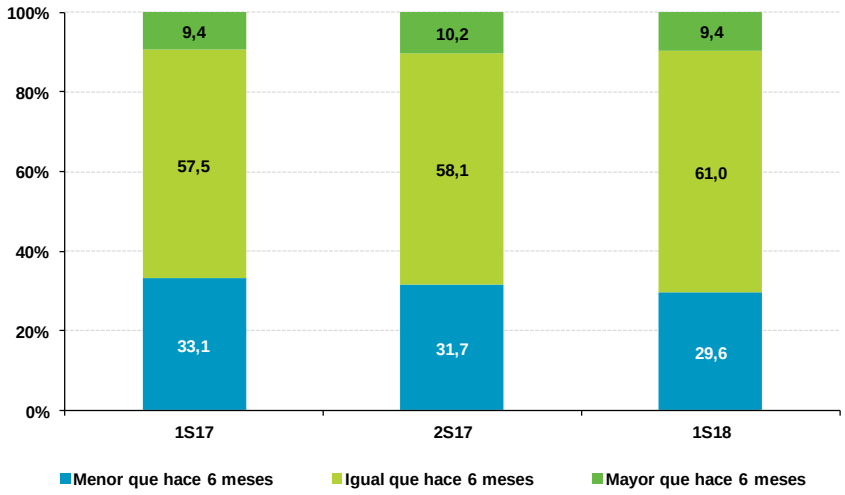
Es recomendable hacer copias de seguridad con regularidad, sobre todo teniendo en cuenta las declaraciones (**FIGURA 12**) de pérdida o borrado datos y archivos (12,8%), pérdida o robo del dispositivo (4,6%), y la amenaza de *ransomware* (**FIGURA 20**) que secuestra el contenido y solicita un rescate– (3,8% de los troyanos presentes en ordenadores y 7,7% en dispositivos móviles Android).

Hoy en día existen multitud de programas, aplicaciones y servicios que se utilizan para el almacenamiento redundante de copias de seguridad que apenas requieren conocimientos técnicos por parte de los usuarios para llevarlas a cabo y constituyen opciones interesantes para evitar las consecuencias anteriormente citadas.

5. Confianza en el ámbito digital en los hogares españoles

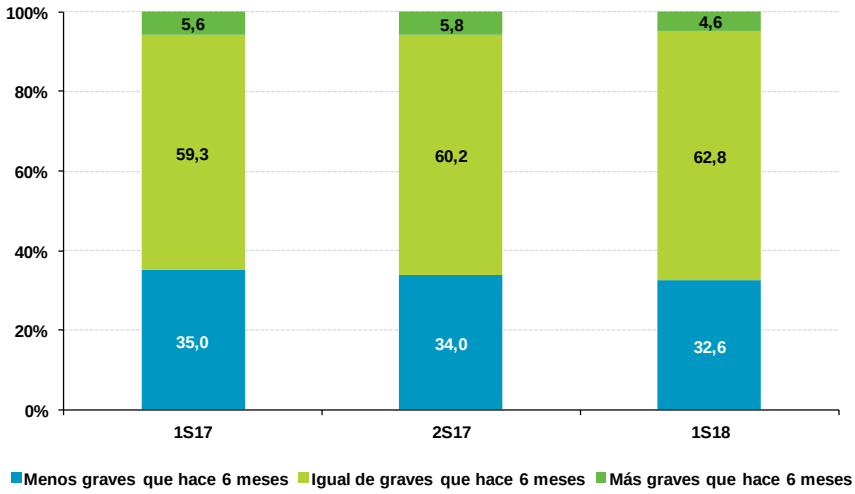
Para finalizar el estudio se realiza un análisis de la opinión y valoración de los usuarios acerca de los riesgos y peligros que se encuentran en Internet, sus consideraciones acerca de la responsabilidad propia en cuanto a la seguridad, y la confianza que tienen en la Red de Redes.

FIGURA 24. EVOLUCIÓN DE LA PERCEPCIÓN DE LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

FIGURA 25. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%)

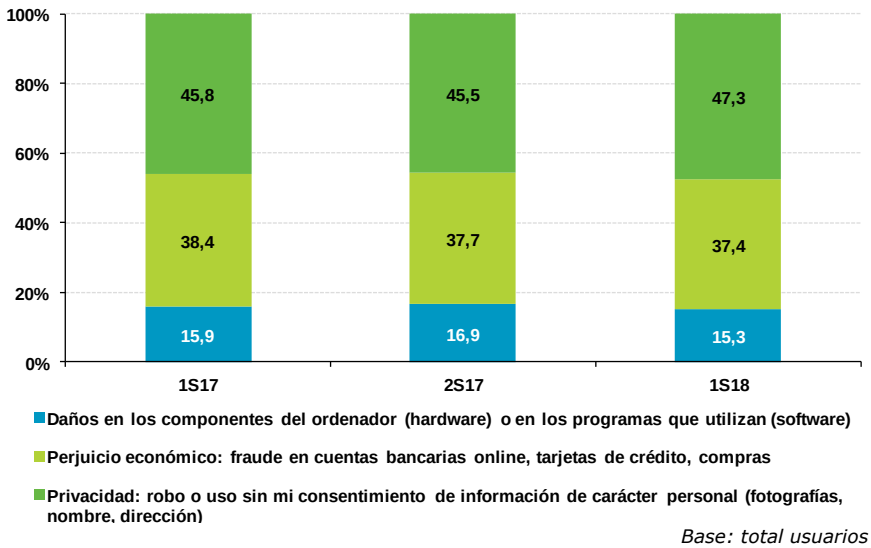


Base: total usuarios
Fuente: Panel hogares, ONTSI

Tres de cada cinco internautas consideran que el número de incidencias de seguridad acontecidas durante los últimos 3 meses y la gravedad de las mismas se ha mantenido en similares proporciones con respecto a las observadas en los meses anteriores (61% y 62,8% respectivamente), y aproximadamente un tercio adicional opina que se han reducido tanto en cantidad (29,6%) como en gravedad (32,6%).

Apenas el 9,4% de los usuarios encuestados considera que el número de incidencias ha aumentado y el 4,6% 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 13** y **FIGURA 14**), el nivel de riesgo en que se encuentran los mismos (**FIGURA 17**), y la falta de percepción del usuario en este tipo de incidencias (**TABLA 1** y **TABLA 2**).

FIGURA 26. EVOLUCIÓN DE LA PERCEPCIÓN DE RIESGOS EN INTERNET (%)



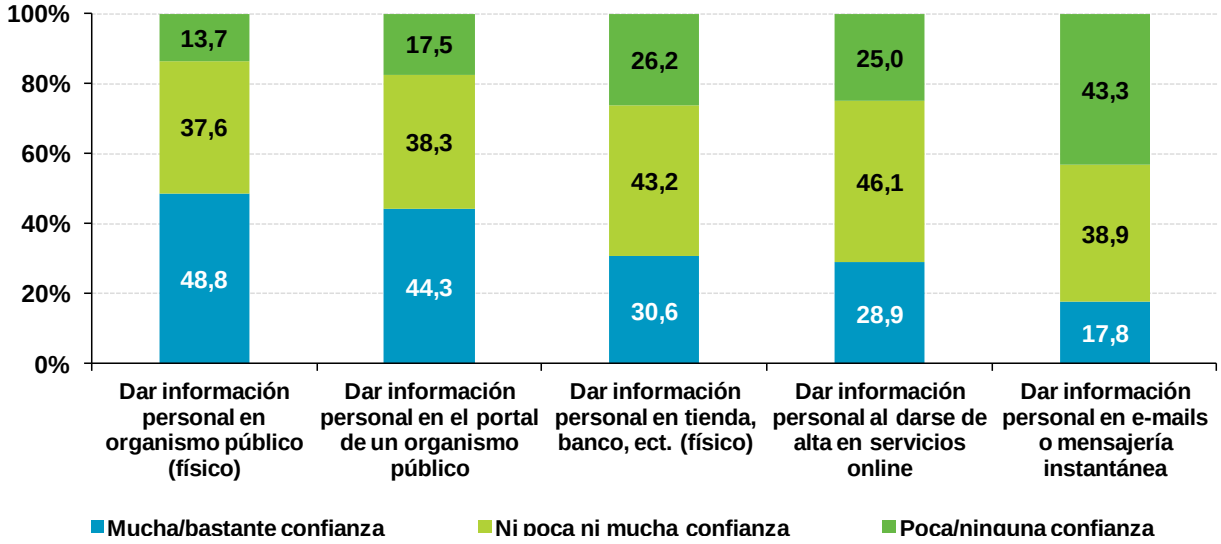
Base: total usuarios
Fuente: Panel hogares, ONTSI

El principal riesgo de navegar por Internet, según la percepción de los usuarios, continúa atentando contra la privacidad. En estos últimos seis meses se aprecia además un aumento de +1,8 p.p. (hasta el 47,3%).

Esta preocupación contrasta un poco con el 35,9% de los usuarios que leen la hoja de licencia y/o condiciones de uso al instalar software en sus equipos y/o registrarse en servicios de Internet (**FIGURA 8**). Estas licencias y condiciones de uso contienen información interesante acerca de la información personal y de uso del programa o servicio que la empresa puede recoger, utilizar e incluso ceder a terceros, y que el usuario acepta en todos sus términos desde el momento de la instalación y/o utilización del software o servicio.

Con objeto de profundizar en este aspecto se analiza a continuación la confianza que le genera al usuario el hecho de facilitar datos personales en diferentes situaciones.

FIGURA 27. NIVEL DE CONFIANZA EN FACILITAR DATOS PERSONALES (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

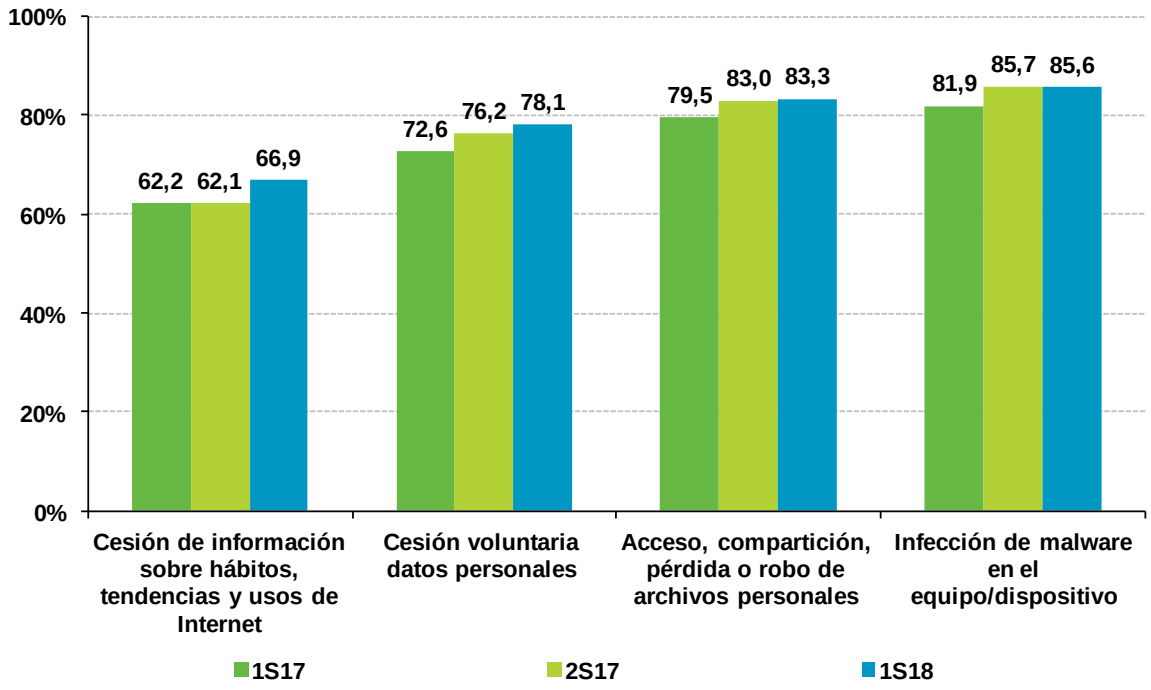
Son numerosas las campañas de *scam*, phishing o cualquier otro tipo de fraude que intente recopilar información personal y/o privada del receptor que son enviadas a través de correo electrónico, y que el ojo poco entrenado puede muchas veces confundir con el *spam* (88,1%, **FIGURA 12**) debido a que, aunque su objetivo no es publicitar nada, son también correos no solicitados o deseados. En cualquier caso, se observa un importante rechazo por parte de un 43,3% de los internautas españoles que desconfían ante solicitudes de información personal o privada a través del correo electrónico o mensajería instantánea.

Sin embargo, este rechazo disminuye hasta un 25% en el caso de que dicha información se solicite durante el registro o alta de un servicio web. Es importante puntualizar que muchos de los *scam* o fraudes comentados anteriormente se pueden presentar en forma de –falsa– promoción de alta en un servicio online con el único objetivo de obtener la información del usuario.

En el otro extremo, destaca el nivel de confianza que el usuario deposita sobre la entrega de documentación a organismos públicos vía telemática (44,3%) o de manera física (48,8%).

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. EVOLUCIÓN DE LA VALORACIÓN DE LOS PELIGROS DE INTERNET (%)



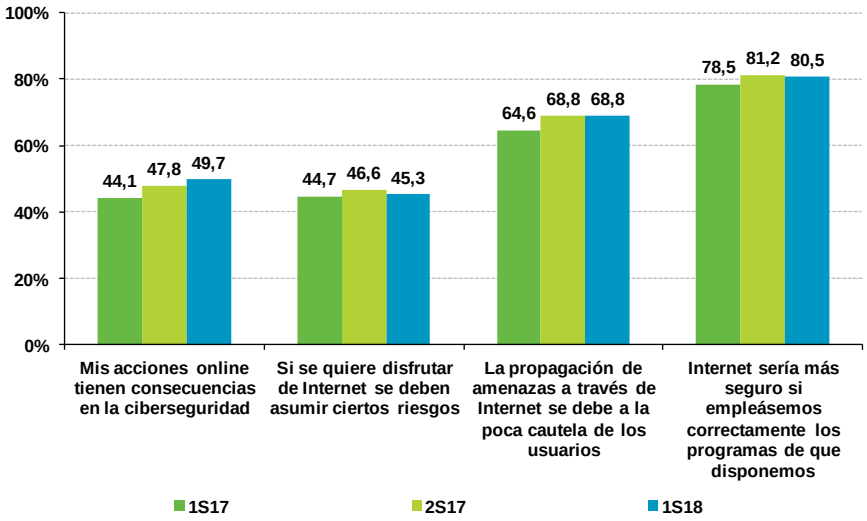
Base: total usuarios
Fuente: Panel hogares, ONTSI

A colación de lo anterior se observa un incremento en la valoración de los peligros de Internet como la cesión voluntaria de datos personales (78,1%) y en la cesión de información sobre hábitos, tendencias y usos de Internet (66,9%).

Igualmente se reafirma la alta preocupación que despiertan tanto el acceso, compartición, pérdida o robo de archivos personales (83,3%) como las infecciones de malware (85,6%).

Los usuarios parecen realmente conscientes de los riesgos que pueden acechar en la red Internet. Sin embargo, parecen existir carencias en el conocimiento de las relaciones causa-efecto en torno a estos peligros y de las herramientas para evitarlos, tal y como se desprende de datos analizados anteriormente tales como el nivel de privacidad en los perfiles de redes sociales, la lectura de los términos y condiciones de uso de software o servicios online, la comprobación de permisos al instalar *apps*, el uso de copias de seguridad de los datos o el cifrado de documentos, entre otros.

FIGURA 29. EVOLUCIÓN DE LA RESPONSABILIDAD EN LA SEGURIDAD DE INTERNET (%)

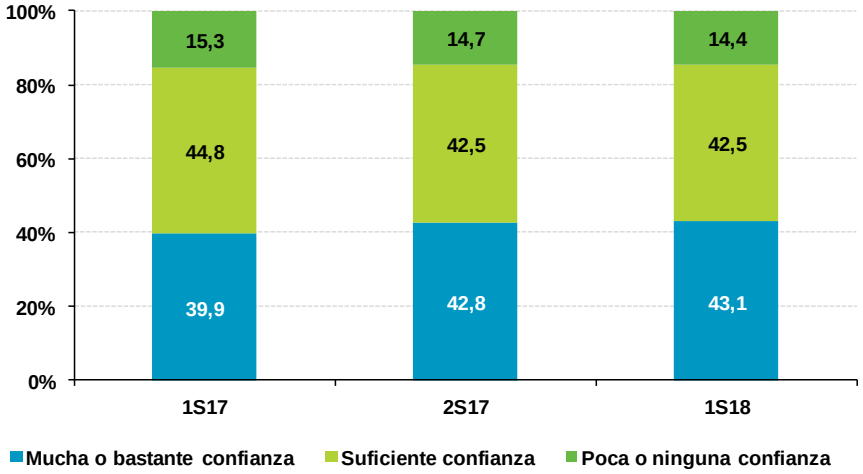


Base: total usuarios
Fuente: Panel hogares, ONTSI

Casi la mitad (49,7%) de los internautas son conscientes de que cada acción llevada a cabo online tiene repercusiones sobre la ciberseguridad y también perciben que la propagación de amenazas se debe a la poca cautela de los propios usuarios (68,8%).

A este respecto, si no se sabe detectar la amenaza, resulta bastante probable que ésta se propague a los círculos más cercanos del usuario, siendo incluso recomendada por este mismo, y así sucesivamente. Como ejemplo se podrían citar las cadenas que se utilizan para propagar fraudes solicitando el envío del mensaje a X contactos con la promesa de obtener un determinado premio, y cuya intencionalidad es la de recopilar datos personales o privados, dar de alta en servicios de pago, etc.

FIGURA 30. EVOLUCIÓN DEL NIVEL DE CONFIANZA EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Aunque levemente, el nivel de confianza en Internet declarado por los internautas españoles continúa su recuperación hasta el 43,1% en este primer semestre de 2018.

Este dato resulta positivo, pero se debe analizar en conjunto a los anteriormente expuestos. 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. Además, el panorama puede tornarse más peligroso debido a la falta de toma de medidas y precauciones –tanto por desconocimiento como por considerarlas innecesarias– para evitar su ocurrencia.

Es importante tener presente que, como dice el refrán, "más vale prevenir que lamentar" y esto también se cumple en el mundo virtual tras la pantalla de los ordenadores y dispositivos móviles conectados a la Red de Redes.

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

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

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