OBSERVACIBER

CÓMO SE PROTEGE LA CIUDADANÍA ANTE LOS CIBERRIESGOS

ESTUDIO SOBRE PERCEPCIÓN Y NIVEL DE CONFIANZA EN ESPAÑA

Edición Diciembre 2021

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
ontsi | incibe_ | OBSERVACIBER

ÍNDICE

CÓMO SE PROTEGE LA CIUDADANÍA ANTE LOS CIBERRIESGOS. ESTUDIO SOBRE PERCEPCIÓN Y NIVEL DE CONFIANZA EN ESPAÑA

1 Contexto del estudio

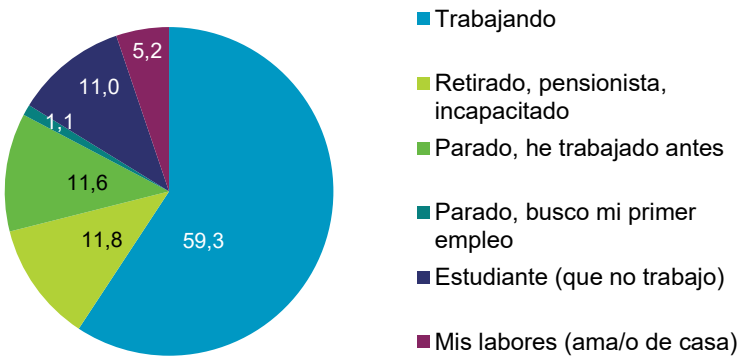
El Observatorio Nacional de Tecnología y Sociedad (ONTSI) publica semestralmente el estudio 'Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España' que analiza, en el ámbito de los hogares la adopción de medidas de seguridad, evaluar la incidencia de ciberriesgos y mide el grado de confianza que los hogares españoles depositan en el uso de las tecnologías. Este resumen ejecutivo corresponde al estudio realizado en el primer semestre de 2021.

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 un *software* ad-hoc y el análisis de las declaraciones aportadas por los internautas encuestados. Los datos declarados son obtenidos de las encuestas online realizadas a los hogares que han conformado la muestra del estudio, mientras que para los datos reales se utiliza el *software* Pinkerton. Este *software* analiza los sistemas de ordenadores personales (PC's) y dispositivos Android recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas, a la vez que detecta la presencia de *malware* en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 70 motores antivirus.

Así se realiza un contraste comparativo entre el nivel percibido de incidencias de seguridad y la realidad obtenida con el escaneo informático de los equipos de la ciudadanía. Se pretende impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe tiene como finalidad, entre otras, informar del comportamiento y utilización segura y privada de las nuevas tecnologías, además de servir como apoyo para solucionar incidencias por parte de los usuarios y la adopción de medidas por parte de la Administración.

Este estudio se realiza sobre una base de datos recogidos desde enero hasta junio de 2021, ambos meses inclusive. Durante el confinamiento se experimentó un creciente interés por la formación, y en este contexto interesa comprender si ha afectado a las pautas de los internautas. Por este motivo es interesante conocer la situación laboral de los panelistas, de cara a discernir su predisposición a la participación en cursos de formación.

FIGURA 1. CONTEXTO LABORAL DE LOS PANELISTAS

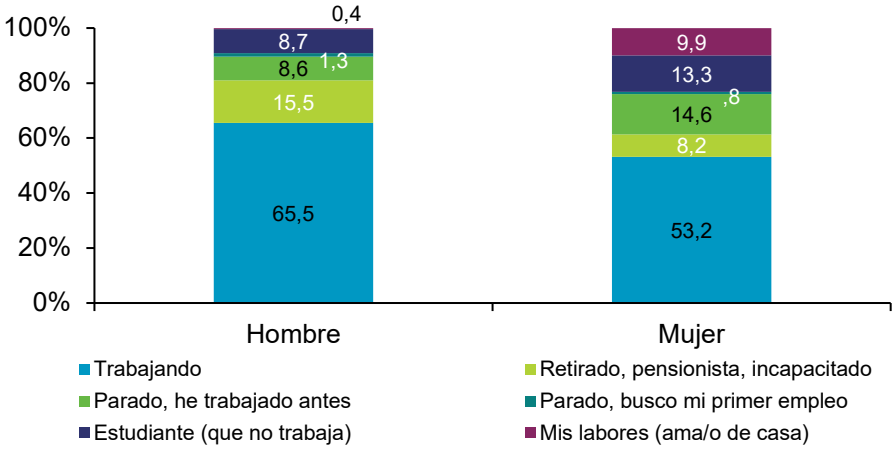


Base: Total usuarios
Fuente: Panel hogares, ONTSI

La participación en acciones formativas podría venir condicionada por políticas de la empresa en el caso de los panelistas que formen parte de la población activa. De hecho, los participantes más propensos a recibir cursos de formación (por ejemplo, para mejorar sus habilidades de cara a su trabajo actual o perspectivas futuras) podrían ser los trabajadores (59,3%), parados en búsqueda de empleo (1,1%) y estudiantes (11%).

Por último como parte de este estudio se han destacado también aspectos de diferenciación por género incluyéndose un informe ad-hoc en una separata. En la FIGURA 2 se indica la diferenciación por ocupación y género. para la realización de este estudio se dispone de una muestra en la que el 49,5% son hombres y el 50,5% son mujeres. Sin embargo, pese al balanceo en el género, sí se observan diferencias que podrían afectar a los resultados discriminatorios en base a la ocupación de los panelistas.

FIGURA 2. OCUPACIÓN DE LOS PANELISTAS POR GÉNERO



Base: Total usuarios
Fuente: Panel hogares, ONTSI

2 Contexto internacional

La Agencia de la Unión Europea para la Ciberseguridad, más conocida como ENISA, realiza la campaña anual titulada 'El mes Europeo de la ciberseguridad'[1]. Su cometido es promover la ciberseguridad entre los ciudadanos de la Unión Europea, objetivo que comparte precisamente el estudio que presentamos a continuación. Más concretamente, se persigue sensibilizar a la población sobre los peligros que existen en la red además de inculcar buenas prácticas en el uso de las nuevas tecnologías.

En particular, en la última campaña llevada a cabo por ENISA se ha realizado un estudio en el que participan personas con edades comprendidas entre los 25 y los 54 años (nuestro estudio incluye a la ciudadanía mayor de 15 años). Son ciudadanos de la Unión Europea que utilizan internet para realizar compras online dentro del estado miembro de la UE en el que tienen su residencia y en cualquier otro estado perteneciente a la UE. Estos responden una serie de cuestiones que evalúan donde se sienten más seguros o donde encuentran más problemas de seguridad al realizar sus compras. Algunos usuarios han reportado problemas de fraude online, en concreto el 2,5%, mientras que el 25% han declarado que el mayor problema que tienen para realizar compras online es la seguridad de los pagos o la preocupación por su privacidad.

Precisamente, el estudio que aquí presentamos aborda la problemática del fraude como uno de los ataques que sigue acumulando más víctimas hoy día, pese a las múltiples campañas de concienciación.

Otros datos de interés en relación con este documento son aportados por la revista Forbes[2]. Forbes ha realizado una serie de estadísticas de ciberseguridad que contribuyen a discernir si estamos preparados para las amenazas que existen y las que puedan surgir a lo largo de este año. También analizan los tipos de amenazas, los datos en riesgo y lo ligada que está la ciberseguridad a la economía. Al respecto de estos puntos, un dato significativo es que el 78% de los directivos de las compañías incluidas en este estudio, creen que su preparación en lo que respecta a la ciberseguridad, es insuficiente.

Además, en cuanto a clasificación relativa a la preparación de los ciudadanos y entidades correspondiente a ciberseguridad realizada por Forbes, la conclusión va en línea de los temas abordados en este documento.

En particular, se destaca que es necesario tener una mejor higiene en la utilización de contraseñas, instalación y desarrollo de parches de seguridad y el uso del doble factor de autenticación. En promedio de los directorios que contienen las empresas, tan solo el 5% de los que contienen información sensible están protegidos según recalca el informe.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

[2] https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-----what-you-need-to-know-for-2021/?sh=53c4a7d558d3

El incremento del teletrabajo también ha aumentado el número de amenazas al que se enfrentan las empresas y esto ha llevado a que el 80% de los líderes del sector tecnológico crean que sus organizaciones carecen de protección suficiente contra ataques. Es por este motivo por el que, conforme a Forbes, se apuesta cada vez más por invertir en seguridad, para proteger los activos más importantes de sus corporaciones frente a posibles ataques.

Si bien este es un estudio que pone el foco en la ciudadanía, más vinculado al promovido por ENISA, cabe destacar que se considera igualmente si los ciudadanos forman parte de la población activa para entender el impacto que los malos hábitos cotidianos podrían tener en las empresas para las que trabajan.

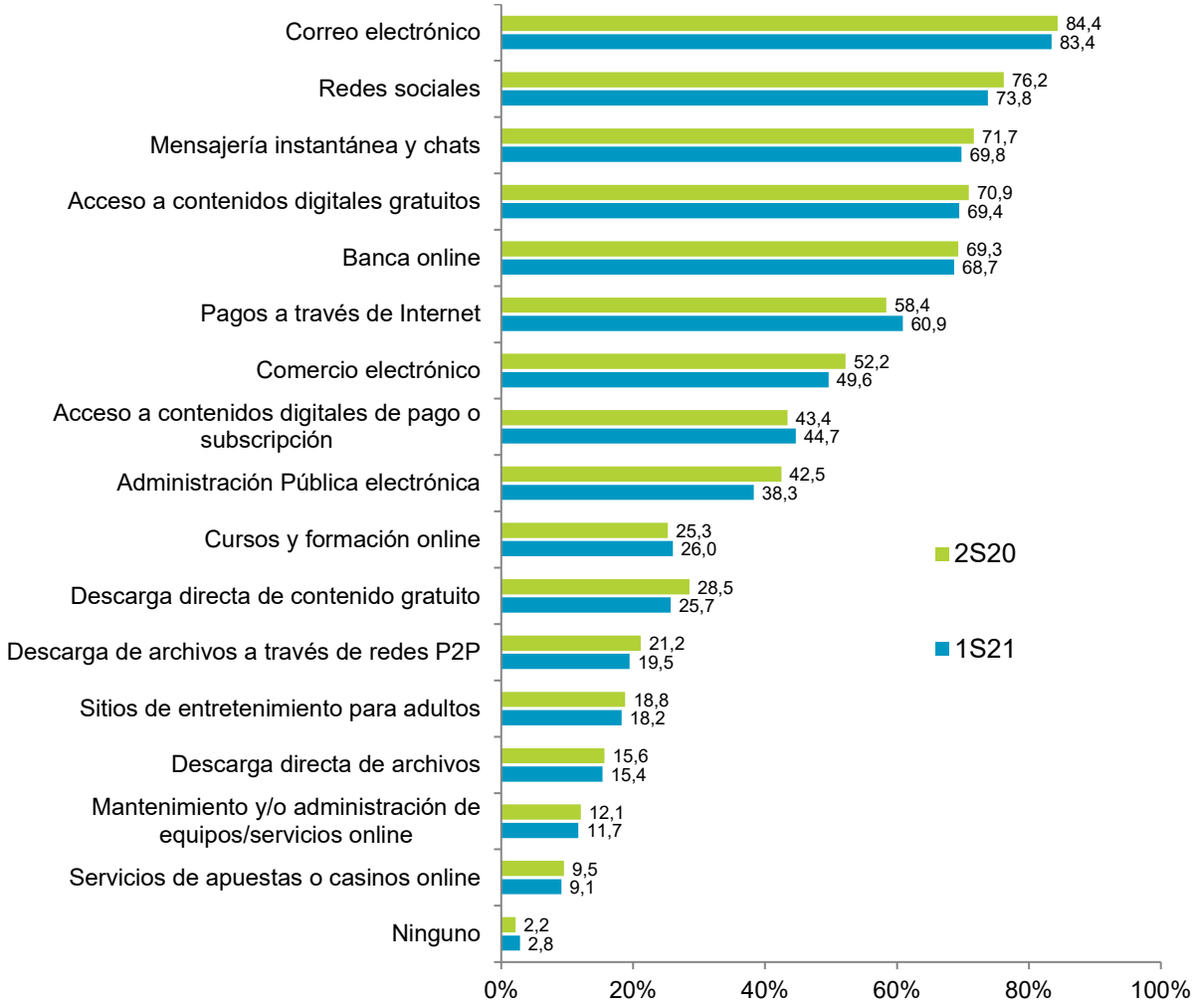
3 Usos de Internet

En general las pautas de uso de Internet descienden muy levemente, a excepción de los pagos a través de Internet (60,9%), el acceso a contenidos digitales de pago o suscripción (44,7%) y la participación en cursos y formación online (26%). También cabe destacar que un mayor número de usuarios declara no emplear ninguno de estos servicios de Internet (2,6%).

Esto último podría deberse a la eliminación de restricciones de movilidad y vuelta paulatina a las actividades rutinarias. No todos los usuarios abrazan de igual forma los trámites electrónicos, o bien no acaban de adaptarse a los mismos, prefiriendo el contacto de ventanilla. Por ejemplo, ya se vio esta tendencia en estudios anteriores cuando se trata de los trámites con la banca: los usuarios tienden a confiar aún bastante en los trámites físicos. No obstante, existen servicios que se contratan/acceden únicamente vía Internet al no depender de sucursales físicas o por su naturaleza, como por ejemplo los contenidos digitales, cuyo uso continúa en aumento. La eliminación de las restricciones de movilidad en este punto no ha significado un descenso, por lo que pudiera ser ya un hábito adquirido por los panelistas. Este hábito suele venir acompañado de un descenso en prácticas de riesgo, como la previsible disminución de la descarga de contenido ilegal desde webs de dudosa reputación.

El aumento de los pagos a través de Internet puede venir motivado incluso por la contratación de los servicios anteriores, aunque tampoco puede descartarse que sea motivado por el uso de pagos a través de servicios como Bizum, empleados ya en algunos comercios.

FIGURA 3. USO DECLARADO DE SERVICIOS DE INTERNET (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

SERVICIOS EN AUMENTO (DATO DECLARADO)

60,9%
PAGOS A TRAVÉS DE INTERNET

44,7%
ACCESO A CONTENIDOS DIGITALES DE PAGO O SUBSCRIPCIÓN

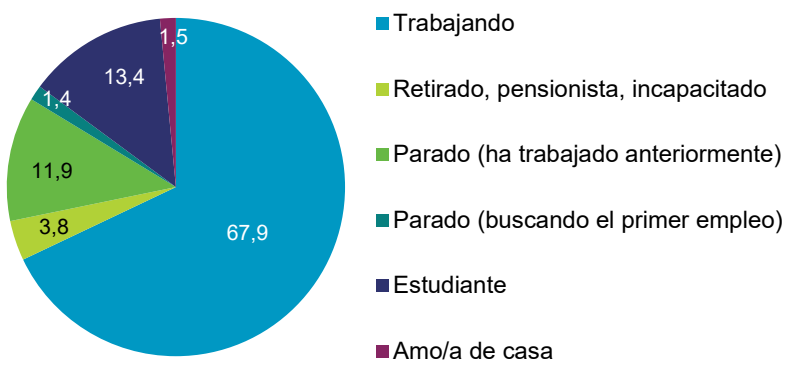
26%
CURSOS Y FORMACIÓN ONLINE

Cabe destacar que, respecto al semestre anterior, el uso de Internet para el acceso a cursos y formación online aumenta un 1,3p.p., situándose en el 26%. Este crecimiento puede darse al hábito adquirido de las ventajas de la formación online, pero también a la necesidad de formación impulsada por las propias empresas.

3.1 Internet como herramienta para la formación

Los cursos de formación online permiten que un gran número de usuarios de muy diverso perfil adquiera conocimiento sobre materias que les ayuda no solo en su mejora profesional, sino en su rutina diaria.

FIGURA 4. ACCESO A CURSOS Y FORMACIÓN ONLINE SEGÚN LA ACTIVIDAD REALIZADA POR LOS USUARIOS (%)



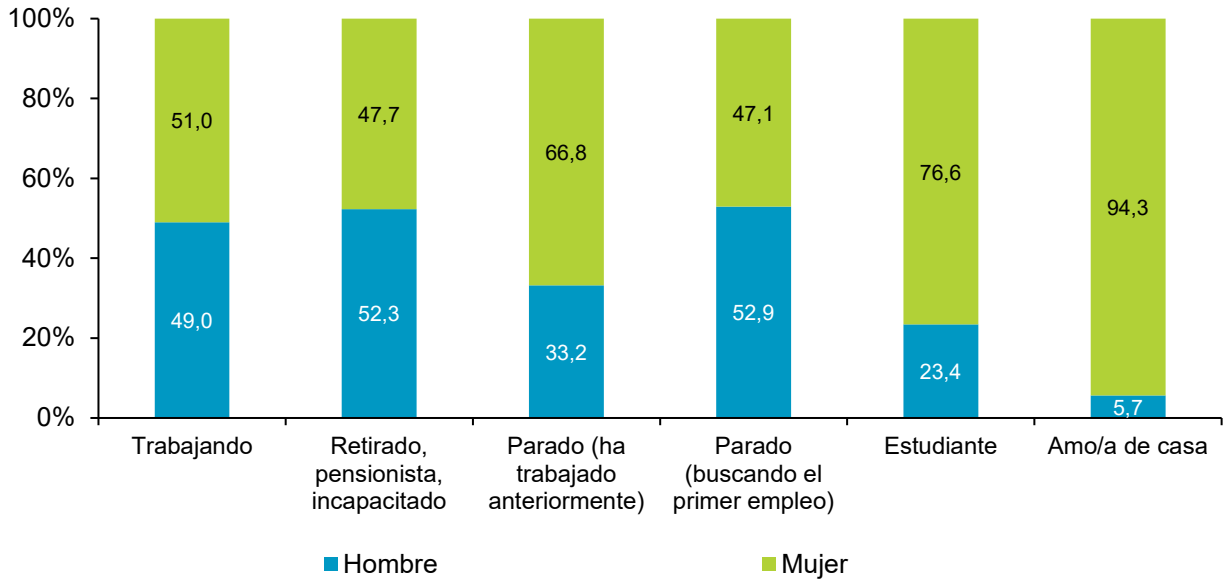
Base: Usuarios que acceden a cursos y formación online
Fuente: Panel hogares, ONTSI

En este semestre se ha observado un crecimiento en el uso de Internet para cursos formativos, aún sin restricciones de movilidad. Es decir, puede que sea una conducta ya adquirida por los panelistas.

Los cursos de formación son un recurso habitual entre estudiantes y trabajadores, aunque también se da entre el resto de la población, conforme indica la FIGURA 4.

Estos datos a su vez se desglosan por género en la FIGURA 5. Por ejemplo, de la población que se encuentra trabajando y que accede a cursos de formación online, el 49% son hombres, frente al 51% que son mujeres. Destaca especialmente que el 76% de los estudiantes que cursa formación online son mujeres.

FIGURA 5. ACCESO A CURSOS Y FORMACIÓN ONLINE SEGÚN LA ACTIVIDAD REALIZADA POR LOS USUARIOS Y GÉNERO (%)



Base: Usuarios que acceden a cursos y formación online por actividad realizada
Fuente: Panel hogares, ONTSI

Las personas dedicadas a las labores del hogar también participan en cursos de formación online. Recordando la FIGURA 2, el número de mujeres trabajadoras del hogar es muy superior en la muestra empleada por el estudio, lo que puede justificar la diferencia de porcentajes de mujeres que son amas de casa y participan en cursos de formación, frente a la población masculina, situada en el 5,7%.

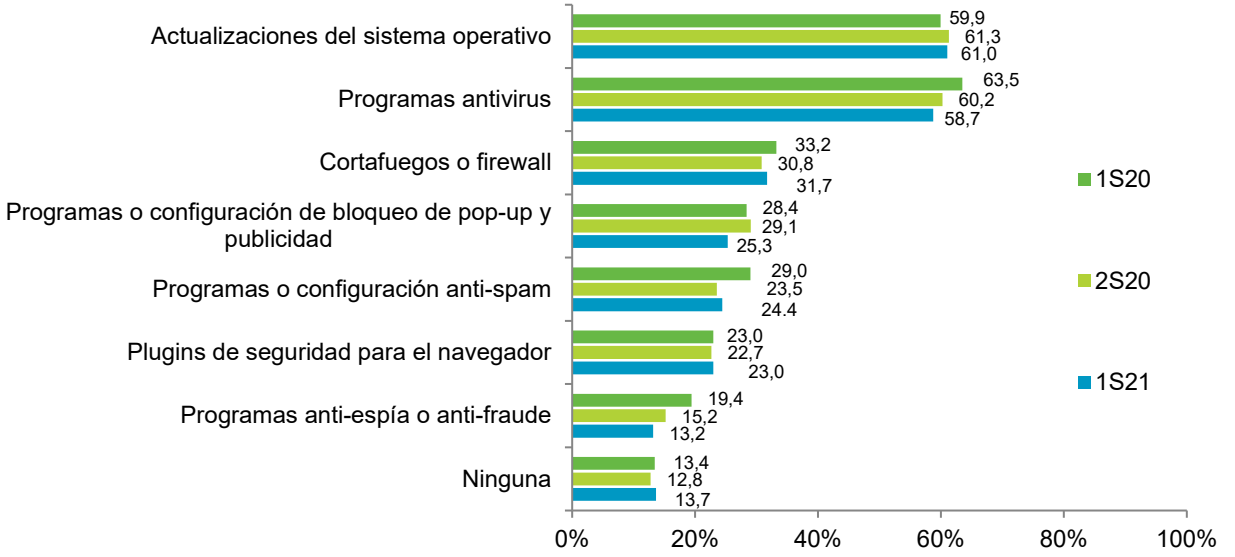
4 Medidas de seguridad

En esta sección se analizan las medidas de seguridad utilizadas por los panelistas españoles durante el primer semestre de 2021. Esta parte del estudio recogerá tanto los resultados de las encuestas como la información recopilada mediante el análisis real de los ordenadores del hogar y los dispositivos móviles. La obtención de los datos de los dispositivos se realiza por medio de la herramienta Pinkerton.

4.1 Ordenador del hogar

Para la realización de este estudio se ha empleado la siguiente clasificación de las medidas de seguridad: la primera de ellas obedece a la catalogación de medidas que pueden ser automatizables (pasivas), es decir aquellas en las que el usuario no necesita tomar parte del proceso, aunque en algunos casos participe en la configuración. El segundo grupo de medidas engloba aquellas que necesitan que el usuario intervenga en el proceso para su correcto funcionamiento -a las que denominamos activas o no automatizables-. Aunque las últimas versiones de las plataformas PC y móviles ya incluyen medidas no automatizables de forma nativa, en este estudio se tiene en cuenta la clasificación expuesta en el párrafo anterior, porque no todos los usuarios que participan en el estudio disponen de dispositivos con las últimas versiones.

FIGURA 6. MEDIDAS DE SEGURIDAD AUTOMATIZABLES EN EL ORDENADOR DEL HOGAR (DATOS DECLARADOS)



Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

Respecto al semestre anterior el uso de cortafuegos o *firewalls* experimenta una tímida subida de 0,9 p.p.

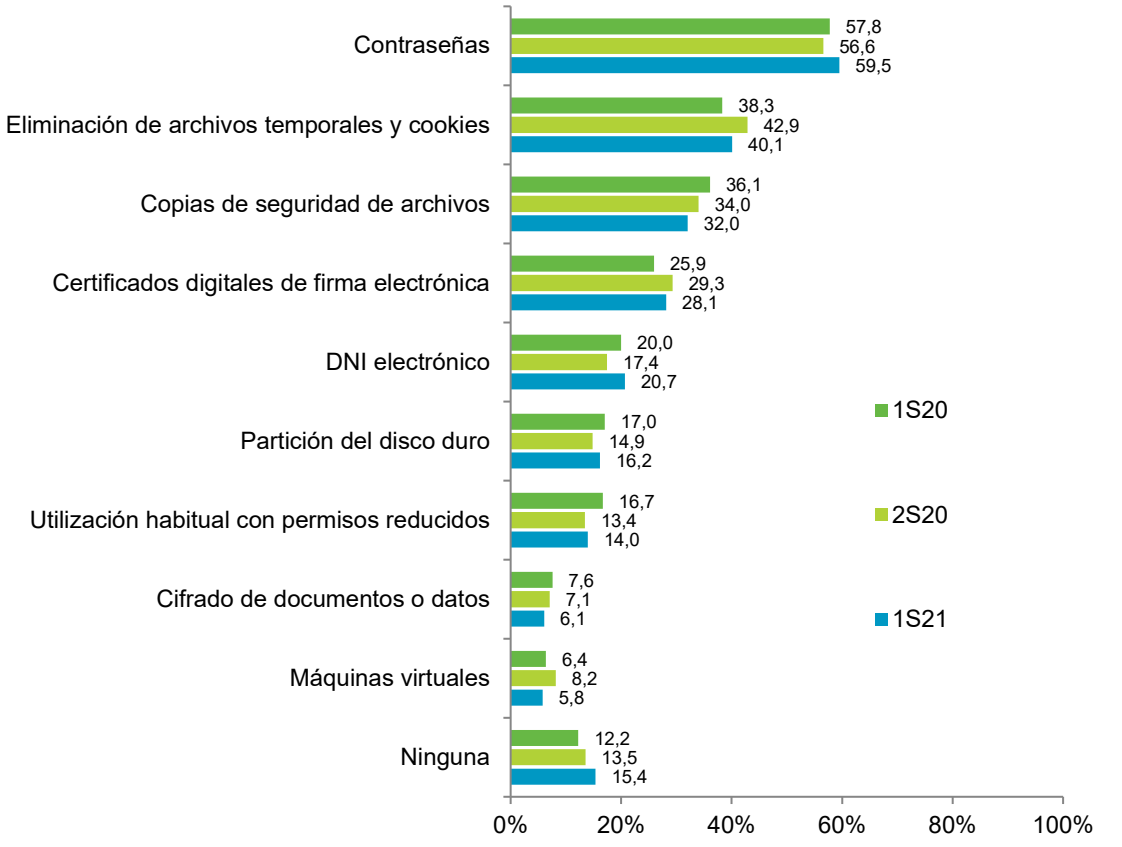
De igual forma los panelistas declaran usar más programas o configuraciones *anti-spam* y plugins de seguridad para el navegador. Sin embargo, en general, se produce un descenso en el uso de mecanismos automatizables, reflejado a su vez en que un mayor número de panelistas declara no emplear ninguna de estas medidas (+0,9 p.p. respecto el semestre anterior).

En el caso de las medidas automatizables, a excepción del uso del cortafuegos o *firewall* 31,7% y el uso de programas *anti-spam* 24,4%, el uso de medidas automatizables ha disminuido nuevamente en el ordenador del hogar.

Conforme a las declaraciones de los panelistas se observa, por tercer semestre consecutivo, un descenso en el uso de los programas antivirus (-1,5 puntos porcentuales respecto a la oleada anterior).

Respecto a las medidas de seguridad activas (FIGURA 7), este semestre destaca el uso de contraseñas (59,5%), aumentando casi 3 p.p. respecto al semestre anterior, y también el ascenso del uso del DNI electrónico 3,3 p.p. en comparación con el semestre anterior. Sin embargo, el uso de certificados digitales sigue siendo la opción más usada por los panelistas frente al DNI electrónico.

FIGURA 7. MEDIDAS DE SEGURIDAD ACTIVAS (NO AUTOMATIZABLES) EN EL ORDENADOR DEL HOGAR (DATOS DECLARADOS)

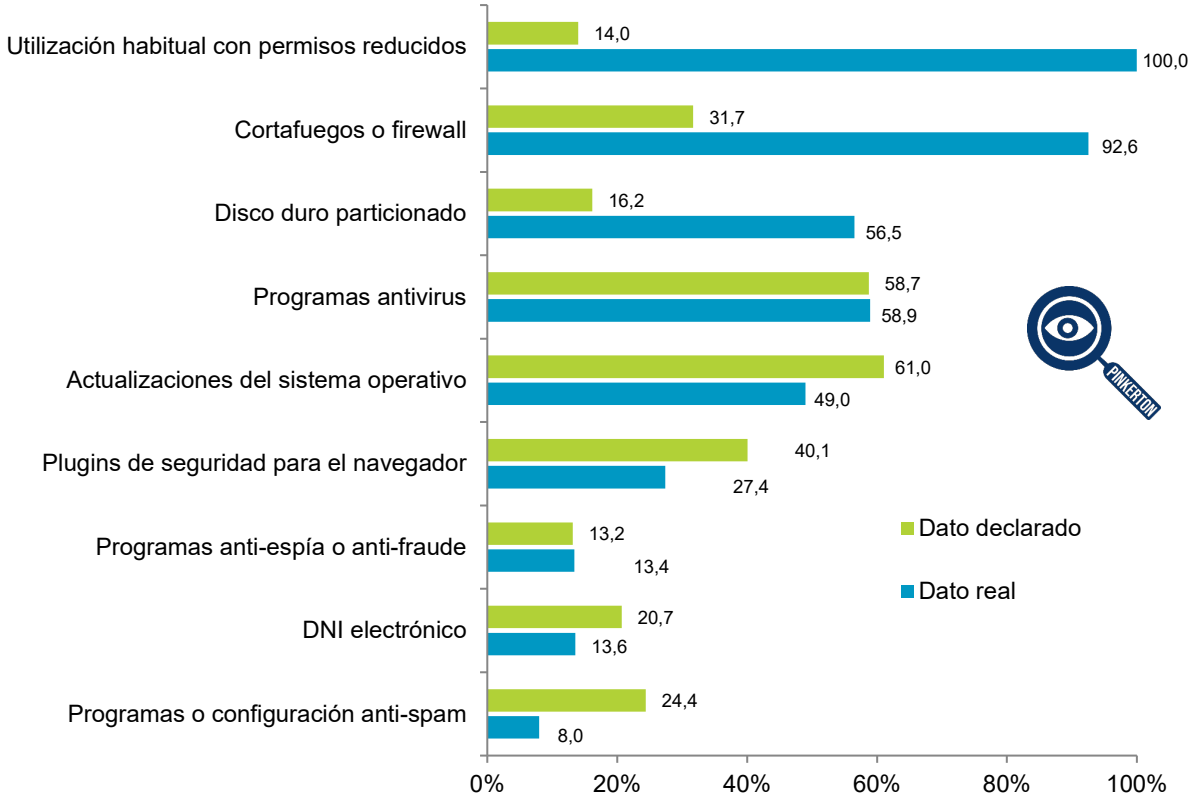


Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

Se aprecia que el uso de máquinas virtuales, que había crecido en el semestre anterior, vuelve a descender al 5.8%, es el menor porcentaje de las tres últimas oleadas. Esto podría deberse a que fueron una opción muy empleada para el trabajo en remoto y un gran número de empresas podrían prescindir de las mismas con la vuelta a la oficina. También podría verse condicionado por otros factores, como emplear las máquinas virtuales en los ordenadores del hogar para evitar la instalación de *software* empresarial o de otros ámbitos no domésticos en el equipo del hogar.

La percepción de los panelistas no siempre corresponde con lo que nos indica su ordenador. Se muestra a continuación (FIGURA 8) el contraste entre el uso declarado y el real conforme a los datos recopilados por el *software* Pinkerton.

FIGURA 8. USO DECLARADO VS REAL DE MEDIDAS DE SEGURIDAD EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

Aunque los usuarios tienen la percepción de que no usan sus dispositivos con permisos reducidos la realidad es que el 100% de los dispositivos analizados para la realización de este estudio lo tienen implementado y en uso. Este hecho puede deberse al desconocimiento de los usuarios de las mejoras implementadas en las actualizaciones del sistema operativo de la plataforma que usan.

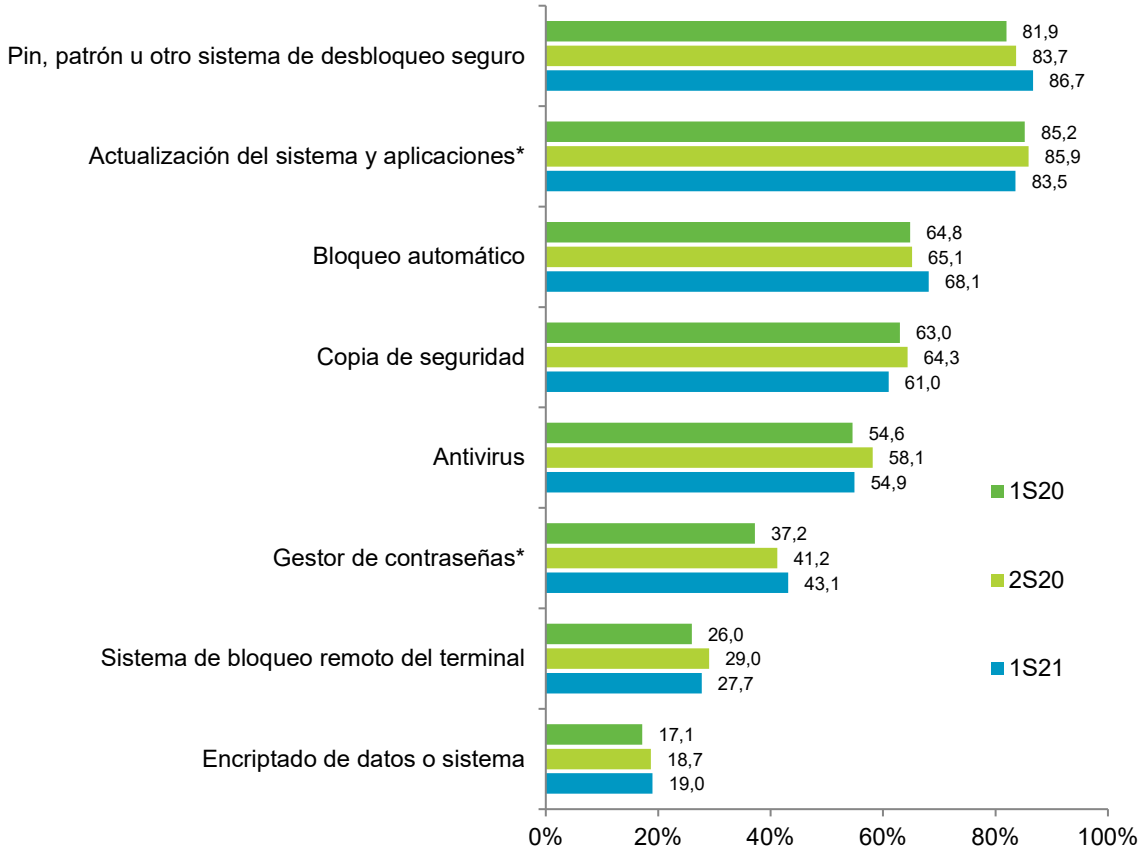
De igual modo destacan el uso de cortafuegos y el particionado de disco. En el caso del cortafuegos el 92,6% de los dispositivos analizados lo tiene activo y sin embargo tan solo el 31,7% de los usuarios afirmaba tenerlo activado.

Y en cuanto a la partición del disco duro, también es reseñable que tan solo el 16,2% de los usuarios afirmaran tener particionado su disco mientras que el análisis confirma que el 56,5% de los dispositivos tenía particionado el disco. Esto puede deberse al desconocimiento del usuario respecto de sus equipos o bien de la terminología técnica empleada.

4.2 Dispositivos Android

Por medio de los resultados mostrados en la FIGURA 9 se observa que medidas de seguridad como el uso de pin o patrón de desbloqueo (86,7%), el bloqueo automático (68,1%), el encriptado de datos (19,0%) y el uso de gestores de contraseñas (43,1%), continúa aumentando en dispositivos Android. Se aprecia una disminución considerable y preocupante en el uso de copias de seguridad y antivirus en estos sistemas por parte de los panelistas.

FIGURA 9. MEDIDAS DE SEGURIDAD EN DISPOSITIVOS ANDROID (%)



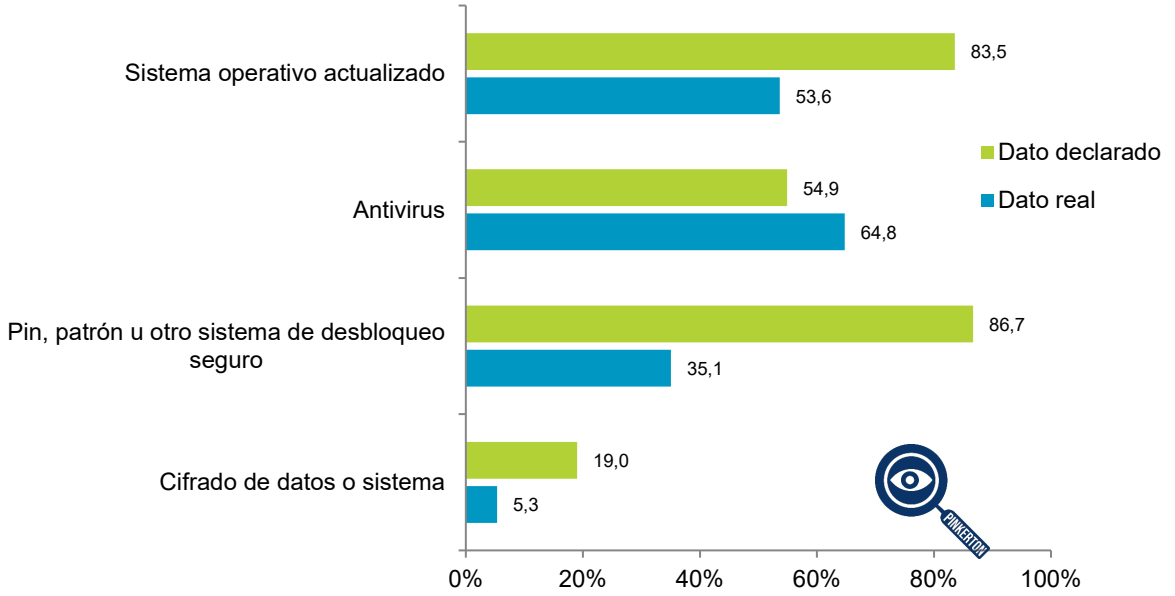
Base: usuarios de dispositivos Android
Fuente: Panel hogares, ONTSI

Es importante destacar el papel de las copias de seguridad ya que en caso de ser víctima de algún tipo de *ransomware*, se pueden recuperar los datos restaurando una copia de seguridad en muchos casos, si el *malware* no se ha extendido. Esta es de hecho la medida más efectiva para evitar encontrarse en el dilema de tener que pagar a los atacantes para recuperar los datos. Pero no solo en ese caso, sino en caso de pérdida o rotura del dispositivo, si se tiene una copia de seguridad, se puede restaurar en el dispositivo nuevo sin tener ninguna pérdida de información.

Aunque las últimas versiones de Android incluyen mejoras sobre la seguridad del dispositivo, no está libre de poder ser atacado. Los antivirus también ayudan a detectar cualquier tipo de *malware* porque suelen tener bases de datos actualizadas.

Respecto al contraste de las declaraciones de los usuarios Android respecto a lo que nos arroja el *software* Pinkerton sobre la configuración de los dispositivos, cabe destacar las aquellas identificadas en la FIGURA 10. En concreto, en torno al 83,5% de los panelistas considera que su dispositivo está actualizado, cuando los datos reales corresponden a un 53,6%. Esta falsa sensación de que el dispositivo se encuentra actualizado podría deberse a suponer que las actualizaciones del sistema son siempre automáticas o bien a no distinguir entre actualización de aplicaciones y actualización del sistema operativo.

FIGURA 10. USO REAL DE MEDIDAS DE SEGURIDAD EN DISPOSITIVOS ANDROID (%)



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

Una de las lecturas de la figura anterior es que los usuarios, en general, pueden sentirse más protegidos de lo que realmente están.

Esta falsa sensación de seguridad puede dar pie a conductas de riesgo que, unidas a las vulnerabilidades existentes a consecuencia de la no actualización del sistema operativo, podrían desencadenar en ataques efectivos contra las plataformas.

También se observa que la percepción de los panelistas respecto del *software* antivirus que protege su dispositivo es errónea, en tanto a que solo el 54,9% declara usar antivirus en su dispositivo, cuando los datos reales arrojan que el 64,8% de los dispositivos tiene esta medida de protección, que podría venir incluida como parte de las medidas nativas de protección de los nuevos sistemas operativos.

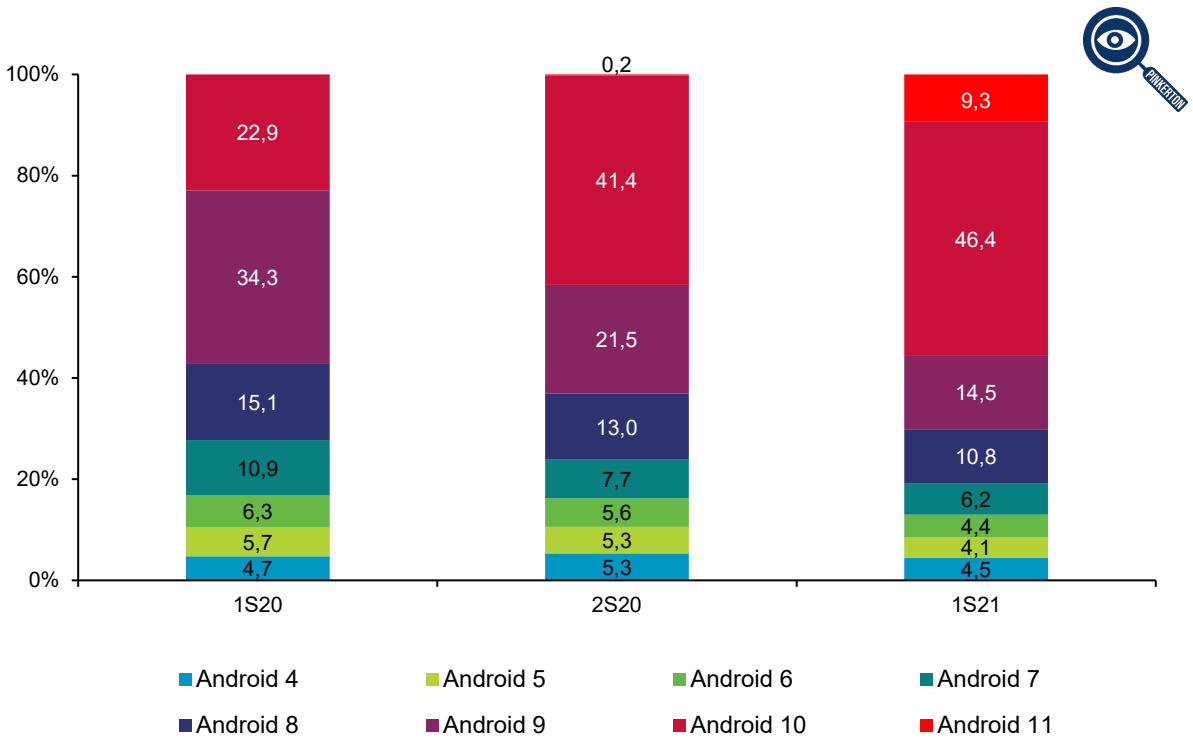
Respecto del semestre anterior los panelistas que disponen de la última versión de Android aumentan 9,2 puntos porcentuales.

Aunque el aumento es significativo no deja de ser insuficiente considerando que Android 11 está disponible en el mercado desde el 11 de septiembre de 2020. Cabe recordar que Android 11 trae consigo mejoras no solo funcionales sino también de privacidad y seguridad. Entre éstas se encuentran:

- La auto revocación de permisos (la aplicación pierde los permisos concedidos pasado un tiempo sin uso), APIs de auditoría de acceso a los datos para los desarrolladores, la obligatoriedad de almacenamiento específico (las aplicaciones solo pueden acceder a su propia carpeta), mejoras en el control de acceso a los datos mediante biométricos

- Las credenciales de identidad, que permiten llevar identificadores físicos (p.ej. DNI, carnet de conducir) en nuestro dispositivo.

FIGURA 11. VERSIONES DE ANDROID EN DISPOSTIVOS MÓVILES (%)



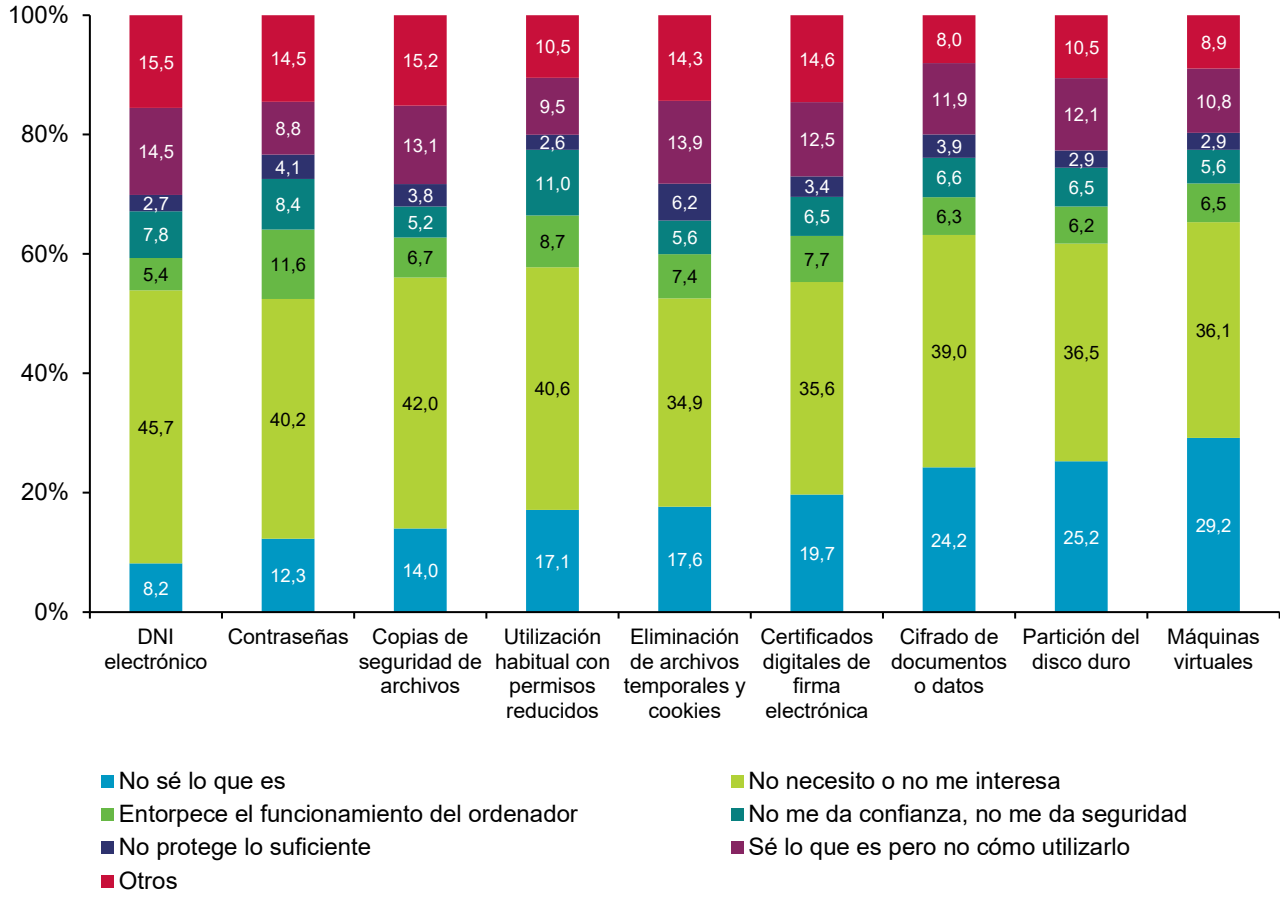
Base: usuarios de dispositivos Android
Fuente: Panel hogares, ONTSI

4.3 No utilización de medidas de seguridad

En este apartado se analizarán cuáles son los motivos para no utilizar las medidas de seguridad sujetas al estudio. Las declaraciones de los panelistas se recogen a continuación, sintetizadas en la FIGURA 12.

Cabría destacar que el DNI electrónico se encuentra entre las medidas de seguridad más conocidas por los panelistas, donde solo el 8,2% no sabe lo que es.

FIGURA 12. MOTIVOS DE NO UTILIZACIÓN DE MEDIDAS DE SEGURIDAD (%)



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

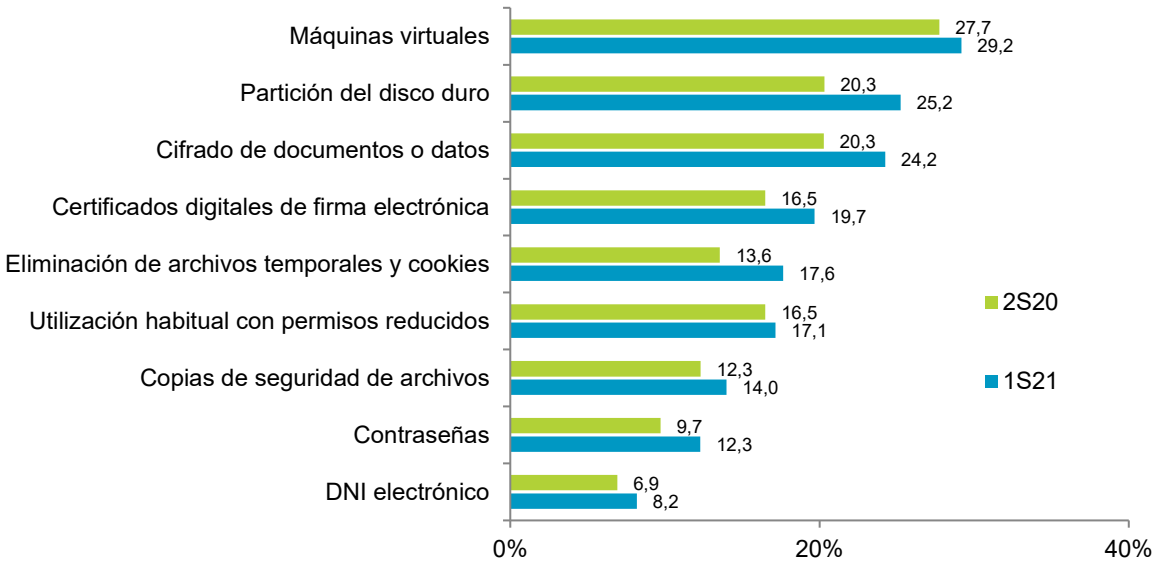
La más desconocida corresponde al uso de máquinas virtuales (29,2% de desconocimiento). Por otro lado, pese a ser la más desconocida, no es la que los usuarios estimen menos necesaria. Ese escalafón corresponde, precisamente, al DNI electrónico (45,7%).

Respecto al resto de medidas, cabe destacar que aún un 12,3% de usuarios no tiene claro qué son las contraseñas o aspectos no solo de seguridad sino de usabilidad y prevención, como las copias de seguridad de archivos (14%). Este dato puede que no sea mayor gracias a los esfuerzos de las compañías por proporcionar a los usuarios mecanismos cada vez más flexibles para sus copias de seguridad.

No obstante, la amplia mayoría consiste en copias en los sistemas *Cloud* externos a la red de los usuarios, protegidos por terceras partes.

Este punto debe considerarse con cautela, ya que, aunque la seguridad en estos sistemas mejora cada día, se conocen casos previos en los cuales no es necesario vulnerar la seguridad de los equipos y dispositivos para hacerse con los datos, sino que apuntan precisamente a los sistemas de terceros.

FIGURA 13. COMPARACIÓN DEL DESCONOCIMIENTO EN LAS MEDIDAS RESPECTO AL SEMESTRE ANTERIOR (%)



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

La FIGURA 13 compara el desconocimiento en las medidas de seguridad respecto al semestre anterior. En este semestre un mayor número de panelistas aseveran desconocer el significado de las medidas de ciberseguridad. La única diferencia en dicho punto respecto al semestre anterior radica en que la utilización habitual con permisos reducidos se encuentra en el cuarto puesto de medidas menos desconocidas con un 17,1%, pero este cuarto puesto puede estar motivado por el aumento del desconocimiento para el resto de medidas. Este aumento puede deberse a conceptos que podrían tener falsamente asumidos y que confunden una vez que necesitan ponerlos en práctica.

Es importante destacar que, conforme la FIGURA 3, el uso de Internet para participar en cursos de formación aumenta, pero, sin embargo, esto no se ve reflejado en un mayor conocimiento en los mecanismos de ciberseguridad. Por ello, parece plausible suponer que los usuarios no están participando en cursos dirigidos al uso de estos mecanismos, y que, por el contrario, diferentes hábitos estén motivando confusión al respecto sobre la terminología o el ámbito de aplicación de los mismos.

Dicha hipótesis se ve reforzada por el resto de declaraciones de los panelistas, en las que "saber lo que es pero no cómo utilizarlo" no parece ser el motivo más destacado por los usuarios para no emplear los mecanismos.

Debe destacarse también que el 45,6% de los panelistas no considera necesario el DNI-e (FIGURA 3), y sin embargo, en este estudio, en la FIGURA 13, es precisamente uno de los hábitos que

se ven reforzados. La tendencia de la administración pública suele venir acompañada de nuevas vías de autenticación en los portales Web que prestan los servicios a los ciudadanos, donde se tiende a facilitar el acceso. El DNI-e no suele ser el medio más empleado, por diversos motivos, destacando entre algunos de ellos su dificultad de instalación.

Este último es más reciente que las declaraciones realizadas por los panelistas en este estudio, pero sí un claro reflejo de la tendencia a facilitar el acceso que puede hacer que medidas de seguridad como el DNI-e puedan caer en desuso si se ofrecen alternativas al mismo.

También puede verse mermada la necesidad de estos mecanismos por el alejamiento de los servicios de Internet destacados en la FIGURA 3.

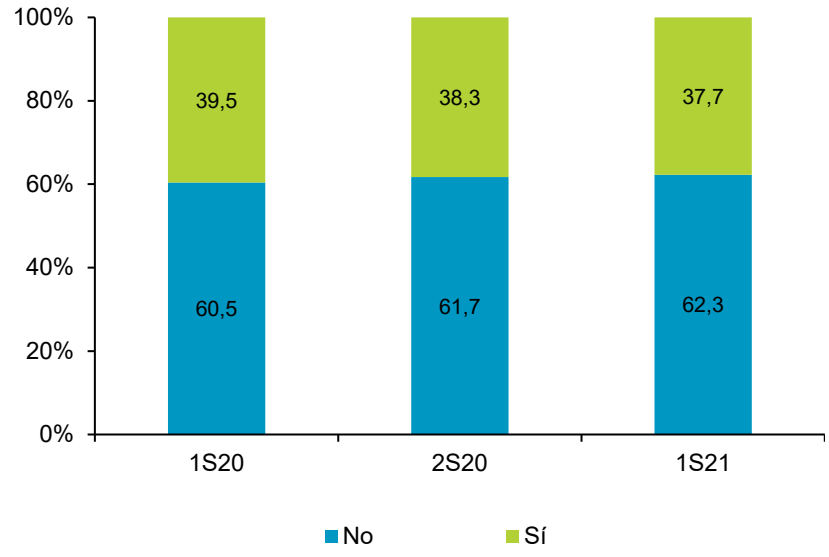
5 Hábitos de comportamiento en la navegación y usos de Internet

En esta sección ponemos el foco en los hábitos de comportamiento de los internautas. Estudiar el comportamiento en la red, las conductas de riesgo asumidas y el grado de conocimiento de sus repercusiones es fundamental para identificar puntos de mejora para futuras guías y campañas de concienciación.

5.1 Evolución de las conductas de riesgo

La evolución de las conductas de riesgo continúa su mejoría respecto a los semestres anteriores. En concreto la FIGURA 14 refleja que el 62,3% de los usuarios declaran no realizar conductas de riesgo de forma consciente, lo que supone una mejora porcentual de 0,6 p.p., manteniendo por lo tanto su progresión ascendente.

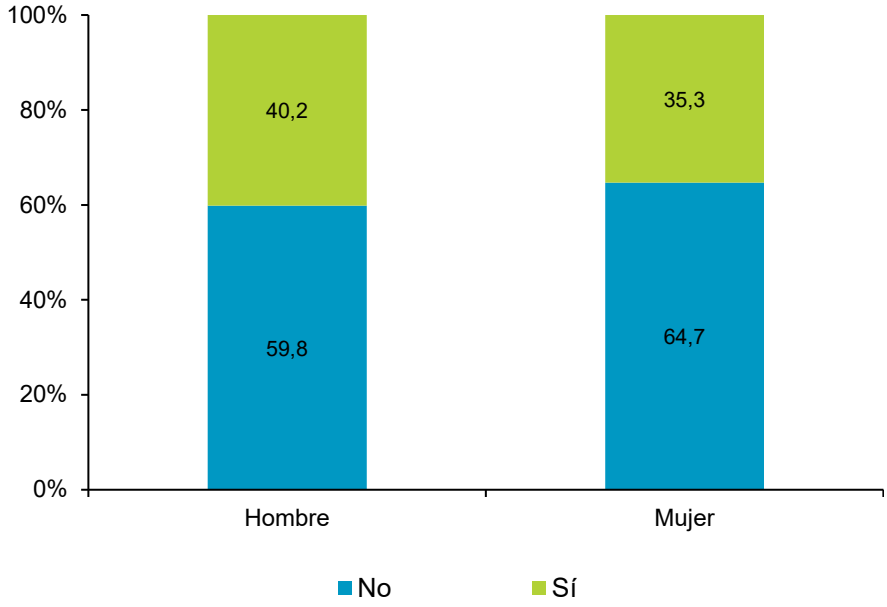
FIGURA 14. EVOLUCIÓN DE LA ADOPCIÓN CONSCIENTE DE CONDUCTAS DE RIESGO (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

Si estudiamos la realización consciente de conductas de riesgo desde una perspectiva de género (FIGURA 15) los hombres afirman en un 59,8% no realizar, de forma consciente, conductas de riesgo mientras que el porcentaje en las mujeres es 4,9 p.p. mayor.

FIGURA 15. REALIZACIÓN CONSCIENTE DE ALGUNA CONDUCTA DE RIESGO CONFORME POR GÉNERO (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

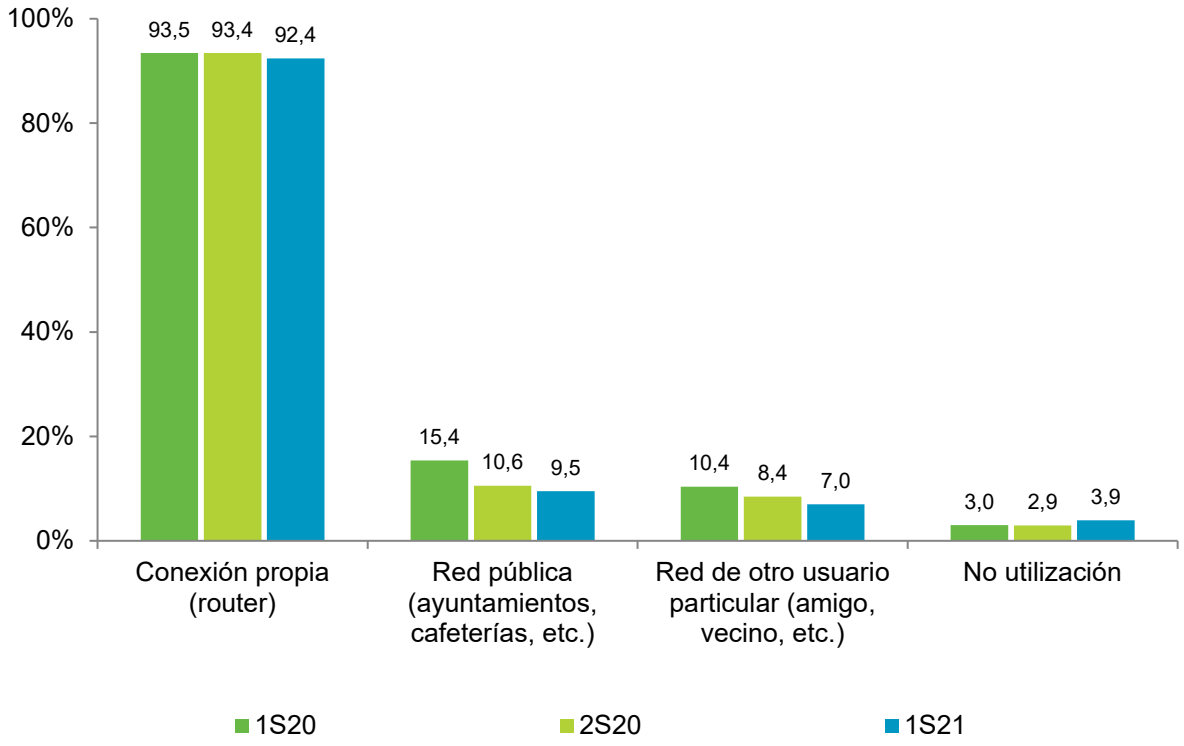
Una de las conductas de riesgo que cada vez tienen más asimiladas los usuarios es el uso de redes Wi-Fi públicas abiertas o de otros usuarios. Quizás por ese motivo cada vez menos usuarios las eligen cuando necesitan conectarse a Internet. Además, se encuentra el factor de la bajada de tarifas móviles, que incluyen en muchos casos la conectividad a Internet, casi como un derecho ya adquirido por la sociedad.

Las redes públicas en centros comerciales, locales de ocio o aeropuertos, suelen ser redes abiertas. Los peligros que entrañan estas redes son el robo de datos que son transmitidos porque pueden ser leídos por cualquier tercero con acceso. Además, un atacante que lograse acceder al dispositivo conectado a la red pública podría robar los datos almacenados en el dispositivo con el que el usuario se conecta a la red Wi-Fi abierta.

En este estudio se ha realizado una comparativa entre las declaraciones de los usuarios entrevistados en los semestres de 2020 y los entrevistados en este primer semestre de 2021.

Dicha comparativa se puede observar en la FIGURA 16, que muestra cómo ha descendido en 1,1p.p. el uso de estas redes, lo cual es una buena noticia ya que los usuarios comienzan a concienciarse sobre los peligros que entraña el uso de redes abiertas.

FIGURA 16. UTILIZACIÓN DE REDES WI-FI PRIVADAS Y PÚBLICAS (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

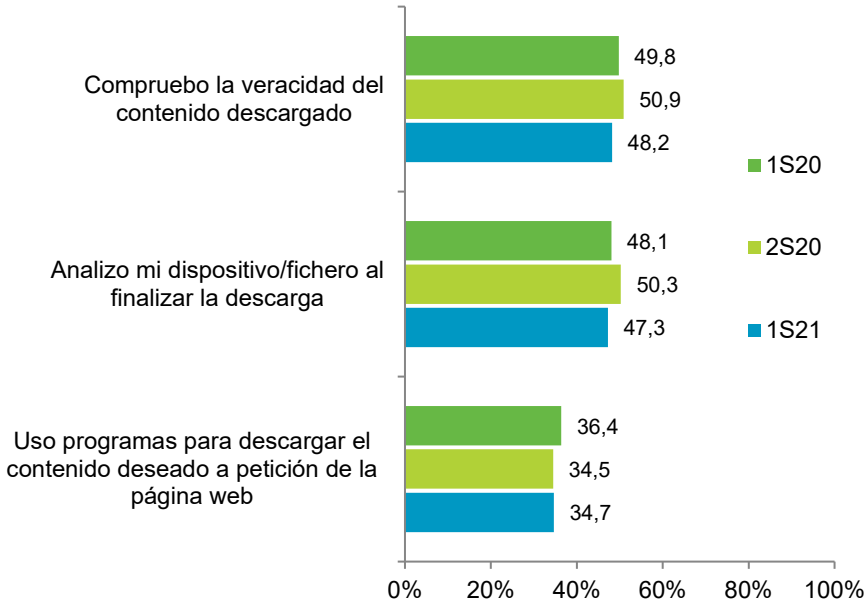
Quizás estas mejoras también sean fruto de las campañas publicitarias que realiza INCIBE en medios de comunicación, en su web y en sus redes sociales (por ejemplo la campaña https://www.incibe.es/hoyesunanuncio)

5.2 Descargas e instalación de programas.

En esta parte del estudio se evalúa si los usuarios tienen buenos hábitos cuando descargan contenido de Internet ya sea mediante descarga directa o bien empleando redes P2P.

Para ello, se estudian los hábitos que tienen tras las descargas, es decir, si comprueban la veracidad de lo que han descargado y si realizan algún tipo de análisis antivirus a esos archivos antes de ejecutarlos. También se analiza el comportamiento que afirman tener los usuarios cuando instalan un nuevo programa en el PC, si se fijan en los pasos que siguen y si leen las políticas de uso. Pero no solo se valoran los hábitos de descarga en PC sino también en dispositivos Android. Se realiza un análisis de los hábitos de descarga de fuentes oficiales o no oficiales para ver el comportamiento de los usuarios.

FIGURA 17. USO DE DESCARGA DIRECTA DE ARCHIVOS, PROGRAMAS, DOCUMENTOS, ETC. (%)



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

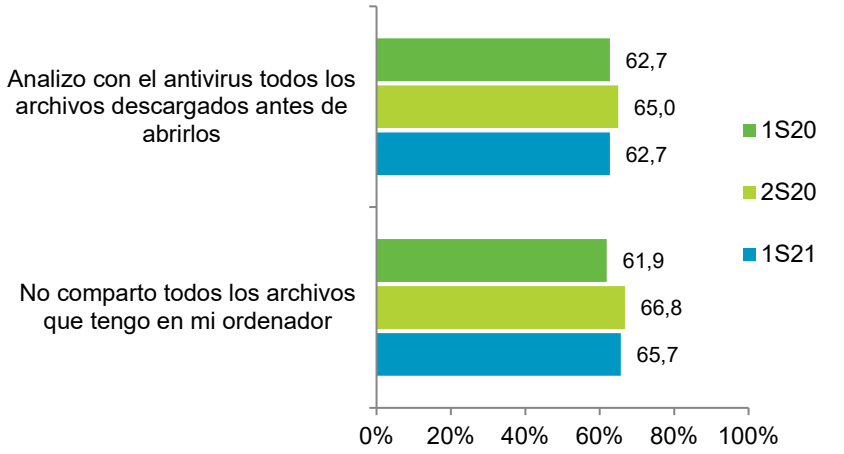
En las declaraciones de los usuarios (FIGURA 17) se ha notado un descenso en el uso de herramientas de análisis de virus para analizar los ficheros que descargan. Además el 48,2% afirma que no comprueba la veracidad del contenido descargado.

Es necesario que los usuarios se habitúen a realizar buenas prácticas cuando descargan contenido de Internet (https://www.osi.es/es/webs-de-descarga). Se debe analizar el contenido del fichero descargado bien con el antivirus instalado en el equipo o comprobando online en páginas como VirusTotal (https://www.virustotal.com/gui/) donde se emplean diferentes antivirus para analizar el fichero en cuestión de segundos y saber si contiene algún tipo de carga maliciosa o está limpio.

La ciudadanía debe prestar atención y cuidado con las webs de descarga directa, ya que habitualmente tienen *banners* de publicidad, imágenes o mensajes que lo que buscan es el clic del usuario, bien para redirigirle a otras páginas o bien para realizar descargas en su equipo de ficheros que pueden ser maliciosos. Para saber exactamente donde llevan esos enlaces una buena práctica es hacer uso de un analizador de enlaces URL.

Por otra parte, el hábito de analizar los archivos descargados cuando se usan redes P2P ha sufrido un retroceso según las declaraciones de los usuarios. En el semestre anterior los panelistas mostraban mayor preocupación por analizar los archivos descargados. En concreto este hábito de comprobación ha descendido en 2,3 p.p. respecto al anterior semestre como se ve en la FIGURA 18.

FIGURA 18. HÁBITOS DE COMPORTAMIENTO EN EL USO DE REDES P2P (%)



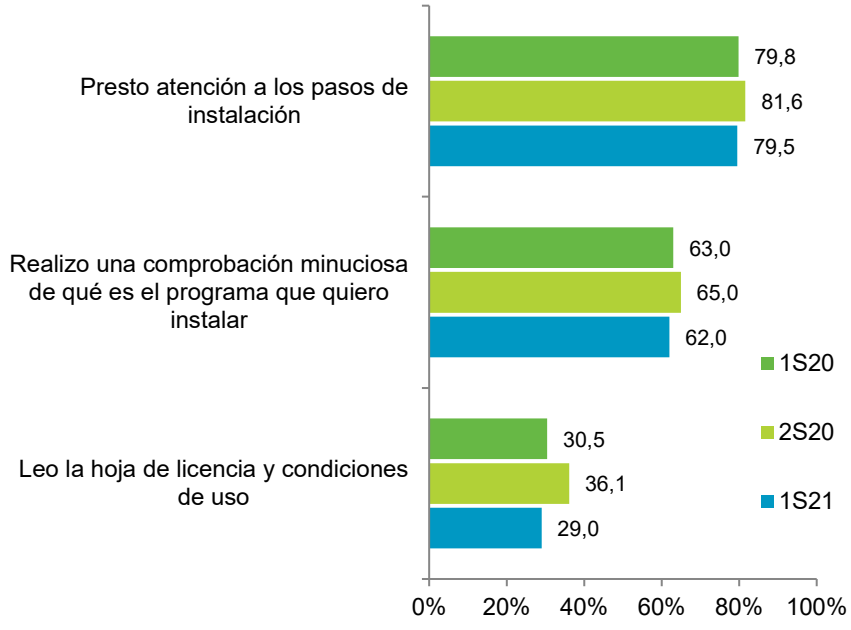
Base: usuarios de redes P2P
Fuente: Panel hogares, ONTSI

Los datos indican que se experimenta una mejora respecto a la compartición de datos con terceros. El 65,7% de los usuarios declara no compartir todos los archivos que tienen en su ordenador.

Tanto el no emplear el antivirus para el análisis (FIGURA 17) como la no verificación de las descargas (FIGURA 18) podrían ser hábitos relacionados. En general, conforme a los datos confesados por los usuarios, los hábitos en la descarga directa han empeorado respecto al semestre anterior.

Tras la descarga y análisis de los programas llega la fase de la instalación del *software* y en este estudio también se han analizado los comportamientos que declaran tener los usuarios a la hora de instalar *software* en sus PC's (FIGURA 19).

FIGURA 19. INSTALACIÓN DE PROGRAMAS (%)



Base: usuarios de PC

Fuente: Panel hogares, ONTSI

Es práctica habitual según declaraciones de los usuarios el prestar atención a los pasos que se van realizando durante la instalación de los programas. No obstante, aunque en este semestre el 79,5% de usuarios admite prestar atención a los pasos de instalación, esta cifra sufre un descenso de -2,1 p.p. respecto al semestre anterior.

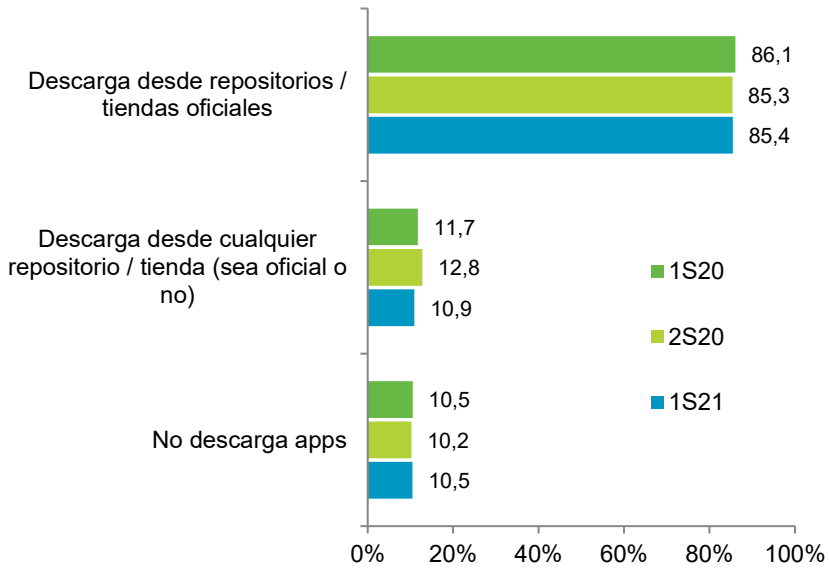
Uno de los primeros pasos durante la instalación de cualquier *software* es la aceptación de la licencia y condiciones de uso. Un dato esperanzador es que el 29% de los usuarios afirma que continúa leyéndola antes de aceptarla.

En algunos pasos de la instalación de *software* a veces se añade *software* de terceros o incluso *software* que puede ser malicioso y si no se presta atención a los pasos de instalación y de manera automática se pasan todas las etapas por alto, se puede llegar a comprometer el equipo. Si a esta práctica además se le añade el descenso de -3 p.p. en la realización de comprobaciones para verificar que es el programa que se quiere instalar, significa que los usuarios están instalando programas sin saber el contenido y si realmente es el programa que necesitan o no.

Continuando con las descargas, el 85,4% de los usuarios con dispositivos Android declara descargar desde repositorios o tiendas oficiales. Lo que hace destacar una mejora en este hábito respecto al semestre anterior (FIGURA 20).

Aunque hay documentados de troyanos que se podía descargar desde Google Play, no son los más habituales, y por lo general que los markets oficiales siempre estarán más controlados que cualquier otro sitio web de terceros.

FIGURA 20. HÁBITOS EN LA DESCARGA DE APLICACIONES EN ANDROID (%)



Base: Usuarios que disponen de dispositivo Android
Fuente: Panel hogares, ONTSI

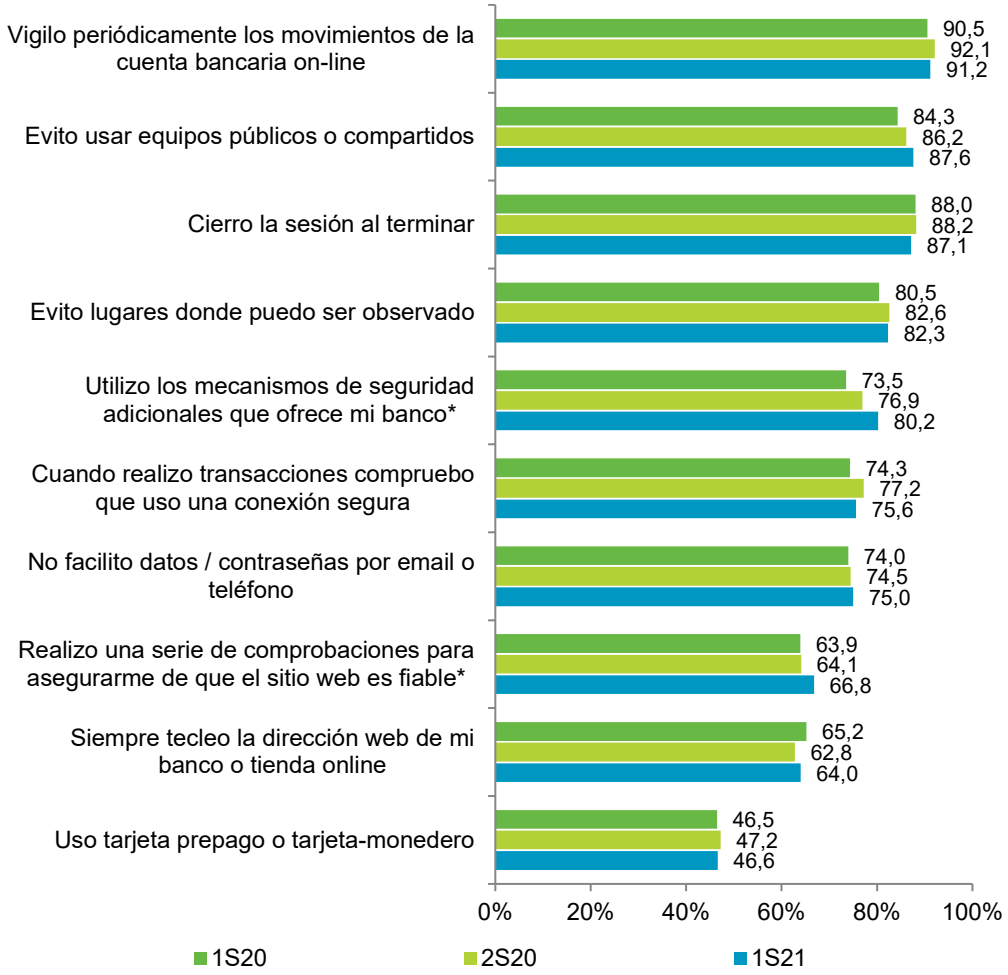
La variación de usuarios que no descarga aplicaciones vuelve a situarse en el 10,5%, como ya ocurriese en el primer semestre de 2020. Aun así ha aumentado muy levemente con respecto al segundo semestre de 2020.

5.3 Evolución de los hábitos en los servicios

El comportamiento de los usuarios respecto a los servicios que las entidades públicas y comercios ponen a su disposición es motivo de estudio, tanto para conocer los intereses de los usuarios como para valorar las medias de seguridad que toman usando determinados servicios.

Es por eso que esta parte del estudio se centra en conocer el comportamiento de los usuarios cuando usan la banca o el comercio electrónicos. Además se analizan las prácticas que llevan a cabo cuando realizan publicaciones en redes sociales.

FIGURA 21. HÁBITOS DE COMPORTAMIENTO EN EL USO DE SERVICIOS DE BANCA ONLINE O COMERCIO ELECTRÓNICO (%)



Base: usuarios que utilizan la banca online y/o comercio electrónico
Fuente: Panel hogares, ONTSI

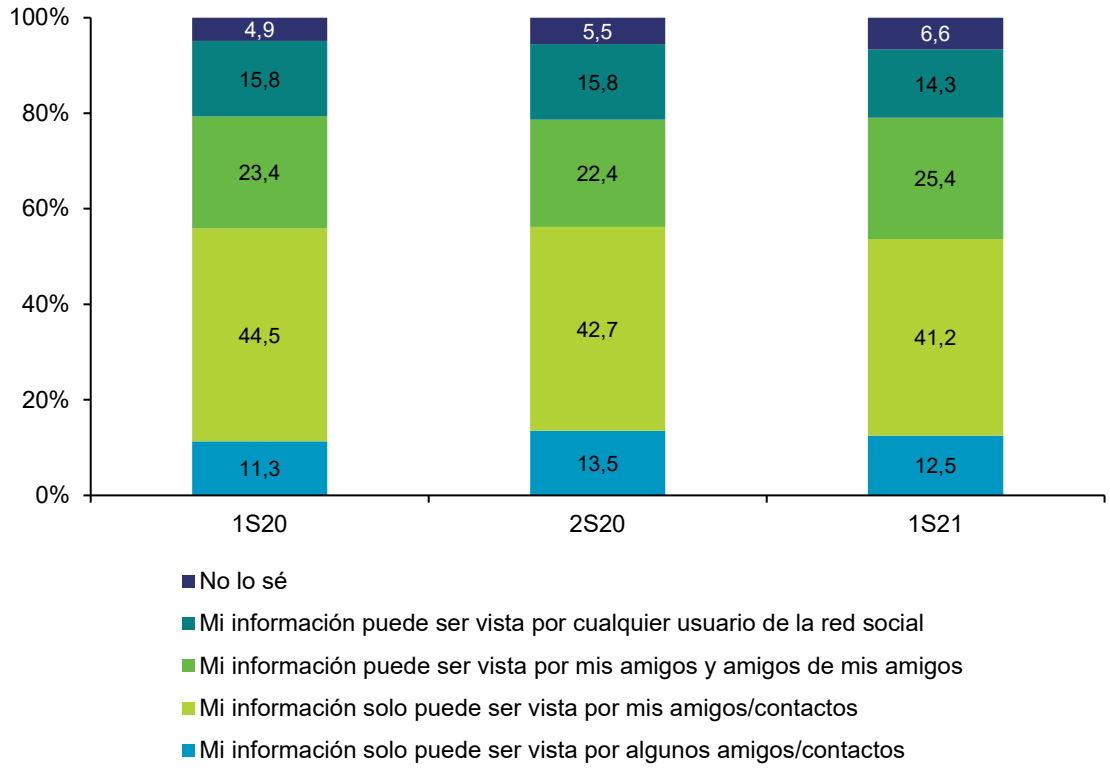
Cada vez es más común que los servicios de banca online implementen medidas de seguridad como el registrar terminales seguros para el usuario en cuestión, tener doble factor de autenticación para acceder a la banca online, emplear medidas biométricas, además de permitir desactivar la tarjeta de crédito o débito desde la aplicación si no se va a usar, entre otras.

El uso de las nuevas medidas de seguridad de entidades bancarias está obligando a los usuarios a emplearlas. En este semestre (FIGURA 21), se puede observar un aumento de 3,3 p.p. con respecto a la anterior.

La mejora de la conducta de los panelistas con relación al compartir datos o contraseñas por Internet, realizar comprobaciones para verificar la fiabilidad de la web que visitan y teclear la web del banco en lugar de hacer clic sobre los resultados de búsqueda sigue aumentando levemente. Quizás pueda ser debido a las campañas *anti-phishing* que se han ido realizado a lo largo del semestre.

El peligro del hábito de compartir contraseñas por correo o por teléfono (FIGURA 21) es extensible a las redes sociales. Pero no solo es peligroso compartir contraseñas sino también información personal o que pueda resultar sensible. En esta línea han respondido los usuarios según los resultados que se registran en la FIGURA 22.

FIGURA 22. HÁBITOS DE COMPORTAMIENTO EN EL USO DE REDES SOCIALES (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

El 6,6% de los usuarios manifiesta que la información que comparten en redes sociales es pública y puede verla cualquiera. Se puede observar un aumento de 1 p.p. respecto al semestre

anterior. También aumenta en 3 p.p. respecto al semestre anterior los usuarios que comparten el contenido de sus redes con amigos y amigos de sus amigos. El uso de las redes sociales para comunicarse con familiares y amigos incrementó en el semestre anterior y en este sigue siendo un medio de comunicación muy utilizado.

Es por tanto necesario vigilar lo que se comparte en las redes, y sobre todo ajustar la privacidad, si es posible, una buena práctica es marcar las opciones de las redes sociales para no permitir indexar información de nuestro perfil en Google (Esta opción no está disponible en todas las redes sociales).

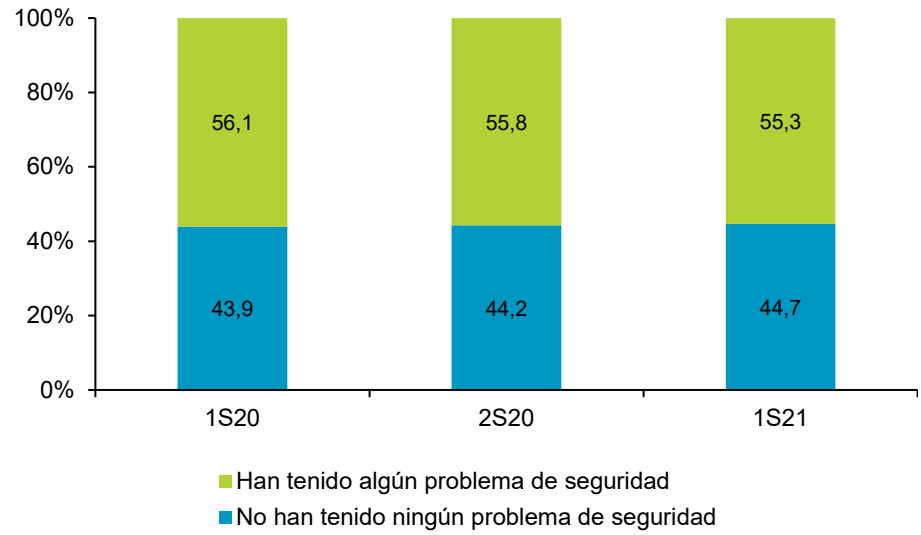
6 Incidentes de seguridad

Esta sección se centra en analizar los resultados relativos a los incidentes de seguridad. Se emplean tanto los resultados de las encuestas (opiniones/percepciones de los panelistas) como los datos reales recopilados por el *software* de escaneo de dispositivos Pinkerton.

6.1 Evolución de las incidencias

Conforme a los datos que arroja la FIGURA 23, la variación respecto al semestre anterior (2S20) en el número de panelistas que afirman haber sufrido una incidencia es de -0,5 p.p. Significa, que disminuyen los usuarios que declaran haber sufrido alguna incidencia de seguridad.

FIGURA 23. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



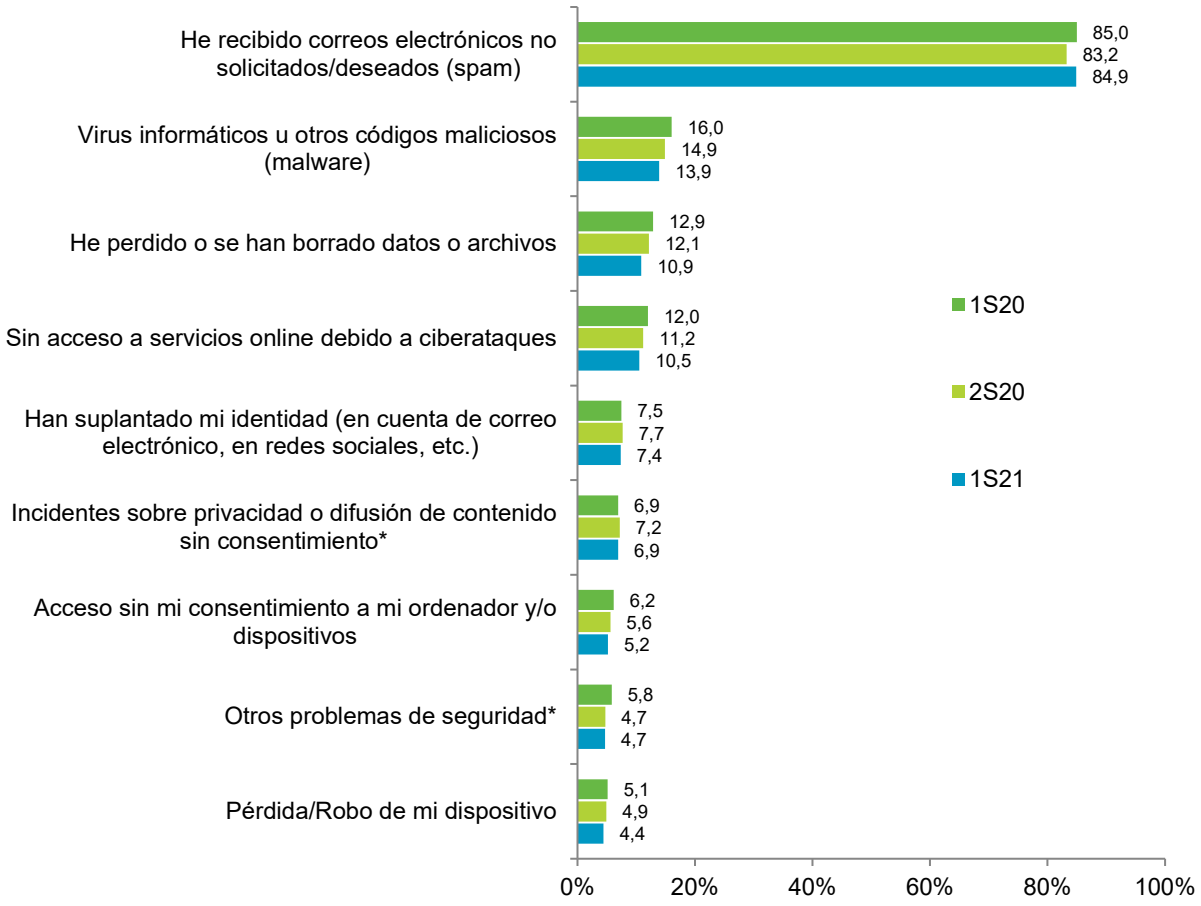
Base: Todos los usuarios
Fuente: Panel hogares, ONTSI

No obstante, la cifra se mantiene por encima del 50%. Concretamente, El 55,3% de los panelistas afirma haber sufrido alguna incidencia de ciberseguridad durante este semestre, frente al 55,8% del semestre anterior. Este hecho puede deberse al aumento de los usuarios que declaran que verifican el origen de las aplicaciones antes de instalarlas. Al prestar más atención a dichos

permisos, los usuarios pueden adquirir una falsa sensación de seguridad.

Por otra parte, la FIGURA 24 refleja la evolución de las incidencias de seguridad, en base a la clasificación de eventos más comunes, dirigidos a los usuarios e identificables por éstos. Para dicha valoración se consideran únicamente los usuarios que han sufrido alguna incidencia de seguridad.

FIGURA 24. EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



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

Pese a que en el anterior semestre los usuarios experimentaron un descenso de los correos electrónicos no deseados, en este semestre han vuelto a aumentar los casos identificados por los panelistas (+1,7 p.p.).

En el resto de incidencias de seguridad se observa un descenso que deberemos comparar con los datos reales recabados por el *software* Pinkerton, para aquellos casos para los que podamos emplear el dato real. Como no siempre va a ser posible establecer la correspondencia con medidas reales, o bien estas pueden ser más tardías, es primordial que los usuarios estén cada vez más formados en ciberseguridad para poder identificar las incidencias de seguridad de forma temprana.

Dicho de otra forma, si la bajada de detección de incidencias observadas corresponde con los datos reales, entonces estaremos frente a una mejora paulatina de la seguridad. Sin embargo, si corresponde a una falsa sensación de seguridad, no serán buenas noticias, dado que significaría que los panelistas identifican cada vez peor las incidencias. Por ejemplo, en el caso del *malware*, esto podría deberse a que las nuevas muestras de *malware* mejoren sus técnicas de ocultación y propagación.

¿QUÉ ES EL MALWARE?

Software malintencionado cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del usuario.

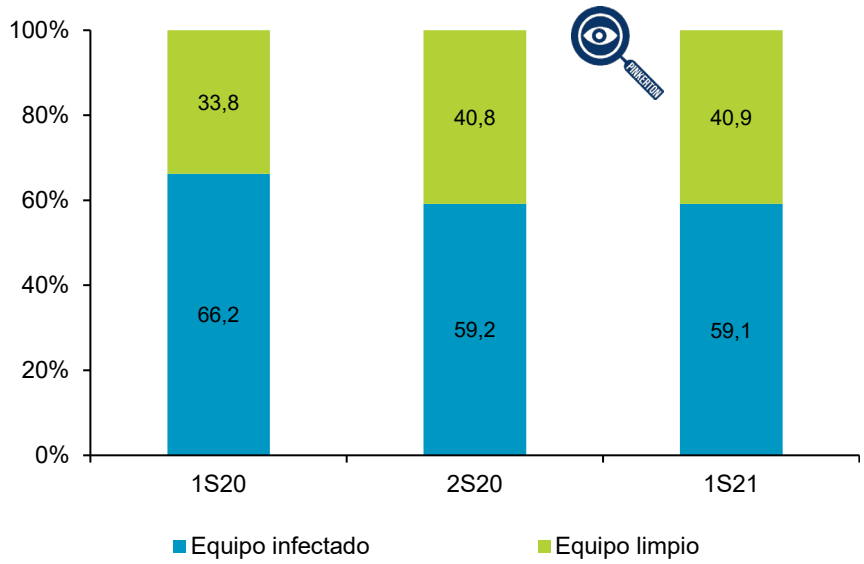
6.2 Infecciones por *malware*

Centramos la atención en los datos reales arrojados sobre las infecciones por *malware*.

6.2.1 Malware en el ordenador del hogar

La FIGURA 25 muestra la evolución del *malware* identificado en los ordenadores del hogar. Se aprecia que no hay cambios significativos en cuanto al número de ordenadores del hogar infectados, ya que prácticamente se mantiene estable con respecto a los datos observados en el semestre anterior, con una diferencia de -0,1p.p.

FIGURA 25. ESTADO REAL DE INFECCIÓN EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

ORDENADORES QUE ALOJAN MALWARE Y SU PELIGROSIDAD

59,1%
DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE

75,5%
DEL MALWARE DETECTADO PRESENTA UN NIVEL DE RIESGO ALTO

No obstante, el 59,1% de los equipos escaneados sigue siendo una cifra elevada, cuando de hecho en la FIGURA 24 solo el 13,9% de los panelistas afirmaba sufrir este tipo de incidencia de seguridad.

Respecto a la peligrosidad, sí se ha observado un aumento de 3,5 puntos porcentuales respecto al semestre anterior de *malware* clasificado como de riesgo alto.

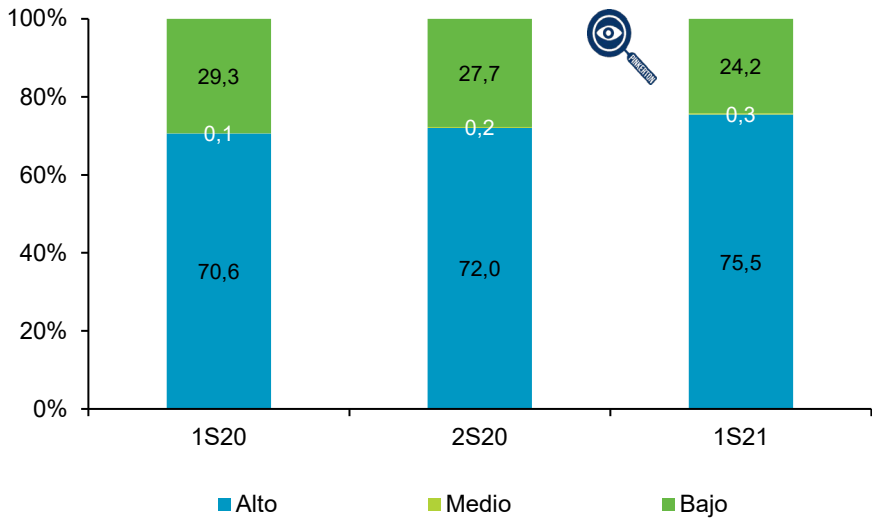
Cabe recordar que la peligrosidad alta se aplica a *malware* que, potencialmente, permite el acceso remoto por parte de un atacante

al sistema víctima; puede suponer un perjuicio económico para el usuario; facilita la captura de información confidencial o sensible de la víctima; se emplea como pasarela para atacar otros equipos (pudiendo acarrear consecuencias legales para la víctima); o mina el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.

También se puede observar un leve aumento en el *malware* de peligrosidad media (+0,1p.p. respecto al semestre anterior). Este tipo de *malware* no perjudica de forma notoria el rendimiento de los equipos. Ejemplos de este tipo de incidencia de seguridad es cuando se abren ventanas no deseadas al navegar, se incrustan publicidad en páginas web legítimas que realmente no contienen publicidad o se crean patrones de navegación para crear perfiles de publicidad dirigida.

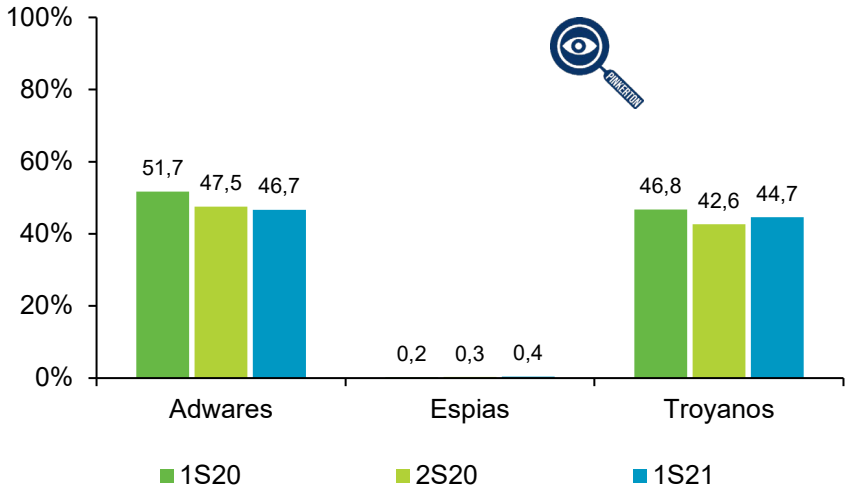
Por lo que, aunque el porcentaje de equipos con *malware* se mantiene con pocas variaciones (59,1%, FIGURA 25), la peligrosidad del *malware* sí da un salto más notorio respecto al semestre previo (FIGURA 26). Respecto a la tipología del *malware* detectado, la FIGURA 27 refleja los datos observados por el *software* de escaneo.

FIGURA 26. PELIGROSIDAD DEL *MALWARE* EN EL ORDENADOR DEL HOGAR (%)



Base: Total de ordenadores infectados
Fuente: Panel hogares, ONTSI

FIGURA 27. EVOLUCIÓN DEL *MALWARE* EN EL ORDENADOR DEL HOGAR (%)



Base: Total ordenadores
Fuente: Panel hogares, ONTSI

En cuanto a la evolución por tipo de *malware* (FIGURA 27) aumenta el porcentaje de muestras que corresponde a troyanos (44,7%), mientras que disminuyen los *adwares* (46,7%). Estos últimos se destinan a ofrecer anuncios a los usuarios, y no tienen un interés particular en el malfuncionamiento del equipo.

Los troyanos, por otro lado, suelen venir acompañados de otro *malware* más nocivo, como por ejemplo, pueden servir para camuflar puertas traseras y comunicaciones con servidores de que podrían permitir el despliegue de *ransomware* tras efectuar otras operaciones.

Por último, la siguiente tabla resume las incidencias de *malware* en el ordenador del hogar. En concreto, se destaca especialmente que el 50% de los panelistas no era consciente de tener *malware* en su ordenador. Este valor es el más preocupante, dado que puede inducir a una falsa sensación de seguridad que alimente las conductas de riesgo. Los panelistas que afirmaron tener *malware* (y que realmente lo tenían) suponen un 9,1%.

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

Declararon tener malware en PC	Su PC presentaba malware		
	Sí	No	Total
Sí	9,13%	3,04%	12,17%
No	50,00%	37,83%	87,83%
Total	59,13%	40,87%	100,00%

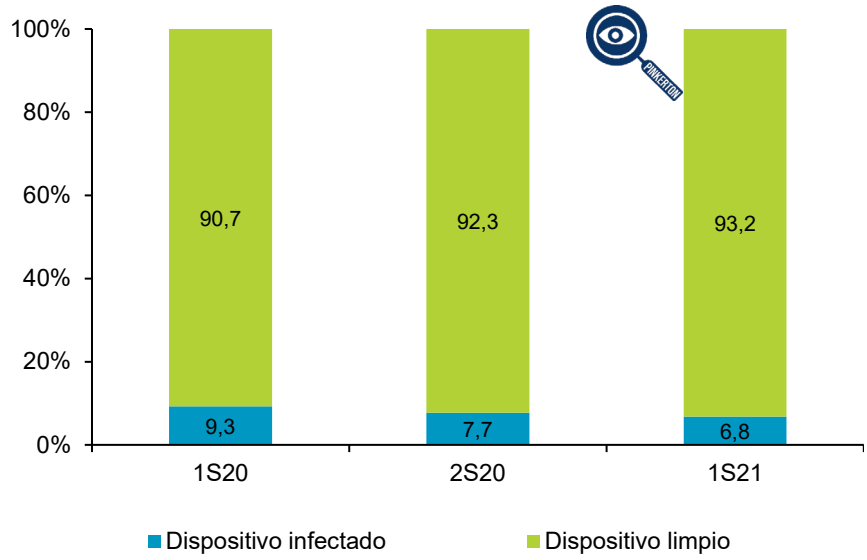
Base: usuarios con PC escaneado
Fuente: Panel hogares, ONTSI

6.2.2 Malware en dispositivos Android

En el caso de la progresión del *malware* en dispositivos Android, se registra un descenso en los casos de infecciones por *malware* en estos dispositivos.

Las sucesivas mejoras en las versiones de Android, las actualizaciones y el bajo nivel de privilegio de los dispositivos con versiones de Android 7 en adelante, contribuyen en la mejora de la seguridad de los dispositivos.

FIGURA 28. ESTADO REAL DE INFECCIÓN EN DISPOSITIVOS ANDROID (%)



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

Así, el 6,8% de los dispositivos analizados está infectado con *malware*. Respecto a esos dispositivos infectados, en torno al 66,1% contiene *malware* de peligrosidad alta, conforme los datos arrojados por la FIGURA 29. No obstante, se vuelve a experimentar una bajada con respecto a los semestres anteriores. La diferencia con respecto al semestre anterior es de 1.5 p.p. situándose en el 66,1% de equipos infectados con *malware* de peligrosidad alta.

EVOLUCIÓN DEL MALWARE EN PC Y ANDROID PARA 1S21

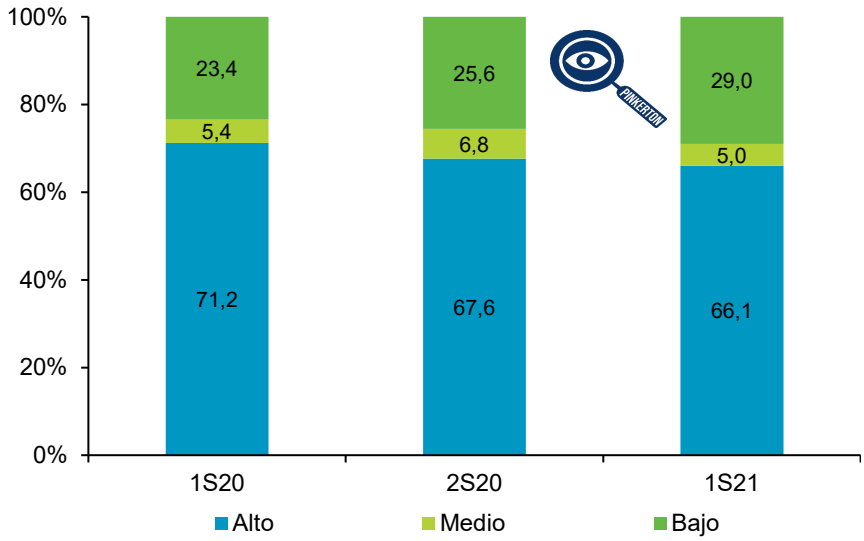
Troyanos & Espías

AUMENTAN EN PC
DISMINUYEN ANDROID

Adware

DISMINUYEN EN PC
AUMENTAN EN ANDROID

FIGURA 29. PELIGROSIDAD DEL *MALWARE* EN DISPOSITIVOS ANDROID (%)

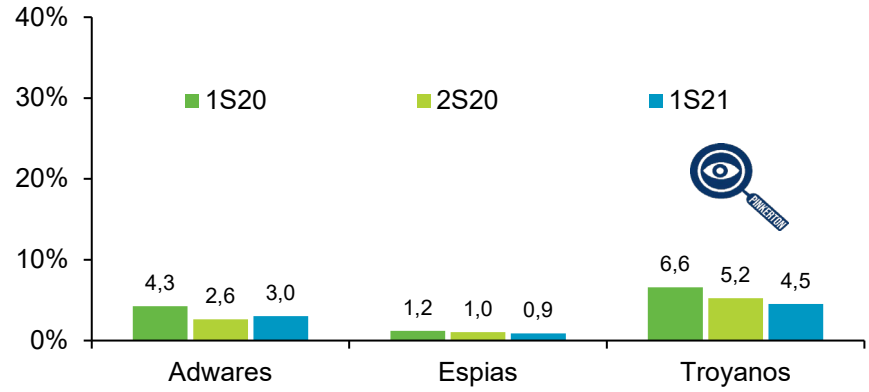


Base: total de dispositivos Android infectados
Fuente: Panel hogares, ONTSI

Con respecto a la evolución del *malware* en dispositivos Android, mientras que en los ordenadores del hogar disminuían los *adware*s y aumentaban los troyanos y espías, en este caso ocurre precisamente lo contrario.

El porcentaje de dispositivos con troyanos y espías disminuye al 4,5% y 0,9% respectivamente. Aumentan los dispositivos con *adware* situándose en el 3,0% (+0,4p.p.).

FIGURA 30. EVOLUCIÓN DEL *MALWARE* EN DISPOSITIVOS ANDROID (%)



Base: Total dispositivos Android
Fuente: Panel hogares, ONTSI

El aumento del *adware* en los dispositivos Android se explica por el cada vez mayor uso de los dispositivos personales para navegar por Internet. En este sentido, los dispositivos móviles serían vehículos perfectos para este tipo de *malware*.

La siguiente tabla sintetiza los datos referentes a las incidencias de *malware*, destacando precisamente aquél que refleja el índice que

tal vez sea el más preocupante. En torno al 6,57% de los usuarios de dispositivo Android no creían tener *malware* en su dispositivo móvil y tras el análisis se ha demostrado que la percepción en este caso es errónea.

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

Declararon tener malware en Android	Su Android presentaba malware		
	Sí	No	Total
Sí	0,26%	4,03%	4,29%
No	6,57%	89,14%	95,71%
Total	6,84%	93,16%	100,00%

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

Al igual que ocurriese en el caso de los ordenadores del hogar, dicho porcentaje refleja desconocimiento por parte de los usuarios respecto a su seguridad. La falsa sensación de seguridad puede inducir conductas de seguridad relajadas. Es más, si los dispositivos personales sincronizan con otros dispositivos, e incluso usan c*loud*s externos para hacer copias de *backup*, entonces el *malware* podría encontrar vías naturales para su propagación y persistencia posterior en el sistema sin levantar sospechas.

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

Los incidentes anteriores repercuten en la seguridad cuando de hecho se materializan en ataques efectivos, y por lo tanto, tienen efecto en el comportamiento de los panelistas y en sus reacciones a posteriori. En particular, el fraude es uno de los incidentes que más notan los usuarios, ya que afectan directamente a su economía.

7.1 Evolución de los intentos de fraude

64,6% DE USUARIOS HAN SIDO VÍCTIMAS DE FRAUDE

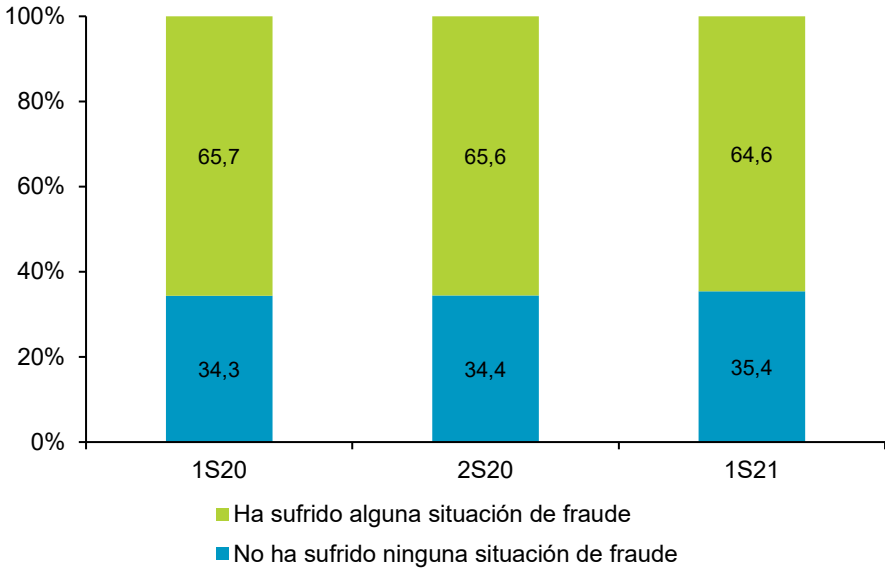
NOTIFICA los casos de FRAUDE ONLINE o MALWARE: incidencias@incibe-cert.es

El fraude es uno de los incidentes de seguridad más peligrosos, dado que el atacante buscará, en última instancia, obtener un beneficio económico de la víctima. En la mayoría de los casos, sobre todo cuando hablamos de ciudadanos, el objetivo es aleatorio.

El conocimiento sobre este tipo de actividad es la mejor arma para que no seamos víctimas de fraude. La OSI pone a disposición de los ciudadanos indicaciones sobre cómo denunciar los casos de fraude.

La percepción de los intentos de fraude ha disminuido en 1 p.p. respecto al semestre anterior, declarando el 64,6% de los panelistas ser víctimas de este incidente.

FIGURA 31. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

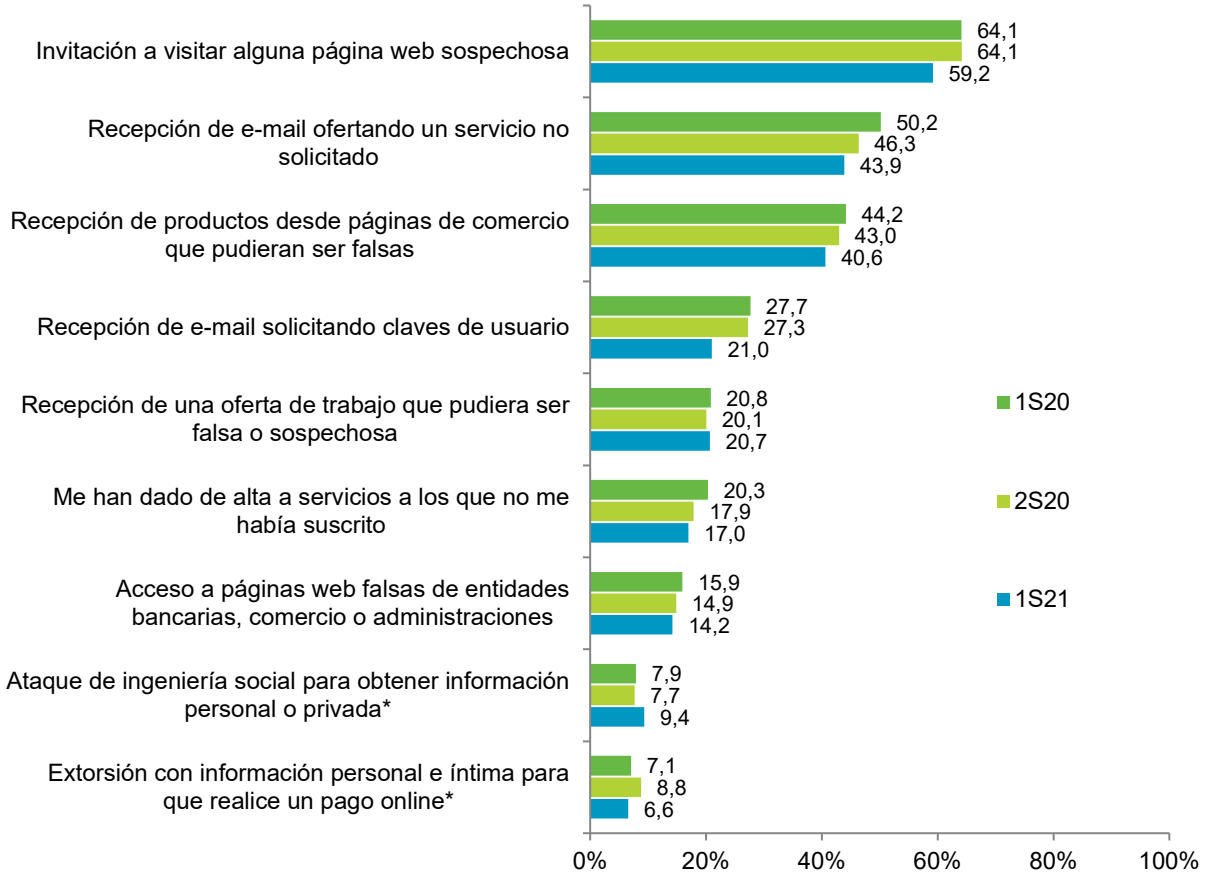
Como se ha mencionado, a diferencia de otras incidencias de seguridad que pueden ser más subjetivas desde el punto de vista del usuario, como las infecciones por *malware*, en el caso del fraude, al afectar al plano económico visiblemente, puede comprenderse que las víctimas de este incidente sean mucho más conscientes de la situación.

La FIGURA 32 muestra la evolución de las situaciones de fraude ocurridas en los últimos meses. Corresponde por lo tanto a las declaraciones de los panelistas que sí han sufrido alguna situación de fraude.

El intento de fraude más destacado por los panelistas sigue siendo la invitación a visitar webs sospechosas 59,2%, pese a que disminuye 4,9 p.p. respecto del semestre anterior. Cabe destacar que este sigue siendo uno de los principales vehículos para el robo de contraseñas. Los atacantes podrían emplear las contraseñas posteriormente para el acceso a datos de los usuarios en diversos sitios web. Entre ellos, el robo de credenciales bancarias afectaría especialmente en este punto.

Aunque en general se observa que han disminuido los intentos de estafa, en este semestre los ataques de ingeniería social han aumentado según indican las respuestas de los usuarios en 1,7 p.p., situándose en el 9,4%.

FIGURA 32. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



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

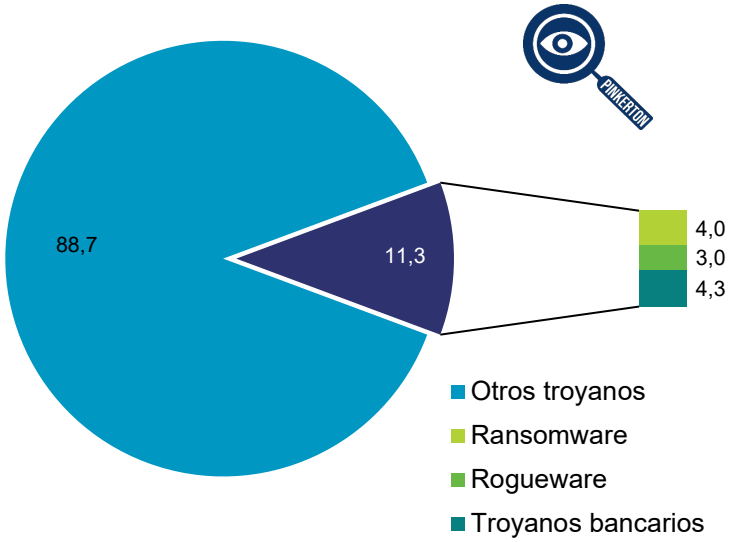
Otra situación que aumenta respecto del semestre anterior son los presuntos intentos de estafa basados en ofertas de trabajo. Dada la crisis generada por la COVID-19, en la que hubo un descenso en el empleo, con la recuperación paulatina de la actividad rutinaria mensajes de ofertas de empleo podrían captar la atención de un gran volumen de víctimas potenciales.

7.1.1 Malware que afecta a los casos de fraude

Aunque el fraude se hace notar más que otros tipos de incidentes de seguridad, en sus primeras fases puede contar con la ayuda de *malware* que se instalaría en los equipos o dispositivos de las víctimas. En estos casos, el *software* de escaneo puede arrojar cierta luz sobre el estado de los equipos del hogar y dispositivos personales de cara a la lucha contra el fraude online.

En los ordenadores del hogar (FIGURA 33), por ejemplo, el 11,3% respecto del conjunto total de muestras recabadas corresponde a *malware* que afectaría especialmente (por su comportamiento) a casos de fraude. Los troyanos bancarios ocupan la primera posición, representando el 4,3% de la tipología analizada.

FIGURA 33. TROYANOS BANCARIOS, *RANSOMWARE* Y *ROGUEWARE* EN EL ORDENADOR DEL HOGAR (%)



Base: total ordenadores con troyanos detectados
Fuente: Panel hogares, ONTSI

FRAUDE ONLINE EN ANDROID

33,6%

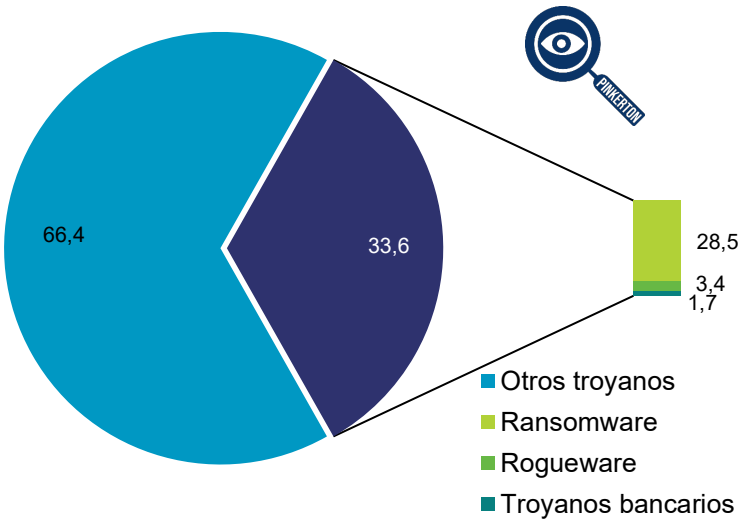
AUMENTO DEL MALWARE ANDROID DIRIGIDO A FRAUDE

28,5%

CORRESPONDE A RANSOMWARE

El contraste con los datos recopilados de los sistemas Android (FIGURA 34) no deja de resultar curioso. En Android la tipología que afecta especialmente al fraude bancario alcanza un 33,6% de las muestras totales de *malware*. En este caso es el *ransomware* el *malware* predominante, pese a que habitualmente se asocia más a los ordenadores del hogar.

FIGURA 34. TROYANOS BANCARIOS, *RANSOMWARE* Y *ROGUEWARE* EN DISPOSITIVOS ANDROID (%)



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

Del total de los troyanos detectados en dispositivos Android, el 33,6% han sido ransonwares, *roguewares* o troyanos bancarios.

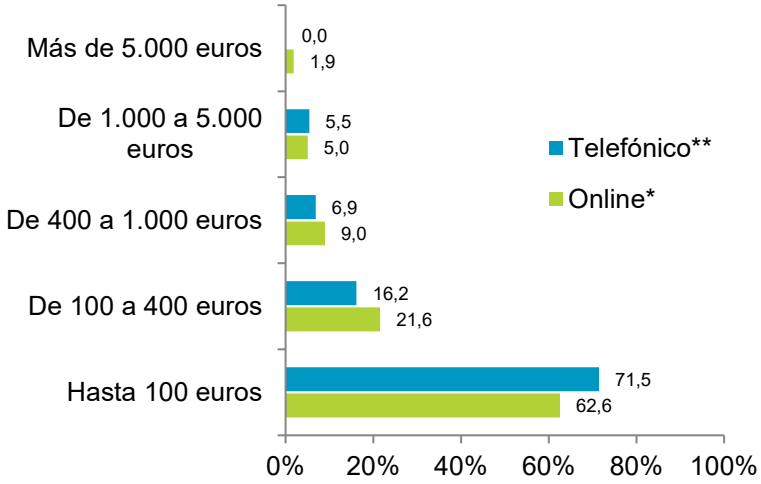
El *malware* de tipo *ransomware* (cifrado y secuestro de datos) ocupa el 28,5% seguido por los *rogueware*, situándose estos últimos en torno al 3,4%.

7.2 Repercusión económica

Como ya se ha mencionado, los ataques de fraude tienen como efecto final repercusiones visibles en la economía de las víctimas. Se recogen a continuación las declaraciones de los participantes respecto a este punto. Concretamente, la

FIGURA 35 recoge las cifras declaradas por los participantes que han sido víctimas de fraude telefónico (vishing) u online.

FIGURA 35. DISTRIBUCIÓN DEL PERJUICIO ECONÓMICO DEBIDO A POSIBLES FRAUDES (%)



Base: usuarios que han sufrido perjuicio económico debido a un fraude online
Usuarios que han sufrido perjuicio económico debido a un fraude telefónico
Fuente: Panel hogares, ONTSI

Se observa que la mayoría de los fraudes, independientemente de su medio (telefónico u online), se centran en cantidades inferiores a 100 euros. Estas cantidades, extrapoladas a un gran número de víctimas pueden ser muy cuantiosas, y además más efectivas desde el punto de vista del cobro.

Las cantidades más cuantiosas se atribuyen a fraude online, salvo en la franja de 1.000 a 5.000 euros. En dicha franja es el fraude telefónico el que adquiere al parecer más relevancia por ahora.

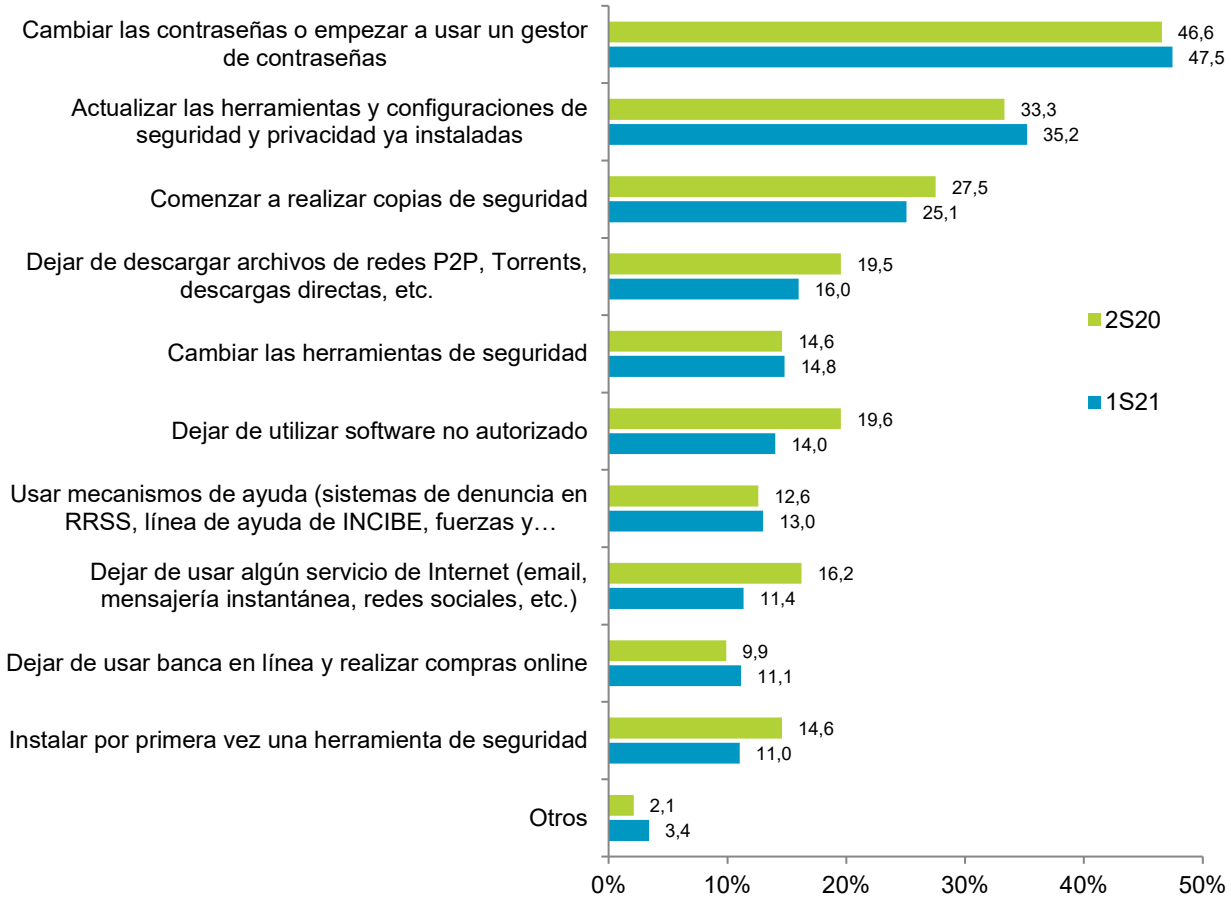
7.3 Cambios de hábitos tras incidente

Cambiar de hábitos tras sufrir un incidente de ciberseguridad podría ser lo habitual, en especial cuando el incidente ha sido motivado por una mala práctica de la que se percata el usuario a posteriori.

La FIGURA 36 muestra la evolución en los cambios de hábitos tras sufrir un incidente de seguridad. El hábito más destacado tras sufrir una incidencia de seguridad sigue siendo cambiar las contraseñas o empezar a usar un gestor de contraseñas (47,5%). Que sea el más

habitual podría venir motivado por, precisamente, la duda de los usuarios tras consultar una web sospechosa (análisis relativo a la FIGURA 32) o bien introducir las credenciales en sitios que podrían generar desconfianza.

FIGURA 36. 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

De esta forma, los hábitos del cambio de contraseña, el uso de un gestor de contraseñas y la actualización de herramientas y configuraciones de privacidad aumentan en 0,9 p.p. y 1,9 p.p. respectivamente respecto del semestre anterior.

El 13% de los usuarios ya aprovecha los Mecanismos de Ayuda

Sin embargo, el tener incidencias de seguridad no motiva a los encuestados a dejar de usar *software* no autorizado ya que el 14% de ellos continúa usándolo frente al 19,6% que decidieron dejar de usarlo en el semestre anterior.

Es significativo el aumento de usuarios que han dejado de usar la banca en línea y realizar compras online quizás debido a la eliminación o disminución de restricciones provocadas por la pandemia.

Un dato muy positivo es que el 13% de los usuarios ya aprovecha los mecanismos de ayuda, continuando el progreso ascendente de esta reacción ante los incidentes en ciberseguridad. Campañas

informativas como la que realiza INCIBE podrían estar ayudando en este sentido.

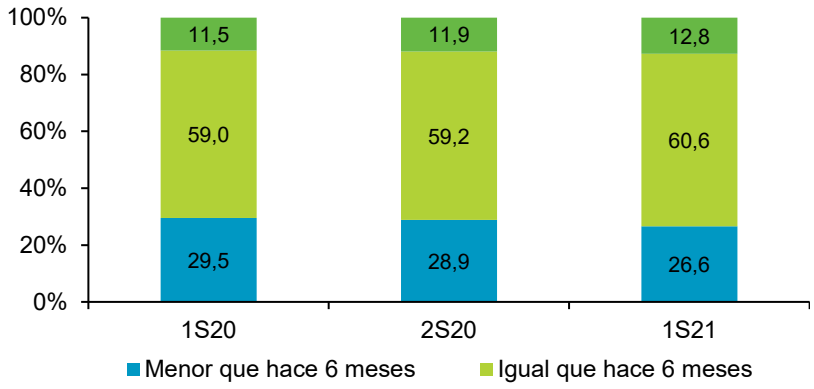
8 Confianza en el ámbito digital en los hogares españoles

Los apartados anteriores reflejan la situación actual de las opiniones de los participantes en el estudio respecto a la seguridad, los mecanismos para proteger los equipos o dispositivos y la seguridad real evaluada por el sistema de análisis de datos que recaba el *software* Pinkerton. A partir de este punto, se concluye con los datos que arrojan luz sobre el progreso del nivel de confianza de los usuarios en Internet.

8.1 Evolución de la percepción de las incidencias y el riesgo

La FIGURA 37 muestra la evolución de la percepción de las incidencias por parte de los panelistas.

FIGURA 37. EVOLUCIÓN DE LA PERCEPCIÓN DE LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD (%)

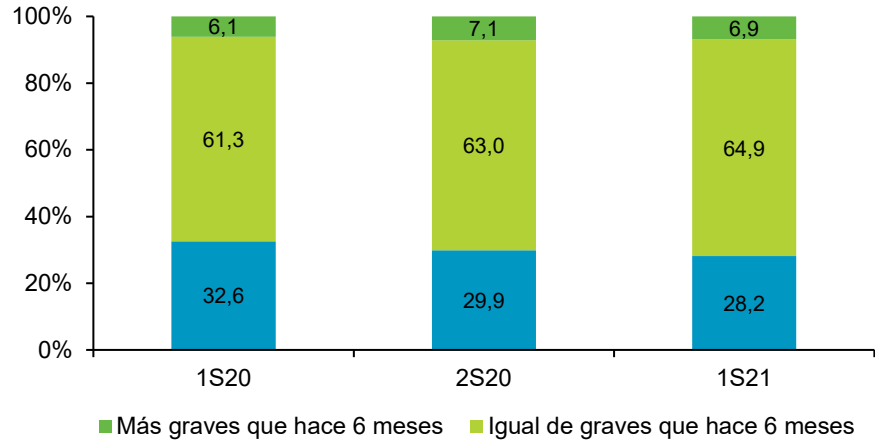


Base: total usuarios
Fuente: Panel hogares, ONTSI

El 12,8% de los usuarios percibe que las incidencias de ciberseguridad se han visto incrementadas respecto de los últimos 6 meses. De sus respuestas se deriva que el número de incidentes declarado ha aumentado en 0,9 p.p. respecto al semestre anterior. También aumenta el número de usuarios que percibe que las incidencias se mantienen estables (60,6%). El 26,6% de los usuarios mantiene, sin embargo, que las incidencias han disminuido este último semestre.

La cantidad de incidencias no tendrían necesariamente que resultar excesivamente preocupantes sin un valor de gravedad asociado. La siguiente gráfica muestra la percepción de los panelistas respecto de la gravedad de las incidencias en los últimos seis meses.

FIGURA 38. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%)

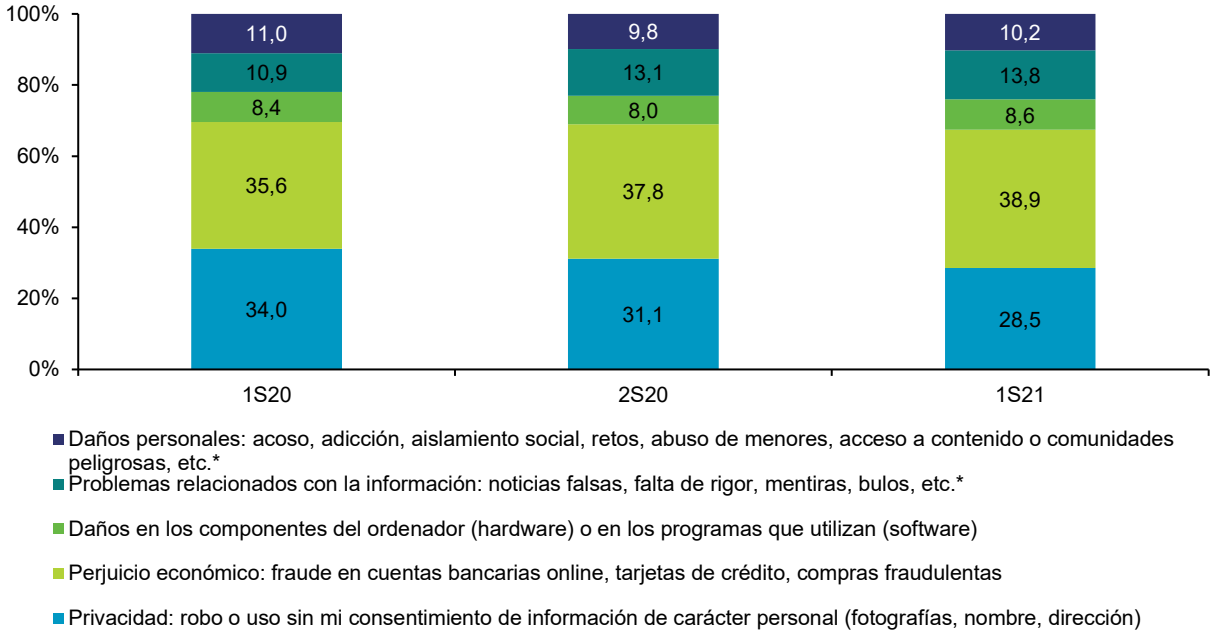


Base: total usuarios
Fuente: Panel hogares, ONTSI

Curiosamente, un menor número de encuestados opina que las incidencias sean más graves que hace seis meses (6,9% respecto al 7,1% del semestre anterior). El 64,9% percibe que los incidentes son igual de graves que hace seis meses, cuando realmente los datos de este estudio muestran un recrudecimiento de la peligrosidad del *malware* identificado en los dispositivos (FIGURA 26)

Por otra parte, el perjuicio económico ocasionado por fraude sigue siendo la opción que más preocupa a los usuarios según las declaraciones del 38,9% de los usuarios, conforme a los resultados que podemos consultar en FIGURA 39.

FIGURA 39. EVOLUCIÓN DE LA PERCEPCIÓN DE LOS RIESGOS EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Esto puede deberse, precisamente como ya se ha mencionado en secciones anteriores, a que es el incidente que más visible o

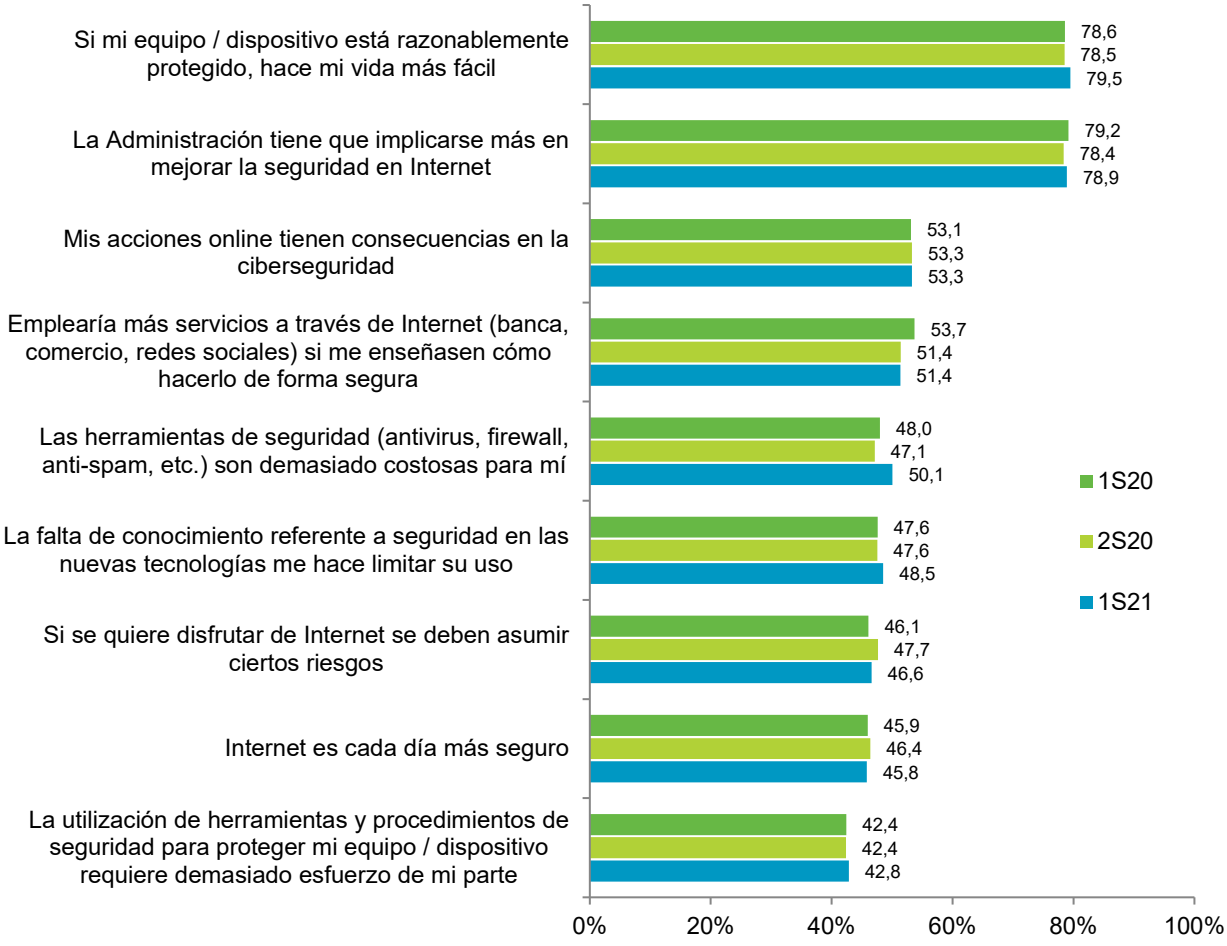
tangible resulta de cara al usuario, víctima de fraude. De hecho, los autores de *ransomware* en la modalidad RaaS (*ransomware* as a service) procuran darse a conocer y que las víctimas potenciales tengan muy claro que están dispuestos a cumplir sus amenazas.

La privacidad mantiene su segundo puesto en este ranking, aunque disminuyendo fuerza respecto al semestre anterior. Se sitúa la preocupación por la privacidad en 28,5%, aunque precisamente pueda ser uno de los motores clave para obtener información que se use contra las víctimas para un ataque de fraude.

8.2 Opiniones sobre la seguridad en Internet

La FIGURA 40 muestra los resultados recabados de las consultas sobre las opiniones de la seguridad en Internet que afectan al nivel de confianza.

FIGURA 40. EVOLUCIÓN DE OPINIONES SOBRE LA SEGURIDAD EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

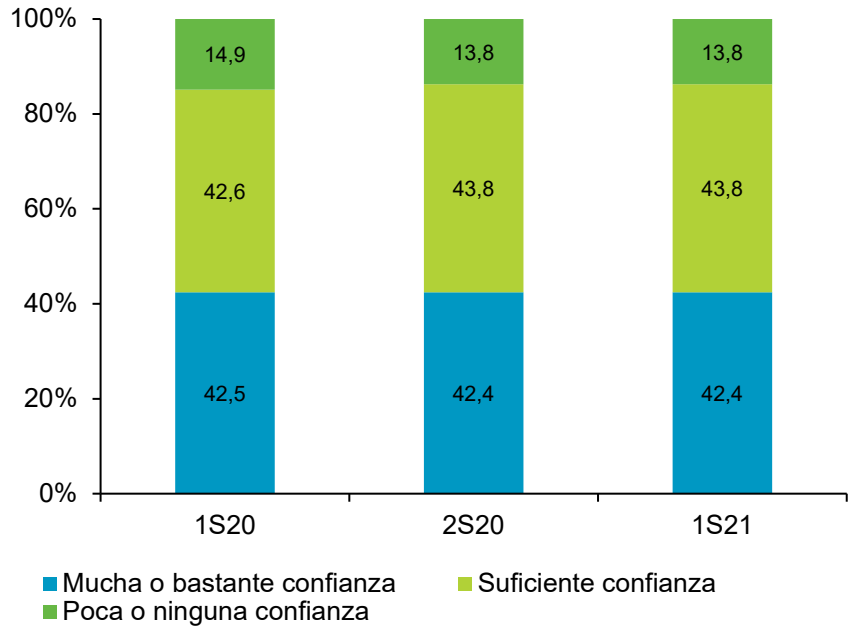
Entre los datos a destacar, en este semestre el 50,1% de los usuarios manifiesta que las herramientas de seguridad como antivirus, *firewall*, *anti-spam*, etc. les resultan demasiado costosas. Esa creencia ha aumentado en 3 p.p. respecto al semestre anterior. No obstante, esta apreciación resulta curiosa en tanto a que muchos sistemas operativos integran ya su propia seguridad nativa que actúa coordinadamente con sistemas de seguridad externos.

Opciones como VirusTotal por ejemplo, aplican motores antivirus sobre datos de los usuarios, de forma gratuita.

Además, se aprecia un aumento del 1 p.p. de los usuarios declaran que la falta de conocimientos sobre seguridad en las nuevas tecnologías limita su uso. Suponen un 48,5% de usuarios para los que formación en esta área podría resultar decisiva para su adaptación.

Nuevamente los usuarios señalan que la administración debería implicarse más en mejorar la seguridad en Internet (78,9%). Lo cierto es que hay portales informativos de muy diverso tipo destinados a los ciudadanos, a los que se está dando mucha difusión, pero tal vez, aun así, no lleguen a todos los ciudadanos por igual.

FIGURA 41. EVOLUCIÓN DEL NIVEL DE CONFIANZA EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Al margen de las variaciones observadas durante este semestre, los niveles de confianza se mantienen, siendo exactamente los del semestre anterior. Las variaciones resultan ínfimas y no se aprecian por tanto cambios en los redondeos.

9 Conclusiones

La ciberseguridad es cosa de todos, independientemente del género, la edad o la profesión que se tenga, así lo hemos podido ver en la parte inicial del informe.

La formación online tomó impulso a causa del confinamiento vivido debido a la situación generada por la COVID-19 y se está adaptando

como hábito en la vida de los usuarios. Deberemos esperar a futuros informes para comprobar si ese hábito persiste y se alimenta. A pesar de que es un ámbito muy atribuido a estudiantes y trabajadores, como se ha visto reflejado también interesa a las personas que trabajan en el hogar. Este punto es crítico, porque implica que con campañas efectivas y bien dirigidas en ciberseguridad se puede llegar a sectores de la población que ya sí están adaptados a nuevas modalidades de formación que aprovechan las nuevas tecnologías. Cabe hacer notar que se observa un rol predominante en el género femenino en cuanto al interés por la formación, en especial entre la población de estudiantes.

Poco a poco los usuarios van tomando conciencia de las medidas de seguridad que tienen a su alcance. En particular, su relación con las administraciones ha hecho que aleguen un mayor uso del DNI electrónico. Sin embargo, por ahora aún hay una parte importante de usuarios que afirma no darle uso quizás porque sean usuarios del certificado digital y no vean la necesidad del DNI electrónico. Otra de las conclusiones que arroja el estudio es que el uso de máquinas / entornos virtuales aún genera mucho desconocimiento por parte de los usuarios, que manifiestan que no las encuentran necesarias para su uso en el hogar.

En cuanto a los hábitos de comportamiento con relación a las descargas realizadas de redes P2P o descargas directas, aproximadamente la mitad de los usuarios no verifican las descargas y más de la mitad no usa el antivirus para comprobar si la descarga lleva algún elemento malicioso. Este es un punto que hay que reforzar para que el usuario conozca los riesgos y las herramientas que tiene a su alcance para mitigar los riesgos de seguridad y con ello las incidencias.

Con los datos recogidos en este estudio podemos concluir que el uso de redes públicas, abiertas o de terceros es cada vez menor y que los usuarios toman consciencia de los peligros que conllevan. Aun así es necesario seguir trabajando este tema en las campañas, charlas y formaciones de concienciación.

Respecto a los incidentes de seguridad, más de la mitad de los panelistas afirma haber sufrido un incidente de seguridad, aunque la percepción de los incidentes baja respecto al semestre anterior. Entre las incidencias más repetitivas se encuentra la recepción de correos electrónicos sospechosos. El aumento del *phishing* como vía ya no solo para el robo de contraseñas sino para la instalación de *malware* puede propiciar este aumento.

Más de la mitad de los equipos analizados contiene *malware*, aunque la percepción de los usuarios sobre este hecho no es acertada.

Conforme a los datos contrastados, el 50% de los usuarios que afirma no tener *malware* en su equipo se equivoca. Además, el 75% del *malware* detectado en los equipos presenta un nivel de riesgo alto. Aunque la incidencia de dispositivos Android que presenta *malware* es menor (6,8%), el 66,1% presenta un nivel de riesgo alto, despuntando el *adware* frente a los troyanos y y espías, que sí afectan más a los ordenadores del hogar. En el caso de Android, además, el 6,57% de los usuarios no es consciente de tener

malware en su dispositivo Android.

De las consecuencias de los incidentes anteriores, la más identificable por parte de los usuarios es el fraude, afectando al 64,6% de los panelistas. De hecho, el 33,6% del *malware* en dispositivos Android tiene como objetivo el fraude online.

Por todo lo anterior, el usuario suele variar su opinión sobre la seguridad en Internet, y, de hecho, es algo que debería evitarse, en tanto a que, bien dirigido, Internet es un motor para el progreso.

Entre los cambios de hábitos tras sufrir algún incidente de ciberseguridad, cabe destacar que incrementa nuevamente el número de usuarios que se decanta por aprovechar los mecanismos de ayuda en ciberseguridad a su disposición (p.ej. la Línea de Ayuda en Ciberseguridad de INCIBE, disponible en https://www.incibe.es/linea-de-ayuda-en-ciberseguridad)

Finalmente, los valores de confianza en Internet se mantienen estables este semestre. Manteniendo los datos del semestre anterior, el 86,2% de los usuarios mantiene su confianza, frente al 13,8% de los panelistas encuestados que afirma no confiar en Internet.

Índice de figuras

EDITA: Ministerio de Asuntos Económicos y Transformación Digital
Paseo de la Castellana, 162
28046 Madrid

NIPO: 094-21-113-5
DOI: 10.30923/ciu_ciberries_2021_2

El informe del *'Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España*' ha sido elaborado por el siguiente equipo de trabajo del Observatorio Nacional de Tecnología y Sociedad (ONTSI):

Lucía Velasco
Alberto Urueña
Santiago Cadenas Villaverde

Estudio realizado con asistencia técnica de Hispasec y Gfk