OBSERVACIBER

CÓMO SE PROTEGE A LA CIUDADANÍA ANTE LOS CIBERRIESGOS

Estudio sobre percepción y nivel de confianza en España

Edición Abril 2022

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

ontsi Observatorio Nacional de Tecnología y Sociedad

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OBSERVACIBER

OBSERVACIBER

1 Introducción

Las tecnologías digitales se usan cada vez con más frecuencia e intensidad. Esto **despliega un abanico de oportunidades, pero también deja la puerta abierta a los riesgos y amenazas**. Conocer el alcance de estos peligros es tan importante como entender cómo los percibe la población; su grado de confianza en redes y dispositivos y qué lugar ocupa la prevención en sus rutinas.

La nueva edición de este estudio **pretende conocer mejor los hábitos y conductas de la sociedad española (durante el último semestre de 2021)**. Los datos obtenidos de encuestas y el monitoreo, previa autorización, de los aparatos evaluados —dispositivos Android, tanto tabletas como móviles, y ordenadores— permiten perfilar la percepción de la gente sobre la ciberseguridad. Se trata de conocer, a través de sus hábitos y conductas, su grado de conocimiento de los riesgos y su prevención. Para ello, se ha analizado información obtenida a través de encuestas y del análisis de sus dispositivos.

Además de leer los datos en clave de concienciación, preparación y percepción de riesgos, en esta edición se ha querido vincular a los hábitos derivados o condicionados por la pandemia, ya reflejados en el último informe. Por poner un ejemplo, enfrentó por primera vez a mucha gente a hacer trámites *online*; muchas personas han comenzado a usar el certificado digital y similares para trámites administrativos, y, a su vez, la Administración ha potenciado y facilitado el uso.

Esta y otras rutinas adquiridas se han solidificado hoy, así que el uso de Internet y sus servicios va en aumento. Esto no tiene por qué ser necesariamente un riesgo siempre. Por ejemplo, el hecho de que haya aumentado el consumo de contenidos digitales de pago o suscripción en detrimento del consumo de páginas web de descarga gratuita, ha supuesto una disminución en el riesgo de infección por *malware*.

Además de este contenido, se aborda el incremento del interés por la formación *online* (que ya se trataba en semestres anteriores), y se añade un capítulo sobre el impacto de las campañas públicas de ciberseguridad, lo que permite que nos hagamos una idea de cómo calan los esfuerzos divulgativos en materia de seguridad *online*, cómo pueden generar una mayor conciencia sobre los riesgos que modifique hábitos de consumo y uso.

Conocer el nivel de confianza digital y seguridad en España es una de las prioridades del Observatorio Nacional de Tecnología y Sociedad (ONTSI). En esta línea, se realiza el estudio titulado *Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea* en el que estudia la situación de España empleando datos de Eurostat. En él participan personas entre los 16 y los 74 años y residentes en alguno de los 27 estados miembros de la Unión Europea.

Su fin es analizar a través de indicadores de confianza digital de la población y de las empresas españolas, los riesgos a los que se enfrentan la ciudadanía y las empresas en ciberseguridad, así como la gestión de la seguridad y privacidad. En esta clasificación europea, España se sitúa en cuarta posición respecto al resto de estados miembros. La mejora en este aspecto puede venir de la mano de la formación.

Por ejemplo, con acciones como las de la Agencia de Ciberseguridad de la Unión Europea (ENISA), que celebra anualmente *El mes de la ciberseguridad*[1] para concienciar e informar sobre esta materia y dura cuatro semanas. En la última edición de este evento, bautizado *Think Before U Click*, la ENISA realizó una campaña de sensibilización para promover recomendaciones actualizadas de seguridad y generar así confianza en los servicios en línea. Se trata de informar al público y ofrecerles recursos para reconocer y reaccionar ante ciberamenazas; así como acercarles importancia de la protección de sus datos personales y financieros *online*.

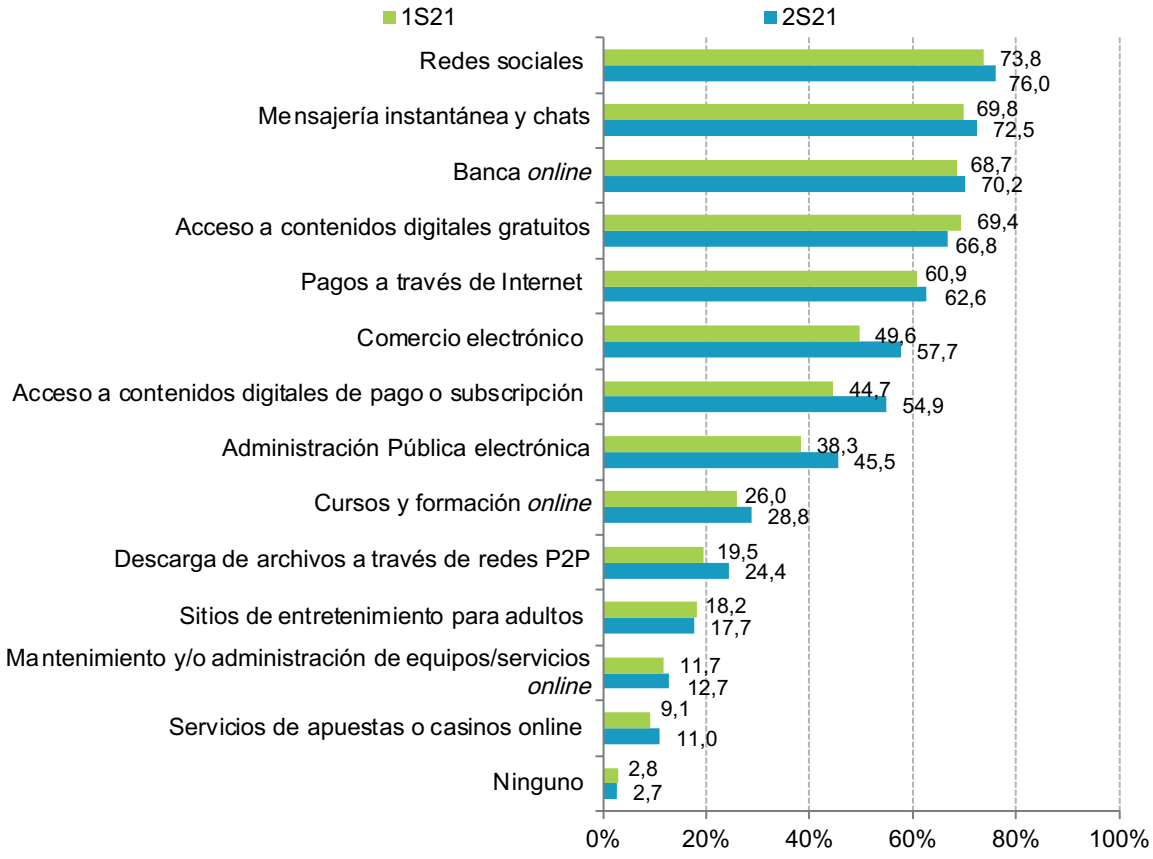
[1] https://www.enisa.europa.eu/news/enisa-news/uniting-to-raise-awareness-on-cyber-threats-european-cybersecurity-month-2021

2 Servicios de internet más utilizados

Durante el segundo semestre de 2021, salvo excepciones, hubo un incremento en el uso de servicios disponibles a través de Internet. Esta sección recopila las principales conclusiones del uso de sus servicios, y ofrece una perspectiva general de las potenciales implicaciones de los resultados. Junto al tradicional uso social y comercial que se hace de las redes, otros ámbitos como el del entretenimiento (en especial reflejado por el acceso a plataformas de contenidos digitales), la formación y la realización de trámites administrativos cobran una importancia fundamental.

En particular, conforme a las declaraciones recogidas en el gráfico 1, cabe destacar tres servicios que han tenido un aumento significativo del uso respecto al semestre anterior: el comercio electrónico, los accesos a contenidos digitales de pago o suscripción y la Administración pública electrónica.

Gráfico 1. Servicios ofrecidos por internet que han sido utilizados por las personas usuarias en el último semestre (2s 2021)



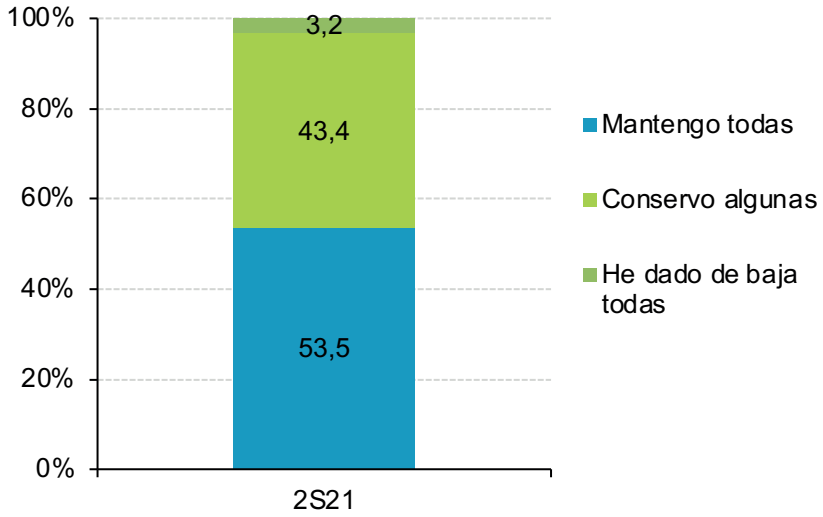
Base: **Total usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

El comercio electrónico ha aumentado en 8,1 puntos porcentuales (p.p.) respecto al semestre anterior. Puede deberse a las campañas publicitarias propias del segundo semestre del año, como el *Black Friday* y las compras de Navidad. Además, el incremento del uso del comercio electrónico se ha visto reflejado los grandes *marketplace*[2].

Otro aumento a destacar es el acceso a los servicios que brinda la Administración pública. Su crecimiento respecto al semestre anterior se sitúa en torno a los 7,2 p.p., alcanzando un 45,5%. Esta mejora significativa puede ser debida al esfuerzo de digitalización de las entidades públicas para flexibilizar trámites que antes eran presenciales, así como a las campañas dirigidas a informar a la población. Las personas que se han visto con dificultades para acceder presencialmente a las oficinas (por ejemplo, por el aislamiento consecuencia de la pandemia) han podido realizar trámites con la Administración sin obstáculos.

Destaca el aumento en el uso del comercio electrónico, el consumo de contenidos de pago y el acceso a la Administración Pública Digital.

Gráfico 2. Mantiene las suscripciones a plataformas de pago realizadas durante el confinamiento



Base: **Usuarios y usuarias que realizaron alguna suscripción nueva a plataformas de pago**
Fuente: **Panel hogares, ONTSI**

[2] https://www.elmundo.es/economia/empresas/2021/10/28/617b187dfdddffd5b08b45cc.html

Por otro lado, el acceso a contenidos digitales aumentaba en ese período 10,2 p.p., debido a varios factores. Uno de ellos es la alta incidencia de la pandemia y las oleadas en las que para evitar contagios o precisamente por sufrirlos, se optaba por permanecer en casa y buscar formas alternativas de entretenimiento.

De igual forma otros factores que han podido influir son, por un lado, el relanzamiento de plataformas de *streaming* y las ofertas promovidas por las habituales, que ofrecen contenidos para todas las edades y semanalmente añaden títulos nuevos a su cartelera que modifican hábitos de consumo.

A este respecto, cabe destacar que el 53,5% de la población usuaria mantiene las suscripciones a todas las plataformas de pago que contrató durante el confinamiento (gráfico 2). Otro 43,4% de usuarios dieron de baja algunas, aunque siguen conservando otras[3].

[3] En el momento en que se publica este informe estas cifras sobre plataformas de vídeo son ligeramente diferentes. https://elpais.com/tecnologia/2022-04-24/soplan-vientos-de-cambio-en-el-streaming.html

3 Medidas de seguridad

De cara a valorar las actitudes y comportamientos en torno a la seguridad *online*, es imprescindible conocer el tipo de precauciones adoptadas y rechazadas por la población, y su motivación para aceptarlas o prescindir de ellas. En esta sección se analiza el tipo de medidas de seguridad utilizadas durante el segundo semestre de 2021. La información contenida está extraída tanto de las declaraciones sobre las medidas de seguridad que se implementan en el ordenador del hogar como en los dispositivos móviles. Además, se ha realizado el análisis de dispositivos con el *software* Pinkerton para contrastar con el estado real de las medidas de seguridad y contrastar con las opiniones.

3.1. PROTECCIÓN DE LOS ORDENADORES DEL HOGAR

Los ordenadores del hogar muchas veces dejan de ser equipos personales para convertirse en puntos comunes de acceso a Internet para la familia. Por ello, es importante asegurar que se comprenden las protecciones desplegadas en sus dispositivos, o bien otras que podrían ser de gran utilidad.

Las medidas automatizables son aquellas que no dependen de la intervención de las personas que las usan. Se incluyen en este grupo, entre otras, las actualizaciones del sistema operativo, el uso de programas antivirus, cortafuegos o *firewall*, programas o configuración de bloqueo de *pop-up* y publicidad.

Todas ofrecen a los usuarios seguridad por defecto, aunque no por ello se excluyen las no automatizables; ambas están orientadas hacia una seguridad más completa. Las declaraciones respecto a este tipo de medidas durante los tres últimos semestres se recogen en el gráfico 3.

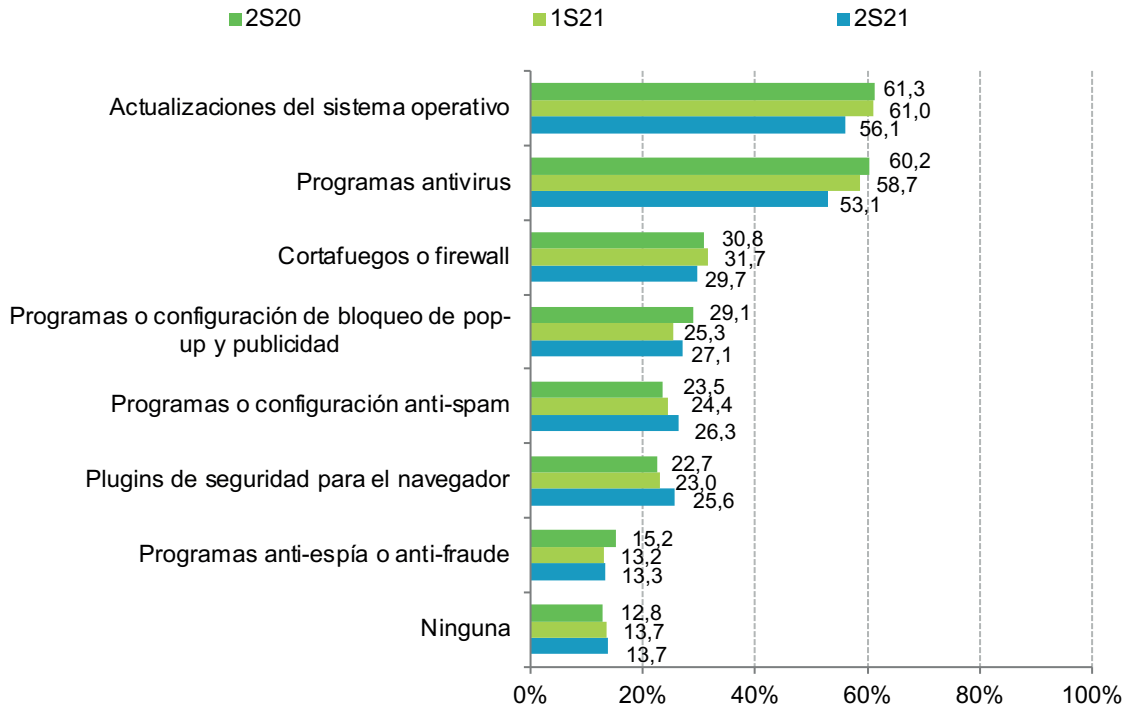
Un menor porcentaje declara emplear equipos actualizados, programas antivirus y cortafuegos, disminuyendo respectivamente 4,1 p.p., 5,6 p.p. y 2 p.p. Quizás porque dificultan la ejecución de algún otro *software* o afectan a su rendimiento. Aunque en muchos casos si son programas nativos del sistema podrían volver a activarse, ya sea automáticamente o tras una actualización. Otro motivo, podría ser que los dispositivos empleados no permitan más actualizaciones, momento en el cual se suele adquirir un nuevo dispositivo.

Descienden considerablemente el uso de antivirus y las actualizaciones del sistema operativo.

Emplean, además, otras medidas, como los programas para bloqueo de publicidad, anti-*spam*, anti-espía, o *plugins* de seguridad para el navegador. Algunos gestores de correo, como es el caso de Gmail, permiten identificar emails con *software* malicioso, aunque no de forma inmediata. Esto puede dar una falsa sensación de seguridad a las personas usuarias, y también confusión sobre las medidas que realmente ha desplegado en su equipo.

Al contrastar con los datos recabados por el *software* Pinkerton completamos esta información, incluso aclaramos posibles incoherencias entre las opiniones recogidas y los datos arrojados por los dispositivos.

Gráfico 3. Medidas de seguridad automatizables en el ordenador del hogar (datos declarados). 2s 2020 – 2s 2021



Base: **Usuarios y usuarias de ordenador**
Fuente: **Panel hogares, ONTSI**

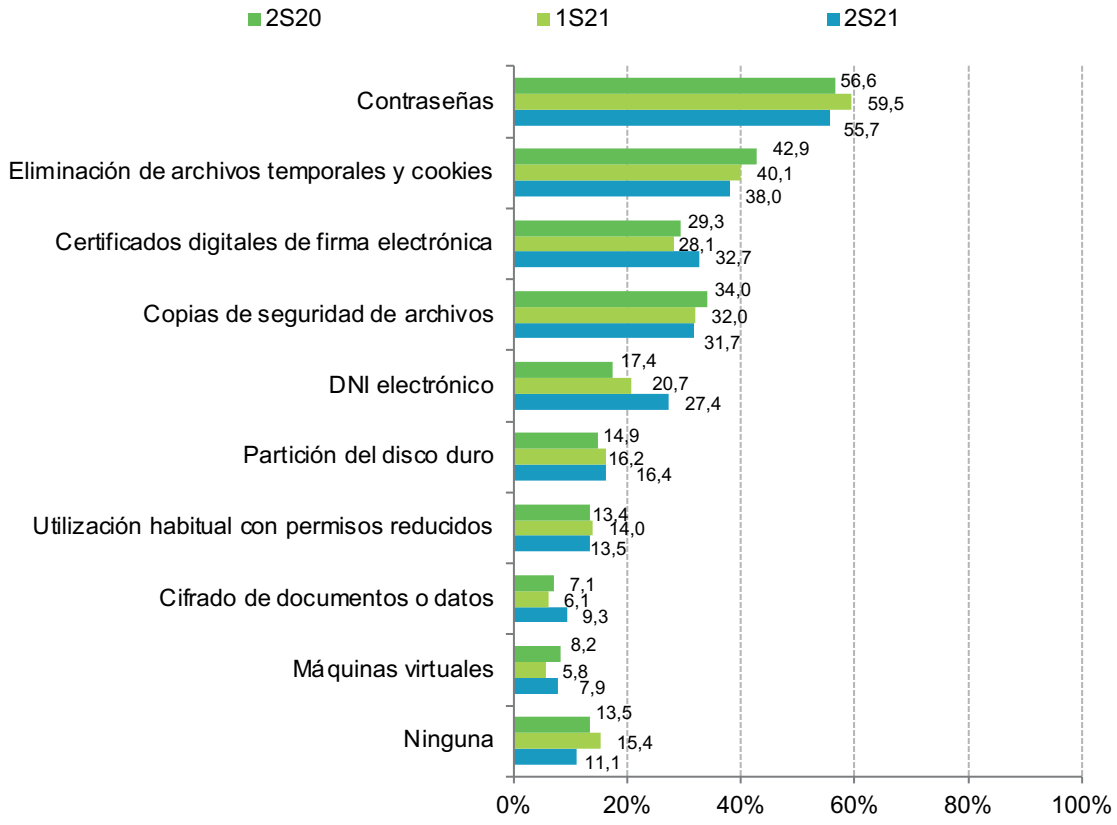
Por otro lado, es importante tener en cuenta las medidas activas o no automatizables. Este tipo de medidas son aquellas que requieren intervención manual por parte de las personas usuarias, como por ejemplo el uso de contraseñas seguras, la eliminación de los archivos temporales, o bien el uso de certificados digitales que deben instalarse en el navegador o en el equipo.

El gráfico 4 recoge las medidas de seguridad no automatizables que dicen tener activas en el ordenador del hogar.

En el segundo semestre de 2021 destaca que un mayor número de internautas declara hacer uso del DNI electrónico (27,4%) y del certificado digital (32,7%). El aumento de trámites *online* con la Administración puede ser uno de los motivos del aumento respecto del semestre anterior del uso del DNI electrónico (6,7 p.p.) y del certificado digital (4,6 p.p.) como medidas de seguridad.

Un 14% de las personas encuestadas declara no usar ninguna medida de seguridad automatizable en el ordenador del hogar.

Gráfico 4. Medidas de seguridad activas o no automatizables en el ordenador del hogar (datos declarados). 2s 2020 – 2s 2021



Base: **Usuarios y usuarias de ordenador**
Fuente: **Panel hogares, ONTSI**

La disminución en el uso de contraseñas podría deberse a emplear otros métodos, como la huella digital. Muchos equipos tienen integrada esta característica, aunque requieren también uso de contraseñas. También puede ser que realmente no se estén empleando claves, por ejemplo, porque la persona se encuentre teletrabajando en casa, porque tenga que compartir necesariamente el equipo doméstico con otros miembros de la familia, o porque sienta una falsa seguridad.

Muchas veces se tiene en cuenta que las contraseñas evitan el acceso físico de terceros al equipo (por ejemplo, en una oficina), pero olvidan que también permiten establecer una barrera de control frente a quienes acceden de forma remota al equipo y necesitan, por ejemplo, elevar privilegios.

Hay dos medidas útiles que han aumentado. Un 9,3% declara usar cifrado de documentos o datos, lo que protege en caso de pérdida o robo. Otra, menos conocida quizá, y que aumenta un 7,9%, es el uso de máquinas virtuales[4]. Su conocimiento ya sería en sí una mejora, porque permite tener en un entorno separado otro *software* que podría interferir con el equipo anfitrión. Si empleamos una máquina virtual (en la que también tomamos precauciones) para instalar las aplicaciones de usos puntuales y minimizamos la instalación de *software* en el sistema anfitrión, expondremos menos nuestro equipo personal.

Los datos recabados por Pinkerton sobre los dispositivos se reflejan en el gráfico 5. Se incluyen medidas automáticas y no automáticas que pueden obtenerse de los ordenadores.

[4] **Una máquina virtual es un *software* que simula un sistema de computación y puede ejecutar programas como si fuese un ordenador real.**

Por ejemplo, mientras que el 56,1% afirma tener las actualizaciones al día (gráfico 3), la realidad conforme los datos de Pinkerton, es que tan solo el 49,7% tiene el ordenador de casa con las últimas actualizaciones para su sistema operativo.

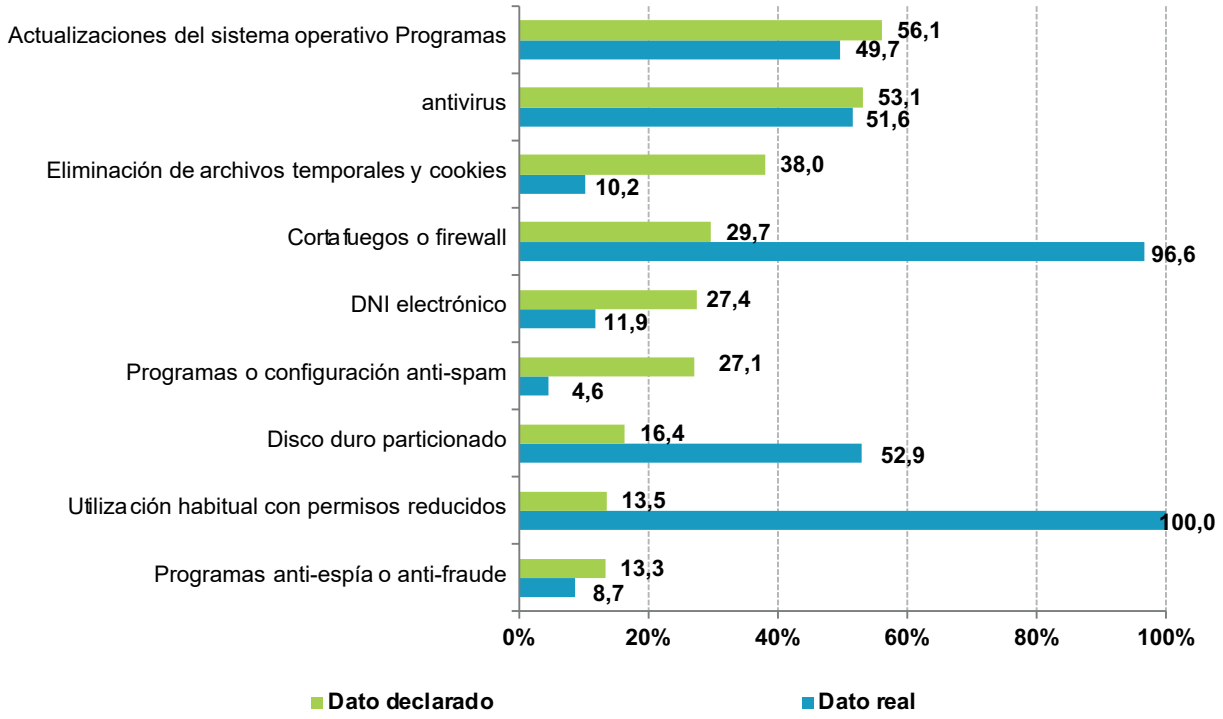
El 100% de los ordenadores del hogar analizados se utilizan habitualmente con permisos reducidos. Este dato ya se observaba en semestres anteriores y puede ser habitual en ordenadores del hogar empleados para un uso básico.

Otra medida de seguridad que también alcanza un valor de uso alto es el cortafuegos o *firewall*, que ejerce de barrera entre el equipo e Internet. Pese a que solo el 29,7% reconoció su uso, se encuentra presente en el 96,6% de las máquinas analizadas.

El uso de antivirus[5] es, según lo observado, cada vez menos popular en los equipos del hogar, las personas usuarias se conforman con la capa de seguridad que ofrece el sistema operativo (como en el caso de Windows, que emplea Defender; en el caso de MAC, se protege por contraseña el acceso a aplicaciones de terceros, por defecto bloqueadas).

En el caso del DNI electrónico los datos recabados por Pinkerton indican que el *software* para su uso solo estaba presente y activo en el 11,9% de los equipos analizados; podría referirse a momentos anteriores al escaneo, o bien a que realizan dichas operaciones con el DNI electrónico desde otros equipos facilitados para eso. También puede deberse no se sepa distinguir entre el DNI electrónico y los propios certificados.

Gráfico 5. Uso declarado vs real de medidas de seguridad en el ordenador del hogar (%)



Base: **Usuarios y usuarias de ordenador**
Fuente: **Panel hogares, ONTSI**

[5] https://www.adslzone.net/esenciales/windows/necesidad-antivirus-windows/

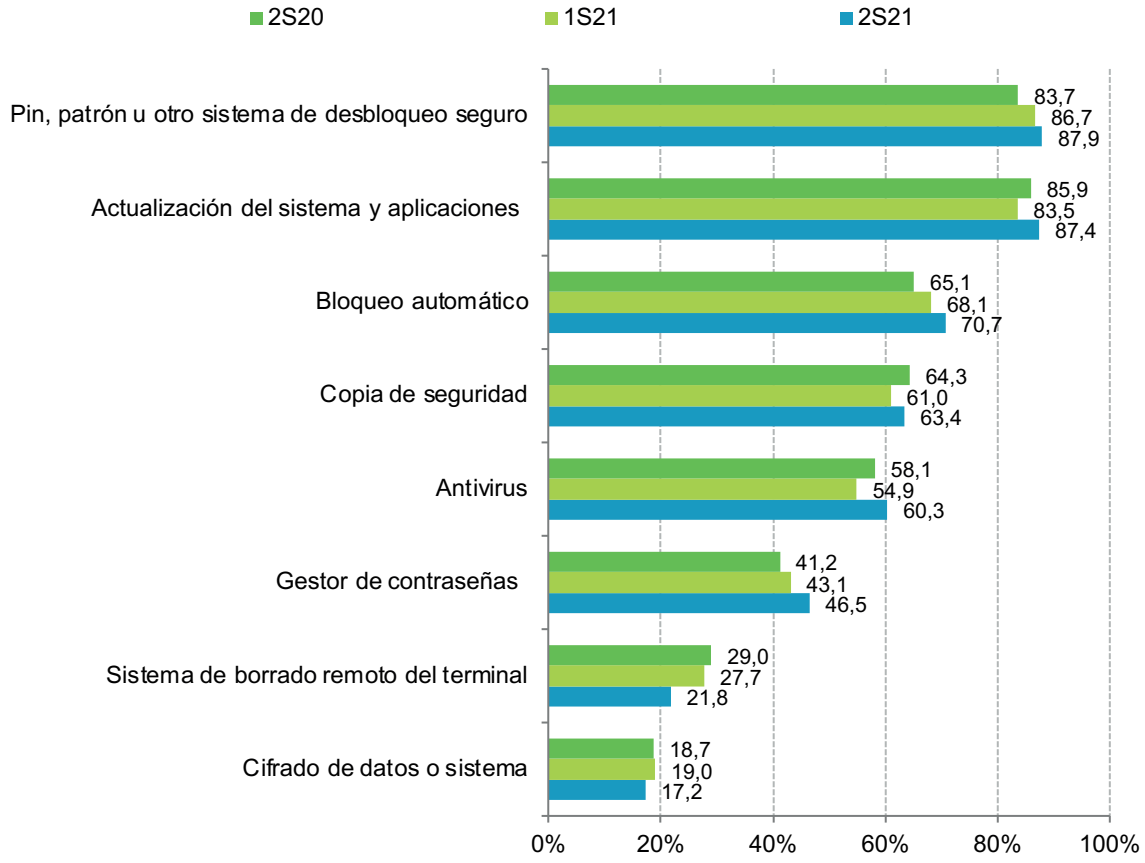
3.2. PROTECCIÓN EN LOS DISPOSITIVOS ANDROID

Se evalúa el uso habitual con permisos reducidos, el de antivirus, la utilización de PIN, patrón u otro sistema de desbloqueo seguro y el cifrado de datos o del sistema completo. Los resultados se muestran en el gráfico 6.

La medida de seguridad más popular es el uso de PIN, patrón u otro sistema de desbloqueo seguro. De hecho, durante el segundo semestre de 2021 el 87,9% declara usarlo (1,2 p.p. más respecto al periodo anterior). Este aumento puede deberse al uso de la banca electrónica y de medios de pago *contactless* en tiendas físicas. Además, las aplicaciones de banca electrónica han impuesto la autenticación de doble factor como obligatoria, y también obligan a utilizar algún medio de bloqueo del terminal[6] para evitar el robo o la utilización indebida por parte de una persona atacante.

El uso de cortafuegos, la partición del disco duro y la reducción de permisos son medidas mucho más comunes de lo que la población realmente cree.

Gráfico 6. Medidas de seguridad usadas en dispositivos android (%)



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

[6] https://cincodias.elpais.com/cincodias/2019/09/05/companias/1567710954_977920.html

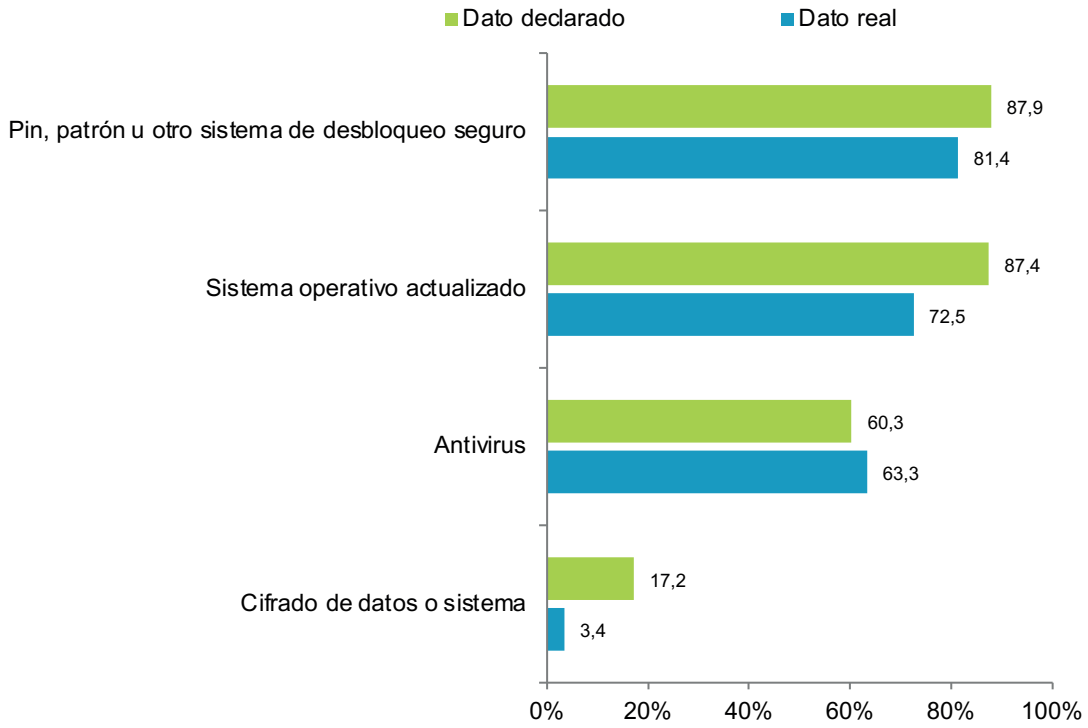
En general, los usuarios declaran que utilizan más las medidas de seguridad como las actualizaciones del sistema o las aplicaciones (87,4%), el bloqueo automático (70,7%) y las copias de seguridad (63,4%). Tal vez estas sean muy utilizadas porque se ejecutan de forma automática sin que el usuario intervenga. En cualquier caso, el usuario las percibe como seguras.

Cada vez se hace más uso de programas antivirus en los dispositivos Android.

En cuanto a los datos obtenidos como resultado del escaneo de los dispositivos que se muestran en el gráfico 7, el 81,4% de los Android analizados por el Pinkerton utiliza a ciencia cierta el PIN o patrón de desbloqueo seguro. Como se ha comentado, es una de las medidas que exigen las aplicaciones de banca electrónica para realizar trámites con el banco o pagos con el móvil. La cifra real en este caso (81,4% de los equipos) se aproxima a la declarada (87,9%).

Al contrario de lo que ocurre en el caso de los ordenadores del hogar, las personas usuarias de Android declaran que en sus dispositivos móviles sí usan antivirus. Este dato es curioso, porque hasta hace muy poco la corriente habitual era asumir que en los dispositivos móviles no era necesario. En concreto, el 63,3% alega tener instalado un antivirus[7] en su móvil. Esto quizás sea debido a que según indica el INE[8], en la actualidad se utilizan más estos dispositivos que los ordenadores para acceder a Internet. En concreto en ese estudio se menciona que, en 2021, el 32% de los usuarios accedió a Internet con ordenador de sobremesa, el 54% con portátil, el 37% con tableta y el 94% con teléfono móvil.

Gráfico 7. Uso real de medidas de seguridad en dispositivos android frente a uso declarado (%)



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

[7] https://elpais.com/tecnologia/2021-04-30/es-realmente-necesario-un-antivirus-en-el-movil-mitos-y-realidades-sobre-el-riesgo-en-estos-dispositivos.html
[8] https://www.ine.es/prensa/tich_2021.pdf

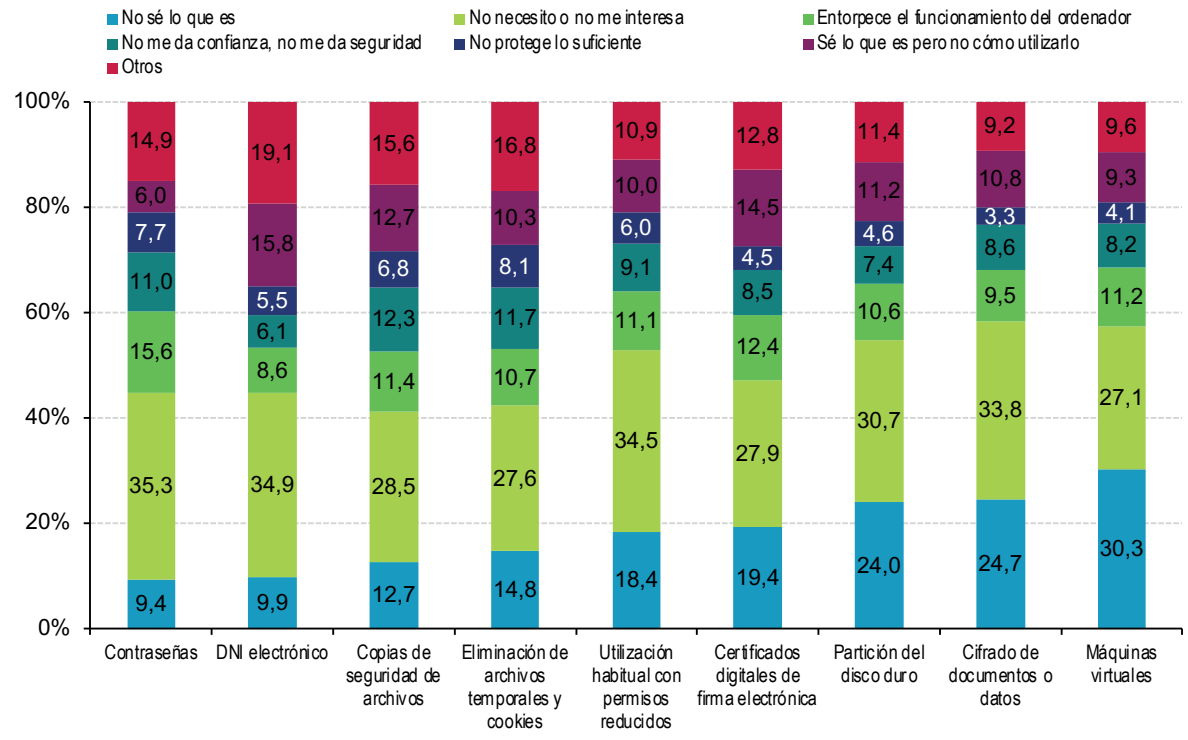
La banca electrónica, que es uno de los servicios que acompaña también al comercio electrónico, ha impulsado, para evitar casos de fraude, recomendaciones de seguridad. Entre ellas, la utilización de contraseñas seguras, el uso de gestores de contraseñas, activar el doble factor de autenticación o utilizar una VPN para acceder a la banca *online*.

Por otra parte, cada vez es más habitual el uso del móvil con permisos reducidos. Las versiones posteriores a Android 11[9] permiten cambiar los permisos de las aplicaciones en función de su uso o quitarlos automáticamente. Si una aplicación tiene permiso de acceso a los contactos del móvil, los dispositivos con Android 11 o posterior permiten que desde los ajustes se pueda cancelar ese permiso en concreto.

3.3. RENUNCIA A LAS MEDIDAS DE SEGURIDAD

Frente a las cifras que revelan el uso activo y automatizado de ciertas medidas de seguridad, es imprescindible tener en cuenta la motivación para renunciar a otras que no cuentan con tanta acogida. Los motivos que se alegan para no usar determinadas medidas de seguridad permiten comprender dónde podríamos centrar futuros puntos de mejora.

Gráfico 8. Pérdida de datos en el móvil como consecuencia de un virus (año 2020)



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

[9] https://support.google.com/googleplay/answer/9431959?hl=es

Ha aumentado el porcentaje que afirma emplear máquinas virtuales (gráfico 4), sin embargo, continúa siendo la medida más desconocida para el 30,3% de las personas entrevistadas (gráfico 8). El uso de máquinas virtuales posibilita crear entornos para poder hacer pruebas, además hace posible el tener diferentes sistemas operativos en un mismo dispositivo, o evitar la dependencia entre diferente *software*.

El porcentaje de internautas que asegura emplear el DNI electrónico (gráfico 4) ha crecido respecto al de quienes aseguran no usarlo. El 34,9% afirma que no lo ve necesario. Esto quizás pueda ser debido a que en su lugar emplean el certificado digital. Aunque también existen las opciones de utilizar los sistemas de autenticación de *cl@ve permanente, cl@ve pin* o vía SMS. Los datos reflejan que hay menos personas que han respondido que no necesitan el certificado digital o que no les interesa.

Sin embargo, el aumento de los trámites con la Administración ha dado lugar a que más personas necesiten usar el DNI electrónico o el certificado digital para autenticarse y firmar documentos. Esto hace que, respecto al semestre anterior, disminuya el número de personas que desconocen o no están interesados en estos medios de identificación digital.

Los principales motivos para renunciar a medidas de seguridad están relacionados con la percepción de que no son necesarias o interesantes, pero también en gran medida con su desconocimiento.

4 Hábitos relacionados con la seguridad y comportamientos de riesgo

Más allá de las medidas de seguridad adoptadas, las pautas de uso tanto de ordenadores como de dispositivos portátiles pueden incrementar o reducir los riesgos de tener algún tipo de problema relacionado con la ciberseguridad. Las costumbres *online* determinan en gran medida la exposición a los ataques. En esta sección, el análisis de los hábitos en cuanto a la navegación y los usos de Internet busca entender cómo influyen éstos en las conductas de riesgo.

Algunas de las conductas más destacables, junto con el aumento generalizado del uso de servicios de Internet, son el acceso a contenidos digitales gratuitos desde webs no oficiales, la descarga e instalación de *software*, y el comercio *online* y las transacciones no verificables. Sin embargo, no son las únicas.

La descarga de contenidos y programas gratuitos desde webs no oficiales o dudosas sigue siendo una de las principales prácticas de riesgo.

Antes de abordar estos puntos resulta de interés conocer el punto de vista de las personas usuarias en cuanto a las conductas consideradas de riesgo, para disponer de una visión general del problema y su posible alcance.

4.1. EVOLUCIÓN DE LAS CONDUCTAS DE RIESGO

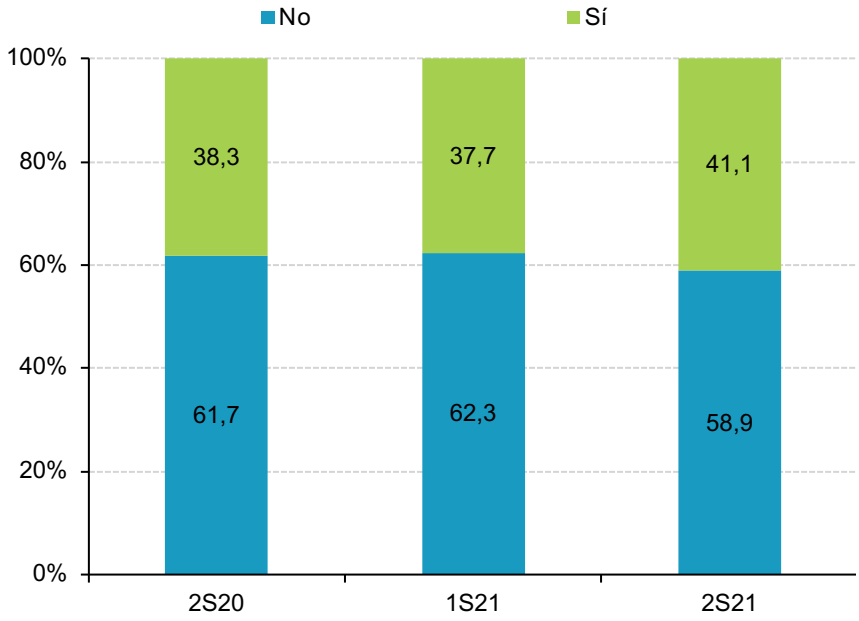
El gráfico 9 refleja la realización consciente de conductas de riesgo en la red. En este último semestre este tipo de conductas aumentan en 3,4 p.p. respecto al anterior, el hecho de exponer sus dispositivos, así como los datos almacenados en ellos.

El 41,1% declara realizar alguna conducta de riesgo a sabiendas. Navegar sin tener las actualizaciones al día, deshabilitar el antivirus o hacer clic en enlaces que redirigen a un sitio web, son algunos de los hábitos de riesgo que se realizan y que se recogen en la gráfico 10.

Las actualizaciones de seguridad de los sistemas operativos y aplicaciones tanto móviles como de ordenador son importantes, y sin embargo un 39,6% reconoce no saber con seguridad si su equipo está actualizado. Con este tipo de actualizaciones se solucionan o parchean problemas de seguridad críticos que hacen vulnerable el dispositivo, y se resuelven errores del *software* que también podrían facilitar un ataque.

El 41% declara realizar alguna conducta de riesgo a sabiendas y el 40% reconoce no saber con seguridad si su equipo está actualizado.

Gráfico 9. Realización consciente de alguna conducta de riesgo (%)



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

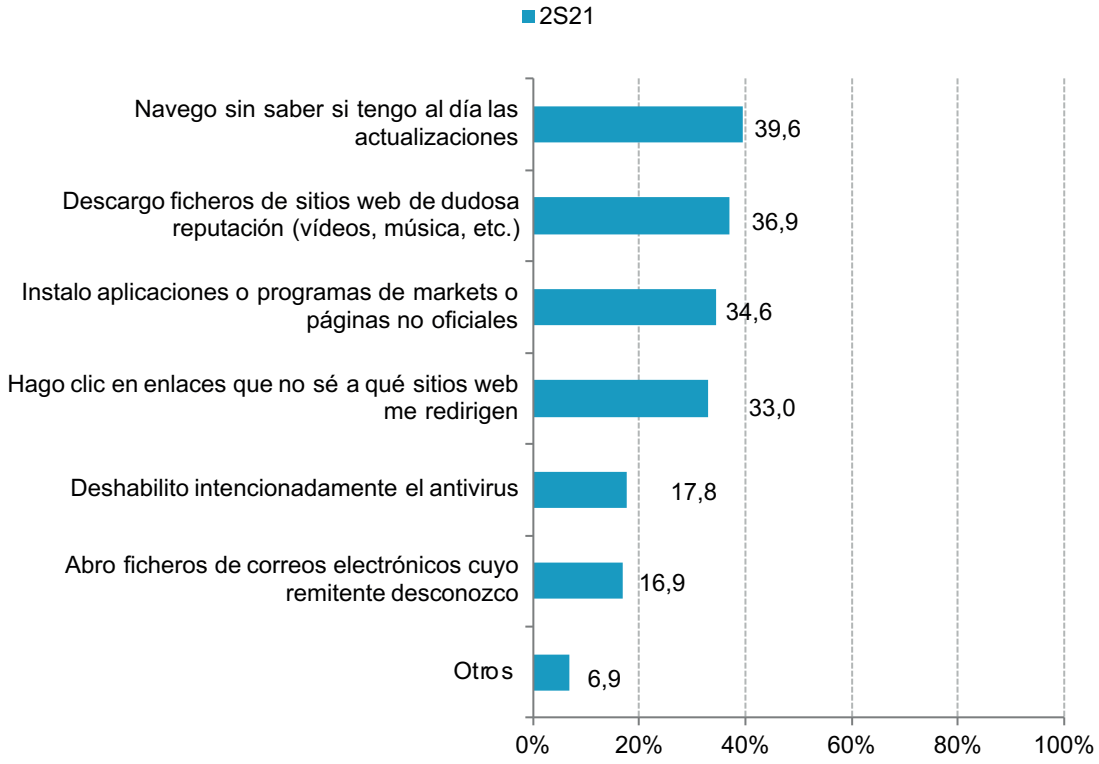
Respecto a conductas de riesgo relacionadas con la descarga de vídeos, música y otros tipos de ficheros, el 36,9% de las personas usuarias utiliza sitios web de dudosa reputación para realizar descargas. Estos son susceptibles de contener amenazas para los ordenadores y dispositivos. El principal riesgo es la posible infección por *malware*, que además puede conllevar robo de información o credenciales bancarias, extorsión y un posible perjuicio económico.

La instalación de programas desde aplicaciones no oficiales (realizada por el 34,6% de quienes responden) es un factor de riesgo que acompaña al punto anterior, dado que es otra vía de entrada para el *software* malicioso en nuestro ordenador o dispositivo móvil.

Además, el 33% afirma que hace clic en enlaces aun sin saber a qué sitio web le redirige, sumado al 16,9% que indica abrir ficheros de remitentes desconocidos, siendo ambas dos comprobaciones imprescindibles para evitar *phishing* (captación de datos privados). Además, el análisis de los archivos descargados es imprescindible para minimizar el riesgo de infección por *malware*. Sin embargo, el 17,8% afirma deshabilitar el antivirus conscientemente. Sin duda estos tres factores son ventajas claras para los atacantes que preparan campañas de *phishing*, dado que supone un amplio abanico de víctimas potenciales.

A continuación, se describen riesgos que se han visto potenciados durante este último semestre por el uso de los servicios de Internet.

Gráfico 10. Realización consciente de alguna conducta de riesgo (%)



Base: **Usuarios o usuarias que realizan alguna conducta de riesgo.**
Fuente: **Panel hogares, ONTSI**

4.2. RIESGOS RELACIONADOS CON LA DESCARGA DE CONTENIDOS GRATUITOS

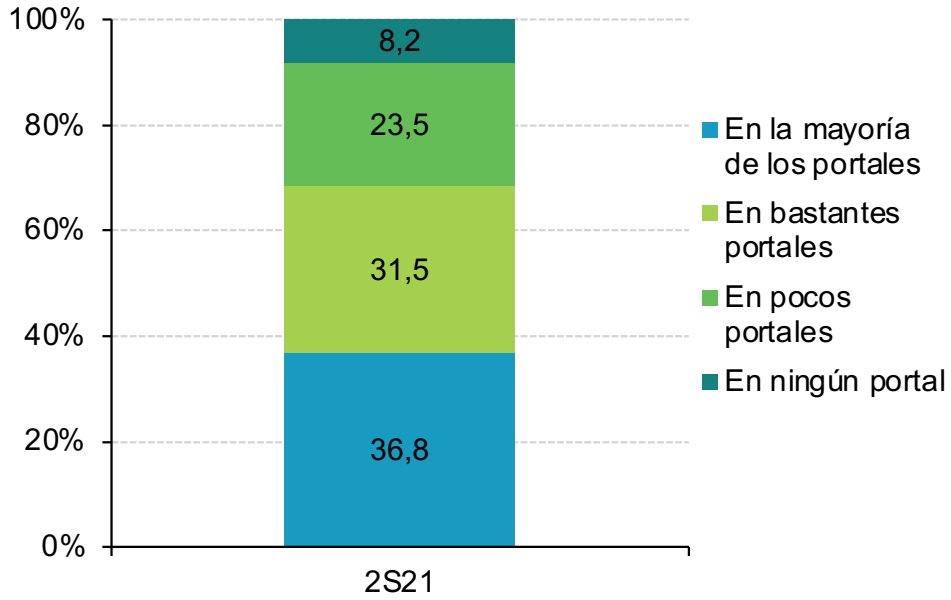
Una de las principales conductas de riesgo está relacionada con el fácil acceso a contenidos gratuitos, cuya descarga puede esconder riesgos de seguridad de diferente magnitud.

Es destacable el hecho de que el acceso a contenidos digitales gratuitos ha descendido en 2,6 p.p. durante la pandemia de Covid-19, en línea con un mayor uso de plataformas de pago para la visualización de contenido en *streaming*. No obstante, el 66,8% continúa haciendo algún uso de portales de descarga de este contenido, que en muchos casos supone un claro riesgo para la seguridad de los dispositivos. Por ejemplo, las plataformas de descarga gratuita requieren en la mayoría de los casos registro previo para la visualización o descarga del contenido. Conforme a las declaraciones, el 68,3% indica que en la mayoría o bastantes de los portales han tenido que registrarse para acceder al contenido (gráfico 11).

El riesgo en este punto se centra en que proporcionan sus datos a terceros y pueden ser usados, por ejemplo, para su posterior venta a otros terceros, empleados en campañas de *spam* y *phishing*, o para posibles ataques de ingeniería social, dependiendo de la cantidad de datos proporcionada.

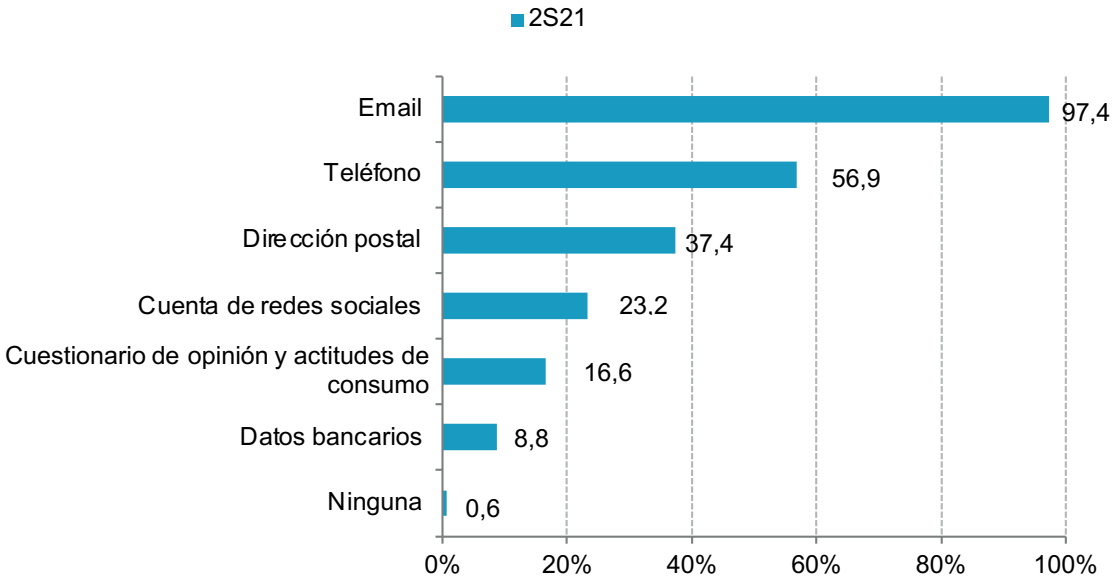
A este respecto, el gráfico 12 recoge los principales datos solicitados para el registro en dichas páginas. Destacan la dirección de email y el teléfono, precisamente dos datos que se emplean asiduamente para los tipos de fraude cubiertos en este estudio (Sección 5.4).

Gráfico 11. Necesidad de registro para el acceso o descarga de contenido gratuito (%)



Base: Usuarios o usuarias que acceden o descargan contenido gratuito.
Fuente: Panel hogares, ONTSI

Gráfico 12. Datos solicitados para completar los registros en portales de descarga de contenido gratuito (%)



Base: Usuarios y usuarias que se registran en portales de descarga de contenido gratuito
Fuente: Panel hogares, ONTSI

Además, la cesión de estos datos y su posible venta a terceros se traduce en un aumento significativo de la publicidad no deseada, declarada por el 76,9% (gráfico 13).

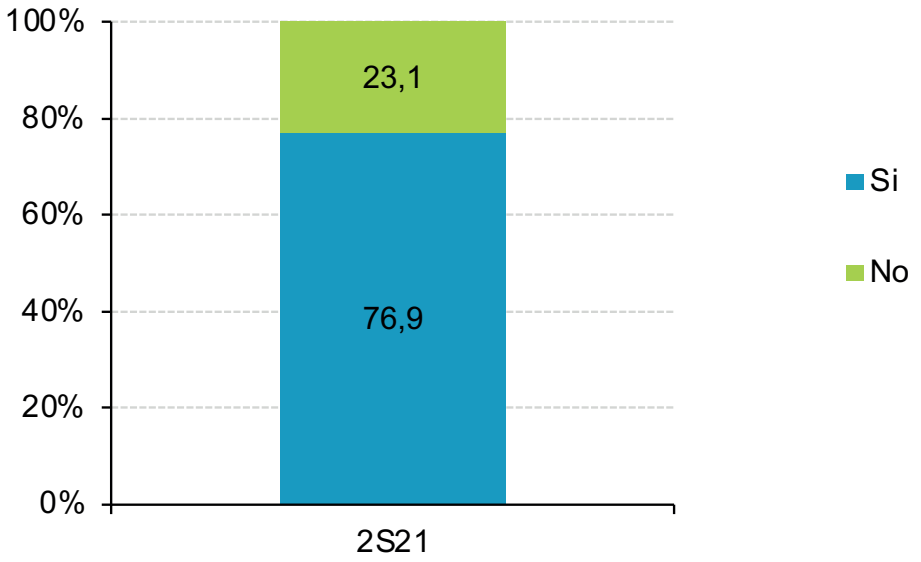
Pese a los riesgos, tras el periodo de confinamiento el 53% de estos continúan recurriendo con la misma frecuencia a las descargas gratuitas, manteniendo los mismos hábitos de la crisis sanitaria (gráfico 14). Tan solo el 14,9% manifiesta disminuir las descargas frente al 32% restante que ha aumentado el hábito.

El 32% de los internautas incrementó la descarga de contenidos gratuitos tras el confinamiento.

Ciertamente se produce un descenso en las descargas gratuitas, aunque aún es una costumbre que se mantiene. Los descensos que se observan pueden deberse no solo al mayor uso de las plataformas de *streaming*, sino también a la cada vez mayor concienciación.

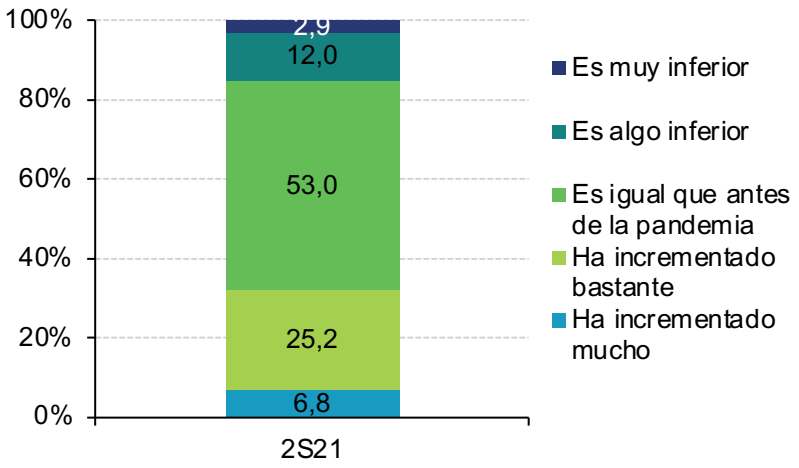
En particular, se es más consciente de los peligros de las descargas y la ejecución de archivos gratuitos de los que se desconoce el contenido interno, en gran parte gracias a las campañas de concienciación impulsadas por la Administración.

Gráfico 13. Incremento de la publicidad tras la utilización de los accesos gratuitos (%)



Base: **Usuarios y usuarias que acceden o descargan contenido gratuito**
Fuente: **Panel hogares, ONTSI**

Gráfico 14. Acceso o descarga de contenidos digitales gratuitos tras el confinamiento (%)



Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

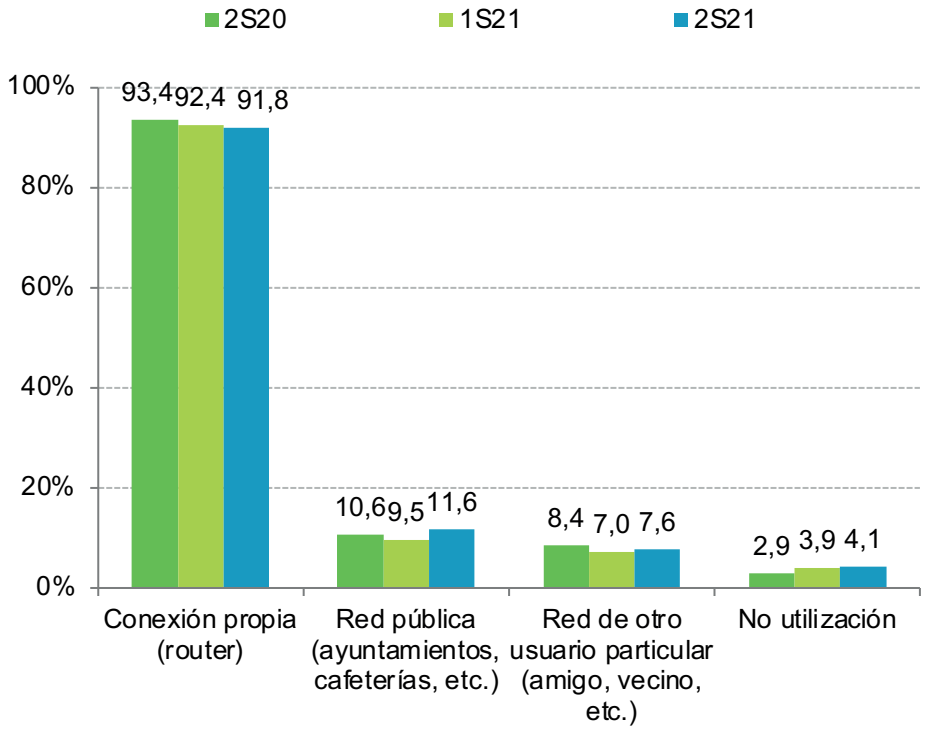
4.3. ACCESO A REDES WI-FI DESCONOCIDAS

El uso de estas redes inalámbricas supone un riesgo si no se toman medidas de seguridad. Emplear puntos Wi-Fi desconocidos o ajenos a la conexión propia del hogar supone un riesgo, ya que pueden tratarse de intermediarios no confiables.

El gráfico 15 destaca la evolución en los hábitos de conexión a redes inalámbricas Wi-Fi. En los tres últimos semestres ha disminuido ligeramente la conexión a través del rúter propio (un 91,8% dispone de conexión propia a través de él) o del equipo doméstico para conectarse a otras redes públicas en su lugar. Para proteger la red del hogar es importante cambiar las contraseñas por defecto por otras seguras que solo conozca la persona usuaria.

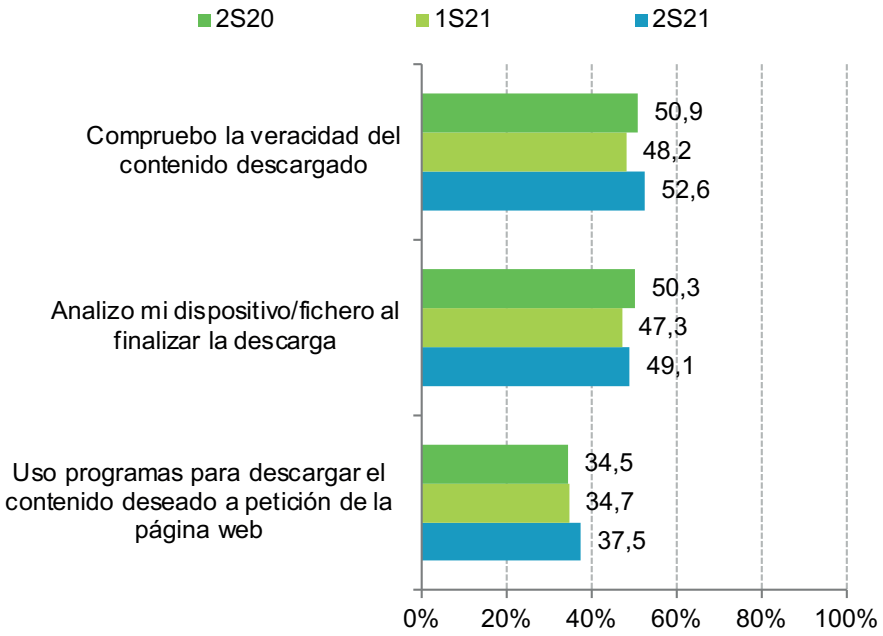
Pese a que un gran número de internautas dispone de red inalámbrica en el hogar, fuera de casa aún existe un porcentaje (11,6%) que utiliza redes públicas, ya sean de Ayuntamientos, cafeterías, aeropuertos, etcétera. Estas últimas son más susceptibles (sobre todo si son abiertas) a la captura ilegítima de tráfico de red por parte de atacantes, suplantando al rúter del lugar, accediendo a todo el tráfico de red y la pertinente información que se comparte a través de Internet. De esta forma, un atacante puede hacerse con credenciales de acceso o información privada de quien esté conectado a la red.

Gráfico 15. Punto de acceso a internet mediante redes inalámbricas Wi-Fi (%)



Base: Total de usuarios y usuarias
Fuente: Panel hogares, ONTSI

Gráfico 16. Comportamiento relacionado con la descarga directa de archivos, programas, documentos, etc. (%) (2s 2020 – 2s 2021)



Base: Total de usuarios y usuarias
Fuente: Panel hogares, ONTSI

4.4. DESCARGA E INSTALACIÓN DE ARCHIVOS Y PROGRAMAS

Independientemente de si se trata de contenidos gratuitos o no, la entrada de nuevos elementos en los equipos puede ocasionar puntos críticos para la seguridad del sistema, ya que cualquier ejecución de *software* ilegítimo es capaz de comprometer el correcto funcionamiento del sistema. En este sentido, el gráfico 16 ofrece una visión general del comportamiento relacionado con la descarga directa de archivos y programas.

No obstante, las personas usuarias no solo realizan prácticas de riesgo al hacer uso de servicios digitales. Durante este semestre aumentan estas tres buenas prácticas: comprobar la veracidad del contenido descargado (52,6%), analizar el dispositivo tras la descarga (49,1%), y usar programas para la descarga del contenido web (37,5%).

No obstante, el comportamiento puede variar dependiendo del tipo de dispositivo empleado para la realización de las descargas. Existen diferencias en las pautas de uso entre el ordenador y los dispositivos móviles, motivo por el cual el análisis se realiza de manera diferenciada.

En el caso de los **ordenadores en el hogar**, se ha preguntado si se presta atención a los pasos de instalación, si se realizan comprobaciones minuciosas sobre el programa que están instalando y si se leen la hoja de licencia y condiciones de uso. Tan solo el último punto se incrementa respecto al semestre previo, aunque ligeramente, en 1,5 p.p. (gráfico 17).

El 75,4% asegura prestar atención a los pasos de instalación, que puede ser una buena práctica no solo por la identificación de posibles errores, sino también para identificar conductas anómalas: por ejemplo, aparición de terminales con código no propio de una aplicación dirigida a usuarios y usuarias. Este porcentaje ha disminuido considerablemente frente al 81,6% del segundo semestre de 2020.

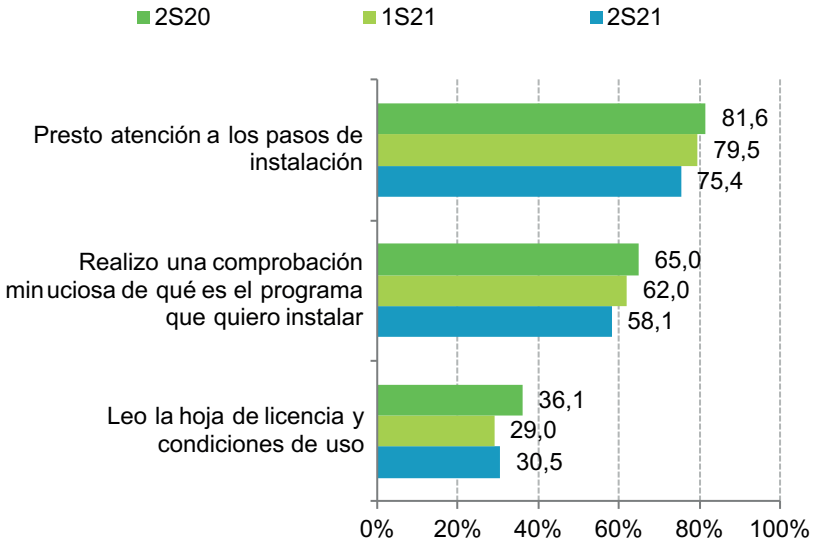
El 86% de usuarios descarga las apps para sus dispositivos móviles desde repositorios o tiendas oficiales.

Antes de realizar una descarga o registrarse en una web, es recomendable conocer la aplicación que se desea instalar, así como los términos de uso. La relación contractual entre el proveedor de un servicio o un programa con el cliente viene especificada en la hoja de licencia y en las condiciones de uso. Según las declaraciones de las personas entrevistadas, en comparación con el semestre anterior, en este último, la proporción de personas que leen dicha documentación se ha incrementado en 1,5 p.p.

Las pautas de descarga en dispositivos Android obedecen a una lógica diferente. A modo de ejemplo, la aparición de troyanos y diferentes tipos de *software* maligno en las aplicaciones descargadas desde sitios no oficiales, es un problema para los usuarios.

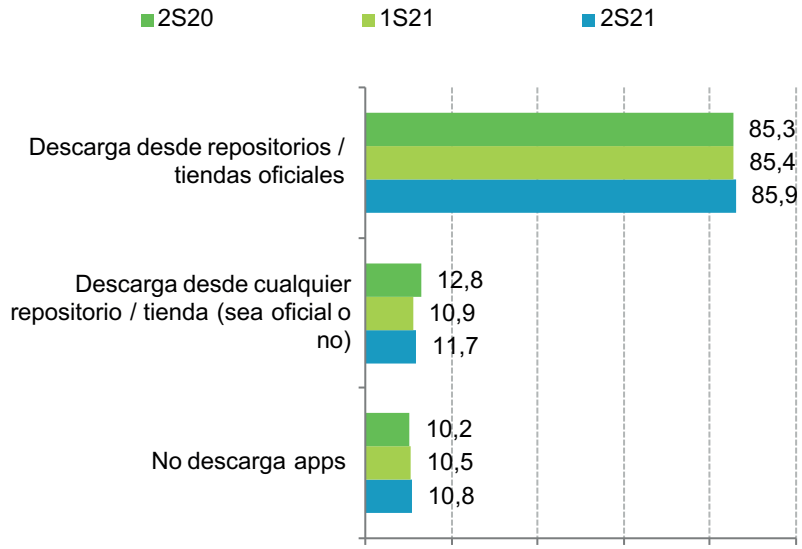
El gráfico 18 ofrece una comparativa de los últimos tres semestres en la que se percibe un aumento muy leve en el número de panelistas que prefieren descargar aplicaciones desde repositorios y tiendas oficiales (85,9%, un incremento de 0,5 p.p.). No obstante, también aumenta levemente el porcentaje quienes declaran descargar desde cualquier repositorio no oficial (11,7%, un incremento de 1,2 p.p.).

Gráfico 17. Comportamientos en la instalación de programas en ordenadores en el hogar (%)



Base: **Total de usuarios y usuarias de ordenadores**
Fuente: **Panel hogares, ONTSI**

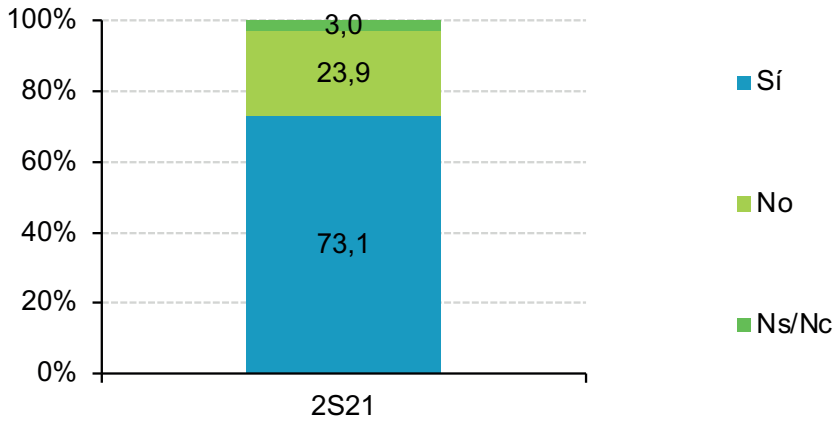
Gráfico 18. Comportamientos en la descarga de apps en el smartphone o tablet (%)



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

Otra buena práctica antes de descargar e instalar una aplicación es leer los comentarios y valoraciones, algo que proporcionan los *markets* y sitios oficiales de descarga. El de 73,1% quienes descargan aplicaciones para su dispositivo Android declara poner en práctica esta medida (gráfico 19). Por otro lado, el 23,9% de personas dentro del grupo reconoce no fijarse en este aspecto antes de instalar una aplicación.

Gráfico 19. Verificar los comentarios y valoraciones de otros usuarios (%)



Base: **Usuarios y usuarias que disponen de dispositivo Android y descargan apps.**
Fuente: **Panel hogares, ONTSI**

4.5. COMERCIO *ONLINE* Y TRANSACCIONES ELECTRÓNICAS

Una fuente adicional de riesgo reside en las actividades relacionadas con el comercio *online* y la realización de transacciones electrónicas, debido al evidente factor económico implicado en dichas actividades.

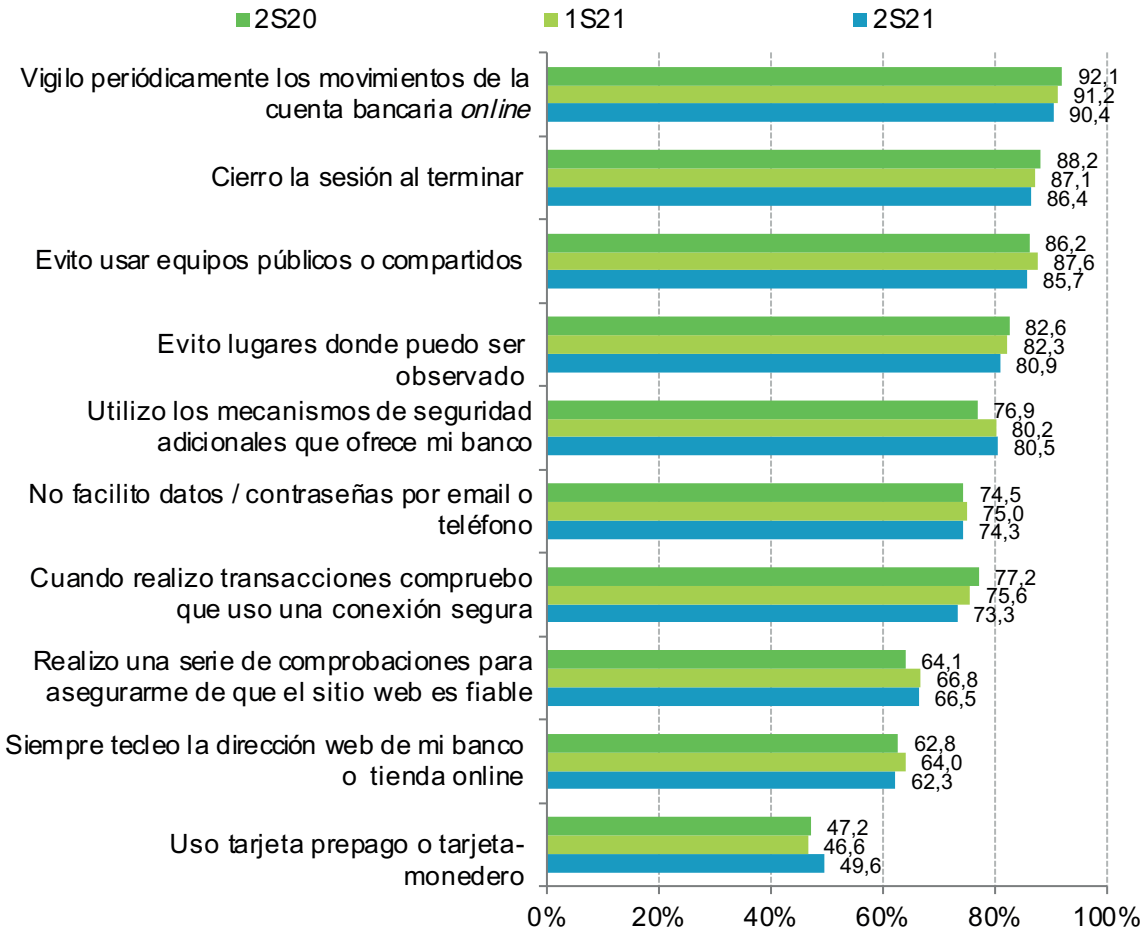
Desde el inicio de la pandemia, el aumento del comercio electrónico es notable. El gráfico 20 recoge los hábitos de comportamiento destinados a garantizar la seguridad declarados en el uso de servicios de banca *online* o comercio electrónico.

Entre las declaraciones de los internautas destacan positivamente el aumento del uso de tarjetas prepago o monedero (49,6%, una subida de 3 p.p.) y la utilización de los mecanismos de seguridad ofrecidos por el banco (80,5%, subiendo 0,3 p.p.).

Por otro lado, parece ser que la confianza en la banca electrónica hace que las personas entrevistadas manifiesten que no comprueban si tienen una conexión segura antes de realizar las transacciones. En concreto ha disminuido la comprobación en 2,3 p.p. respecto al semestre anterior.

Esta relajación, probablemente motivada por el exceso de confianza, afecta no solo a las transacciones, sino al resto de parámetros que descienden, y puede ser una mala práctica que derive en escenarios efectivos de *phishing*.

Gráfico 20. Hábitos de comportamiento en el uso de servicios de banca *online* o comercio electrónico (%)



Base: **Usuarios y usuarias que utilizan banca online y/o comercio electrónico.**
Fuente: **Panel hogares, ONTSI**

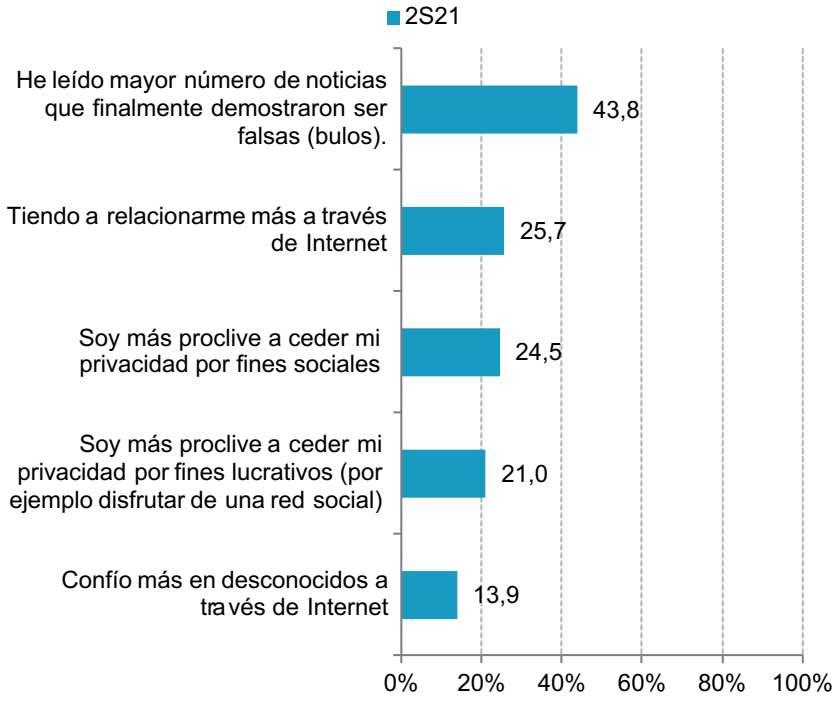
4.6. HÁBITOS ADQUIRIDOS A RAÍZ DE LA PANDEMIA

Cabe esperar que una mayor actividad *online* en el contexto de una situación excepcional, como la originada por la Covid-19, sea origen de una mayor reflexión acerca de los comportamientos digitales, sus riesgos y consecuencias. Para la elaboración de este estudio se ha pedido a las personas encuestadas que identifiquen los hábitos adquiridos tras el confinamiento originado por la pandemia de Covid-19. Los resultados declarados pueden consultarse en el gráfico 21.

Un 43,8% ha leído noticias que resultaron ser falsas. Las llamadas *fake news* son un problema acentuado durante la pandemia que persiste actualmente. Páginas como VerificaRTVE, Maldita o Newtral[10] permiten a las personas internautas contrastar algunas de las noticias para determinar si son o no falsas. El ser cada vez más conscientes de esta problemática es una buena noticia, pero aún queda mucho por hacer en esta línea.

[10] https://www.newtral.es/zona-verificacion/fact-check/

Gráfico 21. Percepción sobre los hábitos adquiridos tras el confinamiento o motivado por la pandemia (%)



Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

Por otro lado, el 25,7% asegura que tras la pandemia tiende a relacionarse más a través de Internet, incluso con gente que no conoce. El 13,9% asegura confiar más en desconocidos a través de Internet, lo que podría ser un problema, que derive en casos de fraude o abusos.

Respecto a la cesión de la privacidad, los fines sociales (24,5%) se imponen a los fines lucrativos[11] (21%) por 3,5 p.p. Cabe destacar que diversas campañas de fraude han aprovechado fines sociales para conseguir víctimas[12].

Un 26% de los usuarios incrementó sus relaciones a través de Internet, incluso con gente desconocida.

[11] Los fines sociales hacen referencia a la instalación de aplicaciones que no implican una finalidad con ánimo de lucro y los fines lucrativos hacen referencia a la instalación de aplicaciones que pueden obtener beneficio de la recopilación de datos personales (como redes sociales).
[12] https://www.caixabank.es/particular/seguridad/fraude-del-romance.html

5 Incidentes de seguridad

Unos hábitos *online* inadecuados pueden traducirse en incidentes de seguridad. En esta sección se abordan tanto los incidentes declarados por los usuarios, como los contrastados mediante los datos recabados por el *software* Pinkerton, que analiza entre otros aspectos la presencia de *malware* y las situaciones en las que los dispositivos se han visto comprometidos.

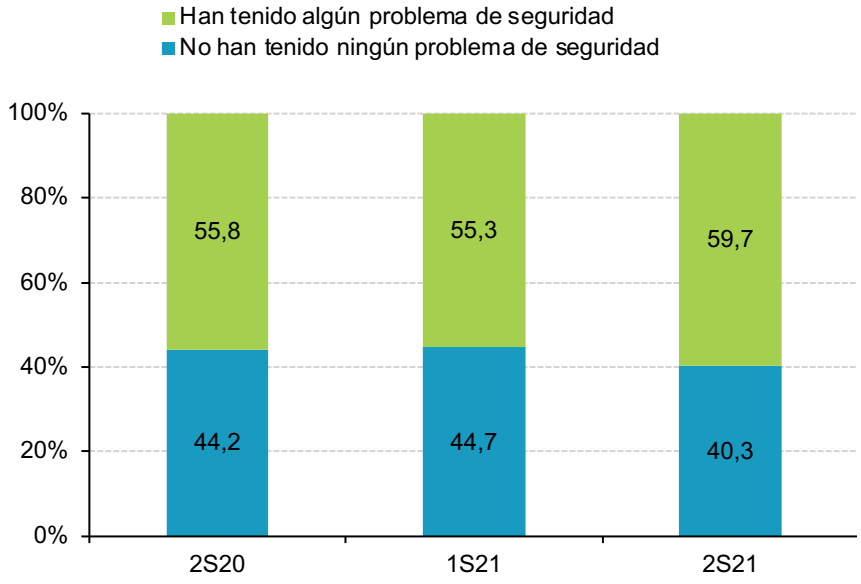
5.1. VISIÓN GENERAL DE LOS INCIDENTES

El 59,7% afirma haber sufrido un incidente de seguridad en el último semestre, un aumento de 4,4 p.p. respecto al semestre anterior (gráfico 22).

Los resultados de las numerosas campañas de *phishing* que se han realizado durante este semestre se ven reflejadas en las declaraciones de los usuarios, en el gráfico 23. El 84,6% afirma haber recibido correos electrónicos que no ha solicitado.

Los incidentes de seguridad declarados aumentan del 55% al 60% durante el último semestre.

Gráfico 22. Incidencias de seguridad en el dispositivo con el que se accede habitualmente a internet (%) 2º semestre 2020 al 2º semestre 2021

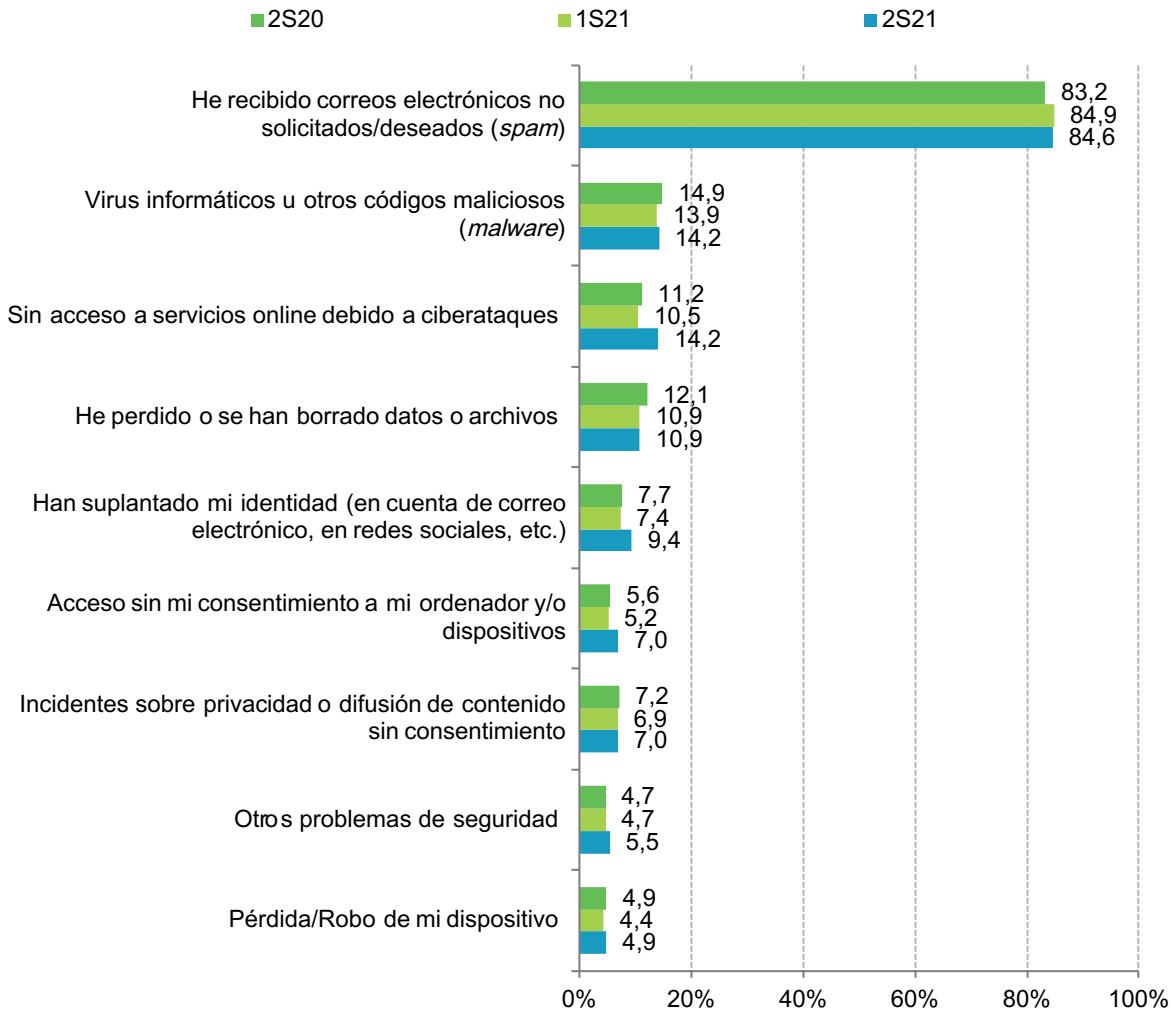


Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

A una gran distancia, el 14,2% manifiesta haber sufrido el ataque de virus o códigos maliciosos, y con esa misma cifra reconocen haberse quedado sin acceso a servicios debido a ciberataques. A este respecto, los ataques de denegación de servicio, según declara Pascal Geenens director de inteligencia y amenazas de Radware[13], han aumentado en el segundo semestre de 2021 en comparación con los detectados en el mismo semestre de 2020. Otro motivo por el que se ha tenido problemas de acceso a servicios es el *ransomware* (secuestro de datos), que no ha dejado de estar presente a lo largo del año.

La incidencia de virus o códigos maliciosos y la relacionada con la restricción de acceso por ciberataques ascienden al 14%.

Gráfico 23. Problemas de seguridad identificados (%). (2s 2020 – 2s 2021)



Base: **Usuarios y usuarias que han sufrido alguna incidencia de seguridad.**
Fuente: **Panel hogares, ONTSI**

[13] https://www.redeszone.net/noticias/seguridad/ataques-ddos-bloqueados-octubre-2021-aumentan-75/

Según ESET[14], se ha producido un aumento en la cantidad de víctimas de esta técnica de engaño respecto al año anterior.

Por otro lado, casi un 11% de las víctimas reconoce haber perdido o que se les han borrado datos o archivos de sus dispositivos.

Los problemas de suplantación de identidad en cuentas de correo y redes sociales también se han visto incrementados según se recoge en la muestra; el 9,4% de quienes sufrieron algún problema de seguridad afirma haber tenido una incidencia de este tipo. La suplantación de identidad en ocasiones es utilizada por los atacantes para realizar campañas de *phishing* con enlaces fraudulentos y llegar a un mayor número de víctimas.

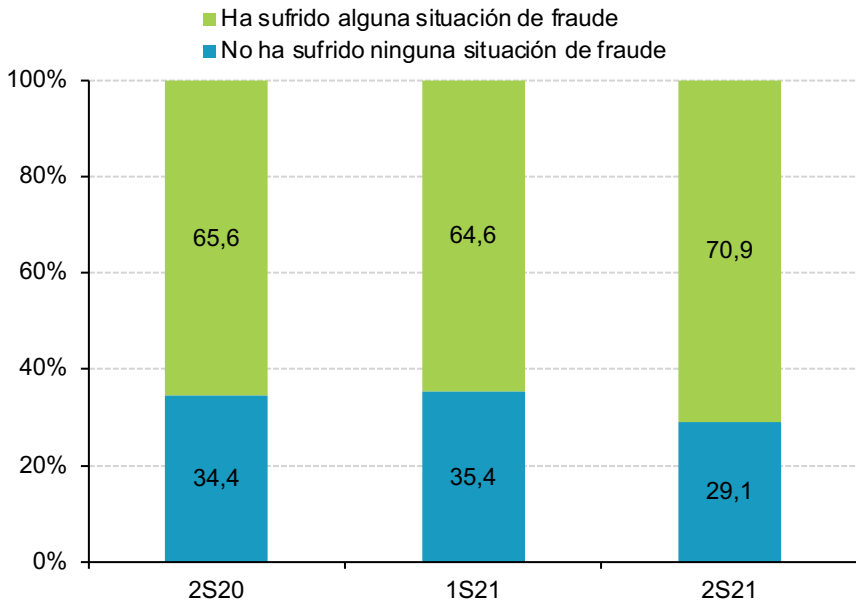
5.2. AUMENTO DE LAS SITUACIONES DE FRAUDE *ONLINE*

El fraude tiene múltiples vertientes y formas de efectuarse, aunque el objetivo final del mismo sigue siendo económico. Durante el segundo semestre de 2021 el porcentaje de quienes aseguran sufrir fraude ha aumentado al 70,9%, lo que supone una subida de 6,3 p.p. sobre el semestre anterior.

El fraude es más efectivo cuanta más información conocen las personas atacantes sobre las víctimas, pero también pesa su confianza y su predisposición. Como ya se ha comentado, precisamente tras la pandemia se han desarrollado hábitos que podrían contribuir positivamente a prácticas fraudulentas. Por ejemplo, la predisposición a confiar en desconocidos a través de Internet, o la cesión de datos entre otros (gráfico 21).

Entre los indicios o situaciones de fraude detectados (gráfico 25) destacan: la invitación a visitar alguna web sospechosa (63,2%), ofrecimiento de servicios o productos no solicitados (46,5%), recepción de

Gráfico 24. Ocurrencia de alguna situación de fraude (%) (2s 2020 – 2s 2021)



Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

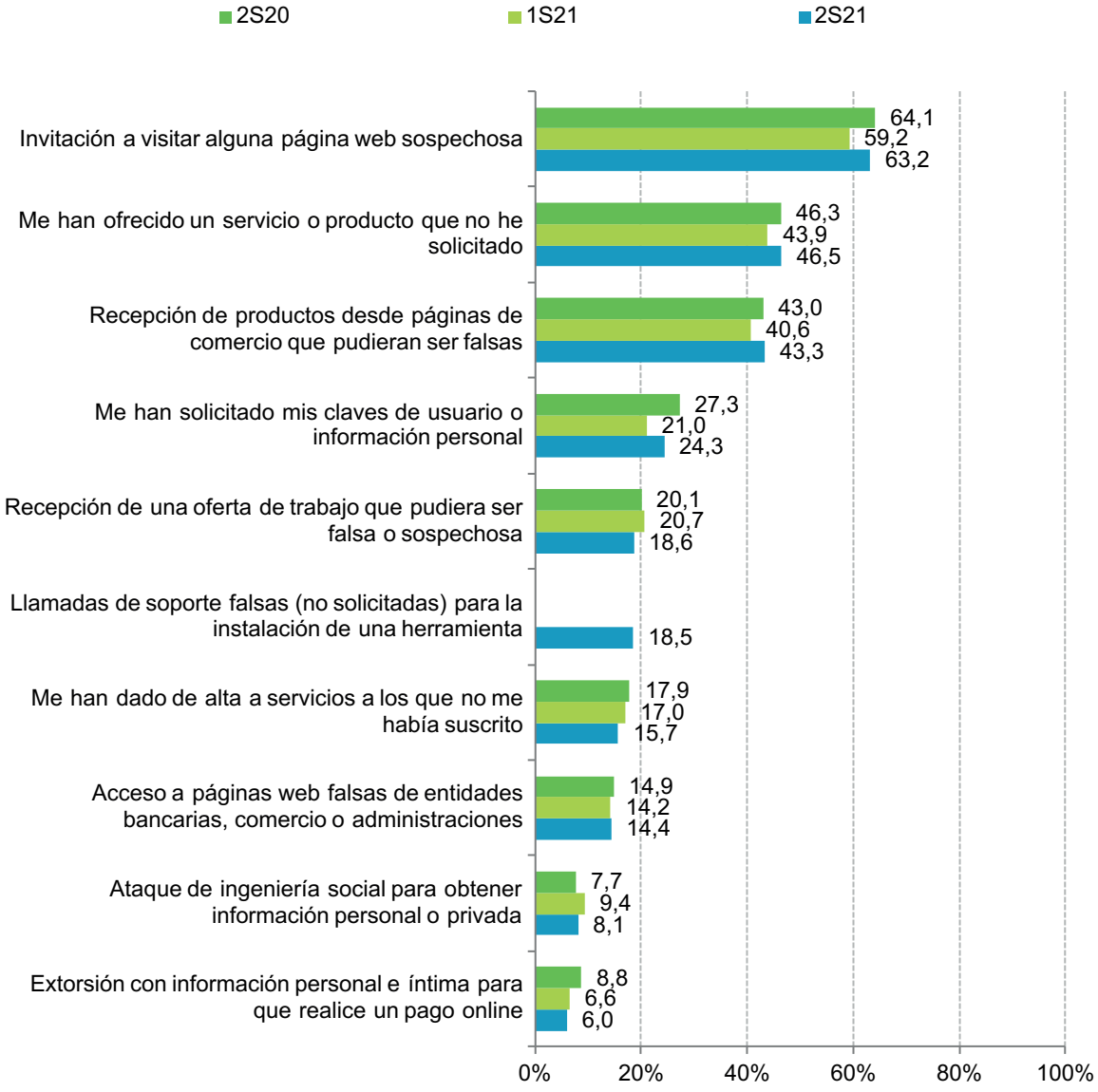
[14] https://www.welivesecurity.com/la-es/2021/12/20/ransomware-2021-datos-ataques-grupos-mas-activos/

productos desde páginas potencialmente falsas (43,3%) y la solicitud de claves de usuario o información personal (24,3%).

Todos estos se sitúan en las fases iniciales del fraude, donde se intenta captar de alguna forma el interés de la víctima, o directamente, como se ha mencionado, hacerse con sus claves de acceso a servicios entre los que destacan los bancarios.

El 71% de los internautas ha sufrido una situación de fraude.

Gráfico 25. Situaciones de fraude ocurridas (%) (2s 2020 – 2s 2021)



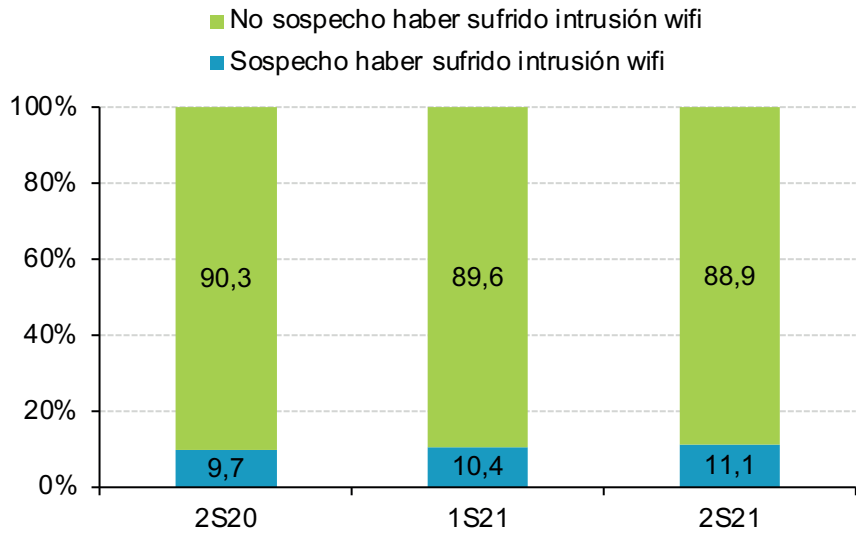
Base: **Usuarios y usuarias que han sufrido alguna situación de fraude**
Fuente: **Panel hogares, ONTSI**

5.3. INTRUSIONES A TRAVÉS DE WI-FI

Los riesgos asumidos por la conexión a través de redes Wi-Fi abiertas, o bien la relajación en cuanto al cumplimiento de las políticas de contraseñas adecuadas, se traduce en muchos casos en intrusiones Wi-Fi (la conexión a la red Wi-Fi sin consentimiento por parte de terceros).

De hecho, conforme a las declaraciones recogidas, el 11,1% de éstos sospecha haber sufrido alguna intrusión en su red Wi-Fi durante el segundo semestre de 2021 (gráfico 26).

Gráfico 26. Sospecha de haber sufrido una intrusión WI-FI (%)



Base: **Usuarios con conexión Wi-Fi propia**
Fuente: **Panel hogares, ONTSI**

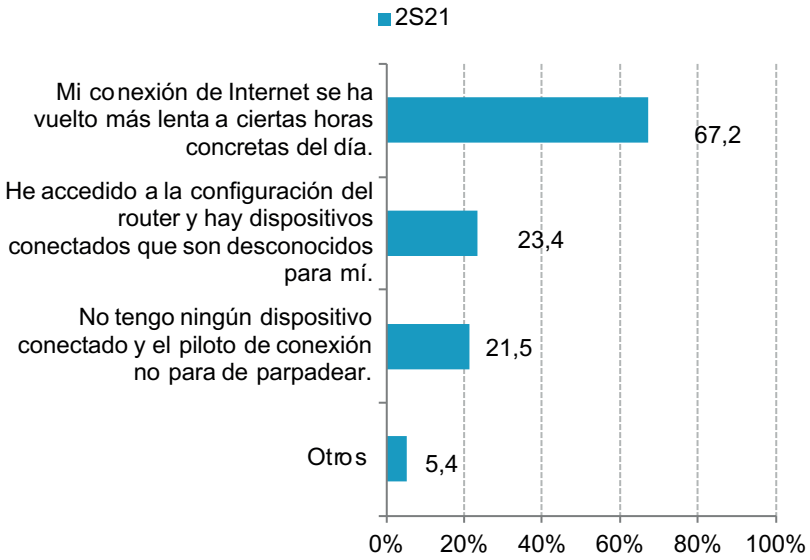
Cuando hay una intrusión en la Wi-Fi del hogar, se puede detectar de diferentes maneras: lentitud en la red, tener dispositivos desconocidos conectados en el panel de Administración del *rúter*, etc. Estos son algunos de los indicios señalados por las personas que afirman haber sufrido una intrusión Wi-Fi (gráfico 27).

Si algún intruso o intrusa está consumiendo el ancho de banda, es posible notar que la red va más lenta. Éste es el motivo principal aducido por el 67,2% de quienes creen haber podido sufrir una intrusión en la red Wi-Fi de su hogar para justificar esta creencia. Sin embargo, aunque es un indicio factible, no tiene siempre esa causa. También una configuración no adecuada de la red o el uso excesivo de dispositivos del hogar conectados podría afectar al rendimiento de la red hoy día.

Otro parámetro más fiable para intuir una posible conexión no autorizada en nuestra red es acceder a la configuración del rúter del hogar. Este permite visualizar, entre otros registros, el nombre o la dirección física de los dispositivos que están conectados en ese momento además de un historial de conexiones. El 23,4% declara que en su caso la intrusión Wi-Fi se ha identificado al comprobar la conexión de dispositivos desconocidos. Esta es una vía de comprobación más efectiva, dado que, si se conoce efectivamente qué dispositivos se han conectado se puede identificar cuál sobra y expulsarlo.

Por último, el 21,5% indica que, sin tener ningún dispositivo conectado, el piloto de conexión parpadea. Esto implica tráfico en la red, con lo cual es un motivo lógico de sospecha. Nuevamente, dependerá de si efectivamente se tiene control total sobre los dispositivos conectados. En numerosas ocasiones los nuevos dispositivos en el entorno del hogar hacen que las necesidades de conexión de estos nuevos objetos, del ya operativo Internet de las Cosas (IoT), pasen desapercibidos y se detecten como intrusiones. Es por ello, más importante que nunca, que se sea consciente de las necesidades de los dispositivos dentro del hogar, de cómo protegerlos y aprovechar sus ventajas de forma segura.

Gráfico 27. Motivos de haber sufrido una intrusión wi-fi (%)



Base: **Usuarios y usuarias que declaran haber sufrido una intrusión Wi-Fi**
Fuente: **Panel hogares, ONTSI**

5.4. INFECCIONES POR *MALWARE*

Las infecciones por *malware* son la puerta de entrada de los atacantes a nuestro hogar. A través de nuestros dispositivos personales el atacante puede acabar controlando toda la red, dado que cada vez tenemos más equipos dependientes de ella, en el mismo entorno doméstico.

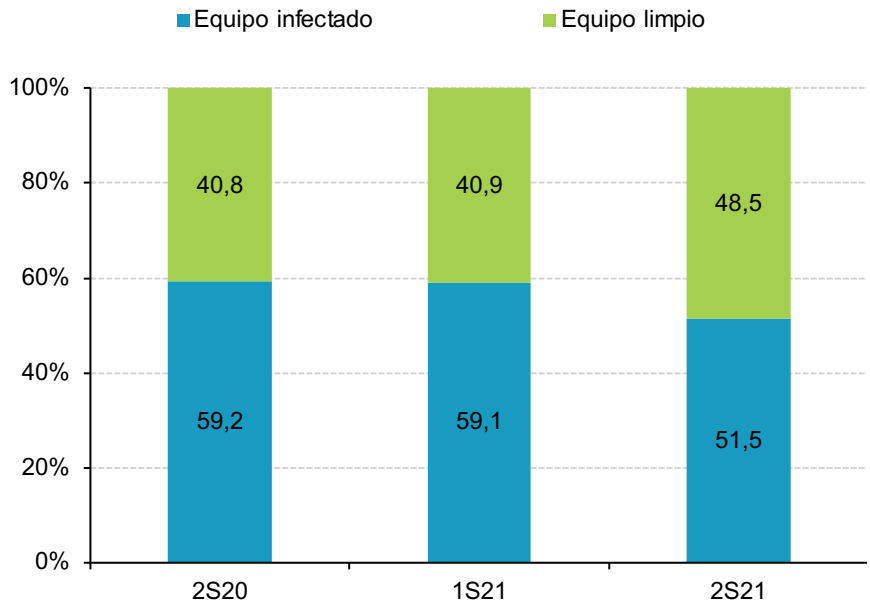
El gráfico 28 recoge los resultados tras realizar el análisis de *malware* de los ordenadores del hogar empleando el sistema Pinkerton. Durante el segundo semestre de 2021 se experimenta un descenso en el número de ordenadores infectados con algún tipo de *malware* (cae 7,6 p.p. sobre el semestre anterior), aunque aún mantiene un porcentaje alto (51,5%).

Aunque un 52% de los ordenadores tienen algún tipo de *malware*, la incidencia cae más de 7 puntos con respecto al semestre anterior

El descenso en la descarga de contenido gratuito desde webs ilegítimas y la adopción de otras buenas prácticas ha podido contribuir significativamente a esta bajada. Además, las mejoras de seguridad que implementan los sistemas operativos permiten desplegar opciones de seguridad nativa, en muchos casos incluso imperceptibles.

El 41% del *malware* encontrado en los ordenadores infectados es *adware*.

Gráfico 28. Estado de infección real del ordenador del hogar (%)



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

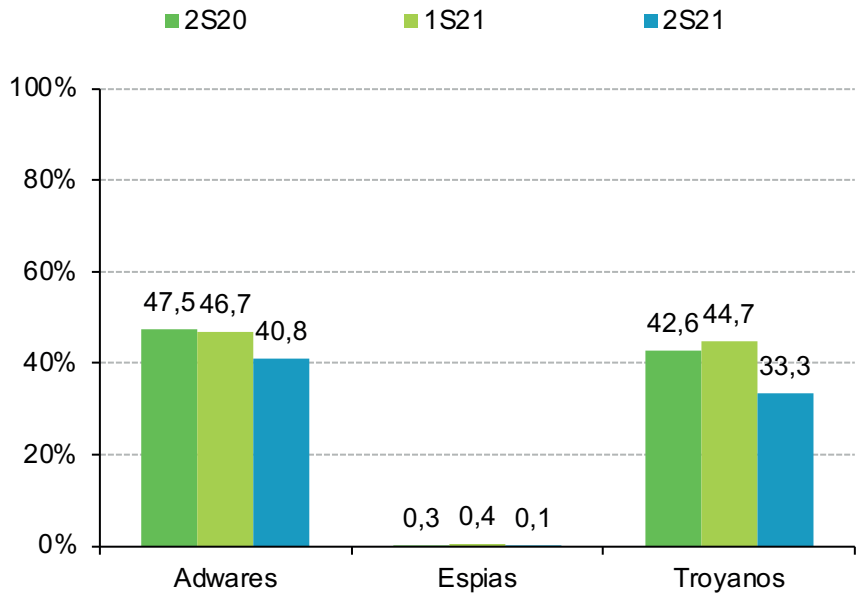
En cuanto a la tipología del *software* malicioso identificado durante el análisis (gráfico 29), el 40,8% del que había infectado los dispositivos era del tipo *adware*. Este tipo de *malware* habitualmente está diseñado para mostrar anuncios en la ventana del explorador y la finalidad que tiene es la de generar beneficios al atacante con los anuncios publicitarios que se muestran[15].

Del 33% de troyanos encontrados entre los casos de *malware* en ordenadores, un 9% son troyanos bancarios y un 6% son casos de *ransomware*.

También se han detectado troyanos. En concreto, el 33,3% de los ordenadores analizados contenía algún tipo. Pese a que el número de los presentes en los ordenadores ha disminuido respecto al semestre anterior, sigue siendo un número considerable por la peligrosidad que tiene este *malware*.

[15] https://es.malwarebytes.com/adware/

Gráfico 29. Tipología de *malware* detectado en el ordenador del hogar (%)

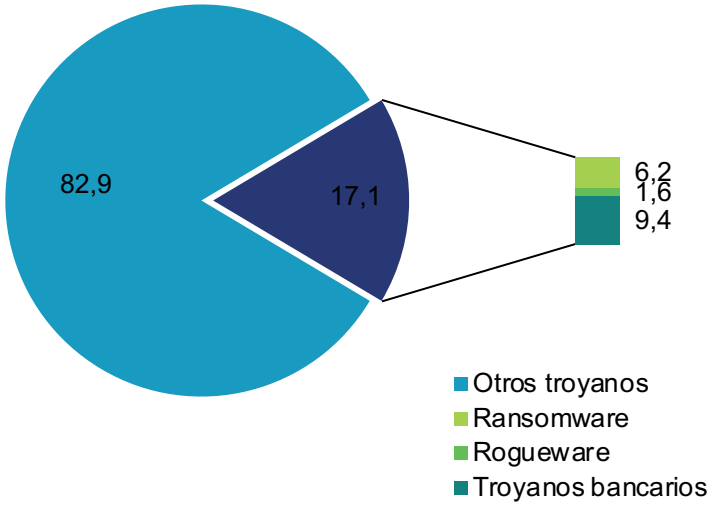


Base: **Total de ordenadores**
Fuente: **Panel hogares, ONTSI**

Cabe destacar que, de los troyanos identificados, el 6,2% corresponde a *ransomware* (gráfico 30). El secuestro de datos es de peligrosidad alta por el riesgo que conlleva para el equipo, pero también para todo el hogar, dado que muchas muestras pueden propagarse a través de la red a otros equipos.

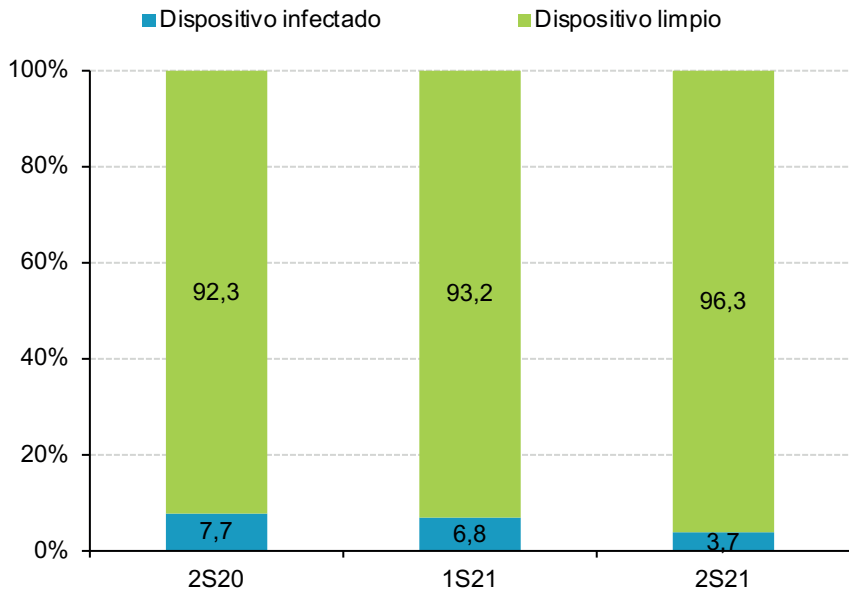
Sin embargo, son los troyanos bancarios los que tienen más aparición en los casos analizados. El 9,4% de los equipos contiene este tipo de *malware* dirigido principalmente a la obtención de credenciales y contraseñas para el fraude.

Gráfico 30. Clasificación de troyanos detectados en ordenador del hogar (%)



Base: **Total de ordenadores con troyanos detectados**
Fuente: **Panel hogares, ONTSI**

Gráfico 31. Estado de infección real en los dispositivos android (%)



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

Baja el número de dispositivos Android infectados con algún tipo de *malware* respecto al semestre anterior (3,7%, una bajada de 3,1 p.p.). Los resultados pueden verse en el gráfico 31.

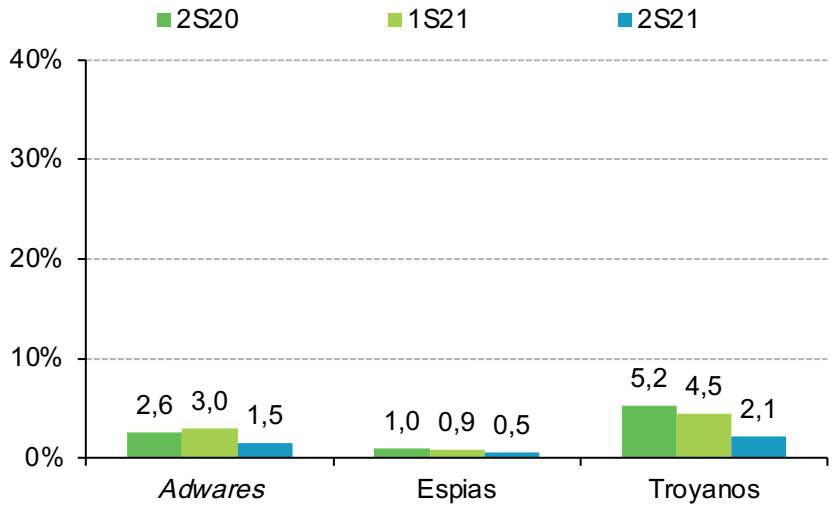
La mejoría se observa también en los semestres anteriores, y puede estar motivada por las nuevas versiones de los sistemas operativos Android. La telefonía móvil es pionera en materia de seguridad, dado que incorporan, antes que otras, mecanismos de seguridad como por ejemplo los sistemas biométricos y la seguridad embebida. Tienen, a su vez, mayor control sobre las instalaciones realizadas.

En cuanto a la tipología de *malware* presente en los dispositivos Android, los resultados recabados se resumen en el gráfico 32. En general, el número de infecciones ha disminuido respecto al semestre anterior, los troyanos en 2,4 p.p., los *adwares* en 1,5p.p. y los espías en 0,4 p.p.

La infección de dispositivos móviles llega al 4% frente al 52% de ordenadores.

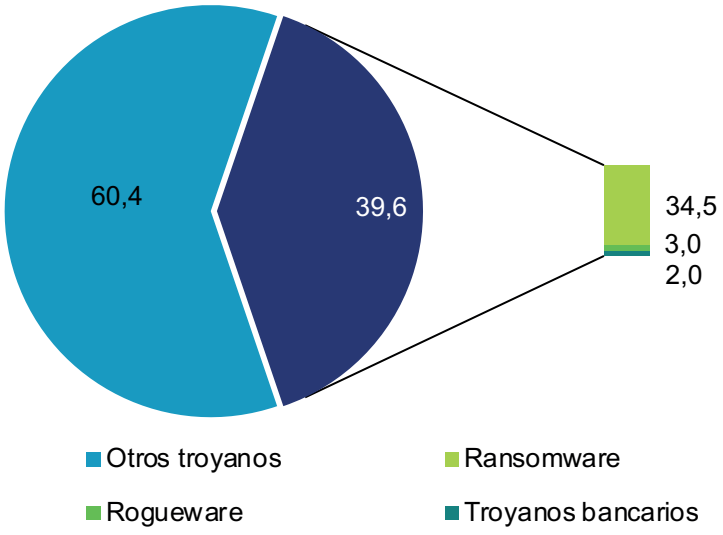
A diferencia de los ordenadores del hogar, en el caso de los dispositivos Android es el despliegue del secuestro de datos o ransomware, con el 34,5% sobre los dispositivos infectados, el objetivo principal de los troyanos identificados (gráfico 33).

Gráfico 32. Tipología de *malware* detectado en dispositivos android (%)



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

Gráfico 33. Clasificación de troyanos detectados en dispositivos android (%)



Base: **Total de dispositivos Android con troyanos detectados**
Fuente: **Panel hogares, ONTSI**

6 Consecuencias de los incidentes de seguridad

Los incidentes de seguridad pueden tener diferentes tipos de consecuencias: pérdidas económicas, infecciones de los equipos e incluso cambios de hábitos. Tanto los incidentes como sus consecuencias pueden alterar la percepción de los servicios de Internet, lo cual a su vez repercute inevitablemente en la confianza de las personas usuarias.

6.1. CONSECUENCIAS ECONÓMICAS DEL FRAUDE

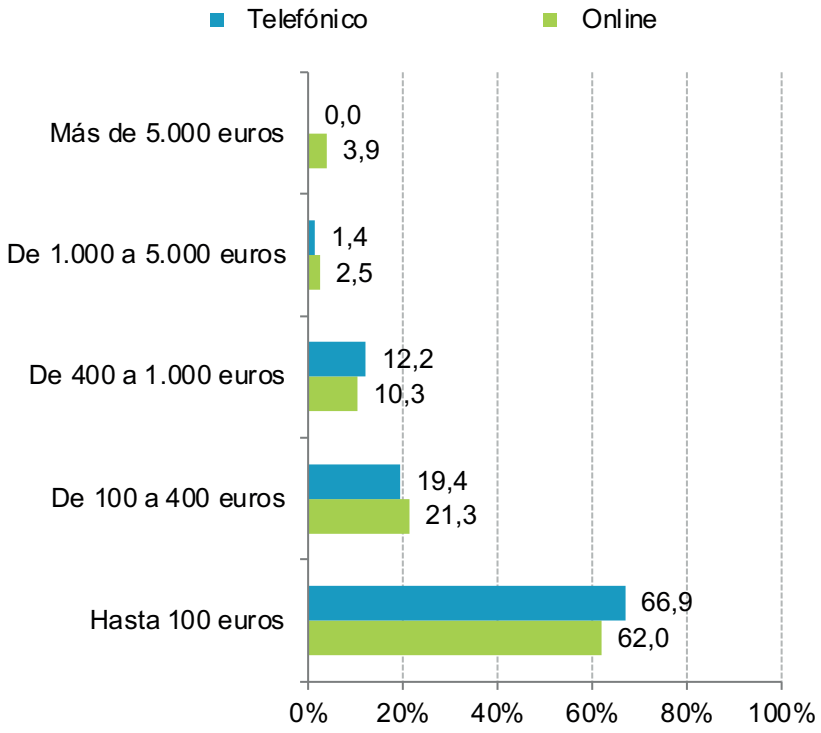
El aumento de las situaciones de fraude no tiene que acompañar necesariamente a un aumento de las consecuencias económicas, en tanto que depende en gran medida de si el intento de ataque fue efectivo o no. Aun así, dado que el engaño puede tener como consecuencia afectar económicamente a las víctimas, la medición del perjuicio económico puede dar cuenta de la efectividad de los ataques. De hecho, el gráfico 34 se centra precisamente en este punto, y destaca las pérdidas económicas declaradas por los internautas que han sido víctimas de fraude y han sufrido algún perjuicio económico.

Específicamente, el gráfico 34 distingue entre fraude telefónico y fraude *online* (a través de Internet, por ejemplo, por *email*). Los resultados indican que las pérdidas de valor más elevado (cuando la víctima declara más de 5.000 euros de pérdida) se dan en el 3,9% de los usuarios de este grupo de afectados por fraude *online*. En las cantidades más bajas (hasta 100 euros), sin dejar por ello de resultar significativas, se sitúan el 66,9% de los casos del fraude telefónico y el 62% del fraude *online*.

El fraude telefónico continúa resultando más creíble para numerosos sectores de la sociedad, que además usan en menor medida los servicios de Internet, o simplemente son más proclives a confiar en una persona física.

La mayoría de las pérdidas económicas causadas por el fraude, tanto telefónico como *online*, son como máximo de 100 euros.

Gráfico 34. Distribución del perjuicio económico debido a posibles fraudes (%)



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

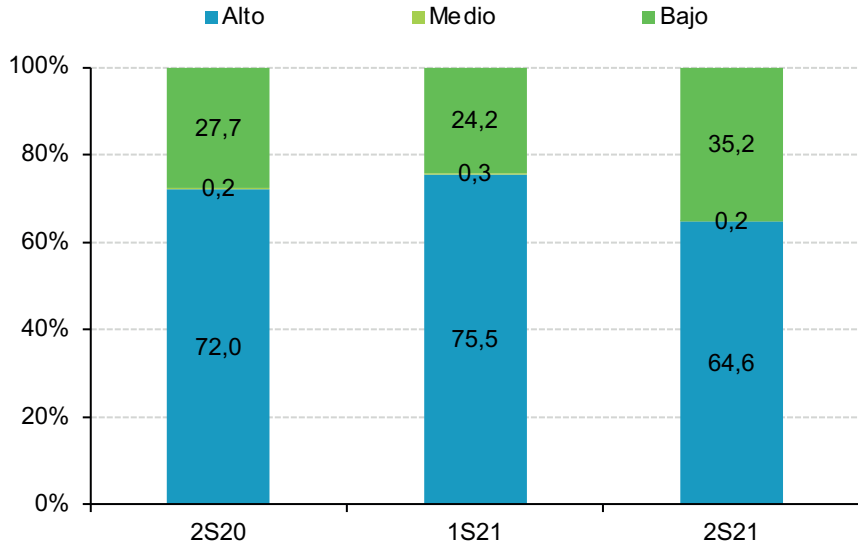
6.2. EVOLUCIÓN DEL RIESGO DE LAS INFECCIONES

En la clasificación de *malware* que podemos considerar de peligrosidad alta por sus efectos dañinos sobre los equipos de los usuarios encontramos: *ransomware, rogueware* (es una aplicación que intenta semejarse a otra, por apariencia o nombre, para engañar y timar a los usuarios) y troyanos bancarios. A este respecto, el gráfico 35 muestra una disminución del *malware* altamente peligroso detectado en los ordenadores del hogar respecto al primer semestre de 2021 y el segundo de 2020.

Aun así, las cifras siguen siendo altas, con más de seis de cada diez ordenadores infectados a este nivel de peligrosidad. Corresponde en este caso a datos reales, extraídos de los equipos analizados y sometidos a más de 80 motores antivirus.

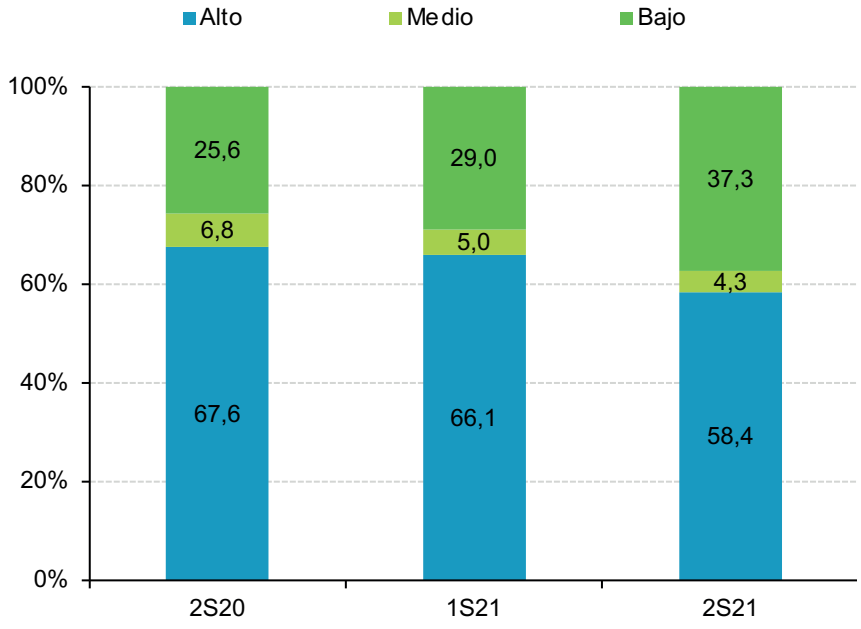
Más concretamente, de los ordenadores en el hogar infectados, un 64,6% lo están por algún tipo de *malware* clasificado como de alta peligrosidad. No obstante, aunque el porcentaje haya disminuido respecto a los dos semestres anteriores, sigue siendo peligroso para internautas en los terminales del hogar porque basta con que un equipo se infecte para comprometer toda la red, en tanto a que los mecanismos de propagación del *malware* cada vez están mejor diseñados para aprovecharse de la conectividad de los dispositivos.

Gráfico 35. Peligrosidad del *malware* detectado en el ordenador del hogar (%)



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

Gráfico 36. Peligrosidad del *malware* detectado y riesgo de los dispositivos Android (%)



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

La existencia de *software* malicioso de peligrosidad alta es un mal nada deseable porque puede destrozar la estación de trabajo por completo. Así que, en muchos casos, el antivirus no es suficiente. Su existencia puede no solo acarrear la pérdida de información, sino en algunos casos dañar el equipo[16].

Respecto al *malware* detectado en dispositivos Android, la cantidad del *software* altamente peligroso para el propio dispositivo y para la privacidad del usuario, también ha disminuido respecto al semestre anterior, en concreto en 7,7 p.p. (gráfico 36). Sin embargo, el porcentaje continúa siendo alto, con el 58,4% de los dispositivos Android infectados conteniendo este tipo de ataques de peligrosidad alta.

Un 65% de los ordenadores y un 58% de los dispositivos Android infectados sufrieron ataques por *malware* de alta peligrosidad.

6.3. CAMBIOS DE HÁBITOS TRAS UN INCIDENTE DE SEGURIDAD

Tras un ataque, es habitual que existan modificaciones en el comportamiento para evitar que se vuelva a producir ese tipo de incidentes. Por ejemplo, frente a un ataque con *ransomware*, si no se hacían con anterioridad copias de seguridad periódicas, es habitual que se comiencen a hacer.

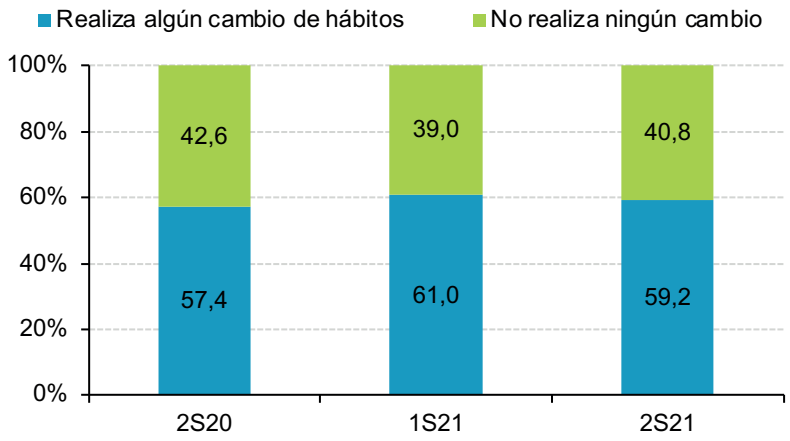
En este semestre, conforme indica el gráfico 22, se declara un menor número de incidentes de seguridad. El gráfico 37 recoge las declaraciones de quienes han sufrido algún incidente de ciberseguridad, y pese a ser víctimas de un incidente, desciende en 1,8 p.p. el porcentaje de panelistas que ha realizado algún cambio de hábitos tras los incidentes.

Entre ese 59,2% de víctimas de incidentes de seguridad que sí cambiaron sus hábitos (gráfico 38) apuestan principalmente por cambiar las contraseñas o empezar a usar un gestor de contraseñas (45,6%), actualizar las herramientas y configuraciones (33,2%) y comenzar a realizar copias de seguridad (28,1%).

El 59% de quienes han sufrido alguna incidencia de seguridad realizan algún cambio de hábitos.

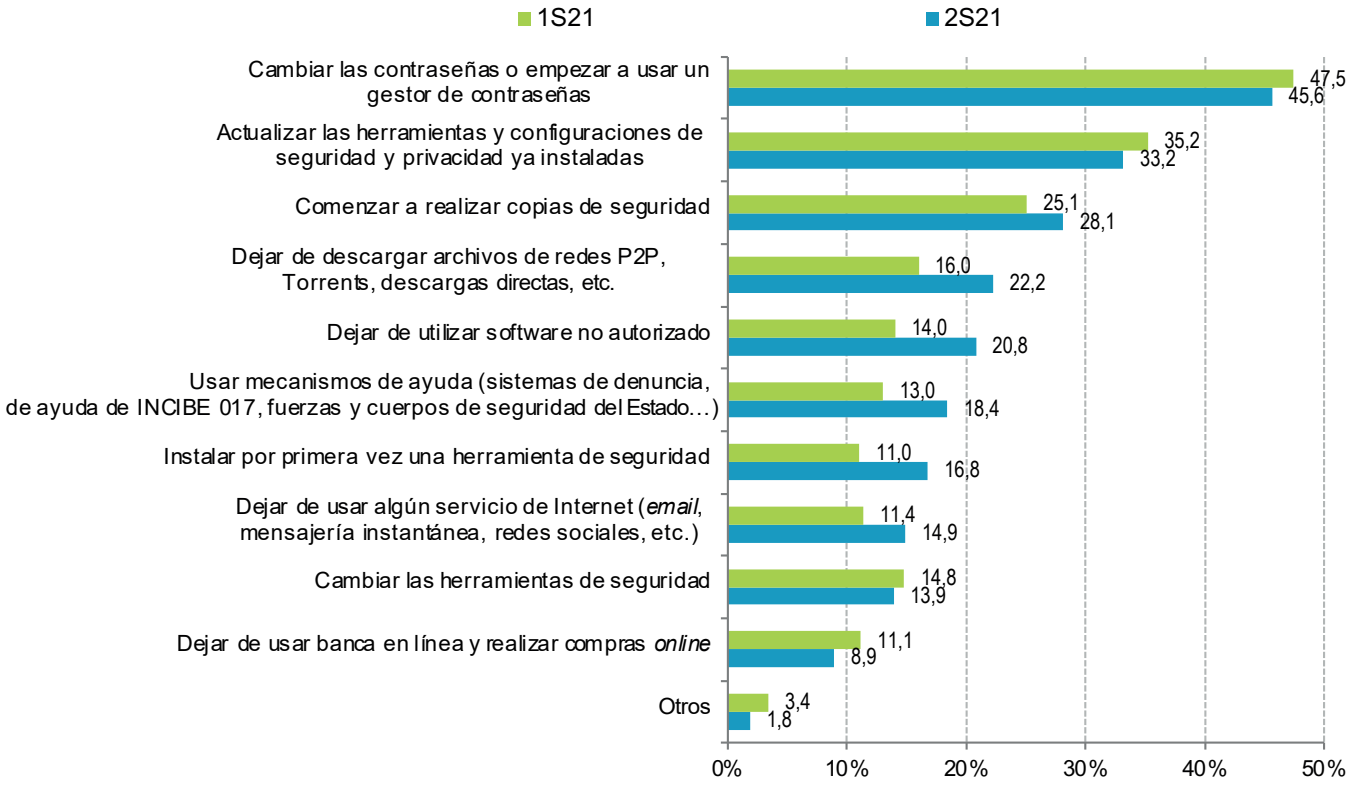
[16] Es el caso del virus troyano 'Zeus': https://latam.kaspersky.com/resource-center/threats/zeus-virus

Gráfico 37. Cambio de hábitos en internet motivados por las incidencias de seguridad experimentadas (%) (2s 2020 – 2s 2021)



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

Gráfico 38. Cambios de hábitos en internet motivados por las incidencias de seguridad experimentadas (%) (1s 2020 – 2s 2021)



Base: **Personas que han sufrido alguna incidencia de seguridad y modifica sus hábitos**
Fuente: **Panel hogares, ONTSI**

Valores que acompañan al resto de los datos analizados en el estudio incluyen, por ejemplo, dejar de descargar archivos de redes P2P (22,2%) o bien dejar de usar *software* no autorizado (20,8%). Estos pasos son críticos para disminuir la probabilidad de infección por *software* malicioso en los equipos.

Otro dato muy significativo es que el 18,4% quienes han tenido algún problema de ciberseguridad ha recurrido a los mecanismos de ayuda (por ejemplo, el 017 de INCIBE). El primer semestre de 2021 solo el 13% las personas que aprovecharon estos mecanismos de ayuda.

Es interesante también que, pese a que aumentan las comunicaciones a través de Internet, los incidentes de seguridad afectan negativamente a esta ventana de interoperabilidad. El 14,9% e las personas argumenta que ha dejado de usar algún servicio de Internet debido a dichos incidentes. También afecta precisamente a las compras y banca *online* (8,9%, baja 2,2 p.p.).

Tras experimentar una incidencia de seguridad el 21% de los internautas ha dejado de usar *software* no autorizado.

7 Confianza de las personas usuarias

En gran parte, la pérdida o no de la confianza en los servicios de Internet es en sí misma una consecuencia de los incidentes de seguridad. Aun así, la confianza es uno de los parámetros más peculiares. Para algunas personas un incidente de seguridad puede no afectar su confianza, mientras que para otros podría significar todo.

Por eso este parámetro requiere su propia sección en este estudio, para analizar las opiniones sobre lo que afecta más a su percepción de los riesgos de Internet y, por supuesto, a su confianza.

7.1. PERCEPCIÓN DE LA GENTE SOBRE LA INFECCIÓN DE SUS EQUIPOS

La excesiva confianza en la ausencia de infecciones o ataques en nuestros dispositivos puede ser peligrosa. Como ya se ha comentado, los cambios de hábitos están motivados principalmente por algún incidente de seguridad percibido por el usuario. Si el incidente, en este caso la infección por *malware* no es identificable, esto implica que se puede continuar con las conductas de riesgo y dejar el equipo totalmente expuesto a la persona atacante.

Desafortunadamente, las declaraciones sobre si creen que su ordenador está infectado con algún tipo de *software* malicioso o no, se contradicen con los datos recabados por Pinkerton. El 51,5% de los ordenadores del hogar analizados se encuentran infectados con algún *software* de este tipo, si bien solo un 10,2 de las personas encuestadas creen que es así.

Hay que recordar que durante el segundo semestre de 2021 los internautas han notado más dichas infecciones. Durante este semestre el *software* maligno de peligrosidad baja ha aumentado (gráfico 35). Este grupo engloba el que no perjudica de forma notoria el rendimiento del equipo, aunque puede ser perceptible por la persona usuaria: abre ventanas no deseadas al navegar, incrusta publicidad en páginas web legítimas que realmente no contienen publicidad o que facilita la captura de información no sensible de la víctima.

El 52% de los ordenadores tienen algún tipo de infección, lo cual es percibido únicamente en el 11% de los casos.

La tabla 1 resume la comparativa entre la detección de *malware* por el *software* Pinkerton y las opiniones recogidas. El 46,9% de quienes afirman no tener *software* malicioso en su ordenador tienen una percepción equivocada, dado que su ordenador está realmente infectado. En ocasiones, la percepción podría distar de la realidad por la falta de uso de antivirus, como se ha reflejado en las declaraciones recogidas en el gráfico 3.

Dicha cifra es muy importante. La creencia de que no hay contagio, puede provocar conductas más relajadas y no se produce cambio de hábitos alguno.

Tomando como referencia el valor de 46,9% de peligro potencial, la tabla 2 y la tabla 3 muestran la cifra del estado real versus la percepción de los usuarios y usuarias.

Tabla 1. Desglose del estado real versus percepción (ordenador del hogar)

Declaran tener malware en PC	Su PC presenta malware		
	Sí	No	Total
Sí	4,5	5,7	10,2
No	46,9	42,9	89,8
Total	51,4	48,6	100

Base: Personas con ordenador escaneado
Fuente: Panel hogares, ONTSI

Tabla 2. Desglose del estado real versus percepción (ordenador del hogar cuyos propietarios son hombres)

Declaran tener malware en PC	Su PC presenta malware		
	Sí	No	Total
Sí	5,6	3,6	9,2
No	49,4	41,4	90,8
Total	55,0	45,0	100

Base: Usuarios con ordenador escaneado que son hombres.
Fuente: Panel hogares, ONTSI

Tabla 3. Desglose del estado real versus percepción (ordenador del hogar cuyas propietarias son mujeres)

Declaran tener malware en PC	Su PC presenta malware		
	Sí	No	Total
Sí	5,6	3,6	9,2
No	49,4	41,4	90,8
Total	55,0	45,0	100

Base: Usuarios con ordenador escaneado que son mujeres
Fuente: Panel hogares, ONTSI

En general, en este caso, los hombres son los que más confían erróneamente en la salud de sus equipos. Esta confianza podría traducirse en conductas más relajadas, pero también en una falsa sensación de preparación para afrontar los riesgos de ciberseguridad. Ellos son los que elevan esta percepción total, pues el 49,4% de los consultados se equivoca al pensar que no tiene *software* pernicioso, cuando en el caso de las mujeres solo un 44,2% cree equivocadamente que su ordenador está libre de *software* maligno (ver tabla 3).

Algunos posibles síntomas relacionados con esta infección por son, por ejemplo, que se cierren solas las aplicaciones, que el ordenador vaya más lento de lo normal o la aparición de publicidad en nuevas ventanas del navegador. En muchas ocasiones, y dependiendo del tipo, son las personas usuarias quienes detectan antes el contagio, porque su máquina no funciona igual.

Los dispositivos Android, analizados en este estudio, son un objetivo muy atractivo para los atacantes, ya que almacenan mucha información personal y son la forma más habitual para conectarse a Internet. En cada actualización ya sea del sistema operativo o de una aplicación, los desarrolladores tratan de mejorar la seguridad de estos dispositivos para evitar que sean infectados. El gráfico 39 ofrece una comparativa entre el estado real y la percepción respecto a la infección en estos dispositivos.

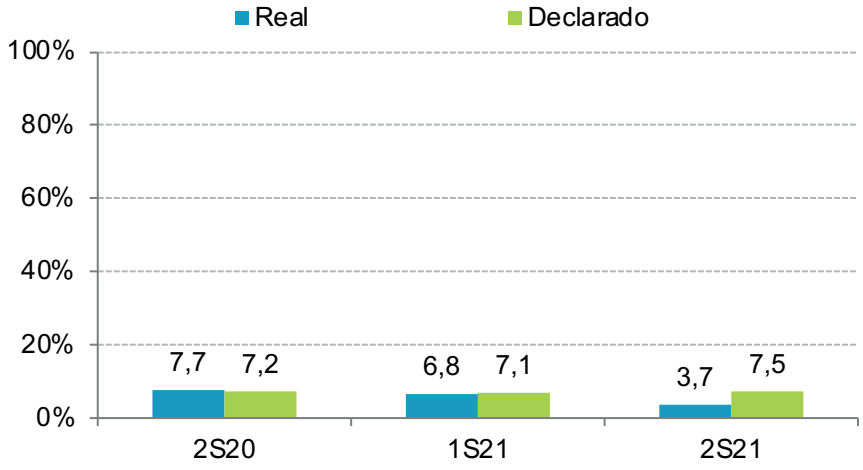
El 4% de los dispositivos Android tiene algún tipo de infección, mientras que un 8% cree tener su dispositivo infectado.

Al contrario de lo que pasaba con el ordenador del hogar (Tabla 1), en el caso de los dispositivos móviles se desconfía de la seguridad de los dispositivos. El 7,5% de las personas creen tener *software* malicioso en su dispositivo, pero la realidad es que tan solo el 3,7% de los dispositivos está infectado. Al tener esa sensación de inseguridad es más probable que las personas usuarias extremen las precauciones para protegerse.

Si se desglosa el porcentaje de dispositivos Android infectados, viendo ahora los datos que da Pinkerton sobre ellos, obtenemos los resultados de la tabla 4. Según esta fuente, un 3,3% de las personas cree no tener *software* malicioso en sus dispositivos y sin embargo su dispositivo sí está infectado. El 89,7%, sin embargo, acierta al opinar que sus dispositivos no están infectados.

Si desglosamos estos resultados por género, obtenemos los resultados mostrados en la tabla 5 y la tabla 6.

Gráfico 39. Estado real versus percepción de infección en dispositivos android (%)



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

Tabla 4. Desglose del estado real versus percepción de infección (dispositivos Android)

Declaran tener malware en el dispositivo Android	Su dispositivo Android presenta malware		
	Sí	No	Total
Sí	0,3	6,6	6,9
No	3,3	89,7	93,1
Total	3,7	96,3	100

Base: Usuarios y usuarias con dispositivo Android escaneado
Fuente: Panel hogares, ONTSI

Tabla 5. Desglose del estado real versus percepción de infección (dispositivos Android pertenecientes a hombres)

Declaran tener malware en el dispositivo Android	Su dispositivo Android presenta malware		
	Sí	No	Total
Sí	0,3	6,6	6,9
No	3,3	89,7	93,1
Total	3,7	96,3	100

Base: Usuarios con dispositivo Android escaneado perteneciente a hombres
Fuente: Panel hogares, ONTSI

Tabla 6. Desglose del estado real versus percepción de infección (dispositivos Android pertenecientes a mujeres)

Declaran tener malware en el dispositivo Android	Su dispositivo Android presenta malware		
	Sí	No	Total
Sí	0,3	6,4	6,7
No	3,4	90,0	93,3
Total	3,7	96,3	100

Base: Usuarias con dispositivo Android escaneado perteneciente a mujeres
Fuente: Panel hogares, ONTSI

Si hacemos alusión a los datos generales (sin diferenciar por género) vemos que éstos son muy similares a los obtenidos analizando las diferencias (tabla 4 y siguientes).

Conforme a los resultados expuestos en la tabla 5, el 3,3% de los hombres tiene infectado su Android, pero lo desconoce.

Significa que el porcentaje de hombres que piensa erróneamente que su equipo no contiene *software* pernicioso no está afectando negativa o positivamente al valor general. Sin embargo, en los resultados para la población femenina resumidos en la tabla 6, vemos que el 3,4% de las mujeres entrevistadas no es consciente de tener *malware* en su dispositivo, cuando los datos empíricos demuestran que sí está infectado.

Si hacemos nuevamente alusión a los datos generales sin diferenciación por género en los que el 3,3% del total de panelistas asegura erróneamente no tener *software* maligno en su dispositivo (tabla 4), encontramos que en este caso el porcentaje de mujeres es superior a dicho valor general (3,4%).

7.2. OPINIONES SOBRE LA SEGURIDAD EN INTERNET

Uno de los puntos críticos de este estudio es promover mejoras relativas al uso de Internet, por lo que analizar las opiniones sobre la seguridad en esta red (gráfico 40) es fundamental.

Como recoge el gráfico 40, el 78,7% de las personas encuestadas opina que si su equipo o dispositivo está razonablemente protegido le hace la vida más fácil. Este dato ya era representativo en el primer semestre de 2021. Esto se puede conseguir activando las medidas de seguridad automatizables del ordenador y el dispositivo móvil, cosa que como ya sabemos, no se hace.

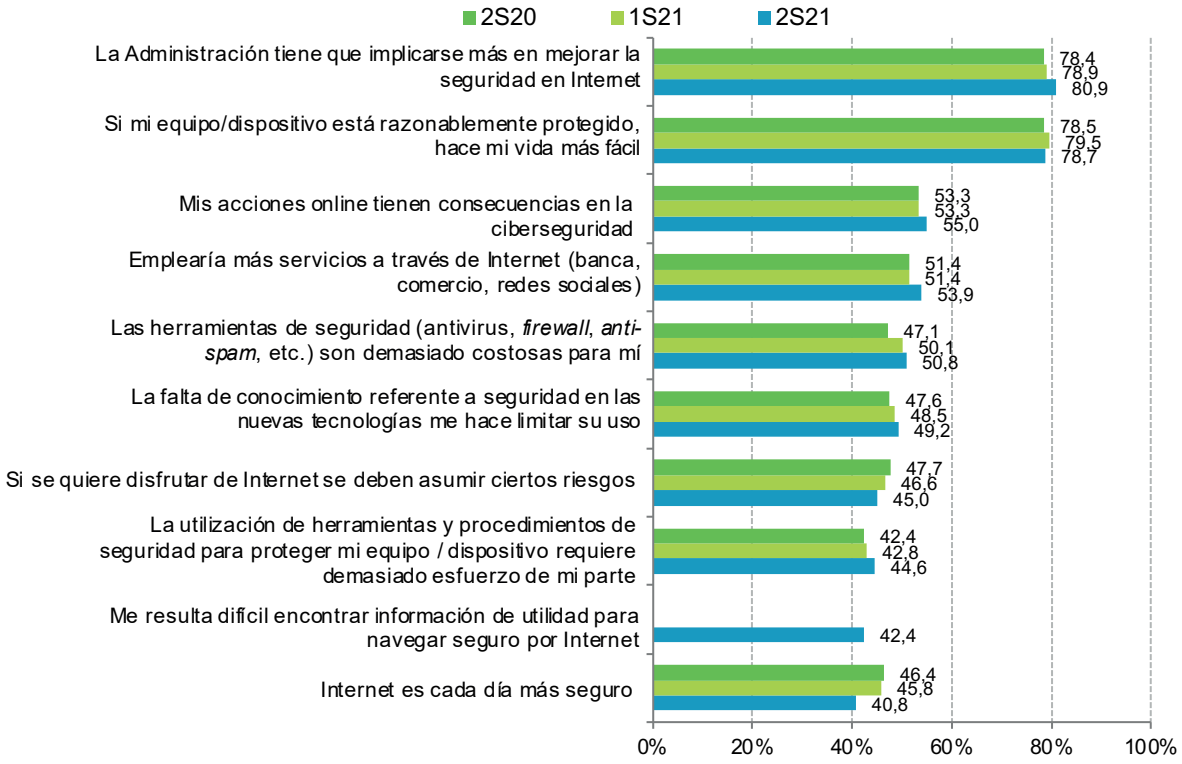
Preguntadas sobre la seguridad en Internet, se manifiesta en un 80,9% de los casos el deseo de que la Administración se implique más, un dato que aumenta incluso respecto al periodo anterior. Precisamente, los organismos públicos organizan cada año campañas de concienciación sobre ciberseguridad a través de medios de difusión (como se verá a continuación en la sección 8.3).

Entre las diferentes afirmaciones, es interesante destacar que un 42,4% declara que le resulta difícil encontrar información de utilidad para navegar seguro por Internet. Para comprender mejor este dato se preguntaba explícitamente por las campañas que conocen.

81% de usuarios y usuarias creen que las entidades administrativas han de implicarse más en mejorar la seguridad en Internet.

42% de usuarios y usuarias ven difícil acceder a información para navegar de manera segura.

Gráfico 40. Opiniones sobre la seguridad en internet (%)



Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

7.3. OPINIONES SOBRE LA SEGURIDAD EN INTERNET

Anualmente el Gobierno, a través de diferentes administraciones, promueve campañas para concienciar de los riesgos derivados del uso de Internet. El gráfico 41 ofrece un listado de las más representativas, dirigidas hacia la concienciación, impulsadas durante 2021.

El Instituto Nacional de Ciberseguridad (INCIBE) pone a disposición de todos los usuarios la Oficina de Seguridad del Internauta[17] (OSI) desde donde lanzan campañas para cuidar la privacidad, estar ciberseguro en casa, evitar los riesgos de los dispositivos conectados (IoT), entre otras. Además, también ponen a disposición de cualquier usuario la web de Internet Segura *for kids*[18] (IS4K) donde también se lanzan diferentes campañas para pequeñas y pequeños y jóvenes internautas, que abordan temas como el ciberacoso o el *sexting* en menores, y se dan consejos a las madres y padres de cómo usar las llamadas herramientas de control parental.

Casi la mitad de la población encuestada desconoce las principales campañas en materia de ciberseguridad.

La campaña *Hoy es un anuncio, mañana no*[19], emitida por televisión en espacio publicitario, simulaba en pantalla cómo un *ransomware* podría secuestrar el SmartTV o el ordenador. Sin embargo, esta acción tan solo

[17] https://www.osi.es/es
[18] https://www.is4k.es/

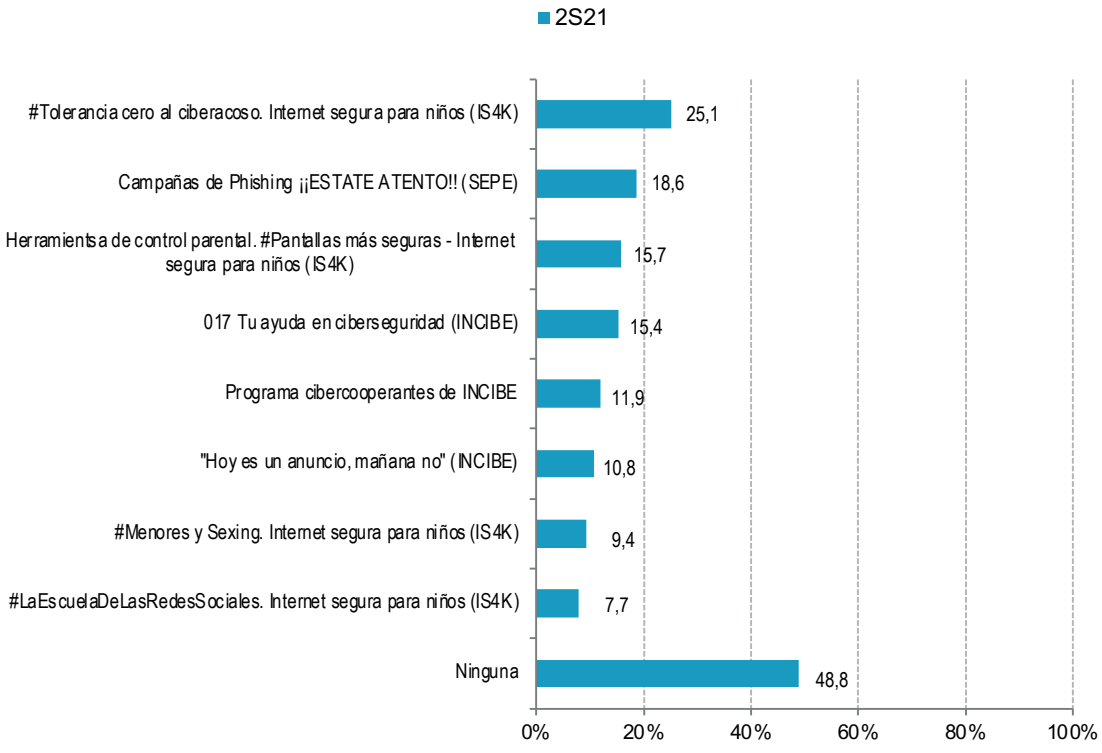
ha sido reconocida por el 10,8% de las personas encuestadas. Existe la opción de que la televisión no sea el canal principal para informarse de estas personas.

A lo largo del semestre se han difundido este tipo de acciones a través de INCIBE o SEPE. También se ha consultado sobre el conocimiento sobre alguna de ellas. El 25,1% ha manifestado conocer la campaña que hizo IS4K sobre el ciberacoso y la Internet segura para niños. El 18,6% conoce la campaña Estate atento, del SEPE, en la que se trató de dar consejos sobre cómo evitar el *phishing*. Entre las campañas de control parental, tan necesarias para prevenir posibles problemas derivados de la conexión a Internet de los más jóvenes a través de los equipos del hogar, la campaña de herramientas de control parental de IS4K alcanza un conocimiento declarado del 15,7% de los participantes.

Cabe destacar que el servicio que ofrece INCIBE a través del teléfono 017, en el que se brinda ayuda sobre ciberseguridad a la ciudadanía y empresas, es conocido por el 15,4% de las personas encuestadas. Recordemos que, ante un incidente de ciberseguridad, es uno de los mecanismos aprovechados ya por el 18,4% de la población internauta. En el primer semestre de 2021 el 13% declaró hacer uso de este y otros mecanismos de ayuda frente a un incidente de seguridad[20], por lo que el aumento puede estar justificado por el éxito de las campañas de concienciación.

En definitiva, los resultados ponen al descubierto que, si bien las campañas son efectivas, por algún motivo no llegan bien, ya que el 48,8% declara no conocer ninguna en concreto.

Gráfico 41. Campañas conocidas realizadas por el gobierno en materia de ciberseguridad (%)



Base: **Personas que se registran en portales de descarga de contenido gratuito**
Fuente: **Panel hogares, ONTSI**

[19] https://www.incibe.es/hoyesunanuncio
[20] https://www.observaciber.es/sites/observaciber/files/media/documents/ciberriesgos_informe_diciembre2021.pdf

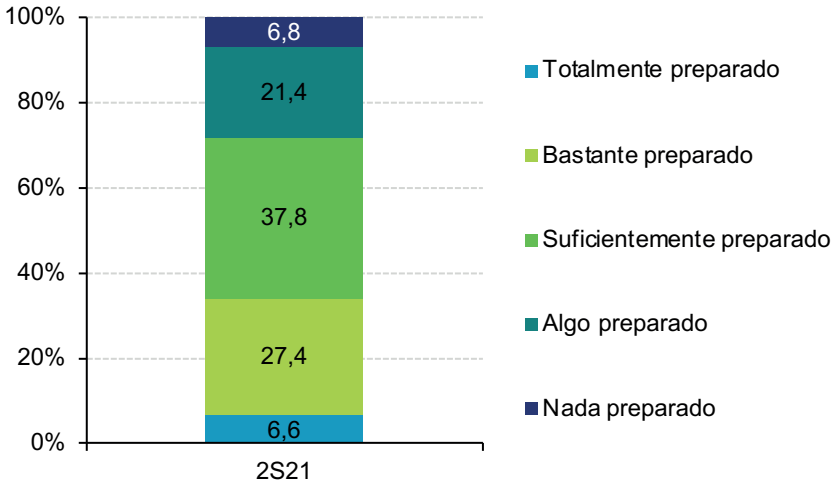
7.4. NIVEL DE PREPARACIÓN PARA AFRONTAR RIESGOS

En este sentido es interesante conocer la autopercepción acerca de cómo de preparada se siente la población a la hora de afrontar posibles riesgos y ataques reales. Al analizar la visión subjetiva hacia las posibilidades de afrontar problemas de ciberseguridad, observamos que las opiniones están bastante distribuidas (gráfico 42).

Tan solo el 6,6% de internautas se considera totalmente preparado o preparada para afrontar los desafíos de seguridad. El 27,3% manifiesta estar bastante preparado o preparada mientras que el 37,8% declara que lo está suficientemente. Los sectores más dudosos abarcan el 21,3% (se consideran algo preparados) y el 6,8% (nada preparado).

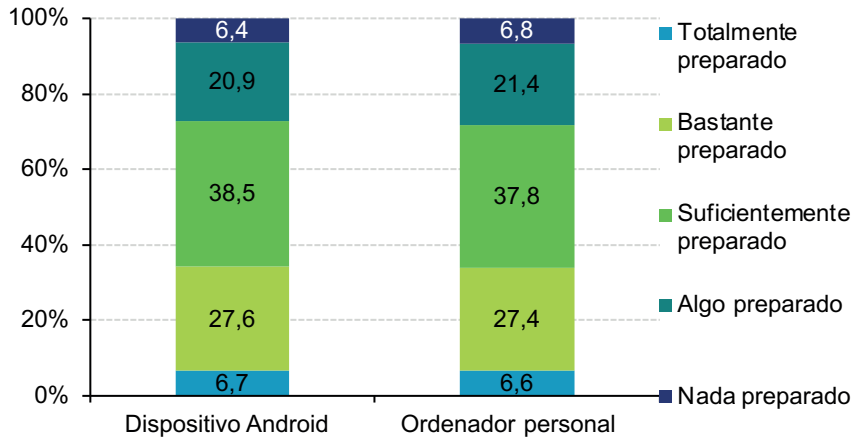
Casi el 7% de la población considera que no está nada preparada para afrontar posibles problemas de ciberseguridad.

Gráfico 42. Percepción de la preparación para afrontar posibles problemas de ciberseguridad (%)



Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

Gráfico 43. Declaraciones sobre el nivel de preparación para afrontar posibles problemas de ciberseguridad en el ordenador del hogar versus dispositivo móvil (%)



Base: **Usuarios y usuarias de Android / Usuarios de ordenador personal**
Fuente: **Panel hogares, ONTSI**

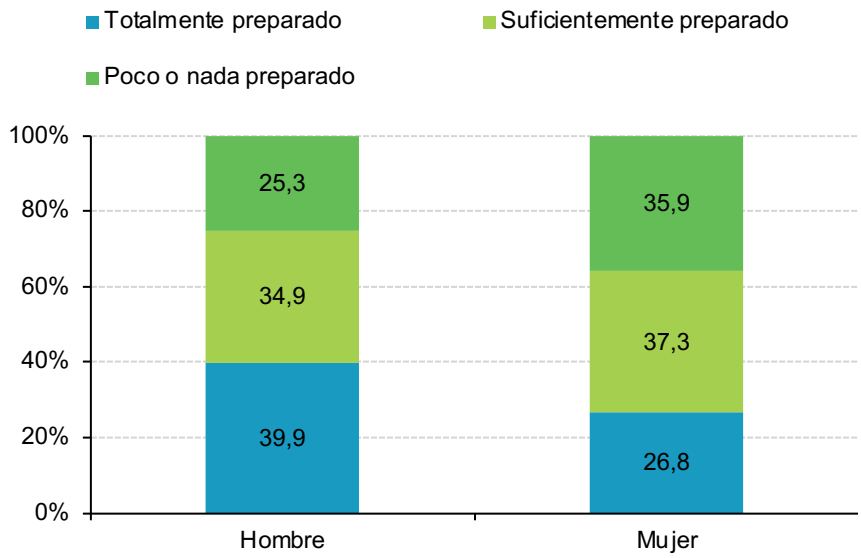
Si hacemos la distinción considerando el tipo de dispositivo, obtendremos resultados bastante similares (gráfico 43), de ahí que podamos intuir que estas declaraciones son independientes del dispositivo del hogar que se use; ordenador o dispositivo personal

Se ha desglosado en el gráfico 50 realizando una distinción por género para saber qué percepción sobre su propia preparación para afrontar posibles problemas de ciberseguridad en su ordenador personal o en su dispositivo Android los hombres y las mujeres (gráfico 44 y gráfico 45 respectivamente) para después compararlo con los resultados del análisis con Pinkerton.

En lo relativo a los problemas de seguridad en ordenadores, el porcentaje de mujeres que reconocen sentirse totalmente preparadas para afrontar posibles problemas de seguridad es inferior al de los hombres (13,1 p.p. menos). Las que declaran estar suficientemente preparadas y poco o nada preparadas es, sin embargo, superior al de los hombres en 2,4 p.p. y 10,6 p.p. respectivamente (gráfico 44).

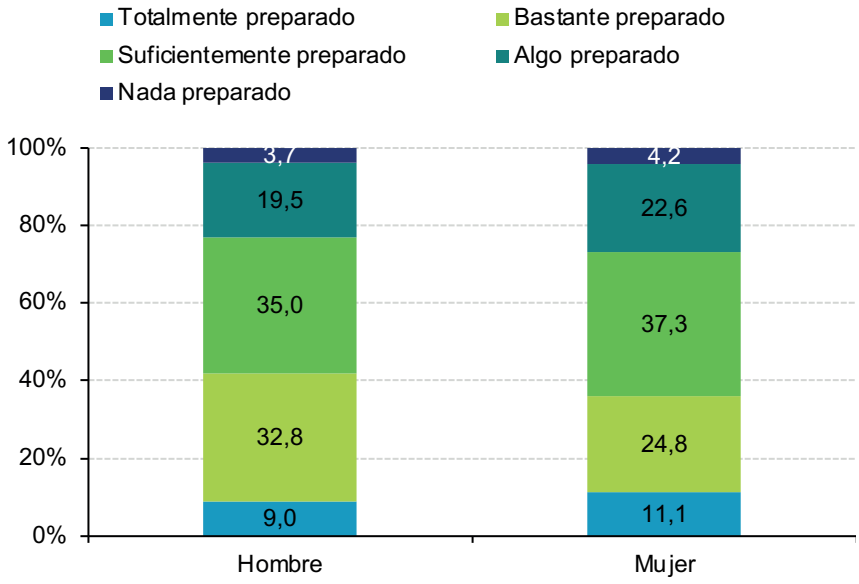
Sobre estos datos, cabe subrayar que, en general, las mujeres son dadas a reconocer, en mayor medida que los hombres, que no saben de algo, por lo que este dato no tiene por qué corresponderse con la realidad. En lo relativo a los dispositivos Android (gráfico 45), en cambio, las mujeres manifiestan estar totalmente preparadas utilizando dispositivos Android, por encima de los hombres (11,1% mujeres, 9% hombres).

Gráfico 44. Preparación para afrontar posibles problemas de ciberseguridad en el ordenador del hogar (diferenciado por género)



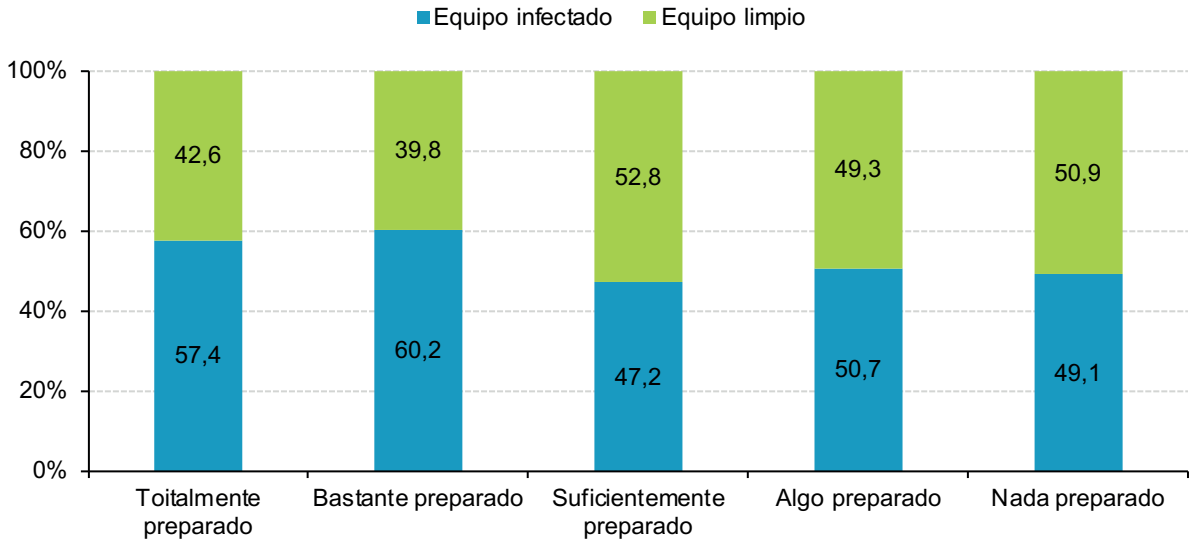
Base: Total de usuarios y usuarias de ordenador.
Fuente: Panel hogares, ONTSI

Gráfico 45. Preparación para afrontar posibles problemas de ciberseguridad en dispositivos Android (diferenciado por género)



Base: Total de personas con dispositivos Android
Fuente: Panel hogares, ONTSI

Gráfico 46. Declaraciones sobre el nivel de preparación para afrontar los riesgos de ciberseguridad de usuarios de ordenador versus infección de los ordenadores del hogar (%)



Base: **Usuarios y usuarias de ordenador**
Fuente: **Panel hogares, ONTSI**

Y después de la opinión de las personas usuarias, compartimos el análisis sobre los desafíos de ciberseguridad y la seguridad real de sus dispositivos (gráfico 46 y gráfico 47), para ordenador y Android respectivamente (en este caso, sin desagregar por género).

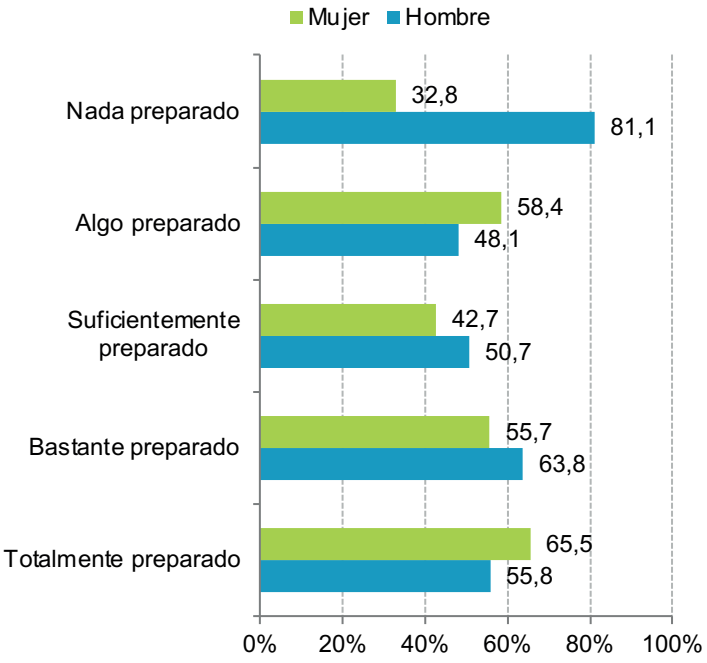
En general, en todos los niveles de percepción se muestran cifras altas de equipos infectados por algún tipo de *software* malicioso. En particular, en el caso de las personas que usan el ordenador que se consideran totalmente preparadas, el 57,4% tiene el equipo infectado. Son las que presentan percepciones más bajas, precisamente, las que tienen mejores resultados en cuanto a salud de los dispositivos.

Separando por género el porcentaje de ordenadores infectados, obtenemos las siguientes lecturas (gráfico 47). Según los datos obtenidos con Pinkerton, el 81,1% de los hombres entrevistados que dicen estar nada preparados para los riesgos derivados de la inseguridad, tiene su ordenador infectado con algún tipo de *software* malicioso.

El 56% de las personas que se consideran totalmente preparadas en ciberseguridad tienen sus equipos infectados.

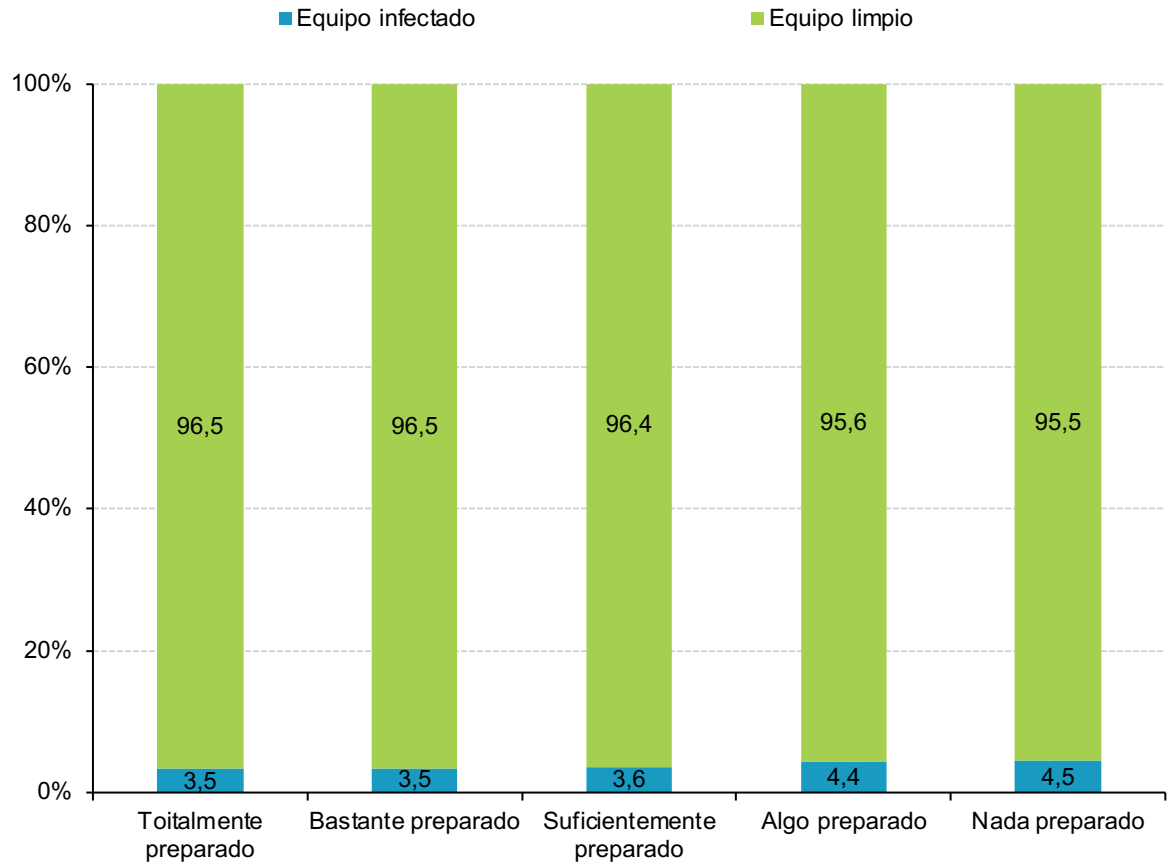
Todos y todas tienen problemas de *malware* en sus equipos, aunque reconocen de forma dispar estar preparadas y preparados. Comparando estos resultados con los obtenidos en los hombres en el nivel de nada preparado, las mujeres tienen menos infecciones en el ordenador que los hombres, pero, en el nivel de totalmente preparado el porcentaje de *software* maligno en ordenador es mayor en las mujeres (9,7 p.p.).

Gráfico 47. Nivel de preparación para afrontar los riesgos de ciberseguridad de usuarios con ordenador infectado con *malware* (desagregado por género)



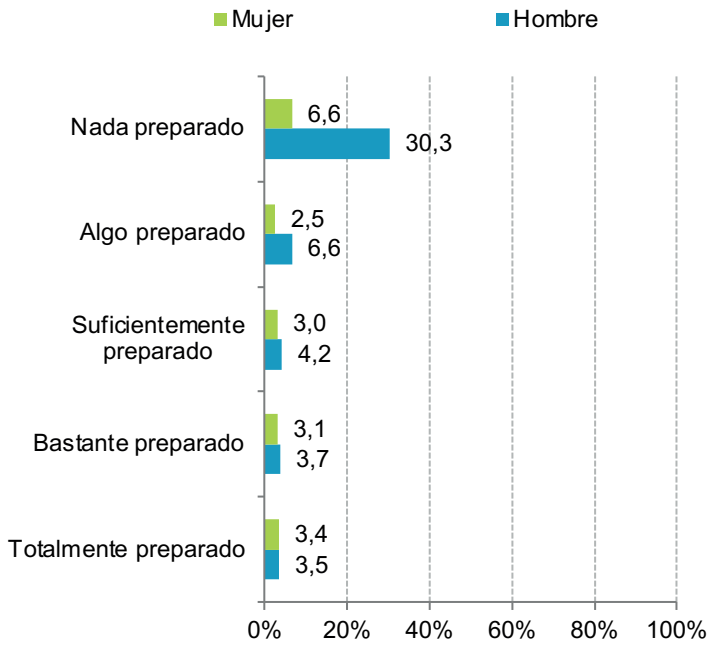
Base: Usuarios y usuarias con ordenador infectado
Fuente: Panel hogares, ONTSI

Gráfico 48. Declaraciones sobre el nivel de preparación para afrontar los riesgos de ciberseguridad de usuarios de android versus infección de los dispositivos (%)



Base: Usuarios de Android
Fuente: Panel hogares, ONTSI

Gráfico 49. Declaraciones sobre el nivel de preparación para afrontar los riesgos de ciberseguridad de usuarios de android con dispositivos infectados (desagregado por género)



Base: **Usuarios y usuarias con dispositivo Android infectado**
Fuente: **Panel hogares, ONTSI**

En el caso de los dispositivos Android (gráfico 48), cabe recordar que encontrábamos menos *malware* presente en éstos. Al igual que ocurre con las declaraciones de los usuarios de ordenador, aún aquellos usuarios que se consideran totalmente preparados tienen dispositivos infectados, aunque con menor porcentaje (3,5%). En estos casos, sin embargo, podemos ver que quienes declaran no encontrarse preparados o solo algo preparados sí tienen mayor porcentaje de dispositivos infectados.

Por ello, parece que las declaraciones de usuarios y usuarios Android pudieran ser más prudentes dados los resultados. Aunque cabe recordar también que los resultados de infección sobre Android también han sido más positivos.

En cualquier caso, la cantidad de peligros a la que están expuestos los dispositivos móviles y los ordenadores es abrumadora, de ahí la importancia de tener una buena base formativa en materia de seguridad.

Si realizamos una desagregación por género encontramos diferencias significativas entre hombres y mujeres. Cabe destacar que el porcentaje de infecciones en dispositivos Android pertenecientes a hombres se ve disminuido conforme aumenta el nivel de preparación a afrontar incidentes de seguridad. En el caso de los que declaran estar nada preparados el porcentaje de dispositivos infectados es del 30,3% y el porcentaje en los totalmente preparados es de 3,5% (gráfico 49).

En general, el nivel de infección con *malware* de dispositivos Android pertenecientes a mujeres es menor que el nivel de infección de estos dispositivos pertenecientes a hombres. Aparentemente, con los resultados obtenidos por Pinkerton, las mujeres parecen ser más cautelosas en la utilización de su dispositivo Android, ya que el nivel de infección es comparablemente bajo para aquellas que declaran contar con alguna preparación (2,5%), suficiente preparación (3,0%) estar bastante preparadas (3,1%) o totalmente preparadas (3,4%).

7.5. NECESIDADES FORMATIVAS EN CIBERSEGURIDAD

Uno de los recursos clave para evitar conductas de riesgo es la formación. Al consultar si se cree que es necesaria en ciberseguridad, más de la mitad, en concreto el 52,9% manifiesta que es necesaria mucha o bastante formación en ciberseguridad (gráfico 50). Sumado al 38,7% que declara necesitar algo de formación, podríamos concluir que el 91,6% de internautas ven necesaria esta formación.

El gráfico 51 desglosa el acceso a cursos y formación *online* disgregando por género. Pese a que el porcentaje de hombres trabajadores (63%) es mayor que el de mujeres trabajadoras (54,5%), la mayoría de quienes declaran acceder a cursos y formación *online* son mujeres (53,8%).

Sin embargo, en el sector retirado, pensionista o incapacitado, el 87% de quienes muestran interés en los cursos son hombres.

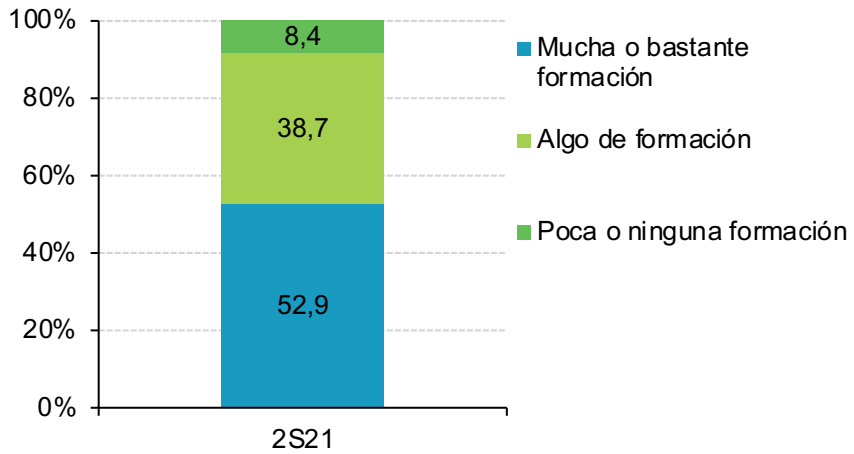
Conforme a los resultados analizados durante todo el estudio se ve más necesario si cabe que se conozcan los peligros a los que se puede enfrentar y las formas de poder mitigarlos. La mejor forma de afrontarlos es disponer de una base sobre conocimientos tecnológicos bien asentada.

El 53% de las personas usuarias consideran que necesitan mucha o bastante formación en ciberseguridad.

La digitalización sin ciberseguridad supone una clara barrera tecnológica muy difícil o imposible de afrontar sin la formación adecuada, adaptada a diferente público o conjuntos poblacionales.

En el segundo semestre de 2021, INCIBE llevó a cabo una serie de jornadas Escolares[21] para mejorar las competencias digitales en profesorado y alumnado de educación primaria y secundaria. Además, se dedican recursos formativos con la llamada experiencia senior para formar a gente de todas las edades y que sean capaces de protegerse y navegar de forma segura por Internet. No obstante, aún queda mucho por hacer.

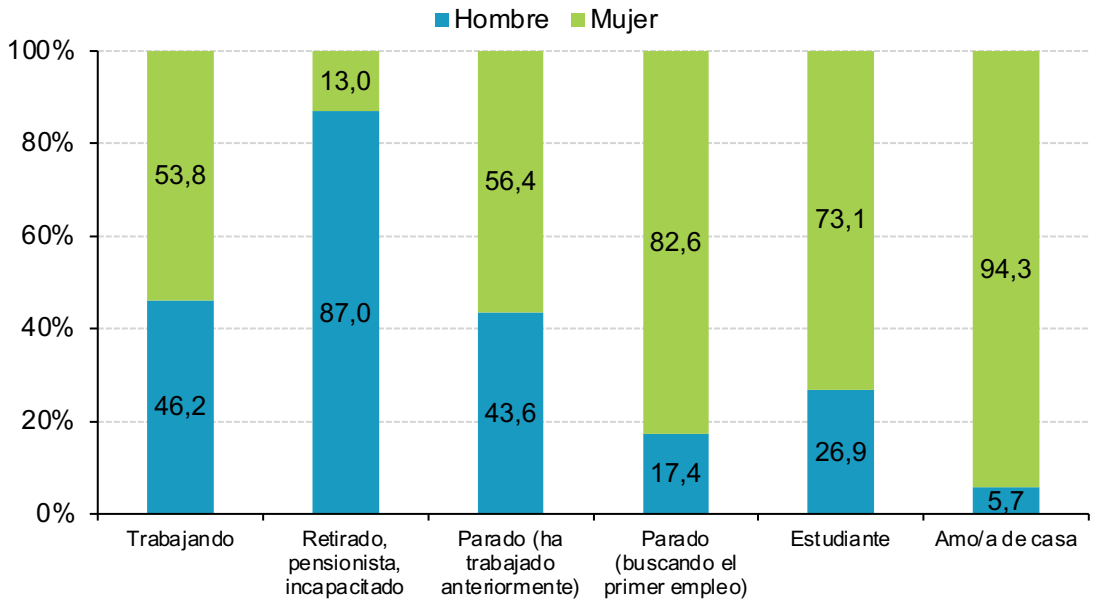
Gráfico 50. Percepción propia sobre necesidad de formación en ciberseguridad (%)



Base: **Total de usuarios y usuarias**
Fuente: **Panel hogares, ONTSI**

[21] https://www.is4k.es/programas/programa-de-jornadas-escolares

Gráfico 51. Acceso a cursos y formación *online* según la actividad realizada por los usuarios (desagregada por género)



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

7.6. ENTIDADES QUE DEBERÍAN IMPULSAR LA CIBERSEGURIDAD

Resulta interesante conocer la opinión sobre los agentes que deberían impulsar las iniciativas en materia de ciberseguridad. A este respecto se ha preguntado si debería liderar dichas iniciativas la Administración pública, la empresa privada o ambas. Los porcentajes se recogen en el gráfico 52. La empresa privada es señalada mayoritariamente.

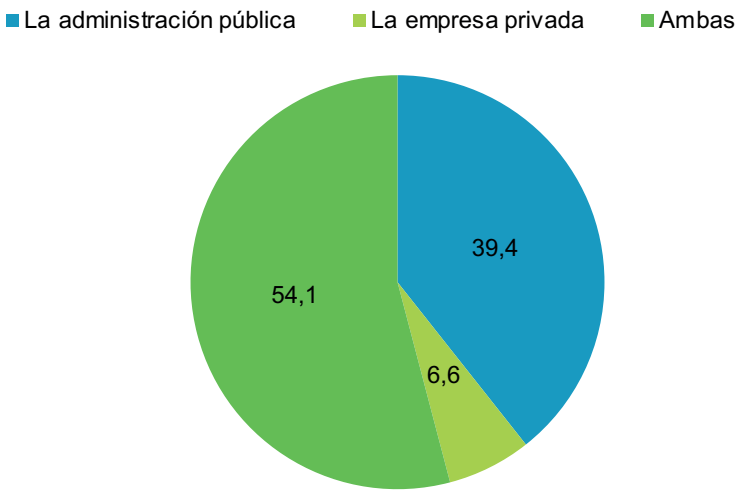
El 54,1% de las personas considera que tanto la Administración pública como la empresa privada deberían impulsar las iniciativas en materia de ciberseguridad. Un porcentaje algo menor (39,4%) opina que debería ser únicamente la Administración pública, y, finalmente, el 6,6% de los internautas opina que el impulso debería provenir únicamente de la empresa privada.

De hecho, los resultados implícitamente avalan los esfuerzos de INCIBE como punto de unión entre empresas y entidades públicas, así como otros esfuerzos conjuntos actuales para que las empresas se involucren cada vez más en dar un impulso a la ciberseguridad. En esta línea, INCIBE celebró en Julio el Cybersecurity Summer BootCamp[22] dirigido a la comunidad de jueces y juezas y magistrados y magistradas: el ministerio fiscal, las fuerzas y cuerpos de seguridad y a especialistas de centros de respuesta a incidentes cibernéticos.

Además, en el mes de octubre se celebró el 15ENISE[23](Encuentro internacional de seguridad de la información) dirigido a profesionales de la ciberseguridad, personas emprendedoras, representantes del sector académico e investigador, empresas de ciberseguridad y empresas interesadas en mejorar la seguridad de la información.

[22] https://www.incibe.es/summer-bootcamp
[23] https://www.incibe.es/enise

Gráfico 52. Opiniones sobre los agentes que deberían impulsar las iniciativas en materia de ciberseguridad (%)



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

8 Conclusiones

Este estudio recoge los resultados de opiniones de internautas **sobre sus hábitos de navegación, utilización de servicios y medidas de seguridad durante el segundo semestre de 2021**. Asimismo, algunas de estas percepciones se han contrastado con la monitorización remota autorizada de dispositivos para evaluar su estado real.

En esta edición se ha querido clarificar **cómo ha influido la pandemia y con ello los diversos estados de confinamiento en los hábitos adquiridos**. Por ejemplo, la crisis sanitaria de 2020 fomentó que, quien aún no lo hacía, tuviera que realizar trámites *online*. Esto ha continuado ocurriendo a lo largo de 2021, de tal forma que la gente se está habituando a utilizar cada vez en mayor medida servicios ofrecidos por Internet.

Entre los servicios más favorecidos se encuentran el **comercio electrónico y el acceso a contenidos digitales de pago o suscripción**. Respecto a este último punto, hay un aumento en el consumo de estos servicios en detrimento del consumo de páginas web de descarga gratuita, lo que supone una disminución en el riesgo de infección por *malware*.

Por otro lado, **la rápida y obligada digitalización como motivo del aislamiento físico** de muchos de los internautas (por ejemplo, por confinamiento debido a la pandemia) ha hecho que más gente comience a utilizar el certificado digital o el DNI electrónico para realizar trámites *online* a través de la **Administración electrónica.** Igualmente, la Administración pública ha potenciado o facilitado el uso de los medios telemáticos dentro de las medidas adoptadas para el control de la emergencia sanitaria.

Aunque las personas usuarias han aumentado la utilización de diversos servicios a través de Internet, **las medidas de seguridad a aplicar en ordenadores del hogar y dispositivos móviles aún son una asignatura pendiente**. Pese a que, por un lado, según las declaraciones recogidas, utilizan en mayor medida los sistemas de desbloqueo seguro en estos dispositivos portátiles, todavía necesitan aumentar la puesta en práctica otras medidas como el uso del antivirus y el cifrado de datos del aparato.

En cuanto a los ordenadores en el hogar es de destacar que deben estar actualizados a la última versión del sistema operativo y con los debidos parches de seguridad además de no desactivar el cortafuegos y añadir una capa de seguridad más al dispositivo utilizando *software* antivirus. En muchos casos, se ha visto reflejado cómo **se confía en la seguridad por defecto de sus dispositivos**. Las medidas automáticas contribuyen a proteger los equipos, pero no son excluyentes de las medidas no automáticas o manuales (por ejemplo, el uso de contraseñas seguras).

Las redes Wi-Fi, como se ha podido analizar en este estudio, son comunes en un alto porcentaje de hogares; por ello, hay que tener en cuenta algunas recomendaciones para mejorar la seguridad. No basta con tener el sistema actualizado, un antivirus y *firewall* activado, también **es necesario tener la red del hogar segura**. A través de los puntos Wi-Fi se conectan múltiples dispositivos del hogar que hay que reconocer y también tener actualizados. La Internet de las cosas (o IoT por sus siglas en inglés), ya es una realidad con la que convivimos en el hogar, y muchas personas aún no reconocen el efecto que sobre la red doméstica puede tener un exceso de dispositivos. Tampoco los riesgos a los que se exponen por no tenerlos actualizados.

Entre otras medidas para mantener la red segura, una de las más inmediatas es cambiar la contraseña del panel de Administración del rúter del hogar, evitando las contraseñas por defecto de la red Wi-Fi del hogar. **Es necesario hacer más difícil el acceso a la red de una posible persona atacante**. Una vez que esta accede a una red repleta de dispositivos solo tiene que encontrar uno vulnerable para intentar ganar más accesos. De esta forma podrían recopilar información que puede ser utilizada para cometer otros delitos tales como fraudes económicos, suplantaciones de identidad, o sencillamente el uso ilegítimo de infraestructuras de conexión.

Entre las **prácticas de riesgo más destacadas podemos incluir la percepción, en muchos casos equivocada, sobre la seguridad de sus ordenadores y dispositivos móviles**. Especialmente, en el caso de los ordenadores del hogar, se tiende a pensar que son más seguros de lo que son. El caso contrario se observa en los dispositivos Android, donde se tiende a pensar que son más vulnerables de lo que han demostrado ser. Tal vez la cercanía y cada vez mayor dependencia de los dispositivos personales móviles facilita que las personas internautas tengan un mejor mantenimiento de estos terminales. Por ejemplo, mantenerlos actualizados o evitar la instalación desde fuentes desconocidas.

Respecto a la percepción de la **preparación de la ciudadanía para afrontar los posibles problemas de seguridad**, en general es optimista, aunque es necesario solventar algunos problemas detectados en esta materia. Por ejemplo, aún se desconocen muchas medidas de seguridad básicas y existe un cierto desconocimiento declarado sobre entidades y campañas de ciberseguridad.

Resulta obvio que las **campañas impulsadas por la Administración pública están contribuyendo positivamente al cambio**, hacia una comunidad de internautas más consciente y preparada para afrontar los riesgos de ciberseguridad. No obstante, quedan muchos aspectos que mejorar para que el total de la ciudadanía tenga la formación necesaria en materia de ciberseguridad.

9 Principales cifras de un vistazo

MEDIDAS DE SEGURIDAD

- **La mayoría de personas usuarias de ordenador utilizan medidas de seguridad, aunque algunas no son conscientes de ello**. El 29,7% declara no usar cortafuegos, cuando los datos de sus dispositivos reflejan que el 96,6% los usa.

- **Muchos hombres creen adoptar medidas de privacidad en los ordenadores, pero la realidad lo desmiente**. El 25,2% de los usuarios de ordenador declara utilizar programas o configuración anti-spam. Pero tan solo el 1,3% lo hace. En lo que respecta a programas anti-espía o antifraude, un 17% declara usarlos; la cifra real es del 4,9%.

- **En el caso de usuarias de ordenador, destaca un mayor uso que los hombres de programas anti-espía o anti-fraude, aunque su uso declarado es menor respecto a ellos**. Los datos del uso de cortafuegos o *firewall* en ordenador pertenecientes a las mujeres demuestran que el 98,5% lo utilizan. Pero tan solo el 23,8% de ellas es consciente.

- **Las mujeres usan dispositivos Android más actualizados, pero ellos hacen mayor uso de programas antivirus**. El 67% de los dispositivos Android de ellos tiene antivirus, frente al 59,8% de ellas.

ORDENADORES Y DISPOSITIVOS INFECTADOS

- **Los incidentes de seguridad declarados aumentan del 55% al 60% durante el último semestre**. La incidencia de virus o códigos maliciosos y la relacionada con la restricción de acceso por ciberataques asciende al 14%. El 71% de internautas ha sufrido una situación de fraude.

- **La mitad de los ordenadores analizados están infectados por *malware*, pero pocas personas son conscientes**. Hay mayor proporción de ordenadores contagiados entre los hombres que entre las mujeres, 54,9% frente a 48%. Un 65% de los ordenadores y un 58% de los dispositivos Android infectados sufrieron ataques por *malware* de alta peligrosidad

- **Las personas que usan dispositivos Android tienden a ser pesimistas en cuanto a la infección: hay menos contagios de las que se declaran**. El 7,5% cree estar infectado con algún tipo de *malware*; la realidad es que tan solo el 3,7% de los dispositivos analizados lo estaba.

FORMACIÓN Y PREPARACIÓN ANTE INCIDENTES

- **El 41% declara realizar alguna conducta de riesgo a sabiendas y el 40% reconoce no saber con seguridad si su equipo está actualizado**. El 37% de las personas utiliza sitios web de dudosa reputación para realizar descargas de contenidos o programas, y un 42% ve difícil acceder a información para navegar de manera segura. El 53% considera que necesita mucha o bastante formación en ciberseguridad.

- **La percepción del nivel de preparación ante problemas de ciberseguridad entre quienes usan ordenador y terminales Android es alta**. Solo el 6,4% de las personas que usan terminales Android y el 6,8% de las que usan ordenador declara falta de preparación ante los ataques. Destaca el porcentaje de quienes declaran estar suficientemente preparados para afrontar algún problema de ciberseguridad en su dispositivo Android (38,5%) o en su ordenador personal (37,8%).

- **Más de la mitad de los hombres que declara sentirse totalmente preparado para afrontar riesgos de ciberseguridad, tiene su ordenador infectado**. Este porcentaje es del 55,8%. Ocurre parecido con quienes aseguran estar bastante preparados; el 63,8% tiene su equipo contagiado. El 81,1% de los que afirman no encontrarse preparados lo tienen infectado.

- **Las personas que usan terminales Android que dicen tener mayor preparación sobre riesgos de ciberseguridad, tienen menores niveles de infección en su equipo**. Quienes piensan que están algo (4,4%) o nada (4,5%) preparados o preparadas son quienes tienen un porcentaje de infecciones mayor en su dispositivo Android.

10 Descripción y alcance del estudio

El Observatorio Nacional de Tecnología y Sociedad (ONTSI) publica semestralmente los resultados del estudio *Cómo se protege la ciudadanía ante los ciberriesgos: estudio sobre percepción y nivel de confianza en España*. Se analizan las medidas de seguridad que implementan los usuarios en los ordenadores del hogar y en sus dispositivos móviles y la incidencia de estos riesgos, además de su grado de confianza en las nuevas tecnologías.

En concreto, en este documento se ofrece un análisis sobre los datos recabados en el segundo semestre de 2021. En el caso de los datos de dispositivos móviles, se han recogido datos solo de tabletas y teléfonos Android. En el de los ordenadores, de equipos con Windows (en varias versiones, desde la 7 inclusive), Linux y macOS.

El estudio se realiza a través de dos vías[24] : el análisis de seguridad real de los equipos informáticos y dispositivos móviles, mediante el escaneo con un *software ad-hoc* y el análisis de las declaraciones aportadas por las personas encuestadas. Los datos son obtenidos de las preguntas en línea realizadas a los hogares que han conformado la muestra del estudio, mientras que para los datos reales se utiliza el *software* Pinkerton, que analiza los sistemas de ordenadores personales 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* (programas malignos) en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 70 motores antivirus.

El informe está enfocado a ofrecer una panorámica del comportamiento y la utilización de las nuevas tecnologías en aspectos relacionados con la seguridad y la privacidad. La pretensión es servir de apoyo para solucionar incidencias por parte de las personas usuarias, así como para la adopción de medidas por parte de la Administración.

Este estudio se realiza sobre una base de datos recogidos desde julio hasta diciembre de 2021, ambos meses inclusive.

[24] Los gráficos que hacen referencia a datos recogidos a través de ese *software* vienen indicados con el icono correspondiente.

Índice de gráficos

Índice de tablas

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_2022_1

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
Luis Muñoz
José María Zavala Pérez
Belén Kayser

Estudio realizado con asistencia técnica de Hispasec y Gfk.

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

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

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · ontsi · incibe_ · OBSERVACIBER · UNIÓN EUROPEA Fondo Social Europeo El FSE invierte en tu futuro

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
ontsi Observatorio Nacional de Tecnología y Sociedad
incibe_
OBSERVACIBER
UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro