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

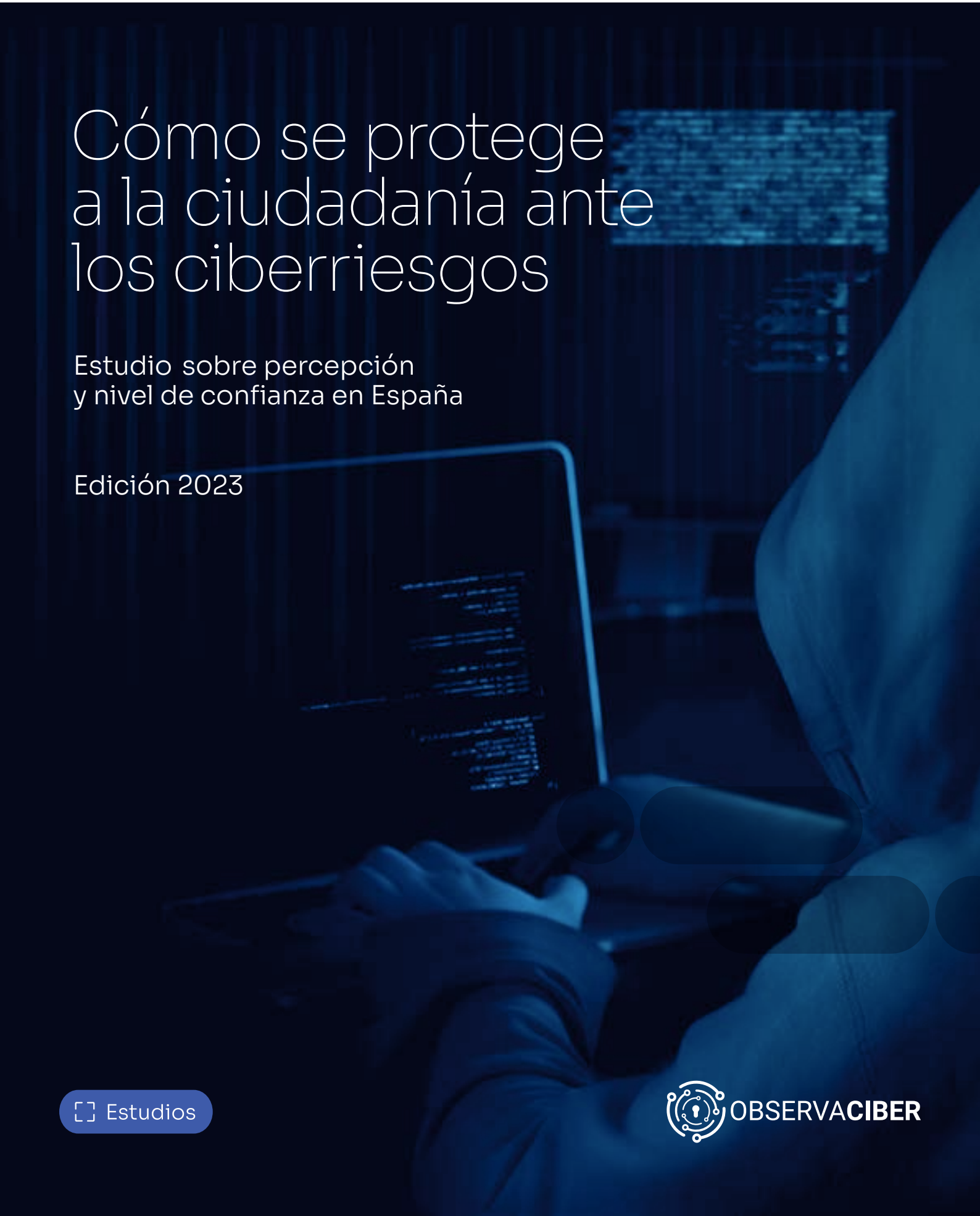
red.es | ontsi

incibe_

Cómo se protege a la ciudadanía ante los ciberriesgos

Estudio sobre percepción y nivel de confianza en España

Edición 2023



Estudios

OBSERVACIBER

Estudios

Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. Edición 2023 ha sido elaborado por el equipo de trabajo del Observatorio Nacional de Tecnología y Sociedad. Estudio realizado con asistencia técnica de Hispasec y Gfk.

Sugerencias para citar este informe:
Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. Edición 2023. Observatorio Nacional de Tecnología y Sociedad.
Red.es. Secretaría de Estado de Digitalización e Inteligencia Artificial. Ministerio de Asuntos Económicos y Transformación Digital.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es | ontsi | incibe_ | OBSERVACIBER

Destacados

Las personas usuarias tienen una falsa percepción de seguridad de sus ordenadores

6,8%

El 56,6% de los ordenadores escaneados presenta algún tipo de *software* malicioso, pero solo un 6,8% percibe esa infección.

En el caso de los terminales Android, el 7,1% de la población cree tenerlo infectado, aunque solo el 3% de aparatos lo estaban realmente.

Aumenta el porcentaje de internautas que modifican sus hábitos de comportamiento tras experimentar una incidencia de ciberseguridad.

El Observatorio Nacional de Tecnología y Sociedad (ONTSI) publica nueva edición del estudio *Cómo se protege la ciudadanía ante los ciberriesgos: Estudio sobre percepción y nivel de confianza en España*, donde se analizan datos correspondientes al primer semestre de 2022 para conocer mejor las costumbres y conductas de la sociedad española.

Servicios de Internet más utilizados

Baja el uso de contenidos digitales gratuitos (-7,5 p.p.) respecto de 2021, y se incrementa del de los de de pago (+8,5 p.p.).

Medidas de seguridad

Casi la totalidad de los ordenadores (97%) **tienen cortafuegos**, pero solo el 27,7% de las personas declaran utilizarlo.

Algunas medidas de seguridad implementadas en **dispositivos Android** coinciden con la percepción que tienen sus usuarios y usuarias. Así:

- El **87%** de la población percibe que **el uso de patrones de desbloqueo está generalizado**, lo que se identifica con su verdadero uso (85,1%).
- Mientras que el **uso declarado del antivirus** es de un 58%, el real es del 56%.
- Aunque un **86,9%** de la población cree tener el **sistema de su terminal Android actualizado,** solo cuatro de diez dispositivos (41,1%) lo está realmente.

Entre las principales **razones de falta de uso** de medidas de seguridad en los dispositivos se encuentra: **no percibirlas necesarias** o interesantes y el desconocimiento.

Hábitos relacionados con la seguridad y comportamientos de riesgo

Cuatro de cada diez personas (40,3%) declara **haberse expuesto deliberadamente a riesgos *online***. De ellos:

- El 37,5% navega sin saber si su equipo está actualizado.
- El 33,4% descarga contenido de páginas de fiabilidad dudosa.

El **61,9% de la población usuaria en España accede a contenidos gratuitos *online***. De ellos:

- Siete de cada diez (71%) personas usuarias experimentaron **incremento de publicidad** después de acceder a esos contenidos.

Mejoran las buenas prácticas en la **descarga de fichero** en línea. Se incrementan respecto al año anterior:

- La comprobación de la veracidad del contenido descargado (51,1%, +2,9 p.p.).
- El análisis de dispositivos después de la descarga (50,5%, +3,2 p.p.).
- Y el uso de programas para descargar contenido web (36,7%, +2 p.p.).

Destacan **buenos hábitos** de la ciudadanía que usa **banca *online* o comercio electrónico**. Más del 80% declara realizar estas acciones:

- Revisa periódicamente la cuenta bancaria (88,8%).
- Cierra la sesión al terminar (85,2%).
- Evita usar equipos públicos o compartidos.
- Evita lugares donde el usuario puede ser visto (80,3%).

La ciudadanía que utiliza servicios *online* suele usar siempre **los mismos valores para todos sus servicios**:

- **Siete de cada diez** continúan utilizando usuario y contraseña para identificarse.
- Solo el **18%** de las personas entrevistadas tiene un **gestor de contraseñas.**
- Más del **40%** declara utilizar mecanismos de **doble factor de autenticación** (48,2%) o **datos biométricos** (42,8%).

Las medidas más utilizadas por los usuarios o usuarias con menores a su cargo para asegurar el **bienestar *online* de menores** son:

- Hablar con ellos sobre los riesgos *online* (43,8%).
- Limitar el tiempo de conexión (40,1%).
- Activar controles parentales (36,8%).
- Monitorizar su uso de Internet (29,4%).

El 66,9% de la población que ha conocido personas por Internet, ha sido a través de redes sociales.

- El 79,9% declara tener **suficiente, bastante o mucha confianza en los contactos desconocidos a través de Internet.**
- Antes de reunirse en persona, el **64,7%** de las personas que ha conocido a otras a través de Internet han tomado precauciones adicionales, como chatear por WhatsApp u otras aplicaciones de mensajería instantánea.

Incidentes de seguridad

La percepción de los usuarios de Internet sobre la **infección de sus ordenadores** difiere de la realidad.

- Solo un **6,8%** percibe tener infección en su PC.
- Aunque el **56,6%** de los ordenadores escaneados presentan algún tipo de *malware*, el dato desciende 2,5 puntos respecto al año anterior.

Aumentan los incidentes de ciberseguridad:

- Seis de cada diez (**60,4%**) personas usuarias de Internet afirman haber sufrido un **incidente de seguridad** durante el primer semestre del año 2022, un aumento de 5,1 p.p. respecto al año 2021.
- El **incidente más común es la recepción de correos no solicitados o deseados** (*spam*) que, aunque desciende 4,5 p.p. interanualmente, se sitúa en el 80,4% de los casos.

56,6%

Se reduce la infección por *malware*. Un 56,6% de los ordenadores tienen algún tipo de *software* maligno, tras un descenso de 2,5 puntos con respecto al año 2021 y 9,6 p.p. respecto a 2020.

- **El *adware* es el *malware* más frecuente** (en 45,3% de los ordenadores infectados), que anuncios en la ventana del navegador con fines publicitarios.
- El 70,2% de ordenadores y de dispositivos Android infectados presentan ***malware* de alta peligrosidad.**

Se reduce el número de infecciones en terminales Android. Aunque 7% de la población cree tener su dispositivo infectado, realmente solo el 3% de los terminales Android presentaban algún tipo de *malware* en el primer trimestre de 2022, 3,8 puntos porcentuales menos que el año anterior.

El perjuicio económico más frecuente debido a un fraude *online* experimentado por las personas entrevistadas se encuentra en la franja de entre **0 y 100 euros.**

Mejora los hábitos de seguridad después de haber tenido un incidente:

- El 67,5% internautas que han experimentado una incidencia de ciberseguridad han modificado sus hábitos de comportamiento en el uso de Internet, 6,5 p.p. más que el año anterior.
- La **mejora de las contraseñas** es el cambio realizado con mayor frecuencia.

Más de **la mitad de la población internauta** (50,8%,) **cree necesario recibir mucha o bastante formación en materia de ciberseguridad.**

Introducción

Para beneficiarse de las oportunidades de la transformación digital, personas, empresas y gobiernos deben confiar en los entornos digitales. La digitalización está creando nuevos desafíos que afectan a la privacidad, la protección de datos confidenciales y las comunicaciones de la red. Pero a pesar de estos nuevos retos, es importante seguir trabajando para aumentar la confianza en las actividades en Internet, al mismo tiempo que se potencia el crecimiento económico y el bienestar social.

Medir, analizar y comprender los riesgos e incidentes de ciberseguridad es un requisito para poder gestionarlos e incrementar de forma eficiente la ciber confianza de la ciudadanía.

En ese contexto, el ONTSI e INCIBE publican una nueva edición del informe *Cómo se protege a la ciudadanía ante los ciberriesgos* en el que analizan la percepción y nivel de confianza de la población española a partir del trabajo de campo realizado en el primer semestre de 2022.

Como en otras ediciones, el informe analiza hasta qué punto la percepción que tiene la ciudadanía sobre la preparación de sus dispositivos ante los ciberriesgos se corresponde con la realidad. Para conseguir este objetivo, se trabaja de dos formas distintas. Por una parte, se encuesta a los participantes de un panel de personas sobre la opinión que tienen sobre concienciación, preparación y percepción de ciberriesgos. Por otra parte, se obtienen datos directos de los dispositivos que estos panelistas utilizan para acceder a Internet. Para ello, mediante el *software* Pinkerton, se escanean, previa autorización de los propietarios, sus dispositivos (dispositivos Android, tanto tabletas como móviles, y ordenadores).

Pinkerton es un *software* desarrollado por Hispasec, seguro y transparente para quienes lo usan; analiza los datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas. También detecta la presencia de programa maligno en los equipos y dispositivos móviles, por tanto, son datos reales obtenidos directamente de los dispositivos de las personas usuarias.

El informe está dividido en 9 capítulos. En el primero se revisa la utilización de los servicios de Internet y sus consecuencias. Las medidas de seguridad que adopta la ciudadanía, en el capítulo 2, con intención de valorar las actitudes y comportamientos en torno a la seguridad en línea. El capítulo 3 describe los hábitos de navegación y uso de Internet con objeto de comprender como estos influyen en el comportamiento de riesgo. Los incidentes declarados y los contrastados mediante los datos recogidos por el *software* Pinkerton se describen en el capítulo 4. El 5 recoge las consecuencias de los incidentes de seguridad, ya sean pérdidas económicas, infecciones de los equipos e incluso cambios de hábitos. Estos incidentes de seguridad provocan en cierta manera la pérdida de confianza en los servicios de Internet, lo que se analiza en el capítulo 6. Las conclusiones obtenidas se enumeran en el capítulo 7, y en el 8 se resumen las principales cifras que se obtienen del informe. Por último, en el capítulo 9 se describe la metodología y alcance del estudio.

01

Servicios de Internet más utilizados

Esta sección resume las principales conclusiones sobre el uso de Internet y sus consecuencias. Además de los tradicionales usos sociales y comerciales de la red, son fundamentales otros ámbitos como el entretenimiento (concretamente a través del acceso a las plataformas de contenidos gratuitos), la formación y la realización de trámites financieros y administrativos.

En particular, deben destacarse los aumentos en el acceso a contenidos de pago y a la Administración Pública electrónica, con unas subidas interanuales de 8,5 p.p. y 5,7 p.p., respectivamente. Prácticas que pueden haberse visto beneficiadas, debido a la modernización y la extensión del teletrabajo que causó la pandemia y que llegó para quedarse.

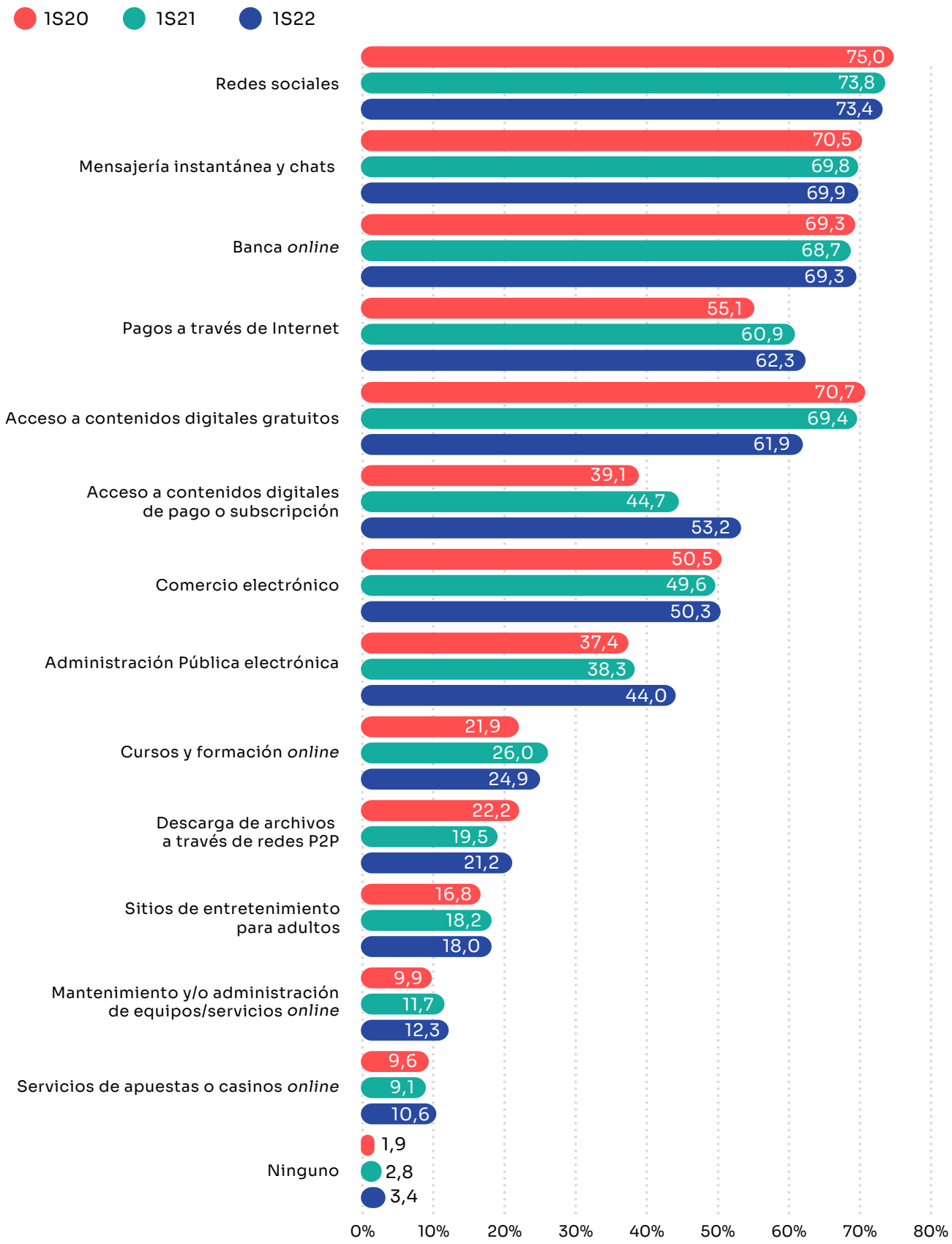
El comercio electrónico recupera los valores de 2020, aunque las constantes campañas de *phishing*[1], fraude y otros ciberdelitos no han dejado de sucederse.

A su vez, los pagos a través de Internet han aumentado ligeramente en un año (+1,4 p.p.).

Destaca el descenso en el uso de la banca *online* y el incremento de acceso a contenidos digitales de pago y a la Administración Pública electrónica

[1] https://www.incibe.es/protege-tu-empresa/tematicas/*phishing*

Gráfico 1 - **Servicios ofrecidos por Internet que han sido utilizados por las personas usuarias por semestre**



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

02

Medidas de seguridad

En esta sección se analizan las medidas de seguridad utilizadas durante el primer semestre de 2022; **la intención es valorar las actitudes y comportamientos en torno a la seguridad en línea**. La información es extraída de las declaraciones de las personas entrevistadas sobre las medidas de seguridad que se implementan tanto en el ordenador de su hogar como en sus dispositivos móviles. Además, se ha realizado el análisis de los dispositivos con el *software* Pinkerton para contrastar con el estado real de las medidas de seguridad y la percepción de las personas consultadas recogida a través de la encuesta.

2.1. Protección de los ordenadores del hogar

Los ordenadores domésticos no siempre son dispositivos personales, a menudo son el punto de acceso a Internet común para la familia. Por este motivo, es importante asegurarse de comprender las protecciones implementadas en su dispositivo u otras adicionales que pueden ser muy útiles.

Las medidas automatizables son aquellas que no dependen de la intervención de las personas que las utilizan. Este grupo incluye, entre otros, actualizaciones del sistema operativo, uso de programas antivirus, *firewalls*, programas o bloqueadores de anuncios y ventanas emergentes.

Todas estas medidas brindan seguridad a la persona usuaria por defecto, pero no excluyen aquellas que no pueden ser automatizadas. Ambas están diseñadas para una seguridad más completa.

En el gráfico 2 se muestra un balance de este tipo de acciones de los últimos tres semestres.

Este semestre aparece una métrica nueva, el *software* anti-rastreo, que limita el acceso a cierto minado de datos al resto de *software* instalado o de terceros. Su presencia lo declara emplear el 11,6% de la población internauta.

Por otro lado, el 54% de personas usuarias declara emplear equipos actualizados y el 27,7% cortafuegos, y disminuyen respectivamente 7 p.p. y 4 p.p. Estas medidas pueden dar la sensación de que dificultan la ejecución de algún otro *software* o afectan a su rendimiento.

A menudo son programas nativos del sistema, pero pueden reactivarse automáticamente o después de una actualización. Otra razón podría ser que el dispositivo que se utiliza no permita más actualizaciones. Esta puede ser una razón por la que se compran nuevos dispositivos.

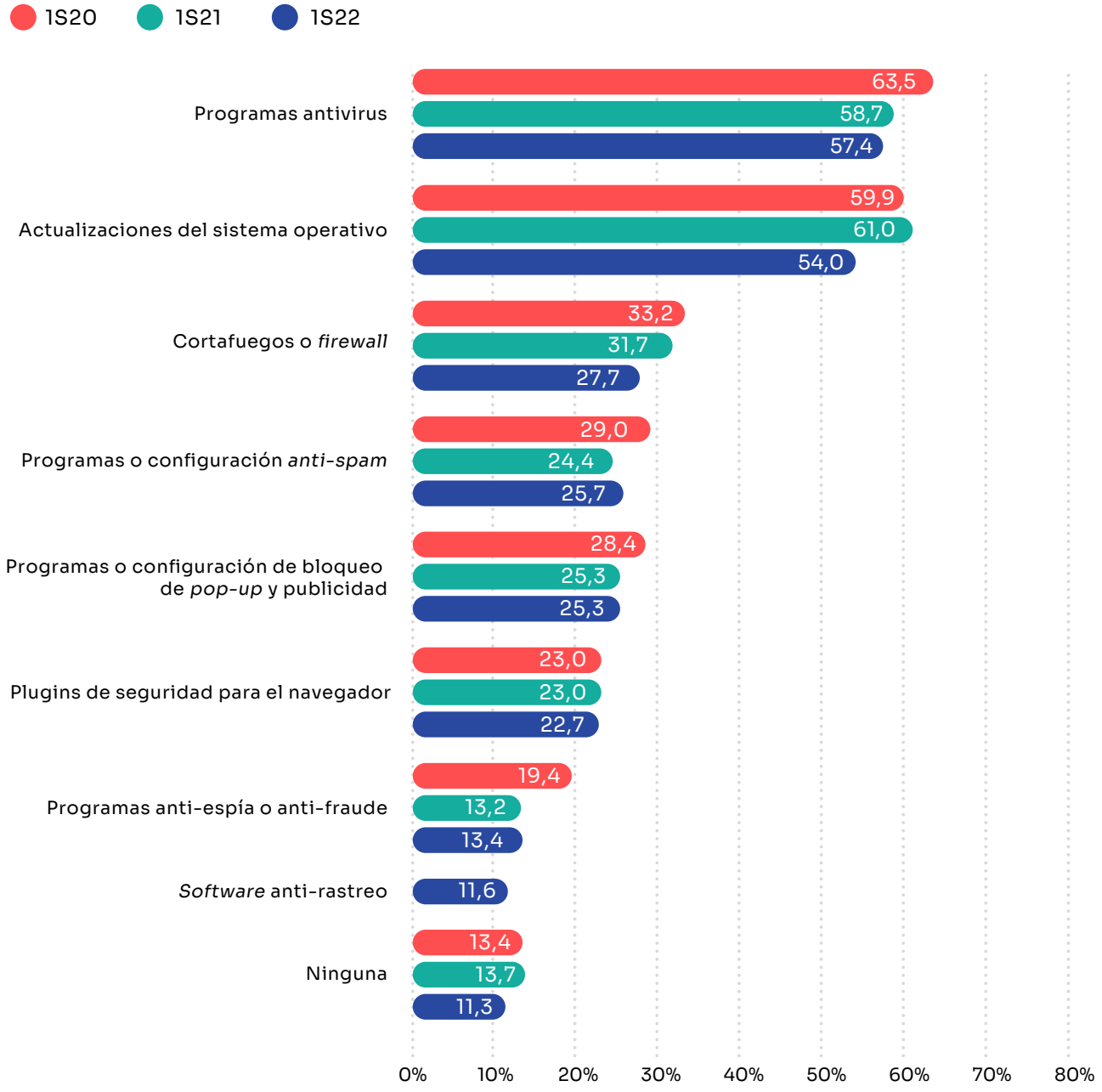
Se emplean, además, otras medidas, como los programas para bloqueo de publicidad, anti-*spam*, anti-espía, o *plugins* de seguridad para el navegador. Algunos gestores de correo permiten identificar correos electrónicos con *software* malicioso, aunque no de forma inmediata.

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.

Se completa esta información y se contrasta con los datos recogidos por el *software* Pinkerton, y revela posibles discrepancias entre las opiniones recogidas y los datos arrojados desde los dispositivos.

Siguen disminuyendo el uso de cortafuegos y las actualizaciones del sistema operativo

Gráfico 2 - **Medidas de seguridad automatizables en el ordenador del hogar (datos declarados)**



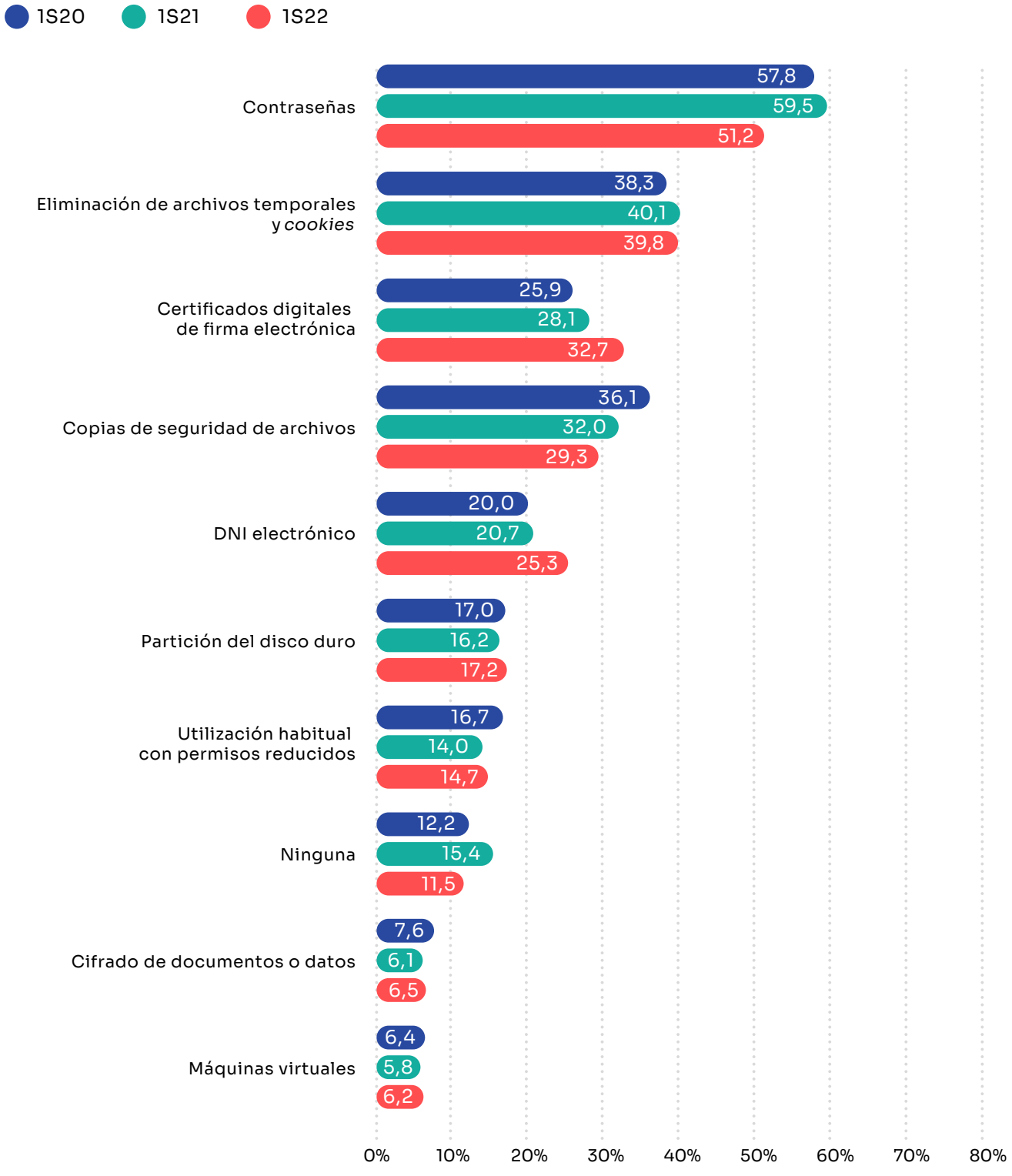
Base: Total usuarios y usuarias
Fuente: Panel hogares, ONTSI

Por otro lado, es importante considerar contramedidas activas o no automatizables. Tales medidas requieren la intervención manual de las personas usuarias, como la utilización de contraseñas seguras, la eliminación de archivos temporales o el uso de certificados digitales que deben instalarse en el navegador o el equipo.

El gráfico 3 recoge las medidas de seguridad no automatizables que los usuarios dicen tener activas en el ordenador del hogar.

En la primera mitad de 2022, el porcentaje de personas usuarias de Internet que declaran usar sus ordenadores con permisos limitados es del 14,7% y particionan su disco duro el 17,2%. Más adelante se verá que el uso real de este tipo de medidas es mucho mayor que el declarado. El DNI electrónico aumenta 4,6 p.p. respecto al año anterior, incremento favorecido, entre otras, por la creciente digitalización de la Administración Pública. De la misma manera, el certificado digital aumenta su popularidad con buena aceptación por parte de la población con un 32,7% de personas usuarias (+4,6 p.p. de crecimiento interanual).

Gráfico 3 - **Medidas de seguridad activas o no automatizables en el ordenador del hogar (datos declarados)**



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

Disminuye 8,3 p.p. interanualmente el uso de contraseñas. Hay que destacar que se han implementado otros métodos de identificación, como la huella digital. Muchos equipos tienen integrada esta característica, aunque requieren también uso de contraseñas.

Es frecuente pensar que las contraseñas evitan que una tercera parte acceda físicamente a un dispositivo (por ejemplo, en una oficina), pero se olvida que también pueden colocar una barrera de control contra cualquiera que acceda a un dispositivo de forma remota y requieran, por ejemplo, elevar privilegios.

Aumenta 0,4 p.p. el uso de máquinas virtuales, lo que brinda un mayor nivel de aislamiento y, por tanto, seguridad.

La comparativa de las declaraciones con los datos recabados por Pinkerton sobre los ordenadores, se reflejan en el gráfico 4, donde se incluyen medidas tanto automáticas como no automáticas.

Por ejemplo, el 54% de las personas usuarias de ordenador, declara tener las últimas actualizaciones instaladas, pero en realidad son el 40%, según datos de Pinkerton. Si los desagregamos por género observamos que el 38,7% los hombres tienen el sistema actualizado, frente al 40% de las mujeres.

El 100% de los equipos domésticos analizados se utilizan con permisos limitados.

Otra medida de seguridad muy útil es un *firewall*, que actúa como una barrera entre su ordenador e Internet. Aunque el 27,7% de la población usuaria reconocía su uso, está presente en el 97% de las máquinas analizadas.

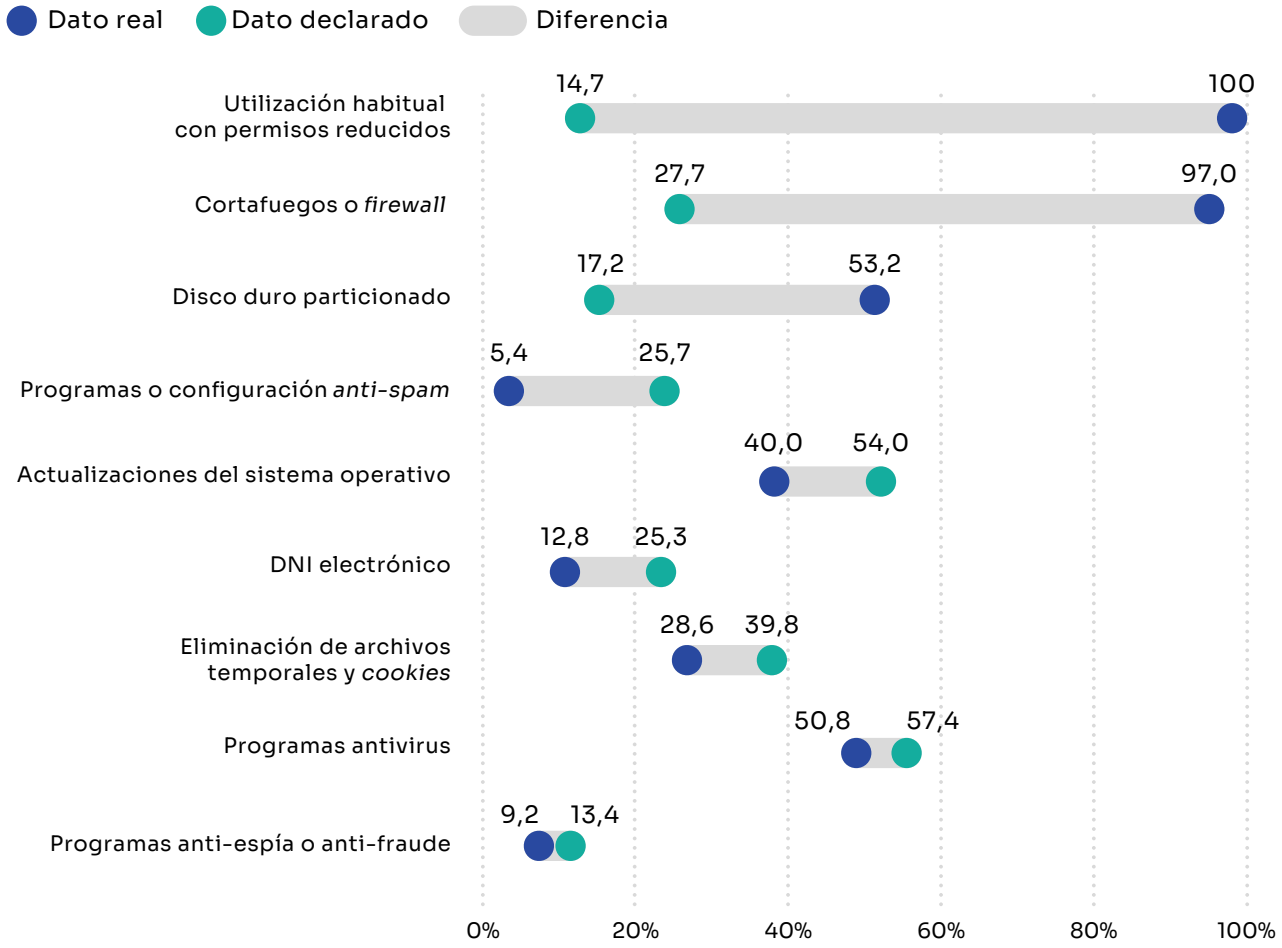
Por otro lado, el uso de antivirus[2] también muestra diferencias entre el dato real (50,8%) y el dato declarado (57,4%). También es cierto que las personas usuarias cuentan con la capa de seguridad que ofrece el sistema operativo en el caso de Windows, se emplea Defender y en el caso de MAC, se protege por contraseña el acceso a aplicaciones de terceros, por defecto bloqueadas.

Para los programas anti-*spam*, los datos recopilados por Pinkerton muestran que este tipo de *software* está presente y activo en solo el 5,4% de ordenadores analizados. Esto contrasta con los datos declarados, donde el 25,7% de las personas entrevistadas dijeron que poseen este tipo de programas.

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

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

Gráfico 4 - **Uso declarado vs real de medidas de seguridad en el ordenador del hogar (%). 1s 2022**



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

Una gran parte de la población desconoce si su ordenador cuenta con uso de permisos reducidos, cortafuegos o el disco duro particionado

2.2. Protección en los dispositivos Android

En este apartado se evalúan las medidas de seguridad utilizadas en los dispositivos Android. Los resultados se muestran en el gráfico 5.

La medida de seguridad más común es el uso de PIN, patrón u otro sistema de desbloqueo seguro. De hecho, durante el primer semestre de 2022, el 87,0% de las personas usuarias de Android, declara que lo utiliza, lo que supone un incremento interanual de apenas 0,3 puntos porcentuales.

Aumenta el uso de medidas de seguridad como actualizaciones del sistema y aplicaciones (86,9%), bloqueo automático (69,9%), copias de seguridad (67,3%), antivirus (58,8%) y gestor de contraseñas (48%). Estas medidas se ejecutan automáticamente sin la intervención de quien lo usa.

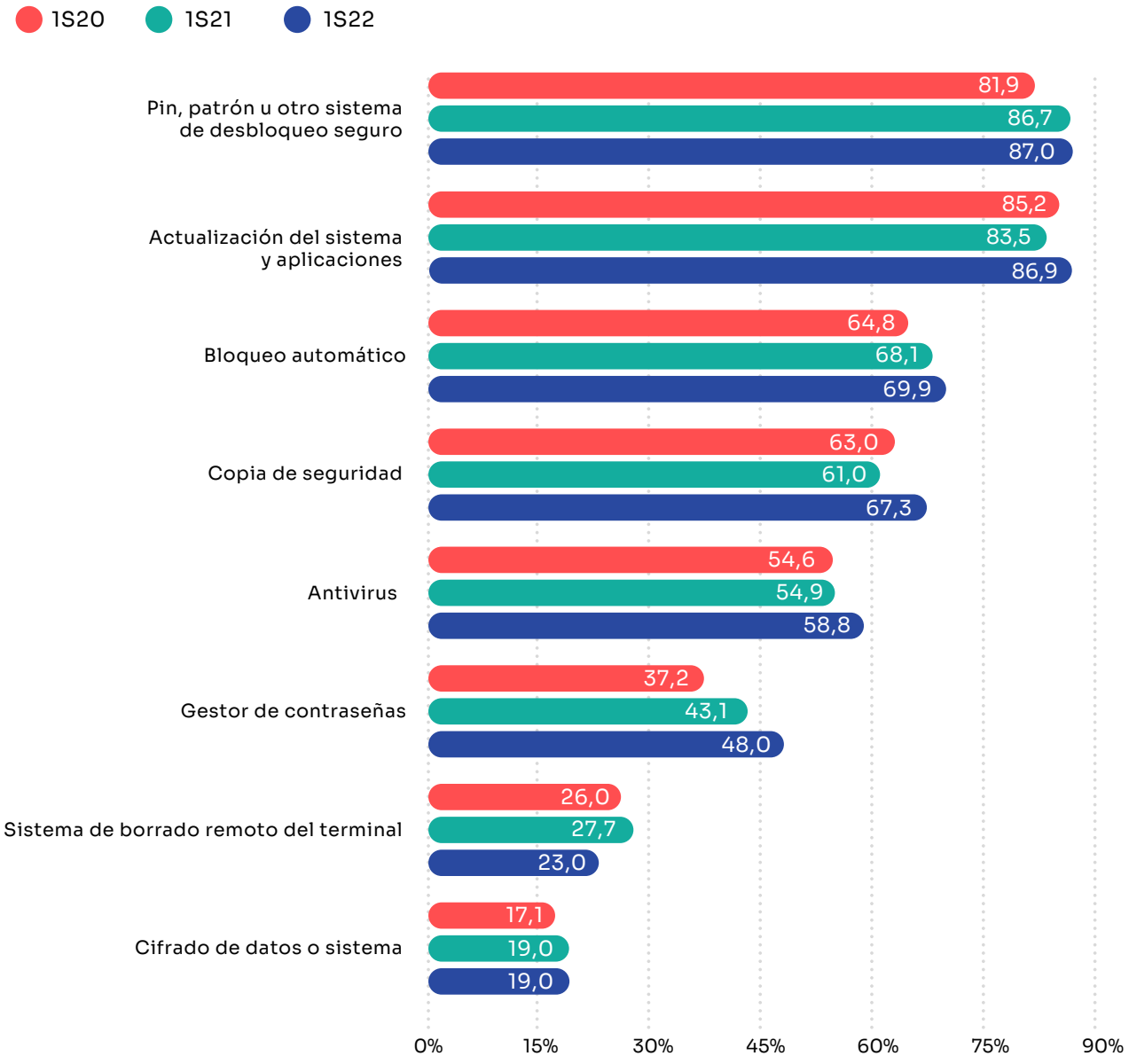
Para los datos resultantes del escaneo de los dispositivos que se muestran en el gráfico 6, el 85,1 % de los dispositivos Android analizados por el *software* de Pinkerton utilizaron de manera confiable un PIN o un patrón de desbloqueo seguro. Esta es una de las acciones que requieren las aplicaciones de banca electrónica para realizar transacciones bancarias y pagos móviles.

El número real en este caso está cerca del número declarado por las personas encuestadas (87%).

A la hora de mantener actualizado el sistema operativo, existe una gran diferencia entre la percepción de la población usuaria (86,9%) y la realidad (41,1%).

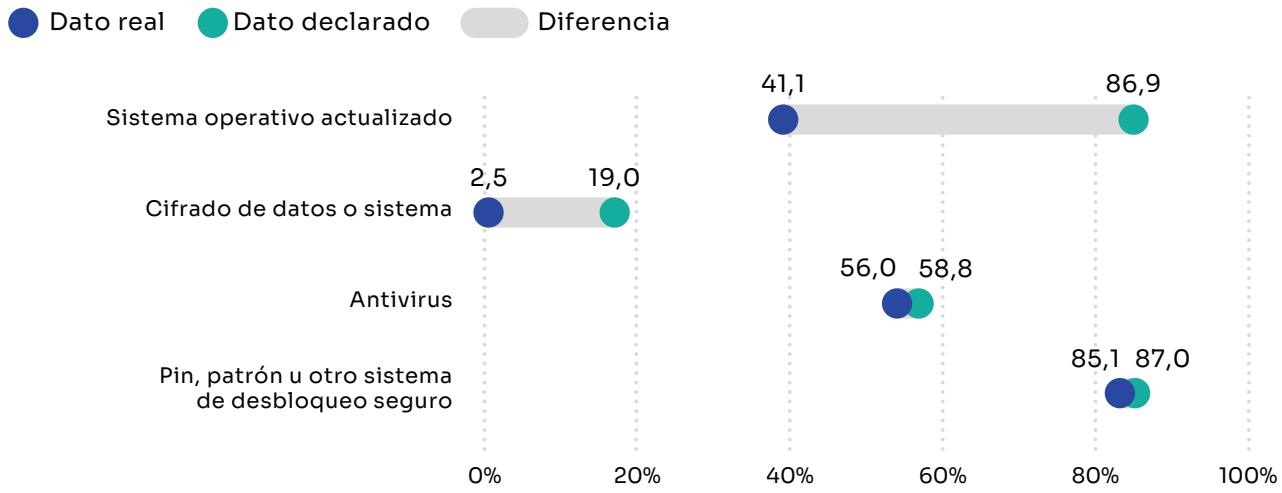
Si desagregamos por género y según Pinkerton, en lo que a actualizaciones del sistema se refiere, el 43,4% de los hombres actualiza su dispositivo móvil frente al 38,8% de mujeres.

Gráfico 5 - **Medidas de seguridad usadas en dispositivos Android (%)**



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

Gráfico 6 - **Uso real de medidas de seguridad en dispositivos Android frente a uso declarado (%). 1s 2022**



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

Quienes usan Android informan que utilizan programas antivirus[3] en sus móviles, en el 58,8% de los casos, cifra que no se aleja mucho del dato real (56%).

Este dato es interesante, ya que hasta hace poco la tendencia habitual era considerar innecesario el uso de antivirus en los móviles. Según el INE[4], en 2021, el 32% accede a Internet en ordenadores de sobremesa, el 54% en portátiles, el 37% en tabletas y el 94% en teléfonos móviles en 2021.

La banca electrónica 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 permiten cambiar los permisos[5] 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.

2.3. Renuncia a las medidas de seguridad

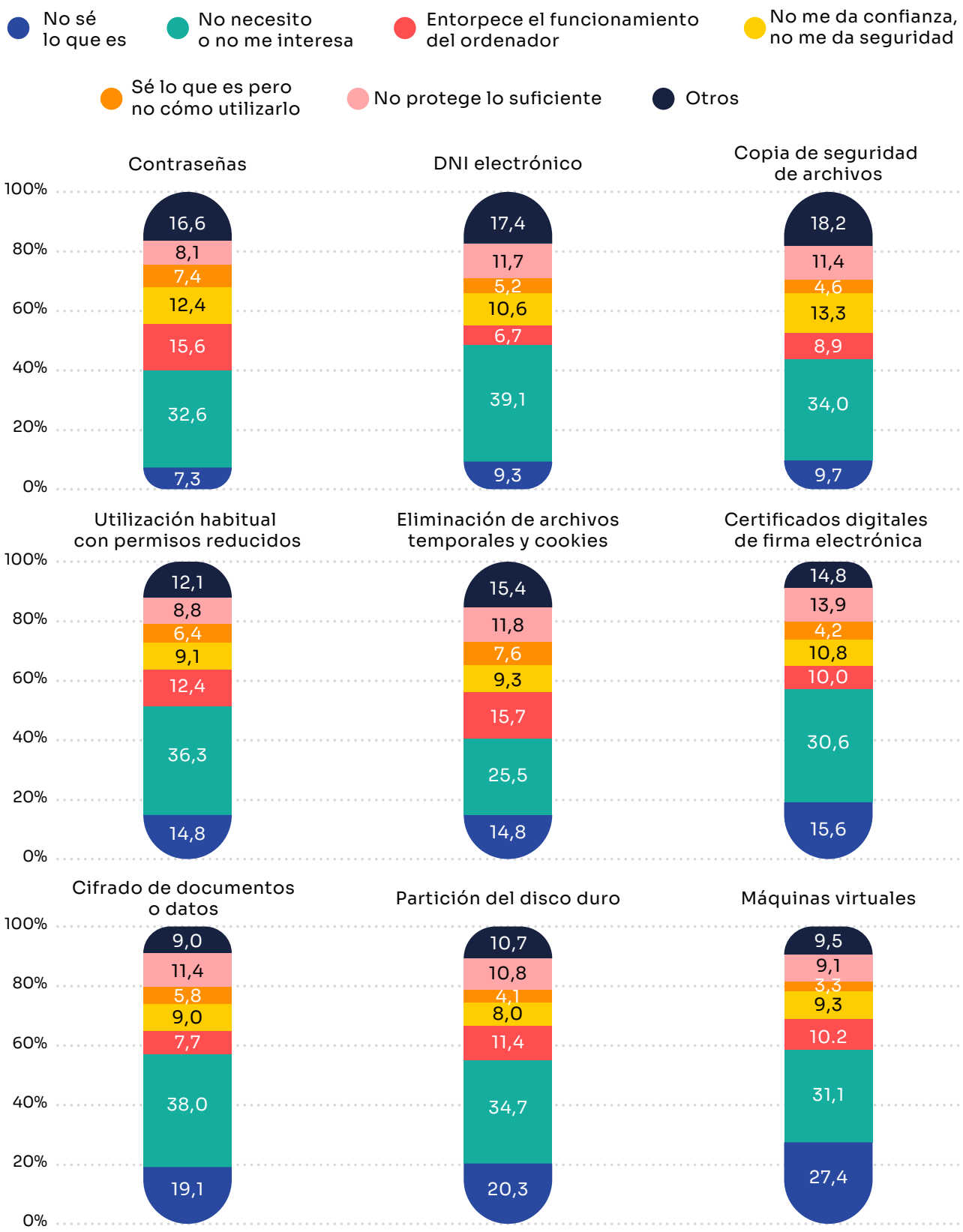
Frente a las cifras que revelan el uso activo y automatizado de ciertas medidas de seguridad, es importante considerar las motivaciones para renunciar a otras medidas que no cuentan con tanta acogida. Las principales razones que se alegan para no aplicar medidas de seguridad nos permiten comprender la percepción y trabajar en futuras medidas de concienciación.

[3] 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

[4] https://www.ine.es/prensa/tich_2021.pdf

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

Gráfico 7 - **Motivos de no utilización de medidas de seguridad. 2022**



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

El uso de máquinas virtuales es la métrica más desconocida para el 27,4% (Gráfico 7). Una máquina virtual permite crear un entorno en el que se puede ejecutar pruebas. También puede usar diferentes sistemas operativos en el mismo dispositivo y evitar dependencias entre diferentes tipos de *software*.

El 39,1% de las personas que utilizan un ordenador sin implementar medidas de seguridad, no considera necesario el uso del DNI electrónico. Aunque es importante destacar que existen otros certificados digitales disponibles en la actualidad como los sistemas de autenticación permanente cl@ve, cl@ve pin o SMS.

Entre las principales razones que se alegan para justificar la falta de uso de esta medida de identificación, los datos reflejan el desinterés y la percepción de que no se necesita.

Aunque hay que destacar que, debido al aumento de los trámites gubernamentales, cada vez más personas acuden a autenticarse y firmar documentos mediante DNI electrónico o certificados digitales.

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

03

Hábitos relacionados con la seguridad y comportamientos de riesgo

Más allá de las medidas de seguridad implementadas, los patrones de uso de ordenadores y dispositivos portátiles influyen en los problemas de ciberseguridad.. Los hábitos en línea afectan en gran medida su vulnerabilidad a los ataques. **En esta sección analizamos los principales hábitos de navegación y uso de Internet para tratar de comprender cómo estos influyen en el comportamiento de riesgo**.

Antes de profundizar, resulta de interés conocer cómo se perciben las conductas de riesgo, para tener una visión general del problema y su posible alcance.

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

3.1 Evolución de las conductas de riesgo

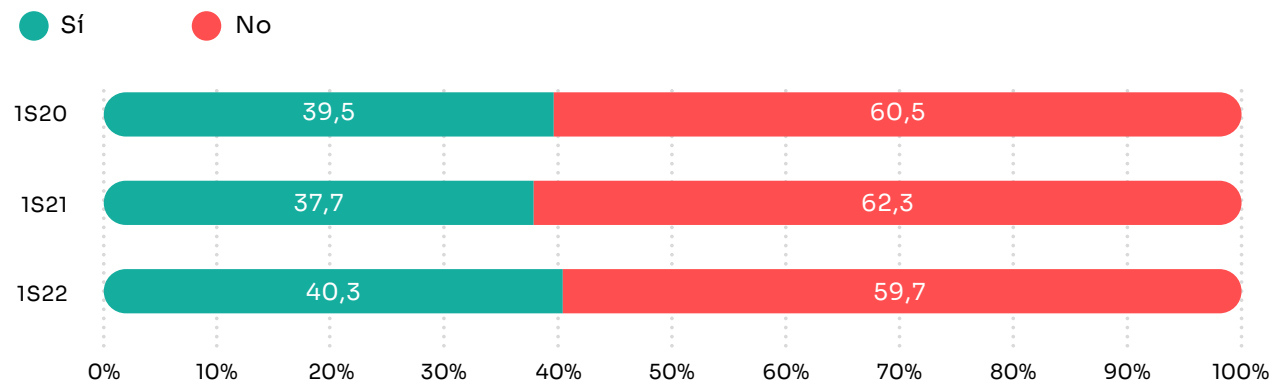
El gráfico 8 refleja la ejecución consciente de conductas de riesgo en la red. Durante el primer semestre de 2022, el 40,3% de la población usuaria de Internet, declaró haber actuado deliberadamente de forma peligrosa.

Entre los hábitos de riesgo se incluyen navegar sin las últimas actualizaciones, deshabilitar antivirus y hacer clic en enlaces que redirigen a sitios web desconocidos. Todos estos se muestran en el gráfico 9.

Sin embargo, un 17% no sabe con seguridad si su equipo está actualizado.

Las actualizaciones de los sistemas operativos y aplicaciones de escritorio son importantes, ya que solucionan o parchean problemas de seguridad críticos que hacen vulnerable el dispositivo y se resuelven errores del *software* que también podrían impedir un ataque.

Gráfico 8 - **Realización consciente de alguna conducta de riesgo (%)**



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

Cuando se trata de comportamientos de riesgo relacionados con la descarga de vídeos, música y otros formatos de archivo, el 33,4% hace descargas desde sitios web con reputaciones cuestionables. Estos pueden contener amenazas para el dispositivo. Entre los principales riesgos se encuentra la posibilidad de infección por *malware*, y el robo de información y datos bancarios, extorsión y daño financiero.

Un 32,8% de las personas encuestadas admitió instalar programas desde fuentes no oficiales, lo cual representa un factor de riesgo adicional. Esta práctica puede abrir las puertas al *software* malicioso en nuestros ordenadores o dispositivos móviles.

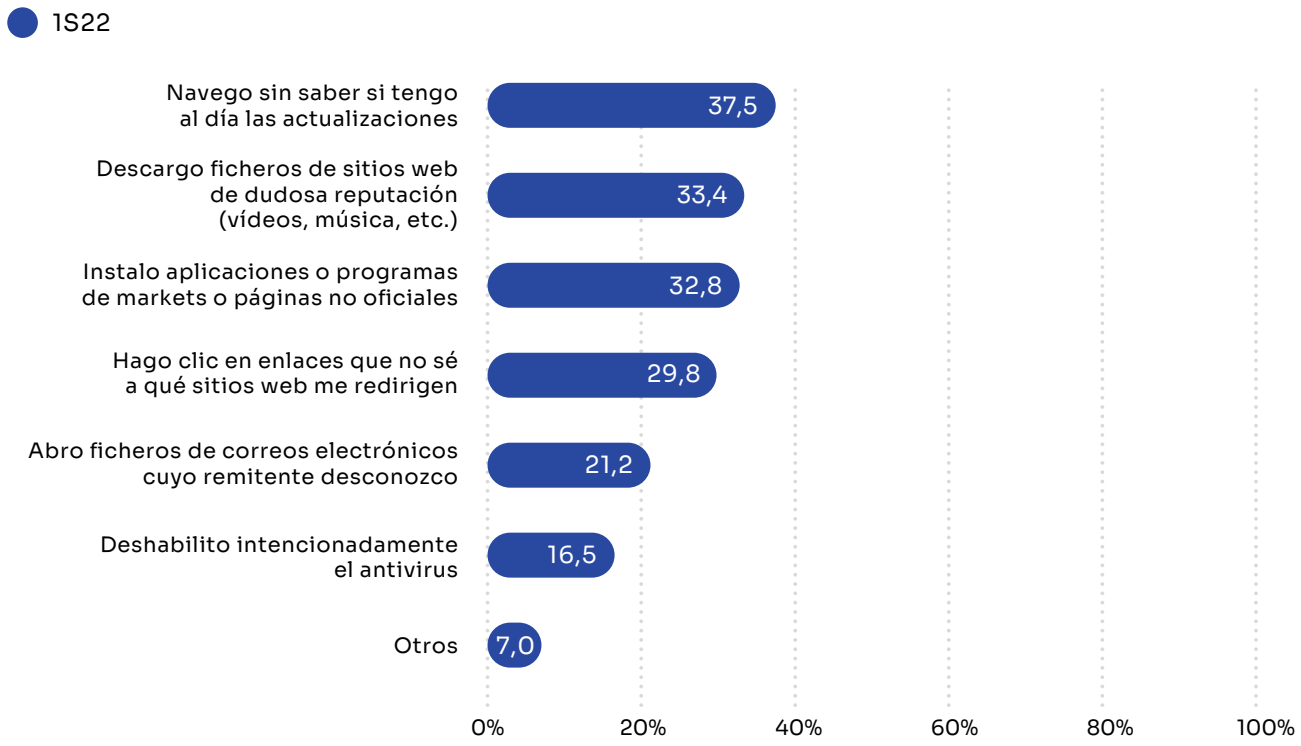
Otra práctica de riesgo es no comprobar la fiabilidad de los enlaces. Alrededor del 29,8% de los encuestados admitió hacer clic en ellos sin saber a qué sitio web conducían, mientras que el 21,2% afirmó abrir archivos de remitentes desconocidos.

Realizar las verificaciones necesarias es una práctica fundamental para evitar el *phishing*, que tiene como objetivo recopilar información personal. Para prevenirlo, es crucial escanear los archivos descargados, lo que reduce el riesgo de infección por *malware*. Sin embargo, sorprendentemente, un 16,5% dijo que desactiva intencionalmente su protección antivirus.

La falta de medidas de seguridad brinda a los atacantes una ventaja clara al preparar campañas de *phishing* debido a la gran cantidad de personas que podrían convertirse en víctimas.

El 40,3% de personas que usan Internet declara realizar alguna conducta de riesgo. De ellos, el 37,5% reconoce no saber con seguridad si su equipo está actualizado

Gráfico 9 - **Realización consciente de alguna conducta de riesgo: tipos (%)**



Base: Total usuarios y usuarias que realizan alguna conducta de riesgo
Fuente: Panel hogares, ONTSI

3.2. Riesgos relacionados con la descarga de contenidos gratuitos

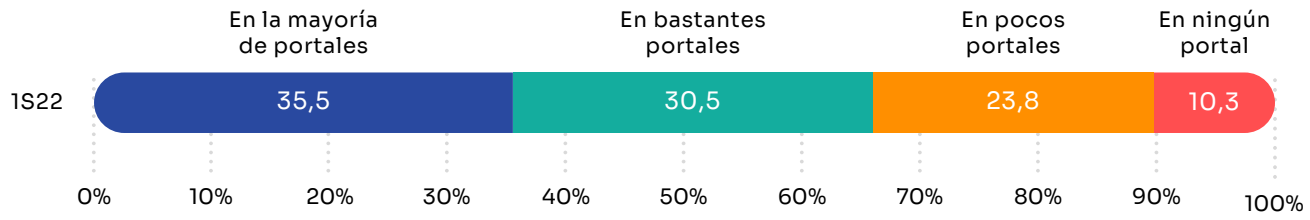
Una de las principales conductas de riesgo está relacionada con el fácil acceso a contenidos gratuitos, cuya descarga puede esconder riesgos de seguridad de diferente magnitud.

El acceso a contenidos digitales gratuitos durante el primer semestre de 2022 es del 61,9% (Gráfico 1), lo que suele suponer un riesgo evidente para la seguridad de sus dispositivos. Por ejemplo, la mayoría de las plataformas de descarga gratuita requieren registro previo para ver o descargar contenido.

Según las declaraciones de los panelistas, el 66% afirmó que necesita registrarse en la mayoría o en bastantes portales para poder acceder a su contenido (Gráfico 10).

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

Gráfico 10 - **Necesidad de registro para el acceso o descarga de contenido gratuito (%)**

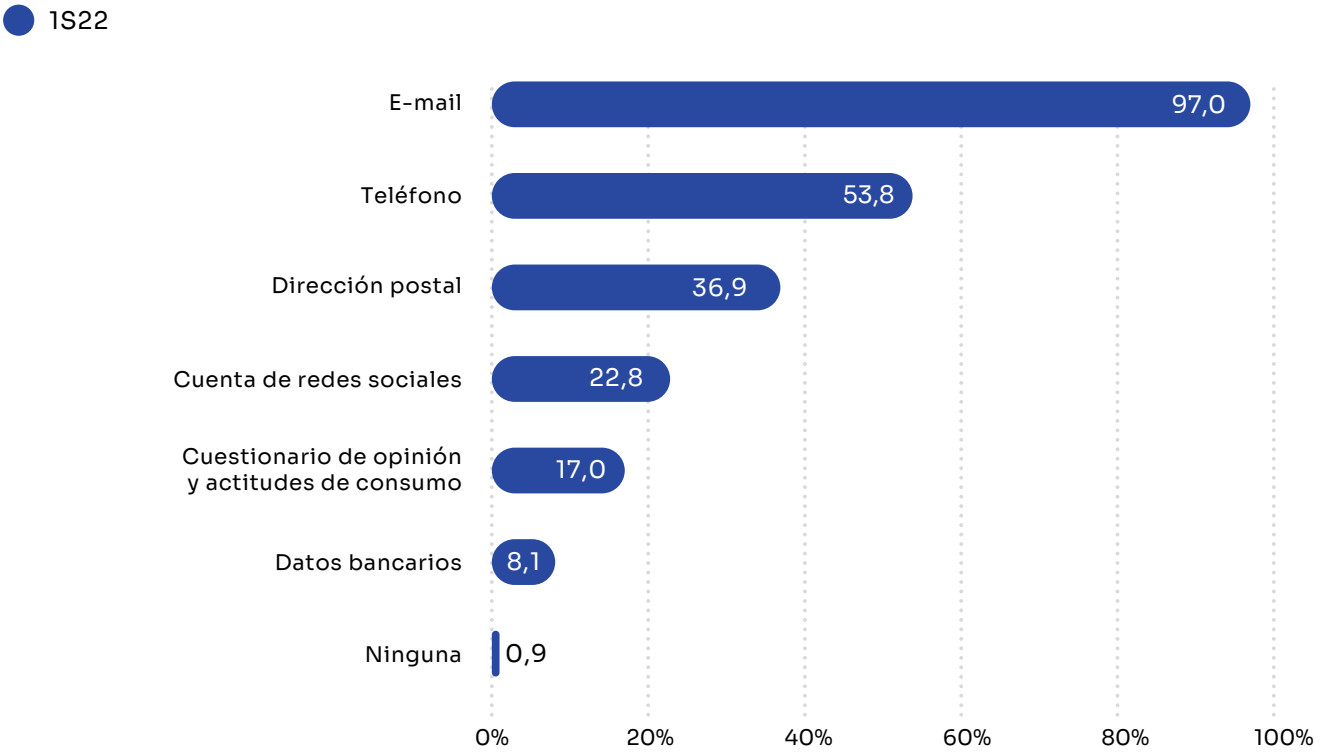


Base: Usuarios y usuarias que acceden o descargan contenido gratuito
Fuente: Panel hogares, ONTSI

En este sentido, el gráfico 11 recoge los principales datos solicitados para el registro en estas páginas. De particular interés son las direcciones de correo electrónico (97%) y los números de teléfono (53,8%).

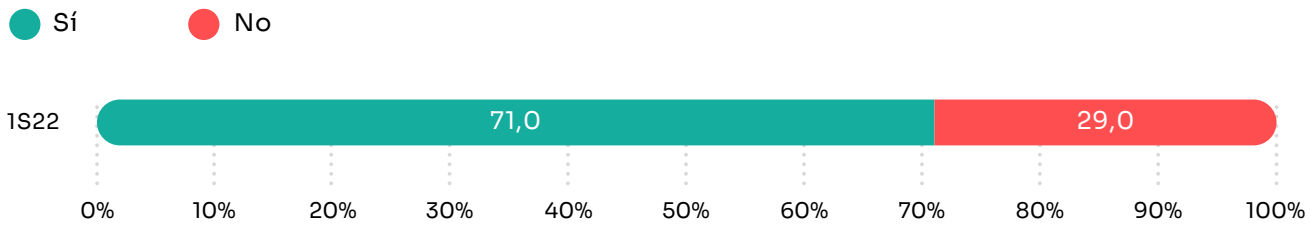
Estas dos piezas de información se usan comúnmente para los tipos de fraude cubiertos en este estudio (Sección 4.2).

Gráfico 11 - **Datos solicitados para completar los registros en portales de descarga de contenido gratuito (%)**



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

Gráfico 12 - **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

Además, tras el acceso a contenidos gratuitos por medio de sistemas de registro e identificación, el 71% de la población usuaria experimentó un incremento de la publicidad no deseada.

Esta forma de proceder, se trata de una costumbre extendida a pesar de que hay una mayor consciencia de los riesgos que implican las descargas y la ejecución de archivos adjuntos de origen y/o contenido desconocido. El deseo por acceder a fuentes de entretenimiento se antepone a la idea de evitar generar agujeros de seguridad.

El 71% de internautas, que acceden o descargan contenido gratuito, notó un aumento de publicidad tras consumir dichos servicios

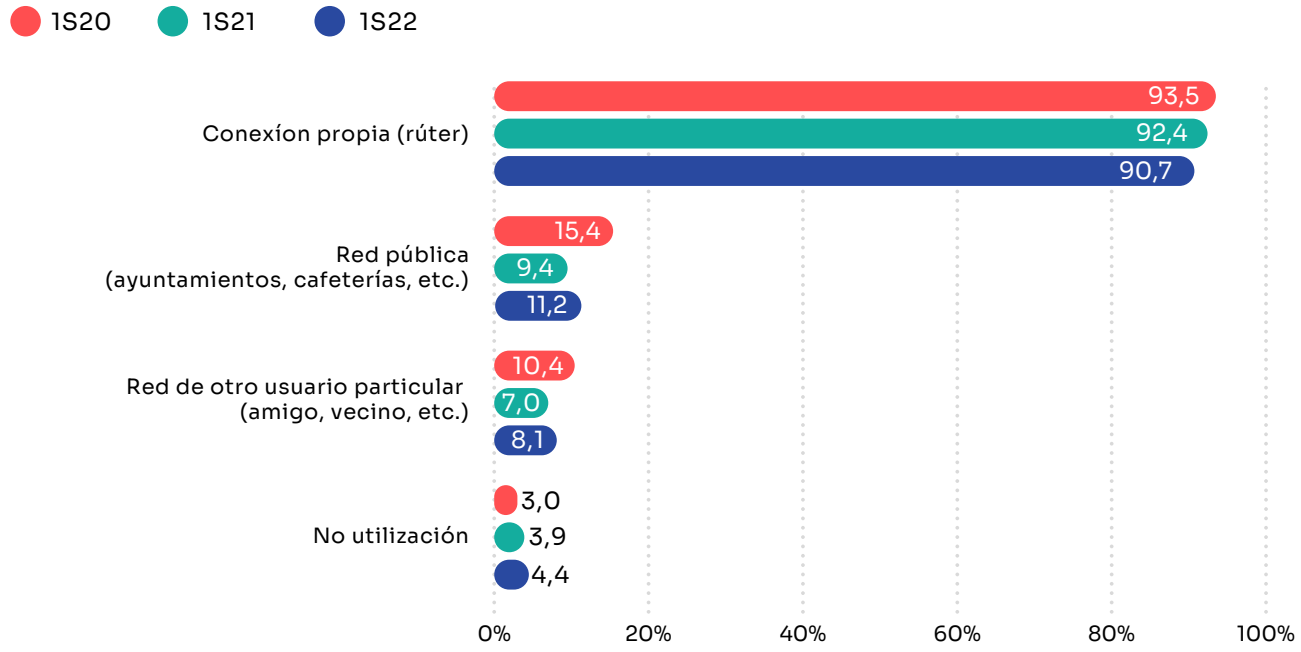
3.3. Acceso a redes wifi desconocidas

El uso de las redes inalámbricas supone riesgos si no se toman medidas de seguridad adecuadas. Usar un punto wifi desconocido o fuera de la conexión de su hogar presenta un riesgo, ya que puede ser un intermediario poco confiable.

El gráfico 13 destaca la evolución en los hábitos de conexión a redes inalámbricas wifi. Aunque es mayoritaria, en el último año la conexión a través del rúter propio ha disminuido 1,7 p.p., con un 90,7% de uso. 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 existe un porcentaje (11,2%) que utiliza redes públicas, ya sean de ayuntamientos, cafeterías, aeropuertos, etcétera. Este tipo de conexiones son más susceptibles (sobre todo si son abiertas) a la captura ilegítima de tráfico de red por parte de atacantes. Pueden suplantar al rúter del lugar y acceder 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 13 - **Punto de acceso a Internet mediante redes inalámbricas wifi**



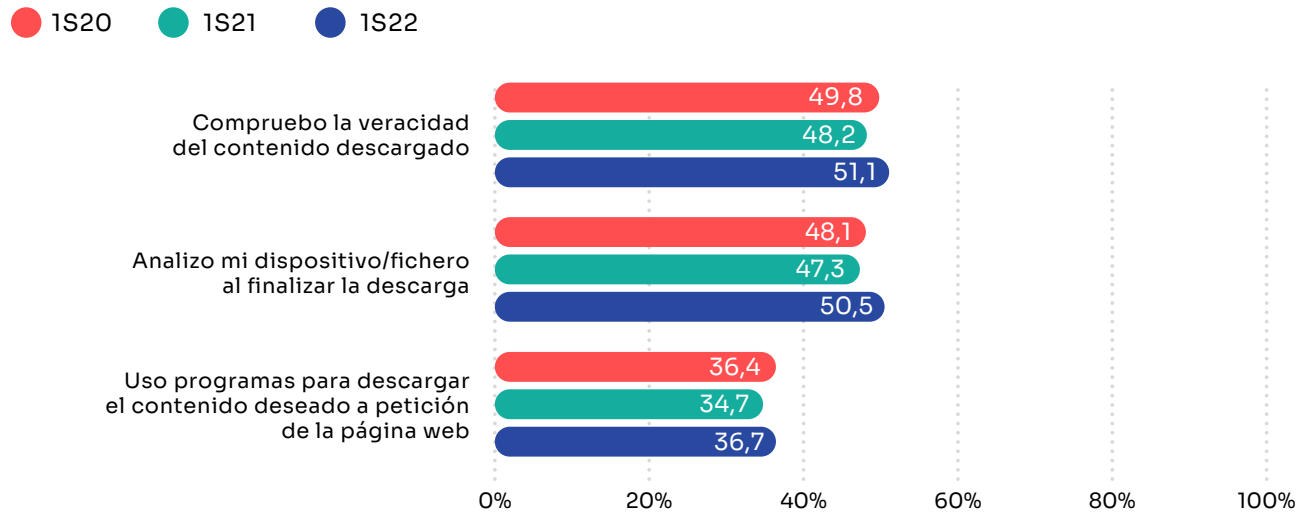
Base: Total usuarios y usuarias
Fuente: Panel hogares, ONTSI

3.4. Descarga e instalación de archivos y programas

Tanto si el contenido es gratuito como si no, la introducción de nuevos elementos en un ordenador puede crear un punto crítico de seguridad del sistema, ya que la ejecución de *software* no autorizado puede comprometer el buen funcionamiento del sistema. Con esto en mente, el gráfico 14 describe lo que sucede cuando se descargan archivos y programas directamente.

No obstante, no solo se realizan prácticas de riesgo cuando se usan servicios digitales, también ponen en práctica acciones prudentes al descargar ficheros. Por ejemplo, comprobar la veracidad del contenido descargado (51,1%), analizar dispositivos después de la descarga (50,5%) y usar programas para descargar contenido web (36,7%) son buenas prácticas aumentado en el primer semestre de 2022.

Gráfico 14 - **Comportamiento relacionado con la descarga directa de archivos, programas, documentos, etc. (%)**

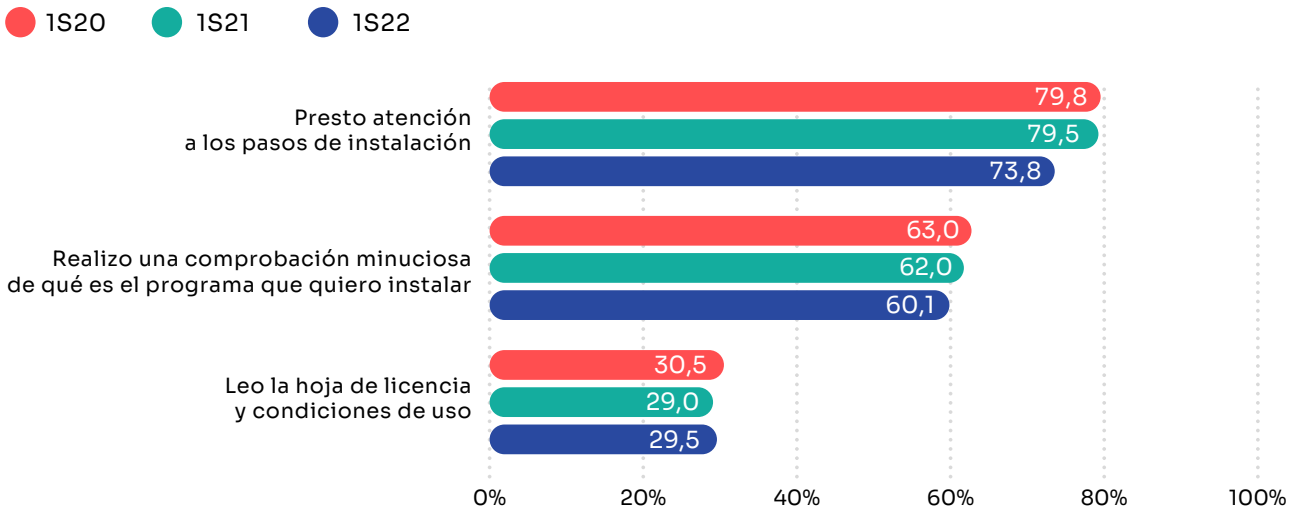


Base: Total usuarios y usuarias
Fuente: Panel hogares, ONTSI

El comportamiento puede variar según el tipo de dispositivo utilizado para realizar la descarga. Debido a las diferencias en las pautas de uso entre ordenadores y dispositivos móviles, el análisis se realiza de manera diferente.

En el caso de los ordenadores del hogar, se preguntó si se habían seguido las instrucciones de instalación, si se habían revisado minuciosamente los programas que estaban instalando y si se habían leído la hoja de licencia y los términos de uso. Solo el último punto registró un ligero aumento de 0,5 p.p. con respecto al año anterior. (Gráfico 15).

Gráfico 15 - **Comportamientos en la instalación de programas en ordenadores en el hogar (%)**



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

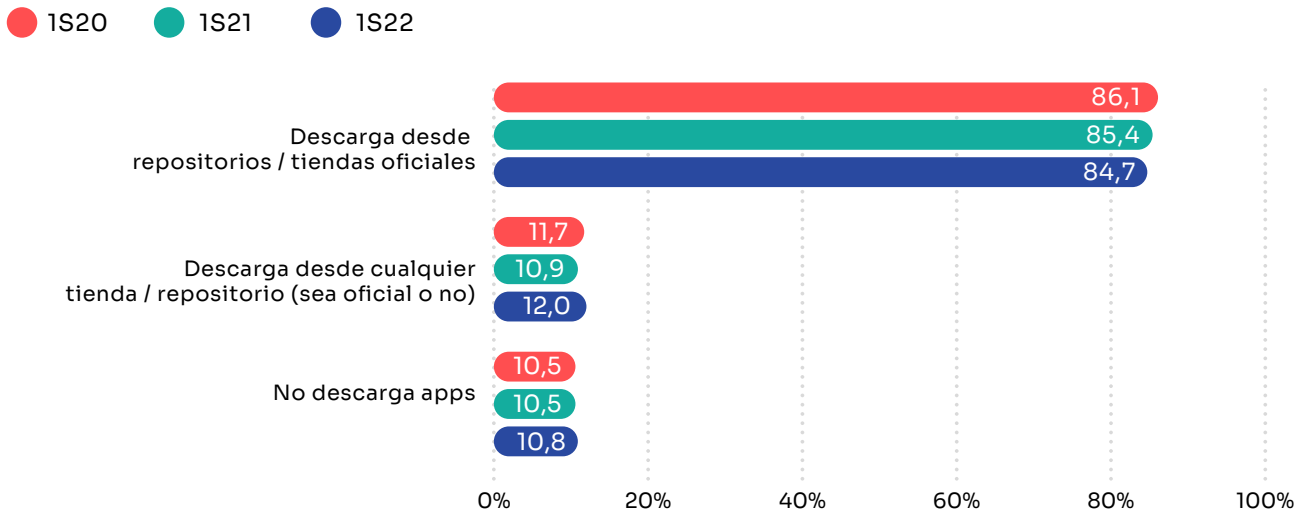
Tras un descenso interanual de 5,7 p.p., el 73,8% de quienes usan ordenador declaró prestar atención a las instrucciones de instalación. Además de identificar posibles errores, esta también es una excelente manera de ver comportamientos anómalos. Por ejemplo, aparición de terminales con código no propio de una aplicación dirigida a la gente.

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. Prestar atención a los pasos de instalación es crucial cuando obtenemos un nuevo *software* que queremos utilizar. Muchas veces, se instalan programas o extensiones de terceras partes no deseados en los equipos aprovechando que no se presta atención mientras se instala el *software* principal y acepta todas las instalaciones sin leerlas.

Son otras las pautas de descarga en dispositivos Android. A modo de ejemplo, la aparición de troyanos y diferentes tipos de *software* maligno en las aplicaciones descargadas desde sitios no oficiales, son un problema para los usuarios.

El gráfico 16 muestra la evolución de ciertos comportamientos en la descarga de apps en el *smartphone* o tableta. Aquí vemos una ligera disminución interanual de 0,7 p.p. en el número de panelistas que prefieren descargar aplicaciones desde repositorios y tiendas oficiales (84,7%). Al mismo tiempo, aumenta levemente el porcentaje de quienes declaran descargar desde cualquier repositorio no oficial (12,0%, un incremento interanual de 1,1 p.p.).

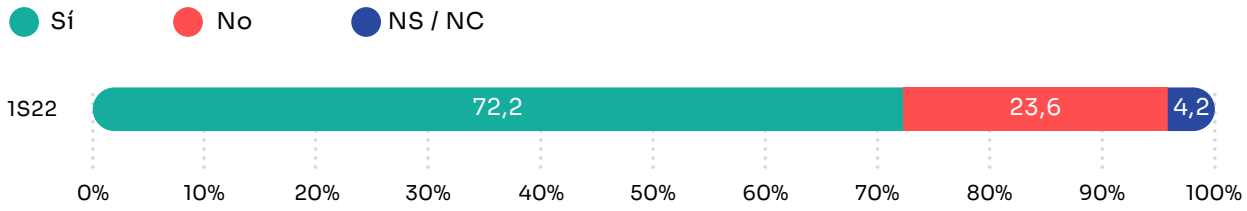
Gráfico 16 - **Comportamientos en la descarga de apps en el *smartphone* o tableta (%)**



Base: Total usuarios y usuarias 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 72,2% de quienes descargan aplicaciones para su dispositivo Android declara poner en práctica esta medida (Gráfico 17). Por otro lado, el 23,6% de estas personas, reconoce no fijarse en este aspecto antes de instalar una aplicación.

Gráfico 17 - **Verificar los comentarios y valoraciones de otros usuarios (%)**



Base: Total usuarios y usuarias que disponen de dispositivo Android y descargan apps
Fuente: Panel hogares, ONTSI

3.5. Comercio *online* y transacciones electrónicas

Una fuente adicional de riesgo radica en las actividades relacionadas con el comercio electrónico y en línea, ya que tales operaciones involucran potenciales pérdidas económicas para las víctimas.

Desde el comienzo de la pandemia, el crecimiento del comercio electrónico ha sido notable. El gráfico 18 muestra las prácticas de comportamiento declaradas para garantizar la seguridad en el uso de servicios de banca en línea o comercio electrónico.

Se puede ver una disminución general en todos los hábitos según declaraciones de quienes usan Internet y utilizan estos servicios respecto al año anterior, con algunas excepciones que muestran solo aumentos menores.

No obstante, los datos declarados respecto a los hábitos de quienes utilizan banca *online* y/o comercio electrónico a la hora de utilizar estos servicios son elevados.

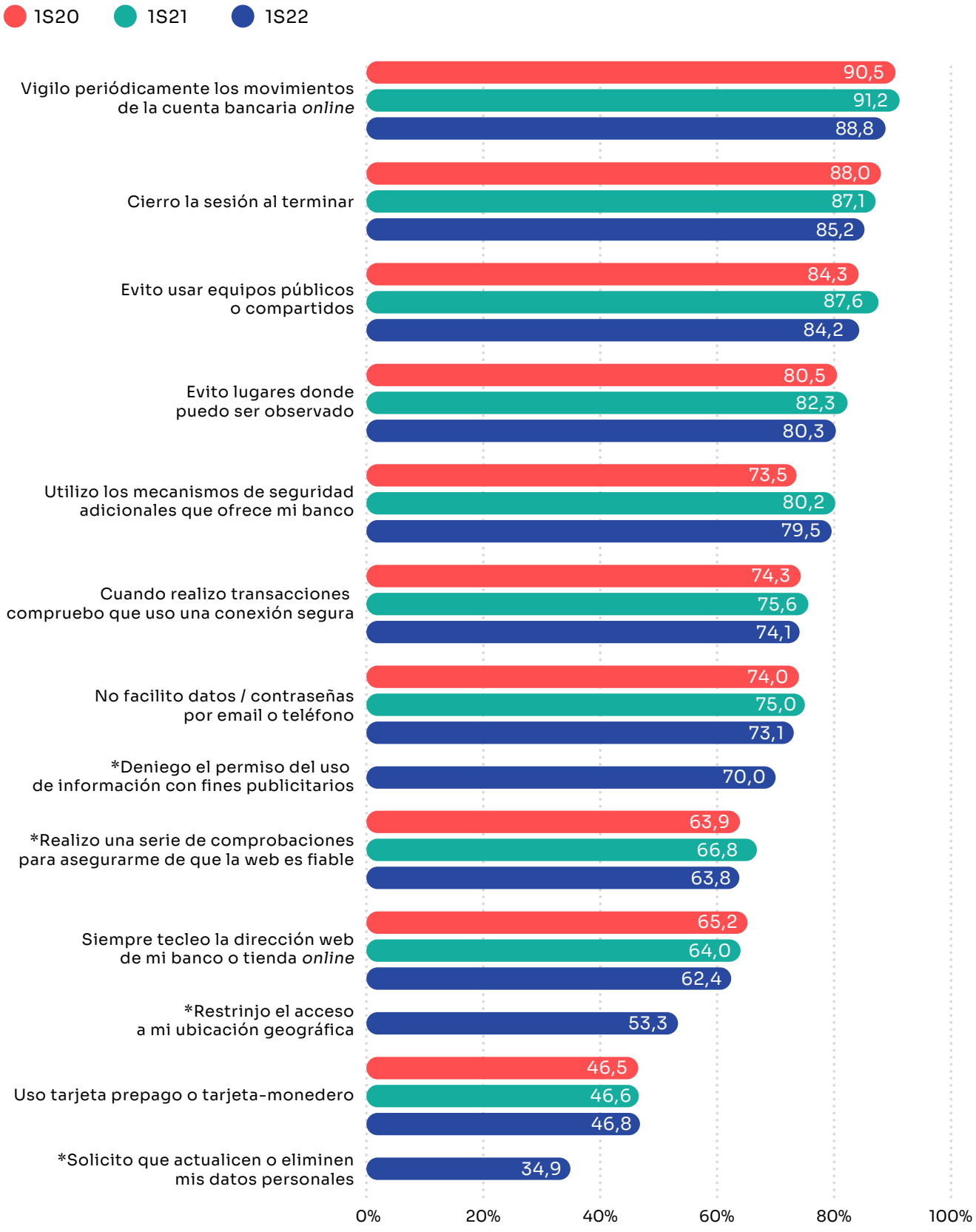
Destacan los comportamientos de revisión periódica de la cuenta bancaria, cierre de sesión al terminar, evitar usar equipos públicos o compartidos y evitar lugares donde el usuario puede ser visto, ya que presentan valores por encima del 80%.

Continuar con estos buenos hábitos es fundamental para evitar problemas de seguridad a la hora de utilizar servicios de banca *online* o comercio electrónico.

Por otro lado, se recogen nuevas métricas este semestre, donde destaca la preocupación por la privacidad, dado que el 70% de la población usuaria de banca *online* y/o comercio electrónico deniega el uso de información con fines publicitarios.

Por otro lado, más de la mitad de estas personas no permite que se acceda a sus datos de geolocalización durante sus sesiones. Además, el 34,9% solicita activamente que sus datos personales sean actualizados o eliminados.

Gráfico 18 - **Hábitos de comportamiento en el uso de servicios de banca *online* o comercio electrónico (%)**



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

3.6. Inicios de sesión y mecanismos de seguridad

Una cuenta de servicios *online* suele ser vulnerada por utilizar credenciales genéricas (comunes o fáciles de adivinar) o por la filtración de estas pese a que fueran seguras.

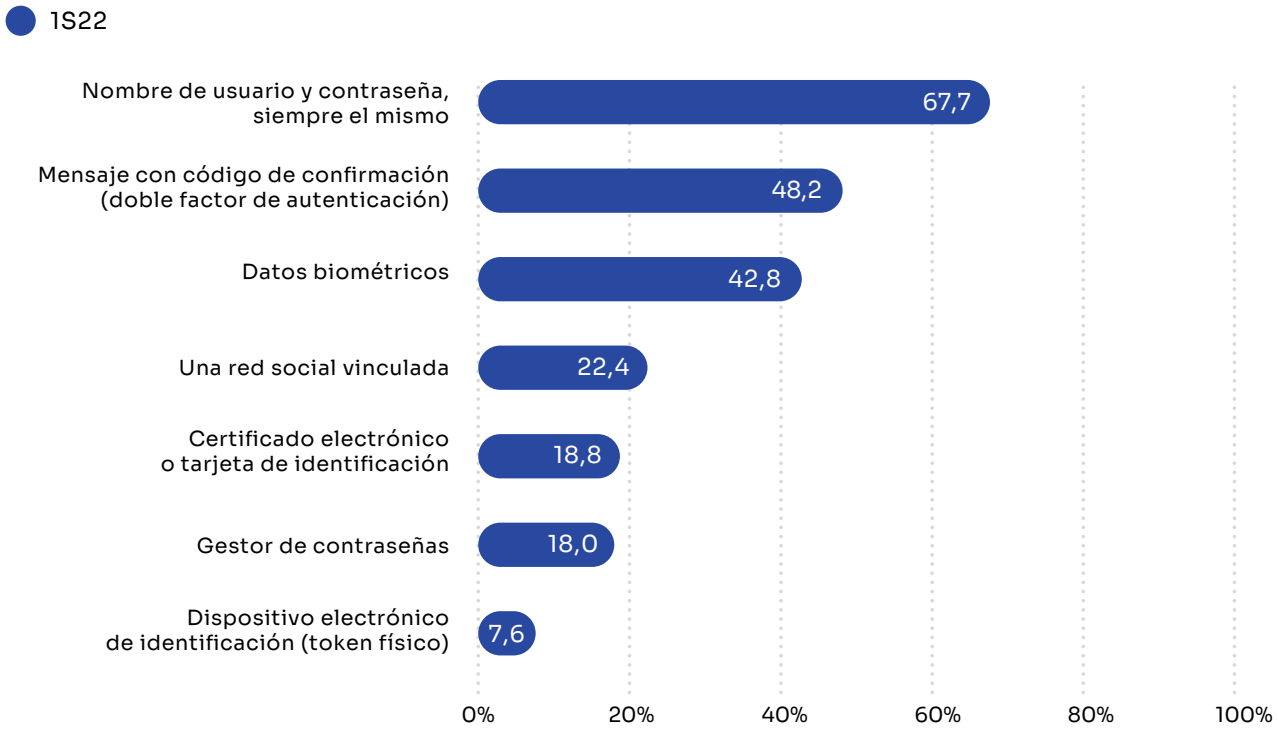
Si se opta por hacer uso de barreras o medidas de seguridad adicionales (como el doble factor de autenticación, por ejemplo), el mero conocimiento de dichas credenciales no es suficiente para suplantar una identidad y acceder a una cuenta. En tal caso sería necesaria una verificación adicional de la identidad, lo cual refuerza la seguridad del acceso.

Pese a la amplia variedad de medidas de inicio de sesión alternativas que hay, la mayoría de la población usuaria (67,7%), continúa utilizando un usuario y una contraseña y además utiliza siempre los mismos datos.

Este método puede mejorar exponencialmente su seguridad si se combina con un gestor de contraseñas que genere claves únicas y seguras, sin embargo, sólo el 18% declara utilizarlo.

Cabe destacar que más del 40% de estas personas declara utilizar mecanismos de doble factor de autenticación o datos biométricos, con un 48,2% y 42,8%, respectivamente.

Gráfico 19 - **Mecanismos de seguridad adicionales empleados en inicios de sesión (%)**



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

Las medidas más utilizadas para asegurar el bienestar *online* de los menores son:

- Hablar con ellos sobre los riesgos *online* (**43,8%**)
- Limitar el tiempo conectado (**40,1%**)
- Activar controles parentales (**36,8%**)

3.7. Protección de menores *online*

Es importante poder supervisar el bienestar *online* del menor.

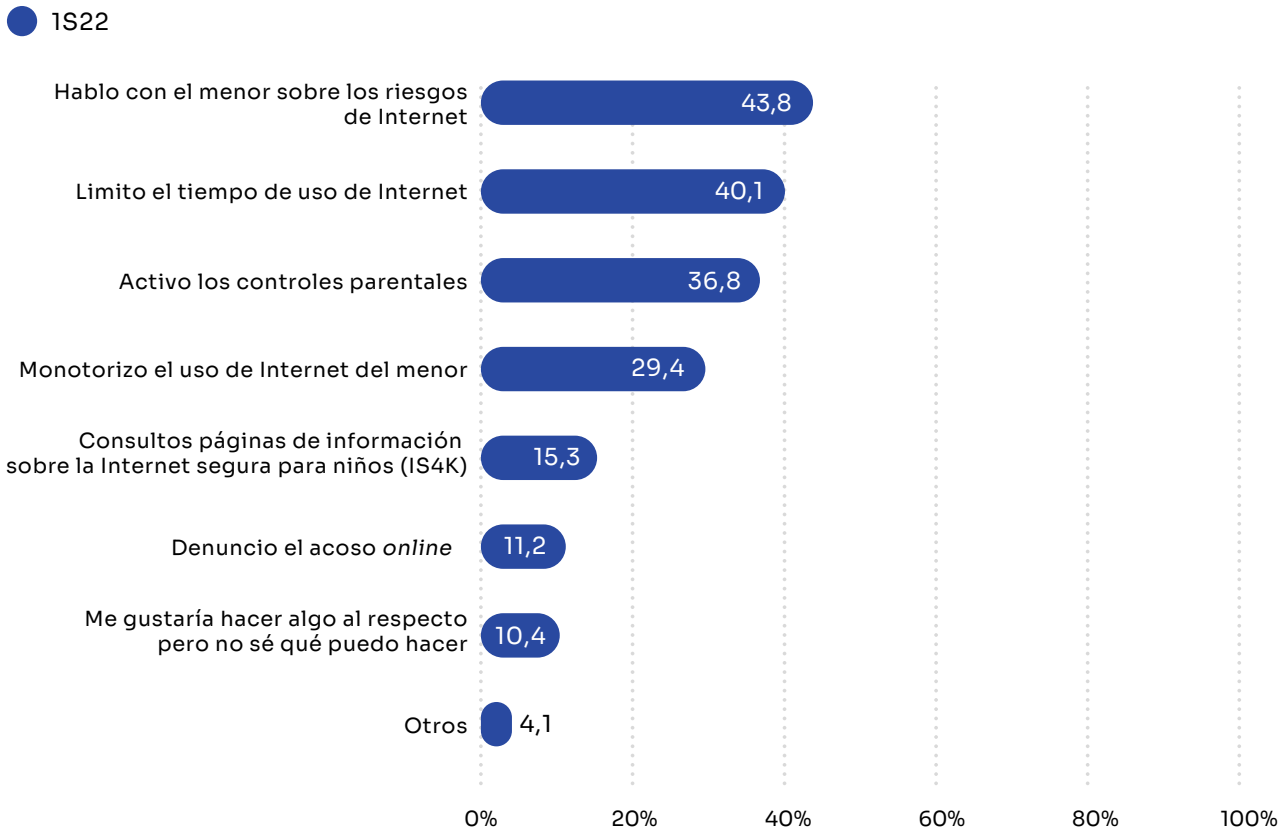
Las medidas más utilizadas para asegurar este bienestar son hablar con ellos sobre los riesgos *online* (43,8%), limitar el tiempo conectado (40,1%) y activar controles parentales (36,8%).

Una de las más olvidadas, pero potencialmente más eficientes es denunciar el acoso en línea, sin embargo, sólo un 11,2% de personas usuarias con menores a su cargo lo denuncian.

Otra opción que permite a los mayores formarse y conocer el entorno y los riesgos que conlleva el hecho de que el menor navegue y se relacione en línea, es consultar páginas de información sobre Internet segura, como is4k[6].

Por desgracia, consultar páginas de información sobre Internet segura para los más pequeños y pequeñas es la opción más desconocida, aunque no se aleja mucho de las denuncias de acoso *online*, 3,9 p.p. menos, supone un 15,3%.

Gráfico 20 - **Medidas para proteger a los menores en entornos en línea (%)**



Base: Usuarios y usuarias que tienen menores a su cargo
Fuente: Panel hogares, ONTSI

[6] https://www.is4k.es/

3.8. Contactos desconocidos a través de Internet

Al igual que con menores, la población adulta también debe protegerse. Las interacciones con perfiles *online* no siempre son lo que creemos, en muchas ocasiones el fraude y los robos de identidad ocurren y no nos damos cuenta hasta que es tarde.

Para discutir este tema, primero es necesario conocer de dónde provienen la mayoría de los contactos iniciales con desconocidos que se hacen por Internet.

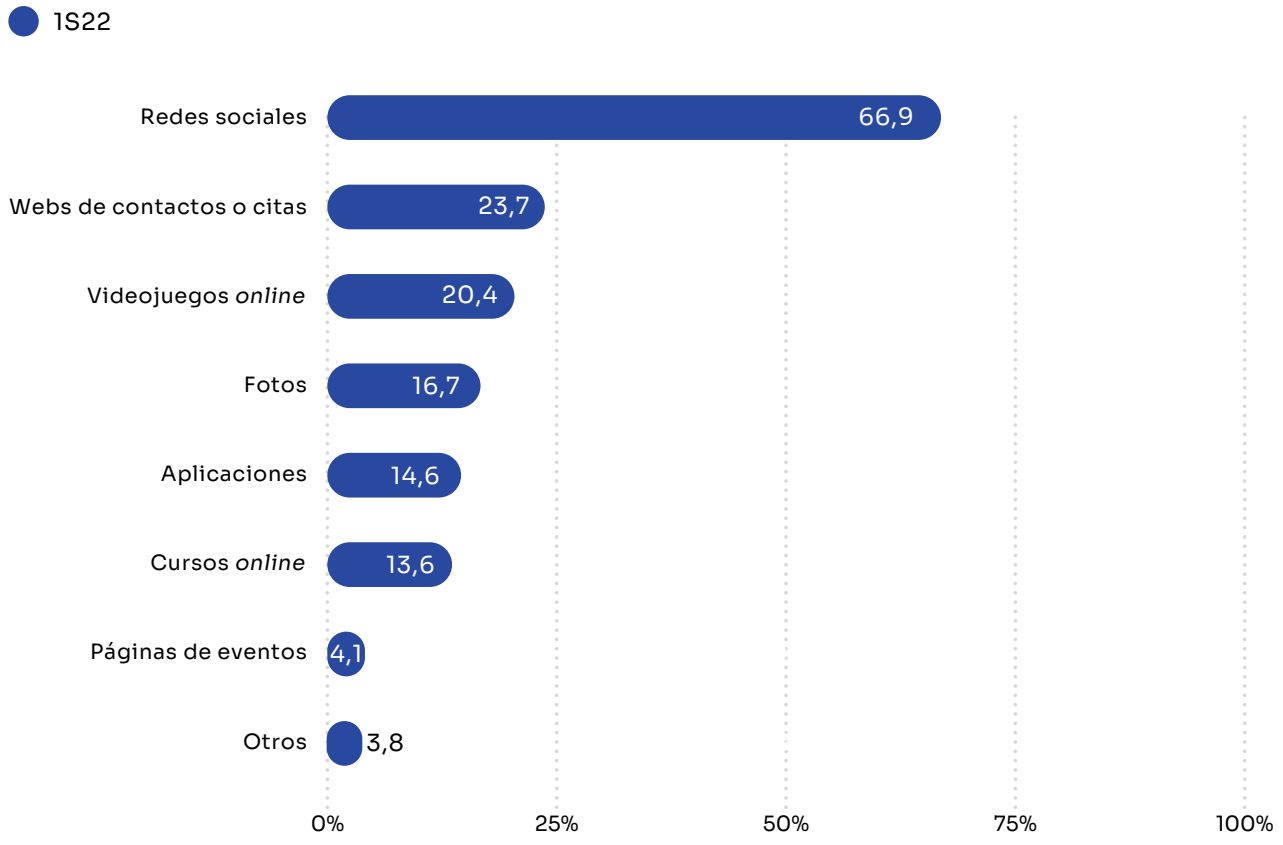
Las redes sociales continúan siendo el motor de la interacción personal en el ámbito digital.

El 66,9% de panelistas declara conocer gente a través de redes sociales.

En segundo puesto quedan las webs de contactos o citas con un 23,7% de personas entrevistadas que declaran interactuar y conocer a desconocidos.

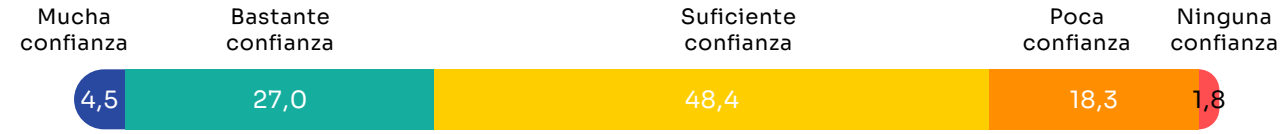
Seguido de cerca, y en tercer lugar , se sitúan los videojuegos en línea (con un 20,4%), que fomentan la complicidad y el trabajo en equipo con personas desconocidas. De esta forma, permiten crear contactos y potenciales relaciones sociales.

Gráfico 21 - **Origen de los contactos desconocidos a través de Internet (%)**



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

Gráfico 22 - **Grado de confianza en contactos desconocidos a través de Internet (%). 1S 2022**



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

Los orígenes de menos contactos *online* son las páginas de eventos y los cursos en línea, con un 4,1% y un 13,6% de panelistas respectivamente.

Una vez conocemos los orígenes de los contactos *online* es pertinente informar sobre el nivel de confianza que generan en los panelistas.

Las cifras de poca o ninguna confianza son bajas, suman 20,1% (1,8% de ninguna confianza y el 18,3% de poca confianza).

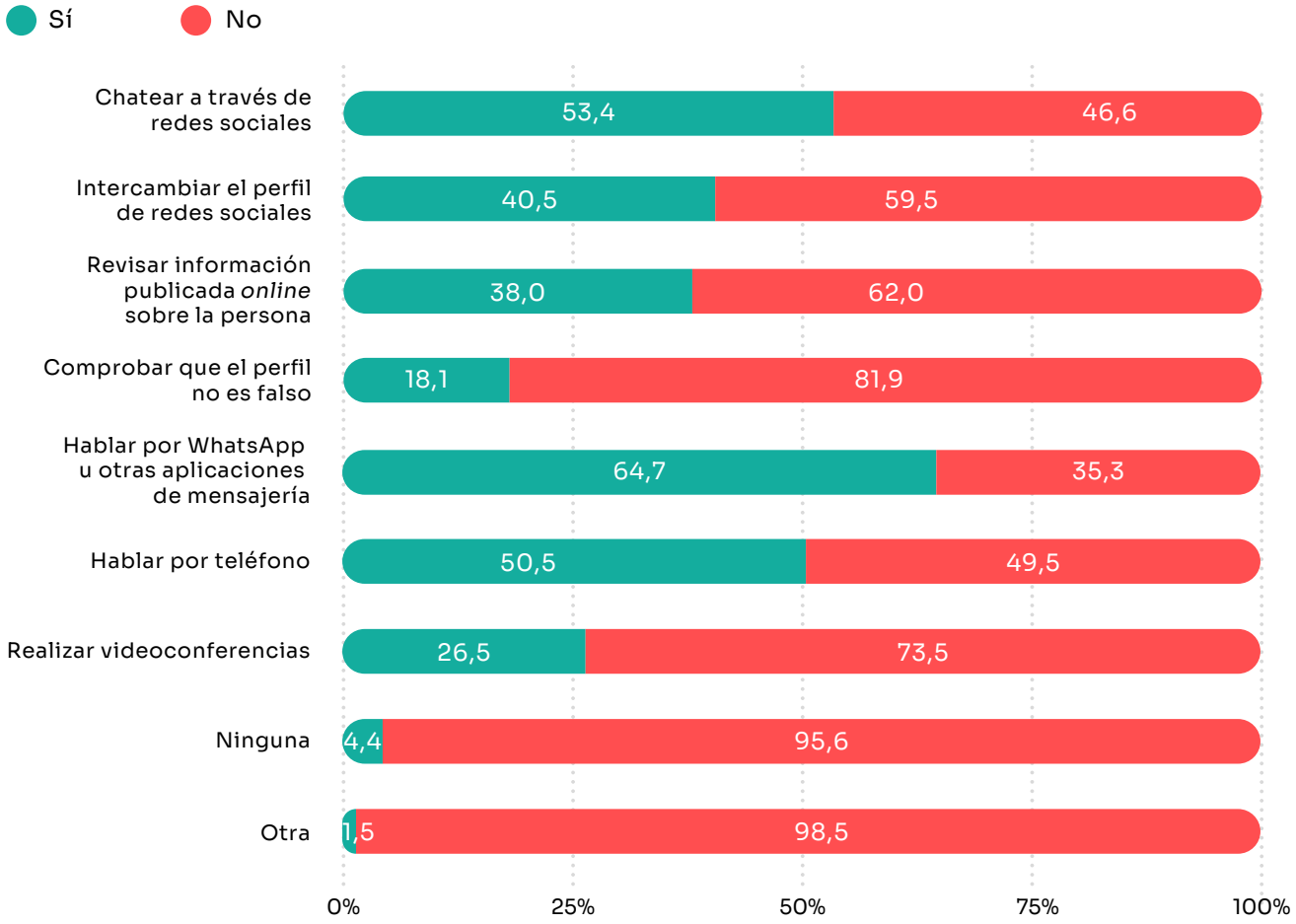
Esto implica que el 79,9% de las personas entrevistadas restantes confían en perfiles desconocidos de Internet. Este casi 80% se desglosa en una mayoría del 48,4% que declara tener suficiente confianza, un 27% que declara tener bastante confianza y, por último, un 4,5% que asegura sentir mucha confianza hacia estos nuevos contactos en línea.

Antes de conocer físicamente a nuestros contactos *online* es conveniente llevar a cabo ciertas comprobaciones. Esta prevención permite reducir el riesgo de exposición a fraudes, robos de identidad, y ciberamenazas relacionadas.

Entre las principales verificaciones de seguridad llevadas a cabo por las personas encuestadas en estos casos destacan hablar por WhatsApp u otras aplicaciones de mensajería instantánea (64,7%), junto a chatear a través de redes sociales (53,4%). También es habitual llevar a cabo precauciones como hablar por teléfono, (50,5%) e intercambiar perfiles de redes sociales (40,5%).

La medida de seguridad menos extendida es comprobar que el perfil no es falso con alguna herramienta o manualmente (18,1%). A este respecto, algunas herramientas de utilidad son *twitteraudit* o *BotCheck*. También es importante saber si la persona que vemos en el perfil es real o ha sido generada por inteligencias artificiales como la de '*This person does not exist*'.

Gráfico 23- **Medidas preventivas antes de conocer a contactos virtuales (%)**



Base: Total usuarios y usuarias que han conocido físicamente a sus contactos virtuales
Fuente: Panel hogares, ONTSI

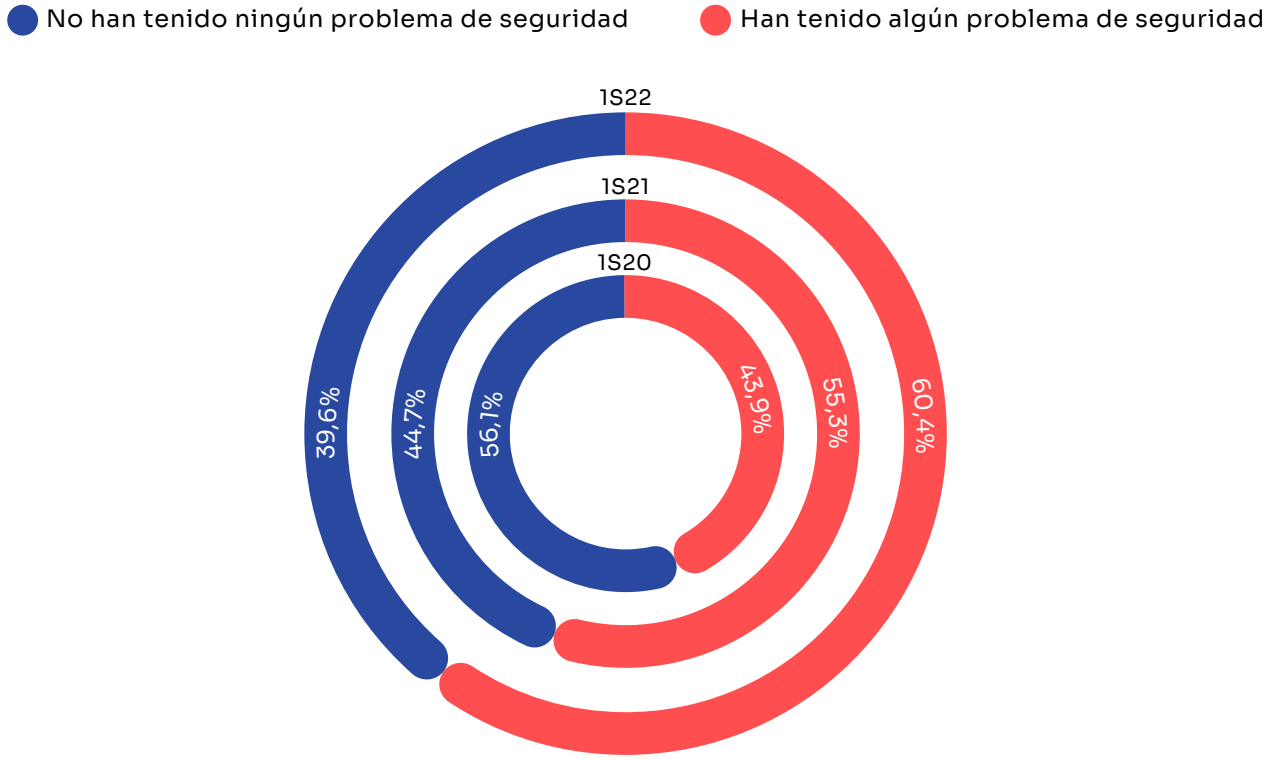
04

Incidentes de seguridad

Unos hábitos *online* inadecuados, o el desconocimiento, pueden traducirse en incidentes de seguridad. **En esta sección se abordan tanto los incidentes declarados, como los contrastados mediante los datos obtenidos por el *software* Pinkerton**.

Los incidentes de seguridad declarados suben del 55,3% al 60,5% en el último año

Gráfico 24 - **Incidencias de seguridad en el dispositivo con el que se accede habitualmente a Internet (%)**



Base: Total usuarios y usuarias (PC y Android)
Fuente: Panel hogares, ONTSI

4.1. Visión general de los incidentes

El 60,5% de la población usuaria afirma haber sufrido un incidente de seguridad durante el primer semestre del año 2022, un aumento de 5,2 p.p. respecto al año 2021 (Gráfico 24).

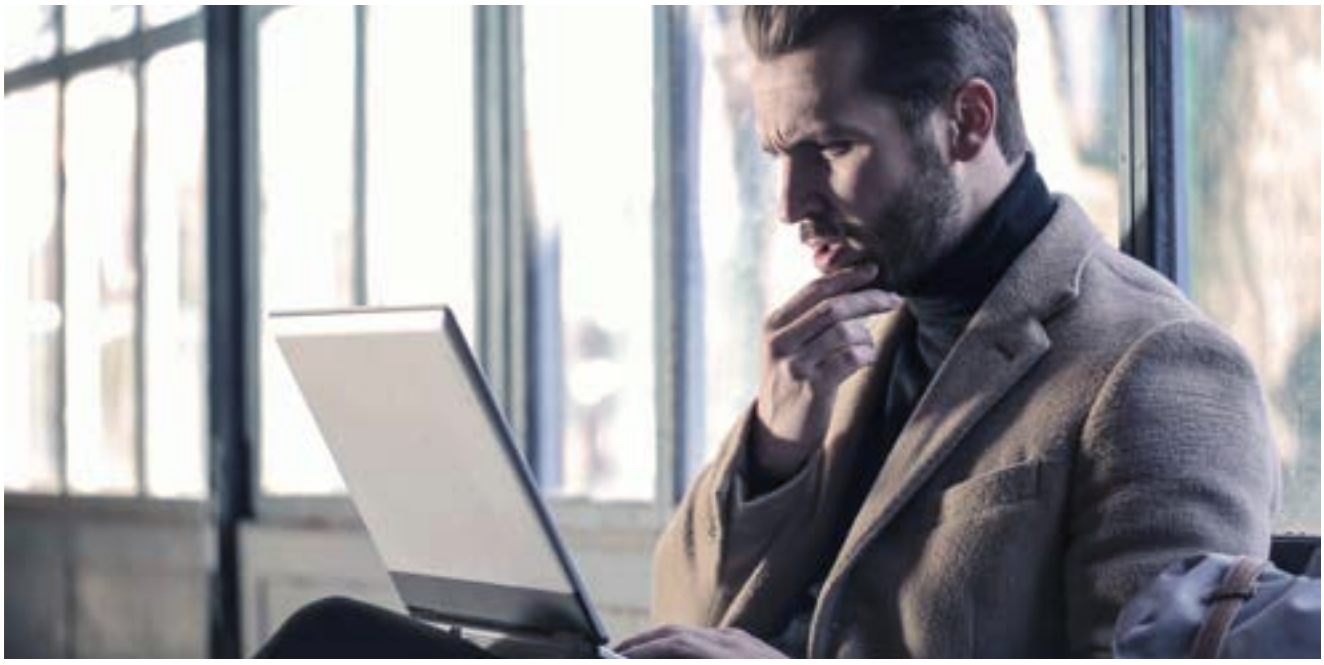
Entre las personas que han experimentado incidencias de seguridad, el problema más habitual es la recepción de correos no deseados (spam), alcanzando el 80,4%. No obstante, se percibe un descenso de 4,5 p.p. respecto al año anterior. Por otro lado, el ataque de virus o códigos maliciosos, es padecido por un 14,6% de los que manifiestan haber sufrido percances. Seguido de un 12,5%, que reconoce haberse quedado sin acceso a servicios debido a ciberataques.

A este respecto, los ataques de denegación de servicio, según declara Cloudflare[7 y 8], han aumentado progresivamente en el segundo semestre de 2022, sobre todo de manera internacional.

Otros problemas de seguridad identificados por las víctimas son la pérdida o borrado de datos (12%) y la difusión de contenido sin consentimiento (8,4%).

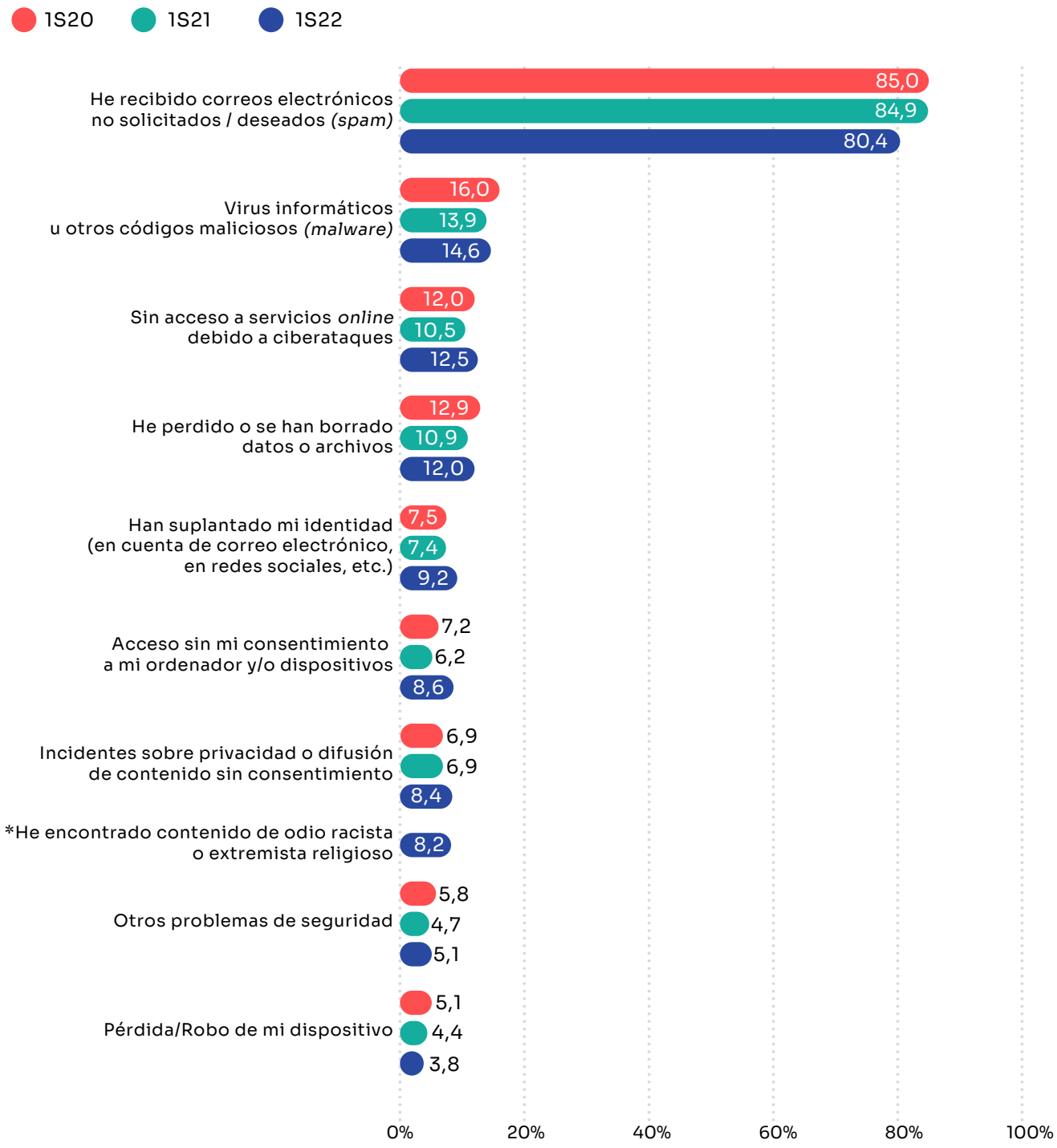
Una de las nuevas métricas estudiadas en este semestre, es encontrar contenido que promueva el odio o extremismo religioso, que se sitúa en el 8,2% de los panelistas.

Por otro lado, el problema de la usurpación de identidad en cuentas de correo electrónico y redes sociales ha aumentado ligeramente. El 9,2% 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.



[7] https://blog.cloudflare.com/es-es/ddos-attack-trends-for-2022-q1-es-es/
[8] https://blog.cloudflare.com/es-es/ddos-attack-trends-for-2022-q2-es-es/

Gráfico 25 - **Problemas de seguridad identificados (%)**



*** Nuevas categorías**
Base: Total usuarios y usuarias que han sufrido alguna incidencia de seguridad.
Fuente: Panel hogares, ONTSI

4.2. Aumento de las situaciones de fraude *online*

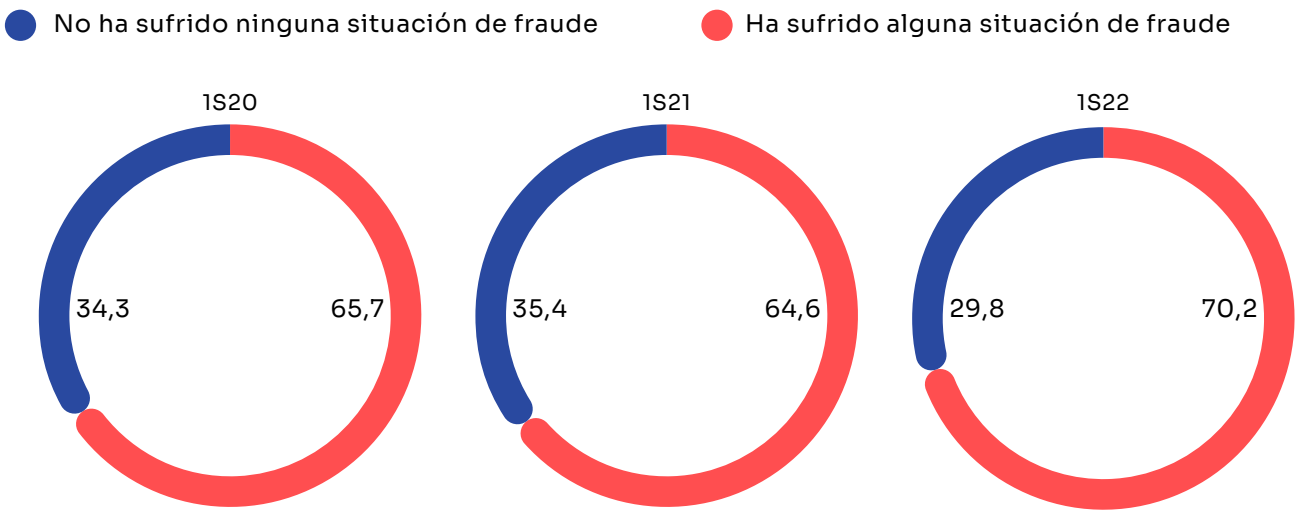
El fraude[9] tiene múltiples facetas y métodos de ejecución, pero su objetivo final sigue siendo financiero. En la primera mitad de 2022, el 70,2% de la población usuaria afirma haber experimentado alguna situación de fraude. Dato que ha crecido 5,6 puntos porcentuales más sobre el mismo semestre del año anterior.

El fraude tiene una motivación económica para el ciberdelincuente y es más efectivo cuanta más información conoce sobre la víctima, pero también pesa la confianza de las víctimas y su predisposición a creer a terceros.

Como se ha podido ver anteriormente, existen prácticas que pueden contribuir positivamente al engaño. Por ejemplo, la predisposición a confiar en desconocidos a través de Internet (Gráfico 22).

Entre los signos o situaciones de fraude detectados (Gráfico 27), se destacan dos tendencias. Por un lado, ha disminuido el número de personas que recibieron productos de páginas potencialmente falsas, pasando del 40,6% al 39,2% en comparación con el año anterior. Por otro lado, ha habido una subida de la solicitud de claves de usuario o información personal, que ha aumentado un 3,4% en comparación con el año pasado, alcanzando el 24,4% de los casos.

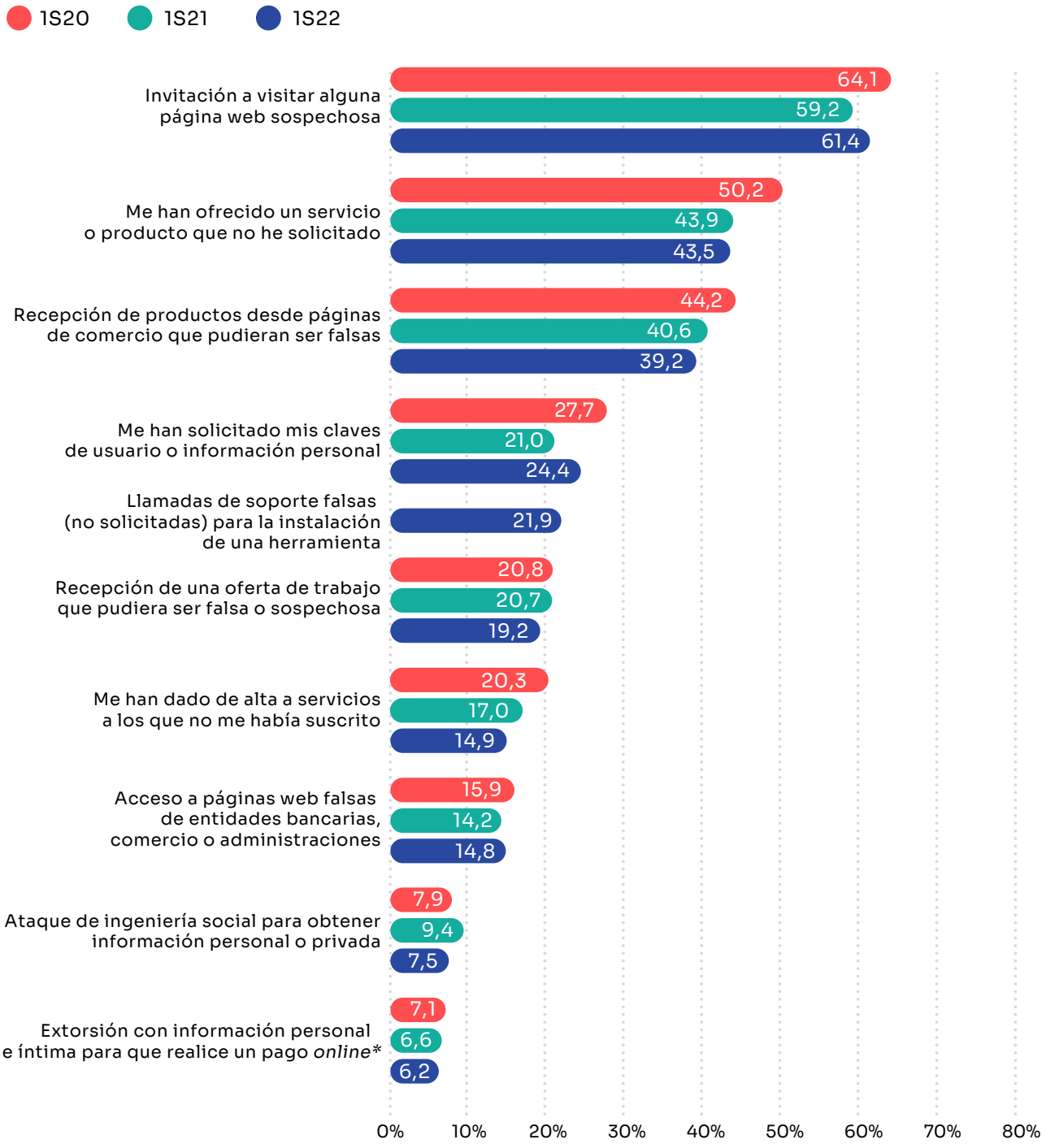
Gráfico 26 - **Ocurrencia de alguna situación de fraude (%)**



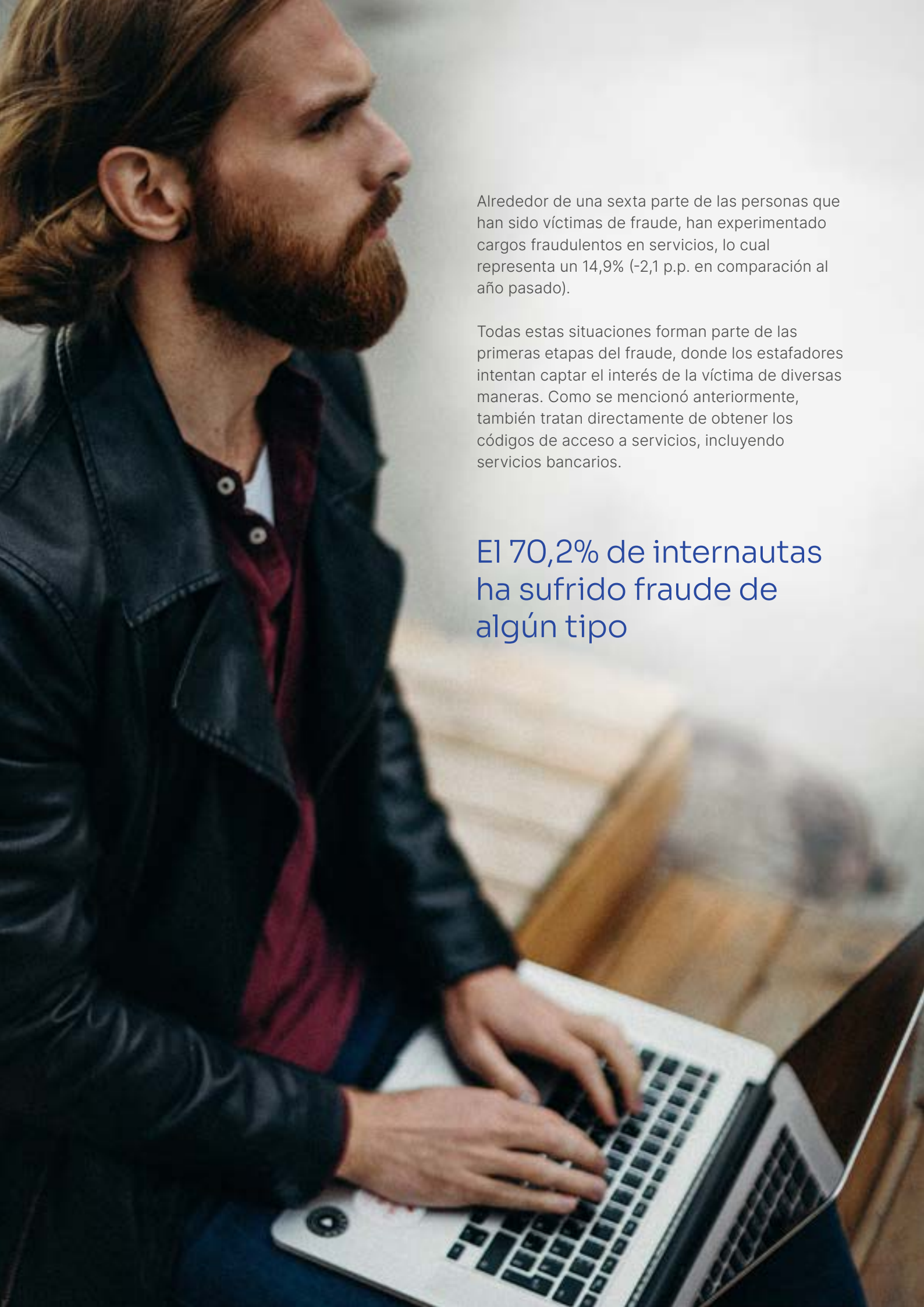
Base: Total usuarios y usuarias
Fuente: Panel hogares, ONTSI

[9] https://www.incibe.es/protege-tu-empresa/blog/fraudes-online-aprende-identificarlos

Gráfico 27 - **Situaciones de fraude ocurridas (%)**



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



Alrededor de una sexta parte de las personas que han sido víctimas de fraude, han experimentado cargos fraudulentos en servicios, lo cual representa un 14,9% (-2,1 p.p. en comparación al año pasado).

Todas estas situaciones forman parte de las primeras etapas del fraude, donde los estafadores intentan captar el interés de la víctima de diversas maneras. Como se mencionó anteriormente, también tratan directamente de obtener los códigos de acceso a servicios, incluyendo servicios bancarios.

El 70,2% de internautas ha sufrido fraude de algún tipo

4.3. Intrusiones a través de wifi

Los riesgos que plantea la conexión a través de redes wifi abiertas o la aplicación laxa de buenas políticas de contraseñas, a menudo, se ven reflejados en incidentes por intrusiones en redes wifi (la conexión a la red sin consentimiento por parte de terceros).

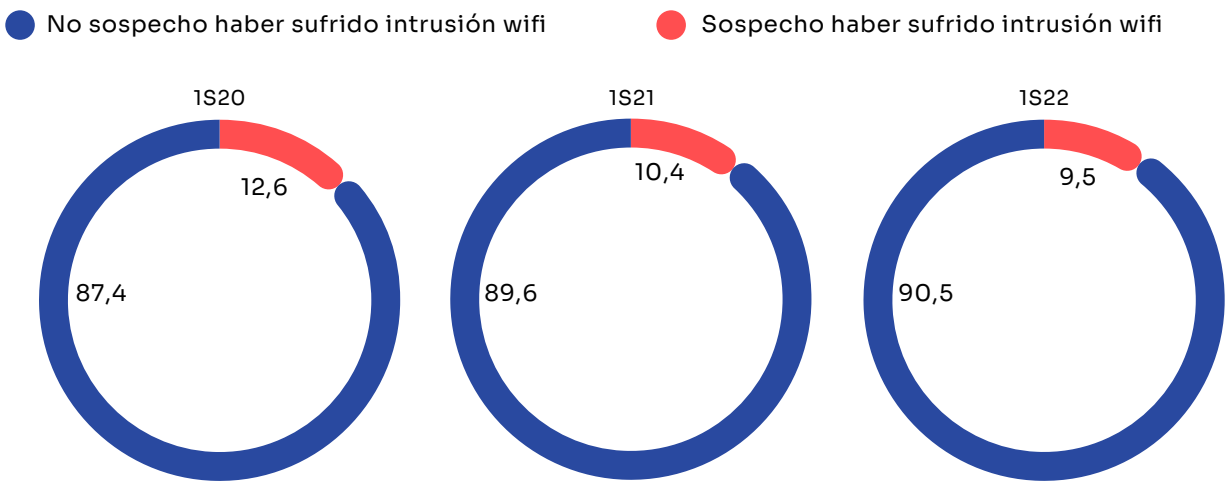
De hecho, conforme a las declaraciones recogidas de quienes disponen de red inalámbrica propia, el 9,5% sospecha haber sufrido alguna intrusión en su red wifi durante el primer semestre de 2022 (Gráfico 28).

Es posible detectar estos incidentes de diferentes maneras como, por ejemplo, lentitud en la red a ciertas horas del día o tener dispositivos desconocidos conectados en el panel de administración del rúter. Estos indicios son señalados por las personas que afirman haber sufrido una intrusión wifi (Gráfico 29).

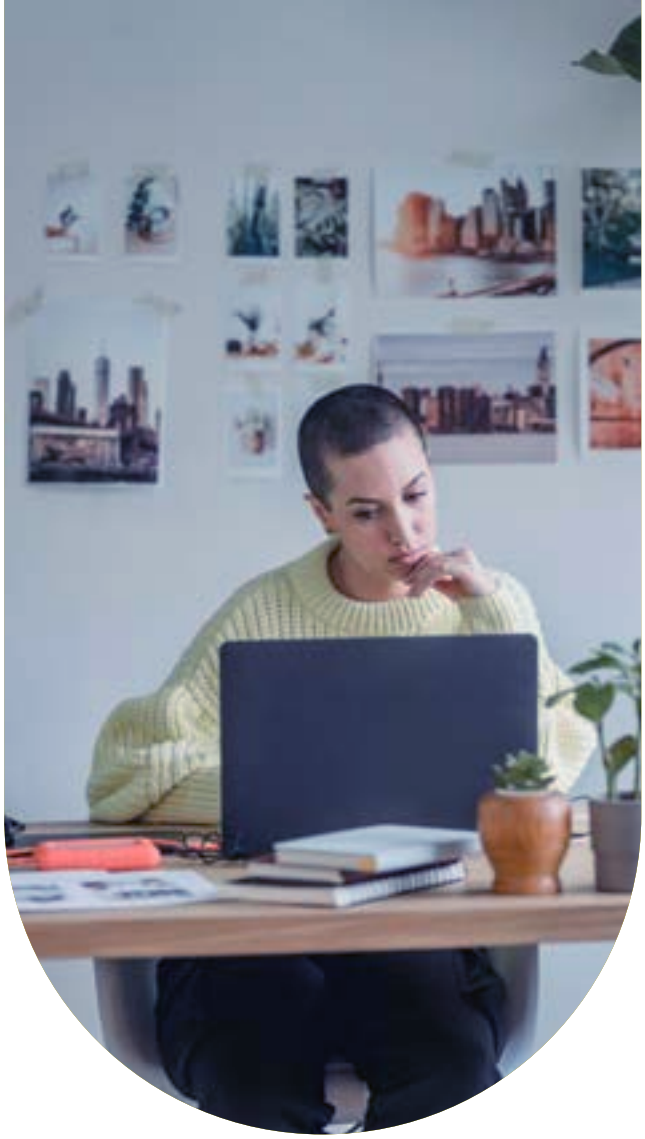
Cuando un ciberatacante está consumiendo ancho de banda, es posible percibir que la red se ralentiza. Este indicio alertó a un 64% de los que creen que su red wifi puede haberse visto comprometida. Se trata de una evidencia plausible que, sin embargo, puede no siempre responder a esta causa. La configuración de red incorrecta y el uso excesivo de dispositivos domésticos conectados también pueden afectar el rendimiento de la red.

Para detectar posibles conexiones no autorizadas en la red, una buena opción es acceder a la configuración del enrutador doméstico. Desde allí, es posible ver el nombre o la dirección física de los dispositivos que están actualmente conectados, así como el historial de conexiones. Sorprendentemente, un 19,7% de las personas que podrían convertirse en víctimas de un fraude creyeron haber identificado un punto de acceso comprometido wifi al verificar la conexión de un dispositivo desconocido. Esta es una forma efectiva de conocer qué aparatos están conectados, así como de expulsar aquellos desconocidos.

Gráfico 28 - **Sospecha de haber sufrido una intrusión wifi (%)**

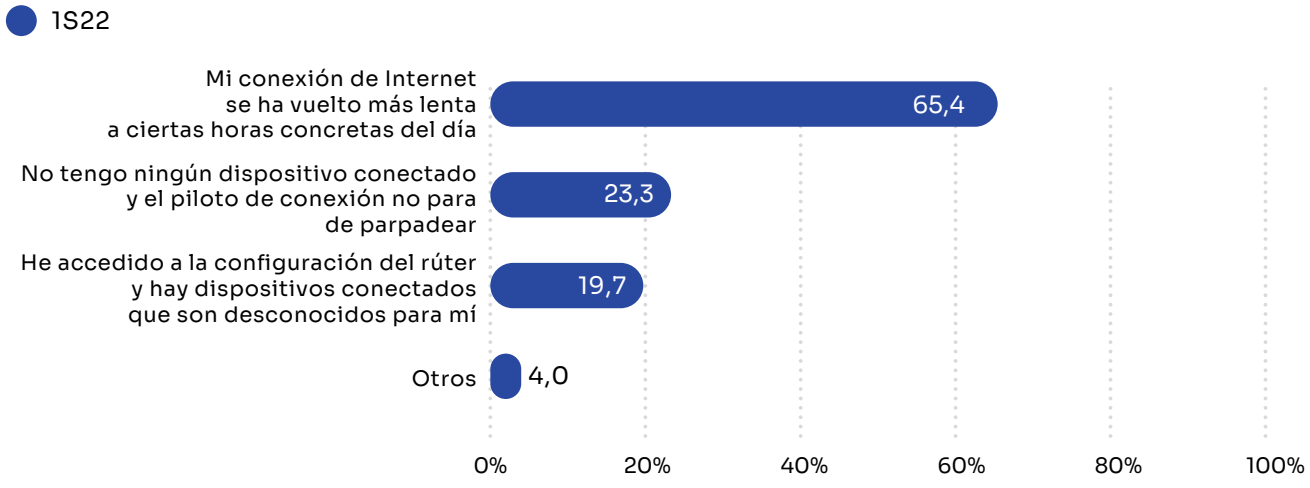


Base: Total usuarios y usuarias con conexión Wifi propia
Fuente: Panel hogares, ONTSI



Otro motivo de sospecha relativo a incidentes de ciberseguridad, ocurre cuando el piloto de la conexión parpadea y no hay ningún dispositivo conectado. Un 23% de los panelistas declara haber experimentado este percance. Sin embargo, hay que tener en cuenta que en muchas ocasiones, cuando hay nuevos dispositivos en casa, es fácil pasar por alto las necesidades de conexión de estos objetos, como los dispositivos del Internet de las Cosas (IoT). Esto puede hacer que se detecten como intrusiones. Por eso, es importante ser consciente de las necesidades de los dispositivos en casa, saber cómo protegerlos y aprovechar sus ventajas de manera segura.

Gráfico 29 - **Motivos de haber sufrido una intrusión wifi (%)**



Base: Total usuarios y que declaran haber sufrido una intrusión wifi
Fuente: Panel hogares, ONTSI

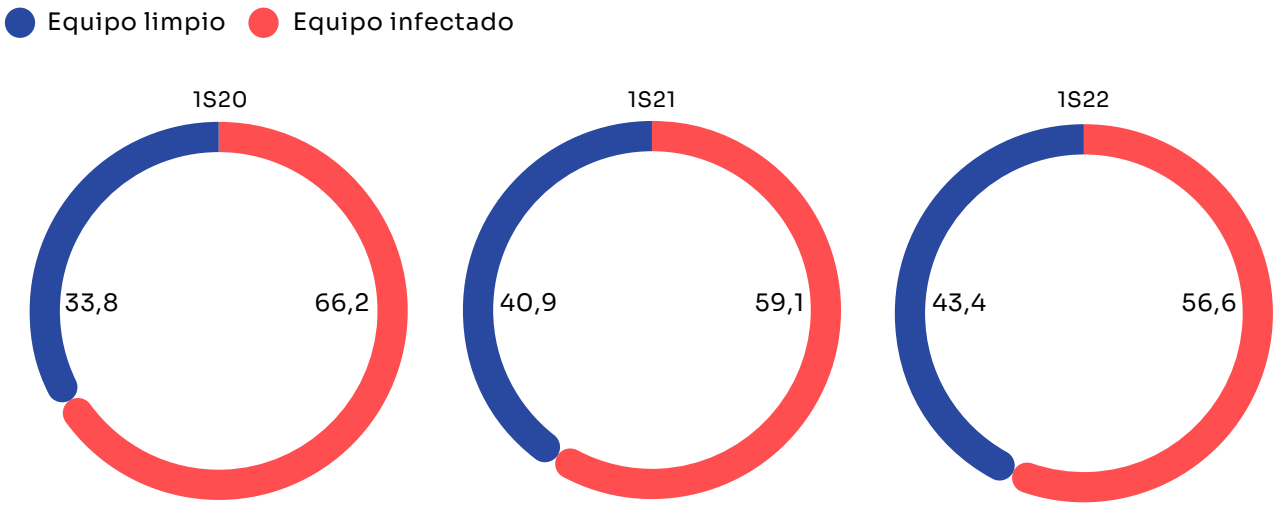
4.4. Intrusiones por *malware*

Las infecciones de *malware* o *software* maligno son puertas de entrada para los ciberatacantes en nuestros hogares, llegándoles a permitir controlar redes enteras a través de nuestros dispositivos personales, dado que cada vez más ordenadores están dentro del mismo entorno doméstico.

El gráfico 30 recoge los resultados tras realizar el análisis de *malware* de los ordenadores del hogar empleando el *software* de escaneo Pinkerton. Durante el primer semestre de 2022 se experimenta un descenso en el número de ordenadores infectados con algún tipo de *malware* (baja 2,5 p.p. respecto el año anterior), y alcanza el 56,6%.

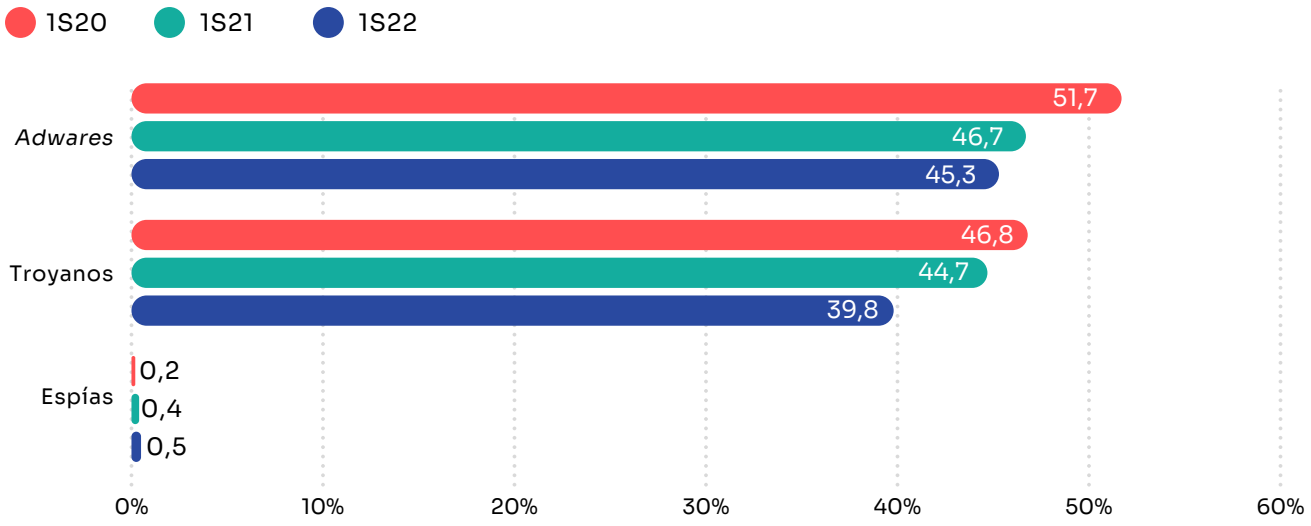
Un 56,6% de los ordenadores tienen algún tipo de *malware*, la incidencia desciende más de 2,5 puntos con respecto al año anterior

Gráfico 30 - **Estado de infección real del ordenador del hogar dividido en periodos anuales (%)**



Base: Total de ordenadores
Fuente: Panel hogares, ONTSI

Gráfico 31 - **Tipología de *malware* detectado en el ordenador del hogar (%)**



Base: Total de ordenadores
Fuente: Panel hogares, ONTSI

En cuanto a los tipos de *malware* identificado durante este análisis (Gráfico 31), el 45,3 % del *malware* que infectó los dispositivos era *adware*. Este tipo de *malware* suele estar diseñado para mostrar anuncios en la ventana del navegador con el objetivo de generar ingresos para los atacantes a partir de los anuncios que se muestran[10].

También se han detectado troyanos. En concreto, el 39,8% de equipos analizados contenía algún tipo. Este número se ha visto rebajado respecto al año anterior en 4,9 p.p., aun así, sigue siendo una cifra considerable por su peligrosidad, ya que da la posibilidad al atacante de acceder en remoto al equipo infectado y espiar o robar datos.

El 45,3 % del *malware* identificado que infectó los dispositivos era *adware*

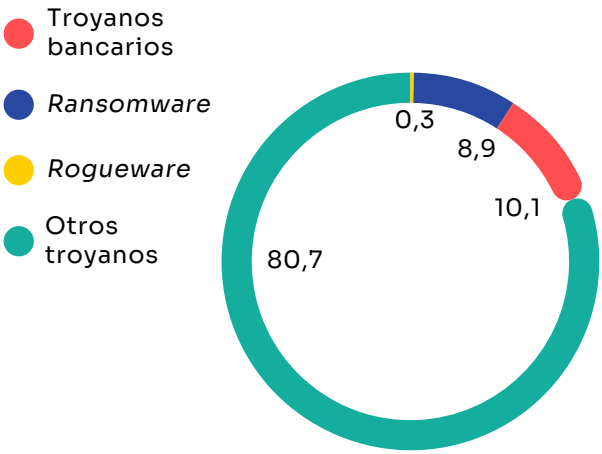
[10] https://es.malwarebytes.com/adware/

Existen distintos tipos de troyanos, el 8,9% de los identificados por Pinkerton eran *ransomware* (Gráfico 32). El secuestro de datos es muy peligroso ya que puede transferir muchas muestras no solo a su ordenador, sino también a otros a través de la red, restringe el acceso a los propios datos personales, y piden un rescate a cambio de quitar esta restricción.

Por otra parte, los troyanos bancarios aparecen en el 10,1% de los equipos analizados, cuyo principal objetivo es obtener credenciales de inicio de sesión y contraseñas con fines fraudulentos.

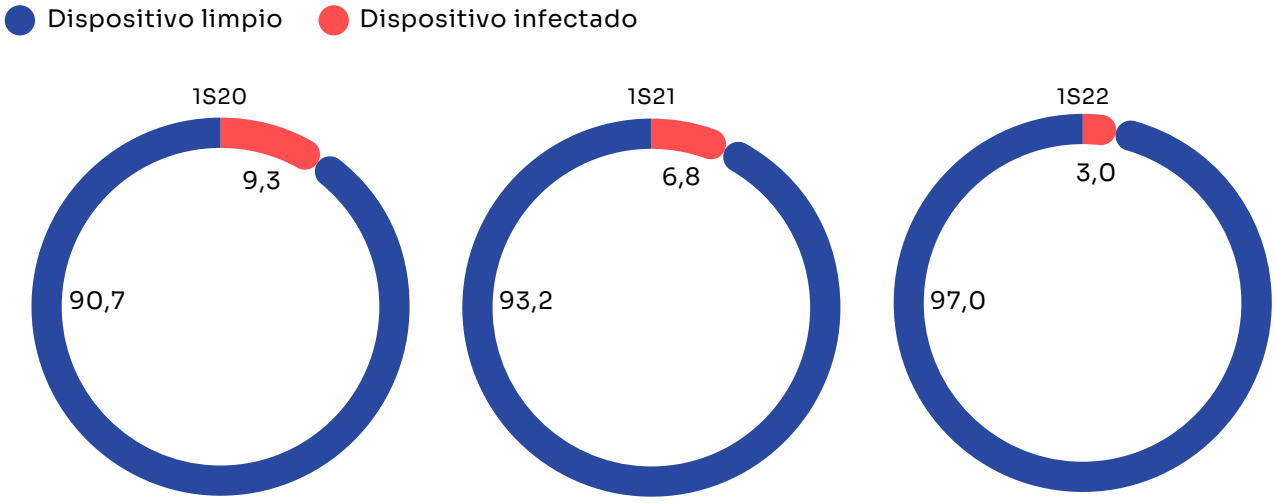
Pinkerton también analiza el número de dispositivos Android infectados con algún tipo de *malware*. Durante el primer trimestre de 2022, disminuyó el número de terminales afectados en comparación con la primera mitad de 2021 hasta situarse en el 3,0% de los casos, lo que supone 3,8 puntos porcentuales menos (Gráfico 33).

Gráfico 32 - **Clasificación de troyanos detectados en ordenador del hogar (%)**



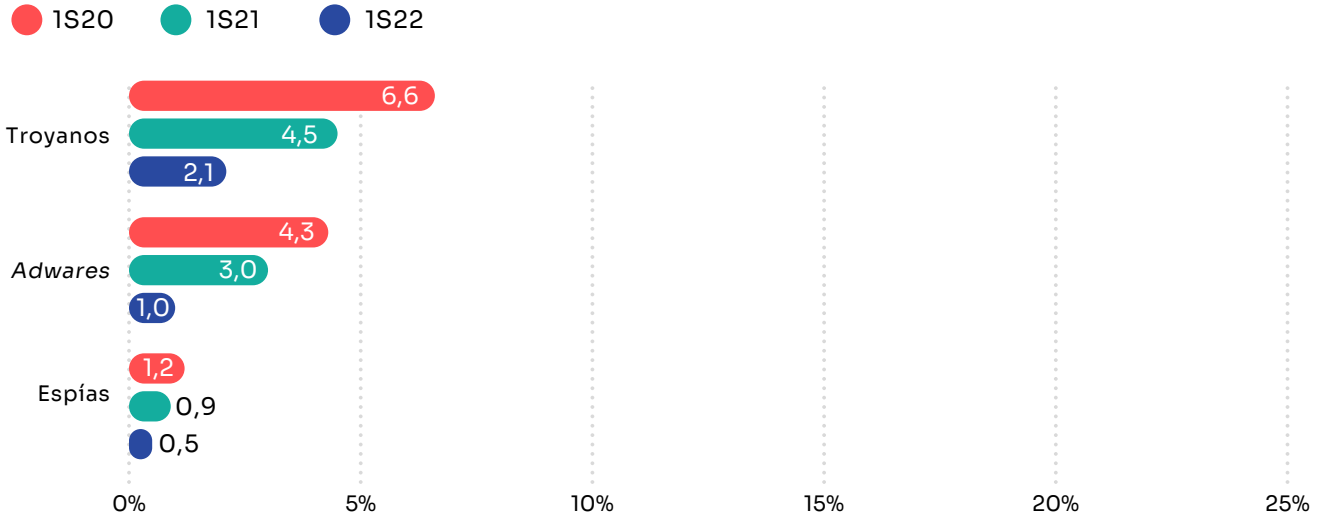
Base: Total de ordenadores con troyanos detectados
Fuente: Panel hogares, ONTSI

Gráfico 33 - **Estado de infección real en los dispositivos Android (%)**



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

Gráfico 34 - **Tipología de *malware* detectado en dispositivos Android (%)**



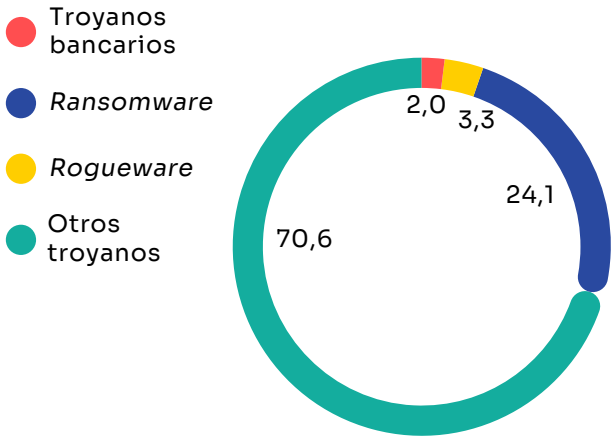
Base: Total de dispositivos Android
Fuente: Panel hogares, ONTSI

Las comunicaciones móviles están a la vanguardia de la seguridad, ya que en su mayoría las versiones más nuevas del sistema operativo Android incorporan mecanismos como la biometría y la seguridad integrada Además, tiene más control sobre las instalaciones que se realizan.

En cuanto a la tipología de *malware* presente en los dispositivos Android, los resultados recabados se resumen en el gráfico 34. En general, el número de infecciones ha disminuido considerablente respecto al año anterior, los troyanos (*software* malicioso aparentemente inofensivo) en 2,4 p.p., los *adwares* (*software* que inyecta anuncios) en 2 p.p. y los espías en 0,4 p.p.

A diferencia de los ordenadores del hogar, en el caso de los dispositivos Android es el secuestro de datos o *ransomware*, con el 24,1% sobre los dispositivos infectados, el objetivo principal de los troyanos identificados (Gráfico 35).

Gráfico 35 - **Clasificación de troyanos detectados en dispositivos Android (%)**



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

05

Consecuencias de los incidentes de seguridad

Los incidentes de seguridad pueden tener diferentes tipos de consecuencias: infecciones de los equipos, robo de datos, pérdida de información y económicas. 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.

La mayor parte del perjuicio económico a causa del fraude, tanto telefónico como en línea, alcanza como máximo el valor de 100 euros

5.1. Consecuencias económicas del fraude

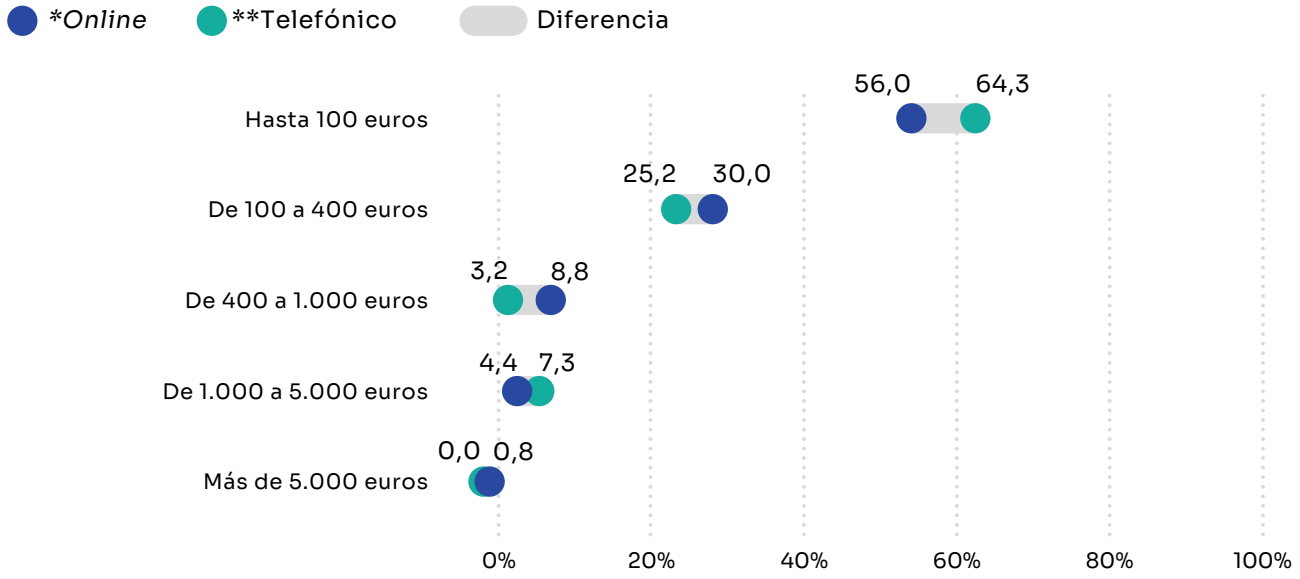
Los datos del informe sobre la cibercriminalidad 2021 del Ministerio del Interior ayudan a poner en contexto el fraude *online*. Señalan 305.477 hechos ilícitos conocidos; un 6,1% más con respecto al año anterior. De esta cifra, el 87,4% corresponde a fraudes informáticos (estafas). Actualmente, la importancia de la Ciberseguridad va creciendo año tras año, como se demuestra con el aumento del número de ataques cibernéticos conocidos[11].

Un aumento de los incidentes de fraude no necesariamente tiene que ir acompañado de un aumento del perjuicio económico, ya que depende en gran medida del éxito de los intentos de ataque. Por este motivo, la medición del daño económico puede ayudar a explicar la efectividad de los ataques. El gráfico 36 se centra en este punto, donde destacan las pérdidas financieras reportadas por víctimas de fraude y de perjuicios monetarios. No obstante, es importante tener en cuenta que los delitos cibernéticos no siempre se denuncian.

Concretamente, el gráfico muestra las diferencias entre el perjuicio económico del fraude telefónico y el que se lleva a cabo en línea (a través de Internet, como el correo electrónico o mensajería instantánea). Los resultados muestran que la gran mayoría de los casos no suponía pérdidas mayores de 400 euros. El intervalo mínimo (de 0 hasta 99 euros) representa el 64,3% de estafas telefónicas y el 56% de las electrónicas, mientras que el 25,2% del fraude por telefono y el 30% del *online* implicaba pérdidas de entre 100 y 399 euros. Sólo el 0,8% del grupo de personas afectadas por el fraude *online* experimentaron las pérdidas más valiosas (cuando las víctimas reclamaron daños de 5.000 euros o más).

[11] Fuente: Ministerio del Interior (2021): Informe sobre la Cibercriminalidad en España. Dirección General de Coordinación y Estudios. Secretaría de Estado de Seguridad https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf

Gráfico 36 - **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

5.2. Evolución del riesgo de las infecciones

En las clasificaciones de *malware* de las muestras pueden categorizarse como altamente peligrosas por sus efectos adversos en los ordenadores los ya conocidos *ransomware*, *rogueware* (aplicaciones que intentan parecerse a un *software* de seguridad en apariencia o nombre para engañar y defraudar a las personas) y troyanos bancarios.

En este sentido, el gráfico 37 muestra un descenso interanual de 4,8 puntos porcentuales en la detección de *malware* de alto riesgo en los equipos domésticos. Aun así, continúa siendo una cifra alta.

En concreto, el 70,2% tanto de ordenadores domésticos como de dispositivos Adroid infectados estaban afectados con un tipo de *malware* clasificado como de alta peligrosidad, lo que es arriesgado para quienes se conectan desde terminales domésticos, dado que solo se necesita un ordenador para infectar toda la red. Esto se debe a que los mecanismos de propagación de *malware* están cada vez más diseñados para explotar la conectividad de los dispositivos.

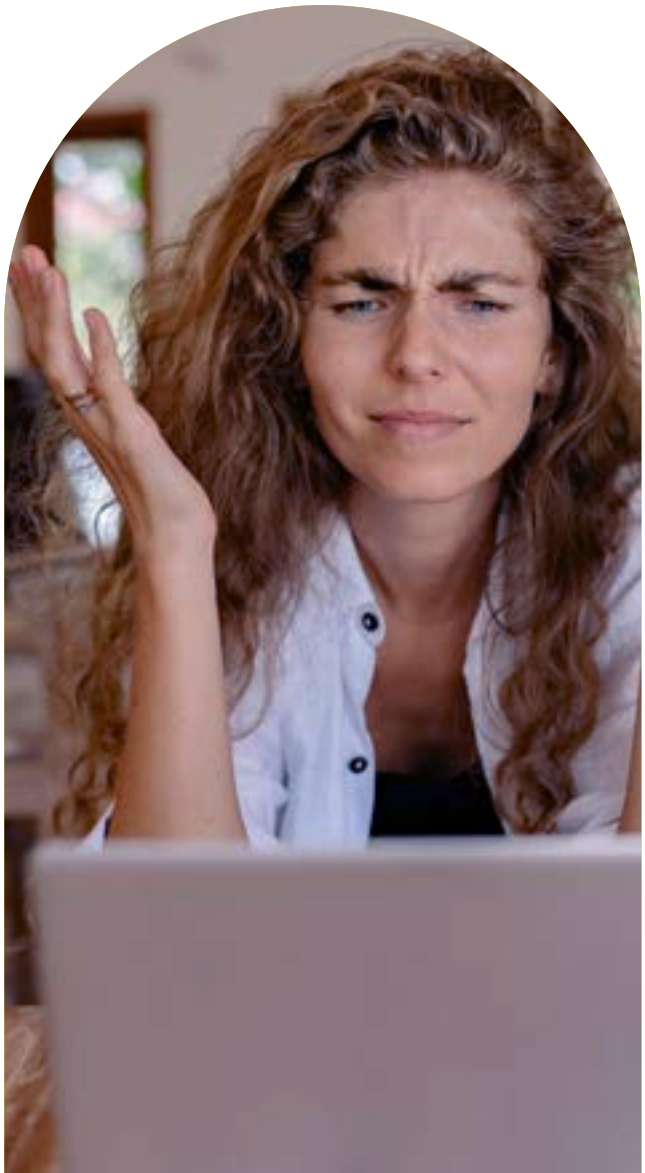
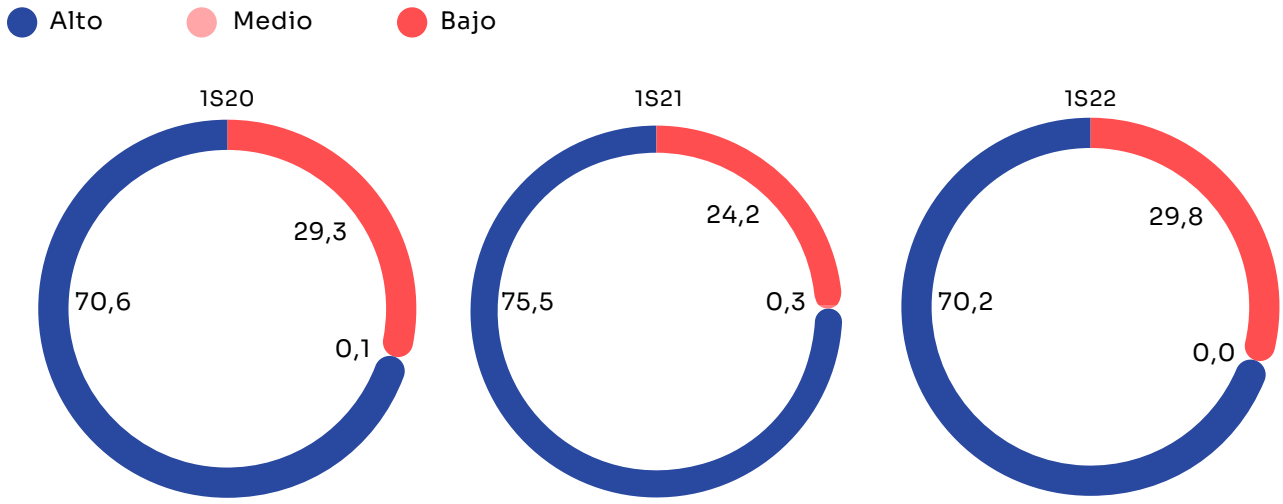
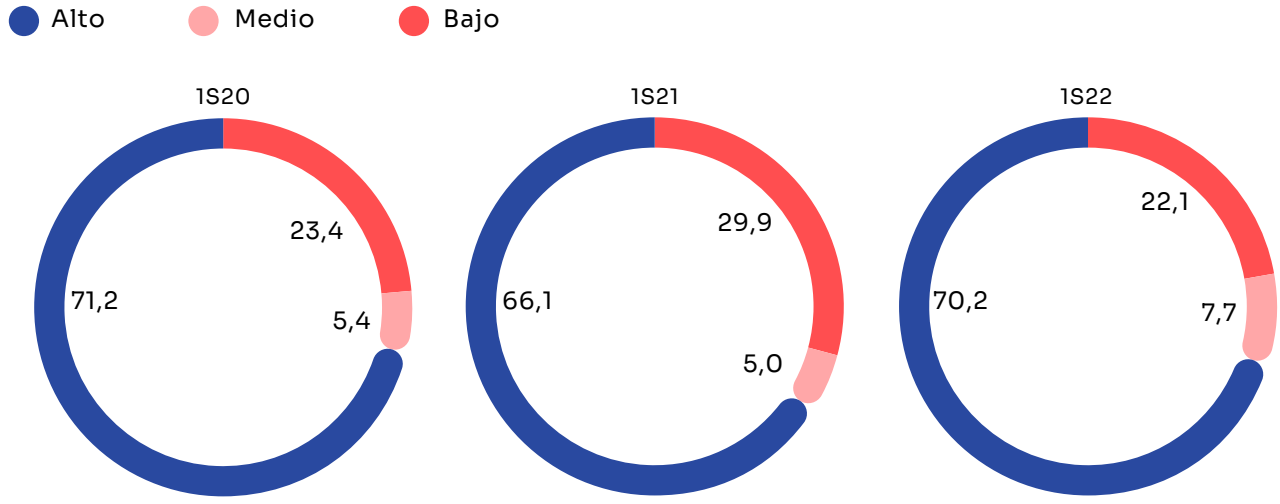


Gráfico 37 - **Peligrosidad del *malware* detectado y riesgo del ordenador del hogar (%)**



Base: Total ordenadores infectados
Fuente: Panel hogares, ONTSI

Gráfico 38 - **Peligrosidad del *malware* detectado y riesgo de los dispositivos Android (%)**



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

La presencia de *malware* altamente peligroso es un mal no deseado, ya que puede tener consecuencias negativas para los dispositivos y, por tanto, para quienes los usan. La protección antivirus por sí sola a menudo no es suficiente. La presencia de *software* malicioso no solo conduce a la pérdida de información, sino que en algunos casos puede dañar físicamente el equipo.[12 y 13]

En lo que al *malware* detectado en dispositivos Android se refiere, la cantidad de *software* de alto riesgo que amenaza los propios dispositivos y la privacidad de los usuarios aumentó en 4,1 p.p. comparado con el año anterior (Gráfico 38). Este repunte acerca las cifras, con un 70,2% de dispositivos infectados, a los máximos alcanzados en 2020, y que habían sufrido un descenso en 2021.

El 70,2% de ordenadores y dispositivos Android infectados presentan *malware* de alta peligrosidad

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

[13] Es el caso del virus troyano 'BRATA para Android: https://cincodias.elpais.com/cincodias/2022/01/26/lifestyle/1643200781_556219.html

5.3. Cambios de hábitos tras un incidente de seguridad

Después de padecer un ataque de seguridad, es común cambiar el comportamiento para evitar la recurrencia de este tipo de incidentes. Por ejemplo, en caso de un ataque de *ransomware*, es común que se comience a realizar copias de seguridad de forma periódica.

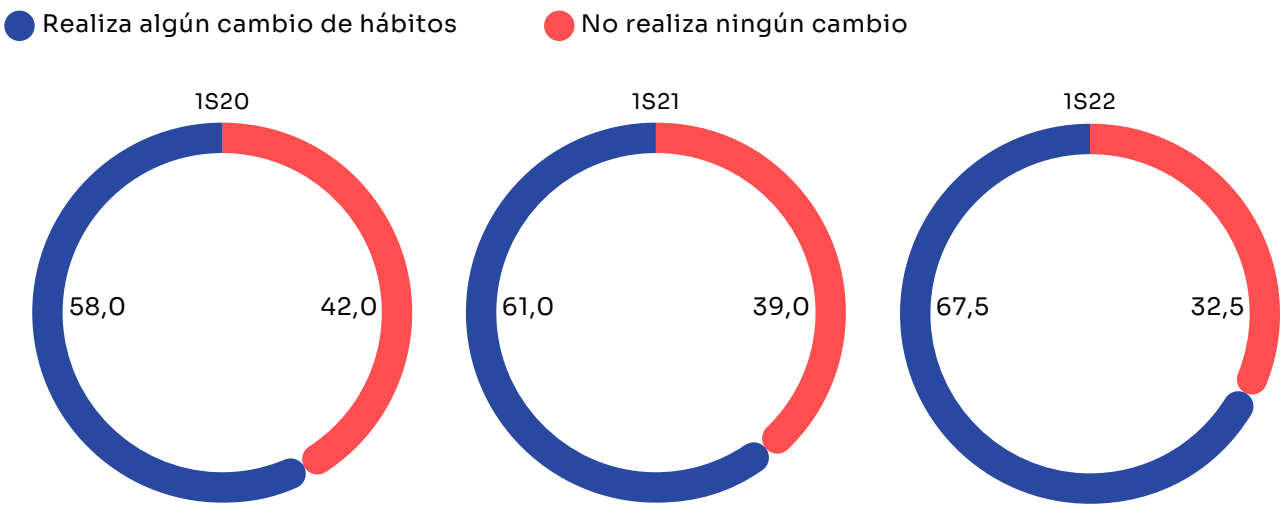
Como se mostraba en el gráfico 24, el número de incidentes de seguridad informados aumentó en el último año. El gráfico 39 recoge el porcentaje de víctimas de incidentes de seguridad cibernética que cambiaron algunos hábitos después de sufrir un incidente de seguridad. Concretamente, un 67,5% de las victimas modifican algún comportamiento, lo que supone un aumento interanual de 6,5 p.p. de este indicador.

Entre las víctimas de incidentes de seguridad que declaran haber cambiado sus hábitos, el 46,3% apuesta principalmente por mejorar el uso de las contraseñas. Ya sea mediante cambiar las contraseñas o empezar a usar un gestor de contraseñas.

Es significativo el incremento interanual en el número de víctimas cibernéticas que después del ataque recurren a mecanismos de ayuda en materia de ciberseguridad. Por ejemplo, la línea 017 de INCIBE, sistemas de denuncia a través de RRSS y fuerzas de cuerpos de seguridad del estado. Este tipo de reportes ha pasado del 13% al 14,5%.

Otras acciones para reducir las posibilidades de que los dispositivos se infecten con *malware* y favorecer la recuperación de los datos que realizan los panelistas son: actualizar herramientas y configuraciones de seguridad y privacidad ya instaladas (30,3%), hacer copias de seguridad (24,3%), y dejar de descargar archivos de redes P2P (22,2%).

Gráfico 39- **Cambio de hábitos en Internet motivados por las incidencias de seguridad experimentadas (%)**



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

Gráfico 40 - **Cambios de hábitos en Internet motivados por las incidencias de seguridad experimentadas (%)**

*** Nuevas categorías**

Base: Personas que han sufrido alguna incidencia de seguridad y modifican sus hábitos

Fuente: Panel hogares, ONTSI

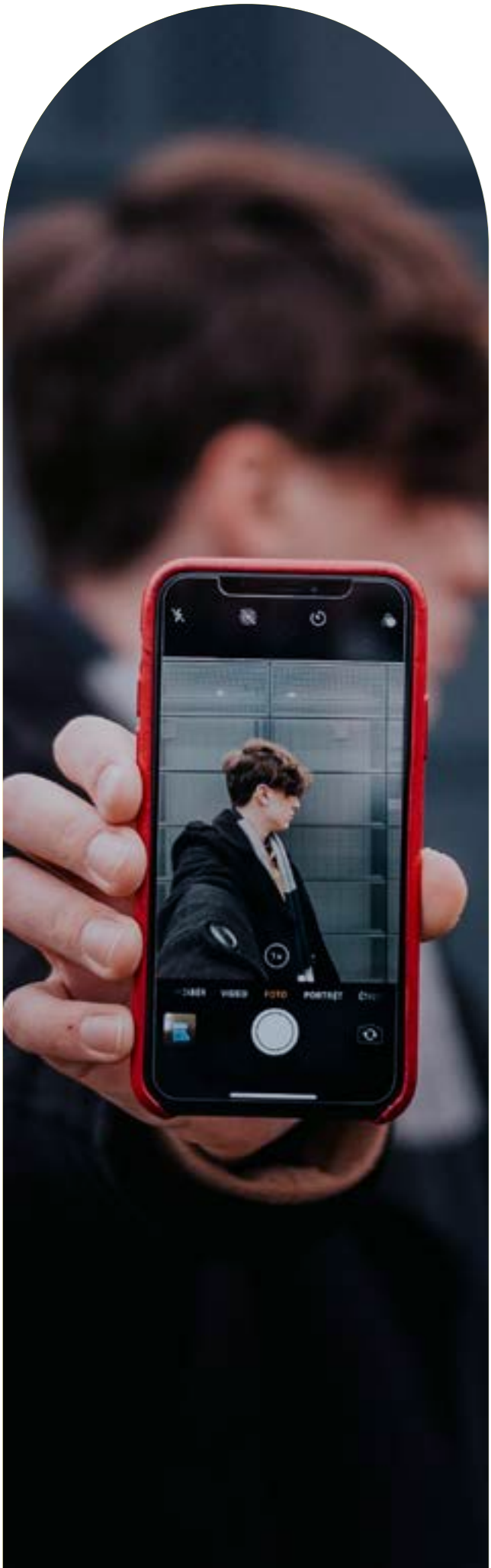
En el gráfico 41 se muestran mejoras implementadas por quienes declaran utilizar de forma más segura sus contraseñas y credenciales tras haber sufrido una incidencia de seguridad.

La mejora más extendida es emplear patrones de seguridad conocidos como alternar números y letras (57,2%).

Cambiar las contraseñas regularmente es una de las mejores medidas que se pueden implementar, ya que pueden ser filtradas si no se almacenan y protegen debidamente. Esta buena medida la han llevado a cabo durante el primer semestre de 2022, el 43,5% de la quienes han introducido mejoras en este sentido.

Evitar utilizar la misma contraseña en diferentes cuentas es también crucial, lo que permite no afectar al resto si una se ve vulnerada. Esta medida es aceptada y puesta en práctica por el 49,8% de quienes introdujeron mejoras.

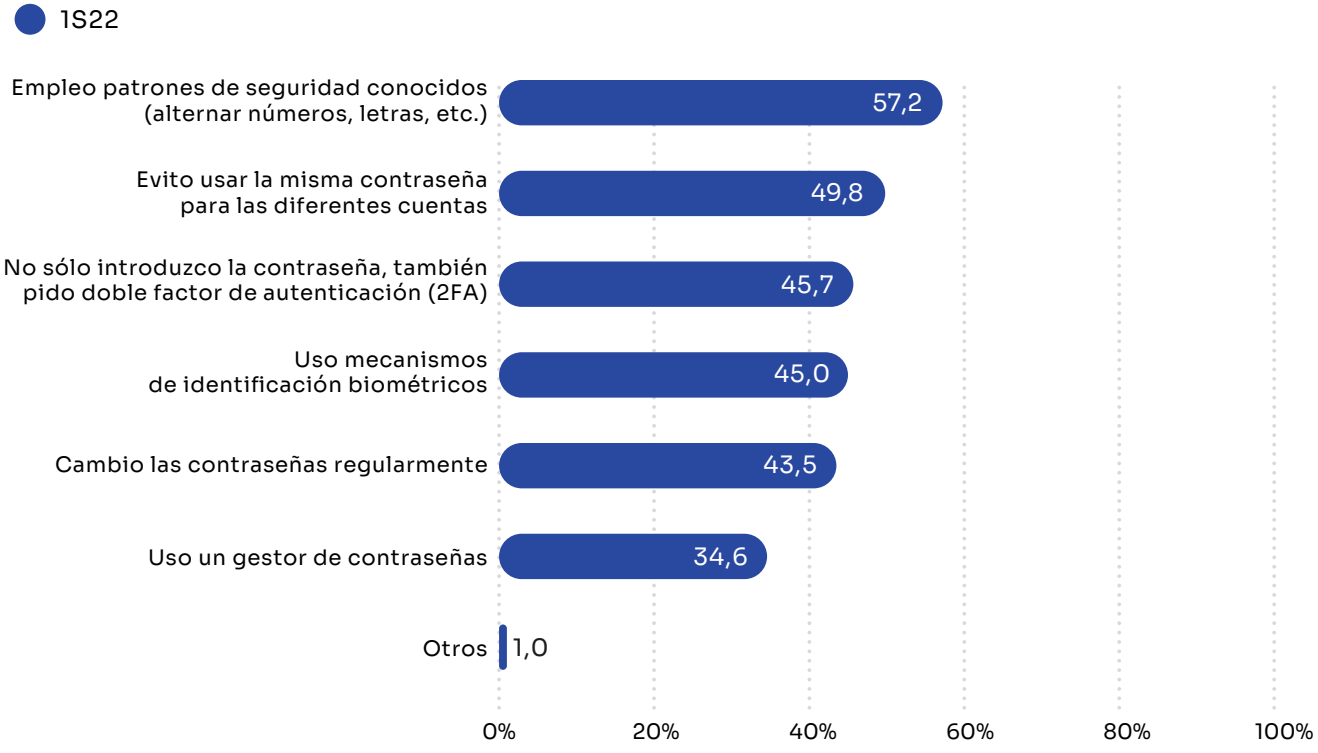
Tras experimentar una incidencia de seguridad, el 45% de los afectados declara utilizar mecanismos de identificación biométricos



El conocimiento de los canales para pedir ayuda o denunciar actividades ilegítimas como ciberdelitos o acoso *online* a las autoridades es vital. Sin embargo, más del 60% de las personas entrevistadas declaran no saber de la existencia de estos canales.

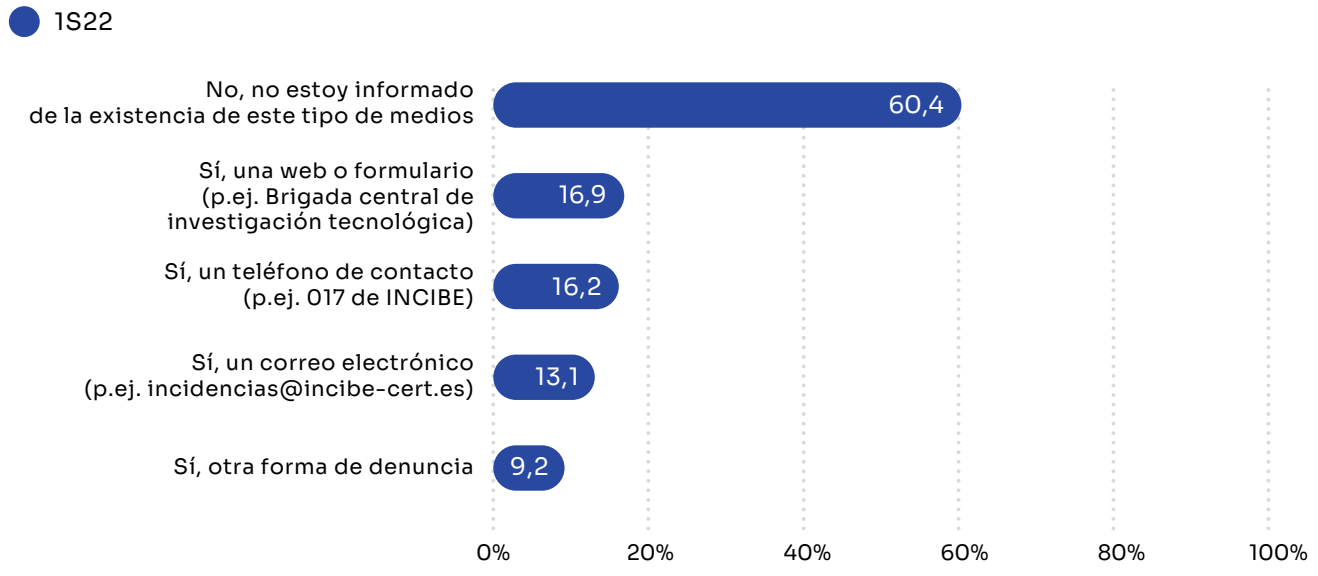
Los canales más conocidos son el formulario de denuncia de la Brigada central de investigación tecnológica de la Policía Nacional y la línea de ayuda telefónica 017 de INCIBE. Con un 16,9% y 16,2% respectivamente de los reportes.

Gráfico 41 - **Mejoras en el uso de contraseñas y credenciales (%)**



Base: Total usuarios y usuarias que han mejorado su uso de las contraseñas tras sufrir incidencia
Fuente: Panel hogares, ONTSI

Gráfico 42 - **Conocimientos de canales para denunciar conducta irregular *online* (%)**



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

06

Confianza de las personas usuarias

En gran parte, la pérdida de confianza en los servicios de Internet es consecuencia de los incidentes de seguridad. No obstante, sigue siendo uno de los aspectos más peculiares. Para ciertas personas, un incidente de seguridad puede no tener un impacto significativo en su nivel de confianza, mientras que para otros puede tener repercusiones de gran alcance.

Por lo tanto, este aspecto merece una sección específica en el presente estudio con el fin de analizar las opiniones acerca de los factores que más influyen en la percepción de los riesgos en Internet y, por supuesto, en la confianza del usuario.

Sólo un 5,6% de quienes tienen *malware* en su PC son conscientes de ello

6.1. Percepción de la población sobre la infección de sus equipos

Confiar demasiado en la ausencia de infecciones o ataques a los dispositivos es peligroso. Los incidentes de seguridad son un factor clave en el cambio de hábitos de las personas usuarias. Sin embargo, aumentar la prevención ante los incidentes implica poder identificar la amenaza, puesto que de lo contrario, los comportamiento de riesgo en línea pueden continuar. De este modo, los dispositivos quedan completamente expuestos a los atacantes.

Lamentablemente, las afirmaciones acerca de si se cree o no que el ordenador está infectado con *malware* no concuerdan con los datos recopilados por Pinkerton. Se encontró que el 56,6% de los equipos domésticos analizados estaban infectados con *software* malicioso, no obstante, solo el 6,8% de los panelistas percibieron esta situación.

El *malware* de bajo riesgo en el ordenador aumentó durante 2022 (Gráfico 37). En este grupo se incluyen aquellos que no tienen un impacto notable en el rendimiento, pero pueden ser perceptibles para quien hace uso. Por ejemplo, abriendo ventanas no deseadas mientras se navega, o incrustando anuncios en páginas web legítimas que en realidad no contienen anuncios y facilitando la captura de información sensible de la víctima.

La Tabla 1 resume la comparación entre la detección de *malware* por el *software* Pinkerton y las opiniones recopiladas. De aquellos que tenían un 56,6% de *software* malicioso en sus PC, un 51% confiaba en que su equipo no estaba infectado, mientras que solo un 5,6% acertó en su percepción. En ocasiones, esta apreciación puede diferir de la realidad debido a la falta de uso de antivirus, como se observa en las declaraciones recogidas en el Gráfico 4 del Capítulo 3 del informe.

Esta cifra es significativa, ya que la creencia de que no hay infección puede llevar a comportamientos más descuidados y a la falta de cambios en los hábitos.

La Tabla 2 y la Tabla 3 muestran las cifras reales en comparación con la percepción de los usuarios, desglosadas por género.

Tabla 1 - **Desglose del estado real versus percepción (ordenador del hogar). 1S2022**

Declaran tener *malware* en PC	Su PC presenta *malware*		
	Sí	No	Total
Sí	5,6	1,2	6,8
No	**51,0**	42,2	93,2
Total	56,6	43,4	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). 1S2022**

Declaran tener *malware* en PC	Su PC presenta *malware*		
	Sí	No	Total
Sí	7,4	1,8	9,2
No	**52,0**	38,8	90,8
Total	59,4	40,6	100

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

Tabla 3 - **Desglose del estado real versus percepción (ordenador del hogar cuyas propietarias son mujeres). 1S2022**

Declaran tener *malware* en PC	Su PC presenta *malware*		
	Sí	No	Total
Sí	3,5	0,9	4,4
No	**49,4**	46,2	95,6
Total	52,9	47,1	100

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

Según los resultados de escaneo de ordenadores, se encontró que el 52% de los hombres y el 49,4% de las mujeres tenían algún tipo de *software* malicioso en sus PCs (ver Tablas 2 y 3). A pesar de esto, muchos de ellos no eran conscientes de la infección, lo cual puede deberse a la falta de conocimiento sobre los síntomas asociados. Algunos posibles síntomas incluyen el cierre inesperado de aplicaciones, un rendimiento más lento de la máquina y la aparición de anuncios en nuevas ventanas del navegador. A menudo, los usuarios son los primeros en notar estos problemas, ya que el sistema no funciona como de costumbre.

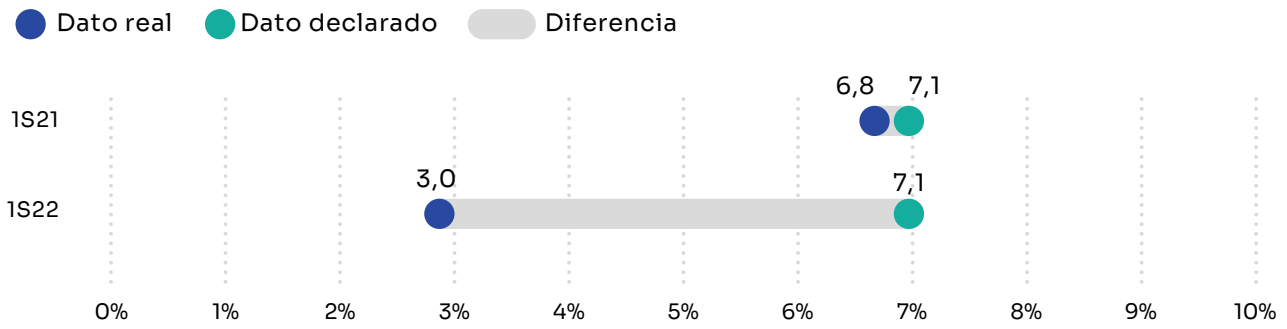
Los dispositivos Android analizados en el estudio son especialmente atractivos para los atacantes debido a que almacenan información personal y son ampliamente utilizados para acceder a Internet. Los desarrolladores trabajan constantemente en mejorar la seguridad de los sistemas operativos y aplicaciones para prevenir infecciones. En el Gráfico 43 se compara la situación real de estos dispositivos con la percepción de infección por parte de los usuarios.

En comparación con los ordenadores (Tabla 1), los dispositivos móviles (Tabla 4) se consideran algo menos seguros. Mientras que el 6,8% de las personas creía tener *malware* en sus PCs, el 7,1% pensaba lo mismo sobre sus dispositivos móviles. Sin embargo, solo el 3,0% de los dispositivos Android estaba realmente infectado (Tabla 4).

Al analizar más detalladamente el porcentaje de dispositivos Android infectados, se observa que un 2,9% de las personas creía erróneamente que sus dispositivos estaban libres de *software* malicioso cuando en realidad estaban infectados. Por otro lado, el 90% acertó al afirmar que sus dispositivos no estaban infectados.

Cuando se desglosan estos resultados por género, se obtienen los datos presentados en las Tablas 5 y 6.

Gráfico 43 - **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). 1S2022**

Declaran tener *malware* en el dispositivo Android	Su dispositivo Android presenta *malware*		
	Sí	No	Total
Sí	0,1	7,0	7,1
No	**2,9**	90,0	92,9
Total	3,0	97,0	100

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

El 3% de los dispositivos Android analizados contenían algún *software* malicioso. Sin embargo, el 7% de los usuarios creía erróneamente que su dispositivo estaba infectado

Tabla 5 - Desglose del estado real versus percepción de infección (dispositivos Android pertenecientes a hombres). 1S2022

Declaran tener *malware* en el dispositivo Android	Su dispositivo Android presenta *malware*		
	Sí	No	Total
Sí	0,3	8,7	9,0
No	**3,3**	87,7	91,0
Total	3,6	96,4	100

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

Tabla 6 - Desglose del estado real versus percepción de infección (dispositivos Android pertenecientes a mujeres). 1S2022

Declaran tener *malware* en el dispositivo Android	Su dispositivo Android presenta *malware*		
	Sí	No	Total
Sí	0,0	5,2	5,2
No	**2,5**	92,3	94,8
Total	2,5	97,5	100

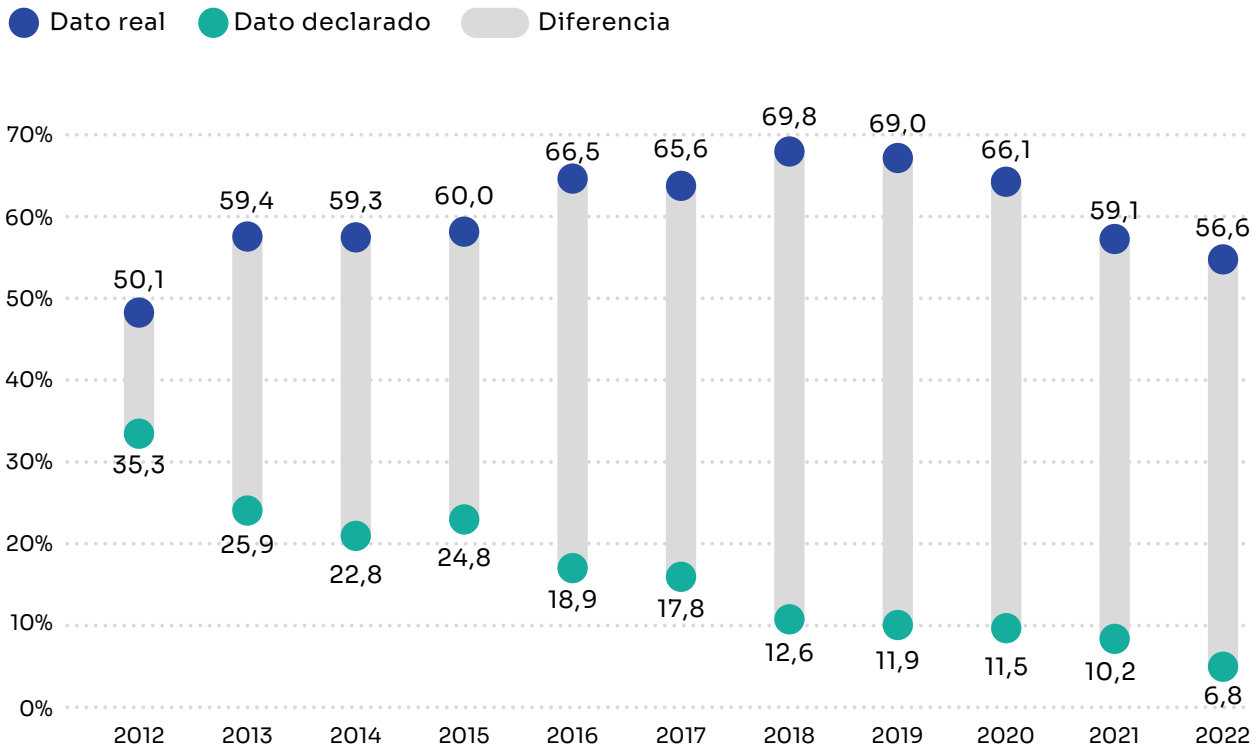
Base: Mujeres con dispositivo Android escaneado
Fuente: Panel hogares, ONTSI

Conforme a los resultados expuestos en la tabla 5, el 3,3% de los hombres desconoce que tiene infectado su dispositivo móvil con sistema Android.

Sin embargo, al observar los resultados para la población femenina resumidos en la tabla 6, el 2,5% de las mujeres encuestadas respondieron que no hay *malware* en sus dispositivos, a pesar de que los datos empíricos indican que estaban infectados.

En el gráfico 44 se observa que, de forma prolongada, la percepción que se tiene sobre las infecciones en el ordenador del hogar ha ido disminuyendo, mientras que las infecciones reales se mantienen si bien, estas han disminuido más de 13 puntos porcentuales en los últimos 5 años, hasta situarse en el 56,6% de los casos.

Gráfico 44 - **Estado real global versus percepción de infección general. Ordenador del hogar.**



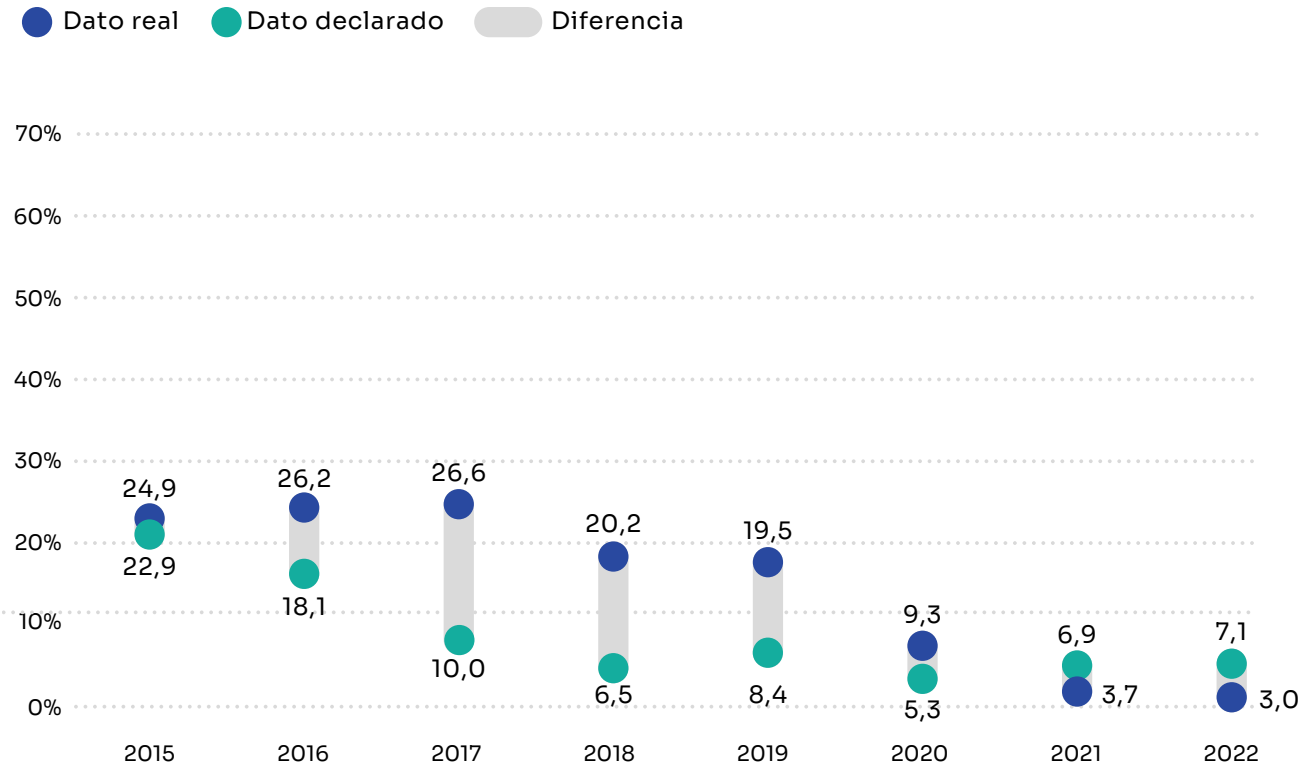
Base: Personas con ordenador escaneado
Fuente: Panel hogares, ONTSI

El panorama del *malware* ha evolucionado, adaptándose a los intereses de los atacantes. Anteriormente, los *adwares* eran comunes y su detección era relativamente sencilla debido a su comportamiento errático y la presencia masiva de publicidad no deseada. Sin embargo, en la actualidad, el *malware* busca pasar desapercibido durante el mayor tiempo posible, aprovechando los recursos de la víctima de manera sigilosa.

Actualmente, los *adwares* han perdido popularidad y han surgido nuevas formas ilícitas de lucro para los cibercriminales, como los mineros de criptomonedas o el *spyware*, que roba archivos confidenciales o captura imágenes para extorsionar a las víctimas posteriormente.

Los actores de amenazas más avanzados utilizan *software* malicioso extremadamente sofisticado para aprovechar vulnerabilidades, evadir defensas y mecanismos de detección, y establecer puertas traseras que les permitan acceder nuevamente a la infraestructura de la víctima en el futuro.

Gráfico 45 - **Estado real global versus percepción de infección general. Dispositivos Android**



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

En el gráfico 45 observamos un fenómeno distinto al caso del PC. Con el paso del tiempo, la infección real en Android disminuye hasta situarse por debajo de la declarada por los usuarios.

Los dispositivos móviles cada vez mejoran más su seguridad, como pueden ser el principio del mínimo privilegio implantado por defecto en Android y la más baja permisibilidad a la personalización a bajo nivel del sistema.

El hecho de que usuarios y usuarias en Android no tengan, y no se les permita por medios convencionales acceder a funcionalidades de administrador del dispositivo, reduce exponencialmente su superficie de exposición o vulnerabilidad.

Asimismo, la restricción y aviso del sistema a la hora de descargar aplicaciones de fuentes desconocidas, también es una buena precaución y prevención frente a potencial *malware* por parte del sistema operativo.

6.2. Opiniones sobre la seguridad en Internet

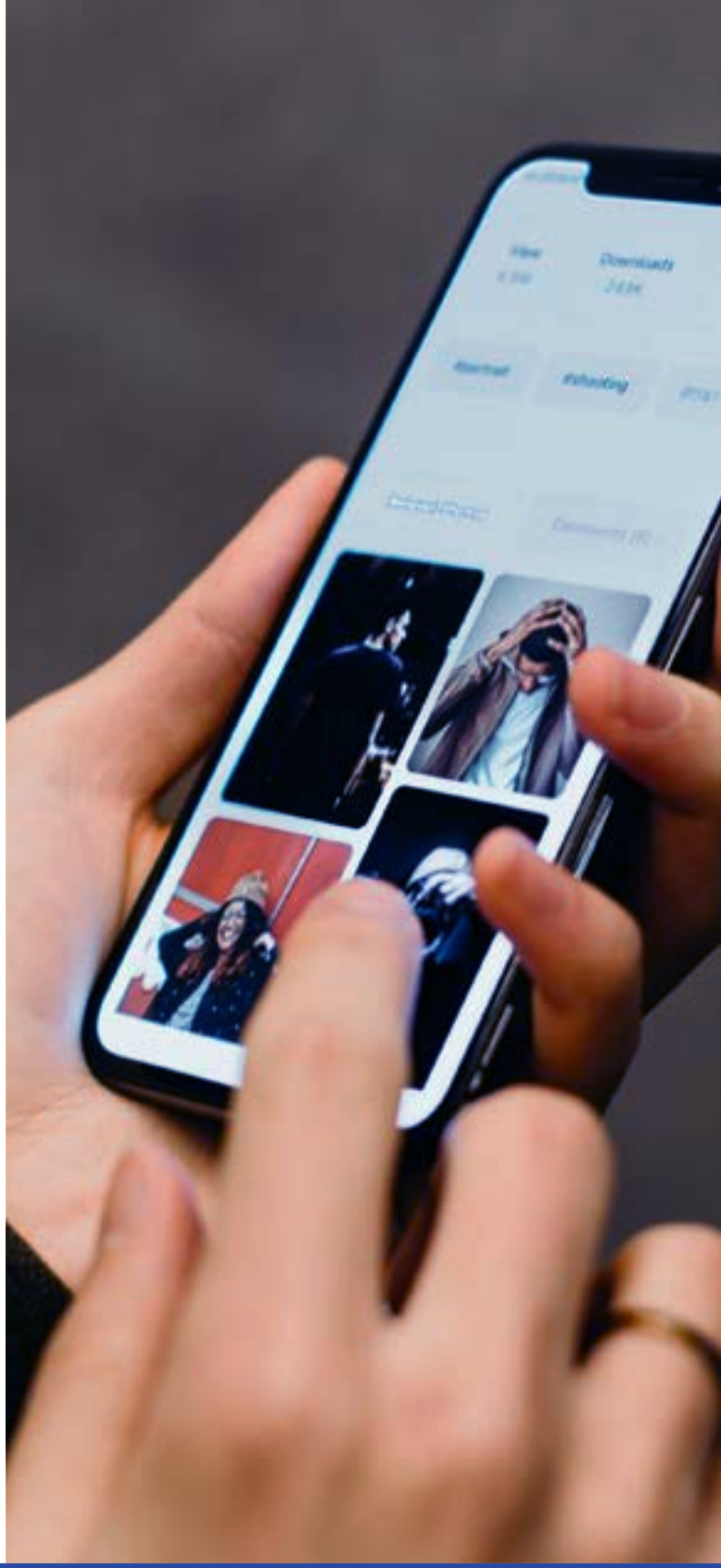
El uso responsable de Internet es fundamental en la prevención de los ciberriesgos. Actuar de forma consciente está muy relacionado con las opiniones de la seguridad en la red (Gráfico 5).

Como recoge el gráfico 46, el 78,3% de las personas encuestadas opina que si su equipo o dispositivo está razonablemente protegido le hace la vida más fácil. Este dato ha disminuido 1,2 p.p. con respecto al 2021.

Cada año se llevan a cabo numerosas campañas de concienciación sobre ciberseguridad a través de medios de comunicación. Sin embargo, al 80,7% de los panelistas manifestó su interés por que los gobiernos se involucren de más formas para preservar la seguridad en Internet, una cifra ligeramente superior a la del año anterior.

Es importante resaltar que el número de personas que afirman limitar su uso de las nuevas tecnologías debido a la falta de conocimiento en seguridad se ha mantenido constante. Ha habido una ligera variación del 0,1 punto porcentual, pasando del 48,5% en 2021 al 48,4% en 2022.

Además, es relevante mencionar que un 45,6% de las personas usuarias señala que les resulta complicado encontrar información útil para navegar de manera segura en Internet.



Un 80,7% cree que los organismos públicos han de implicarse más en mejorar la seguridad en Internet

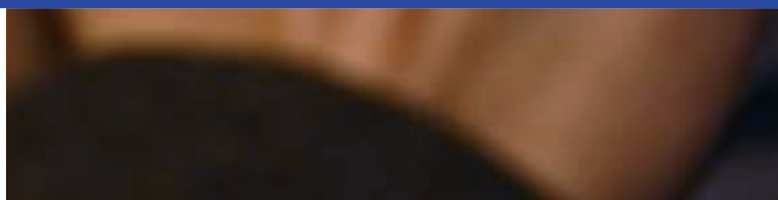
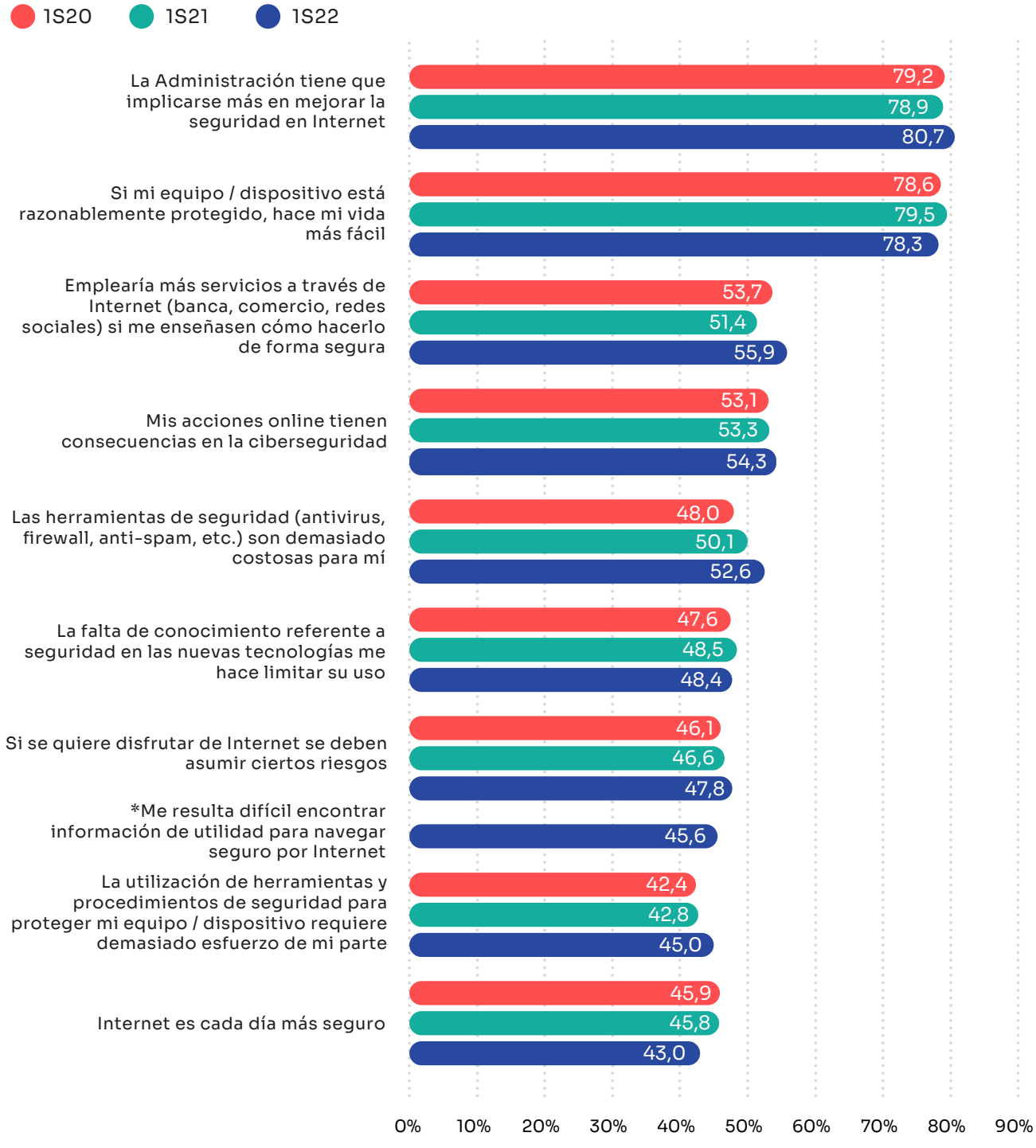


Gráfico 46 - **Opiniones sobre la seguridad en Internet (%)**



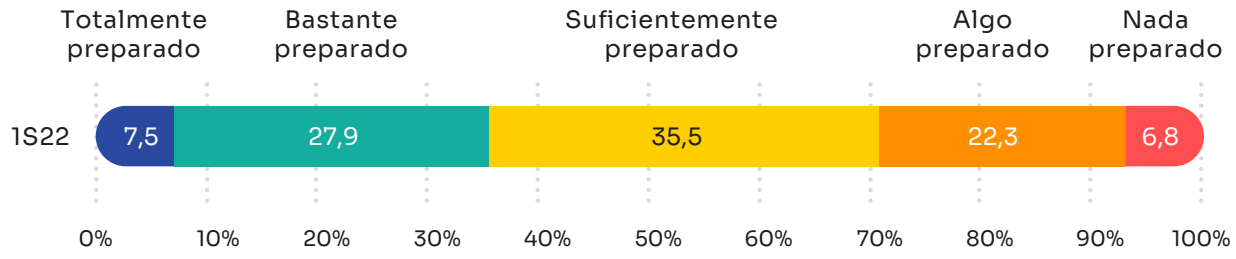
***Nueva clasificación**
Base: Total de usuarios y usuarias
Fuente: Panel hogares, ONTSI

6.3. Nivel de preparación para afrontar riesgos

Es interesante conocer la autopercepción acerca de cómo de preparada se siente la población a la hora de afrontar posibles riesgos y ataques reales en su día a día utilizando tecnologías. Al analizar la visión subjetiva hacia las posibilidades de afrontar problemas de ciberseguridad, observamos que hay una amplia variedad de opiniones (Gráfico 47).

Solo el 7,5% de quienes usan Internet cree tener la capacidad de afrontar los retos de seguridad. El 27,9% manifiesta estar bastante preparado o preparada mientras que el 35,5% declara que lo está suficientemente. Los sectores más dudosos abarcan el 22,3% que se consideran algo preparados/as y el 6,8% que declaran estar nada preparados/as.

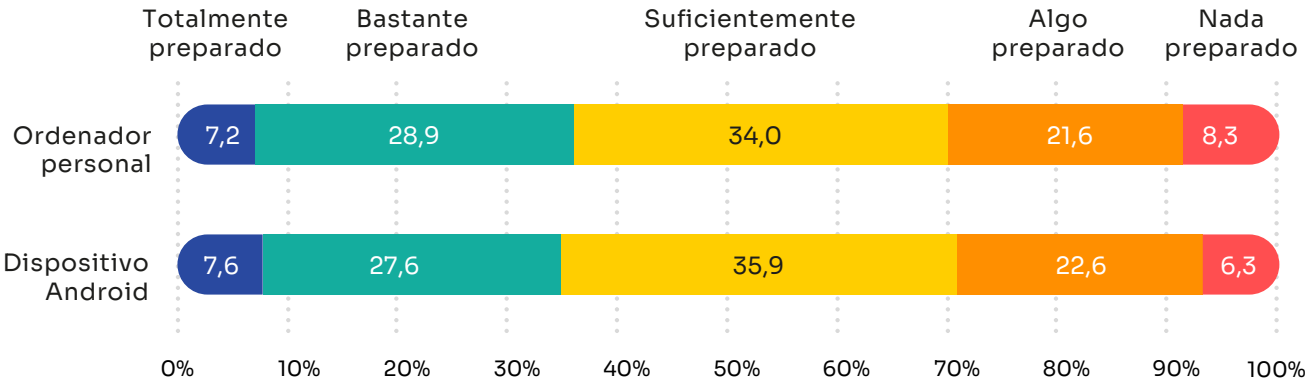
Gráfico 47 - **Percepción de la preparación para afrontar posibles problemas de ciberseguridad (%)**



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

Casi el 30% de la población usuaria de Internet considera que está poco o nada preparada para afrontar posibles problemas de ciberseguridad

Gráfico 48 - **Percepción del nivel de preparación para afrontar posibles problemas de ciberseguridad en el ordenador del hogar versus dispositivo móvil (%)**



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

Si distinguimos por tipo de dispositivo, llegamos a resultados similares (Gráfico 48). La percepción sobre el nivel de preparación para afrontar posibles problemas de ciberseguridad en el ordenador del hogar o en dispositivo móvil es similar.

Los gráficos 49 y 50 muestran esta distinción por género. Los datos se miden en relación con su ordenador personal (Gráfico 49) y con su dispositivo Android (Gráfico 50) para después compararlos con los resultados del análisis con Pinkerton.

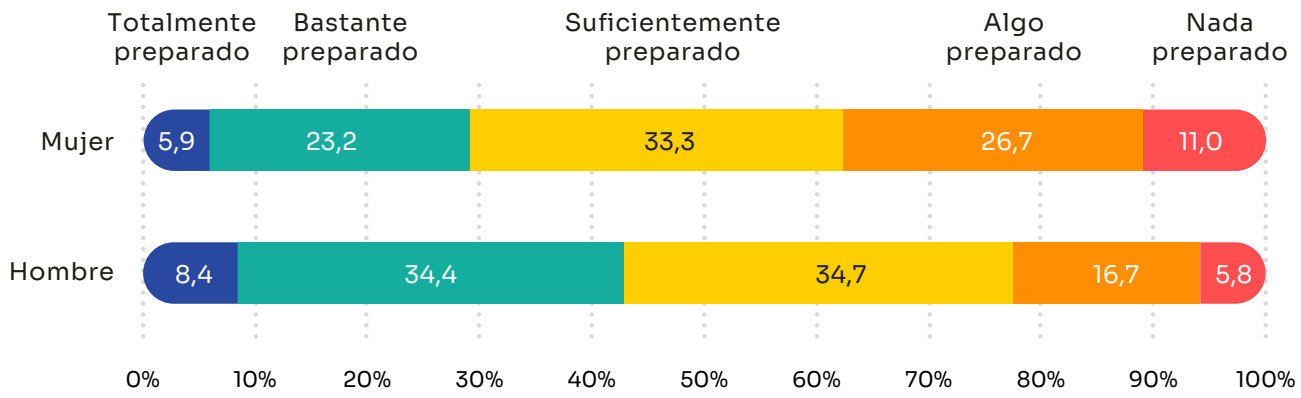
La proporción de mujeres que indica sentirse poco o algo preparadas para enfrentarse a ciberriesgos es mayor que la de hombres en la misma situación. En concreto, un 11% de mujeres se considera poco preparada y un 26,7% se siente algo preparada, en comparación con un 5,8% y un 16,7% respectivamente en el caso de los hombres.

Ocurre lo contrario con las declaraciones de bastante y total preparación viéndose un porcentaje masculino superior al femenino. Concretamente 34,4% y 8,4% de hombres bastante y totalmente preparados frente al 23,2% y 5,9% de mujeres total y bastante preparadas.

La situación es similar para los dispositivos Android (Gráfico 50), donde las mujeres que reportan estar total o bastante preparadas para usar dispositivos Android son menos que los hombres que afirman lo mismo (42,3% hombres, frente a 28,4% mujeres).

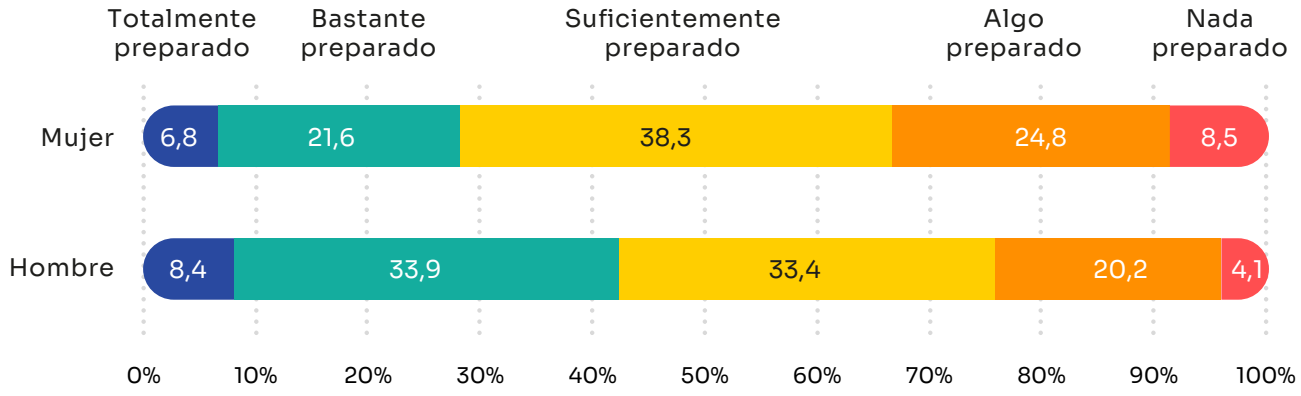
Estos datos se concluyen en que los hombres declaran sentirse más preparados que las mujeres a la hora de afrontar posibles problemas de ciberseguridad.

Gráfico 49 - **Preparación para afrontar posibles problemas de ciberseguridad en el ordenador del hogar (diferenciado por género)**



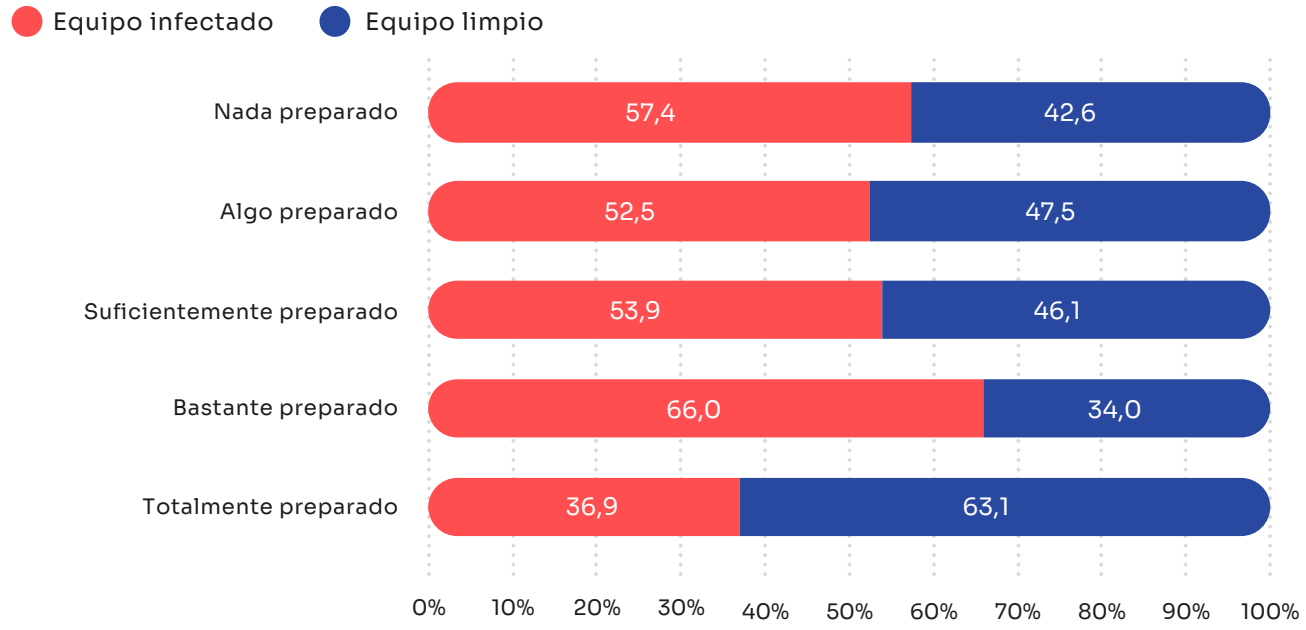
Base: Total de usuarios y usuarias de ordenador
Fuente: Panel hogares, ONTSI

Gráfico 50 - **Preparación para afrontar posibles problemas de ciberseguridad en dispositivos Android (diferenciado por género)**



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

Gráfico 51 - **Percepción del nivel de preparación para afrontar los riesgos de ciberseguridad de usuarios de ordenador versus infección de los ordenadores del hogar (%)**



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

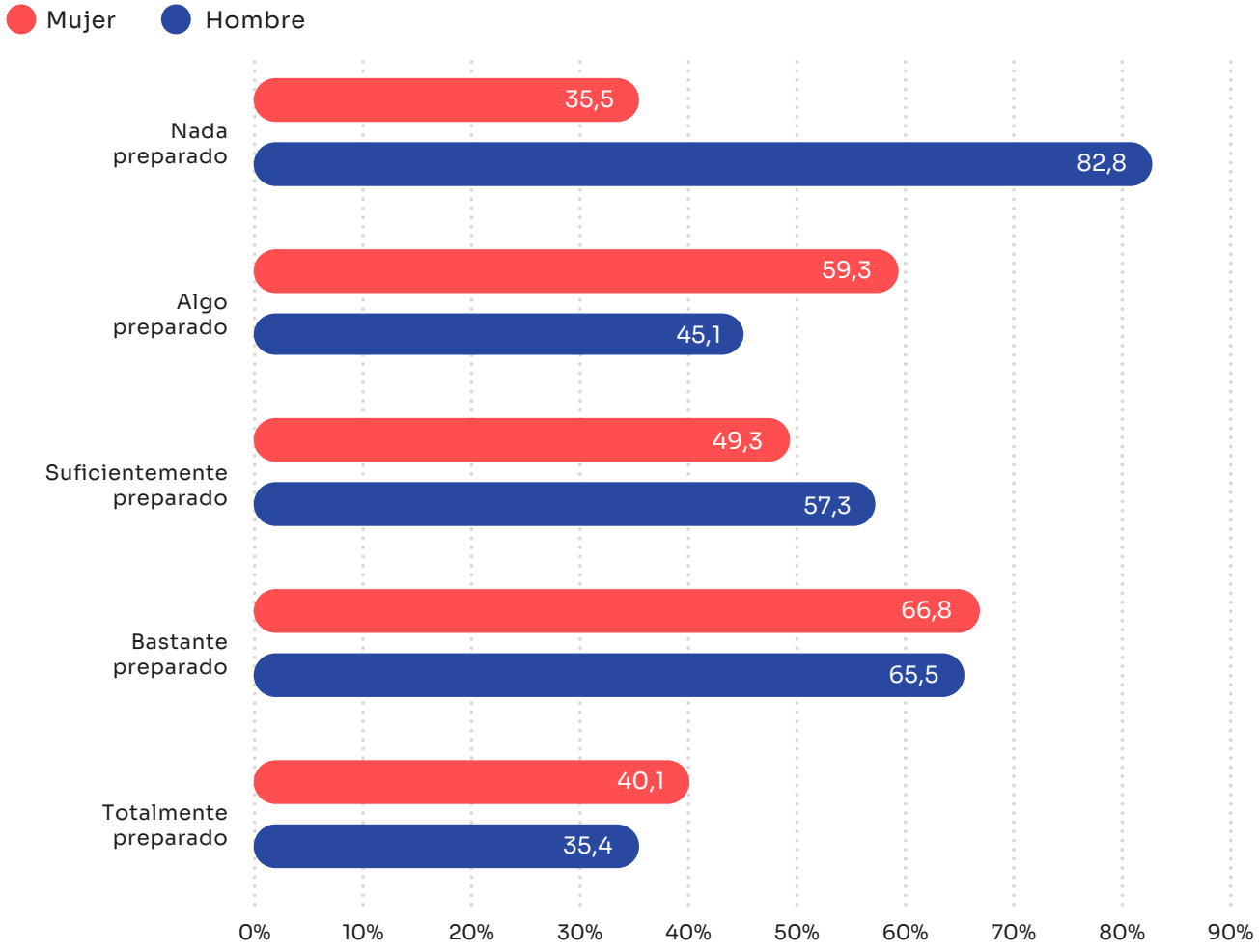
Tras conocer la opinión de las personas usuarias, también se analizan los desafíos de la ciberseguridad y la seguridad real (aquella reflejada por los datos de Pinkerton) para PC y dispositivos Android, respectivamente.

En casi todos los niveles de percepción se encuentran ordenadores con *software* dañino o malicioso. Específicamente, el 36,9% de las personas que utilizan ordenadores que consideran estar totalmente preparadas tienen dispositivos infectados. Sin embargo, aquellas que se encuentran en esta categoría presentan mejores resultados en cuanto a la salud de sus dispositivos. Es importante destacar que las demás categorías de percepción muestran niveles de infección por encima del 50%.

Si separamos por género el porcentaje de ordenadores infectados, obtenemos las siguientes lecturas (Gráfico 52). Según los datos obtenidos con Pinkerton, el 82,8% 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. En el caso de las mujeres este porcentaje se reduce al 35,5%.

En general, todas las personas usuarias enfrentan problemas de *malware* en sus equipos, y aunque su nivel de preparación varía, cuando comparamos los resultados entre hombres y mujeres, se observa que las mujeres tienen menos infecciones en sus ordenadores en el nivel de “nada preparado”. Sin embargo, en el nivel de “totalmente preparado”, el porcentaje de *software* maligno en los ordenadores es mayor en las mujeres, con un aumento de 4,7 puntos porcentuales en comparación con los hombres.

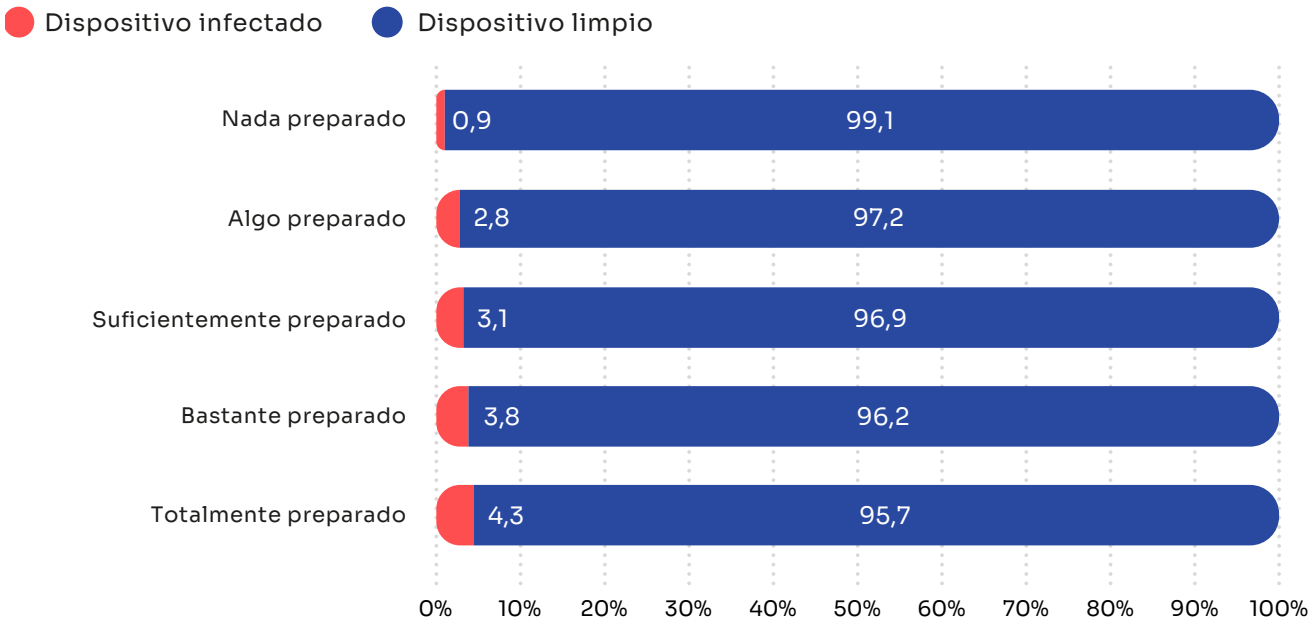
Gráfico 52 - **Porcentaje de ordenadores infectados según nivel de preparación autopercibido para afrontar los riesgos de ciberseguridad (desagregado por género)**



Base: Total de usuarios con ordenador infectado
Fuente: Panel hogares, ONTSI

El 36,9% de las personas que se consideran totalmente preparadas, junto con el 66% de las que creen estar bastante preparadas en ciberseguridad tienen sus equipos infectados

Gráfico 53 - **Porcentaje de dispositivos Android infectados según las declaraciones sobre el nivel de preparación para afrontar los riesgos de ciberseguridad (%)**



Base: Total de usuarios con dispositivo Android
Fuente: Panel hogares, ONTSI

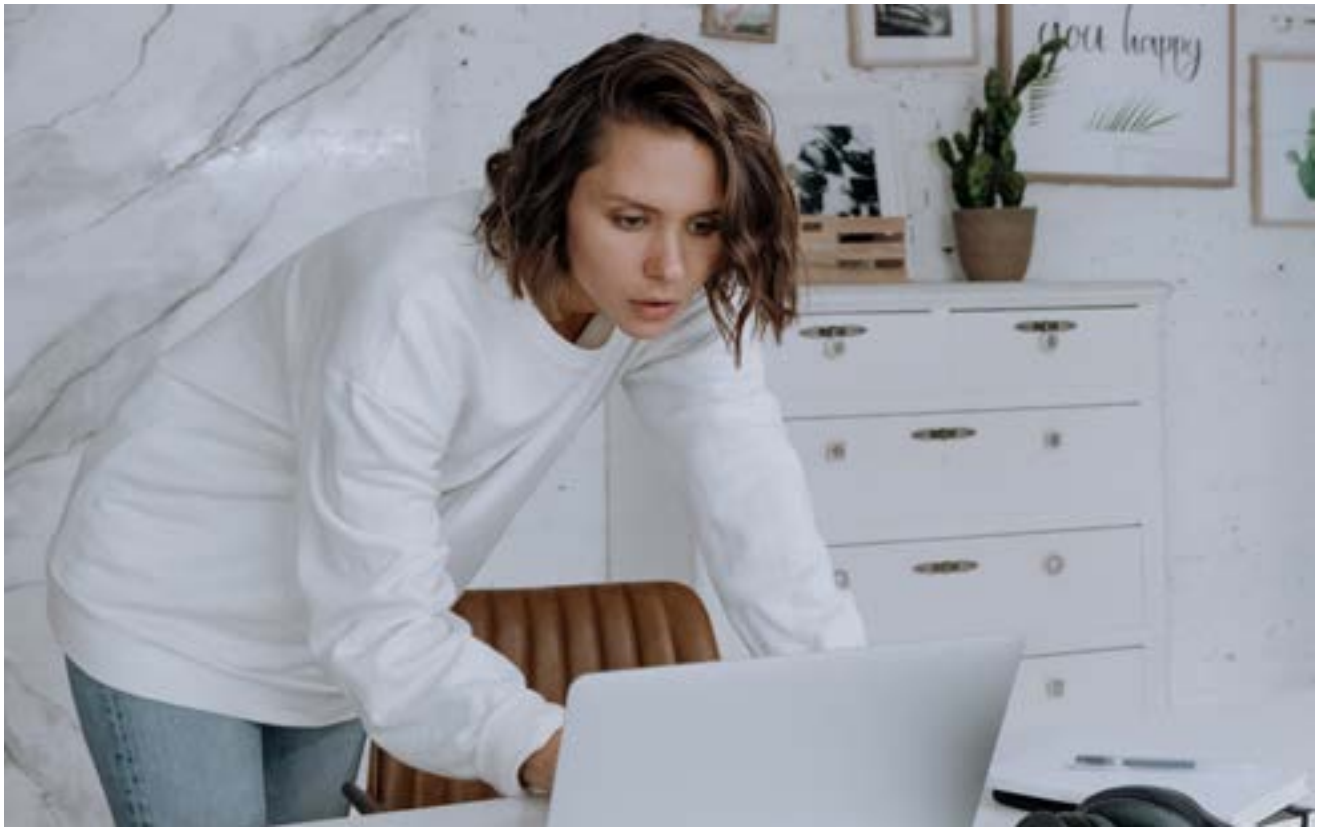
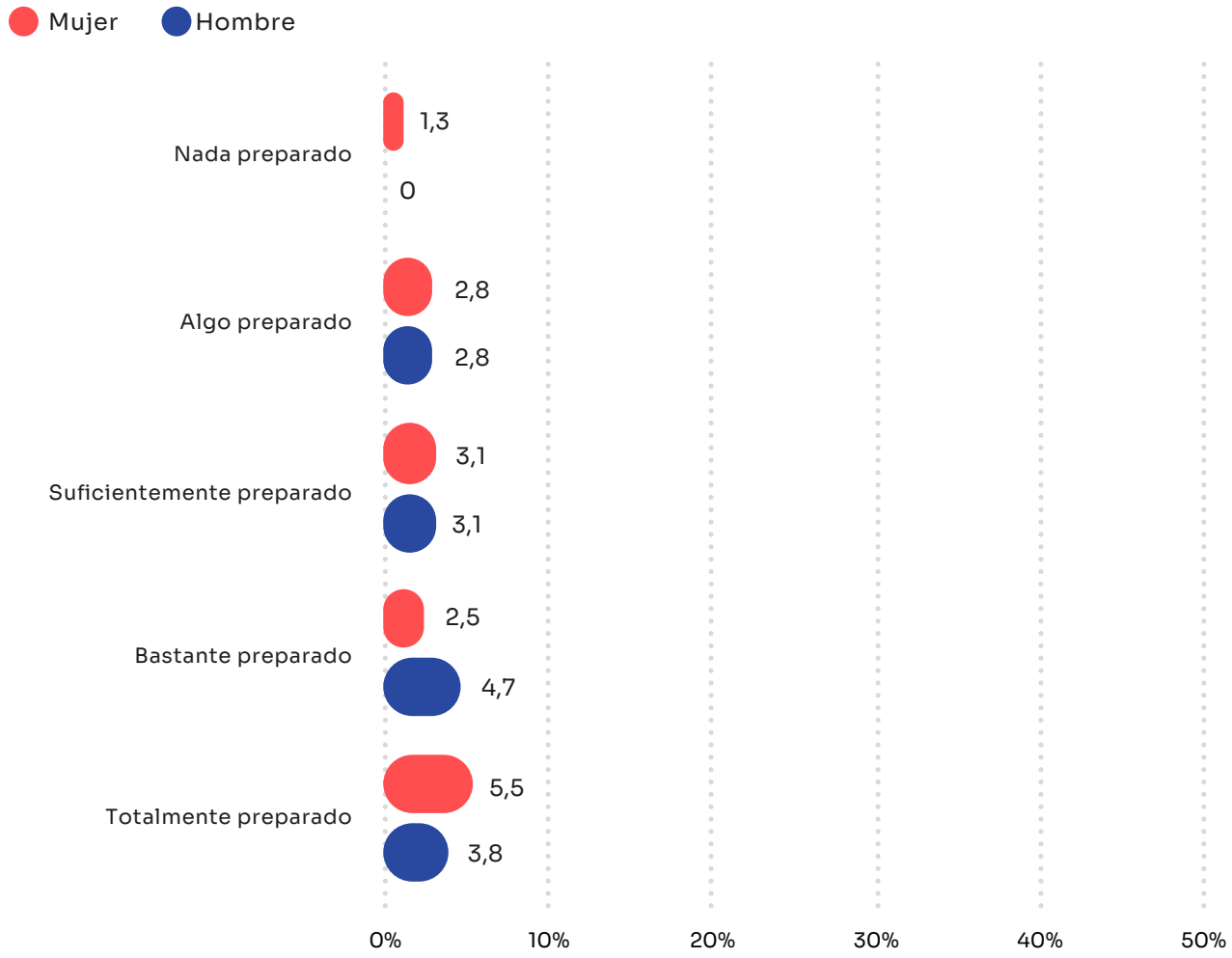


Gráfico 54 - **Declaraciones sobre el nivel de preparación para afrontar los riesgos de ciberseguridad de usuarios de Android con dispositivos infectados (desagregado por género)**



Base: Total de usuarios con dispositivo Android infectado
Fuente: Panel hogares, ONTSI

En el caso de los dispositivos Android (Gráfico 53), es oportuno resaltar el hecho de que fue detectado mucho menos *malware* que en los ordenadores. Las personas con este tipo de dispositivos que se consideran totalmente preparadas tienen dispositivos infectados (4,3%). Sorprende observar, que quienes declaran no encontrarse preparados o solo algo preparados tienen menor porcentaje de dispositivos infectados.

Esto podría ser debido a que quienes creen contar con más preparación asuman mayores conductas de riesgo en línea, causando infecciones en sus dispositivos.

La cantidad de amenazas que afrontan tanto los dispositivos móviles como los ordenadores es elevada y frecuente, por lo que es importante tener una capacitación adecuada en formación de seguridad para el uso normal y diario.

En esta ocasión, también es posible percibir diferencias en cuanto al género. Aunque es cierto que se observa que el nivel de infección entre los que se declaran “algo preparado” y “suficientemente preparado” son parejos entre géneros, no sucede lo mismo entre los usuarios que se perciben bastante preparados o totalmente preparados.

Los que se consideran bastante preparados y tienen una mayor tasa de infección en sus dispositivos suelen ser hombres, mientras que ellas presentan mayor nivel de infección en sus dispositivos Android cuando se consideran totalmente preparadas (Gráfico 54).

6.4. Necesidades formativas en ciberseguridad

Uno de los recursos más importantes para evitar conductas de riesgo es la formación. Ante la pregunta de si se cree necesitar formación en ciberseguridad en los próximos años, más de la mitad, el 50,8%, afirma que la formación en ciberseguridad es bastante o muy necesaria (Gráfico 55). Combinado con el 39,8% que dijo que necesita algo de formación. Estos datos constatan que la gran mayoría de la ciudadanía usuaria piensa que la formación en ciberseguridad es necesaria en mayor o menor medida.

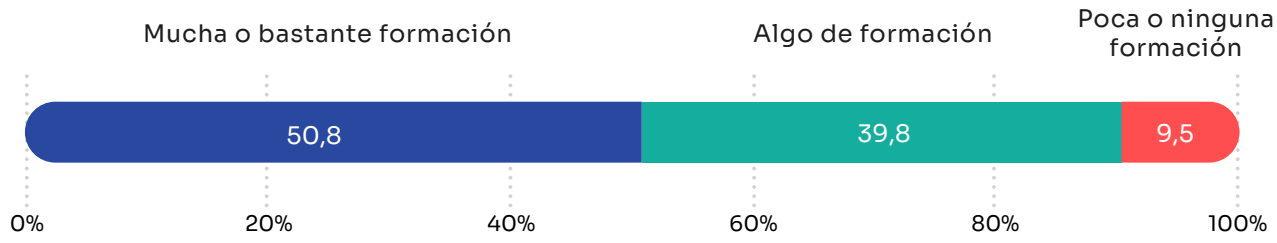
De acuerdo con los resultados analizados a través de la investigación, es aún más importante conocer los peligros que uno puede enfrentar y cómo mitigarlos. La mejor manera de enfrentarlos es a través de una base de conocimiento técnico bien establecida.

La digitalización sin ciberseguridad es una barrera técnica grande, muy difícil o imposible de superar sin una formación adecuada adaptada a los diferentes grupos demográficos.

Entidades públicas como INCIBE en su pagina web www.incibe.es tienen numerosos recursos y material formativo dirigidos a la ciudadanía, empresas y el entorno del menor.

[14] http://www.is4k.es/programas/programa-de-jornadas-escolares

Gráfico 55 - **Percepción sobre necesidad de formación en ciberseguridad (%). 1S22**



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

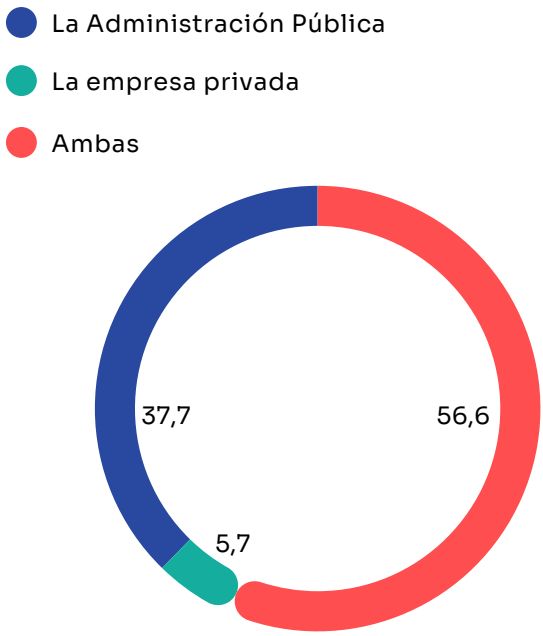
6.5. Entidades que buscan impulsar la ciberseguridad

Es interesante escuchar las opiniones respecto a los agentes que tratan de impulsar iniciativas de ciberseguridad. En este contexto, se preguntó si los gobiernos, las empresas privadas o ambos deberían liderar estas iniciativas. En el gráfico 56 se encuentra la relación.

El 56,6% cree que tanto el gobierno como las empresas privadas deberían impulsar los esfuerzos de ciberseguridad. Un porcentaje inferior (37,7%) piensa que solo debe venir del gobierno, y finalmente un 5,7% de las personas usuarias piensa que el impulso debe venir solo de las empresas privadas.

De hecho, los resultados implícitamente avalan los esfuerzos que se están realizando por todos los organismos con competencias en ciberseguridad para impulsar la cultura de esta materia y conseguir que tanto la ciudadanía como las empresas tengan más conocimiento de los riesgos y de la necesidad de invertir en ciberseguridad.

Gráfico 56 - **Opiniones sobre los agentes que deberían impulsar las iniciativas en materia de ciberseguridad (%)**



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

En este sentido, cabe destacar que en la Estrategia Nacional de Ciberseguridad 2019[15] hay una línea de acción específica para impulsar la ciberseguridad de ciudadanos y empresas, y se indica, que la seguridad cibernética es una responsabilidad compartida con los actores privados y no es posible conseguirla sin su participación. Por ese motivo, en julio de 2020 se constituyó un Foro Nacional de Ciberseguridad[16] para dar respuesta a las dudas y preocupaciones que se asocian a la ciberseguridad en un entorno de colaboración global, iniciativa liderada por el Consejo de Seguridad Nacional.

Este Foro está integrado por representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

[15] Estrategia de Ciberseguridad 2019: https://foronacionalciberseguridad.es/

[16] Mas información:
Foro Nacional de Ciberseguridad - Inicio (foronacionalciberseguridad.es) https://foronacionalciberseguridad.es/
Estrategia Nacional de Ciberseguridad 2019 | DSN https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

07

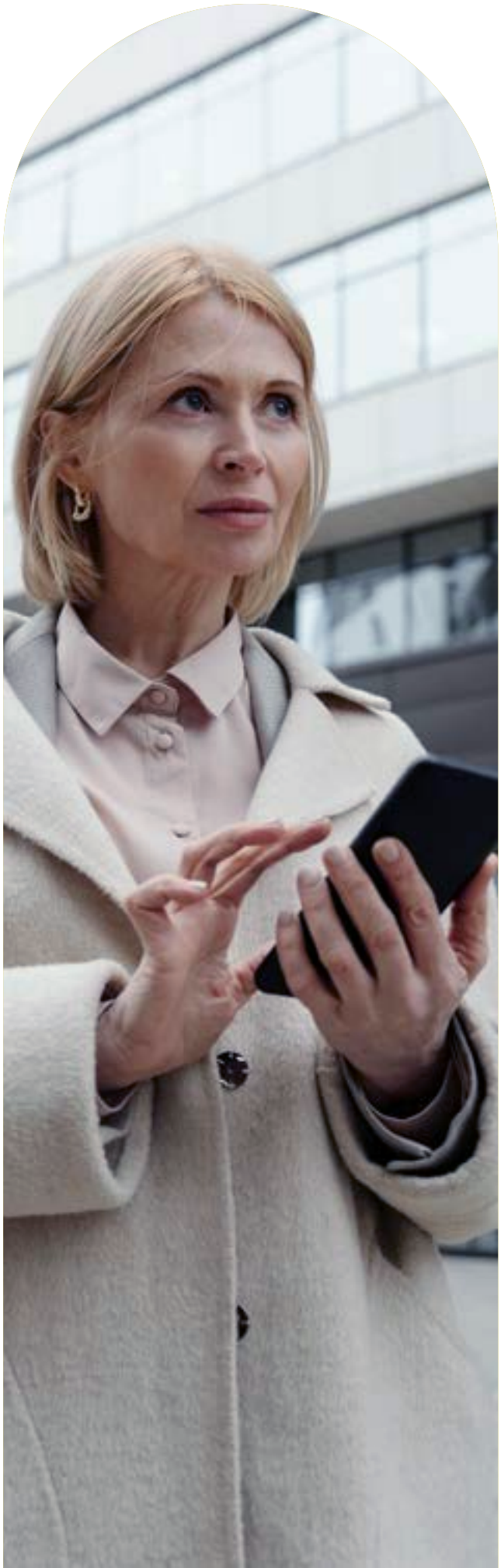
Conclusiones

Este estudio recoge los resultados de **hábitos de navegación, utilización de servicios y medidas de seguridad en Internet durante el primer semestre de 2022**, además de percepciones relacionadas con la confianza, la formación y la capacidad para afrontar amenazas. Asimismo, algunas de estas mediciones se han contrastado con la monitorización remota autorizada de dispositivos para evaluar su estado real.

Los hábitos recogidos se han podido ver afectados **por las consecuencias de la pandemia de COVID-19 y los recientes cambios en el panorama internacional que han influido a todos los niveles**. Entre ellos, las consecuencias de la crisis humanitaria y económica a causa del conflicto bélico entre Rusia y Ucrania, que ha desencadenado una subida generalizada de precios, además de incrementar la sensibilización a amenazas tales como los ciberataques y la desinformación.

Con tales matices, se ha podido observar que los servicios más favorecidos en lo que a popularidad se refiere, se encuentran **las redes sociales, mensajería instantánea y acceso a la banca *online***; junto a un descenso en el consumo de contenidos gratuitos que siguen potenciando la infección por *malware*.

Además, **la acelerada digitalización de los últimos años y el crecimiento de la Administración electrónica** ha derivado en un aumento del uso del certificado digital o el DNI electrónico para realizar trámites en línea. Situación que se ha visto favorecida por múltiples campañas de la Administración para promover y facilitar el uso consciente de medios telemáticos.



Ha disminuido en el uso de servicios gratuitos en línea que arriesgan al usuario a sufrir brechas de ciberseguridad. Sin embargo, la aplicación de medidas para salvaguardar el bienestar en los dispositivos aún tiene un amplio margen de mejora. Tanto en lo referido a ordenadores del hogar, como a dispositivos móviles. Aunque las declaraciones recopiladas muestran que la mayoría de las medidas básicas de seguridad se utilizan con mayor frecuencia, todavía es necesario promover la implementación de soluciones más avanzadas, como el uso de máquinas virtuales y el cifrado de datos del dispositivo.

En cuanto a los ordenadores del hogar, es destacable la necesidad de actualizar a su última versión el sistema operativo, junto a los parches de seguridad. Además, se recomienda implementar otra clase de medidas como evitar desactivar el cortafuegos y añadir una capa de seguridad adicional al dispositivo utilizando *software* antivirus. Esto a menudo refleja cómo se confía erróneamente en la **seguridad predeterminada** del dispositivo. Las medidas automáticas ayudan a proteger el ordenador, pero no excluyen las medidas manuales o no automáticas (como el uso de contraseñas seguras, programas anti-spam o anti-fraude).

Un alto porcentaje de hogares tienen redes wifi; 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 contar con una red del hogar segura**. Debemos también ser conscientes de los riesgos que implica el conectarnos a redes de terceros bajo las que no tenemos control o conocimiento alguno, práctica bastante habitual aún hoy en día.

Entre otros medios para proteger su red, una de las formas más apremiantes es cambiar la contraseña del panel de administración del rúter de su hogar y evitar las contraseñas predeterminadas de la red wifi doméstica. Otro método muy recomendado es habilitar una lista de direcciones físicas (MAC) para que solo los

dispositivos agregados puedan acceder a su red. **Es necesario hacer más difícil el acceso a la red de un posible atacante malintencionado**. Una vez que un ciberdelincuente accede a una red repleta de dispositivos solo tiene que encontrar uno vulnerable para intentar ganar más accesos, a veces, incluso de forma automatizada. De esta manera 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 que podrían acarrear serias consecuencias para el dueño de la maquinaria.

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 realmente 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 falta de libertad que conlleva el *software* de terminales móviles y los permisos limitados por defecto hacen que la ratio de vulnerabilidad de estos terminales sea menor. Aun así, contrasta el hecho de que, aunque sea sencillo mantenerlos actualizados o evitar la instalación desde fuentes desconocidas, el usuario medio suele fracasar para acometer este tipo de mantenimiento.

Respecto a la percepción de la **capacidad de la ciudadanía para afrontar los posibles problemas de seguridad**, en general es relativamente optimista, aunque es necesario solventar algunos problemas detectados en esta materia. Por ejemplo, aún se ignoran muchas medidas de seguridad básicas y existe un desconocimiento abundante declarado sobre entidades y campañas de ciberseguridad. Además, pese a que un segmento importante de la población se considere preparado, las métricas de infección lo desmienten, probando así que **la preparación real es bastante inferior a la declarada**.

Se observan los resultados a raíz de las **campañas impulsadas por la Administración pública, que están contribuyendo positivamente al cambio**, hacia una comunidad *online* más consciente y preparada para afrontar los riesgos de ciberseguridad. Esto se ha hecho notar en el aumento de uso de líneas de ayuda con relación a incidencias. No obstante, quedan muchos aspectos que mejorar para que el total de la ciudadanía tenga la formación necesaria en materia de ciberseguridad.[16]

[16] Recomendaciones de Ciberseguridad 2022: https://www.osi.es/es/actualidad/blog/2022/03/04/estas-recomendaciones-de-ciberseguridad-te-interesan

08

Principales cifras de un vistazo

MEDIDAS DE SEGURIDAD

- **La mayoría de la población usuaria de ordenador utiliza medidas de seguridad automáticas, aunque una porción significativa no es consciente de ello**. El 14,7% declara no usar permisos reducidos, cuando los datos de sus dispositivos reflejan que el 100% si los usa. De la misma forma, el 27,7% declara utilizar *firewall* cuándo en realidad es el 97% quien lo usa.

- Las máquinas virtuales y el cifrado de datos siguen siendo prácticamente invisibles para el grueso de la población con un 6,2% y 6,5%, respectivamente.

- **Las actualizaciones del sistema operativo y los programas antivirus siguen siendo las medidas más declaradas**. Encabezan las encuestas en lo que a popularidad se refiere, pero siguen sin alcanzar el 60% y, en la realidad siempre quedan por debajo los datos comprobados que los declarados.

- **Los hombres usan dispositivos móviles más actualizados.** El 43,4% de los dispositivos Android de ellos están actualizados, frente al 38,8% de los de ellas. Aunque con menor diferencia, ocurre lo contrario en el caso de los ordenadores del hogar, teniendo los hombres un 38,7% de los sistemas actualizados frente al 40% de las mujeres.

ORDENADORES Y DISPOSITIVOS INFECTADOS

- **Los incidentes de seguridad declarados se mantienen en torno al 60% durante el último semestre** (aumentan algo más de 5 p.p. respecto al año anterior). La recepción de correos no solicitados o deseados (*spam*) es con diferencia, el problema de seguridad más frecuente. No obstante, este dato ha descendido 4,5 p.p. respecto al año anterior y se sitúa en el 80,4% de quienes han tenido un problema de seguridad.

- **Más de la mitad de los ordenadores analizados están infectados por *malware*, pero muy pocas personas son consciente**s. Hay mayor proporción de ordenadores contagiados entre los hombres que entre las mujeres, 59,4% frente a 52,9%. Un 70,2% de los ordenadores y de dispositivos Android infectados sufrieron ataques por *malware* de alta peligrosidad.

- **Las personas que usan ordenadores del hogar tienden a ser optimistas en cuanto a la infección: hay más contagios de los que se declaran**. Solo el 5,6% cree estar infectado con algún tipo de *malware*; la realidad es que el 56,6% de los dispositivos analizados lo estaba.

FORMACIÓN Y PREPARACIÓN ANTE INCIDENTES

- **El 40% de las personas usuarias declara realizar alguna conducta de riesgo conscientemente y el 37,5% reconoce navegar sin saber si tienen al día las actualizaciones.** El 33,4% descarga ficheros de sitios web de dudosa reputación, y un 32,8% instala aplicaciones o programas de *markets* o páginas no oficiales.

- **En cuanto a formación en ciberseguridad**, el 91,6% de los panelistas considera que necesita formación en ciberseguridad en mayor o menor medida.

- **La percepción del nivel de preparación ante problemas de ciberseguridad entre quienes usan ordenador y terminales Android es alta**. Solo el 7,6% de las personas que usan terminales Android y el 7,2% de las que usan ordenador declara no tener preparación ante los ataques. Destaca el porcentaje de quienes declaran contar con preparación suficiente para afrontar algún problema de ciberseguridad en su dispositivo Android (35,9%) o en su ordenador personal (34,0%).

- **El 40,1% de las mujeres que declara sentirse totalmente preparada para afrontar riesgos de ciberseguridad, tiene su ordenador infectado**. Este porcentaje es del 35,4% en el caso de los hombres. Ocurre parecido con quienes aseguran estar solamente algo preparadas; el 59,3% tiene su equipo contagiado frente al 45,1% de hombres.

- **Quienes usan terminales Android que dicen tener mayor preparación sobre riesgos de ciberseguridad, tienen en realidad mayores niveles de infección en su equipo**. Quienes piensan que están algo (2,8%) o nada (0,9%) preparados o preparadas son quienes tienen un porcentaje de infecciones menor en su dispositivo Android. Quienes se consideran totalmente o bastante preparados alcanzan porcentajes de infección del 4,3% y 3,8%, respectivamente.

09

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 miden, clasifican y analizan las métricas de seguridad que implementan los usuarios en los ordenadores del hogar y en sus dispositivos móviles y la incidencia de estos riesgos y su peligrosidad, además de su grado de confianza en las nuevas tecnologías y su necesidad de formación.

El estudio se realiza a usuarios y usuarias españoles de Internet mayores de 15 años con acceso a Internet desde el hogar (al menos una vez al mes).

El tamaño muestral del estudio es de 3.620 encuestados y encuestadas e igual número de dispositivos analizados, 816 de estos dispositivos son ordenadores PC/Portátiles, 2.262 smartphone y 542 tabletas.

En concreto, en este documento se ofrece un análisis sobre los datos recabados en el primer semestre de 2022. 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[17]: 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 y recogen 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 en Internet. 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 enero hasta julio de 2022, ambos meses inclusive.

[17] 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

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es | ontsi
incibe_