ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

1.1 MEDIDAS DE SEGURIDAD

1.2 HÁBITOS DE COMPORTAMIENTO EN LA NAVEGACIÓN Y USOS DE INTERNET

1.3 INCIDENTES DE SEGURIDAD

1.4 CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

1.5 CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

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

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

El objetivo de este estudio es el análisis del estado de los hogares españoles a través de indicadores de seguridad basados en la percepción de los usuarios sobre la misma, así como el nivel de confianza de éstos respecto a la seguridad y su evolución, haciendo un contraste comparativo con el nivel real de seguridad que mantienen tanto los equipos informáticos como los dispositivos Android.

Se pretende impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe tiene como finalidad, entre otras, informar del comportamiento y utilización segura y privada de las nuevas tecnologías, además de servir como apoyo para solucionar incidencias por parte de los usuarios y 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.

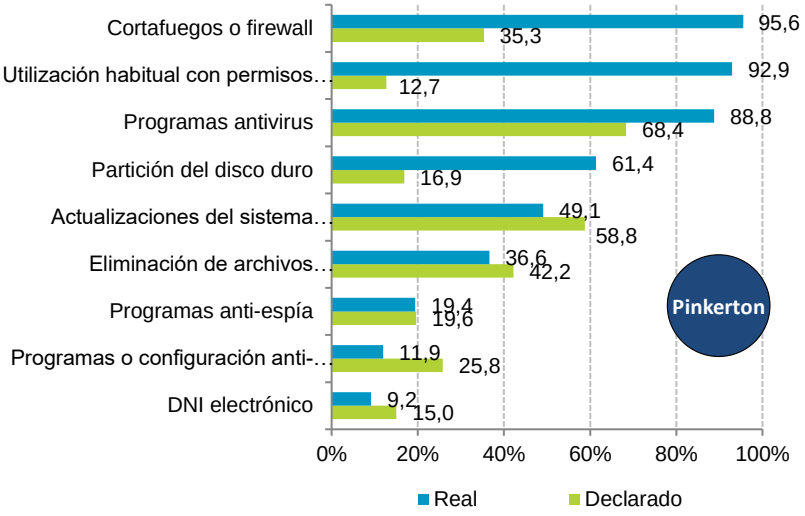
Los datos declarados son obtenidos de las encuestas online realizadas a los hogares que han conformado la muestra del estudio, mientras que para los datos reales se utiliza el software Pinkerton. Este software analiza los sistemas recogiendo datos del sistema operativo, su estado de actualización y las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

1.1 Medidas de seguridad

El uso de medidas de seguridad tanto pasivas como activas son uno de los pilares fundamentales de la seguridad de la información.

Los siguientes resultados respecto a las medidas de seguridad proceden de las declaraciones de los usuarios españoles y de los datos recopilados mediante el análisis real de sus sistemas (ordenadores del hogar y dispositivos móviles) con 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

En el análisis sobre medidas de seguridad en el ordenador del hogar se siguen apreciando notables diferencias entre las declaraciones de los internautas españoles y los datos reales recopilados con Pinkerton, siendo las más significativas las discordancias en cuanto a la utilización habitual con permisos reducidos (+80,2 p.p. de uso real), en el uso de cortafuegos o firewall (+60,3 p.p. de uso real), y en la existencia de particiones en el disco duro (+44,5 p.p. de uso real).

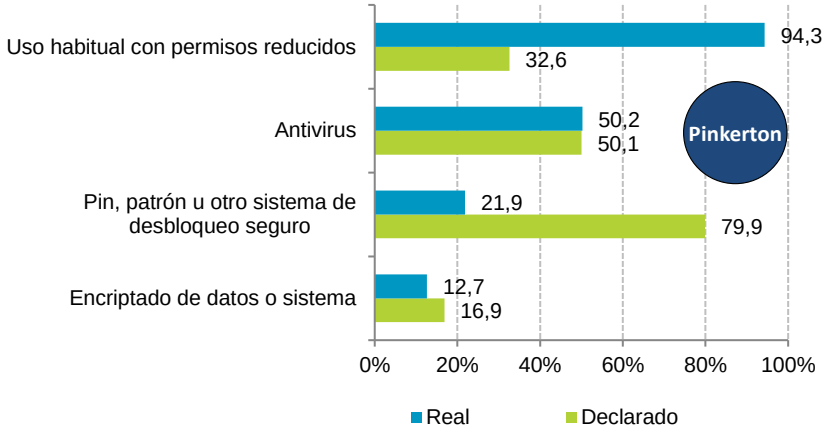
Una posible explicación de estas diferencias puede ser el desconocimiento por parte del usuario de las medidas de seguridad que vienen implementadas por defecto en el sistema operativo de sus equipos. Por ejemplo, en el caso del uso de la utilización habitual con permisos reducidos, los sistemas operativos suelen crear usuarios sin permisos de administrador y solicitan autorización expresa del usuario para realizar determinadas acciones que requieren mayores privilegios.

En el caso del uso de software cortafuegos o firewall, puede deberse a que el usuario emplee una suite de seguridad que tenga incorporada dicha herramienta, pero el usuario no asocia el uso de la suite con el cortafuegos propiamente dicho.

Y respecto a las particiones de disco duro, tanto los sistemas preinstalados como la gran mayoría de los sistemas operativos actuales, crean más de una partición de forma transparente para el usuario que será usada para la recuperación del sistema o para tareas de diagnóstico.

Cabe resaltar no obstante que, a pesar de las discrepancias entre dato declarado y dato real, tanto el uso de cortafuegos (95,6% dato real), como el de programas antivirus (88,8% dato real) y la utilización habitual con permisos reducidos (92,9% dato real) están ampliamente extendidas entre los usuarios. Por el contrario, el uso de programas antiespía (19,4% dato real), de programas antispam (11,9% dato real) y el del DNI electrónico (9,2% dato real) gozan de poca popularidad entre los internautas.

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



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

Respecto a los dispositivos Android, en la Figura 2 se aprecia también una discrepancia notable (+61,7 p.p. uso real) entre el uso habitual con permisos reducidos declarado y el real, lo que puede deberse a que una parte significativa de los usuarios no son conscientes de que no están usando sus terminales como usuario 'root'.

Hay que señalar que para lograr dichos privilegios es necesaria la manipulación del dispositivo de una forma que no suele estar al alcance de todos los usuarios y que podría suponer la anulación inmediata de la garantía por parte del fabricante.

Otra discrepancia entre las respuestas de los usuarios y los datos reales obtenidos mediante Pinkerton reside en el uso del sistema de desbloqueo seguro (-58 p.p. uso real). Siendo este caso especialmente preocupante debido a que gran parte de los usuarios (79,9%) creen que están usando correctamente esta medida de seguridad (que implica una contraseña, clave numérica o PIN, patrón de forma o algún parámetro biométrico) cuando en la realidad (21,9%) resulta que una gran parte emplea un sistema de desbloqueo no seguro tal como la suspensión del terminal que puede reactivarse simplemente pulsando el botón de encendido o un movimiento deslizante en la pantalla.

Sin las debidas medidas de seguridad frente al desbloqueo, en caso de pérdida o robo, el terminal permitiría el libre acceso a la información confidencial contenida en el mismo (e incluso la almacenada en la nube en caso de que las aplicaciones se encontrasen con la sesión ya iniciada), o su uso sin restricciones.

Pese a la importancia del uso de software antivirus para prevenir infecciones de malware, su uso (tanto declarado como real) se mantiene alrededor del 50%. Teniendo en cuenta que los dispositivos móviles cada vez ofrecen más funcionalidades, como el uso de la banca en línea, la administración del correo electrónico, la mensajería instantánea o las compras en tiendas en línea, resulta preocupante que el uso de este tipo de medidas de seguridad continúe manteniendo un nivel tan bajo.

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

100,0%
CON PERMISOS REDUCIDOS EN WINDOWS 10

99,1%
CON PERMISOS REDUCIDOS EN WINDOWS 8

70,6%
CON PERMISOS REDUCIDOS EN WINDOWS 7

USO HABITUAL CON PRIVILEGIOS REDUCIDOS EN ANDROID (DATO REAL)

100,0%
CON PERMISOS REDUCIDOS EN ANDROID 9

99,5%
CON PERMISOS REDUCIDOS EN ANDROID 8

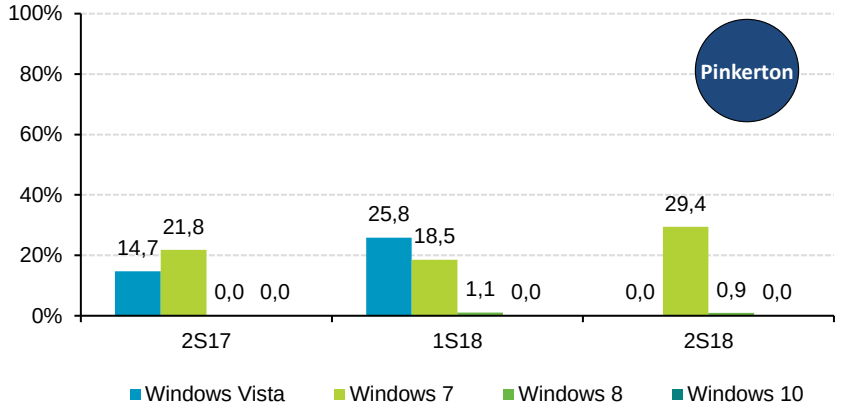
96,7%
CON PERMISOS REDUCIDOS EN ANDROID 7

95,7%
CON PERMISOS REDUCIDOS EN ANDROID 6

88,1%
CON PERMISOS REDUCIDOS EN ANDROID 5

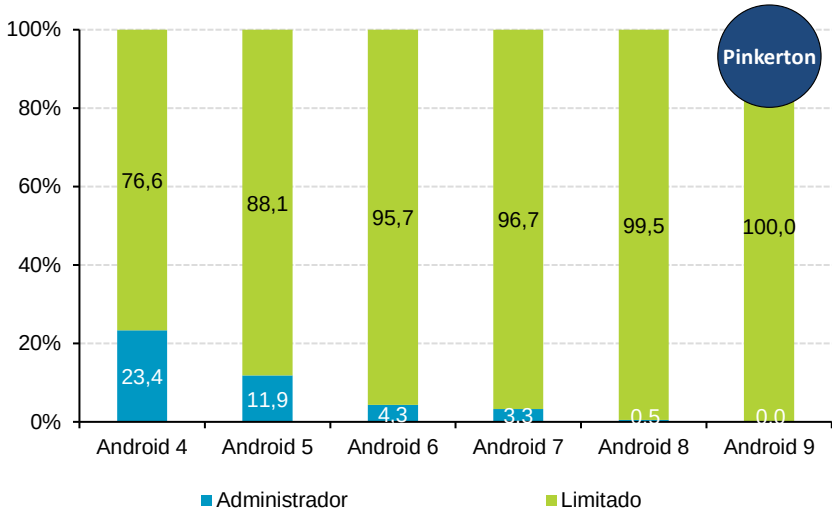
76,6%
CON PERMISOS REDUCIDOS EN ANDROID 4

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

El porcentaje de usuarios que siguen usando cuentas sin restricción de privilegios presenta un descenso significativo en la mayoría de los sistemas operativos, tanto en equipos de sobremesa como en terminales móviles.

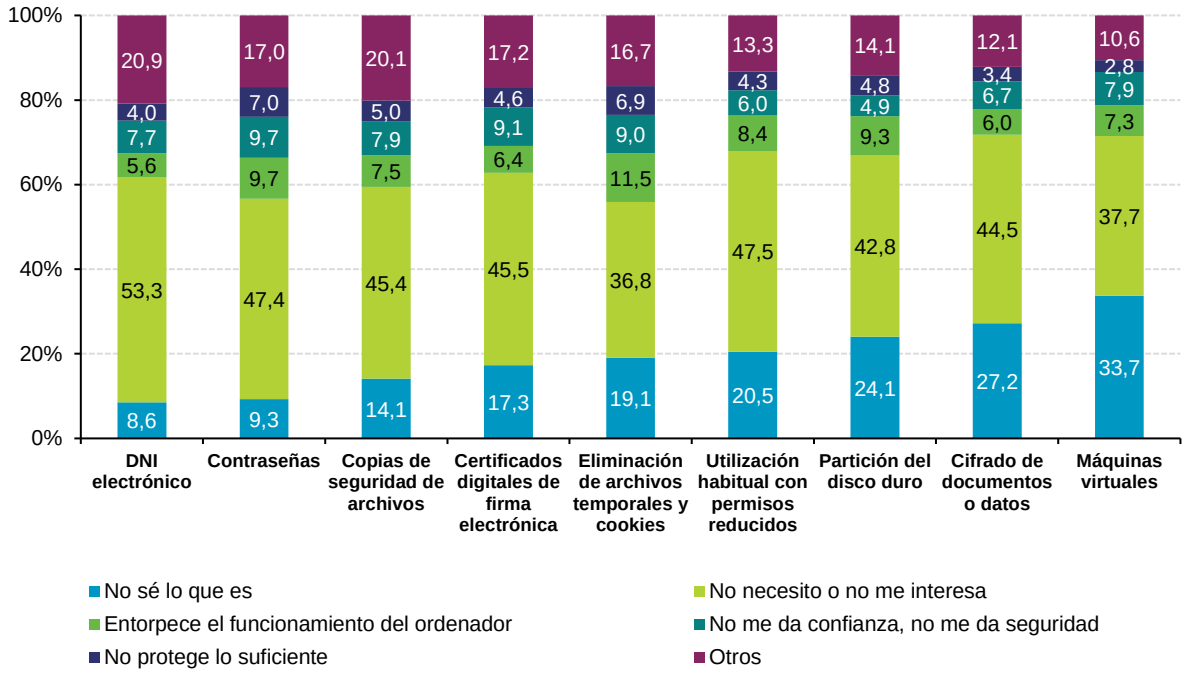
En el caso de los dispositivos Android es necesario destacar que el sistema operativo configura por defecto la cuenta de usuario con privilegios reducidos, siendo necesario dar permiso manualmente a cada nueva aplicación instalada. Para cambiarlo, es necesario manipular el terminal expresamente para obtener permisos 'root' que podría derivar en la anulación de la garantía del dispositivo. Por otro lado, los equipos de sobremesa suelen presentar una cuenta de administrador independiente para la instalación de actualizaciones e instalación de nuevo software crítico.

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

En ambos dispositivos, ordenador y móvil, se observa que el uso de cuentas con privilegios de administrador es más común en versiones antiguas. En el caso de los ordenadores, Windows 7 presenta un 29,4% frente a cerca del 0% del resto; y en el caso de Android, son también las versiones más antiguas las que cuentan con un mayor porcentaje de terminales 'rooteados': Android 4 con un 23,4% y Android 5 con un 11,9%, mientras que las versiones más actuales no superan el 5%.

La tendencia a manipular los terminales antiguos puede deberse a la finalización del periodo de garantía del dispositivo y al cese del soporte oficial por parte del fabricante, por lo que recae en el propio usuario la búsqueda de alternativas para poder seguir utilizando el terminal con un sistema operativo actualizado o poder instalar aplicaciones más modernas.

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



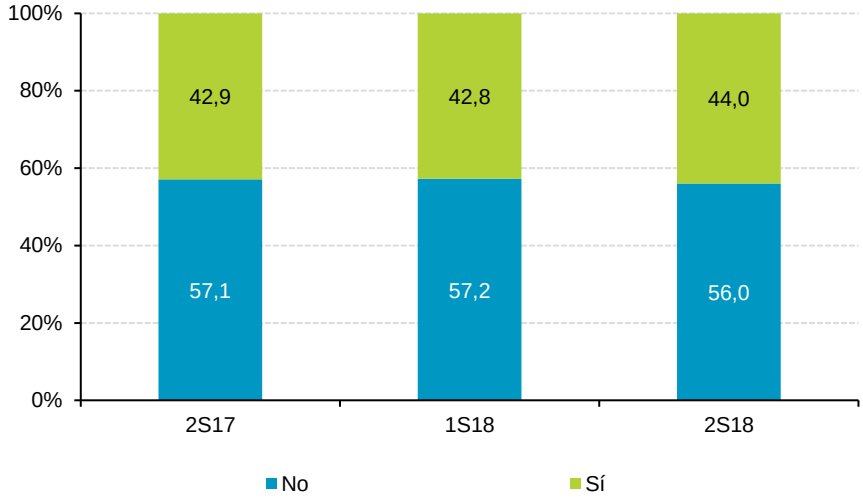
Base: usuarios que no utilizan alguna de las medidas de seguridad
Fuente: Panel hogares, ONTSI

Los principales motivos aportados por los internautas para no emplear las medidas de seguridad recomendadas son su consideración como innecesarias y el desconocimiento de la medida en cuestión. Las medidas más desconocidas son el uso de máquinas virtuales (33,7%) y el cifrado de documentos o datos (27,2%); mientras que las medidas más menospreciadas son el DNI electrónico (53,3%) y el uso de contraseñas seguras (47,4%).

1.2 Hábitos de comportamiento en la navegación y usos de Internet

En la Figura 6 puede apreciarse que el número de usuarios que admite tener conductas de riesgo de forma consciente ha aumentado ligeramente (1,2 p.p.), por lo que el porcentaje total de usuarios asciende hasta el 44% durante este semestre.

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



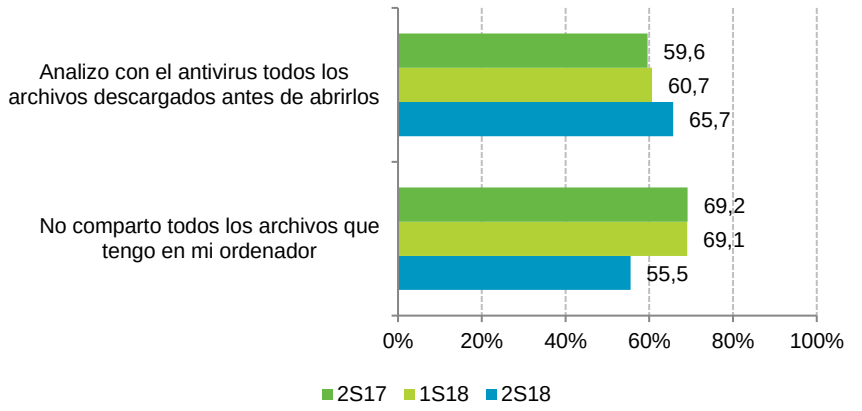
Base: total usuarios
Fuente: Panel hogares, ONTSI

El aumento del número de usuarios que adopta conscientemente conductas de riesgo durante el último semestre, junto con los resultados observados sobre medidas de seguridad empleadas y el conocimiento sobre las mismas declarado, resulta bastante preocupante debido a que –potencialmente- se están exponiendo de forma voluntaria a incidentes sin contar con la protección de las medidas de seguridad adecuadas.

A continuación se analizan los hábitos de seguridad mínimos que se recomiendan para la navegación, las descargas desde Internet y la instalación de programas y aplicaciones para identificar los riesgos que suelen adoptar los usuarios.

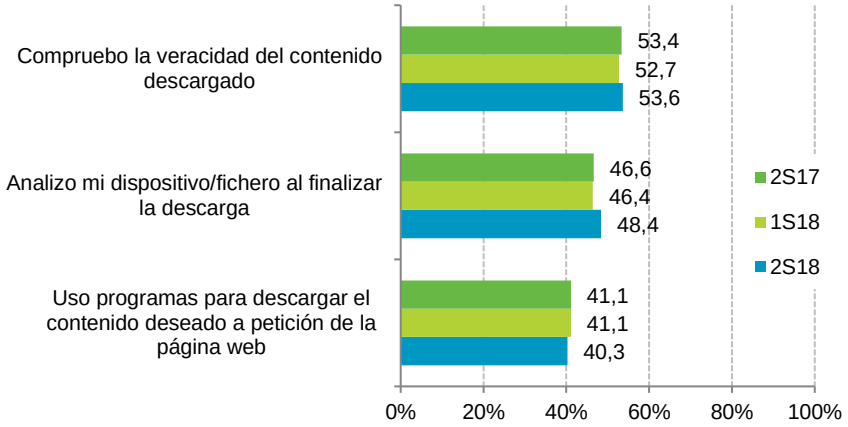
Durante el último semestre, el uso de antivirus en los archivos descargados antes de abrirlos presenta un aumento de 5 p.p. alcanzando el 65,7%, mientras que la medida de restricción de carpetas compartidas ha disminuido 13,6 puntos porcentuales.

FIGURA 7. DESCARGAS EN REDES P2P (%)



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

FIGURA 8. DESCARGAS EN INTERNET (%)

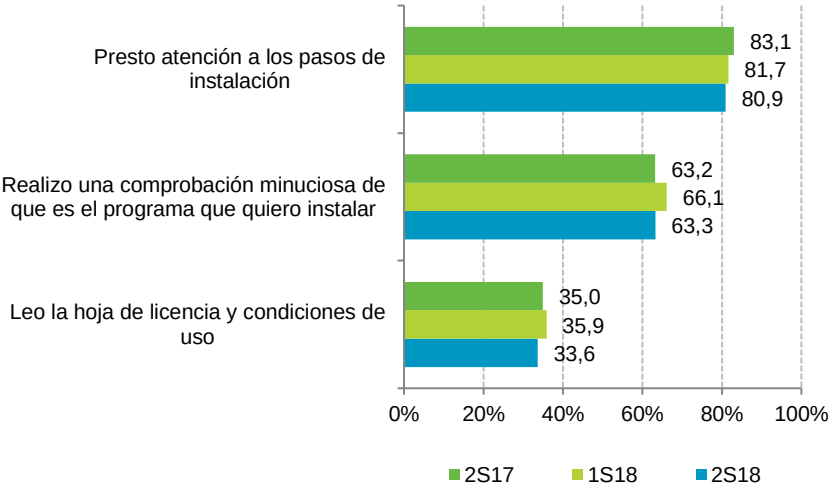


Base: total usuarios
Fuente: Panel hogares, ONTSI

No hay que olvidar que los ficheros descargados de Internet, tanto por descarga directa como a través de redes P2P, no ofrecen ninguna garantía a priori sobre su contenido real (alta probabilidad de tratarse de archivos de mala calidad o incluso con otro tipo de contenido distinto del esperado), e incluso conllevan el riesgo potencial de ocultar malware destinado a infectar los equipos informáticos y dispositivos móviles de los usuarios.

Por otro lado, los sitios de descarga o visualización de contenidos en directo (streaming) emplean como reclamo la oferta gratuita de contenido sujeto a derechos de autor atractivos para el público con el objeto de exponerlo a publicidad no deseada, o de engañarlo para que se descargue algún tipo de malware mediante diversas técnicas como el uso de botones falsos de descarga, suplantación de archivos, aplicaciones falsas de descarga o generación de claves de producto, siendo la tendencia más actual la instalación de software específico de minado de criptomonedas, como el caso de Coinhive.

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



Base: total usuarios
Fuente: Panel hogares, ONTSI

Respecto a las descargas de Internet, no se aprecian grandes cambios en las conductas de prevención de los usuarios, aunque merece la pena reseñar un ligero aumento de 2 p.p. en el análisis de los archivos tras su descarga por parte del software antivirus.

Sin embargo, este semestre se aprecia otro pequeño paso atrás en cuanto a los hábitos de seguridad tomados en la instalación de programas en el ordenador del hogar. Los usuarios parecen seguir una tendencia al prestar cada vez menos atención a los pasos de la instalación (-2,2 p.p. con respecto al año anterior).

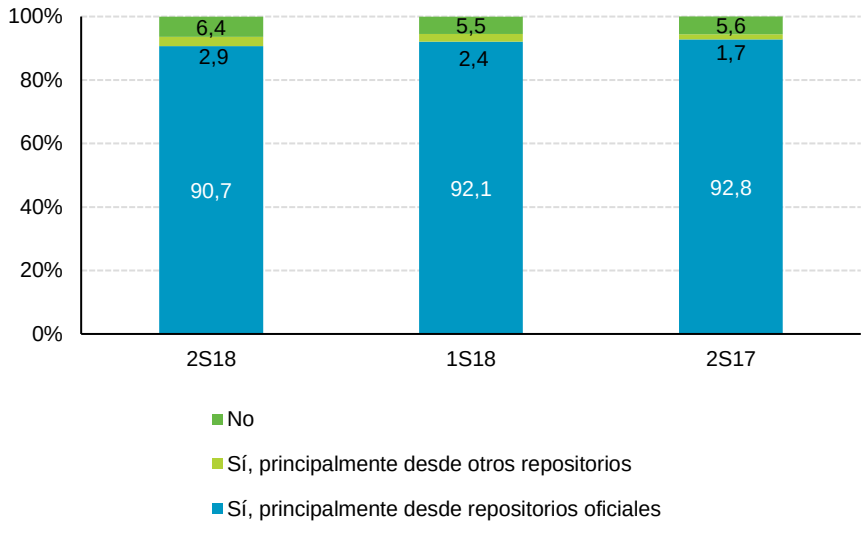
La costumbre de comprobar minuciosamente que el programa que se va a instalar es el deseado, que mostró un aumento de casi 3 p.p. durante el primer semestre de 2018, regresa a los valores identificados durante el segundo semestre de 2017.

Por otra parte, el hábito de leer la hoja de licencia y condiciones de uso ha experimentado un receso de 2,3 p.p., descendiendo hasta el 33,6% y situándose en valores por debajo de los mostrados a finales del año pasado.

Es significativo este bajo porcentaje de usuarios que tiene la costumbre de verificar la hoja de licencia y las condiciones de uso, de modo que normalmente desconocen las condiciones que aceptan al instalar nuevos programas.

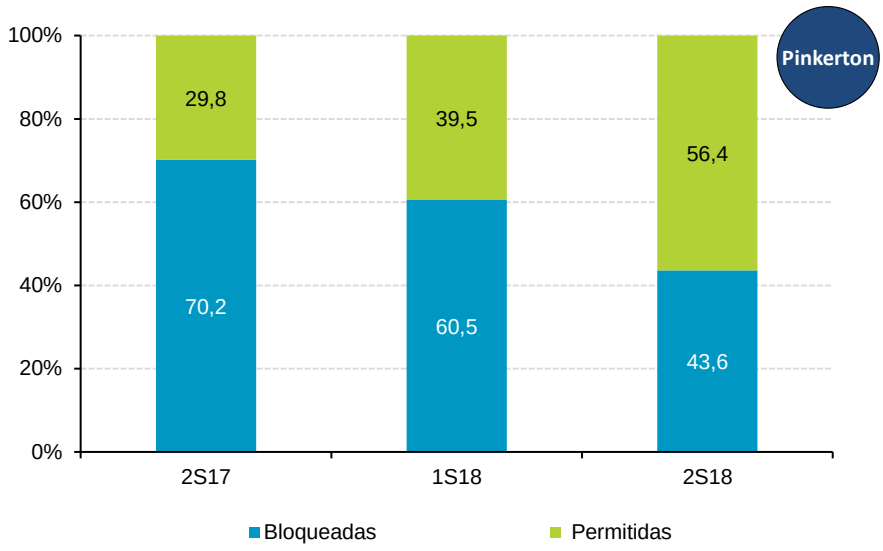
Las aplicaciones freeware y shareware normalmente solicitan permiso al usuario para instalar software de terceros que patrocinan sus servicios, y dado que dos tercios de los usuarios no leen las condiciones de uso, terminan instalando también este *software no deseado*.

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



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

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



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

La mayoría de usuarios de dispositivos Android (90,7%) afirma que recurre principalmente a repositorios oficiales para la instalación de aplicaciones, aunque más de la mitad (56,4%) de los dispositivos analizados tiene activada la opción para permitir la instalación de *apps* desde fuentes desconocidas, opción que requiere ser activada expresamente por el usuario.

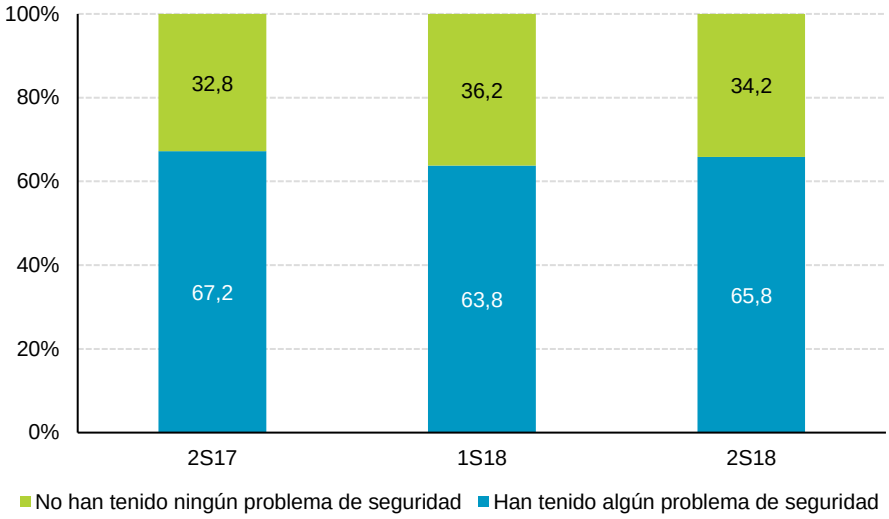
Además, se observa una tendencia general de incremento de usuarios que recurren a los repositorios no oficiales. El número de usuarios que recurren principalmente a este tipo de repositorios ha aumentado en 0,5 p.p., mientras que aquellos que han desbloqueado su uso presenta un aumento de 16,9 p.p.

El uso de los repositorios no oficiales para la instalación de aplicaciones móviles supone un riesgo elevado para la seguridad debido a que no disponen de las medidas de análisis y detección de malware o aplicaciones falsas, ni controlan la procedencia de las mismas, de modo que el reclamo que supone la posibilidad de instalarse aplicaciones de forma gratuita es aprovechado por los atacantes para conseguir que el usuario final se descargue todo tipo de malware, como por ejemplo, los droppers, que se encargan de descargar código malicioso adicional en el terminal infectado.

1.3 Incidentes de seguridad

La configuración, actualización y uso adecuado y responsable de los equipos y el software utilizado evitarán numerosos incidentes de seguridad, pero desafortunadamente no podrán evitar la totalidad de los mismos. Esto es debido a que las amenazas se encuentran en continua evolución con el fin de saltarse los actuales sistemas de seguridad. En este apartado se analizan los incidentes de seguridad sufridos por los usuarios en el período comprendido entre julio y diciembre de 2018.

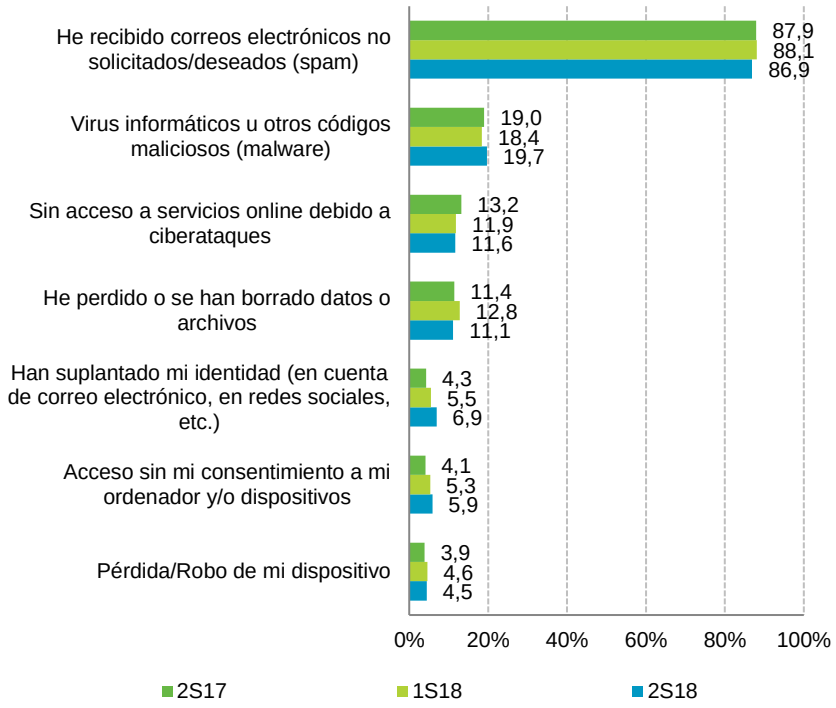
FIGURA 12. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Como puede observarse en la Figura 12, el volumen de usuarios que reporta haber tenido algún problema de seguridad ha subido 2 p.p. tras la caída observada durante el semestre anterior. Esta situación puede explicarse fácilmente con la relajación observada en los hábitos de seguridad y el incremento en la confianza de los usuarios, respaldada por la mayor asunción de riesgos en el uso de la Red.

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



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

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

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

El mayor número de incidentes de seguridad reportados se corresponde principalmente con la recepción de correo electrónico no deseado (spam), que, no obstante, muestra un decremento de 1.2 p.p. Sin embargo, el aumento del número total de incidentes observado durante este semestre se debe al malware (+1,3 p.p.), la suplantación de identidad en redes sociales y correo electrónico (+1,4 p.p.) y al acceso sin consentimiento a los dispositivos (+0,6 p.p.).

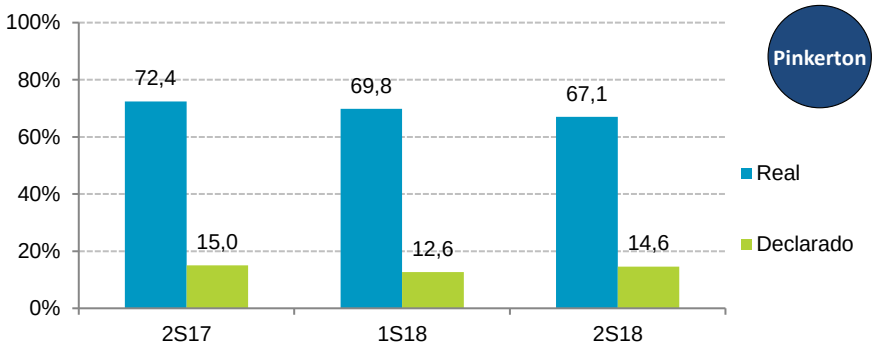
Por otro lado, las pérdidas de acceso a servicios online debido a ciberataques (-0,3 p.p.) y la pérdida de datos (-1,7 p.p.) o dispositivos (-0,1 p.p.) muestran un ligero descenso en el número de incidencias, como puede apreciarse en la Figura 13. Esta evolución negativa podría deberse a una mayor concienciación sobre la introducción de datos personales en páginas webs sospechosas y a la tendencia de los ciberdelincuentes detectada desde finales de año a cambiar el uso del ransomware por el criptominado.

ORDENADORES QUE ALOJAN MALWARE (DATO REAL VS. PERCEPCIÓN)

67,1%
DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE

14,8%
DE LOS USUARIOS PERCIBEN MALWARE EN SUS ORDENADORES PERSONALES

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



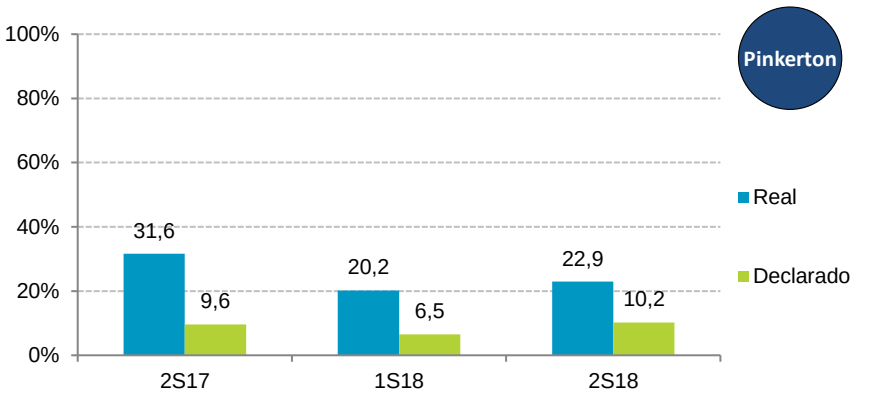
Base: usuarios de PC
Fuente: Panel hogares, ONTSI

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

22,9%
DE LOS DISPOSITIVOS ANDROID ESCANEADOS CON PINKERTON ALOJAN MALWARE

10,2%
DE LOS USUARIOS PERCIBEN MALWARE EN SUS DISPOSITIVOS ANDROID

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



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

Respecto a la evolución de incidencias de malware detectado en equipos del hogar, como puede comprobarse en la Figura 14, continúa observándose un descenso, cayendo 2,7 p.p. durante el pasado semestre el porcentaje de equipos en los que se detectó algún tipo de *software* malicioso. Asimismo, pese a que el volumen de equipos en los que se detectó malware y el porcentaje de usuarios que declaró haber detectado alguna infección siguen

siendo muy dispares (52,5 p.p.), se aprecia un ligero aumento en el número de usuarios que es consciente de este tipo de infecciones (+2 p.p.).

En el caso de los dispositivos Android, aunque el número de dispositivos infectados es significativamente inferior respecto al de equipos del hogar, se aprecia un ligero aumento (+2,7 p.p.) respecto al semestre anterior, pero sin alcanzar aún los valores del segundo semestre de 2017.

Como se observó previamente (Figura 11), los usuarios españoles están recurriendo cada vez con mayor frecuencia a *markets* no oficiales, en los que el control de calidad y seguridad no está garantizado y las aplicaciones publicadas en los mismos pueden contener código malicioso pensado para mostrar publicidad no deseada (*adware*), introducir troyanos en el dispositivo o descargar cualquier *dropper* para instalar aplicaciones no deseadas sin el conocimiento del usuario.

En las tablas siguientes se comparan las respuestas de los usuarios con los datos reales obtenidos con la herramienta Pinkerton en equipos de hogar (Tabla 1) y dispositivos Android (Tabla 2).

En primer lugar, es notable el porcentaje de usuarios que, teniendo una infección en su equipo del hogar, parecen no ser conscientes de la misma, llegando a alcanzar el 59,2 %. Una gran mayoría (86,5 %) de los usuarios considera que su PC no está infectado por malware, por lo que no toma medidas para acabar con la infección y prevenir futuros problemas de seguridad.

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

Pinkerton

Declararon tener malware en PC	Su PC presentaba malware		
	Sí	No	Total
Sí	7,9	5,6	13,5
No	59,2	27,4	86,5
Total	67,1	32,9	100

Base: usuarios de PC
Fuente: Panel hogares, ONTSI

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

Pinkerton

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

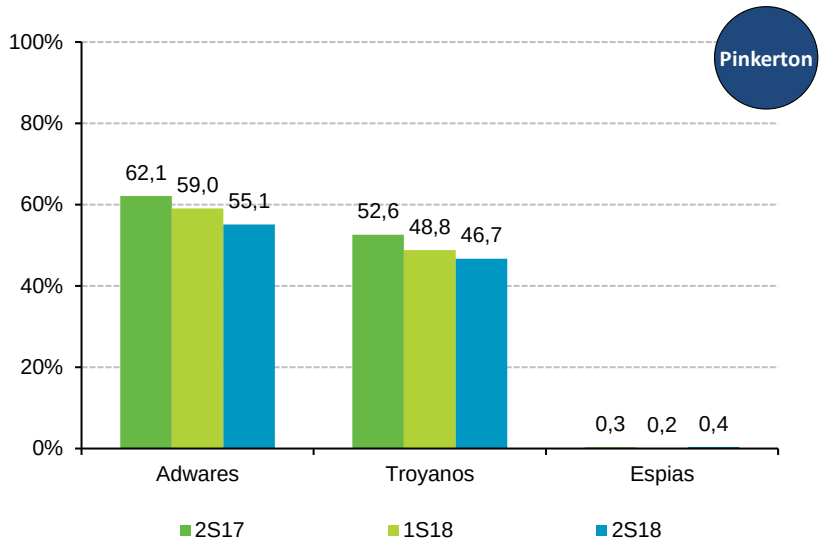
Base: usuarios de dispositivos Android
Fuente: Panel hogares, ONTSI

En contraste, los usuarios de Android sufren menos casos de infección por malware, pero no parecen estar más concienciados de las mismas que los usuarios de PC, puesto que del 22,9 % de usuarios con dispositivos infectados, nada menos que el 21,4 % considera que no sufre ningún tipo de infección. Por lo que, aunque el número de infecciones sea menor, las medidas tomadas para enfrentarse a las mismas no se producen debido al desconocimiento de los usuarios sobre su situación real.

Mientras que los equipos del hogar suelen tener más de un usuario y con niveles de conocimiento muy dispares, lo cual podría explicar el desconocimiento de infecciones o el mayor número de las mismas, los dispositivos Android suelen tener un único usuario, pero el conocimiento del mismo sobre la situación de infección del mismo no es significativamente superior.

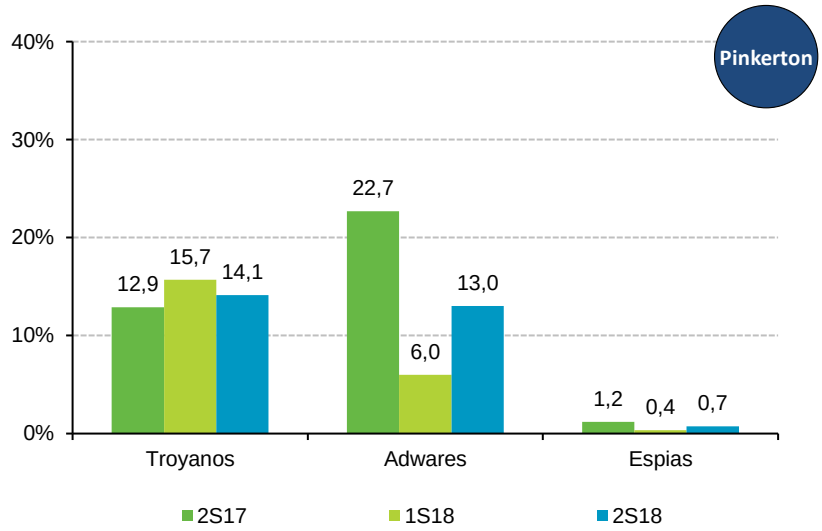
Los ordenadores del hogar se encuentran afectados principalmente por *adware* y troyanos

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



Base: Total ordenadores
Fuente: Panel hogares, ONTSI

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



Base: Total dispositivos Android
Fuente: Panel hogares, ONTSI

Como puede observarse en la Figura 16, el número de infecciones de malware en PC continúa mostrando un descenso, cayendo 3,9 p.p. el porcentaje de adware detectados y 2,1 p.p. el de troyanos. El porcentaje de programas espía continúa siendo muy poco significativo. Respecto a los dispositivos Android, se aprecia un repunte (+7 p.p.) en el uso de adware por parte de los atacantes y un ligero descenso (1,6 p.p.) en el uso de troyanos.

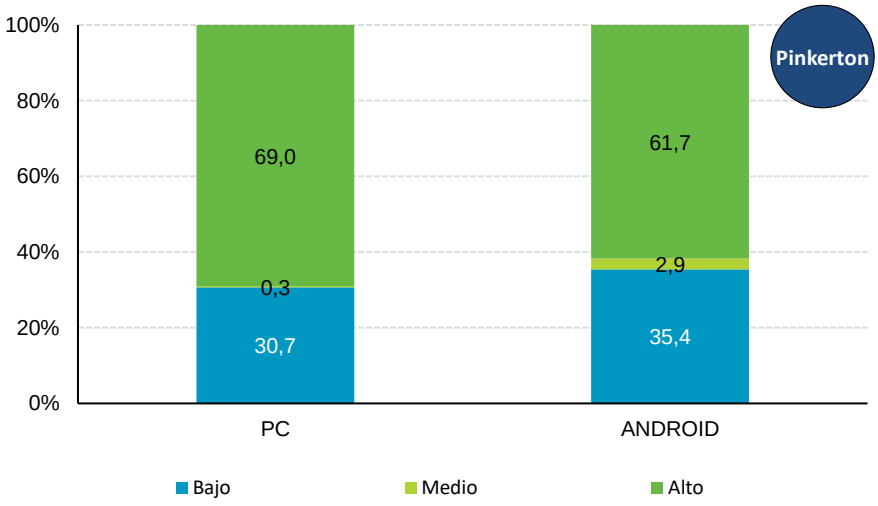
Por tanto, el adware publicitario continúa siendo el preferido por los atacantes, tanto en los equipos del hogar (53,8%) como en los dispositivos Android (13%). Aunque en el caso de los dispositivos Android el uso de troyanos se haya muy cercano al del adware.

No obstante, no debe olvidarse que el usuario de dispositivos Android está acostumbrado al uso de aplicaciones gratuitas que se financian mediante la publicidad mostrada dentro de la misma por lo que se puede dar el caso de sufrir una infección de adware que el usuario identifique erróneamente con la publicidad a la que ya está acostumbrado, reportando un número menor de ataques del real.

Por otro lado, dado que uno de los objetivos principales del malware espía y los troyanos es precisamente el pasar desapercibidos, podría darse un caso similar al del adware, que el usuario esté infectado, pero no lo reporte al no ser capaz de identificarlo correctamente y asociar sus efectos a otros factores.

Lo más significativo de estos resultados es que se aprecia un descenso continuado de las infecciones de equipos del hogar frente a un aumento en el de las infecciones de dispositivos móviles, siendo el más notable el incremento de adware en los dispositivos Android.

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



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

El 69% de los ordenadores y el 61,7% de los dispositivos Android infectados con *malware* se encuentran en un nivel de riesgo alto.

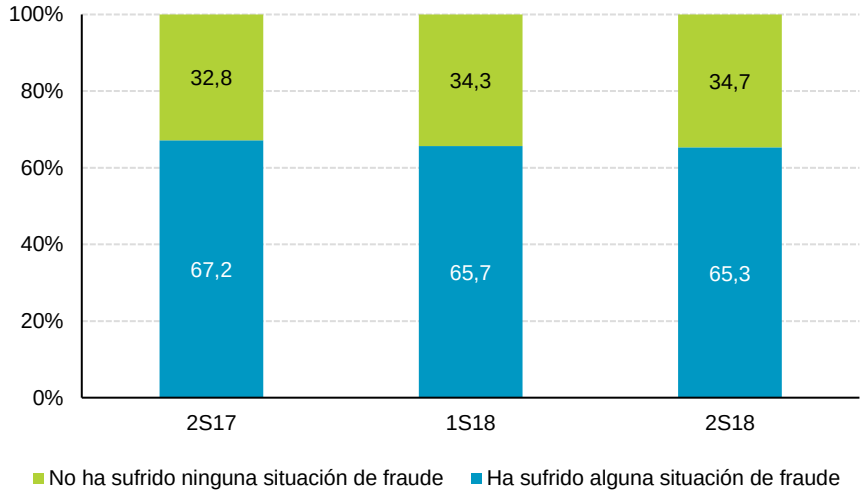
Según el nivel de peligrosidad estimado para las diferentes tipologías de malware detectado en los equipos analizados por Pinkerton, se observa que el nivel de riesgo es alto para el 69,0% de los PCs y para el 61,7% de los dispositivos Android.

Comparando el nivel de riesgo estimado por Pinkerton con la creciente adopción consciente de conductas de riesgo por parte de un número significativo de internautas (Figura 6) y el desconocimiento de la situación real de sus equipos (Figura 14 y Figura 15), queda patente el aumento en el número de incidencias de seguridad que se está detectando y su tendencia a aumentar.

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

Cualquier usuario suele reaccionar ante un incidente de seguridad introduciendo determinados cambios en sus pautas de comportamiento y realizando algunas modificaciones en sus sistemas de seguridad con el fin de paliar las consecuencias de dicho ataque y prevenir futuras incidencias similares o de algún otro tipo aprendiendo de la situación. Por tanto, se podrían clasificar las reacciones como modificaciones de los hábitos de seguridad utilizados al navegar por Internet o como modificaciones de las medidas de seguridad existentes en el equipo.

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



Base: Total usuarios
Fuente: Panel hogares, ONTSI

El porcentaje de internautas que declaran haber sufrido algún tipo de fraude online se mantiene cerca de los dos tercios (65,3%) como en los semestres anteriores, no apreciándose prácticamente ninguna evolución en el tiempo.

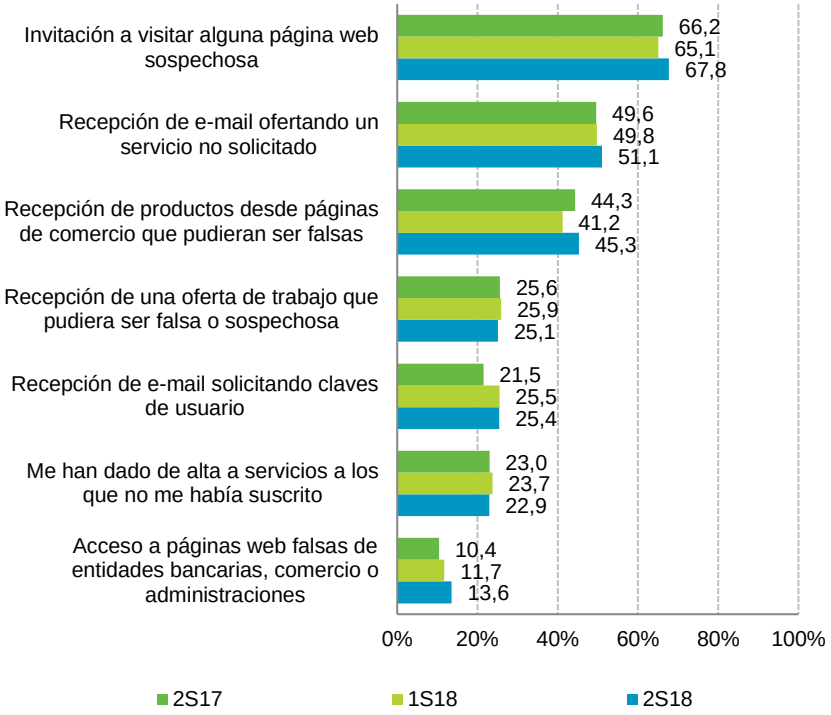
Este tipo de intentos de fraude pueden realizarse de diferentes formas, reflejándose en la Figura 20 la frecuencia con la que se ha declarado cada tipo de ataque.

El tipo de ataque más común siguen siendo las invitaciones a páginas sospechosas, mostrando incluso un aumento de 2,7 p.p. durante el último semestre.

Los tipos de ataque menos comunes continúan siendo las altas no deseadas en servicios Premium (22,9%) y el acceso a páginas falsas de entidades bancarias, comercios o administraciones (13,6%).

Por otro lado, se aprecia un aumento significativo en el porcentaje de intentos de fraude mediante la recepción de productos desde páginas de comercio que pudieran ser falsas o sospechosas de 4,1 p.p.

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



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

Prácticamente todos estos tipos de fraude online continúan siendo enviados al usuario a través de correo electrónico no solicitado, o SPAM, y de las redes sociales.

Por lo tanto, gran cantidad de estos fraudes puede evitarse configurando correctamente el correo electrónico y siguiendo unas pautas mínimas de seguridad en la gestión de los correos recibidos como son el no abrir correos de remitentes desconocidos ni los ficheros adjuntos sospechosos y/o procedentes de remitentes que no son de confianza.

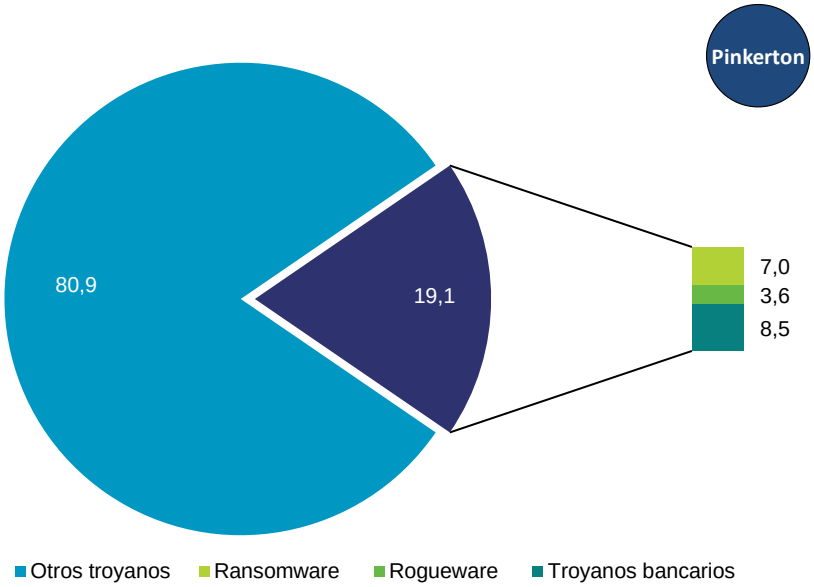
El porcentaje de páginas web falsas de entidades bancarias, comercios o administraciones es relativamente reducido debido a las herramientas antiphishing que hay actualmente implementadas en navegadores web y servicios online que bloquean de antemano dichas webs y requieren de una acción directa por parte del usuario para saltarse dicha medida de seguridad.

Los intentos de engañar al usuario mediante encuestas, falsos premios, cupones descuento, cheques regalo, o cualquier otro ardid intentando suplantar la identidad de alguna marca conocida o cadena comercial siguen teniendo un éxito moderado suscribiendo a sus víctimas en servicios Premium no deseados (22,9%) o robándoles información privada, como la dirección de correo electrónico, para el envío de promociones, servicios no solicitados (51,1%) y publicidad no deseada.

Tipología del malware analizado

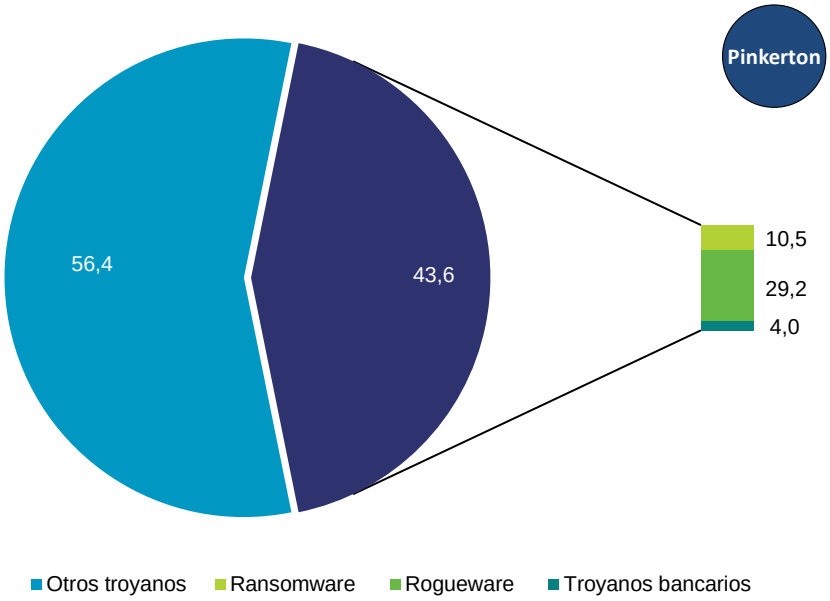
- Troyano bancario: *malware* que roba información confidencial a los clientes de banca y/o plataformas de pago online.
- *Rogueware* o rogue: *malware* que hace creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto 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 21. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN EL ORDENADOR DEL HOGAR (%)



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

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



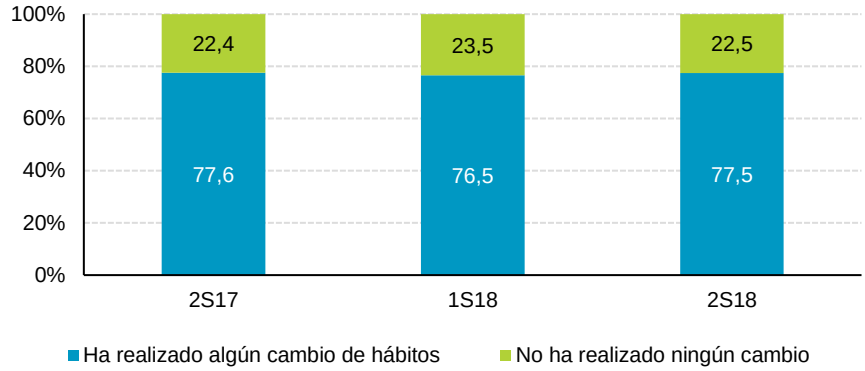
Base: Equipos con troyanos detectados en dispositivos Android
Fuente: Panel hogares, ONTSI

En los PCs siguen siendo más comunes los troyanos de tipo bancario (8,5%) y los ransomware (7%), mientras que en los dispositivos Android los más comunes son, con gran diferencia, los troyanos de tipo rogueware (29,2%).

Es decir, que la estrategia más común en dispositivos móviles sigue siendo el alertar a la víctima con una falsa alarma sobre una infección para conseguir que el usuario se descargue el malware auténtico.

Casi cuatro de cada cinco internautas españoles modifica sus hábitos prudentes tras experimentar una incidencia de seguridad.

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

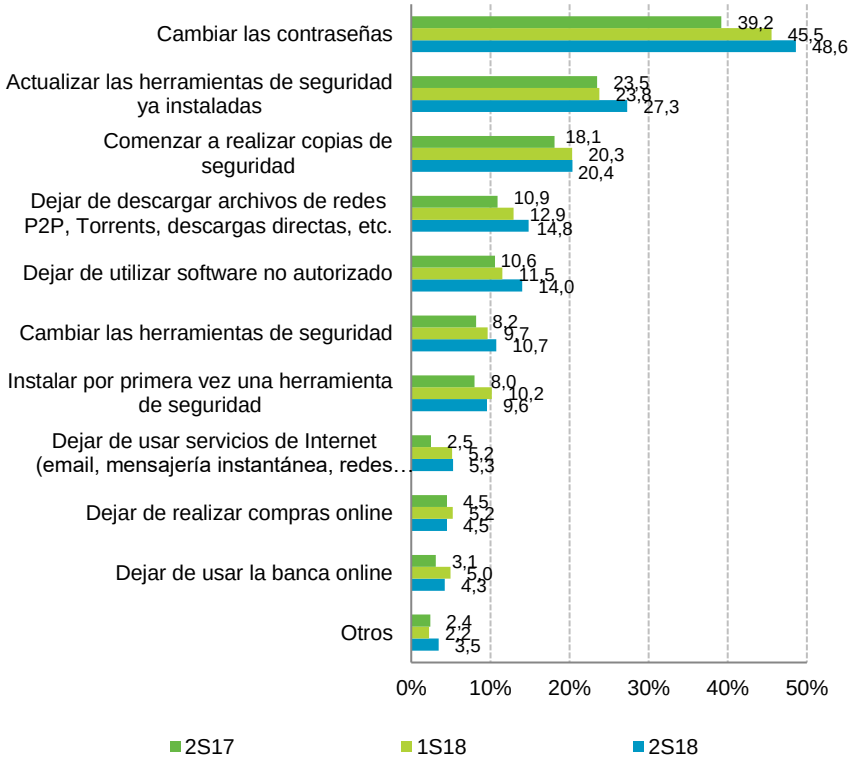


Base: Usuarios que han sufrido un incidente de seguridad
Fuente: Panel hogares, ONTSI

Este segundo semestre de 2018 se ha observado una inversión en las reacciones del usuario ante un incidente de seguridad, alcanzando valores que rondan los mostrados a finales de 2017. Así, tras un aumento de 1 p.p. en el último semestre, el porcentaje de usuarios que opta por realizar algún cambio tras un incidente se sitúa en el 77,5%.

En la Figura 24 se observa cómo la medida que presenta mayor popularidad es el cambio de contraseñas, que alcanza el 48,6% de los casos con un incremento de 3,1 p.p., seguida por la actualización de las herramientas de seguridad ya instaladas (27,3%) y del inicio de la realización de copias de seguridad (20,4%).

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



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

El cambio de contraseñas es una medida altamente recomendable especialmente tras un incidente de seguridad, pero se aconseja igualmente cambiarlas de forma periódica, usar contraseñas robustas y no repetirlas en diferentes servicios.

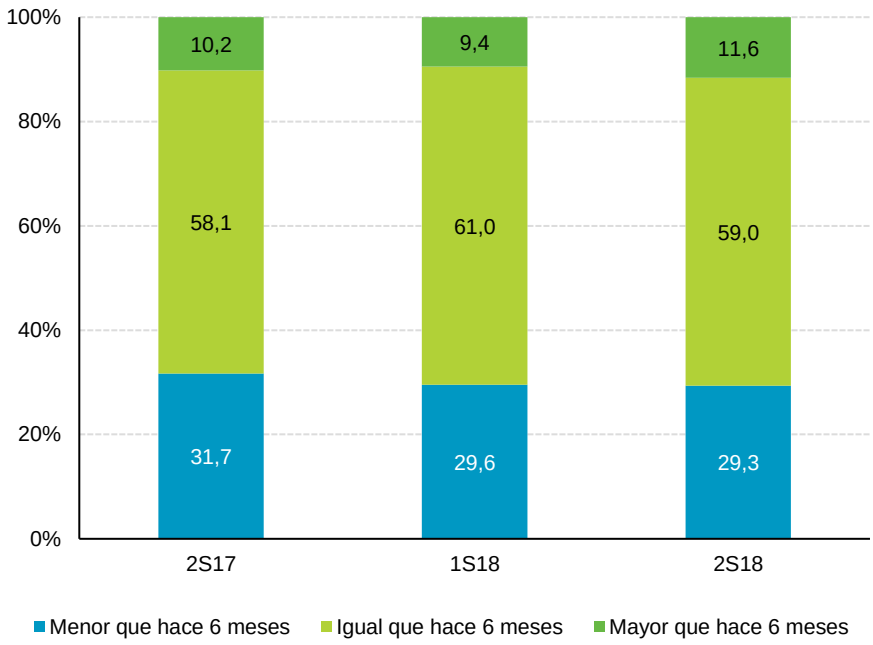
En general, todas las medidas presentan incrementos en sus adopciones, salvo la instalación de nuevas herramientas de seguridad y el cese del uso de los servicios de compras y banca online.

Se considera muy positivo que vaya aumentando paulatinamente el uso de copias de seguridad para prevenir la pérdida de datos y minimizar los perjuicios causados por malware de tipo ransonware, sobre todo teniendo en cuenta que hoy en día se dispone de una gran variedad de servicios y software orientado a la creación de copias de seguridad de forma sencilla, cómoda y rápida.

1.5 Confianza en el ámbito digital en los hogares españoles

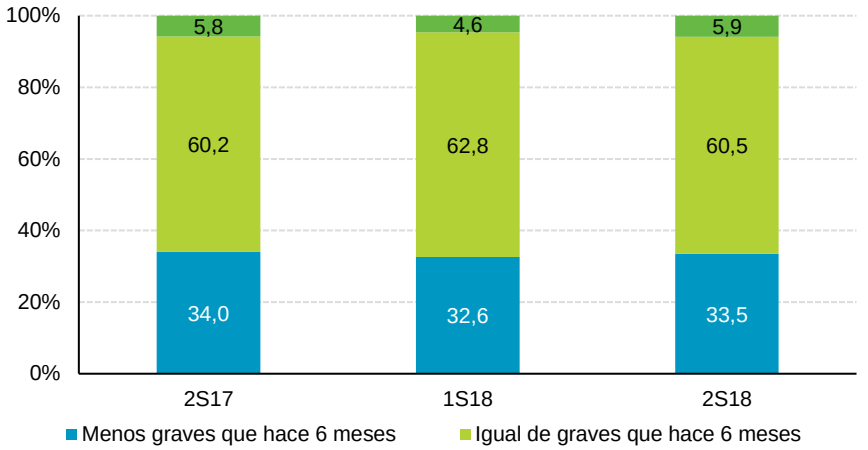
La última parte de este estudio se centra en la valoración de los usuarios sobre los riesgos y peligros de Internet, sus opiniones y consideraciones acerca de la propia responsabilidad en cuanto a seguridad y la confianza general en la Red de Redes.

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



Base: total usuarios
Fuente: Panel hogares, ONTSI

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

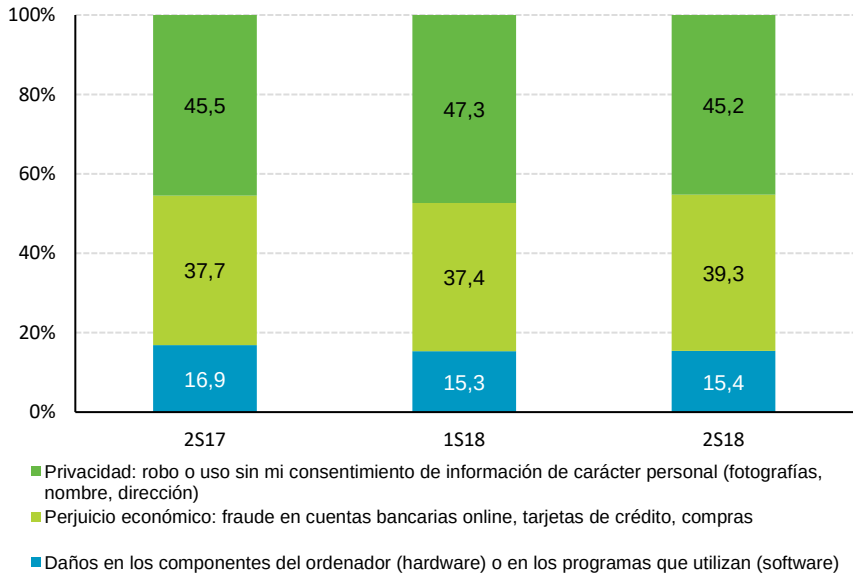


Base: total usuarios
Fuente: Panel hogares, ONTSI

El número de incidencias percibido por los internautas parece seguir aumentando ligeramente semestre a semestre, de modo que aproximadamente uno de cada diez internautas opina que hay más incidencias actualmente (11,6%) mientras que tres de cada cinco (59%) considera que el número de incidencias de seguridad no ha variado. Respecto a la percepción sobre la gravedad de las incidencias, la opinión de los internautas se mantiene más estable, opinando aproximadamente un tercio que son menos graves frente a menos de un 6% que considera que son de mayor gravedad.

No obstante, como se ha visto anteriormente, el estado de los equipos en relación al malware detectado (Figura 14), el nivel de riesgo en que se encuentran los mismos, y la falta de percepción del usuario en este tipo de incidencias (Tabla 1 y Tabla 2), indica que los usuarios no son plenamente conscientes de su situación real.

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



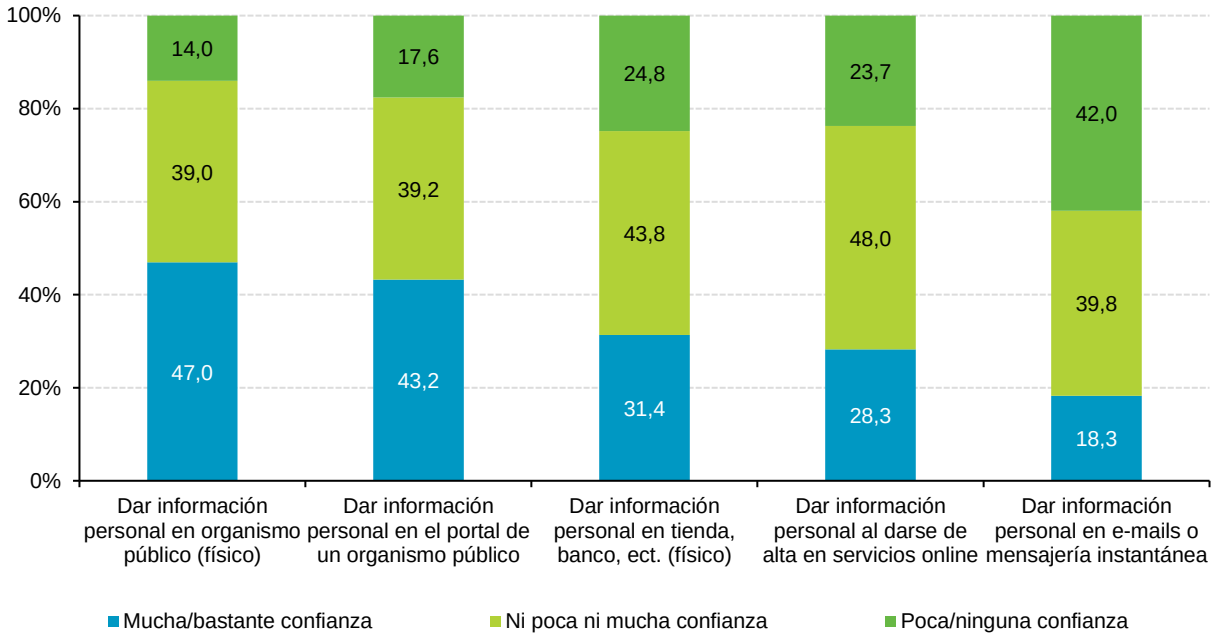
Base: total usuarios
Fuente: Panel hogares, ONTSI

En la Figura 27 se observa que los usuarios siguen opinando mayoritariamente que el riesgo más significativo de Internet es la pérdida de privacidad debido al robo o uso sin consentimiento de información de carácter personal (45,2%) y al perjuicio económico sufrido por el fraude relacionado con datos bancarios o compras por Internet (39,3%).

Sigue siendo significativo que los usuarios se preocupen por el robo de datos personales cuando no suelen prestar atención a las hojas de licencia y/o condiciones de uso al instalar software en sus equipos y/o registrarse en servicios de Internet (Figura 9). Es de notar que en muchas ocasiones están cediendo estos datos de forma explícita pese a no ser conscientes de ello por renunciar a leer dichas licencias y condiciones de uso previamente a su aceptación. Dichos documentos contienen información interesante acerca del uso del programa o servicio y la información personal 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 28. NIVEL DE CONFIANZA EN FACILITAR DATOS PERSONALES (%)



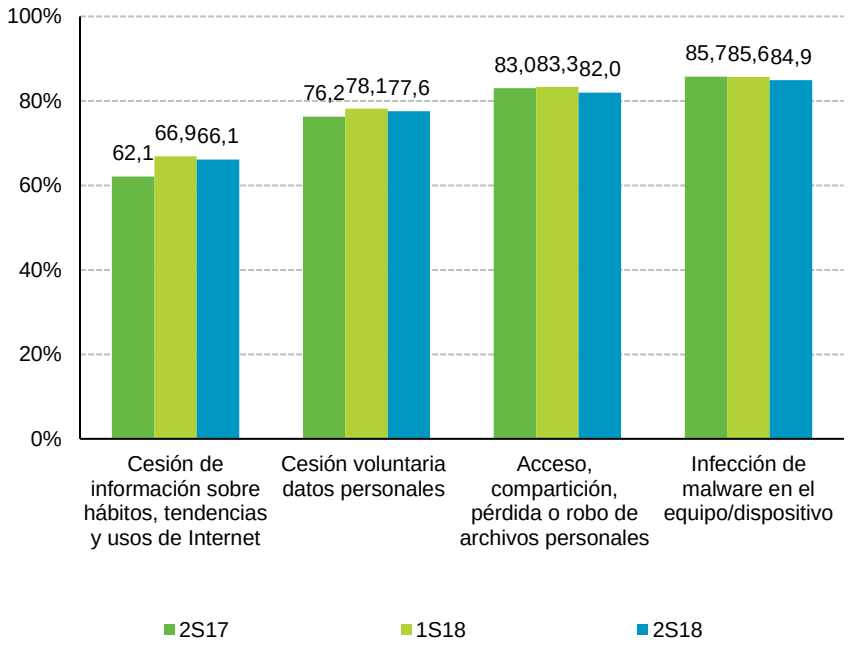
Base: total usuarios
Fuente: Panel hogares, ONTSI

Las campañas de SCAM, phishing o cualquier otro tipo de fraude que intente recopilar información personal y/o privada del receptor siguen siendo bastante numerosas, empleando el correo electrónico como vía principal. Aunque afortunadamente hay un elevado número de usuarios (42%) que desconfían de este medio para la comunicación de dicha información.

Por otro lado, el porcentaje de usuarios que desconfía al dar información privada al darse de alta en servicios online es significativamente menor (23,7%) pese a que es igualmente un medio bastante común para el robo de información usado por campañas de phishing y SCAM.

Por otro lado, hay un porcentaje significativo de usuarios que confían en los organismos públicos, existiendo una diferencia relativamente pequeña entre las sedes físicas y las sedes electrónicas (3,8 p.p.).

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



Base: total usuarios
Fuente: Panel hogares, ONTSI

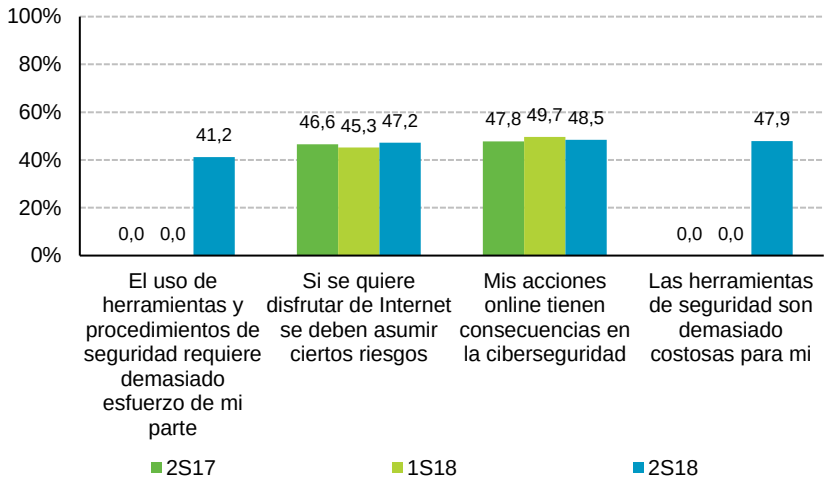
Respecto a la valoración de los peligros de Internet, los usuarios siguen pensando que el mayor peligro es la infección por malware (84,9%), y en segundo lugar, la pérdida o robo de archivos personales (82%).

La cesión de información sobre hábitos, tendencias y usos de Internet continúa asimismo siendo el riesgo de menor preocupación, aunque es objeto de preocupación por parte de nada menos que dos tercios de los internautas.

Los usuarios parecen realmente conscientes de los riesgos que pueden acechar en la red. Aunque siguen declarando que asumen riesgos debido a que son necesarios para poder aprovechar plenamente los servicios de Internet, tal y como se desprende de los 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.

Prácticamente la mitad de los internautas (48,5%) son conscientes de la importancia y consecuencias que tienen sus propias acciones en la ciberseguridad.

FIGURA 30. EVOLUCIÓN DE LA RESPONSABILIDAD EN LA SEGURIDAD DE INTERNET (%)[2]

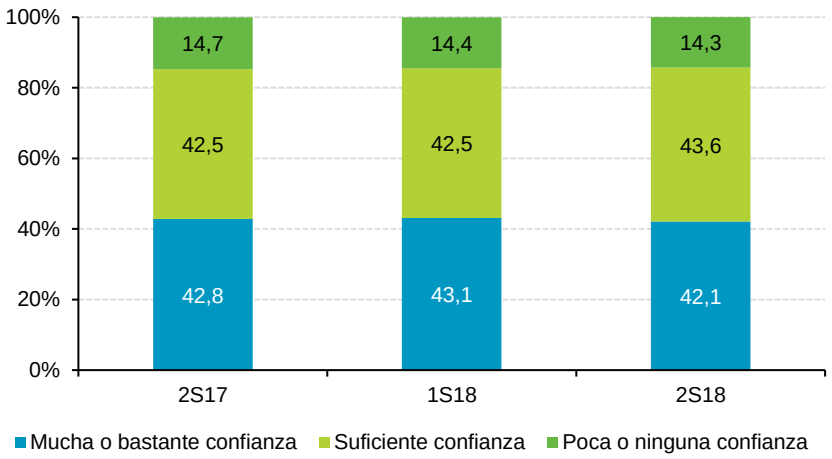


Base: total usuarios
Fuente: Panel hogares, ONTSI

Sin embargo, una cantidad similar de usuarios considera que es necesario asumir riesgos para disfrutar de la experiencia de navegar por la Red (47,2%), presentando un aumento de 1,9 p.p. respecto al semestre anterior. El tema se agrava con la existencia de un número similar de panelistas que consideran que las herramientas de seguridad son demasiado caras (47,9%) o que son demasiado complejas y suponen demasiado esfuerzo de su parte (41,2%).

A la vista de estas declaraciones se puede presumir de que a pesar de ser conscientes de los riesgos y de cómo sus propias acciones tienen relación directa con las incidencias de seguridad, existe una tendencia a relajarse tanto en la utilización de herramientas de seguridad como en los hábitos prudentes.

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



Base: total usuarios
Fuente: Panel hogares, ONTSI

[2] Las opciones "El uso de herramientas y procedimientos de seguridad requiere demasiado esfuerzo de mi parte" y "Las herramientas de seguridad son demasiado costosas para mi" se analizan por primera vez en el segundo semestre de 2018.

Teniendo en cuenta la evolución de los hábitos de seguridad y las incidencias de seguridad reportadas, es comprensible que haya habido un ligero descenso en el porcentaje de usuarios con mucha o bastante confianza. Sería recomendable que los internautas revisasen las medidas de seguridad empleadas y se concienciaran de que ciertas conductas aumentan las probabilidades de sufrir una incidencia de seguridad, cuyas consecuencias siempre resultan negativas para la experiencia y el disfrute de 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:

Asimismo, se quiere también agradecer la colaboración de:

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

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