OBSERVACIBER

CÓMO SE PROTEGE LA CIUDADANÍA ANTE LOS CIBERRIESGOS

ESTUDIO SOBRE PERCEPCIÓN Y NIVEL DE CONFIANZA EN ESPAÑA

Edición Abril 2022

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
ontsi Observatorio Nacional de Tecnología y Sociedad
incibe_
OBSERVACIBER

ÍNDICE

OBSERVACIBER

Módulo I:
Servicios usados en Internet

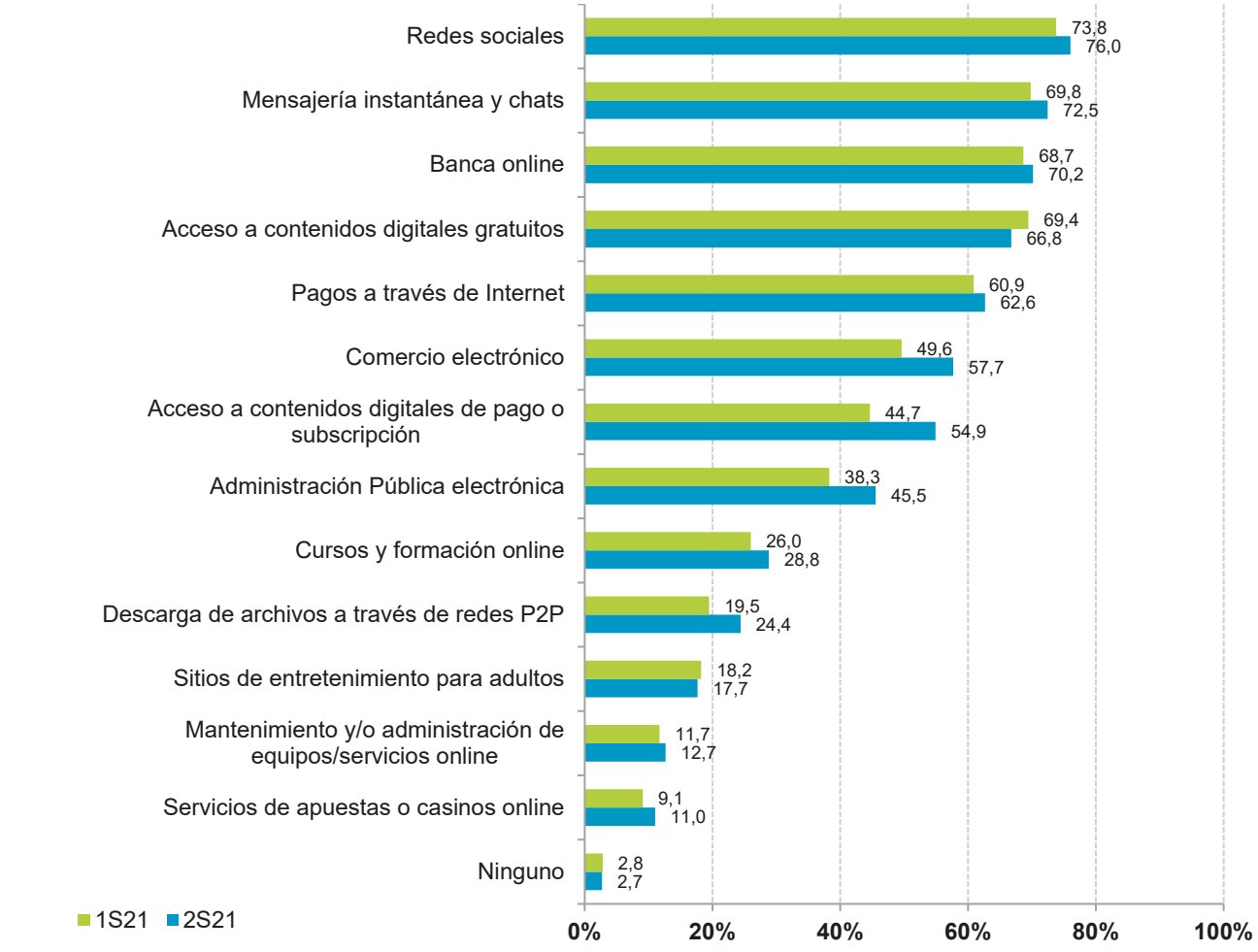
Módulo I: Servicios usados en Internet

Servicios ofrecidos por Internet que han sido utilizados por el usuario en el último semestre

Según declaraciones de los panelistas, en el segundo semestre de 2021 han utilizado en mayor medida los servicios ofrecidos por Internet.

Cabe destacar tres servicios. El comercio electrónico (57,7%), el acceso a contenidos digitales de pago o suscripción (54,9%) y la administración pública electrónica (45,5%).

Además, los cursos y formación online siguen aumentando, situándose en el 28,8%.



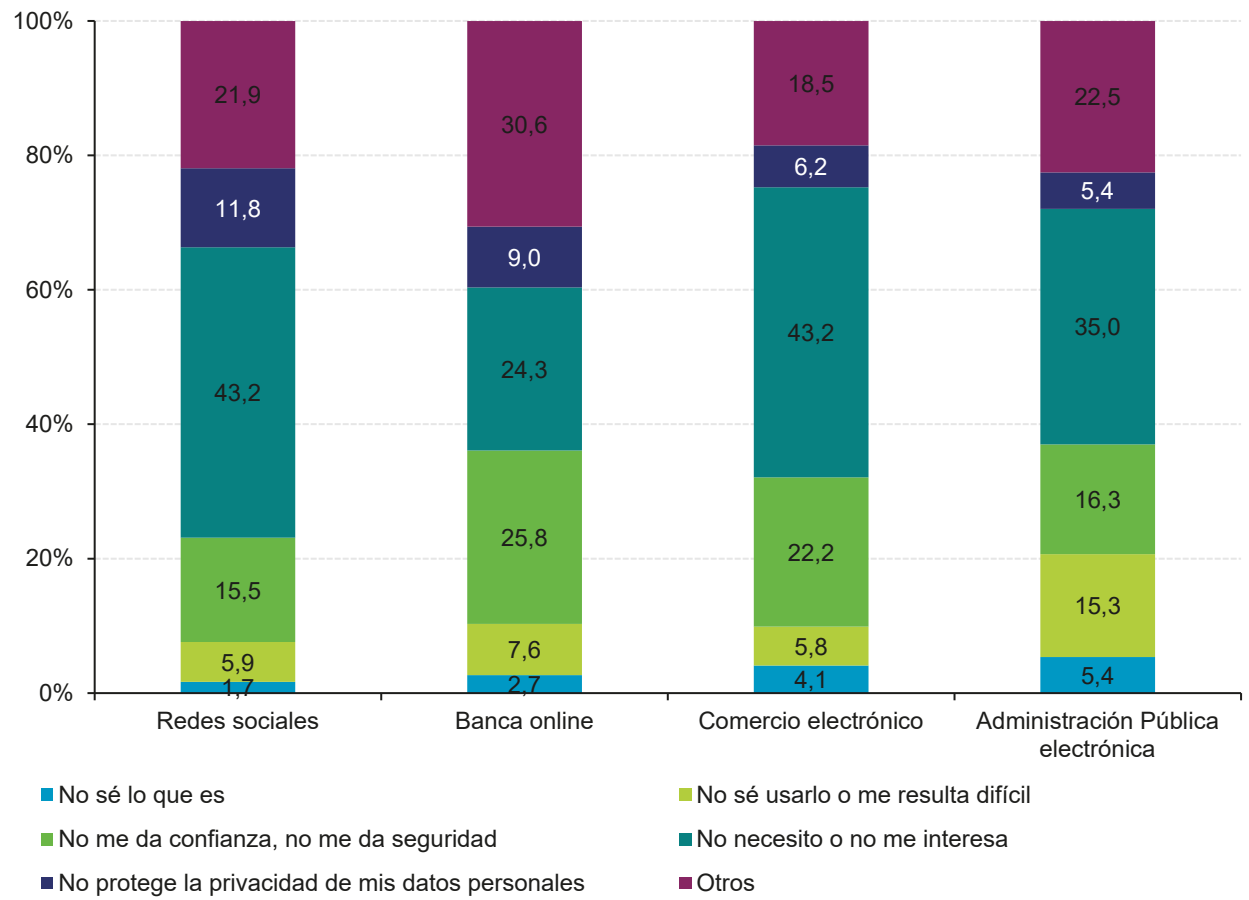
Base: Total usuarios

Módulo I: Servicios usados en Internet

Motivos de no utilización de los servicios ofrecidos por Internet

Pese al incremento del comercio electrónico en el último años tras la pandemia, el 43,2% de los usuarios entrevistados no esta interesado en realizar sus compras online. Esto quizás pueda ser debido al aumento de las estafas por Internet y el desconcierto que generan para el usuario.

Respecto a la utilización de la banca online tan solo el 25,8% de los usuarios afirma que le provoca desconfianza el uso de este servicio sin embargo el porcentaje de usuarios que desconocen los servicios de la banca online es mínimo, el 2,7% de los entrevistados.



Base: Usuarios que no utilizan alguno de los servicios

Módulo I: Servicios usados en Internet

Necesidad de registro como usuario para el acceso o descarga de contenido gratuito.

La privacidad del usuario es importante, por eso es necesario controlar los lugares donde se comparten los datos. En este sentido, hay páginas en las que para poder descargar o acceder al contenido que ofrecen, solicitan el registro del usuario en el que se piden de forma obligatoria ciertos datos como el nombre y apellidos, fecha de nacimiento, sexo etc. El 36,8% de los usuarios entrevistados afirma que en la mayoría de los portales a los que ha accedido, le han pedido que se registre.

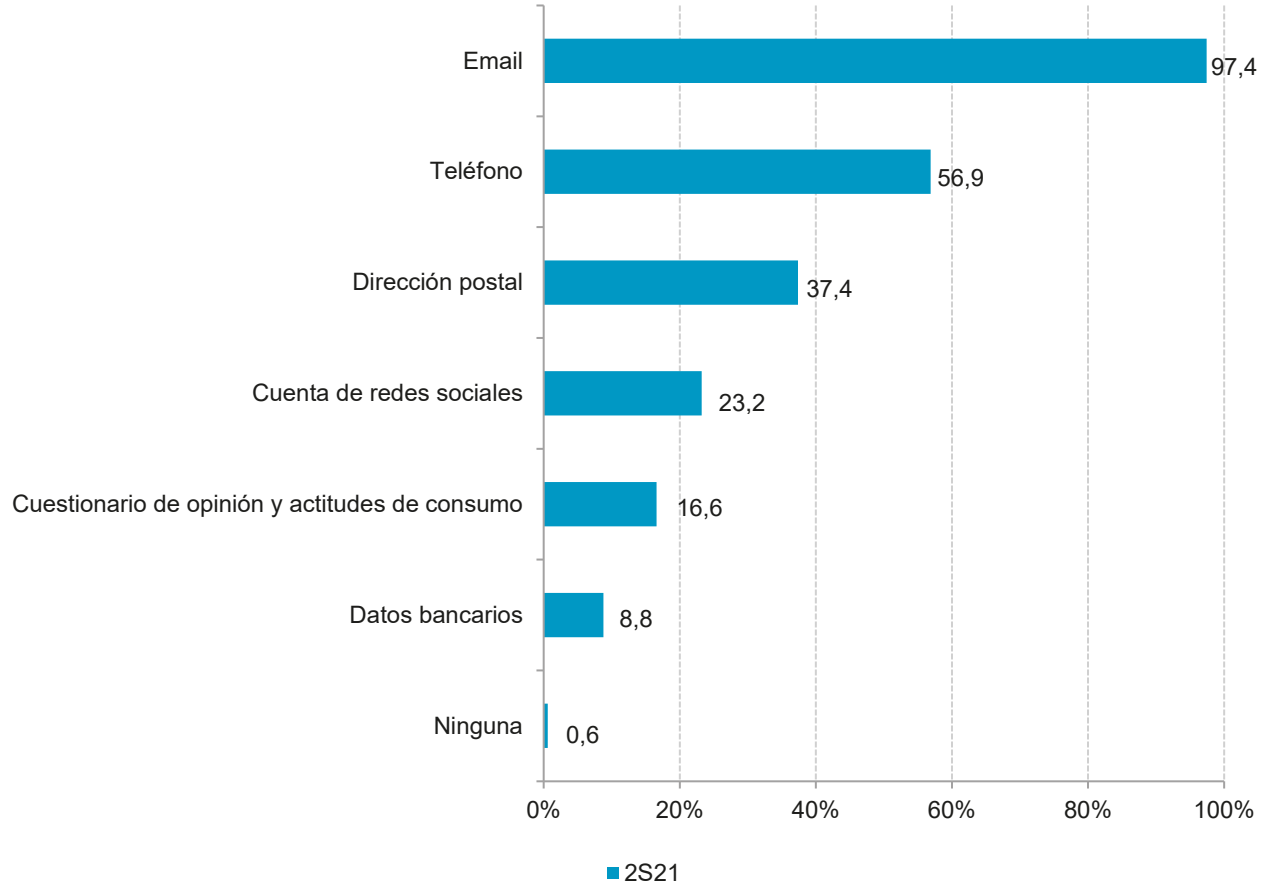
BASE: Usuarios que acceden o descargan contenido gratuito.

Módulo I: Servicios usados en Internet

Datos solicitados para completar los registros en portales de descarga de contenido gratuito

De entre los principales datos solicitados a los usuarios para el registro en dichas páginas, destacan la dirección de email y el teléfono, precisamente dos datos que se emplean asiduamente para los tipos de fraude.

Los panelistas de este estudio declaran que el 97,4% han tenido que dar su email y más de la mitad del total de entrevistados han tenido que facilitar su teléfono.



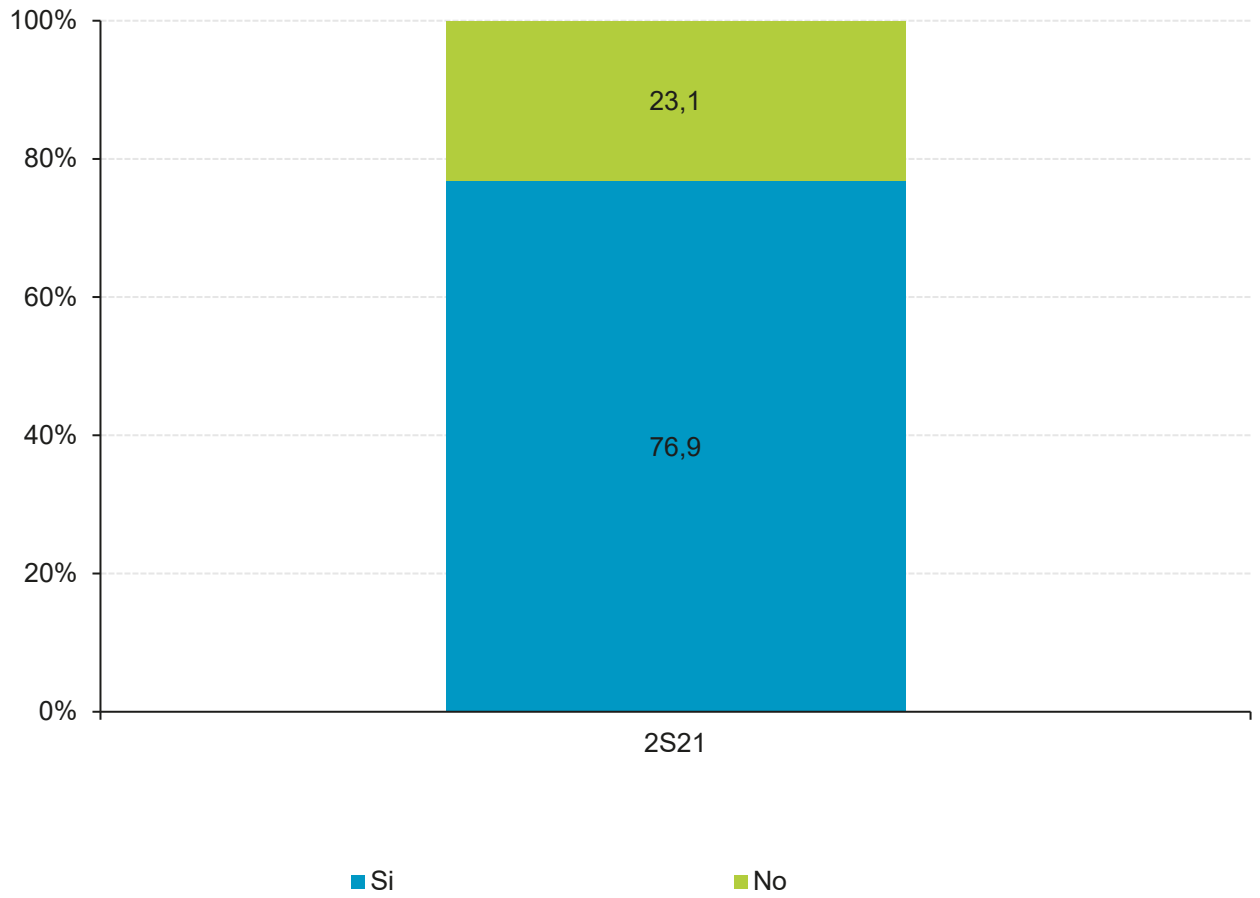
Base: Usuarios que se registran en portales de descarga de contenido gratuito

Módulo I: Servicios usados en Internet

Incremento de la publicidad tras la utilización de los accesos gratuitos

Compartir o ceder los datos de navegación a páginas que ofrecen contenido gratuito puede conllevar al uso de esos datos para ofrecer publicidad relativa a esos datos que se han consultado.

La cesión de estos datos y su posible posterior venta a terceros se traduce en un aumento significativo de la publicidad no deseada, declarada por el 76,9% de los usuarios.



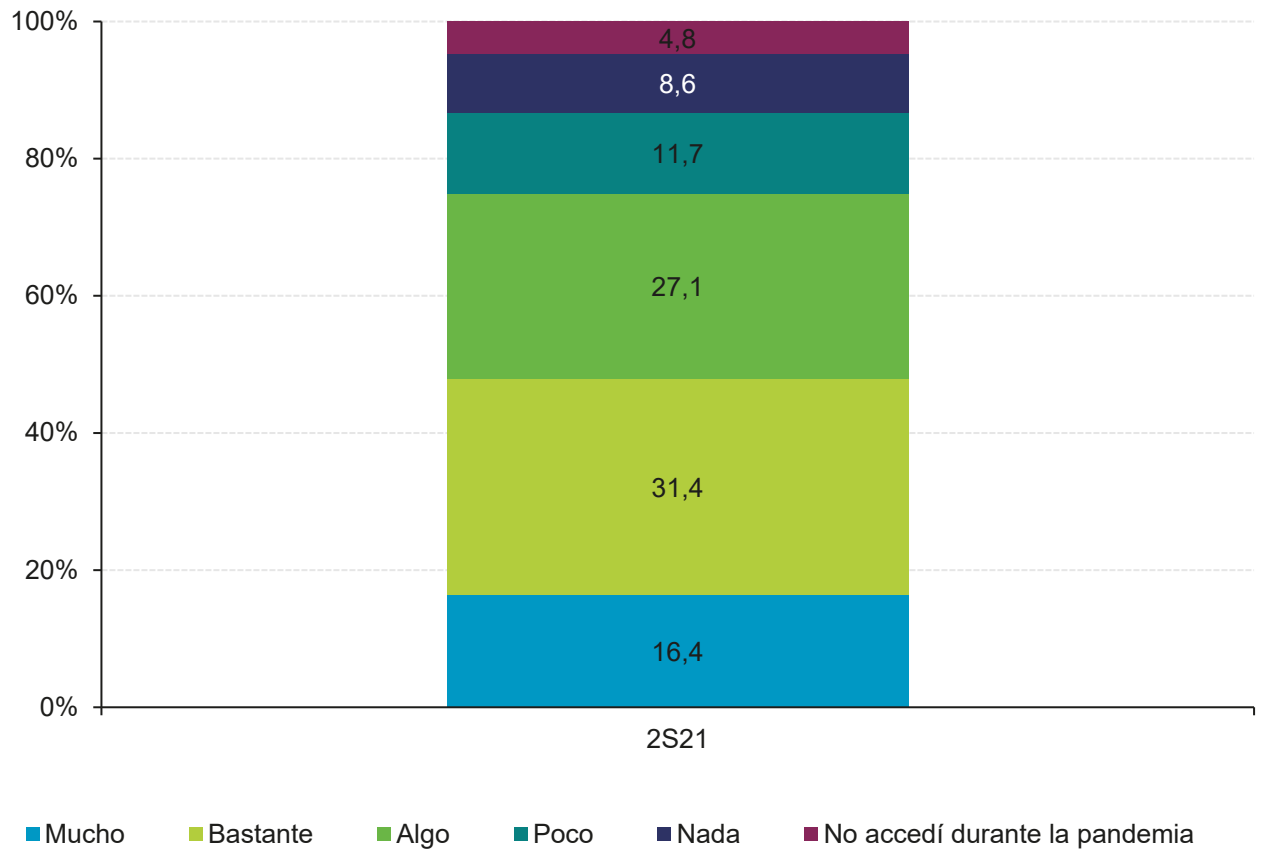
BASE: Usuarios que acceden o descargan contenido gratuito.

Módulo I: Servicios usados en Internet

Acceso o descarga de contenidos digitales gratuitos durante la pandemia

Durante la pandemia el 31,4% de los usuarios que participan en este estudio afirma haber accedido o descargado bastante contenido digital gratuito y el 27,1 declara haber descargado algo.

Quizás sea debido a los largos periodos de confinamiento y a la búsqueda de entretenimiento derivada de estar todo el día encerrados en casa, o del bombardeo de noticias en medios y redes sociales con la temática de la pandemia. Puede que estos usuarios buscaran contenido diferente para abstraerse de la situación que se estaba viviendo en ese momento.



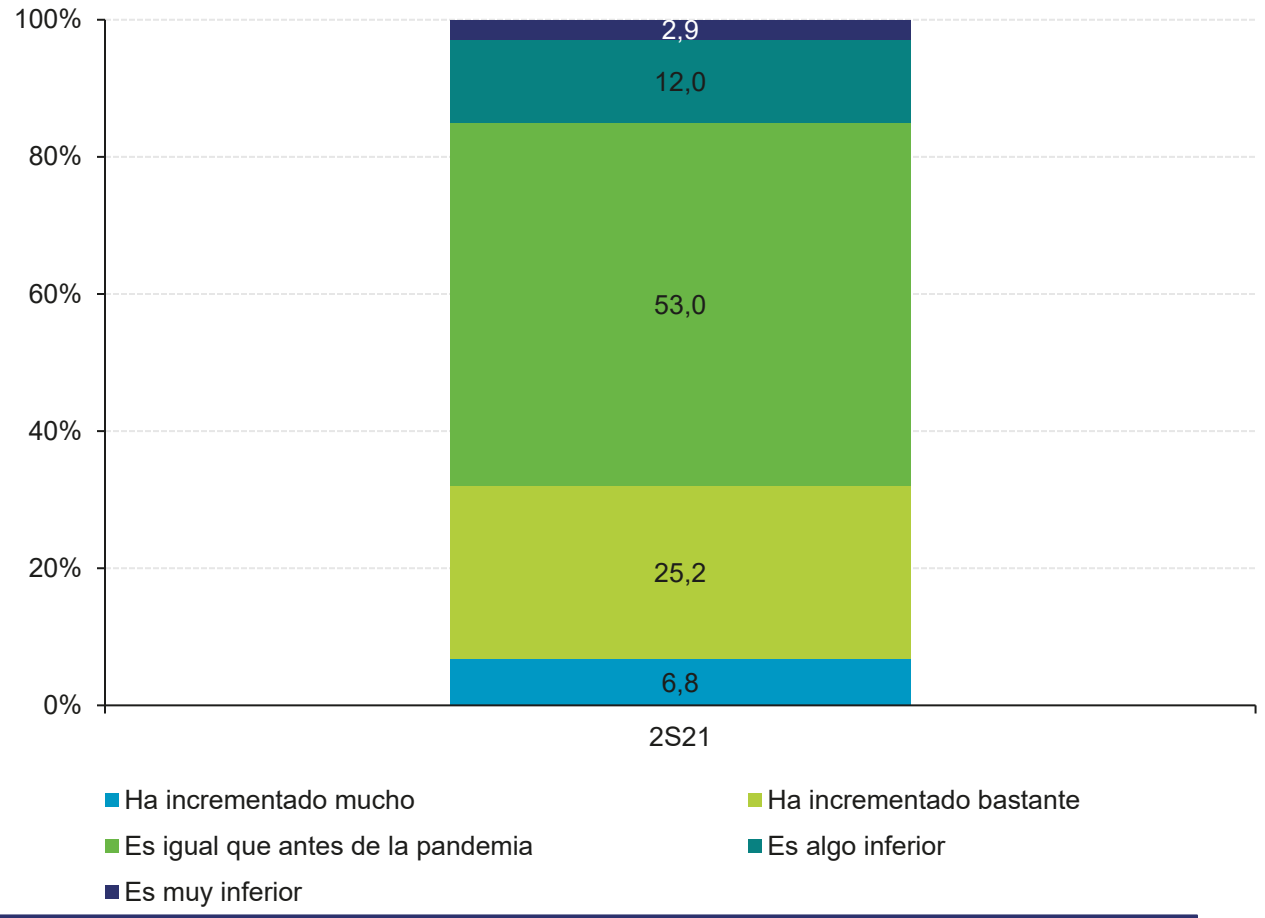
BASE: Todos los usuarios

Módulo I: Servicios usados en Internet

Acceso o descarga de contenidos digitales gratuitos tras la pandemia

Tras la pandemia el 53% de los panelistas continúa recurriendo de forma ocasional a las descargas gratuitas, manteniendo los mismos hábitos que durante la pandemia.

Tan sólo el 14,9% manifiesta disminuir las descargas frente al 32% restante que ha aumentado las descargas.

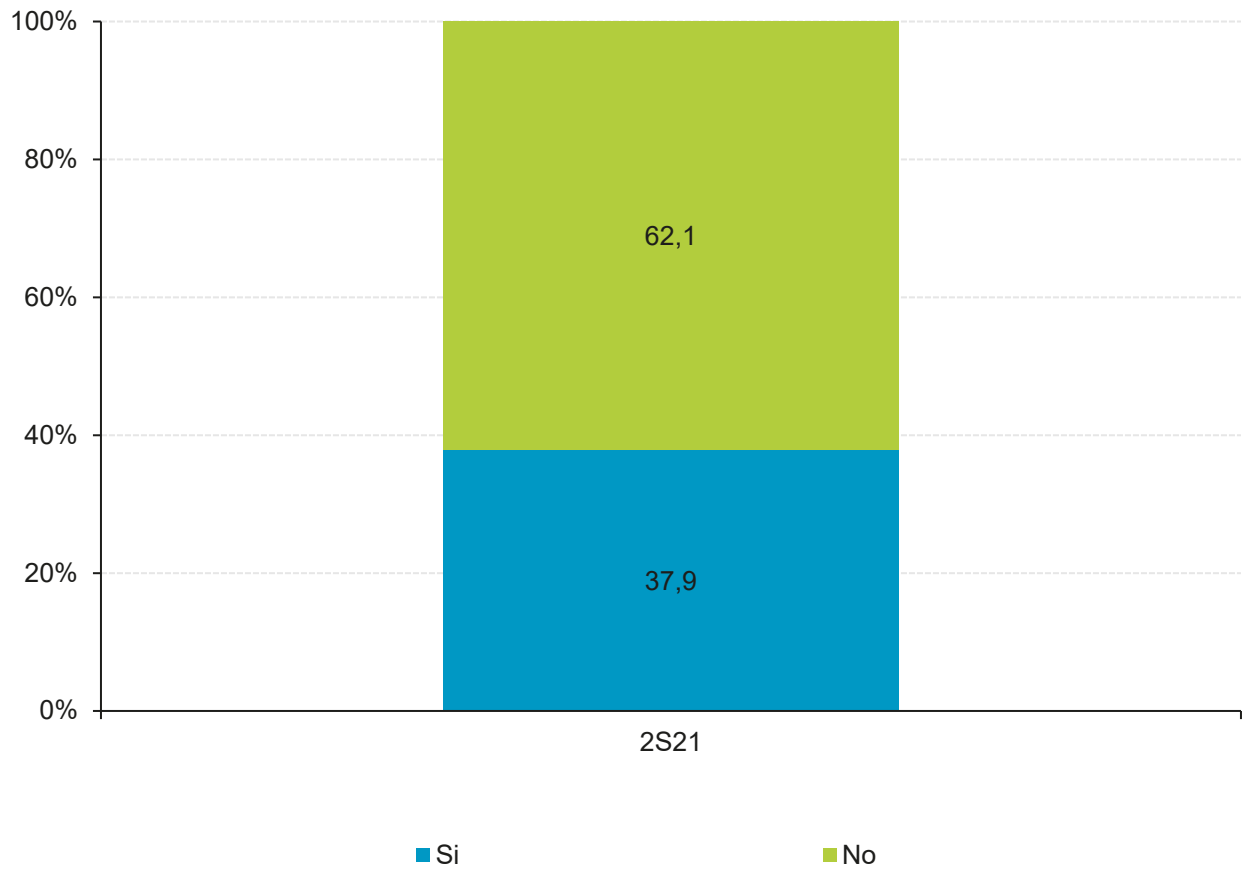


BASE: Todos los usuarios.

Módulo I: Servicios usados en Internet

Nuevas suscripciones a plataformas de pago durante el confinamiento

El 37,9% de los usuarios entrevistados, se suscribió a una o más plataformas de pago durante el confinamiento de 2020. Quizás motivados por el encierro y la búsqueda de contenido como entretenimiento y distracción para sobrellevar la crisis sanitaria.



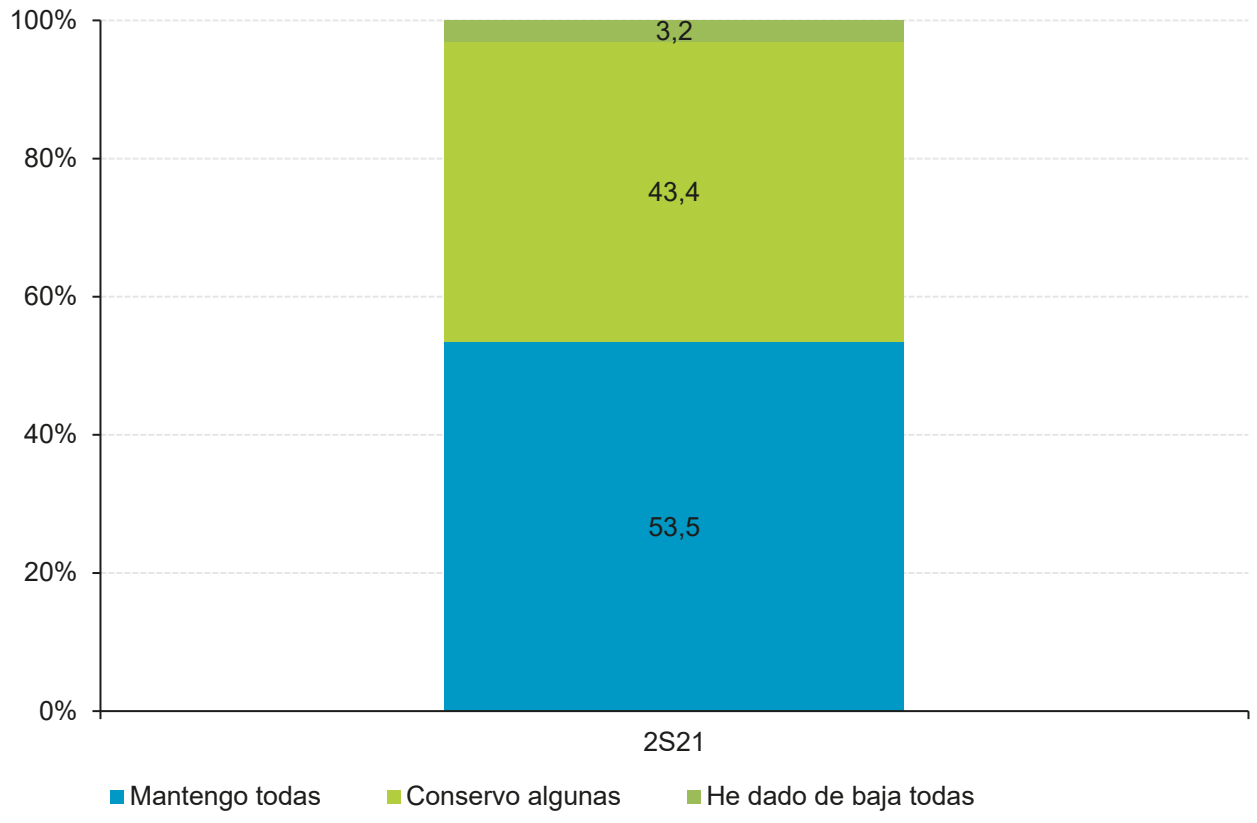
BASE: Todos los usuarios.

Módulo I: Servicios usados en Internet

Mantiene las suscripciones a plataformas de pago realizadas durante el confinamiento

Cabe destacar que el 53,5% de los usuarios mantiene las suscripciones a todas las plataformas de pago que contrataron durante la situación de confinamiento en 2020 debido a la crisis sanitaria provocada por la COVID-19.

Mientras que el 43,4% de usuarios dieron de baja algunas, aunque siguen conservando otras.



BASE: Usuarios que realizaron alguna suscripción nueva a plataformas de pago.

Módulo II:
Medidas y hábitos de seguridad en Internet

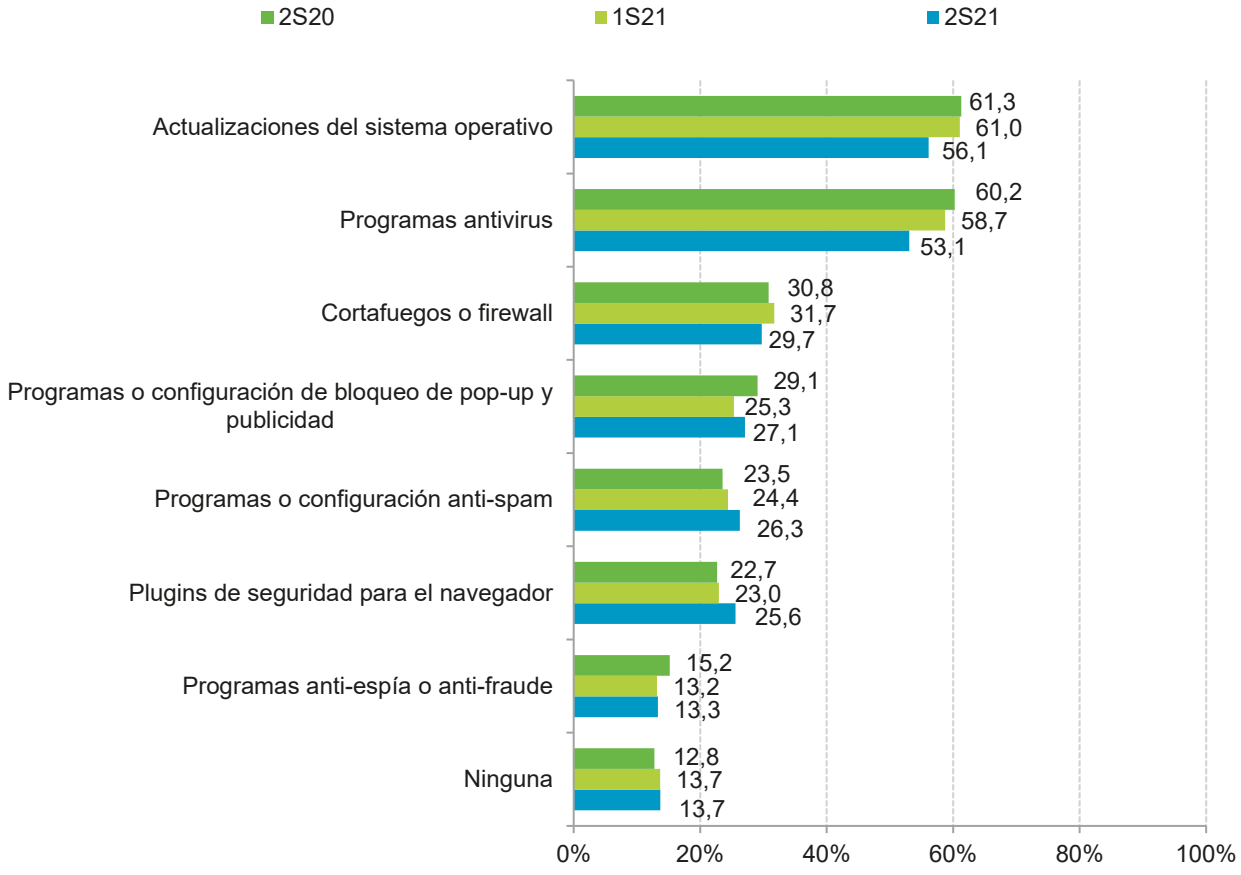
Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad automatizables en el ordenador del hogar

Un menor porcentaje de usuarios declara emplear equipos actualizados, programas antivirus y cortafuegos, disminuyendo respectivamente 4,1 p.p., 5,6 p.p. y 2 p.p. Los usuarios podrían bien desinstalar estos programas, por ejemplo por dificultar la ejecución de algún otro software o afectar a su rendimiento, aunque en muchos casos si son programas nativos del sistema podrían volver a activarse ya sea automáticamente o tras una actualización.

La funcionalidad de los programas antivirus no se limita únicamente a eliminar el malware presente en el equipo informático. Su cometido más importante es prevenir y evitar las infecciones de malware.

Vídeo: Antivirus. ¿cómo nos protegen?
https://youtu.be/f8FWKR7YUq0



Base: Usuarios de PC

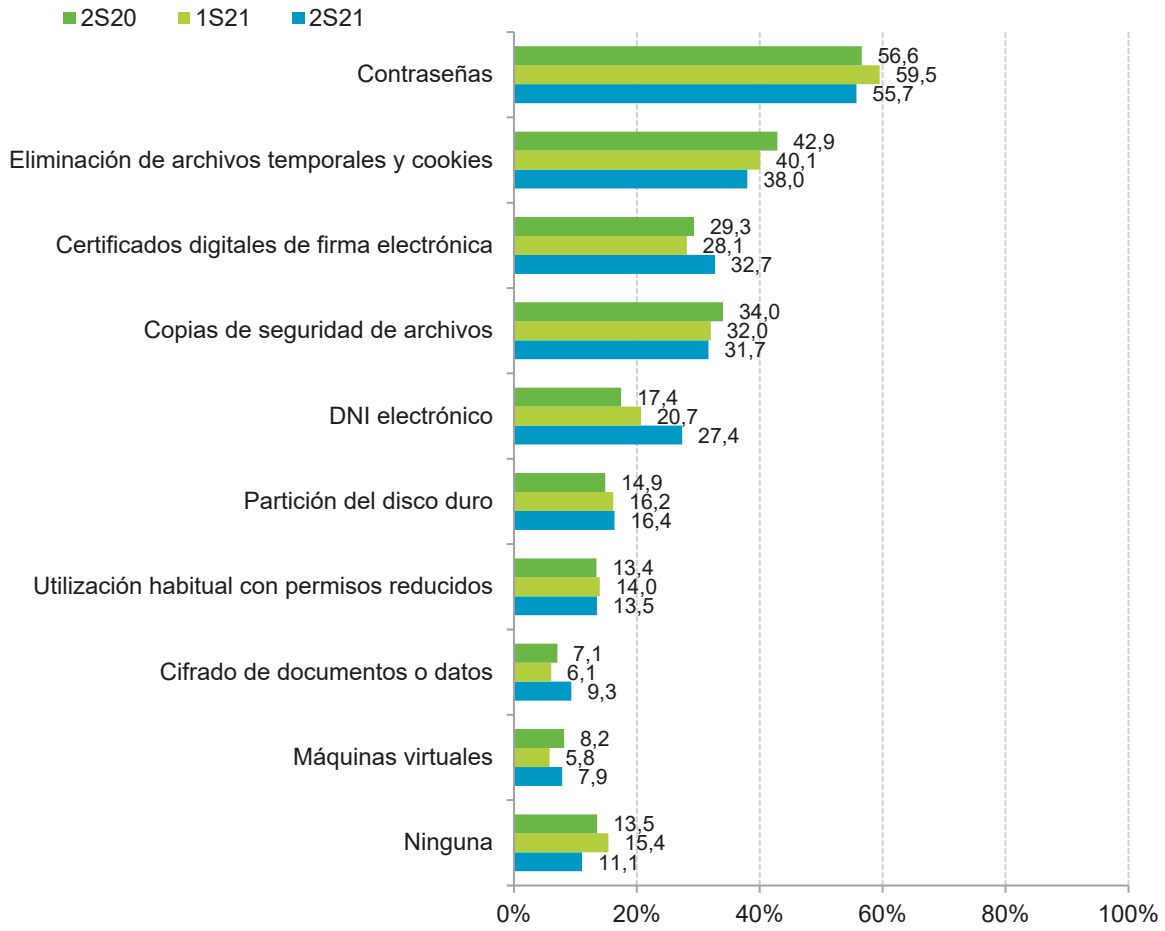
Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad activas o no automatizables en el ordenador del hogar

En el segundo semestre de 2021 destaca que mayor número de internautas declara hacer uso del DNI electrónico (27,4%), y también del certificado digital (32,7%). El aumento de la realización de trámites online con la administración puede ser uno de los motivos del aumento respecto del semestre anterior del uso del DNI electrónico (6,7 p.p.) y del certificado digital (4,6 p.p.) como medidas de seguridad. Esto es así debido a que para realizar esos trámites es necesario identificarse por alguno de esos medios o bien cl@ve o PIN.

Es muy importante gestionar correctamente las contraseñas y, además, realizar copias de seguridad de los datos que queremos salvaguardar. Obtén más información sobre cómo realizar estas tareas:

- ✓ ***Contraseñas:*** *https://www.osi.es/es/campanas/contrasenas-seguras*
- ✓ ***Copias de seguridad:*** *https://www.osi.es/es/campanas/copias-cifrado-informacion*

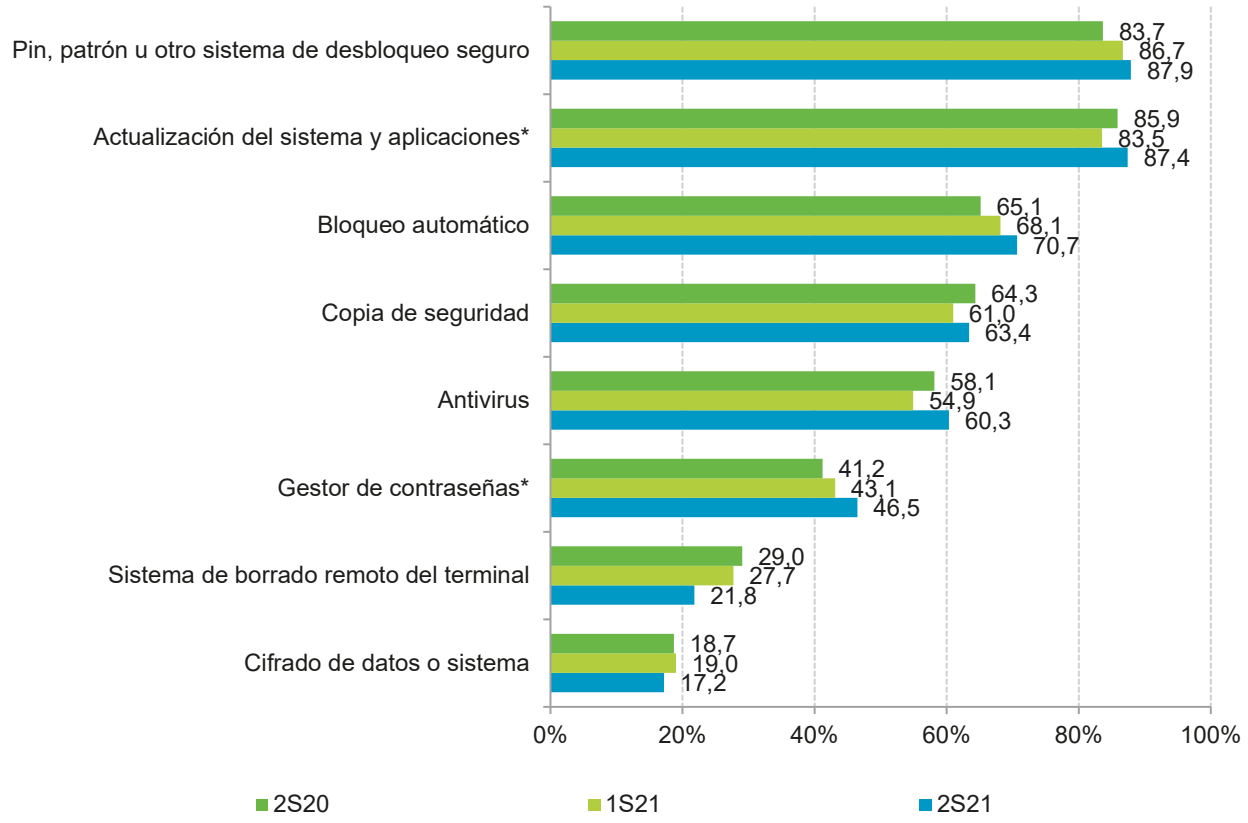


Base: Usuarios de PC

Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad en dispositivos Android

La medida de seguridad más popular es el uso del pin, patrón u otro sistema de desbloqueo seguro. De hecho, durante el segundo semestre de 2021 el 87,9% de los internautas declara usarlo (+1,2 p.p. respecto al semestre anterior). Este aumento puede deberse al aumento del uso de la banca electrónica y a que los panelistas declaran utilizar más asiduamente los medios de pago contactless en tiendas físicas.



*nuevas categorías

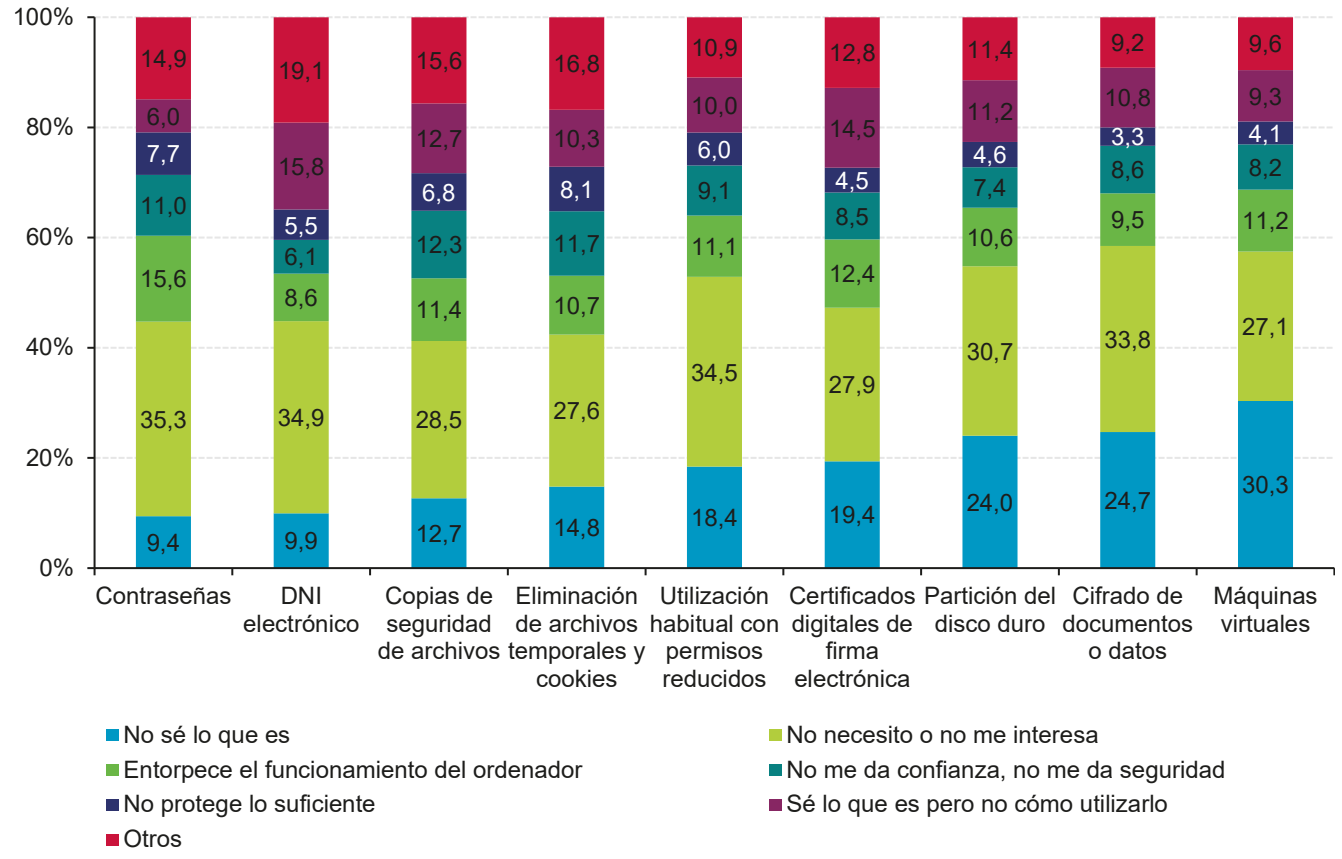
Base: Usuarios que disponen de dispositivo Android

Módulo II: Medidas y hábitos de seguridad en Internet

Motivos de no utilización de medidas de seguridad

Las máquinas virtuales siguen siendo un gran desconocido para el 30,3% de los usuarios entrevistados.

Mientras que el 34,9% no ve necesario el uso del DNI electrónico. Esto quizás pueda ser debido a que en su lugar emplean el certificado digital. Ya que se puede ver que el certificado digital hay menos usuarios que han respondido que no lo necesitan o no les interesa. El aumento de los trámites con la administración ha dado lugar a que más usuarios necesiten usar el DNI electrónico y el certificado digital para poder identificarse. Esto hace que respecto al semestre anterior disminuya el número de panelistas que desconocen o no les interesan estos medios de identificación digital.



Base: Usuarios de PC que no utilizan alguna de las medidas de seguridad

Módulo III:
Hábitos de comportamiento en la navegación y uso de Internet

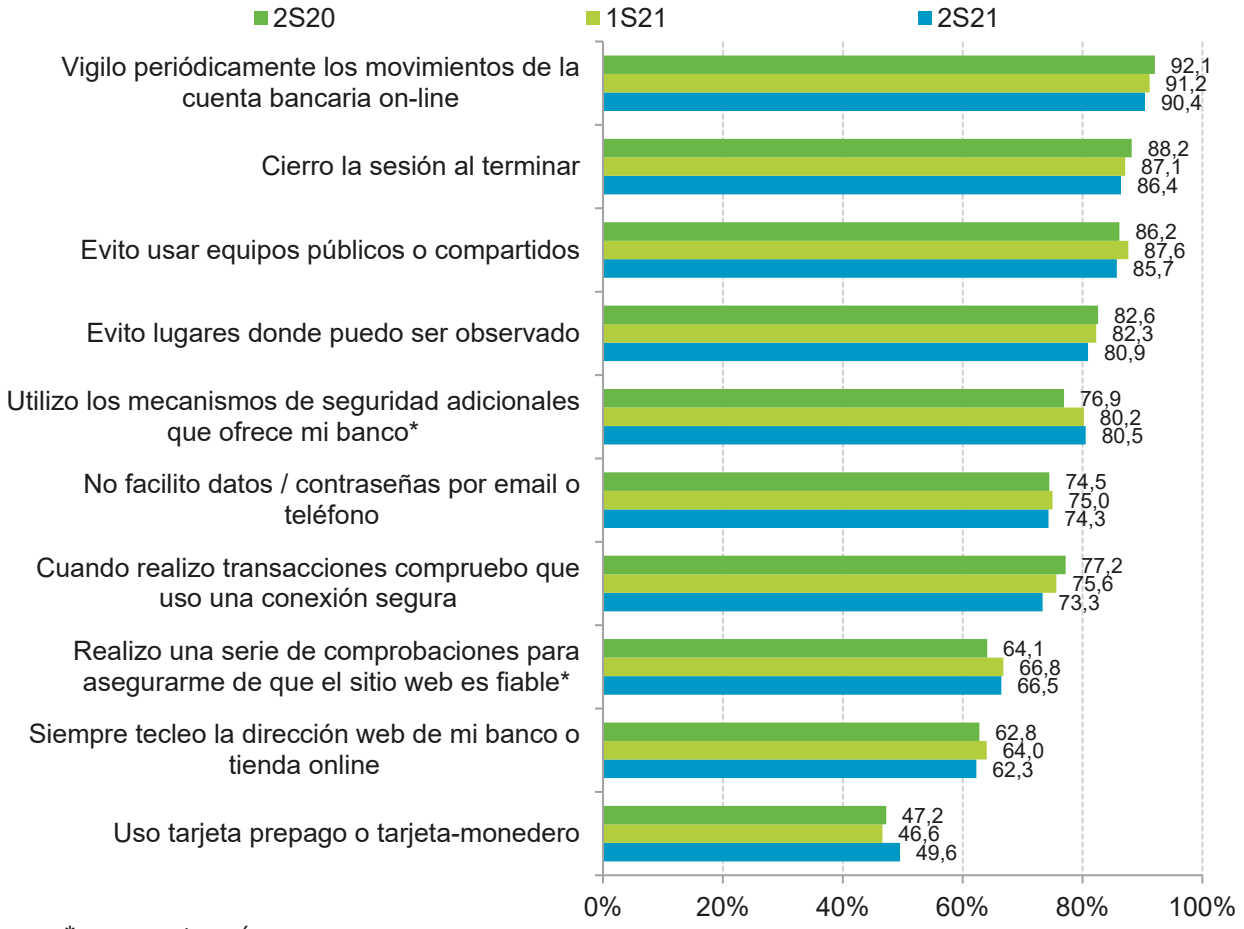
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de servicios de banca online o comercio electrónico

Desde el inicio de la pandemia el aumento del comercio electrónico sigue siendo notable. Esto conlleva a que los panelistas entrevistados declaren que en este semestre, están utilizando más tarjetas prepago o tarjetas monedero (3 p.p.). Por otro lado, parece ser que la confianza en la banca electrónica hace que los entrevistados manifiesten que no comprueban si tienen una conexión segura antes de realizar las transacciones. En concreto ha disminuido la comprobación en 2,3 p.p. respecto al semestre anterior.

Las entidades bancarias nunca solicitan datos y contraseñas del usuario. Dicha información es confidencial y únicamente debe ser conocida por el usuario y normalmente las entidades bancarias avisan a sus clientes de estas prácticas. La finalidad es evitar fraudes online y/o telefónicos que buscan obtener las credenciales del usuario y conseguir acceso a sus cuentas.

El 1 de enero de 2021 se acabó el plazo para la implantación de la Autenticación Reforzada de Cliente (SCA). Infórmate más sobre la directiva de pago en: https://www.osi.es/es/actualidad/blog/2019/09/17/informate-lo-que-debes-saber-si-quieres-hacer-pagos-online-partir-de



*nuevas categorías

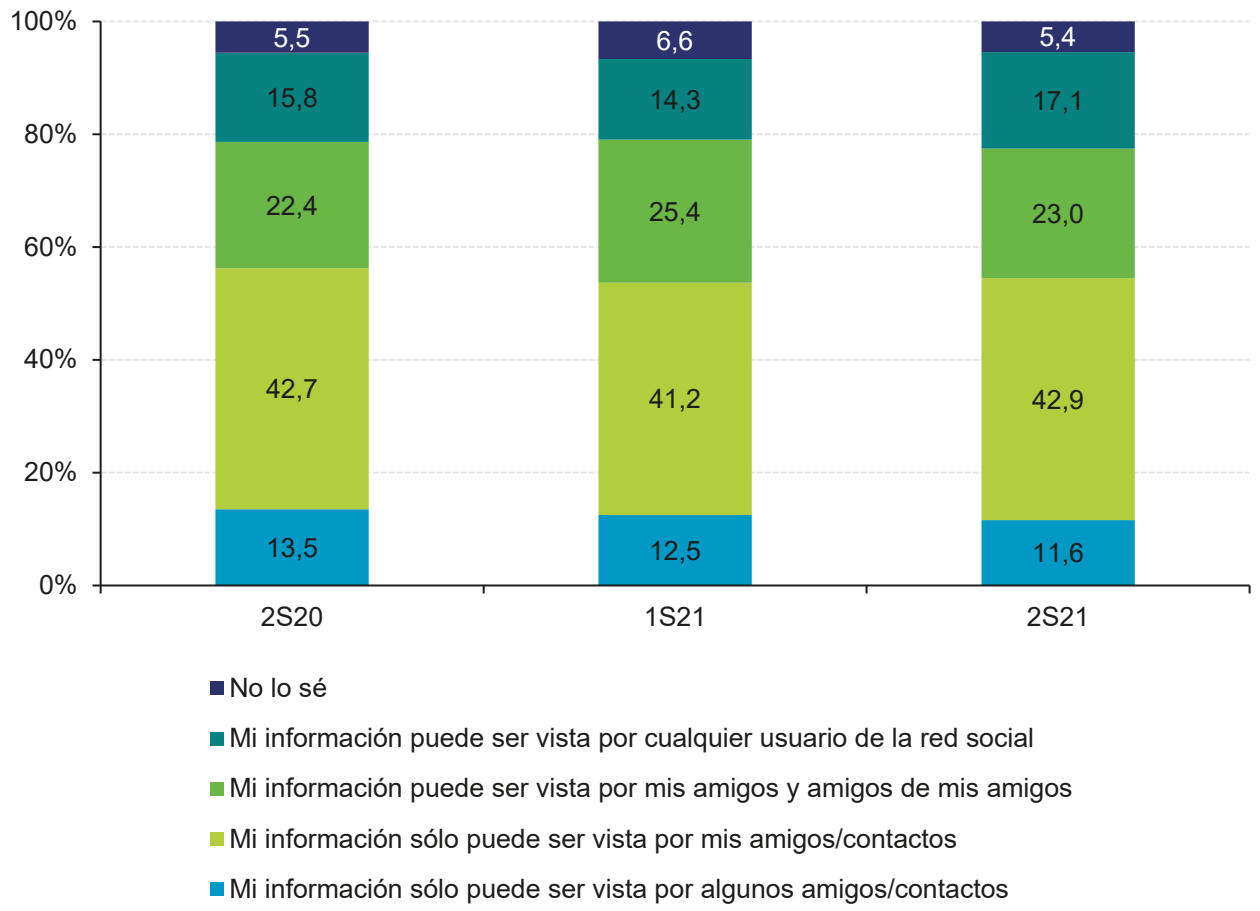
BASE: Usuarios que utilizan banca online y/o comercio electrónico

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de redes sociales

Durante este año, son diversas las redes sociales que se han visto obligadas a cambiar sus términos de servicio, respecto a la política de privacidad e informar a los usuarios. Quizás por ese motivo los entrevistados son más conscientes de los datos que comparten en esas redes. Se puede ver un aumento (1,5 p.p.) en los usuarios que declaran que comparten su información en redes con sus amigos y contactos. Aunque también se ve un aumento en el número de panelistas que declaran que su información en redes sociales es publica, pero siguen siendo el mínimo (15,8%).

Descubre qué información se almacena en las redes sociales Facebook, Instagram, Twitter y LinkedIn sobre ti y quién puede acceder a ella:
https://www.osi.es/es/actualidad/blog/2020/01/22/descarga-tu-vida-de-las-redes-sociales



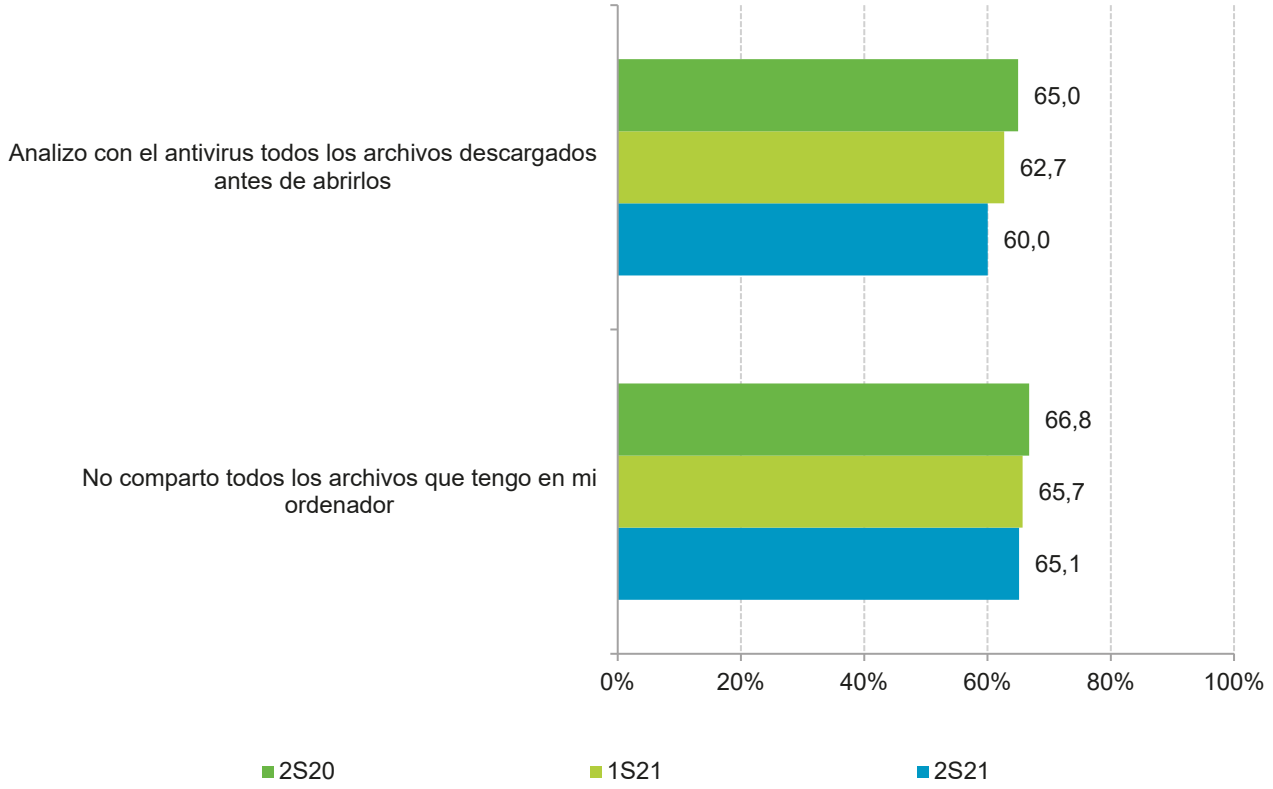
BASE: Usuarios de redes sociales

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de redes P2P

Aunque es una buena práctica el analizar los archivos que se descargan de Internet, los panelistas entrevistados cada vez están menos habituados a analizar las descargas antes de abrir el archivo. Ha disminuido en 5p.p. desde el año pasado según sus declaraciones.

Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de malware. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como por ejemplo novedades de software, cinematográficas, musicales, etc.) logran el objetivo de infectar el equipo informático de usuarios poco precavidos.



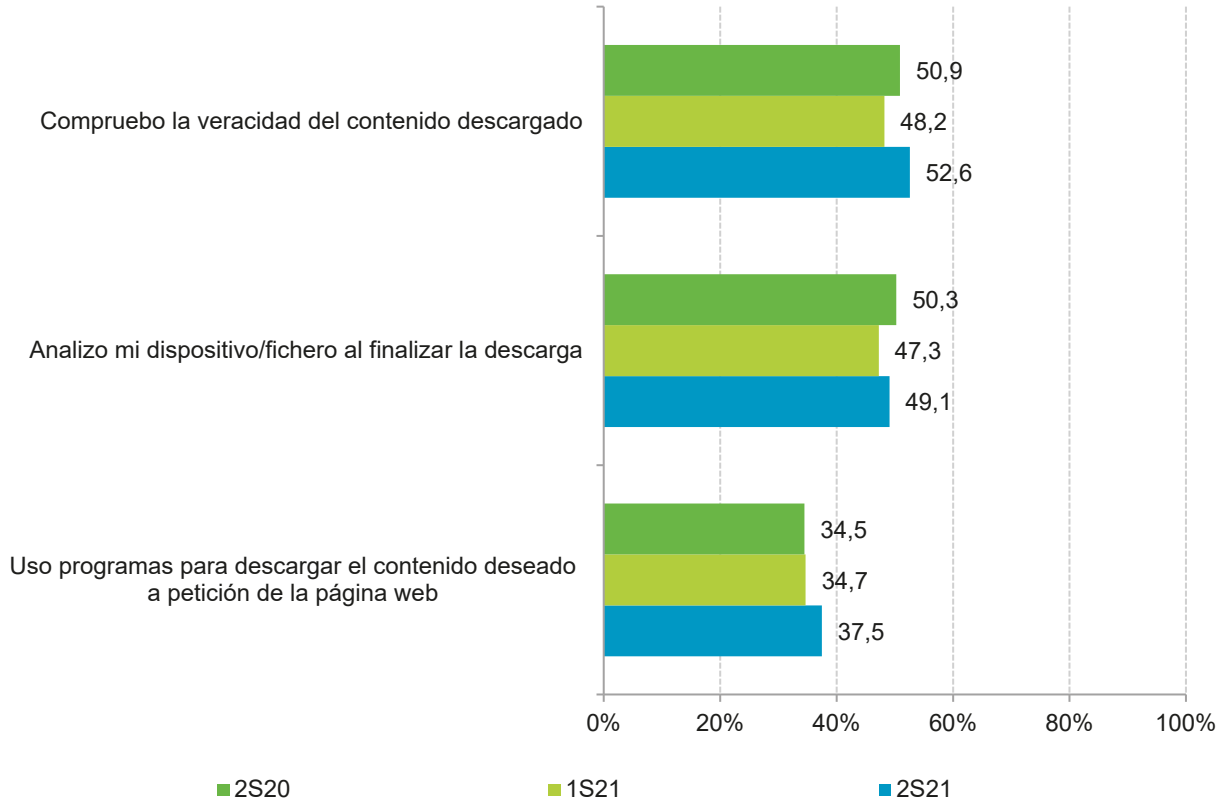
BASE: Usuarios de redes P2P

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en el uso de descarga directa de archivos, programas, documentos, etc.

Este semestre aumentan las tres buenas prácticas: comprobar la veracidad del contenido descargado (52,6%), analizar el dispositivo tras la descarga (49,1%), y usar programas para la descarga del contenido web (37,5%).

No obstante, el comportamiento de los usuarios puede variar dependiendo del dispositivo empleado para realizar las descargas. Dado que hay características adicionales que deben considerarse en el caso por ejemplo de las aplicaciones móviles, analizamos los dos grupos por separado.



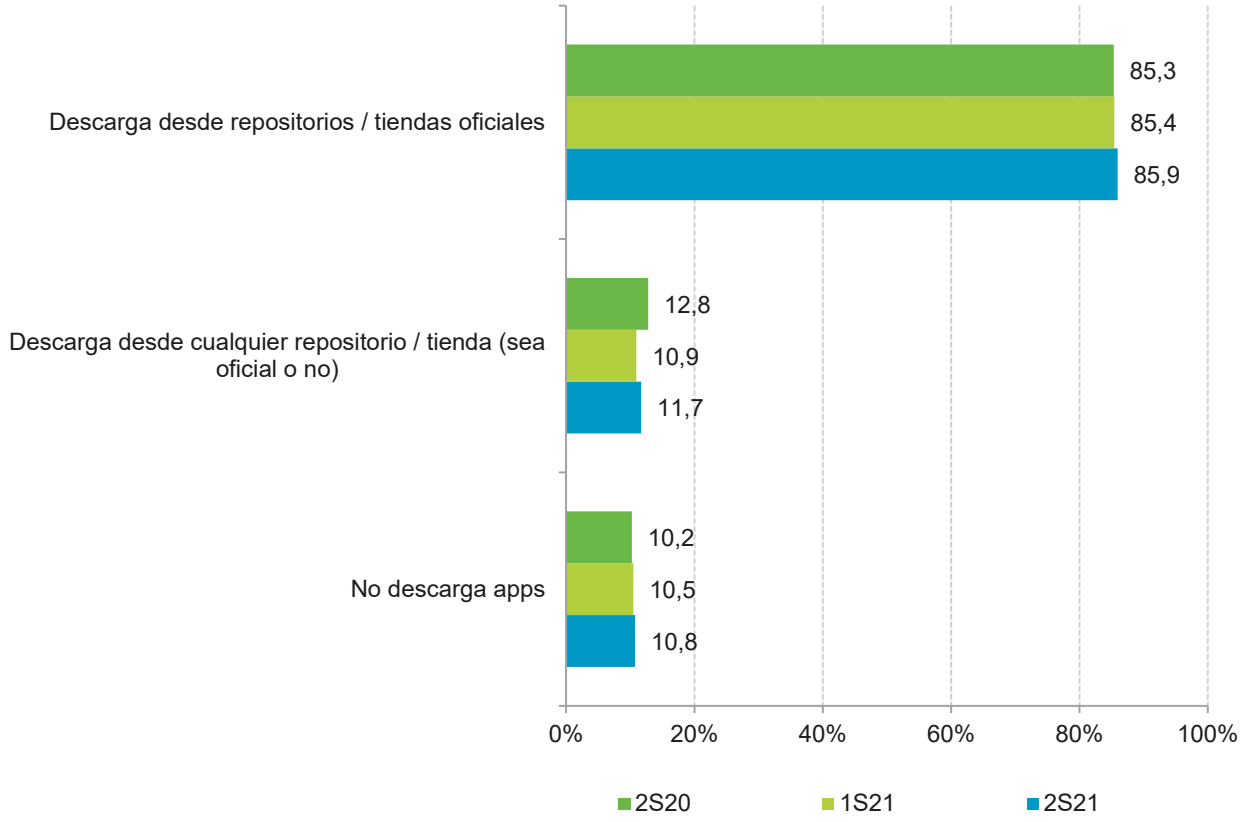
BASE: Total usuarios

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en la descarga de apps en el smartphone o tablet

En los últimos tres semestres se percibe un aumento muy leve en el número de panelistas que refieren descargar aplicaciones desde repositorios y tiendas oficiales (85,9%, +0,5 p.p.). No obstante, también aumenta levemente el porcentaje de usuarios que declara descargar desde cualquier repositorio no oficial (11,7%, +1,2 p.p.).

¡Ayuda! Instalé una app no fiable
https://www.osi.es/es/campanas/dispositivos-moviles/instale-app-no-fiable



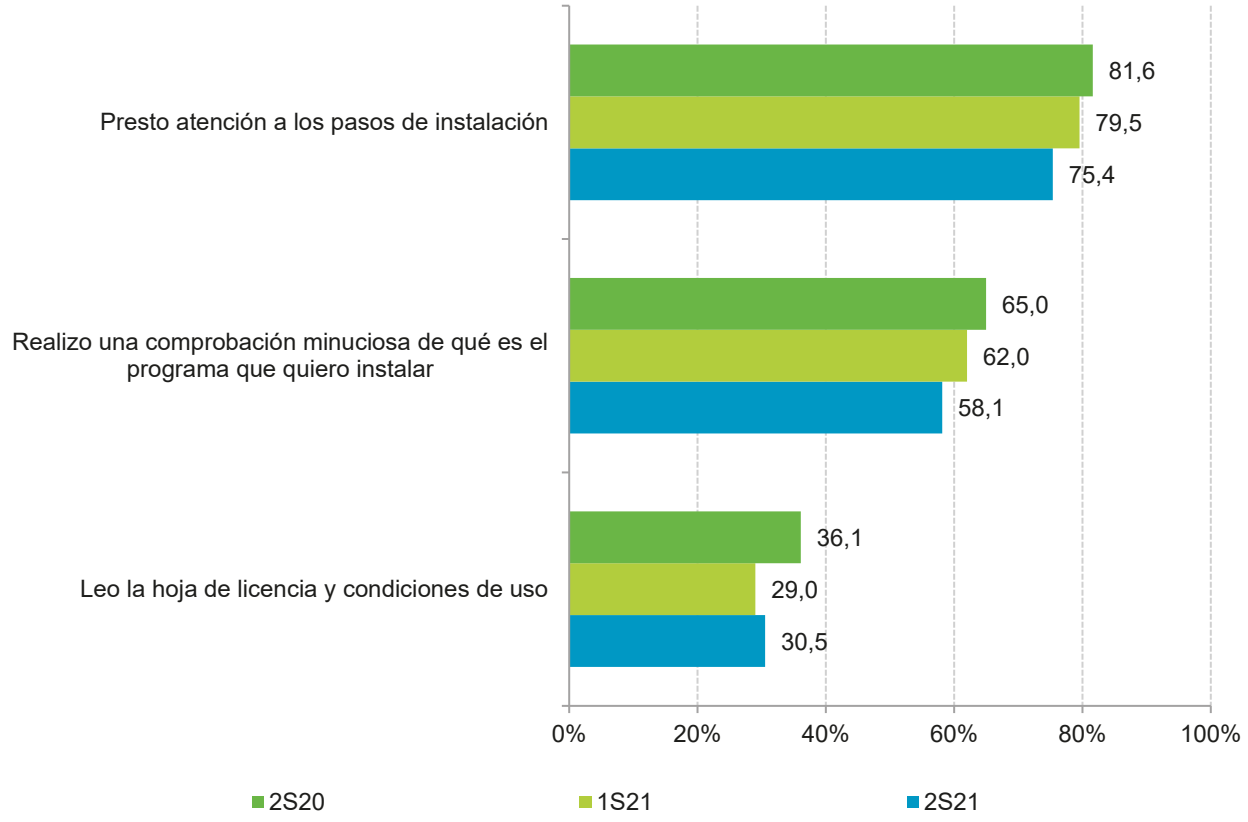
BASE: Usuarios que disponen de dispositivo Android

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Hábitos de comportamiento en la instalación de programas

Tan sólo el punto relativo a si leen la hoja de licencia y condiciones de uso se incrementa respecto al semestre previo, aunque ligeramente, en 1,5 p.p.

El 75,4% de los participantes asegura prestar atención a los pasos de instalación, que puede ser una buena práctica no sólo por la identificación de posibles errores, sino también para identificar posibles conductas anómalas: por ejemplo, aparición de terminales con código no propio de una aplicación dirigida a usuarios.



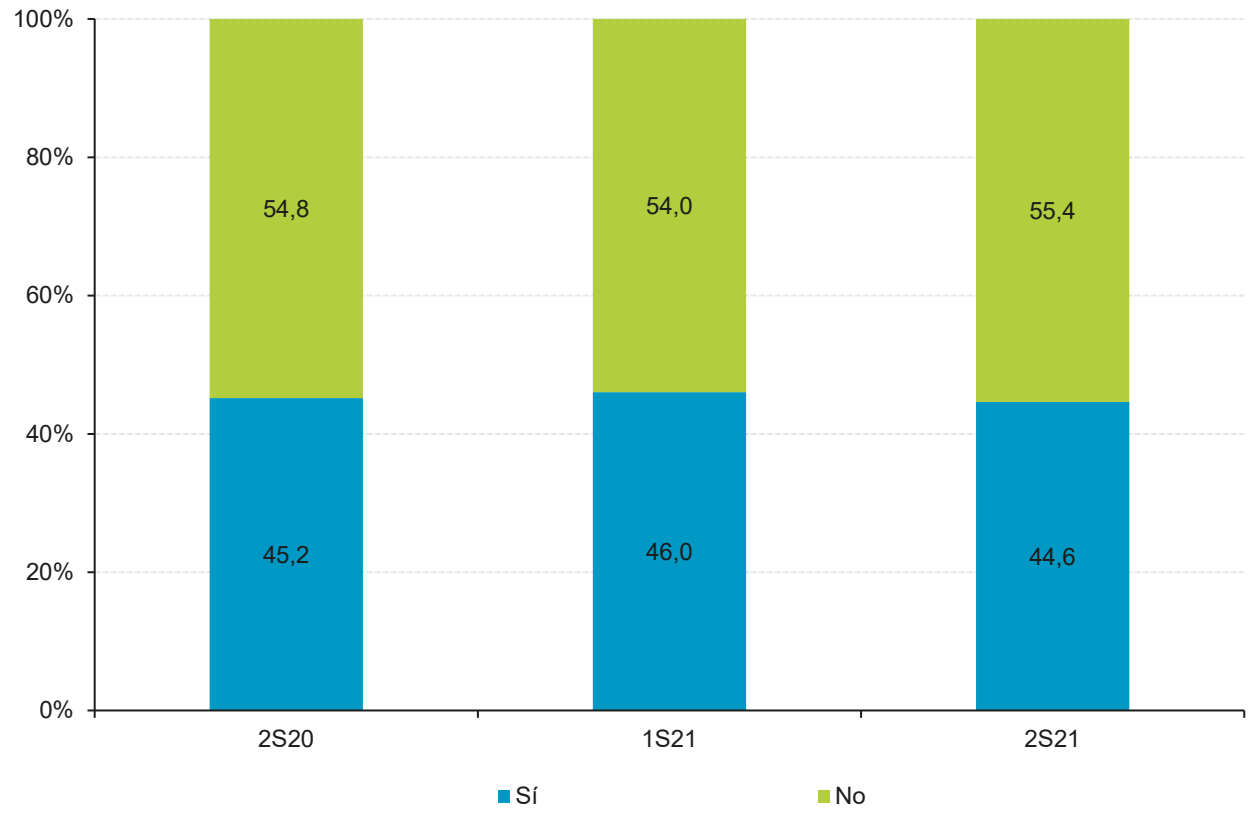
BASE: Usuarios de PC

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Lectura y aceptación de la información legal al registrarse o darse de alta en proveedores de servicios en Internet (redes sociales, comercio electrónico, etc.)

Cuando el usuario solicita el alta de un servicio, es obligatorio aceptar las condiciones del servicio. Ya sea en redes sociales o en páginas que ofrecen comercio electrónico. Del total de entrevistados el 55,4% pasa por alto leer las condiciones del servicio, simplemente las aceptan y no se preocupan de lo que están aceptando. Esta práctica es peligrosa para la privacidad de los usuarios ya que en esos términos puede aparecer para que van a usar los datos que generes accediendo e interactuando con la web o con el resto de personas de esa red social.

Gestión de riesgo y evaluación de impacto en tratamientos de datos personales
https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd



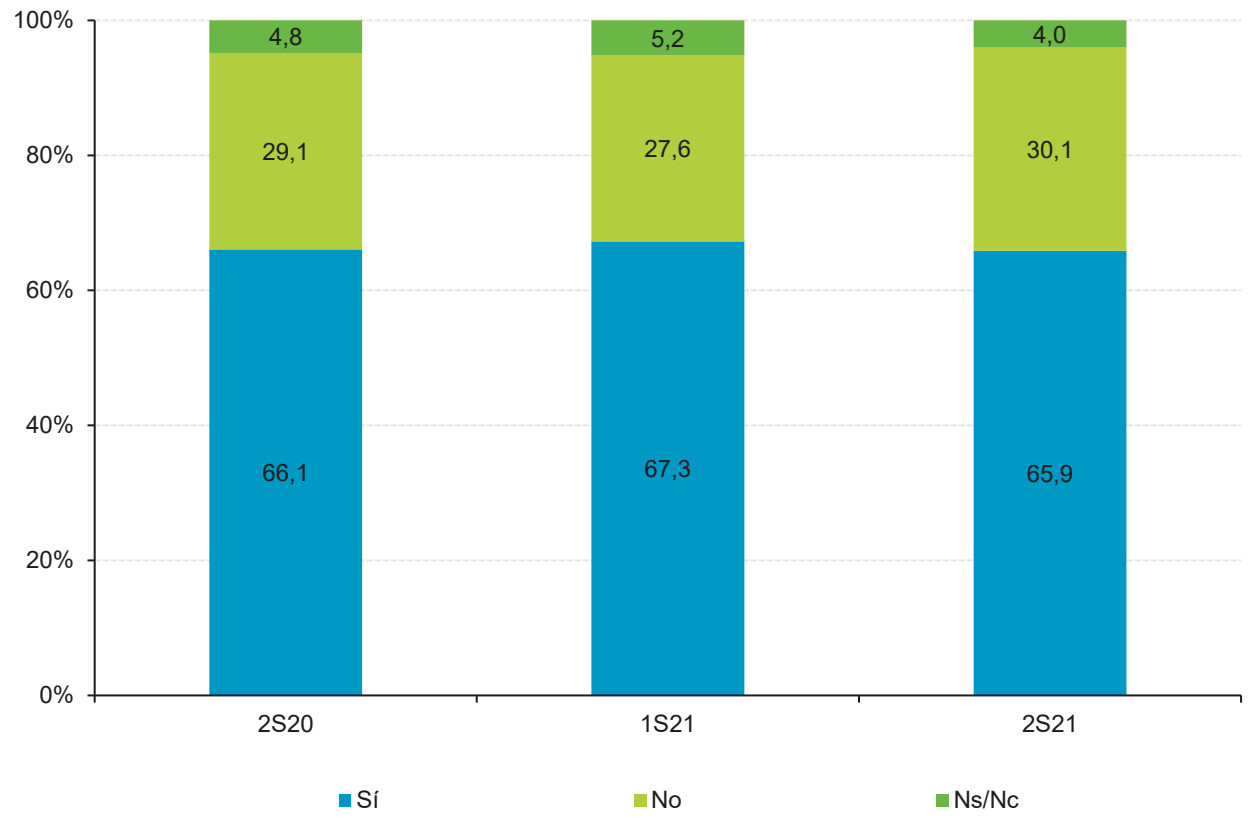
BASE: Total usuarios

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Comprobación de permisos al instalar apps

Se ha dado el caso en el que una aplicación que contiene un troyano bancario, solicita permiso para activar los servicios de accesibilidad que posteriormente el troyano usará para hacerse con las credenciales bancarias de la víctima. De ahí la importancia de comprobar los permisos antes de instalar una aplicación. Según declaran para este estudio, el 65,9% de los usuarios entrevistados comprueba los permisos que van a conceder a la aplicación que está instalando pero se puede ver un descenso de 1,4 p.p. respecto a los usuarios que confirmaron que los comprobaban en el semestre anterior.

Permisos de apps y riesgos para tu privacidad
https://www.osi.es/es/permisos-de-apps-y-riesgos-para-tu-privacidad



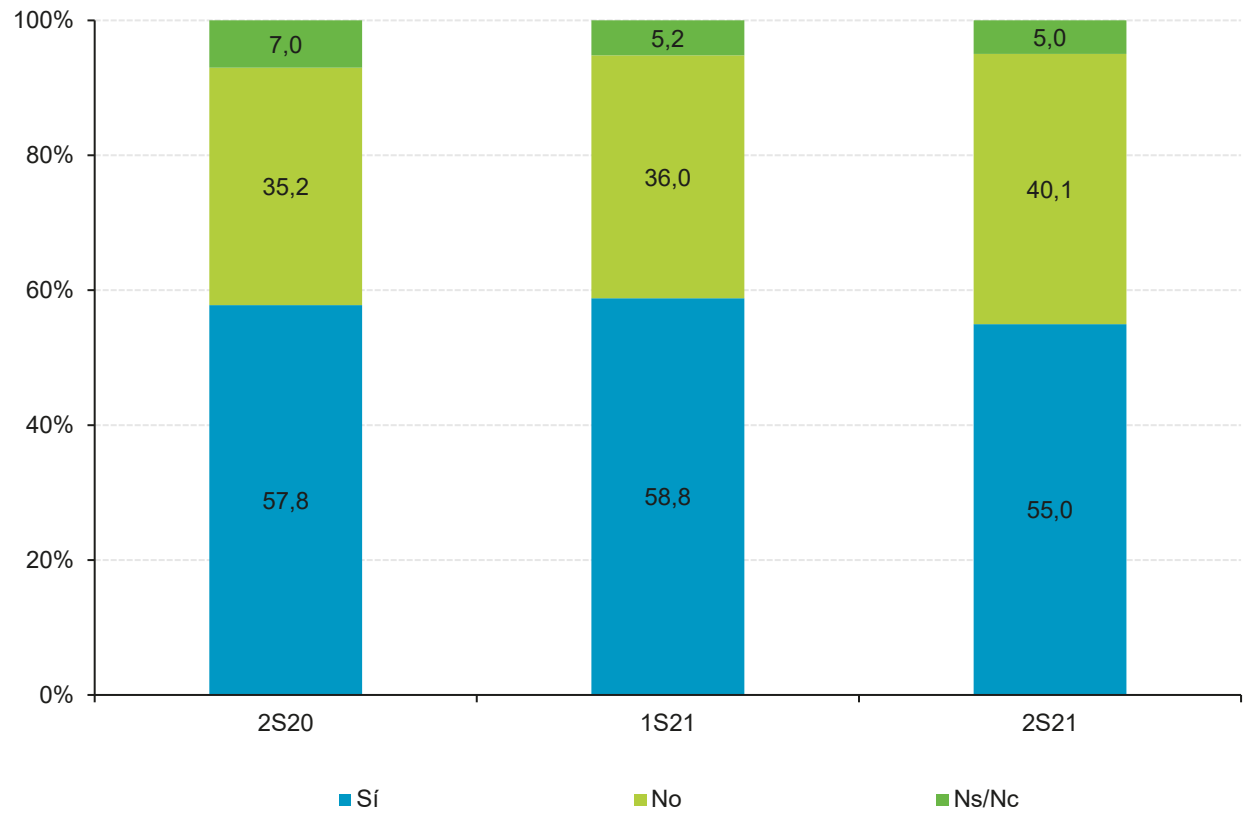
BASE: Usuarios que disponen de dispositivo Android y descargan apps

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Verificación del origen al instalar apps

El uso de repositorios no oficiales para descargar aplicaciones es un peligro para los dispositivos y para los propios usuarios. El problema de instalar aplicaciones desde markets no oficiales es que no han pasado una serie de controles que si que tienen por ejemplo el Play Store o el App Store. Las aplicaciones de repositorios no oficiales pueden acarrear sorpresas para el usuario como la instalación de un troyano o algún otro malware y dar lugar a perdidas monetarias o robos de información.

Según declaran los panelistas que participan en este estudio, hay una diferencia de -3,8 p.p. en el número de usuarios que verifican el origen de las aplicaciones.

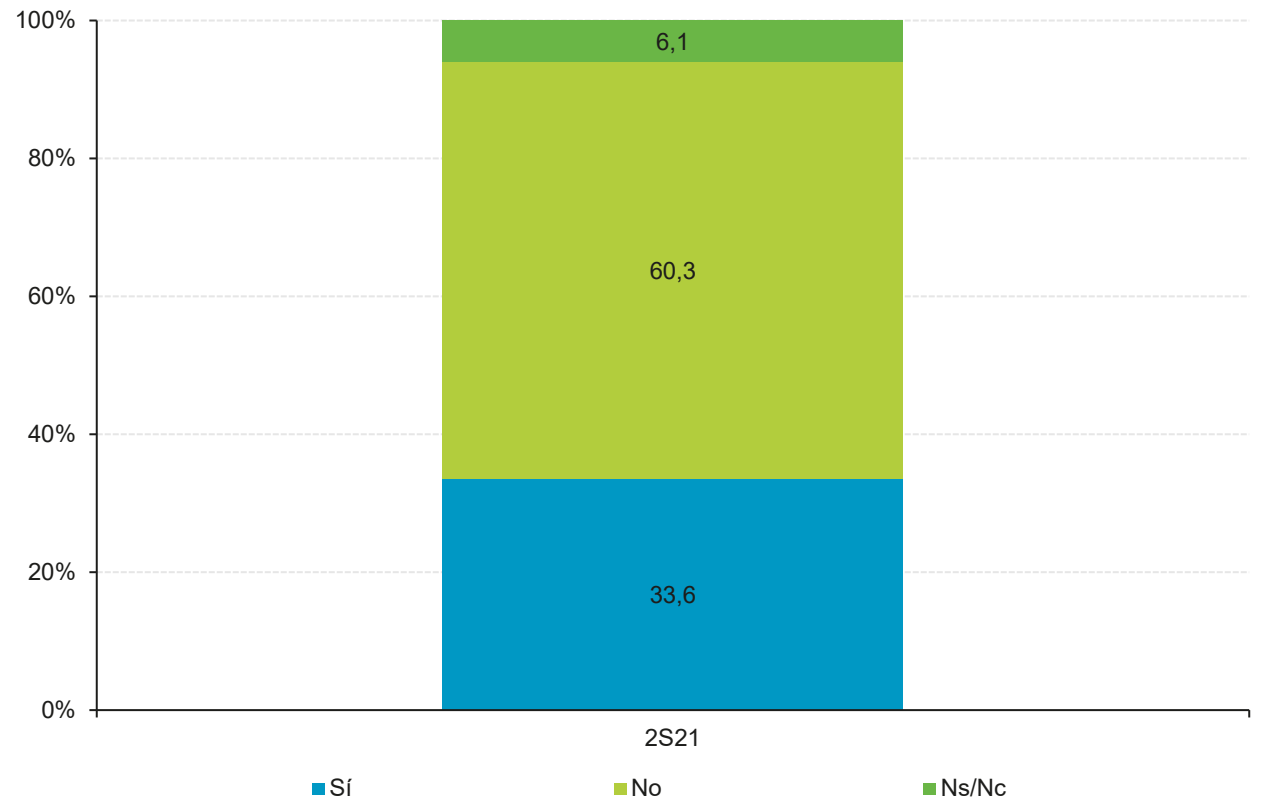


BASE: Usuarios que disponen de dispositivo Android y descargan apps

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Revisar el desarrollador de la aplicación

Es una práctica poco habitual entre los usuarios que participan en este estudio la de consultar quien es el desarrollador de la aplicación. En concreto más de la mitad de los usuarios entrevistados (60,3%) no comprueba quien es el desarrollador o desarrolladores de las aplicaciones que instalan. Esta es también una práctica de riesgo para el dispositivo y los datos que se registran en él.

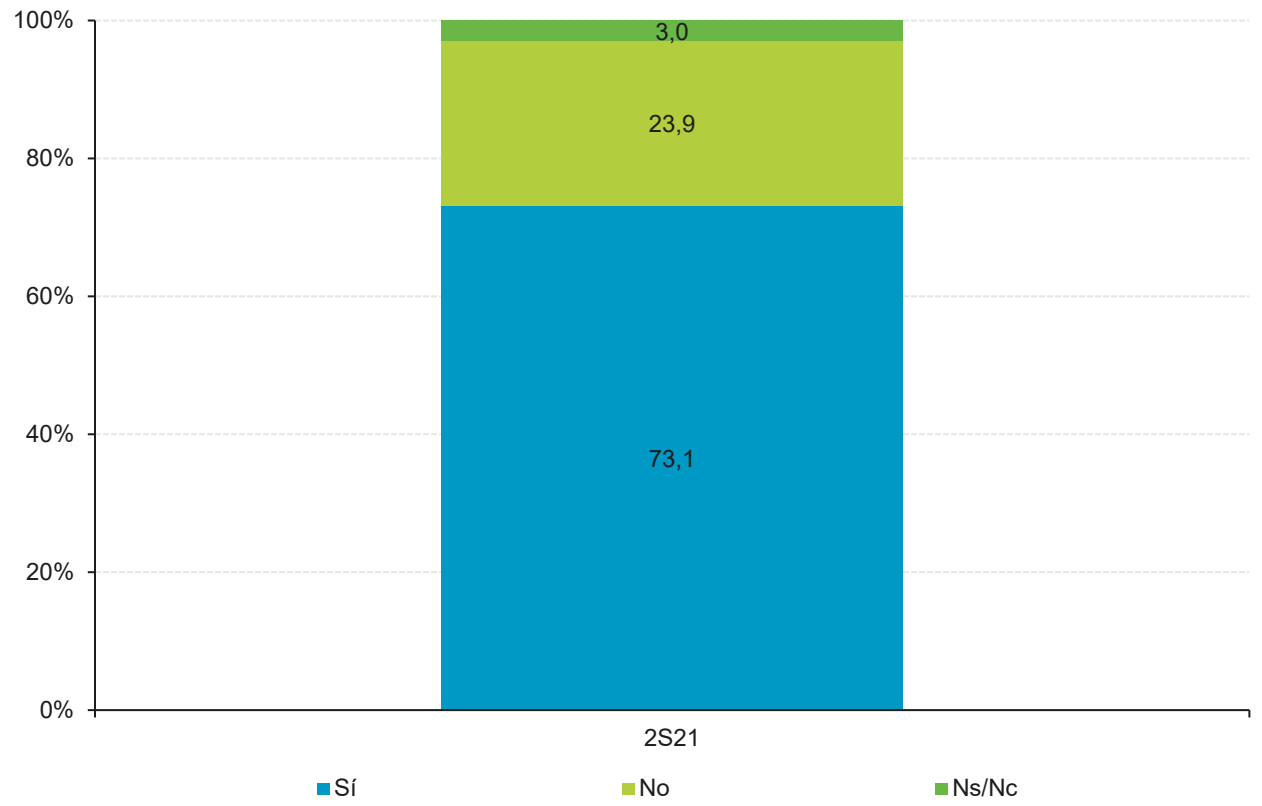


BASE: Usuarios que disponen de dispositivo Android y descargan apps

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Verificar los comentarios y valoraciones de otros usuarios

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



BASE: Usuarios que disponen de dispositivo Android y descargan apps

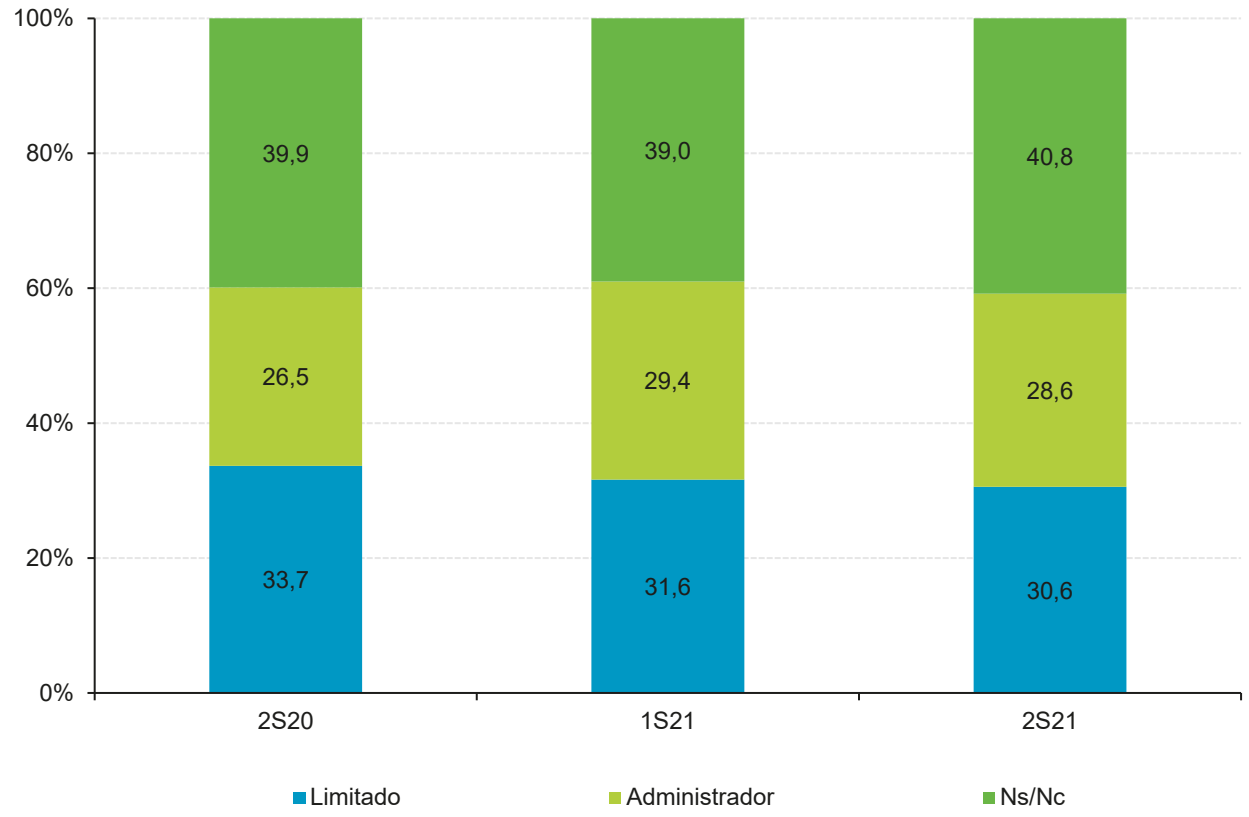
Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Privilegios del usuario en el dispositivo Android

Del total de panelistas entrevistados, el 28,6% piensa que utiliza el dispositivo en modo administrador mientras que el 40,8% desconoce que tipo de privilegios son los que tiene respecto a su dispositivo. Uno de los principales peligros de rootear los dispositivos es que al estar en modo administrador, el malware tendría más fácil el acceso al dispositivo a través de las aplicaciones instaladas.

Se conoce como "rooteo" o "rootear" a la obtención de privilegios de administrador (root). Esto permite al usuario acceder y modificar cualquier aspecto del sistema operativo. Pero también existen riesgos ya que el malware puede aprovecharse de esto logrando un mayor control y/o acceso al dispositivo.

Más información:
https://www.osi.es/es/actualidad/blog/2019/04/24/conocias-el-termino-jailbreaking-o-rooting



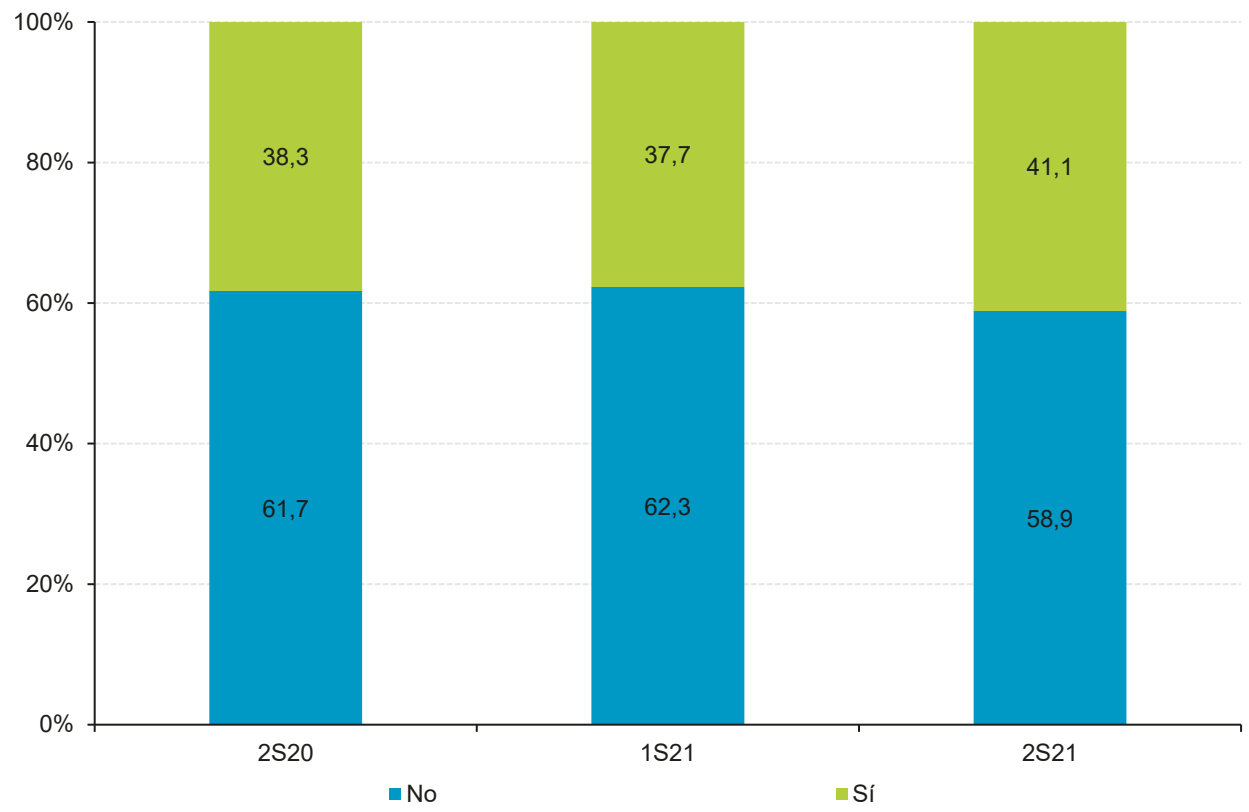
BASE: Usuarios que disponen de dispositivo Android

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Realización consciente de alguna conducta de riesgo

En este último semestre aumenta en 3,4 p.p. respecto al semestre anterior, la realización consciente de conductas que ponen en riesgo sus dispositivos y/o los datos que hay almacenados en ellos.

El 41,1% de los internautas declaran realizar conscientemente alguna conducta de riesgo.



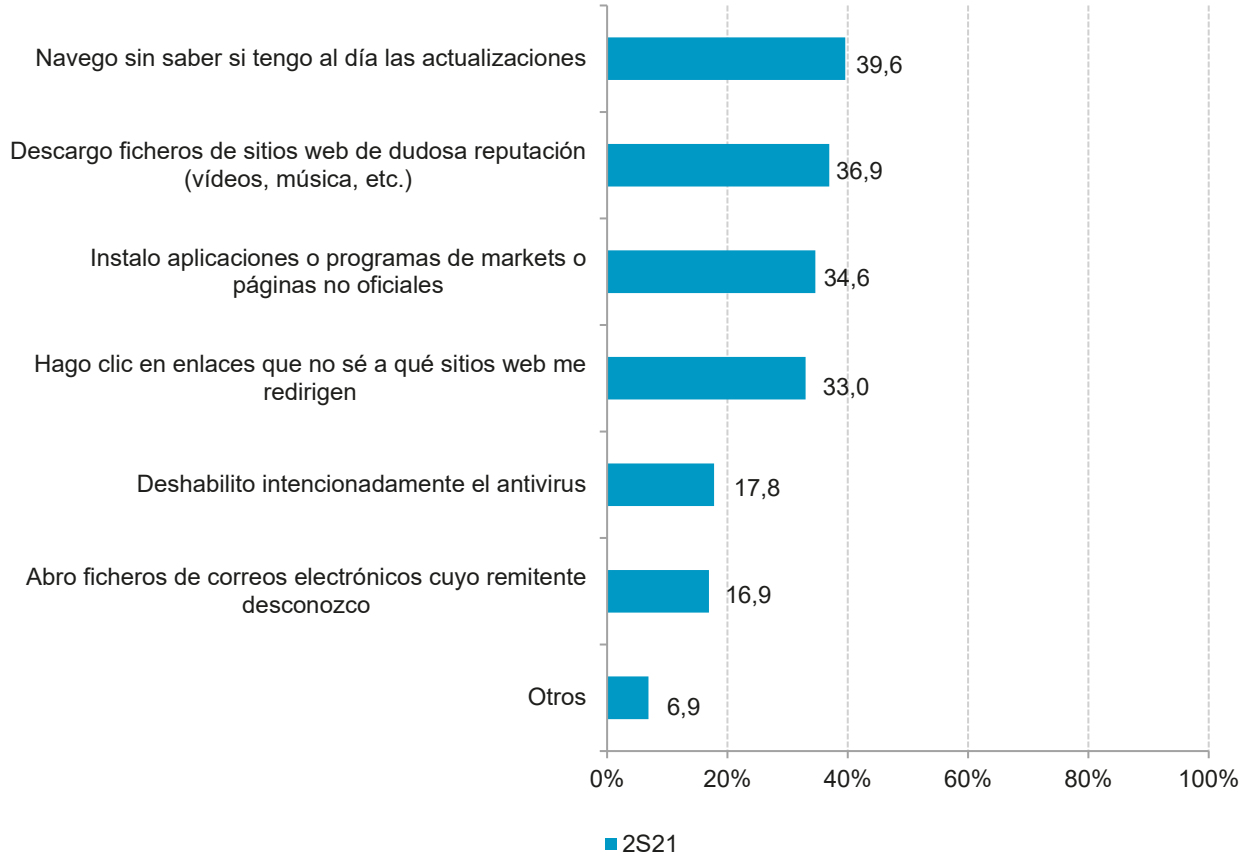
BASE: Total usuarios

Módulo III: Hábitos de comportamiento en la navegación y uso de Internet

Realización consciente de conductas de riesgo

Las actualizaciones de seguridad de los sistemas operativos y aplicaciones tanto móviles como de ordenador son muy importantes, y sin embargo el 39,6% de los usuarios reconoce no estar seguro de que su equipo esté actualizado. Con esas actualizaciones se solucionan o parchean problemas de seguridad críticos que hacen vulnerable el dispositivo, y se resuelven errores del software que también podrían facilitar un ataque.

Respecto a más conductas de riesgo relacionadas con los hábitos de descarga de videos, música y otros tipos de ficheros, el 36,9% de los usuarios utiliza sitios web de dudosa reputación para realizar descargas.



Base: Usuarios realizan alguna conducta de riesgo

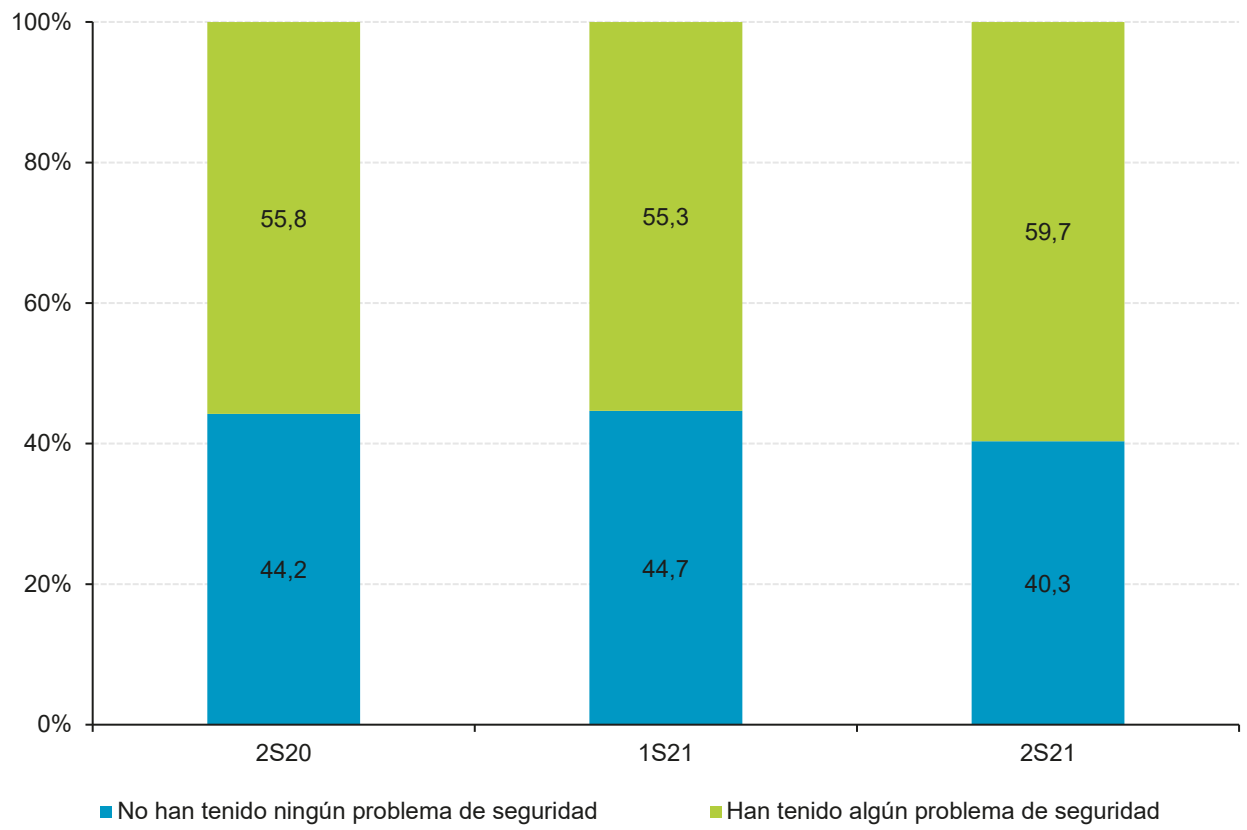
Módulo IV:
Incidencias de seguridad

Módulo IV: Incidencias de seguridad

Incidencia de seguridad en los últimos seis meses en el dispositivo con el que se accede habitualmente a Internet

En el segundo semestre de 2021 el número de troyanos y/o malware detectados para Android ha continuado aumentando. Esto es una amenaza para los dispositivos de los usuarios que a diario utilizan este sistema operativo.

De los usuarios entrevistados, el 59,7% afirma que ha tenido alguna incidencia de seguridad en los últimos 6 meses. Se ve un aumento entre las declaraciones del primer semestre y las del segundo semestre en 4,4p.p. de los usuarios que afirmando haber tenido algún problema de seguridad.



BASE: Total usuarios

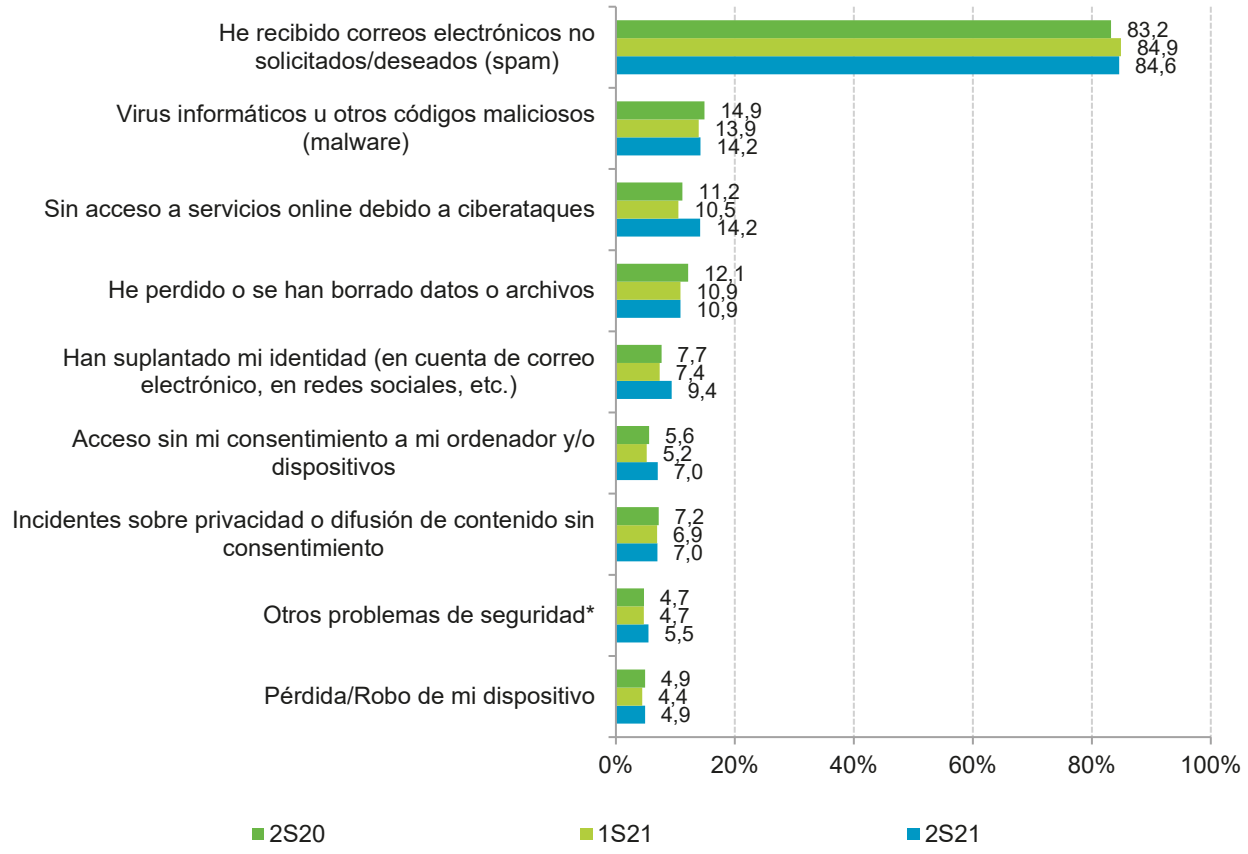
Módulo IV: Incidencias de seguridad

Problemas de seguridad acontecidos en los últimos seis meses en el dispositivo con el que se accede habitualmente a Internet

Vuelven a ser destacables sobre cualquier otro problema de seguridad las declaraciones de los panelistas sobre la recepción de correos electrónicos no solicitados o sospechosos de ser spam (84.6%). Además los entrevistados manifiestan un aumento en los servicios online a los que no han podido acceder debido aun ataque (14,2%).

La suplantación de identidad puede conducir a otros ciberataques. Protégete y reacciona ante la suplantación de identidad
https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar

Guía OSI sobre ciberataques:
https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf



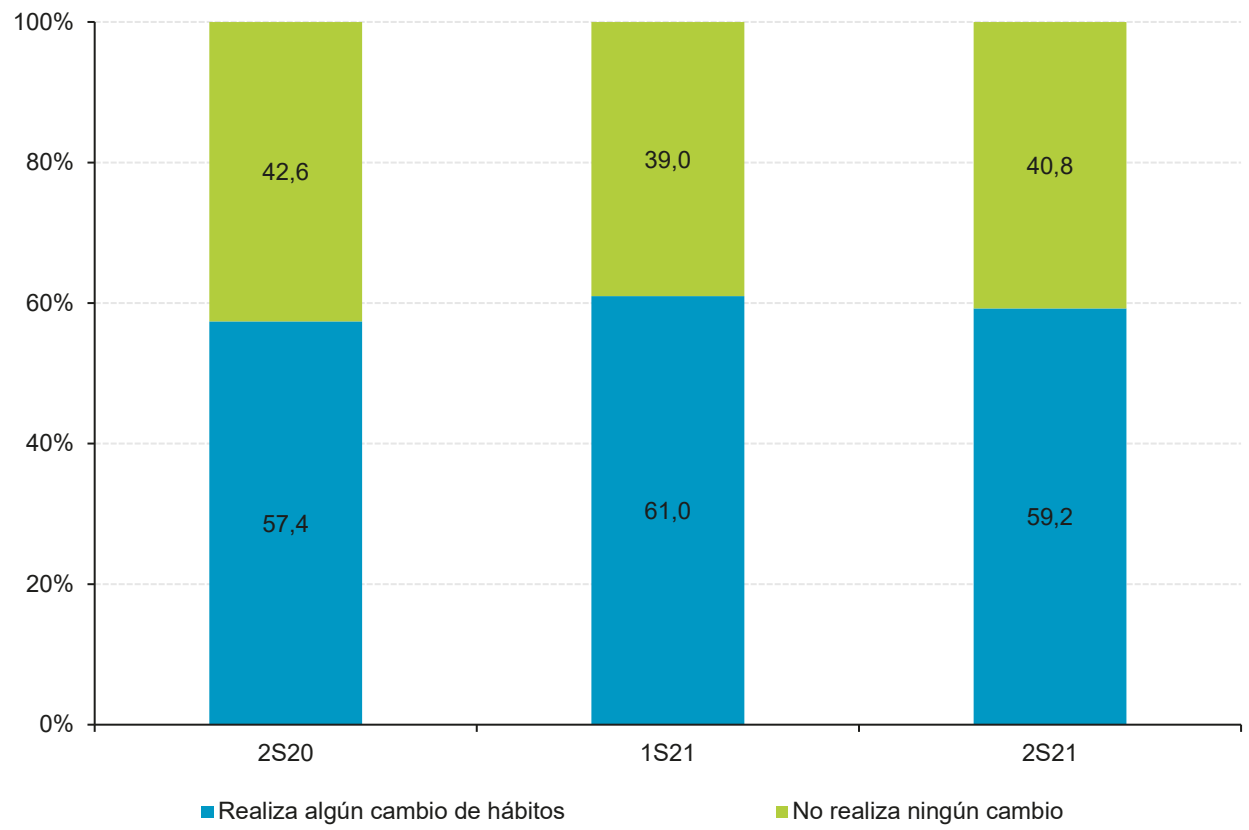
BASE: Usuarios que han sufrido alguna incidencia de seguridad

Módulo IV: Incidencias de seguridad

Realización de cambio de hábitos en Internet motivados por las incidencias de seguridad experimentadas durante los últimos seis meses

Tras un incidente de seguridad, lo habitual es modificar el comportamiento para evitar que se vuelva a producir ese incidente. Por ejemplo, frente a un ataque con ransomware si no se hacían con anterioridad es una buena practica tomar como costumbre realizar copias de seguridad periódicas.

Pese a ser víctimas de un incidente, desciende en 1,8 p.p. el porcentaje de panelistas que ha realizado algún cambio de hábitos tras los incidentes.

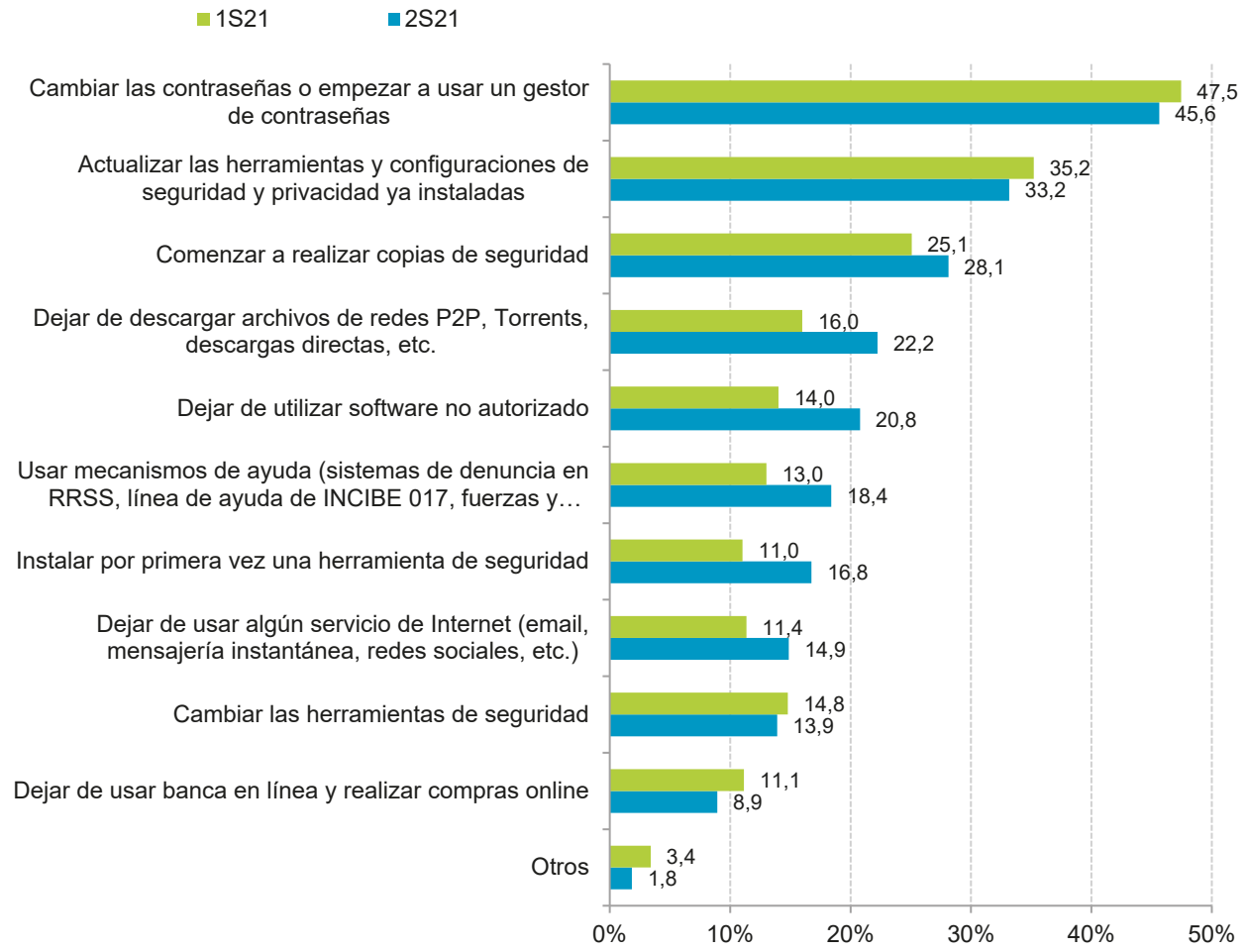


BASE: Usuarios que han sufrido alguna incidencia de seguridad

Módulo IV: Incidencias de seguridad

Cambios de hábitos en Internet motivados por las incidencias de seguridad experimentadas durante los últimos seis meses

La proliferación de ransomware y troyanos bancarios y la publicidad que se ha hecho sobre ellos en los medios de comunicación, pueden haber influido en los hábitos de los usuarios entrevistados para este estudio. Tal es el caso que entre los cambios más notables que declaran haber hecho, destacan el dejar de usar software no autorizado (20,8%), dejar de descargar de redes P2P (22,2%) y la utilización de la línea de Incibe 017 (18,4%). Además el 14,9% declara dejar de usar algún servicio de Internet ya sea redes sociales, plataformas de mensajería o bien el correo electrónico.



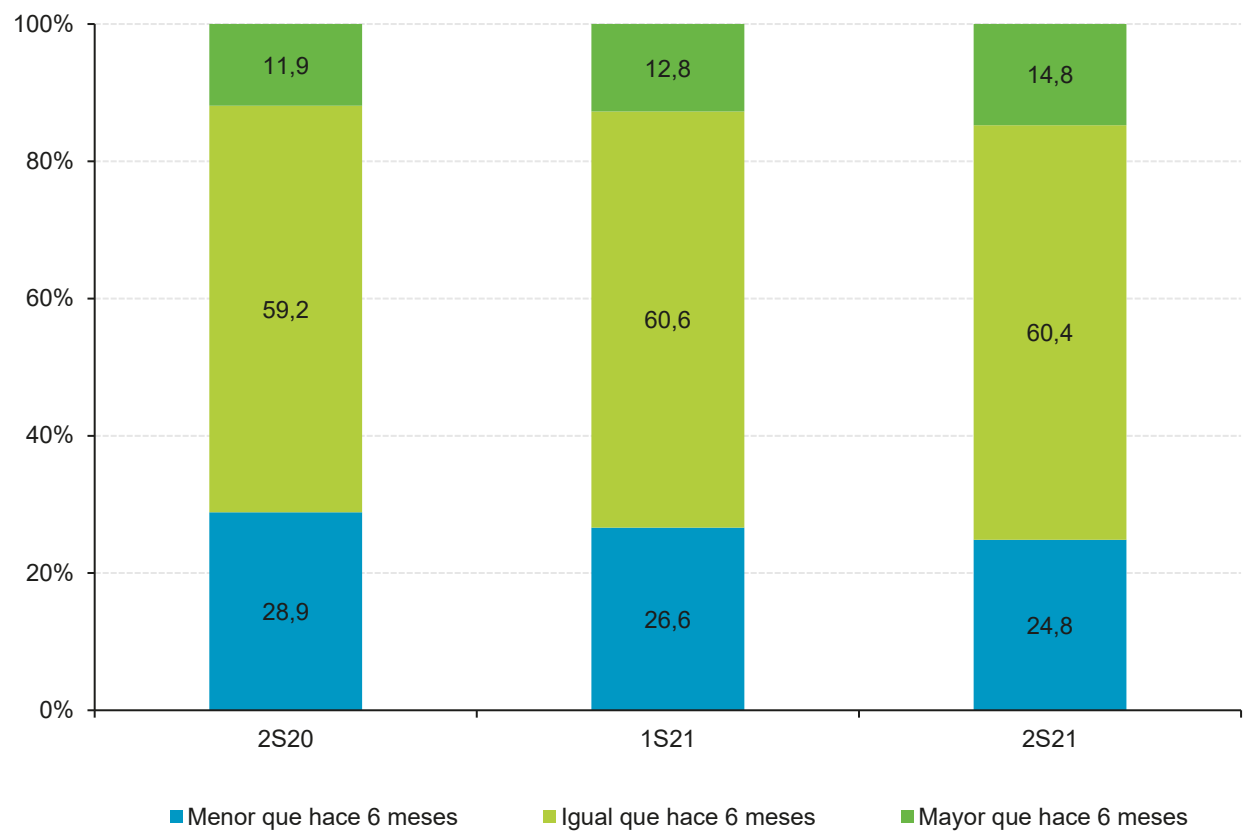
BASE: Usuarios que han sufrido alguna incidencia de seguridad y modifica sus hábitos

Módulo IV: Incidencias de seguridad

Percepción del usuario respecto al número de incidentes de seguridad que ha sufrido

A veces los usuarios sufren incidentes de seguridad pero no son conscientes de ello. Las declaraciones de los panelistas, respecto al número de incidentes que han sufrido, no varían sustancialmente respecto al semestre anterior.

El 14,8% piensan que el número de incidentes sufridos es mayor respecto al anterior mientras que el porcentaje de los que piensan que el número de incidentes sufridos es igual al anterior, se mantiene estable.

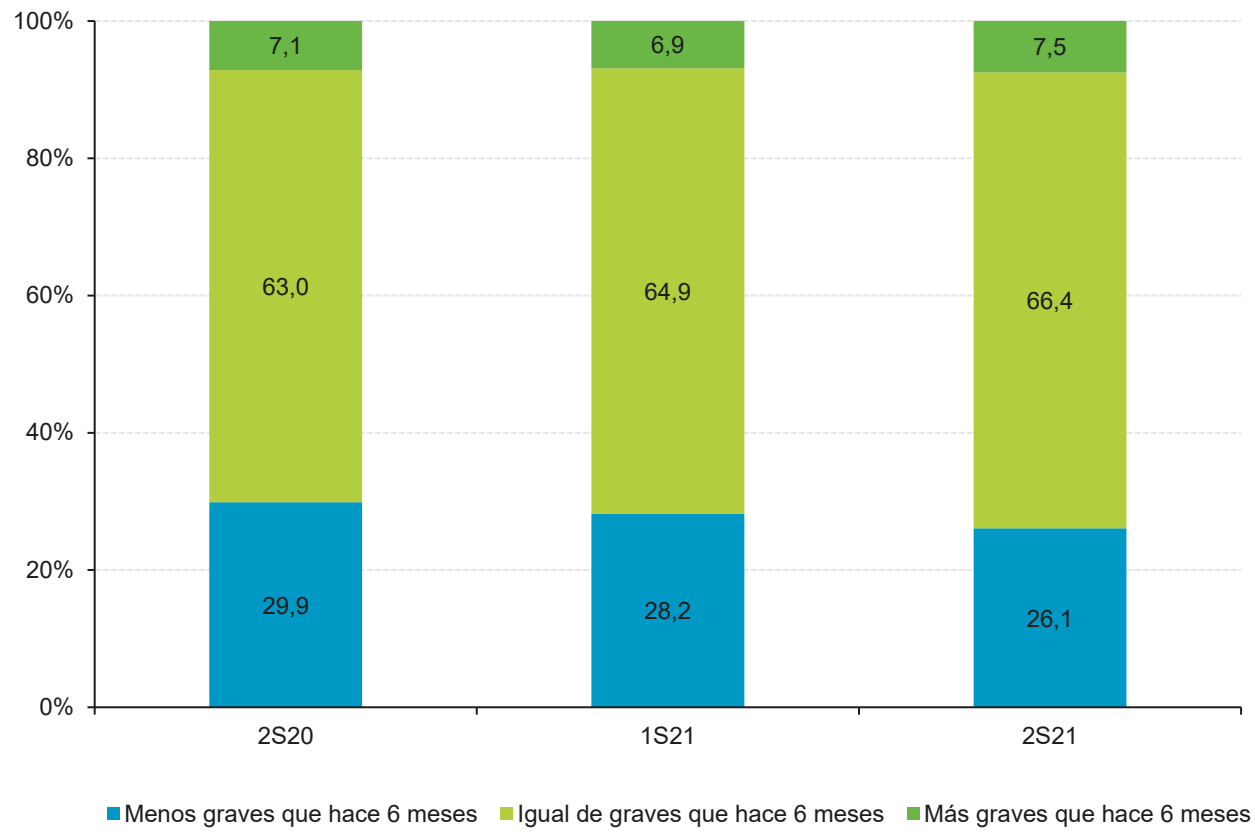


BASE: Total usuarios

Módulo IV: Incidencias de seguridad

Percepción del usuario al respecto a la gravedad de los incidentes de seguridad que ha sufrido

Quizás los usuarios no sean conscientes de la gravedad que puede conllevar el sufrir un incidente de seguridad, ya que tan solo el 7,5% opina que los incidentes sufridos son más graves que en el semestre anterior. Mientras que el 66,4% cree que son igual de graves que en el semestre anterior.



BASE: Total usuarios

Módulo V:
Fraude

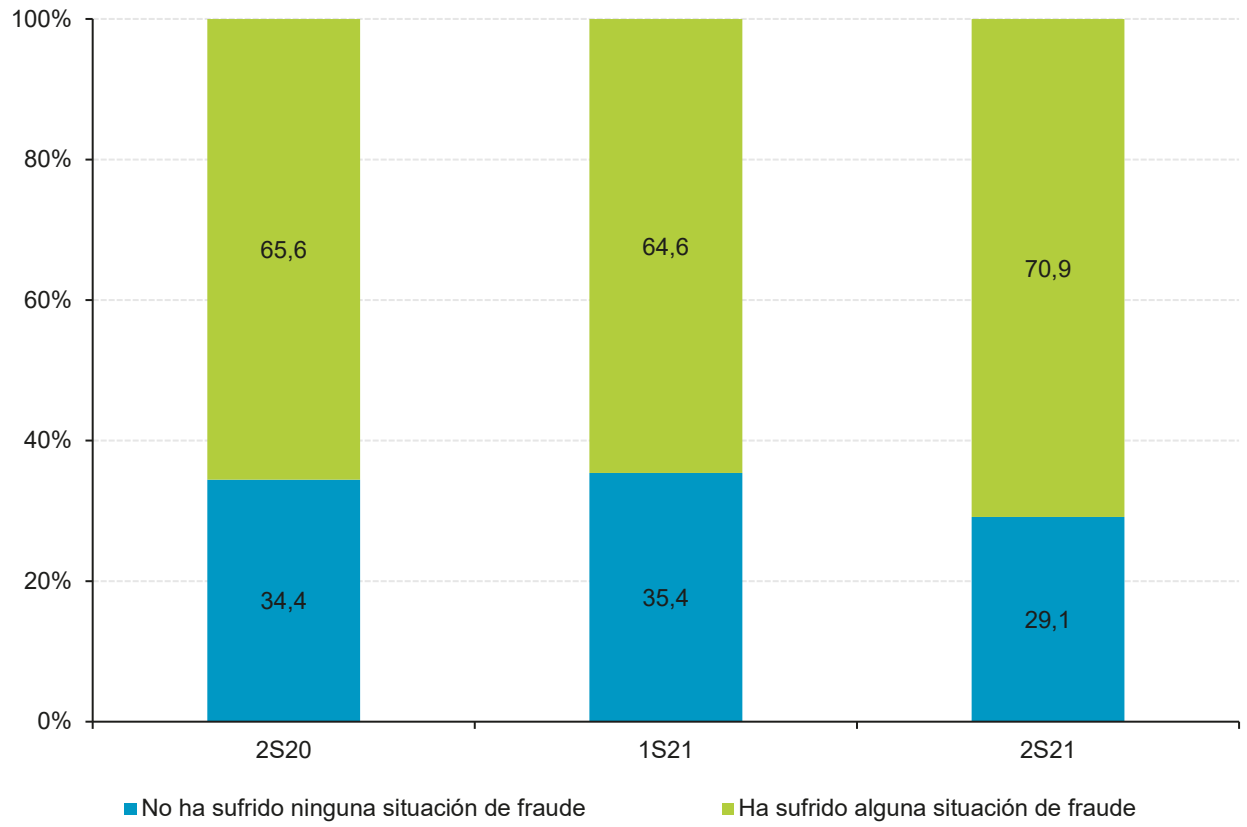
Módulo V: Fraude

Ocurrencia de alguna situación de fraude en los últimos seis meses

El fraude tiene múltiples vertientes y formas de efectuarse, aunque el objetivo final del mismo sigue siendo económico.

Durante el segundo semestre de 2021 el porcentaje de internautas que asegura sufrir fraude ha aumentado al 70,9%, lo que supone una subida de 6,3 p.p. sobre el semestre anterior.

¿Sabes como denunciar el fraude online?
https://www.osi.es/es/reporte-de-fraude



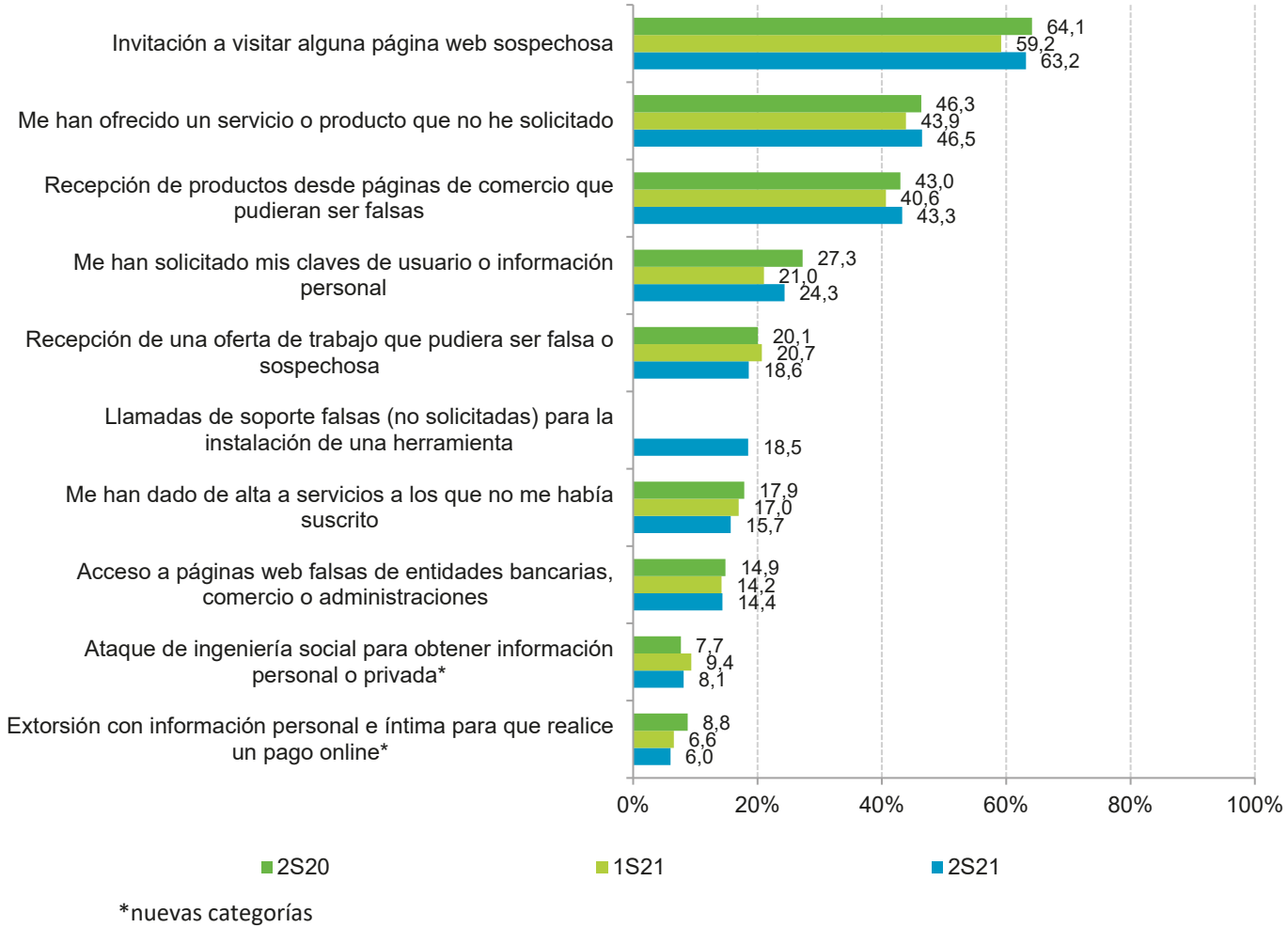
BASE: Total usuarios

Módulo: Fraude

Situaciones de fraude ocurridas en los últimos seis meses

Entre los indicios o situaciones de fraude detectados por los panelistas destacan: la invitación a visitar alguna web sospechosa (63,2%), ofrecimiento de servicios o productos no solicitados (46,5%), recepción de productos desde páginas potencialmente falsas (43,3%) y la solicitud de claves de usuario o información personal (24,3%).

¿Sabes como identificar el fraude online?
https://www.osi.es/es/guia-fraudes-online



*nuevas categorías

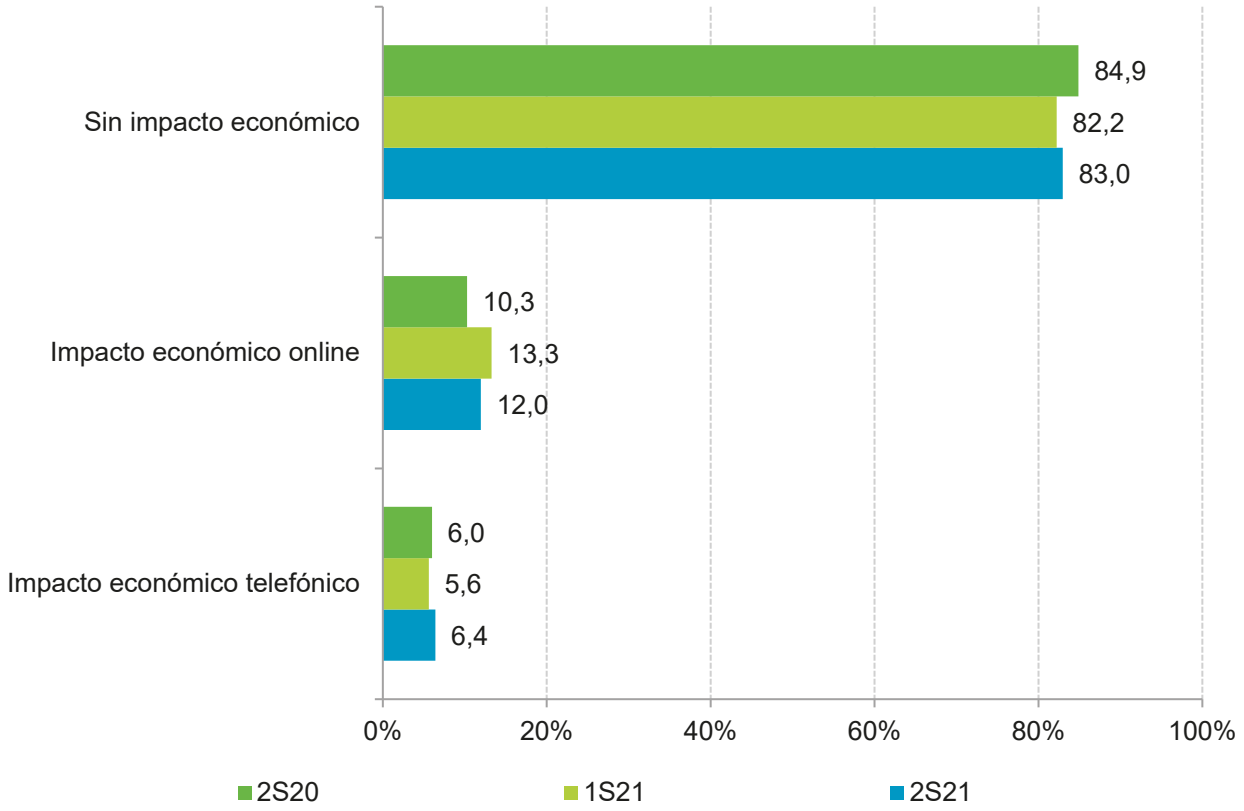
BASE: Usuarios que han sufrido alguna situación de fraude

Módulo V: Fraude

Perjuicio económico debido a posibles fraudes

La subscripción sin consentimiento del usuario a servicios de tarificación especial es otro tipo de fraude. Durante este estudio se ha consultado a los usuarios participantes si han sufrido fraude de algún tipo y si ese fraude ha conllevado un impacto económico.

Según declaran los usuarios el impacto económico telefónico ha aumentado 1,2 p.p. respecto al semestre anterior, sin embargo el 83% afirma que no han sufrido ningún perjuicio económico debido a posibles fraudes.



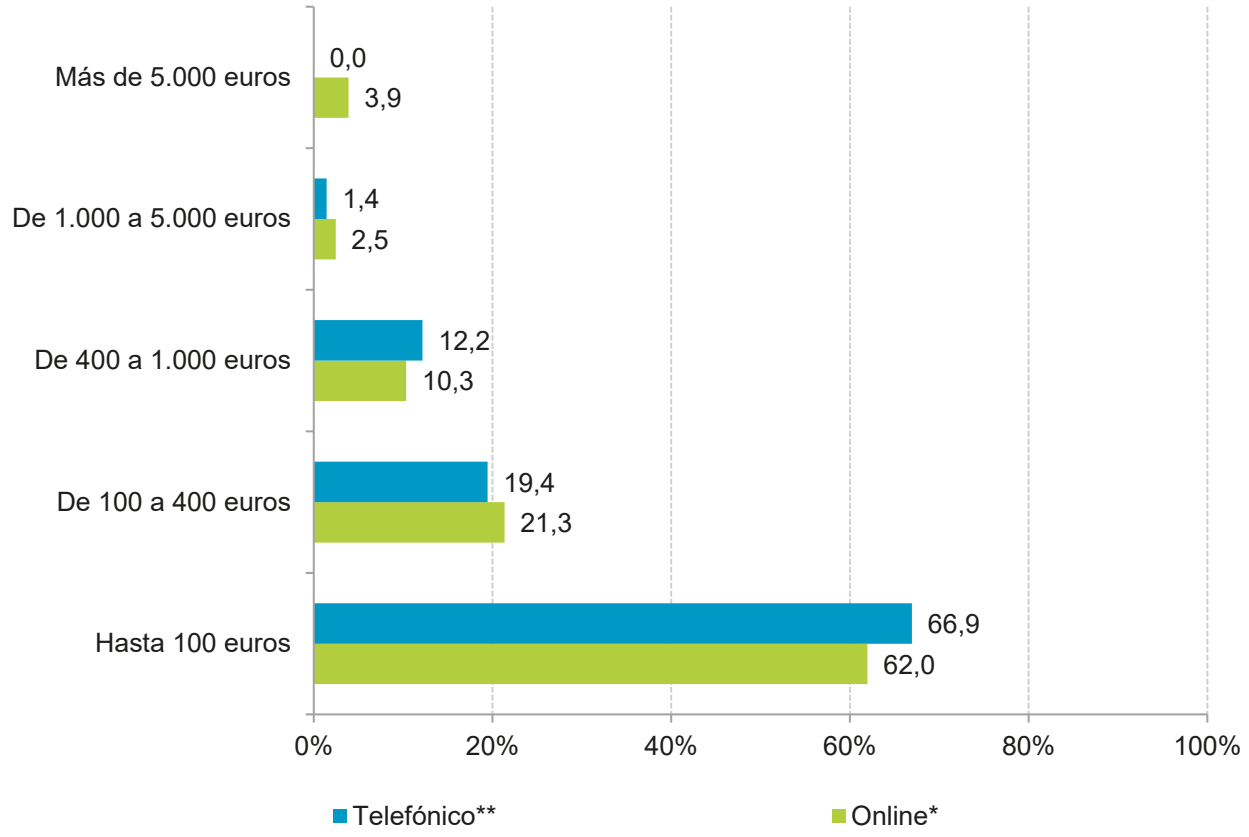
BASE: Usuarios que han sufrido alguna situación de fraude

Módulo V: Fraude

Distribución del perjuicio económico debido a posibles fraudes

Las cantidades superiores a 5000 euros se declaran para esta oleada sólo en casos de fraude online. También destaca este tipo de fraude en cantidades entre 1.000 y 5.000 euros y de 100 a 400 euros.

El fraude telefónico, sin embargo, es de los más presentes para cantidades inferiores o iguales a 100 euros, afectando al 66,9% de los panelistas. De igual forma destaca en el rango de pérdidas de los 400 a los 1.000 euros.



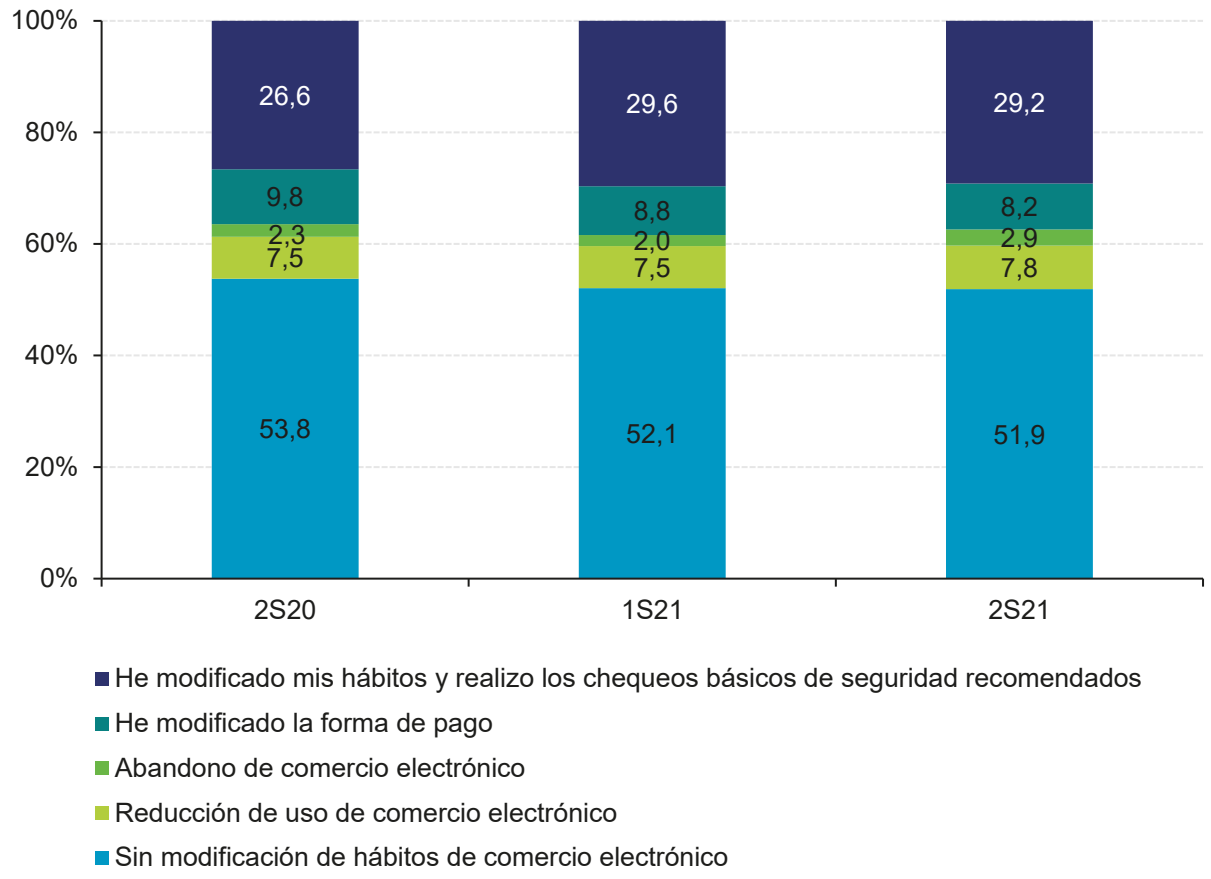
*** BASE: Usuarios que han sufrido perjuicio económico debido a un fraude online**
**** BASE: Usuarios que han sufrido perjuicio económico debido a un fraude telefónico**

Módulo V: Fraude

Modificación de hábitos en la compra online a causa de la situación de fraude sufrida

Durante la pandemia de 2020 se potenció el comercio electrónico y a lo largo de 2021, ha continuado siendo uno de los medios habituales de adquirir productos por parte de los usuarios. Este aumento del comercio electrónico ha sido aprovechado aún más por los delincuentes ya que ponen a la venta productos que realmente no existen o que no están en su posesión para que la víctima los compre, piden un adelanto del coste del producto y a la víctima nunca le llega el envío.

El 51,9% de los panelistas declara no haber cambiado los hábitos de compra online tras sufrir un fraude, mientras que el 29,2% afirma que tras el incidente, realiza chequeos básicos de seguridad para no volver a ser víctima de fraude.



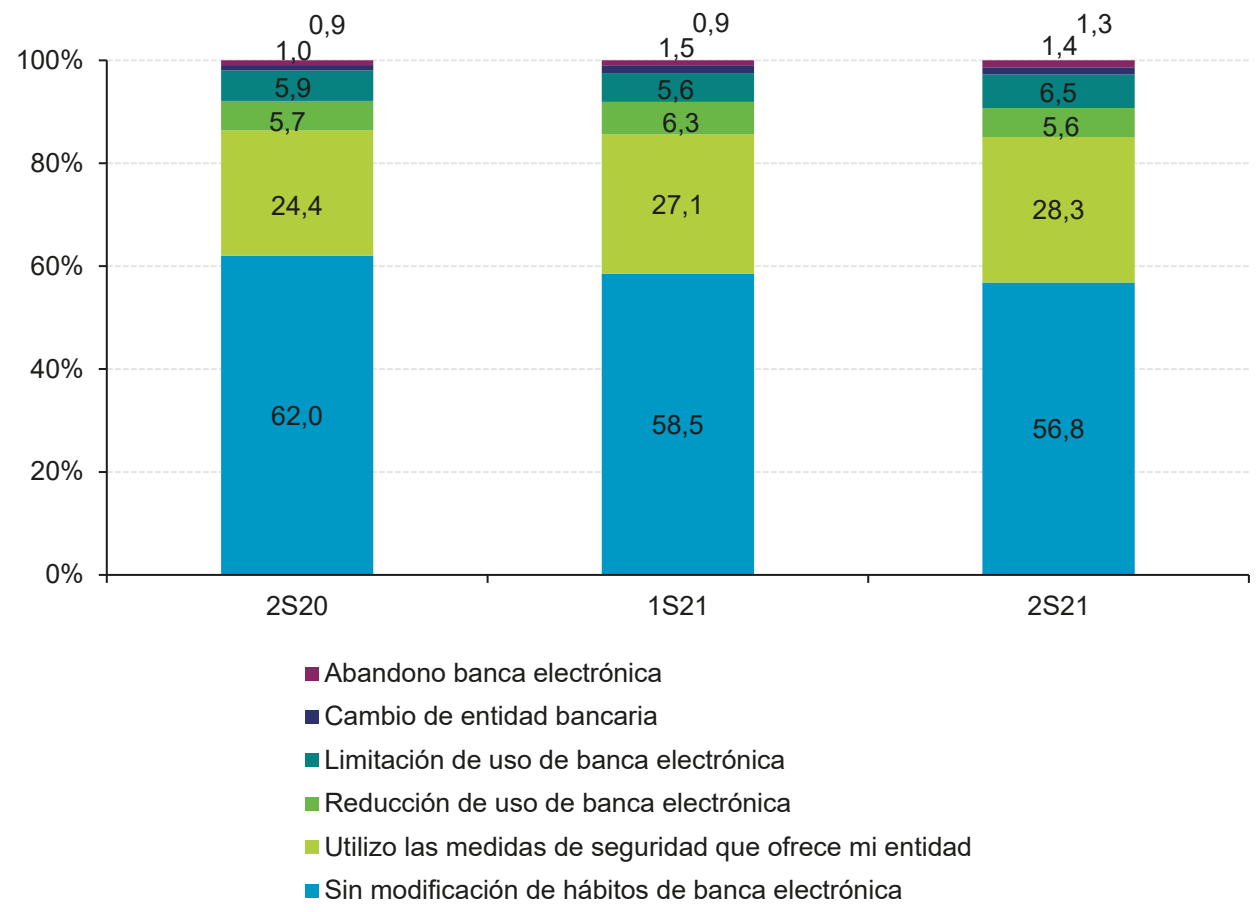
BASE: Usuarios que usan comercio electrónico y han sufrido alguna situación de fraude o perjuicio económico

Módulo V: Fraude

Modificación de hábitos en el uso de banca online a causa de la situación de fraude sufrida

Los semestres anteriores se mantuvo constante la tasa de abandono del uso de la banca electrónica por parte de los panelistas que sufrieron algún fraude. Sin embargo en este último semestre se observa que el número de panelistas que declaran haber dejado de usar la banca electrónica es mayor (1,3%).

Mientras que las medidas de seguridad que la banca electrónica pone a disposición de los usuarios son mejor aceptadas por los panelistas entrevistados. Ya que aumenta 1,2 p.p. el número de panelistas que declaran utilizar estas medidas. La banca electrónica está en continua mejora de los servicios de seguridad que ofrecen para evitar que los atacantes puedan romper los controles de seguridad que ofrecen a sus clientes para mantener sus bienes monetarios a salvo.



BASE: Usuarios que usan banca online y han sufrido alguna situación de fraude o perjuicio económico

Módulo VI:
Seguridad en Wi-Fi

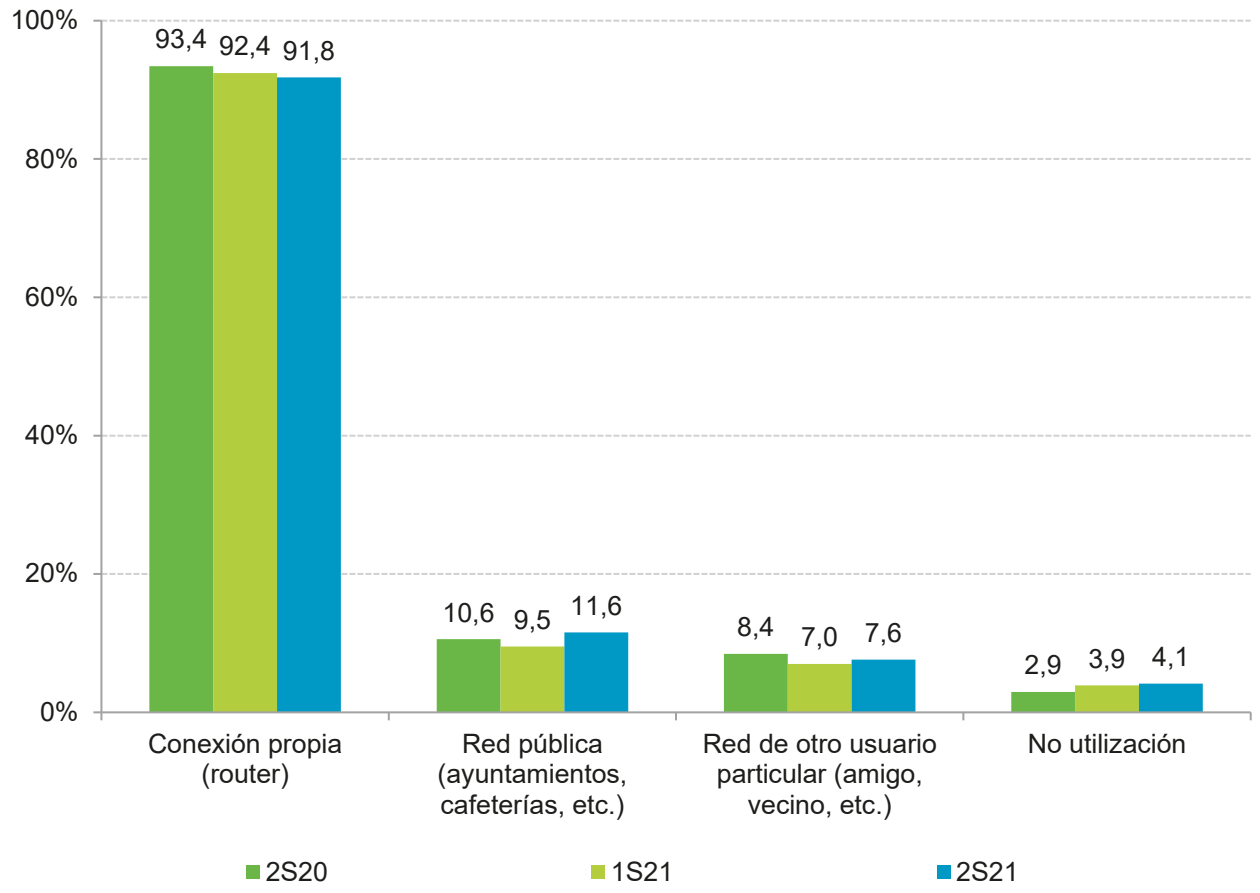
Módulo VI: Seguridad en Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

Es destacable que aunque paulatinamente, en los tres últimos semestres los internautas han optado por disminuir la conexión a través de su propio router o equipo doméstico para conectarse a otras redes públicas en su lugar, o, en el lado totalmente opuesto, no emplear este tipo de conexión.

Aún así, el 91,8% de los usuarios dispone de una conexión propia a través de un router. No obstante, disponer de esta conexión no hace que sea totalmente seguro el acceso a Internet sino que hay que tomar otras medidas de seguridad adicionales.

Protección y seguridad al navegar por Internet. Conexiones seguras. https://www.osi.es/es/conexiones-seguras



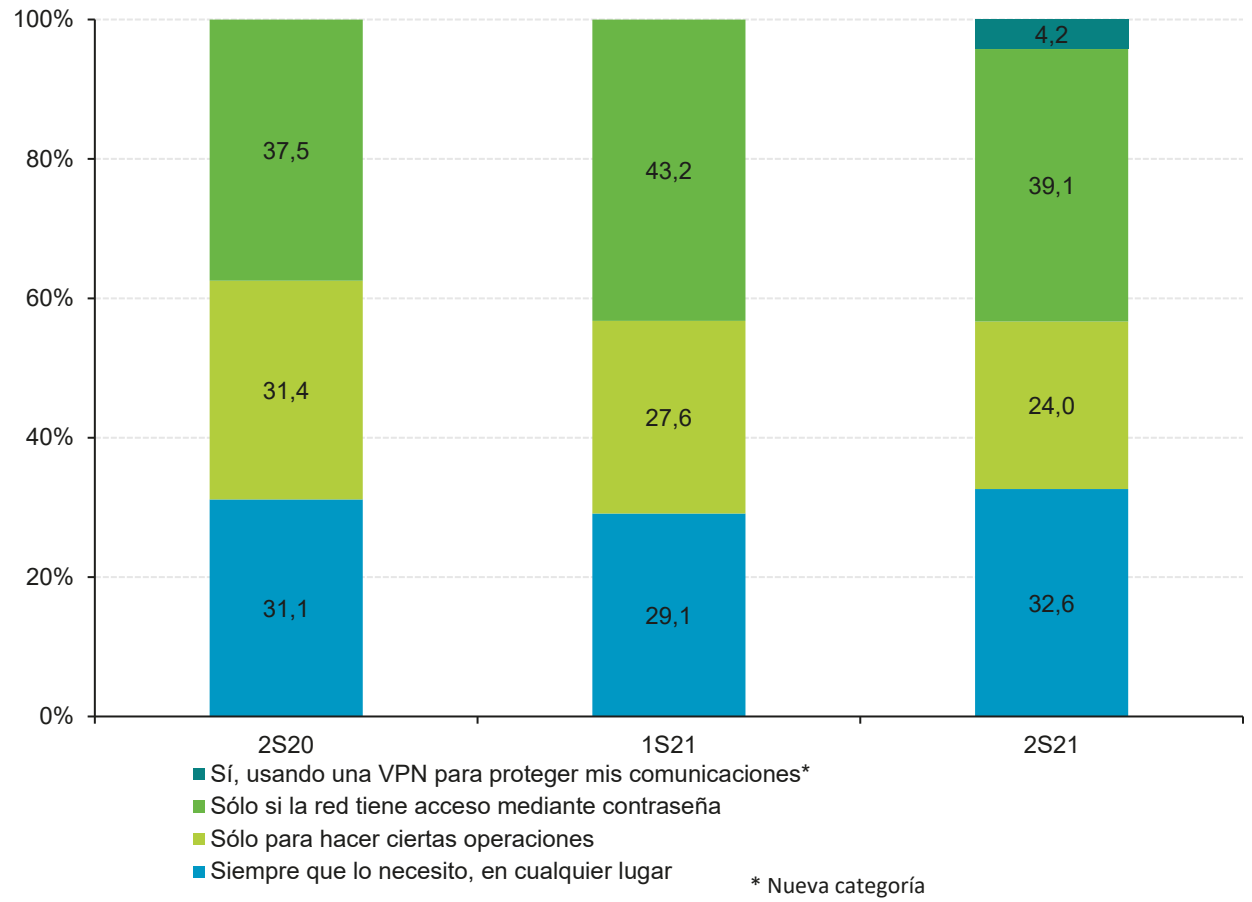
BASE: Total usuarios

Módulo VI: Seguridad en Wi-Fi

Motivo de uso de redes inalámbricas Wi-Fi públicas o de terceros

Aún hay un porcentaje elevado de panelistas que declara utilizar redes inalámbricas WiFi siempre que lo necesita sin importar si tiene contraseña o independientemente de la operación que va a realizar. Ésta es una práctica peligrosa para la privacidad. Siempre es recomendable la utilización de una VPN para usar este tipo de conexiones. El 4,2% de los usuarios declara el uso de VPN con este tipo de conexiones.

Cómo conectarte a redes Wi-Fi públicas de forma segura:
https://www.osi.es/es/actualidad/blog/2019/05/02/conexion-gratis-la-vista-conecto-mi-movil



BASE: Usuarios que se conectan a una red Wi-Fi pública o de otro usuario

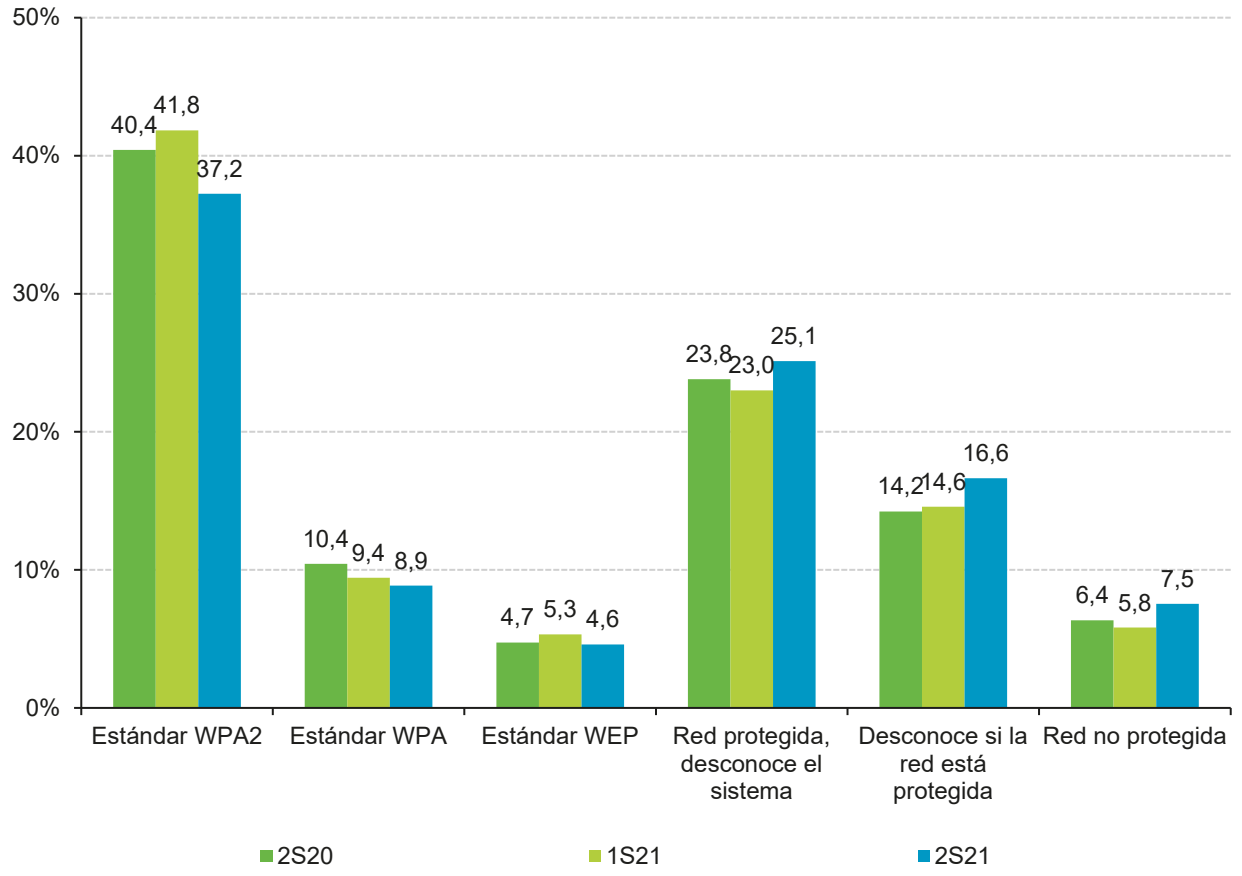
Módulo VI: Seguridad en Wi-Fi

Sistema de seguridad en la red Wi-Fi del hogar

El estándar WEP está en desuso ya que es el más fácil de romper. Sin embargo conforme a las declaraciones de los entrevistados, todavía el 4,6% utiliza este estándar para proteger la red de su domicilio.

Si es peligroso utilizar un estándar poco seguro, mucho más lo es el no tener protegida de ninguna forma la red del domicilio. Esta práctica ha aumentado entre los panelistas, en 1,7p.p. respecto al semestre anterior.

Cómo configurar tu red Wi-Fi de modo seguro: https://www.osi.es/protege-tu-wifi



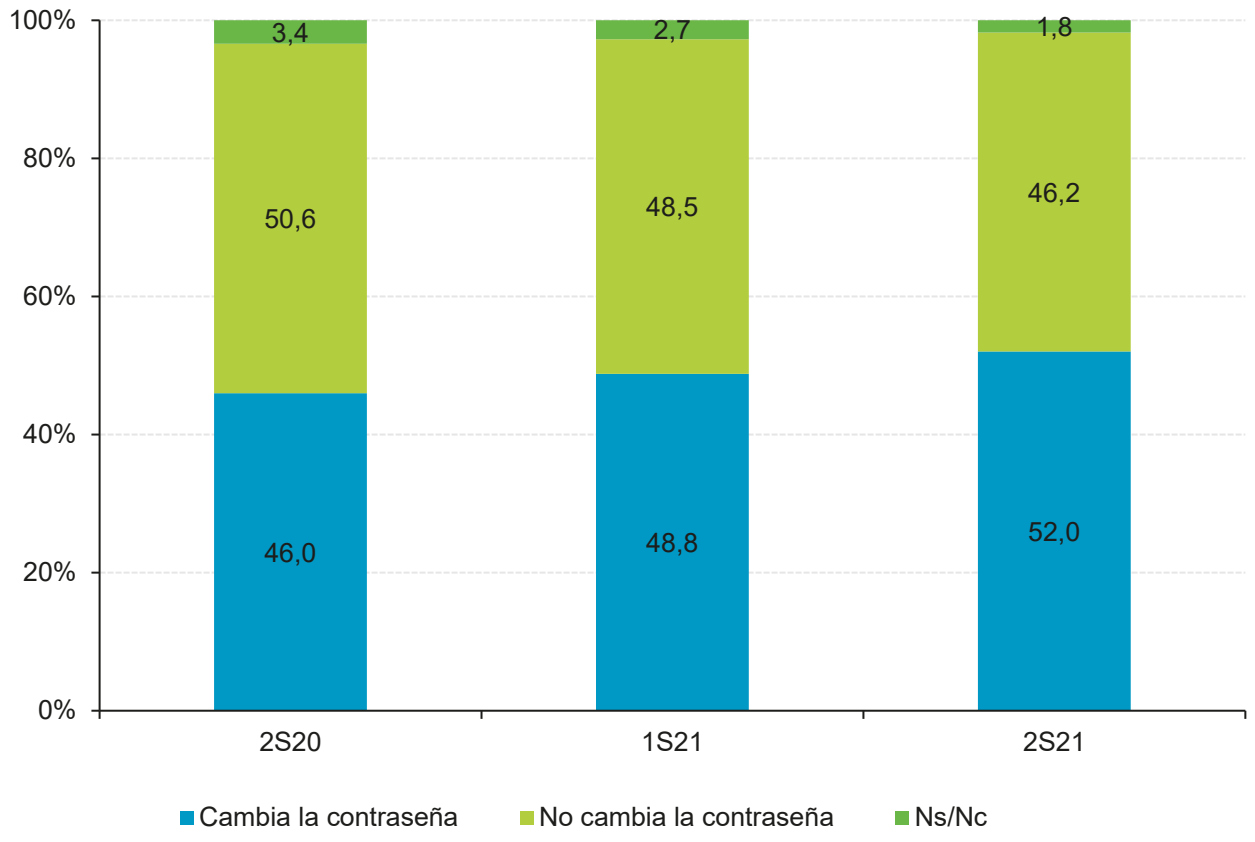
BASE: Usuarios con conexión Wi-Fi propia

Módulo VI: Seguridad en Wi-Fi

Modificación de la contraseña por defecto de la conexión Wi-Fi

Además de utilizar WPA2, WPA o WEP, es necesario cambiar la contraseña por defecto que traen los dispositivos de los operadores, como los routers. Ya que utilizar una contraseña personalizada, de un alto número de caracteres, símbolos, mayúsculas, minúsculas y números es más difícil de averiguar mediante ataques de fuerza bruta.

Parece que poco a poco los panelistas declaran cambiar la contraseña por defecto de la red WiFi de sus hogares, en concreto ha aumentado el número de panelistas en 3,2p.p.



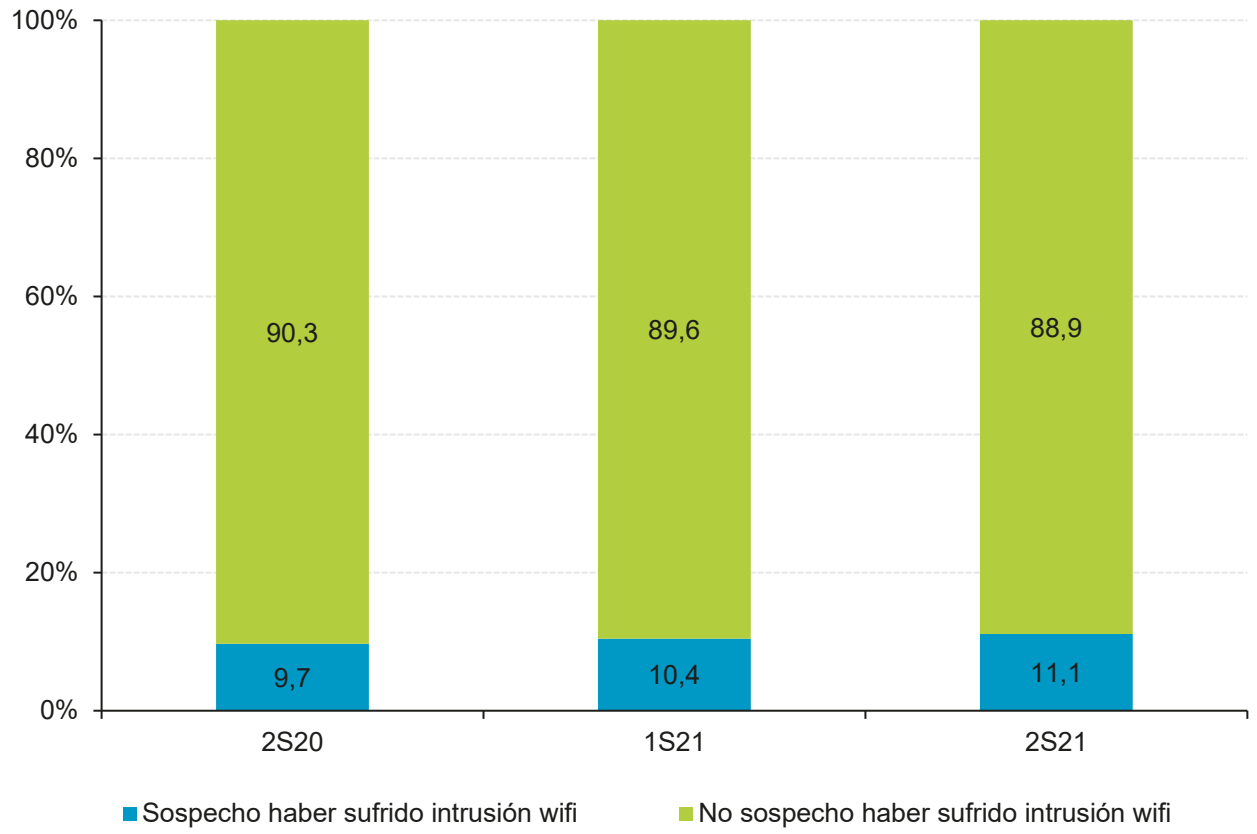
BASE: Usuarios con conexión Wi-Fi propia y sistema de seguridad

Módulo VI: Seguridad en Wi-Fi

Sospecha de haber sufrido una intrusión Wi-Fi (conexión a la red Wi-Fi sin consentimiento)

El porcentaje de panelistas seguros de no haber sufrido alguna intrusión a través de una red WiFi es levemente menor al del semestre anterior, en concreto 0,7 p.p.

¿Sabes cómo averiguar si alguien está conectado a la red inalámbrica Wi-Fi de tu hogar, cómo actuar al respecto, y como proteger la red para evitarlo?
https://www.osi.es/es/actualidad/blog/2019/09/25/descubre-y-elimina-los-intrusos-de-tu-red-wifi



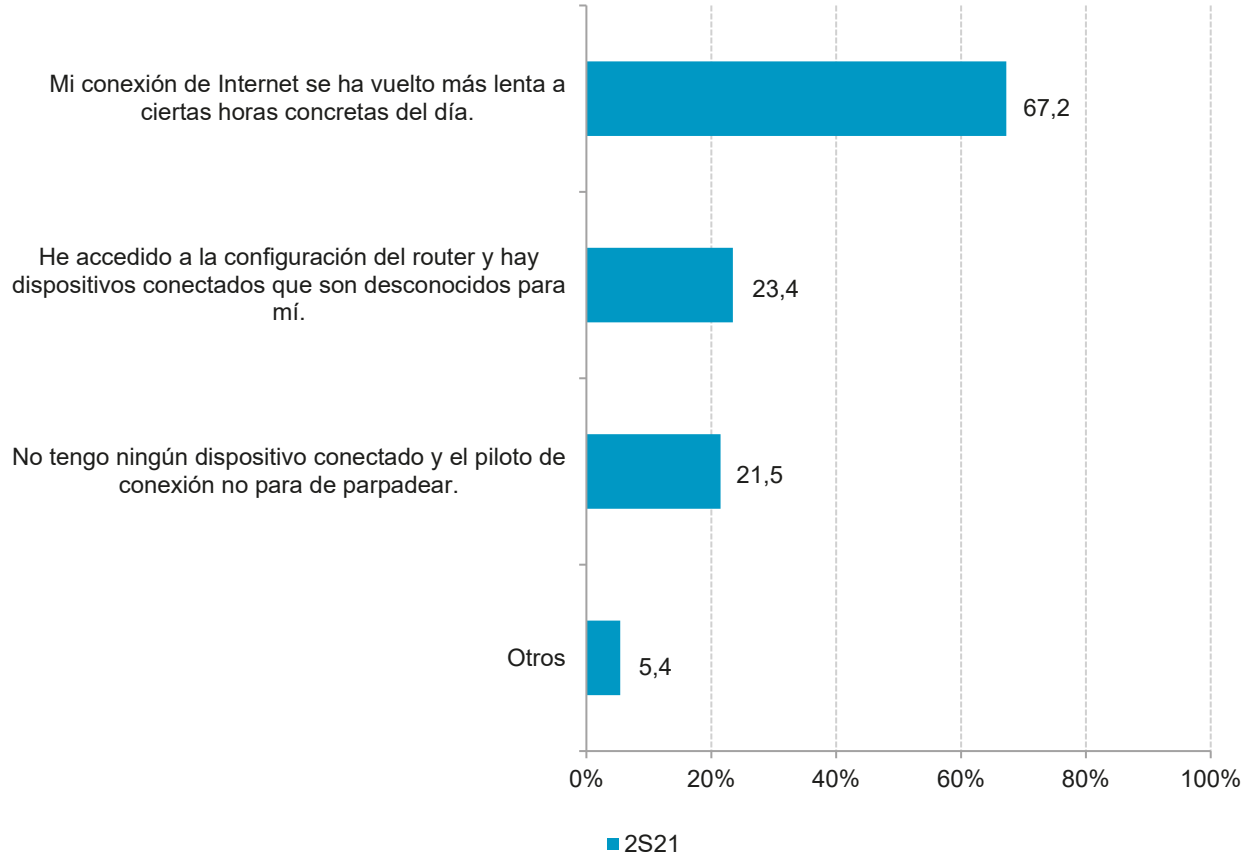
BASE: Usuarios con conexión Wi-Fi propia

Módulo VI: Seguridad en Wi-Fi

Motivos de sospecha de intrusión WiFi

Si algún intruso está consumiendo el ancho de banda, es posible notar que la red va más lenta. Éste es el motivo principal por el cual, el 67,2% de los usuarios opina que ha podido sufrir una intrusión en la red Wi-Fi de su hogar. Sin embargo, aunque es un indicio factible, no tiene que ser siempre motivado por una intrusión.

Otro parámetro más fiable para intuir una posible conexión no autorizada en nuestra red es acceder a la configuración del router del hogar. El 23.4% de los panelistas declaran que en su caso la intrusión Wi-Fi se ha identificado al comprobar la conexión de dispositivos desconocidos.



Base: Usuarios que declaran haber sufrido una intrusión WiFi

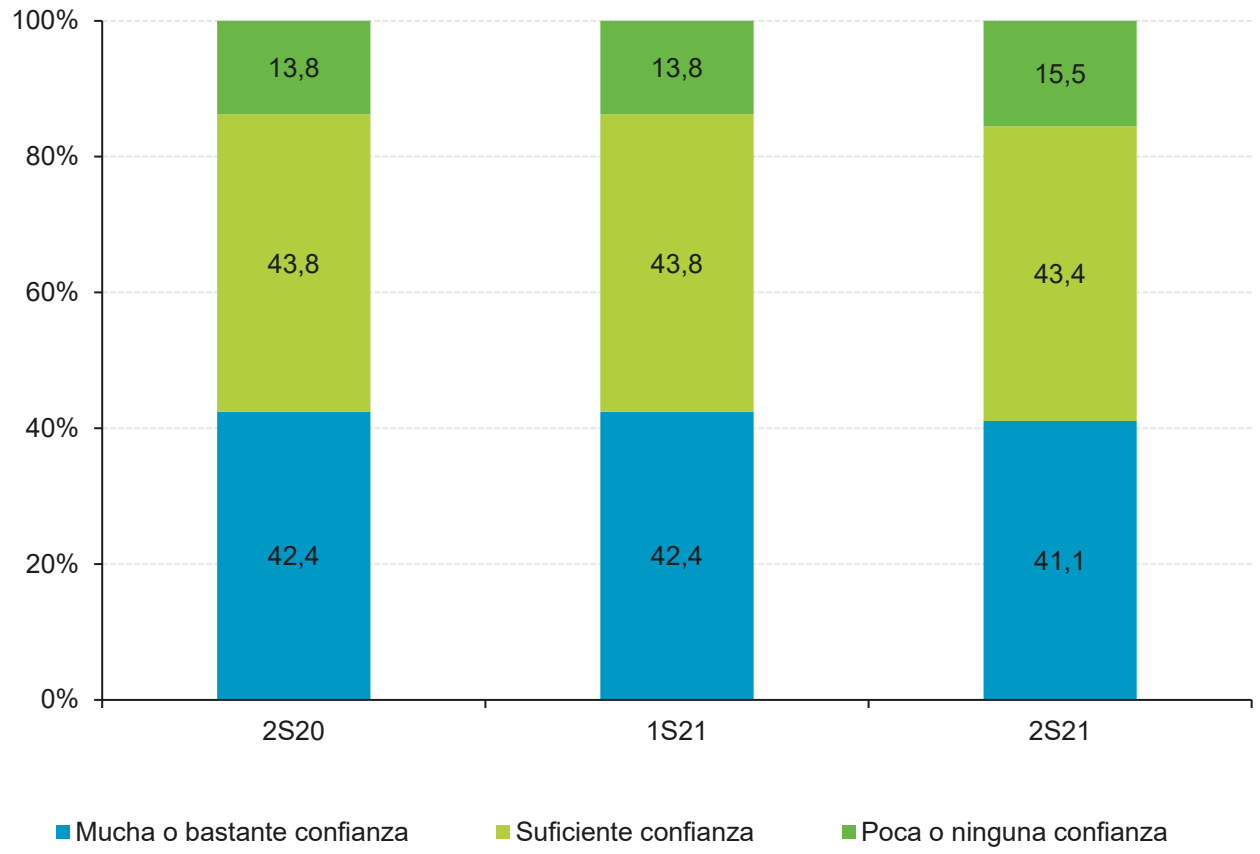
Módulo VII:
Opinión

Módulo VII: Opinión

Nivel de confianza en Internet

El nivel de confianza en Internet entre los panelistas, según sus declaraciones se mantiene constante o con leves variaciones a lo largo de 2021. Desciende en 1,3 p.p. el número de panelistas que declaran tener mucha confianza en Internet y se ve un leve aumento de 1,7 p.p. del número de usuarios entrevistados que tienen poca o ninguna confianza en Internet.

Estos datos quizás sean debidos al aumento de las estafas online, a la cantidad de phishing diario que se recibe a través del correo electrónico o quizás al aumento del smishing (mensajes SMS con enlaces a sitios web fraudulentos).



BASE: Total usuarios

Módulo VII: Opinión

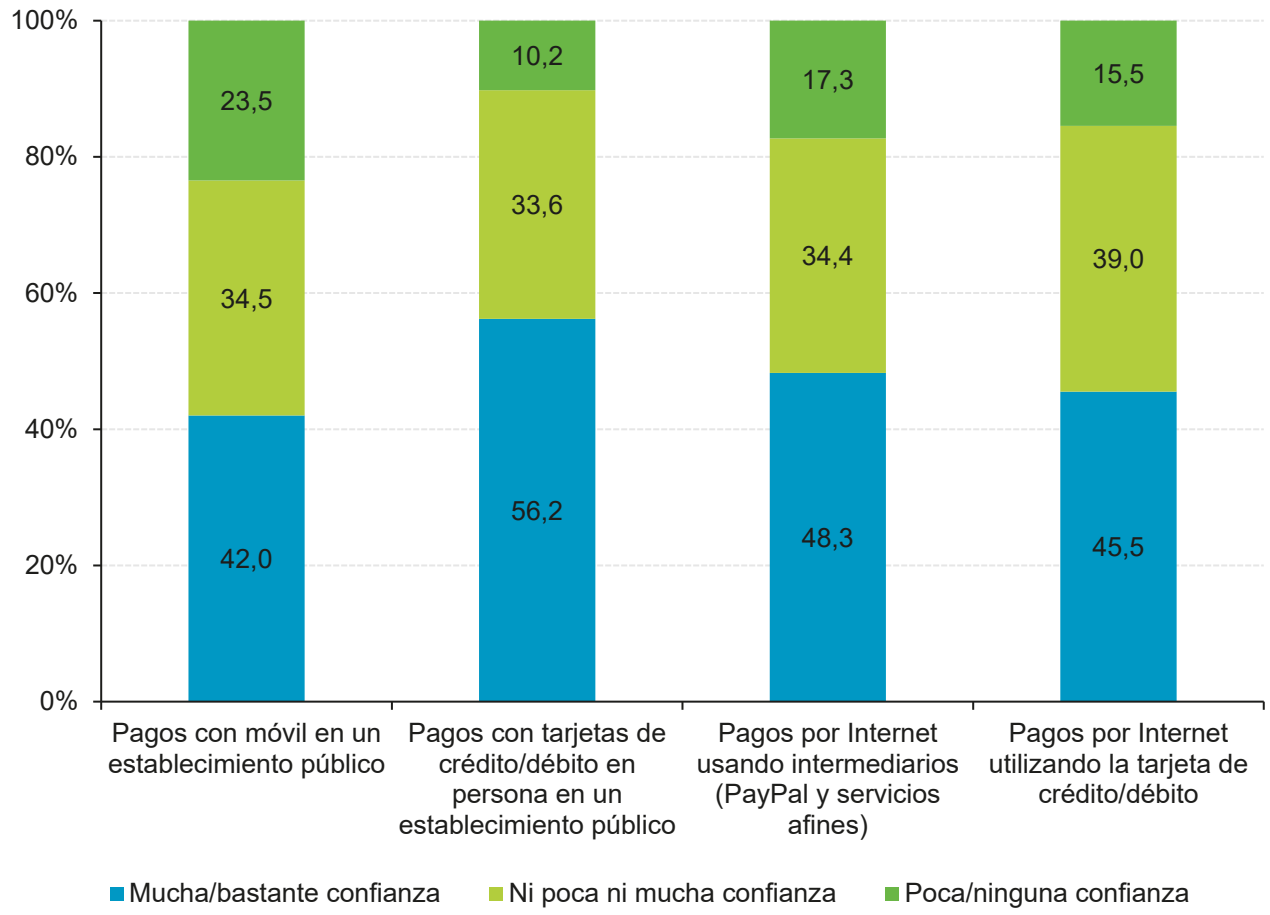
Nivel de confianza al realizar pagos (online y offline)

Desde el comienzo de la pandemia en 2020, se ha fomentado en establecimientos públicos, el pago a través de medios contactless. Bien sea a través de tarjetas de crédito/debito o a través de dispositivos electrónicos inteligentes como teléfonos móviles o Smartwatch.

Esto se puede ver reflejado en las declaraciones de los usuarios, en concreto respecto al medio más usado que es el pago con tarjeta de crédito/debito. El 56,2% tiene mucha confianza en este método de pago, seguido por el uso de PayPal y otros servicios (48,3%) en los que se utiliza un intermediario para realizar los pagos por Internet.

¿Sabes qué precauciones debes tener en cuenta para evitar caer en un engaño al realizar compras online?

https://www.osi.es/es/campanas/compras-seguras-online

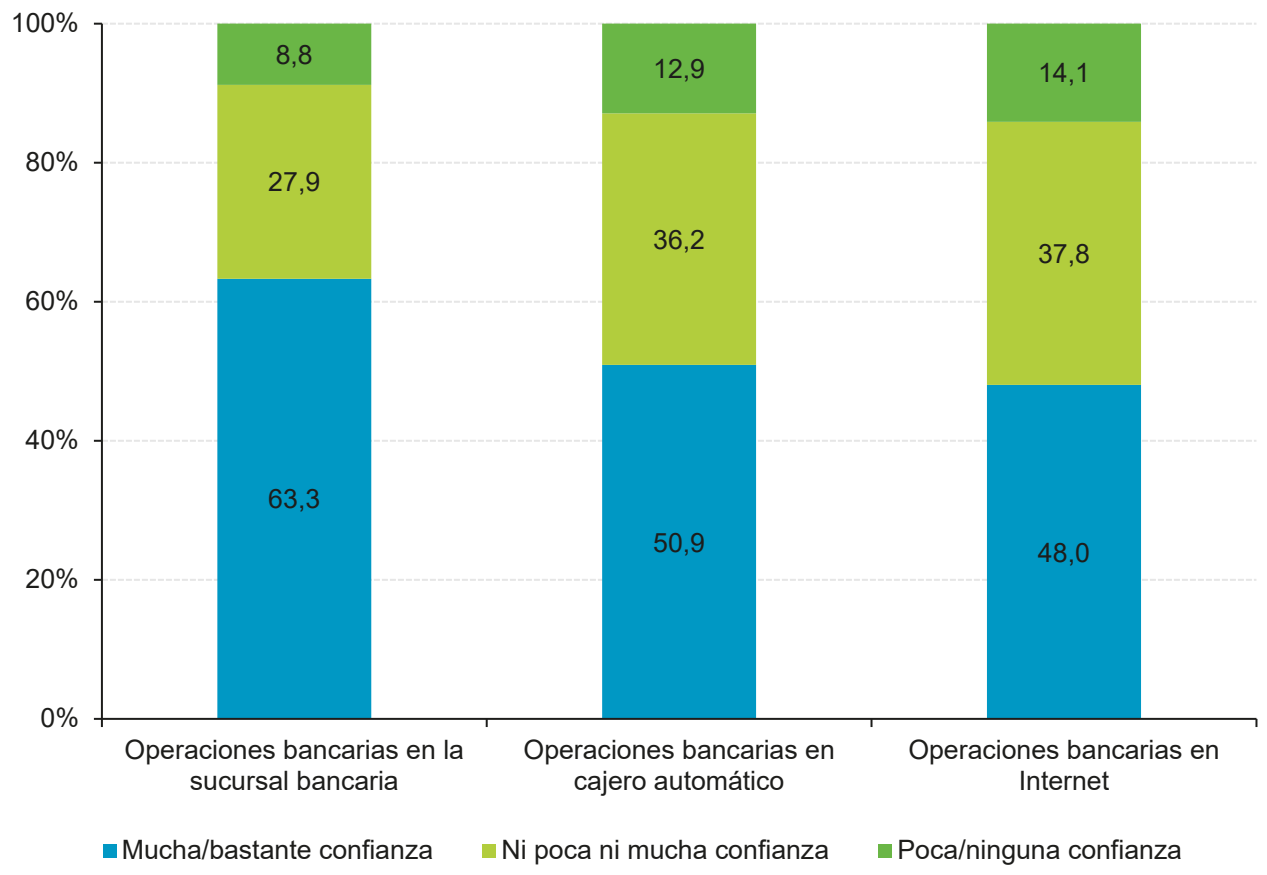


BASE: Total usuarios

Módulo VII: Opinión

Nivel de confianza al realizar operaciones bancarias (online y offline)

El nivel de confianza que declaran los entrevistados, respecto a las operaciones bancarias varía dependiendo del lugar donde se realicen las operaciones. Por ejemplo, el 63,3% de los entrevistados declara tener mucha confianza en la realización de operaciones en la propia sucursal bancaria. Mientras que el 48,8% tiene mucha confianza en realizar operaciones con su banco a través de Internet. Quizás este porcentaje pueda deberse a los controles de seguridad que ofrecen las diferentes entidades de banca online.

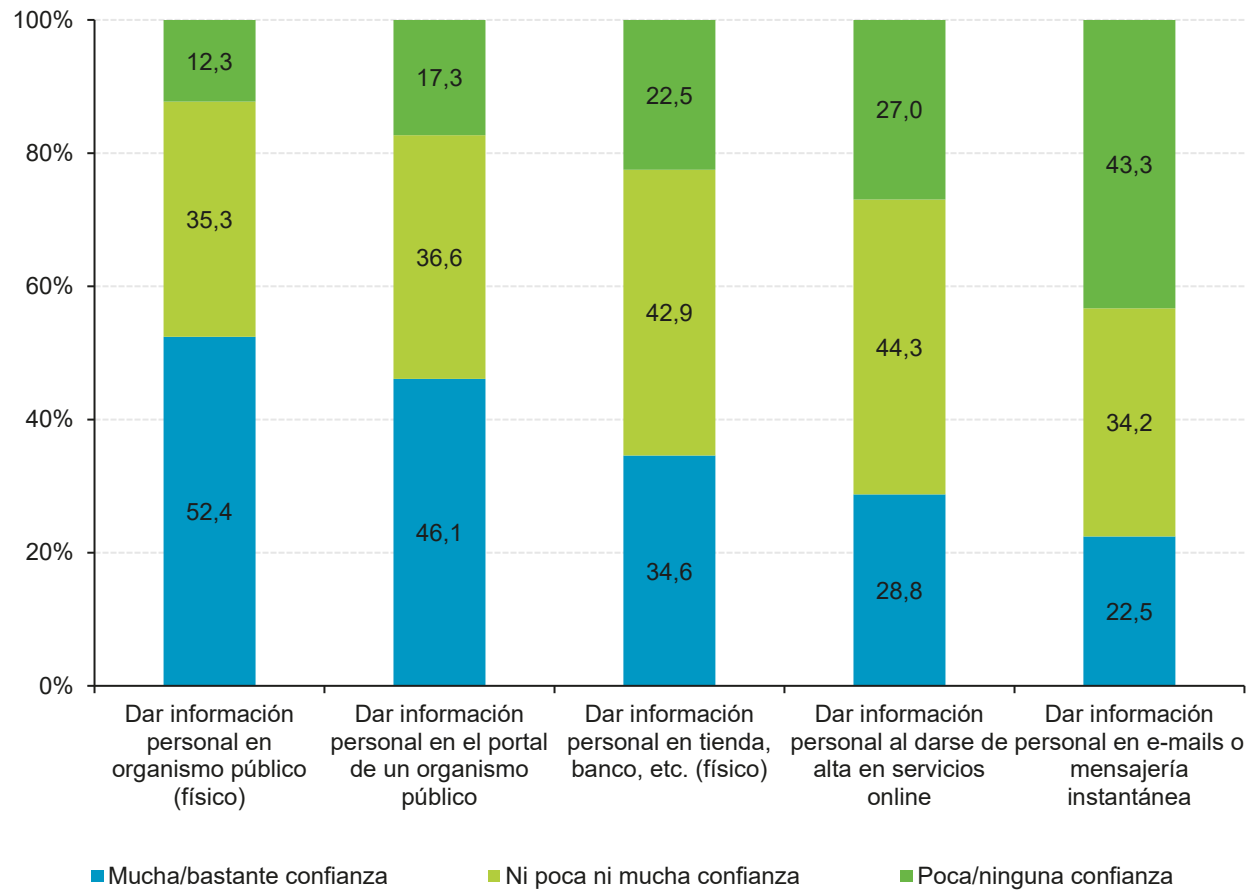


BASE: Total usuarios

Módulo VII: Opinión

Nivel de confianza al facilitar información personal
(online y offline)

En Internet es habitual encontrar que para acceder a una información o descargar un archivo, el portal que ofrece ese recurso solicite cierta información sobre el usuario a cambio de facilitar ese recurso. Esta práctica es de las más extendidas. Quizás por este motivo un alto porcentaje de panelistas declaran que tienen poca confianza en dar información por correo (43,3%) o en alta de servicios (27%). En contraposición declaran más confianza en facilitar información personal en un organismo público de manera física (52,4%) que a través de Internet en la página oficial (46,1%).



BASE: Total usuarios

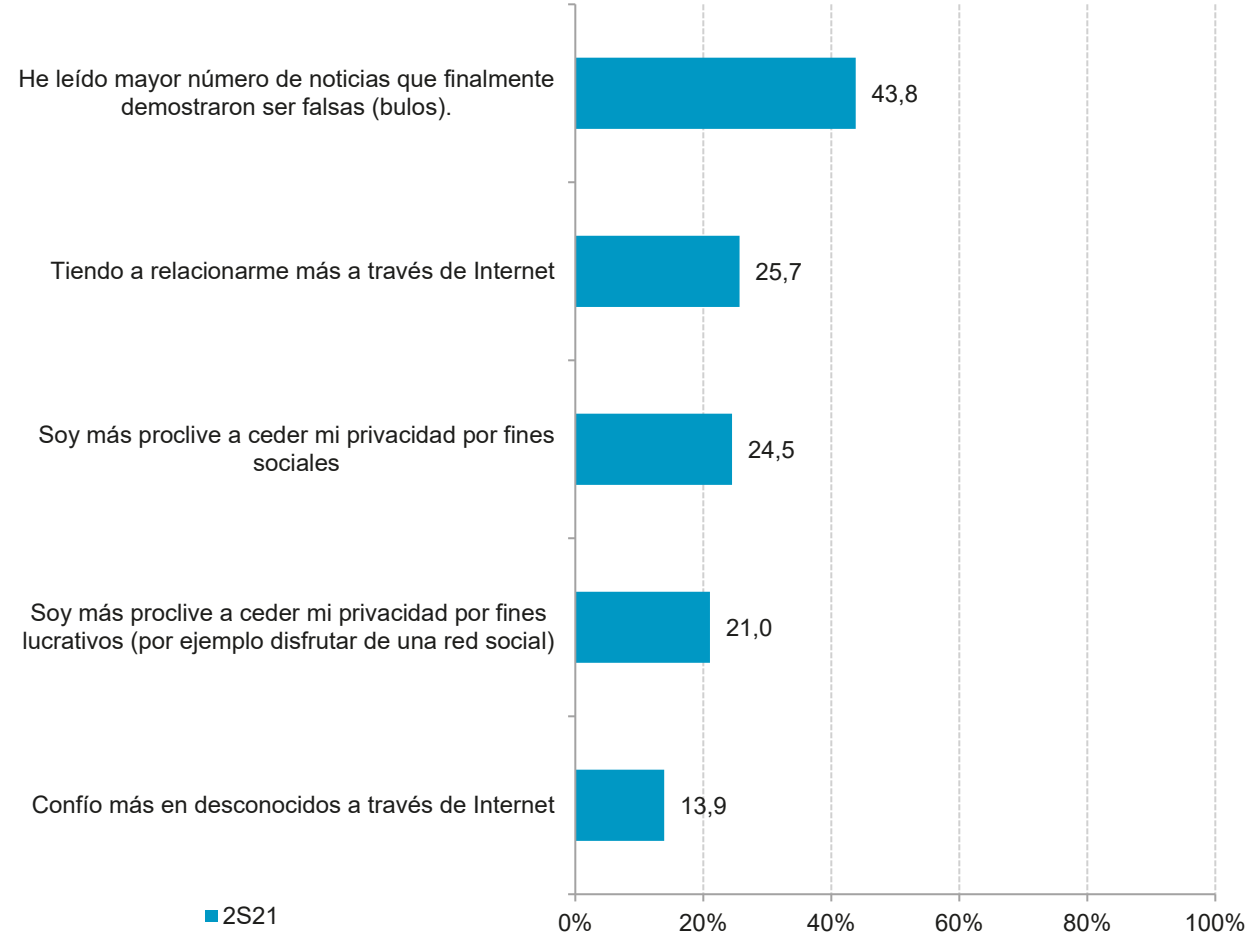
Módulo VII: Opinión

Opiniones sobre hábitos adquiridos tras el confinamiento motivado por la pandemia

(de acuerdo o totalmente de acuerdo)

Durante la crisis sanitaria del Covid19 de 2020, estuvieron en auge las fake news, noticias falsas o bulos. Pero no solo en ese periodo de tiempo sino que el 43,8% de los usuarios que participan en este estudio, opina que en 2021 ha leído un mayor número de noticias que finalmente han resultado ser bulos.

Dado que la pandemia en 2021 no ha terminado y pese a lo que podría parecer, tan solo el 25,7% de los entrevistados manifiesta que tiende a relacionarse más a través de internet.



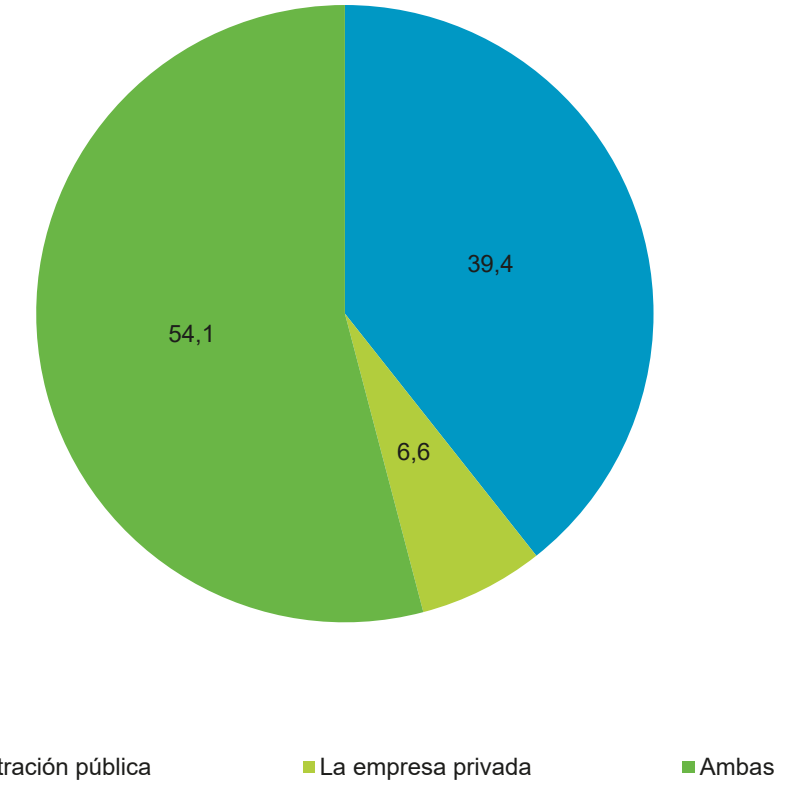
BASE: Total usuarios

Módulo VII: Opinión

Opiniones sobre los agentes que deberían impulsar las iniciativas en materia de ciberseguridad

Los usuarios entrevistados manifiestan en un 54,1% que las entidades que deberían impulsar iniciativas en materia de seguridad deberían ser tanto la administración pública como las empresas privadas. Y en un porcentaje un poco menor (39,4%) opinan que debería ser la administración pública.

Anualmente el gobierno, a través de diferentes administraciones, promueve campañas para concienciar de los peligros derivados de Internet en concreto durante 2021 en las cadenas de televisión se ha podido ver la campaña de "hoy es un anuncio, pero mañana puede pasarte a ti" en la que simulaban en pantalla como un ransomware podría secuestrar el SmartTV o el ordenador.



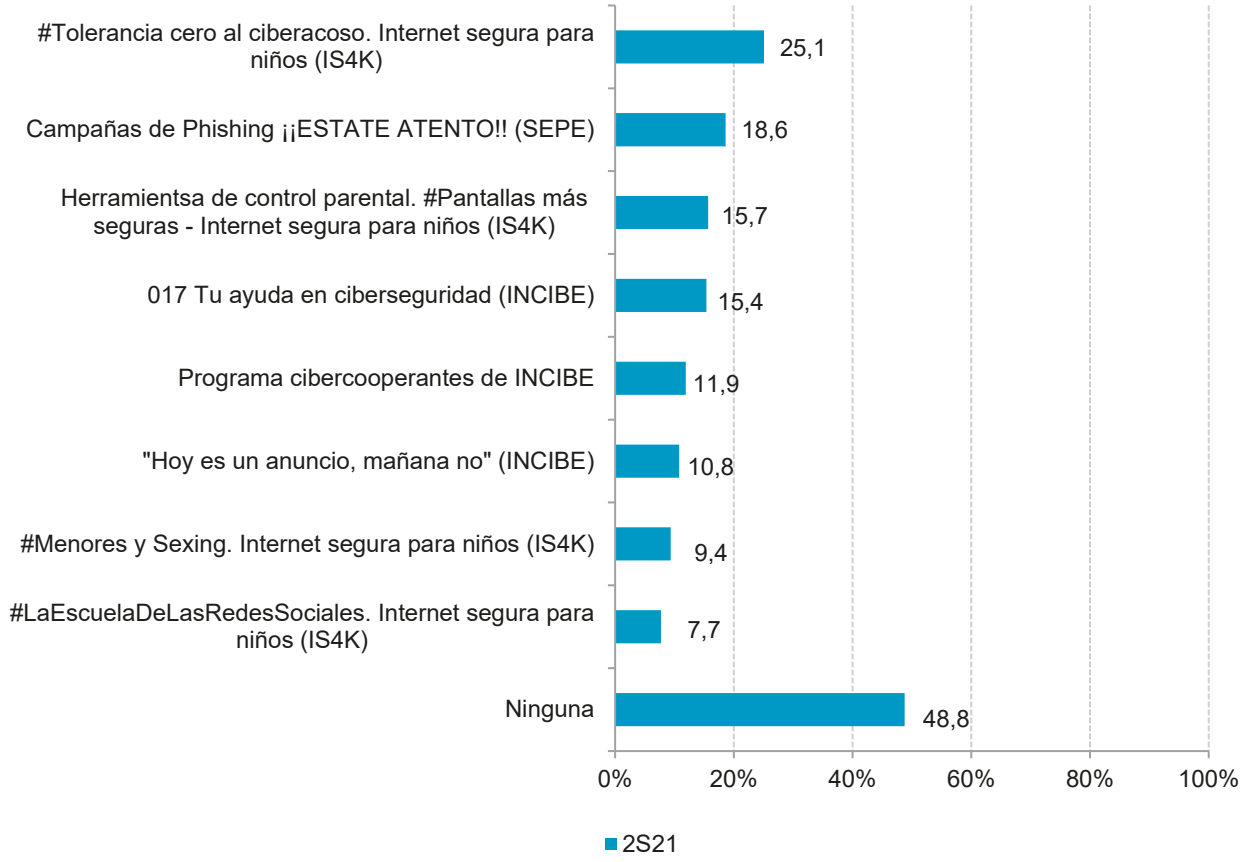
BASE: Total usuarios

Módulo VII: Opinión

Campañas conocidas realizadas por el gobierno en materia de ciberseguridad.

Tal vez una de las campañas que previsiblemente ha podido llegar a más público fuera de las redes es la campaña de "hoy es un anuncio, mañana no" esta campaña cuyo medio de difusión fue la televisión tan solo ha sido reconocida por el 10,8% de los panelistas.

A lo largo del semestre se han difundido diferentes campañas por parte de diferentes administraciones como son INCIBE, IS4K y SEPE. También se ha consultado a los usuarios si conocían alguna de ellas. A este respecto, el 25,1% ha manifestado conocer la campaña que hizo IS4K sobre el ciberacoso y la Internet segura para niños. El 18,6% conoce la campaña "Estate atento" del SEPE en la que se trataron de dar consejos sobre cómo evitar el phishing.



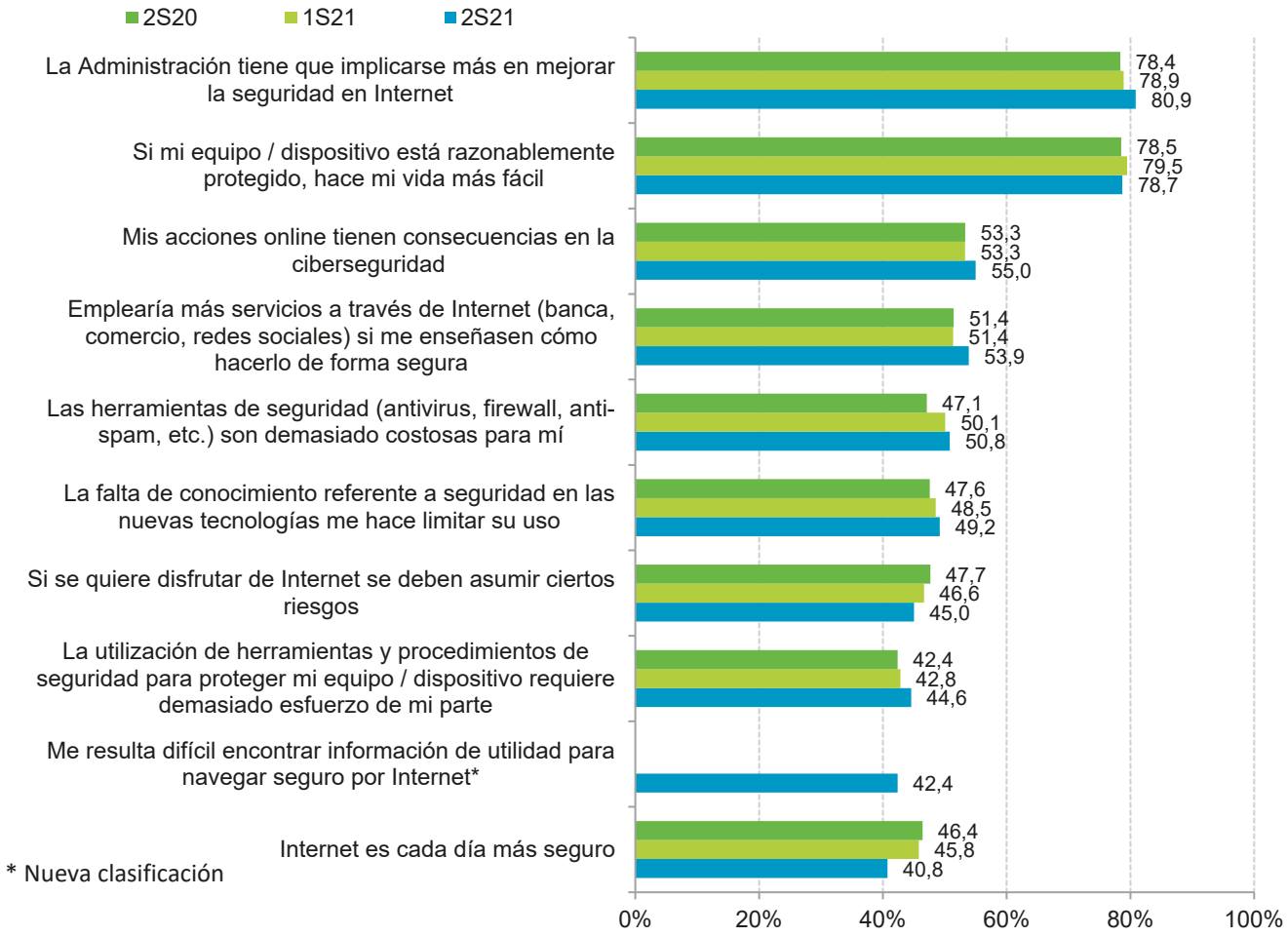
Base: Usuarios que se registran en portales de descarga de contenido gratuito

Módulo VII: Opinión

Opiniones sobre la seguridad en Internet
(de acuerdo o totalmente de acuerdo)

Uno de los puntos críticos de este estudio es promover mejoras para los usuarios de Internet, por lo que analizar las opiniones de los internautas sobre la seguridad en Internet resulta fundamental para abordar este objetivo.

La opinión más destacada por los usuarios entrevistados es que la administración tiene que implicarse más en mejorar la seguridad en Internet. Esta opinión la manifiestan el 80,9% de los usuarios, aumentando incluso respecto al semestre anterior. Precisamente, la administración pública cada año organiza diferentes campañas de concienciación sobre ciberseguridad que hace llegar a los usuarios a través de diferentes medios de difusión, empleando inclusive campañas televisivas



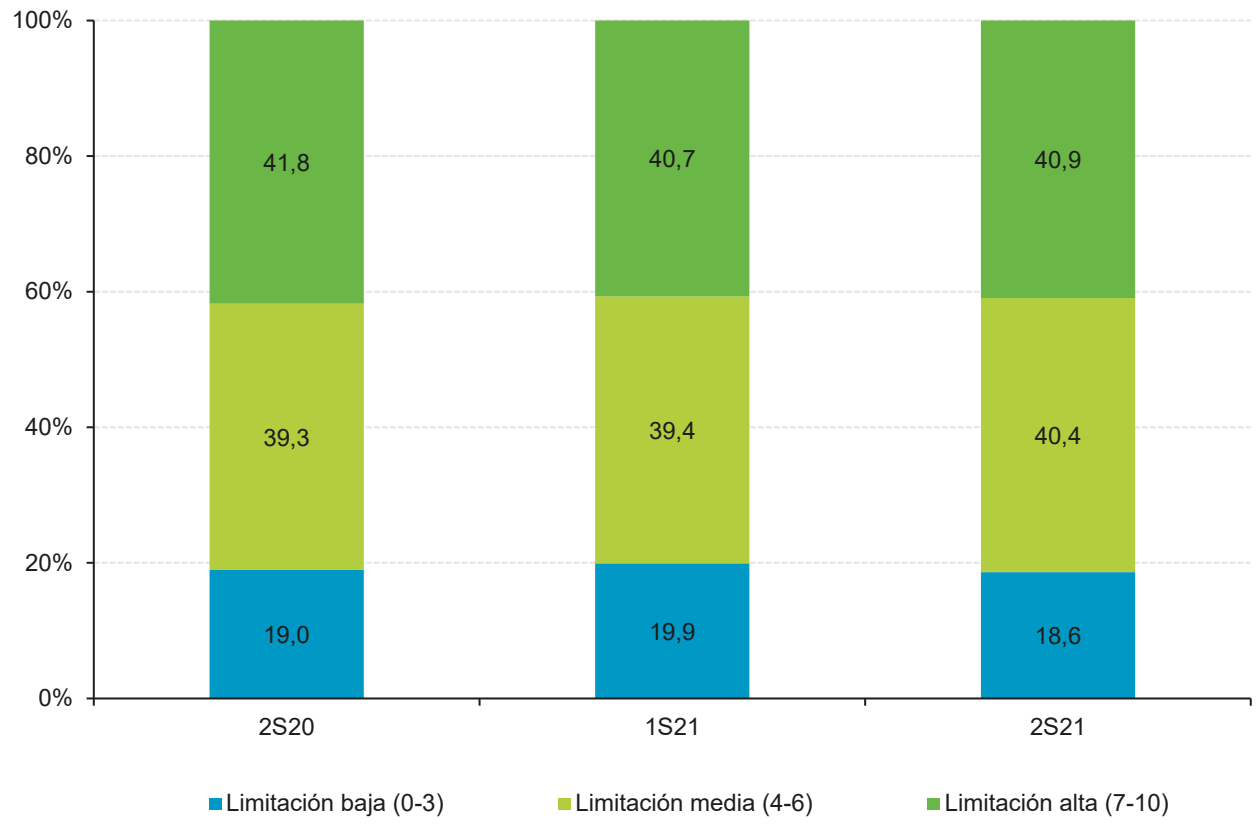
* Nueva clasificación

BASE: Total usuarios

Módulo VII: Opinión

Seguridad como factor limitante en la utilización de nuevos servicios en Internet

La opinión sobre si la seguridad es un factor limitante en el uso de nuevos servicios de Internet se mantiene prácticamente sin cambios a lo largo de los semestres. Las declaraciones de los panelistas entrevistados muestran que el 40,4% cree que la seguridad limita el uso de nuevos servicios de Internet.



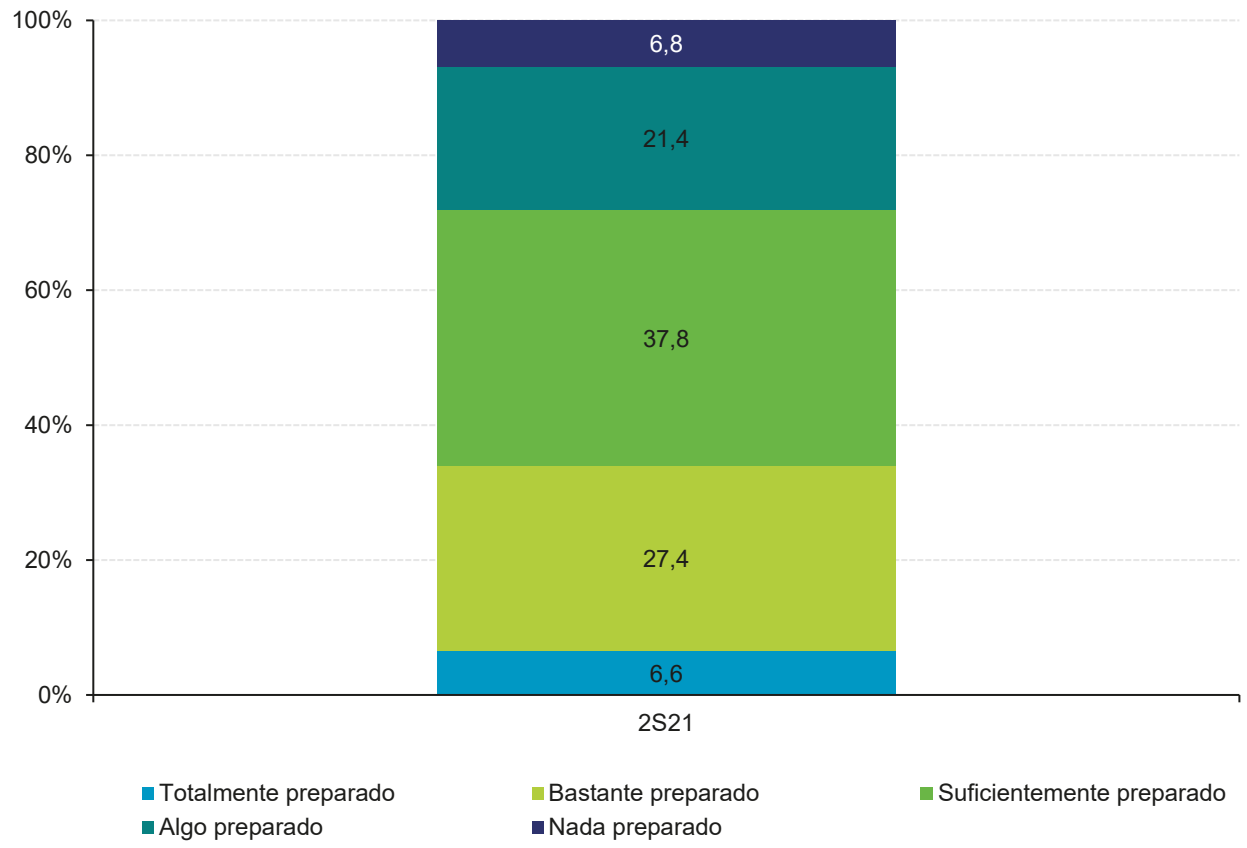
BASE: Total usuarios

Módulo VII: Opinión

Preparación para afrontar posibles problemas de ciberseguridad

Si abordamos la preparación sobre cómo afrontar posibles problemas de seguridad, las opiniones de los usuarios entrevistados están divididas.

Tan sólo el 6,61% de los internautas se considera totalmente preparado para afrontar los desafíos de seguridad. El 27,39% manifiesta estar bastante preparado mientras que el 37,83% declara que está suficientemente preparado. Los sectores más dudosos abarcan el 21,35% (se consideran algo preparados) y el 6,82% (nada preparado).

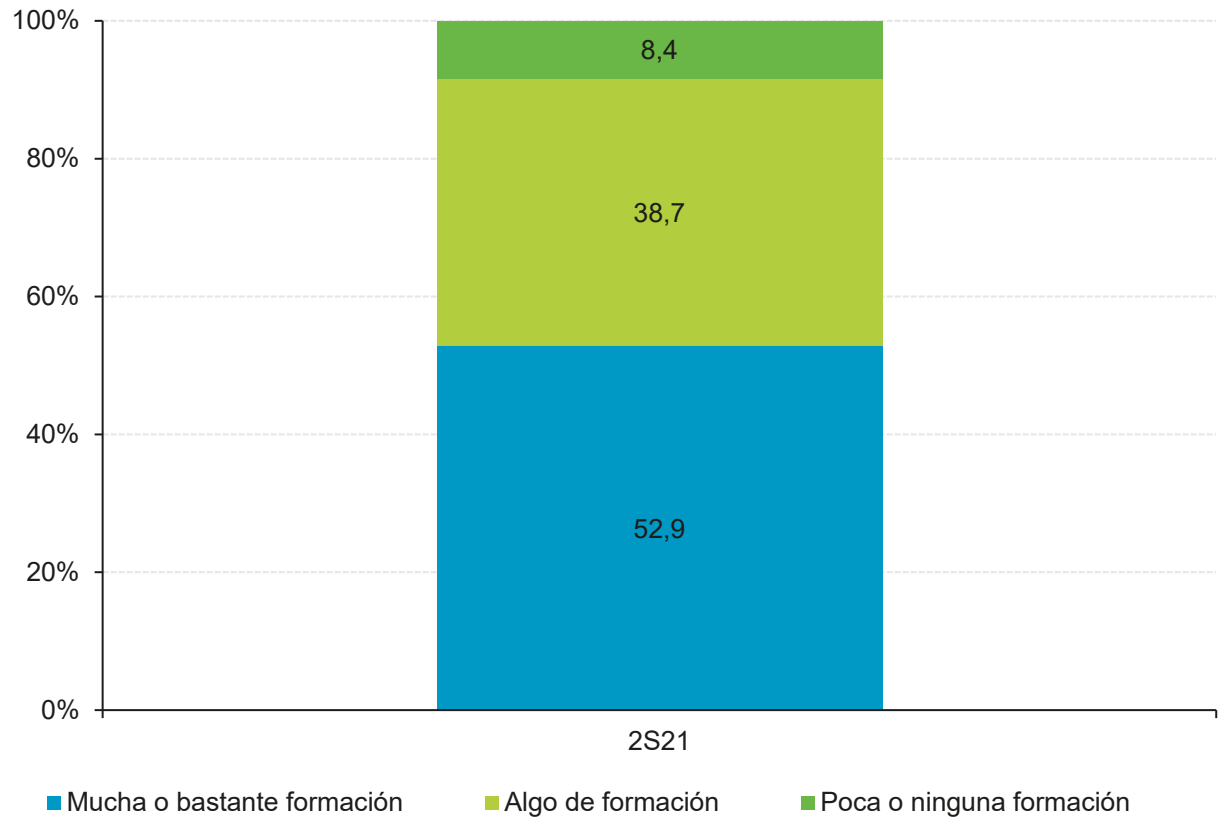


BASE: Total usuarios

Módulo VII: Opinión

Necesidad de formación en ciberseguridad

Cuando se ha consultado a los internautas si creen que es necesaria la formación en ciberseguridad, más de la mitad de los entrevistados, en concreto el 52,9%, manifiesta que es necesaria mucha o bastante formación en ciberseguridad. Sumado al 38,7% que declara necesitar algo de formación, podríamos concluir que el 91,6% de los internautas ven necesaria la formación en esta materia.



BASE: Total usuarios

Módulo VII: Opinión

Percepción de los riesgos a los que se está más expuesto al navegar por Internet

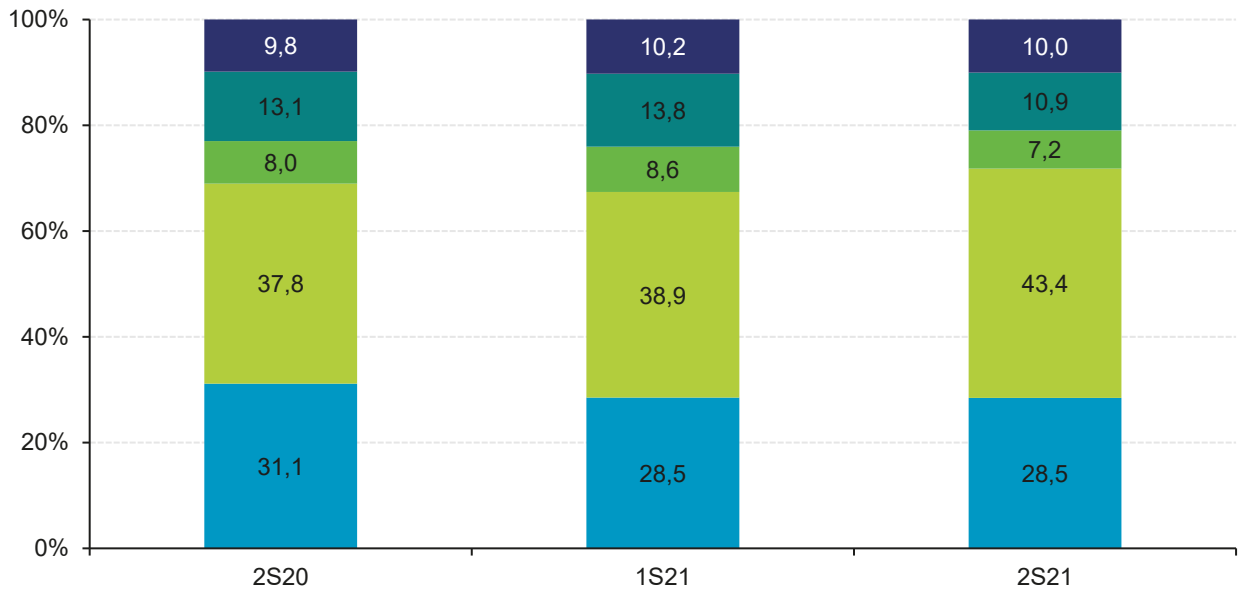
Un mayor número de usuarios de los entrevistados, en concreto 4,5 p.p. tienen la percepción de que están muy expuestos a fraudes online. Además la preocupación por la privacidad también sigue siendo un factor que les preocupa, aunque el porcentaje no varia respecto al semestre anterior.

¿Sabes como cuidar tu privacidad en Internet y tus datos en la nube?

✓ ***Borra tu huella:*** *https://www.youtube.com/watch?v=FT1FjR1XQ2w&feature=youtu.be*

✓ ***Cómo disminuir tu rastro en Internet:*** *https://www.osi.es/es/como-disminuir-tu-rastro-en-internet*

✓***Ejerciendo el "derecho al olvido":*** *https://www.osi.es/es/actualidad/historias-reales/2020/11/04/ejerciendo-el-derecho-al-olvido*



*nuevas categorías

BASE: Total usuarios

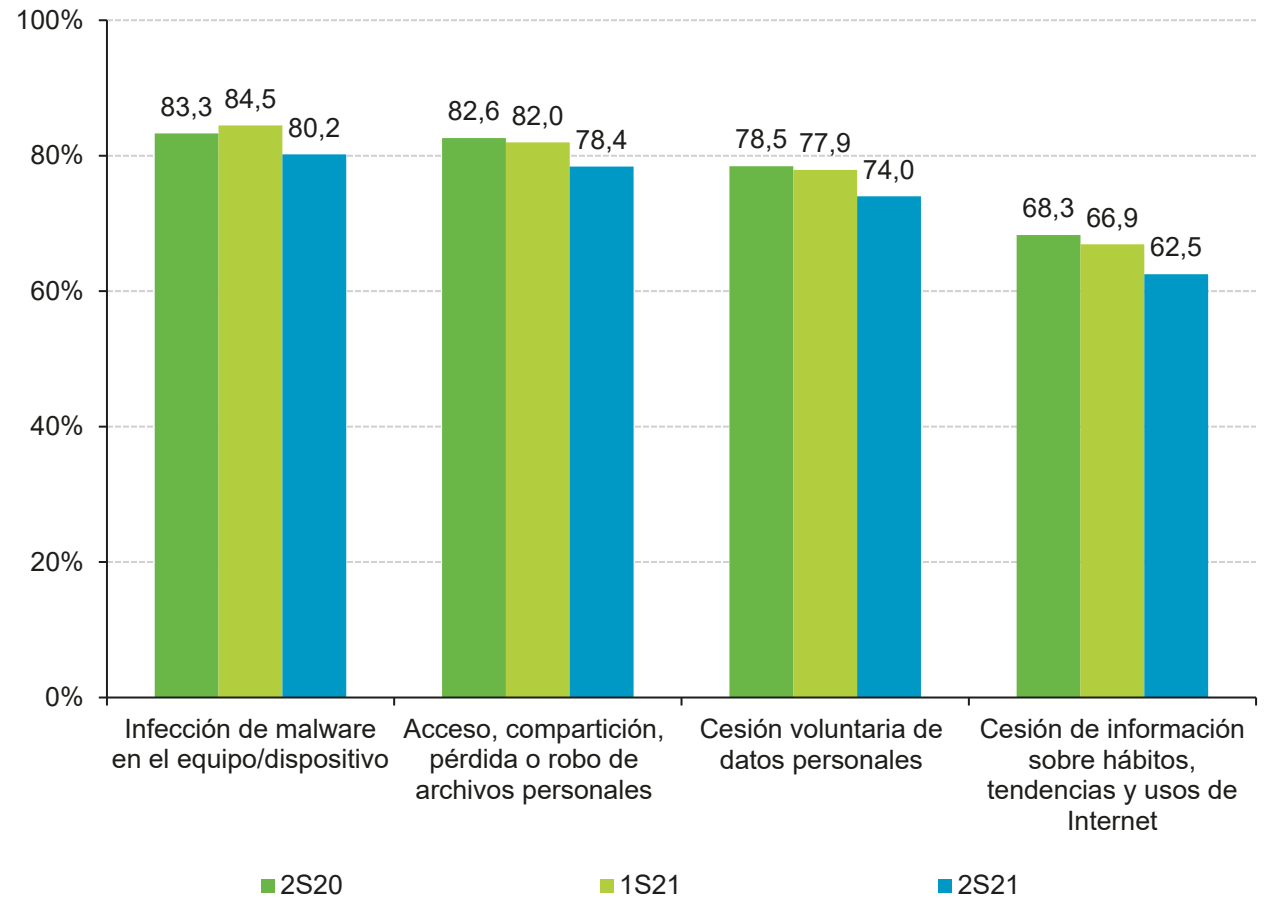
Módulo VII: Opinión

Valoración de los peligros al navegar por Internet

(bastante o muy importante)

Los peligros del malware son evidentes pero no son los únicos peligros a los que hay que enfrentarse a diario. La pérdida o robo de datos personales y la cesión del historial de uso de páginas web o aplicaciones también son perjudiciales ya que, hacen que pierdan privacidad.

Analizando la percepción de los panelistas frente a los peligros ya mencionados, el que más importancia adquiere según declaran, es la infección de malware (80,2%) seguido por el robo o perdida de datos (78,4%) y lo que consideran menos importante en comparación con los dos ítems ya mencionados, es la cesión de datos personales ya sea voluntaria (74%) o no (62,5%).



BASE: Total usuarios

Módulo VIII:

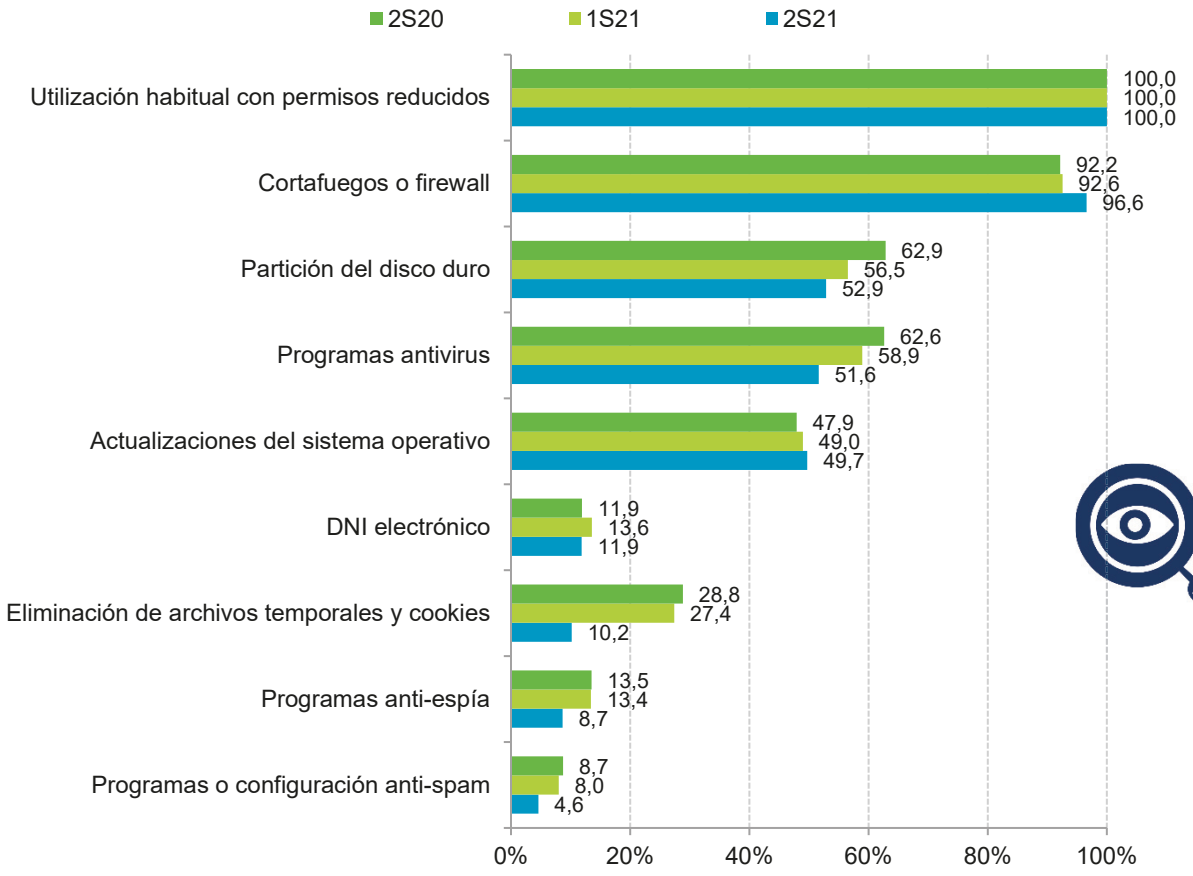
Datos reales procedentes de los análisis realizados por Pinkerton

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Uso real de medidas de seguridad en el ordenador del hogar

Mientras que el 56,1% de los entrevistados afirma tener las actualizaciones al día, la realidad conforme los datos recabados por el software Pinkerton, es que tan solo el 49,7% tiene el ordenador de casa actualizado con las últimas actualizaciones para su sistema operativo.

Utiliza la cuenta de usuario estándar para el uso diario del ordenador, dejando la cuenta de administrador sólo para cuando sea estrictamente necesario. Más información sobre las cuentas de usuario y cómo configurarlas en: https://www.osi.es/cuentas-de-usuario



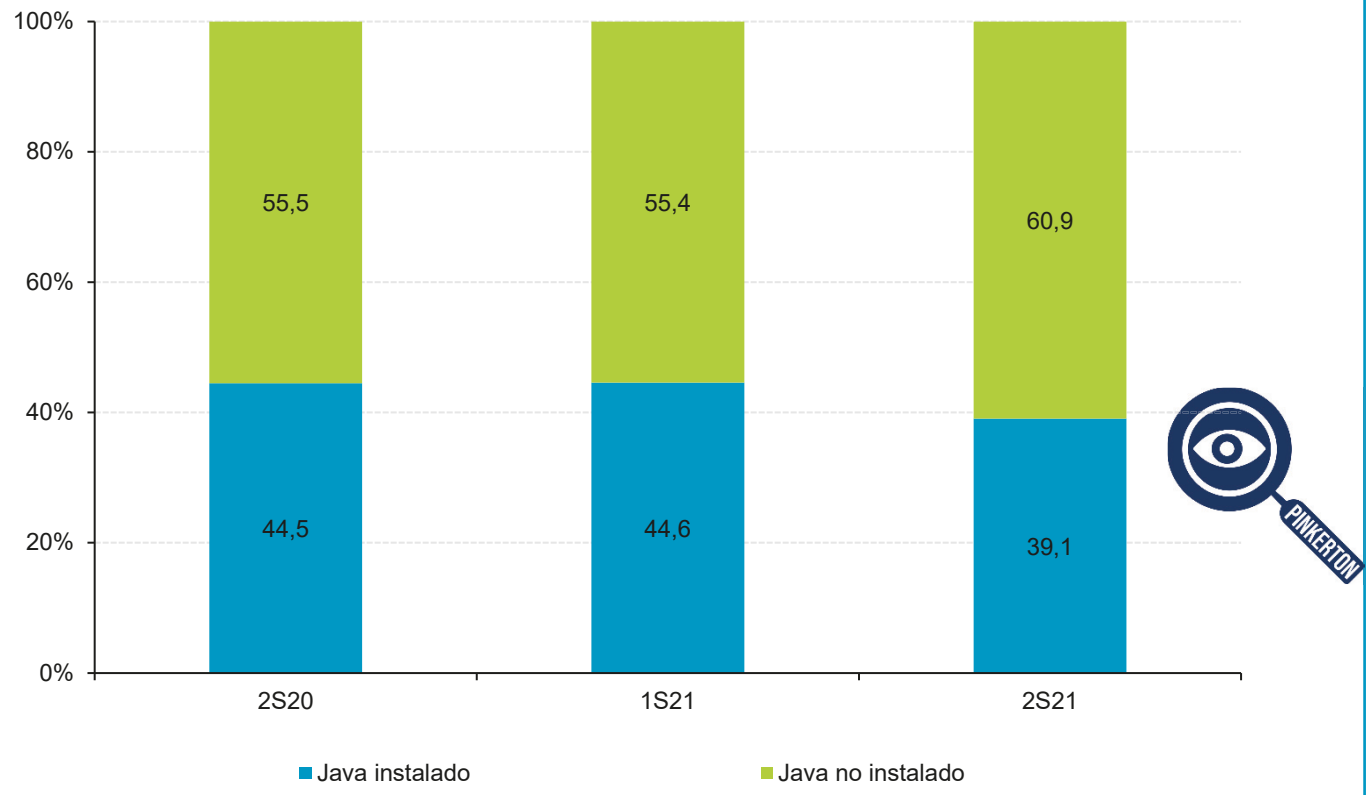
Base: Usuarios de PC

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Entorno Java en el ordenador del hogar

Los sistemas operativos como Windows tienen una serie de características de seguridad para mitigar las amenazas como puede ser Windows defender. Han sido diversas las ocasiones en las que los atacantes han tratado de incluir malware en el entorno Java. Este entorno es utilizado por cantidad de programas para que funcionen correctamente. El software con el que se realiza este estudio, arroja que el 60,9% de los usuarios no tiene Java instalado en su equipo con Windows. Se ve un aumento del número de usuarios en 5,5 p.p. respecto a los usuarios que no tenían instalado Java en el semestre anterior.

El aprovechamiento y explotación de vulnerabilidades en Java ha sido, a lo largo de los últimos años, uno de los vectores de entrada más utilizados por el malware para infectar equipos con una versión de este software desactualizada.



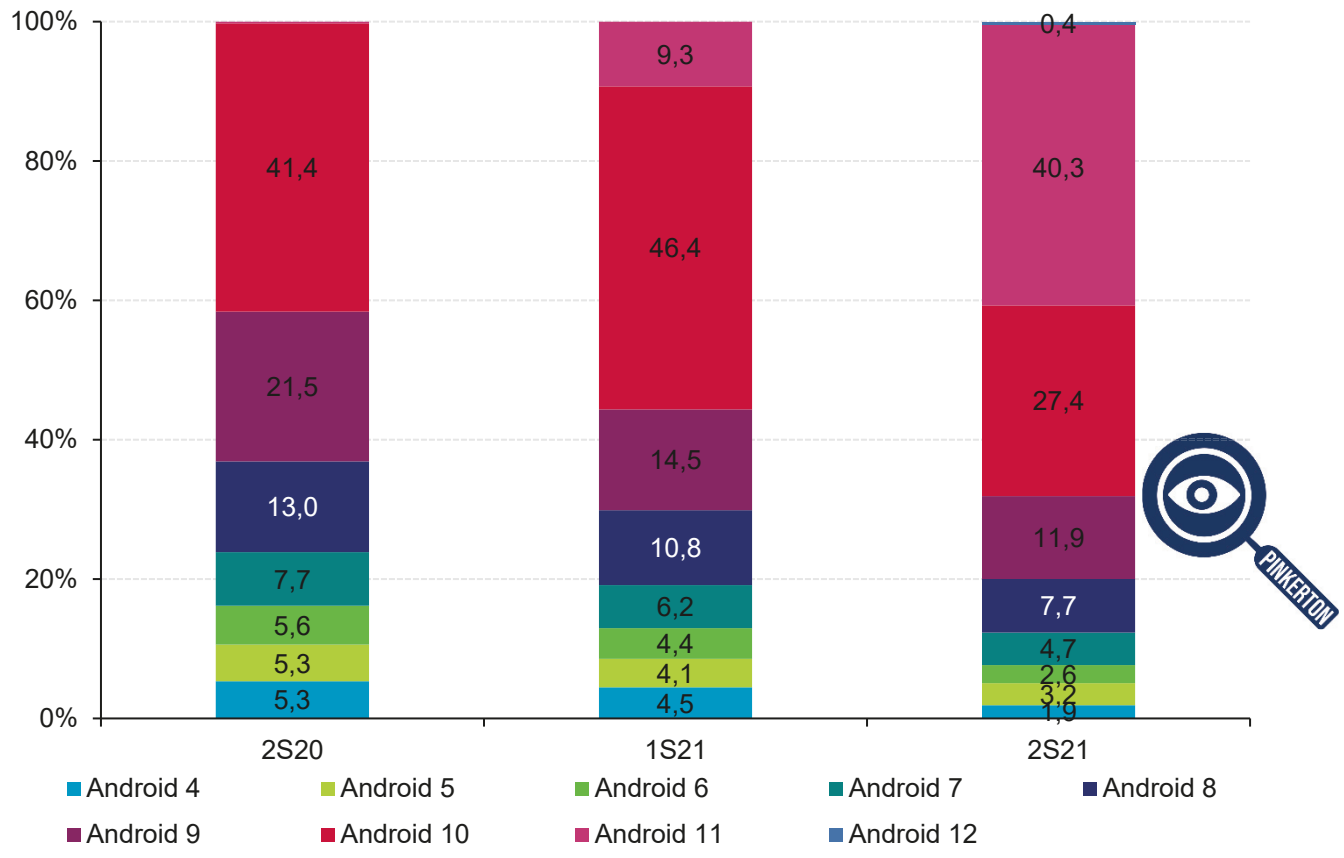
Base: Usuarios de Microsoft Windows

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Versiones de Android

Android 12 salió en su versión beta el 18 de mayo de 2021, siendo su primer lanzamiento oficial el 4 de octubre de 2021.

Sólo el 0,4% de los dispositivos Android analizados se encuentra actualizado a esta última versión, aunque aumenta significativamente el número de dispositivos actualizados a la versión previa, Android 11.



Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Uso real de medidas de seguridad en dispositivos Android

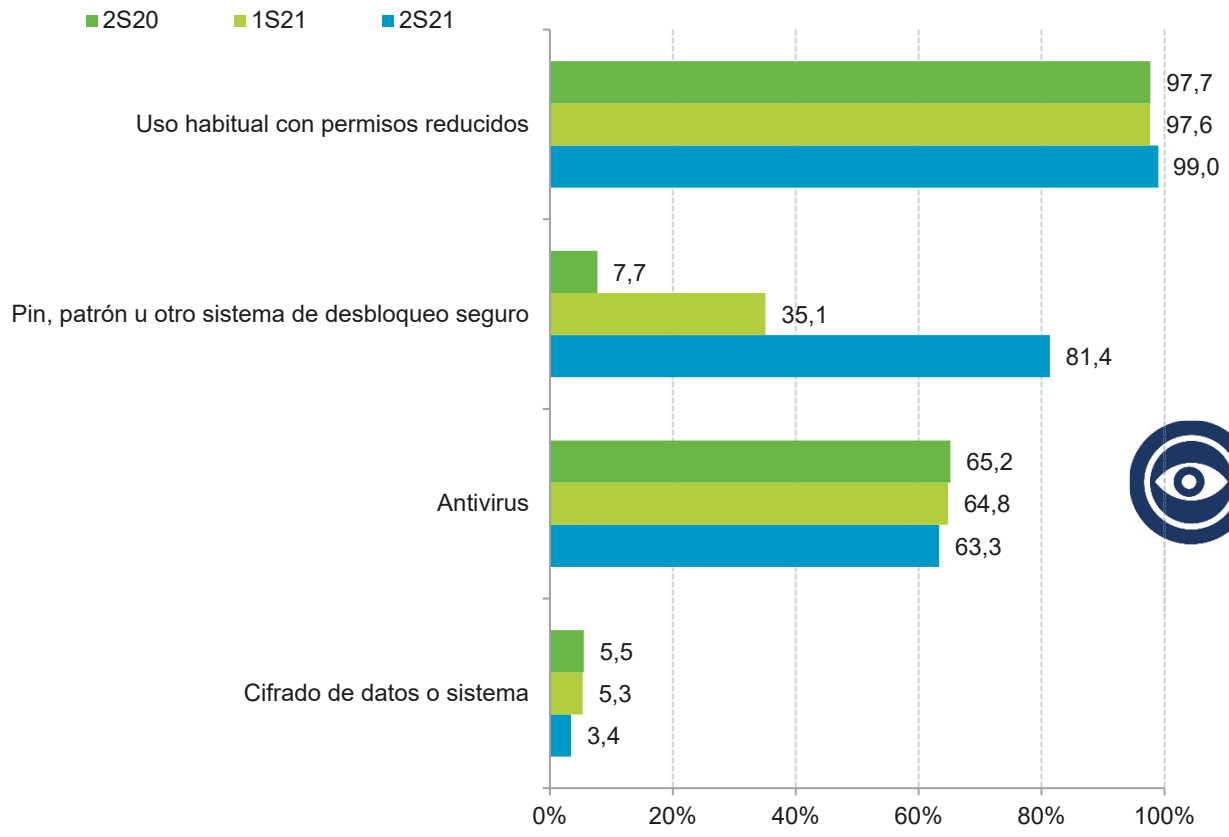
El 81,4% de los dispositivos Android analizados por el software utilizado en este estudio, utiliza el pin o patrón de desbloqueo seguro. Esto puede ser debido al aumento del uso de la banca electrónica y de los pagos contactless a través de teléfonos móviles. Ya que las aplicaciones de banca electrónica, entre otras medidas de seguridad, obligan a tener activado alguno de estos métodos de desbloqueo para poder ser utilizadas.

*La utilización de un sistema de desbloqueo seguro mediante **patrón, PIN, sistemas biométricos**, etc., permite evitar de manera sencilla los **accesos no autorizados o no deseados** al dispositivo móvil y su contenido, **protegiendo la privacidad del usuario**.*

Más información:

https://www.osi.es/es/actualidad/blog/2020/10/23/bloquear-dispositivo-android-ios-biometria

https://www.aepd.es/es/areas-de-actuacion/recomendaciones/medidas

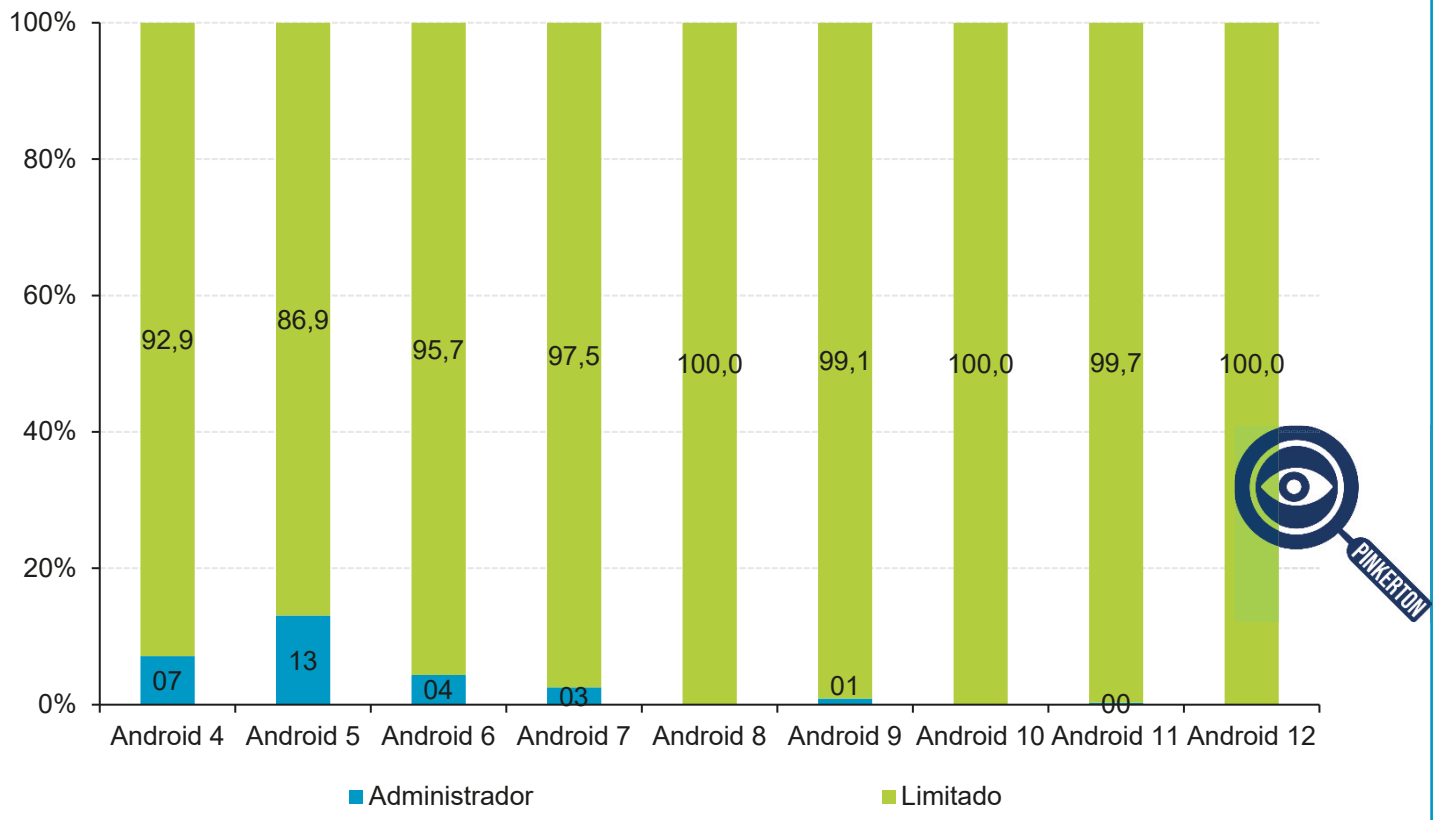


Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Nivel real de privilegios en los perfiles de usuario de dispositivos Android

Se ha detectado con el software utilizado para este estudio para analizar los dispositivos móviles de los panelistas, que la práctica totalidad de los dispositivos con versiones superiores a Android 8 tienen un nivel de privilegios limitados.



Base: Usuarios de dispositivos Android

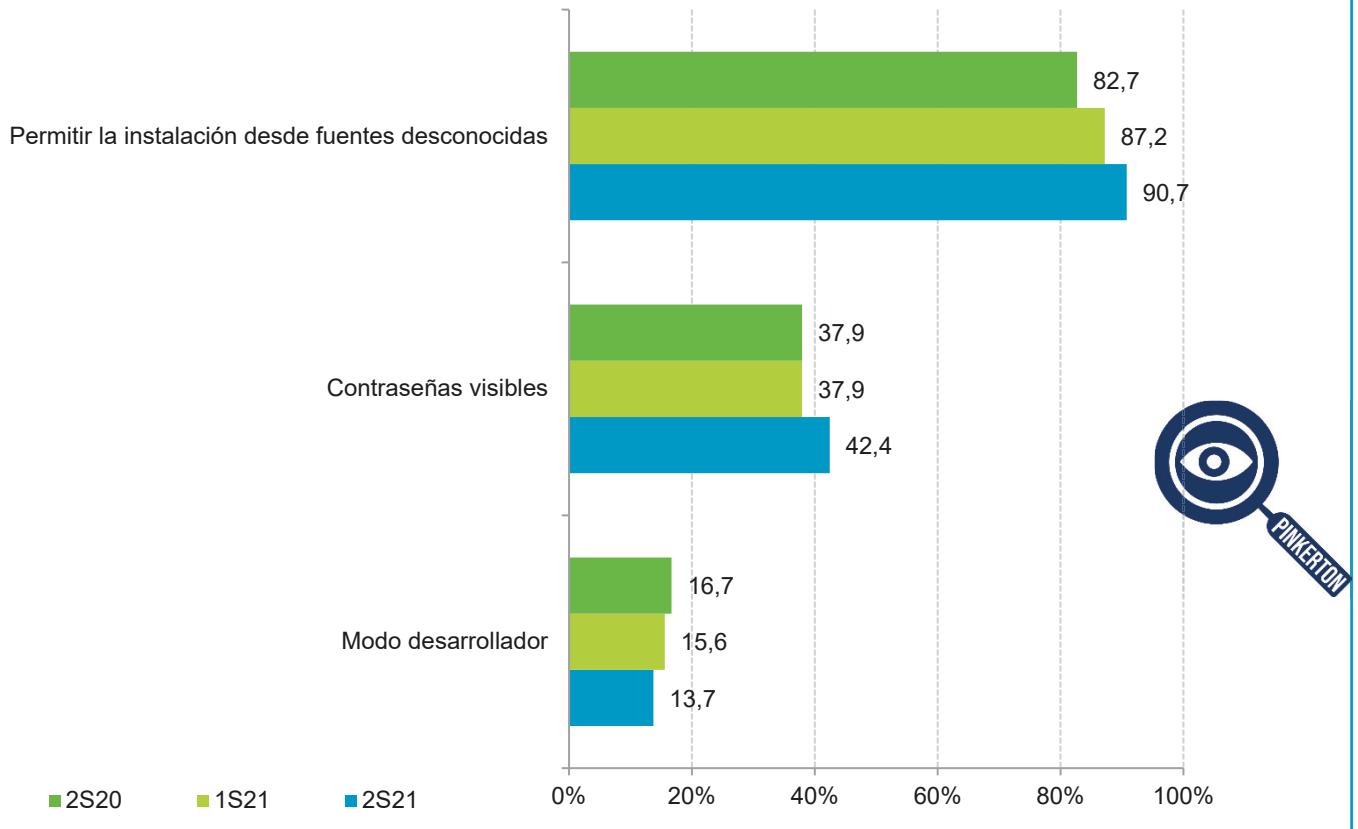
Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Configuraciones activas en dispositivos Android

Los dispositivos Android tienen diversas funcionalidades que, si están activadas, permiten mejorar la seguridad del dispositivo. Entre ellas está el permitir o no la instalación de aplicaciones desde fuentes desconocida. Si esta opción está activada, permite al usuario instalar aplicaciones de markets no oficiales, con el consecuente peligro de que la aplicación incluya algún tipo de malware.

El 90,7% de los dispositivos analizados con el software utilizado en este estudio tienen activada esta opción, lo cual hace que el dispositivo esté en riesgo.

Los keyloggers (un tipo de malware), capturan las pulsaciones de teclado entre otras cosas pero, si está activada la opción de contraseñas visibles, es más fácil que si el dispositivo tiene algún software espía acceda a tus credenciales. El 42,4% de los dispositivos analizados tiene activada la opción de contraseñas visibles.



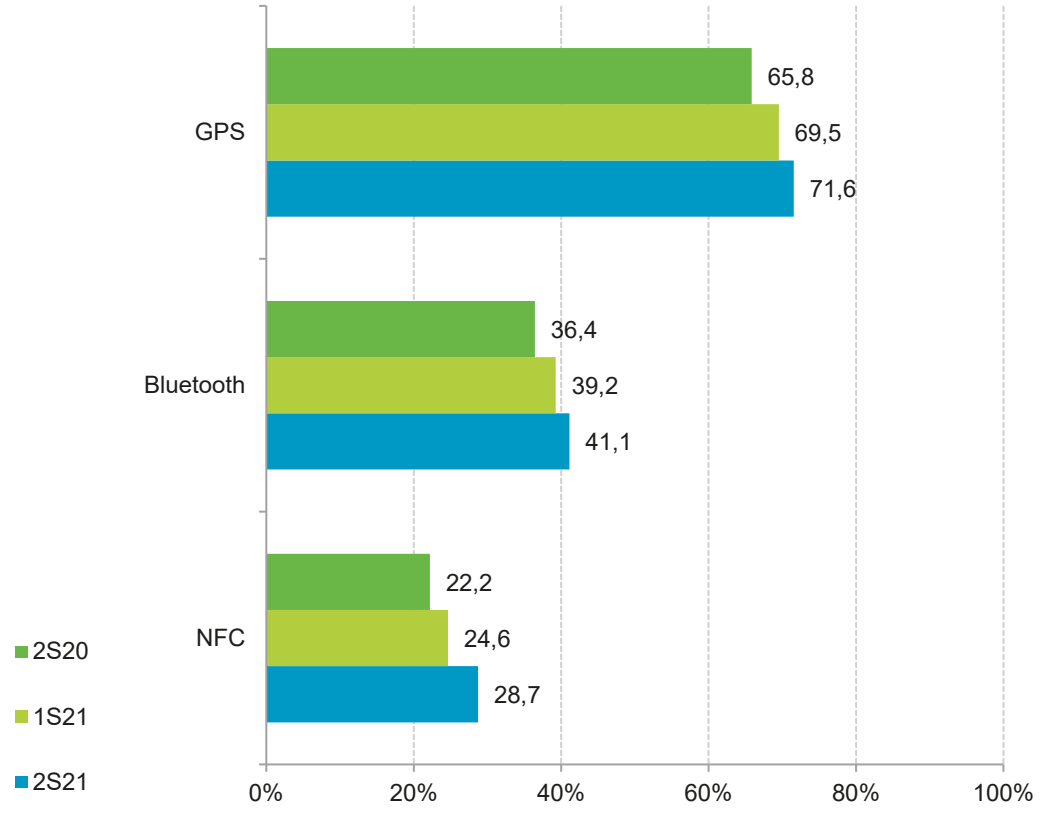
Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Tecnologías activas en dispositivos Android

El aumento del uso de la banca electrónica, también ha repercutido en las tecnologías que tienen activos los dispositivos de los usuarios que participan en este estudio. En concreto la NFC que se utiliza para realizar pagos por contactless.

El software utilizado para la realización de este estudio, confirma un aumento de 4,2 p.p. en el número de dispositivos que tienen la tecnología NFC, respecto del semestre anterior. También hay un aumento en el número de dispositivos con el Bluetooth activo (1,9p.p.) y el GPS (2,1p.p.) también respecto al semestre anterior.



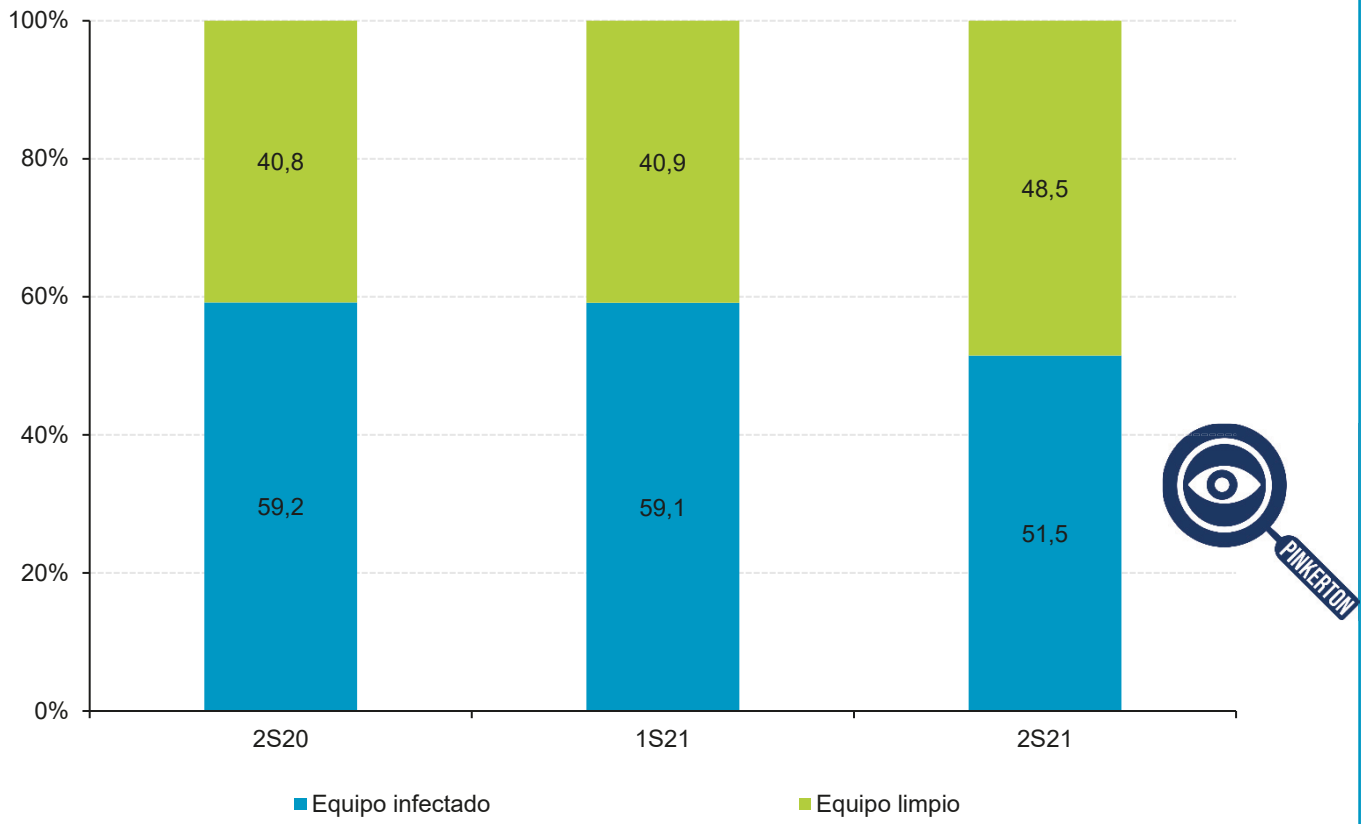
Base: Usuarios de dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Estado de infección real del ordenador del hogar

Durante el segundo semestre de 2021 se experimenta un descenso en el número de ordenadores infectados con algún tipo de malware (-7,6 p.p. sobre el semestre anterior), aunque aún mantiene un porcentaje alto (51,5%).

Aprende los pasos que debes dar para la eliminación de los virus de tu equipo:
https://www.osi.es/es/desinfecta-tu-ordenador

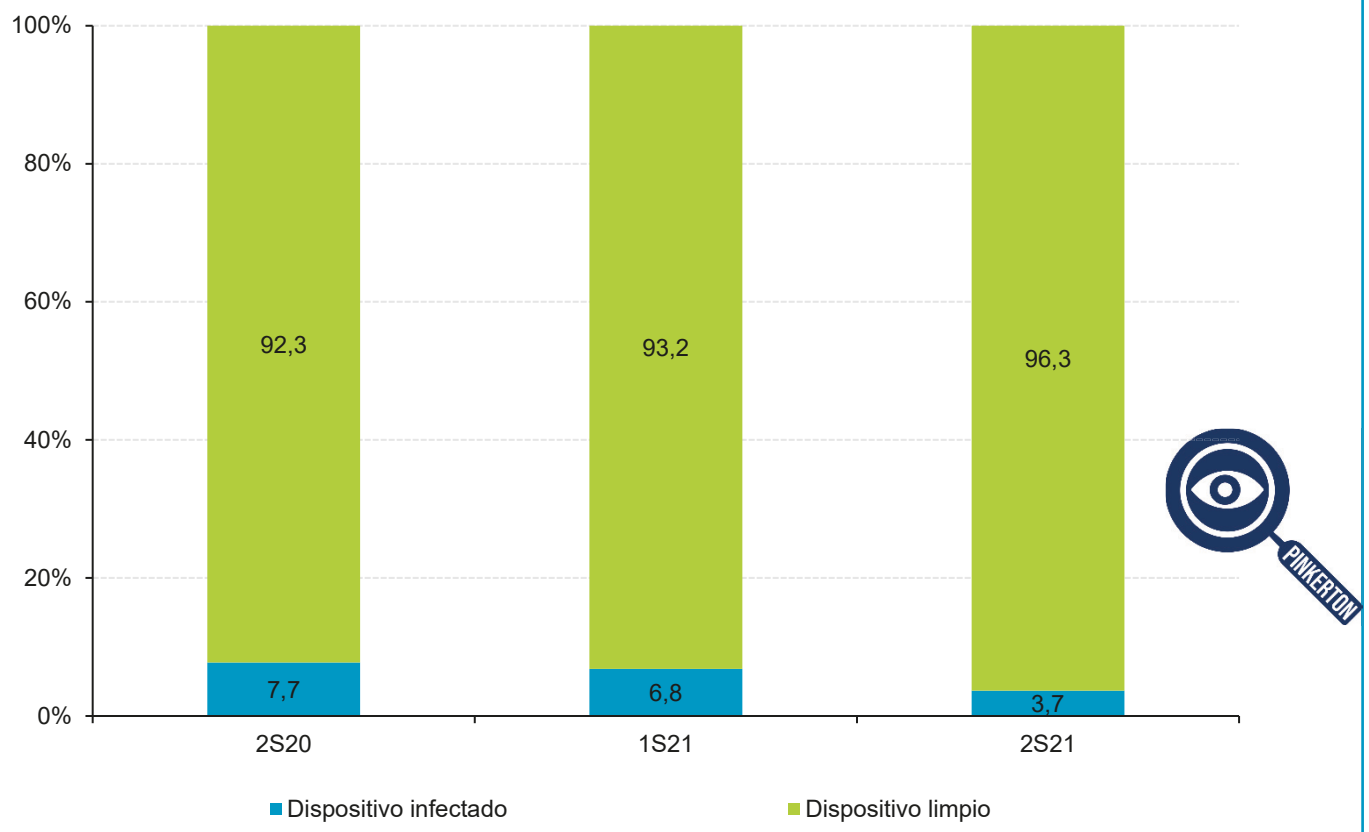


BASE: Total ordenadores

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Estado de infección real de los dispositivos Android

En el caso de los dispositivos Android infectados con algún tipo de malware, también se ha visto reducido respecto al semestre anterior (3,7%, -3,1 p.p.). Esta progresión se observa también en los semestres anteriores, y puede estar motivada por las mejoras arquitecturales en las nuevas versiones de los sistemas operativos Android.



BASE: Total dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

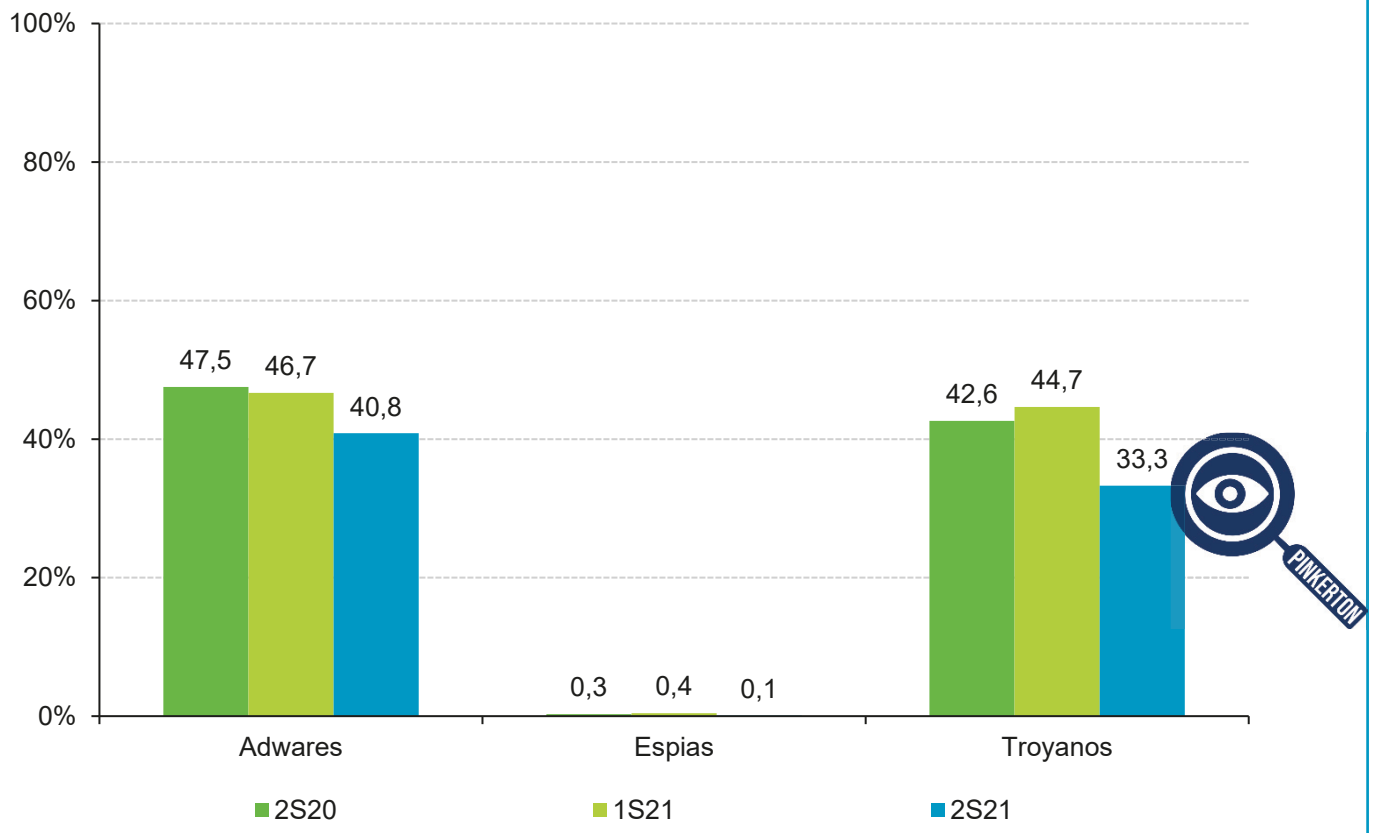
Tipología del malware detectado en el ordenador del hogar

Desciende el porcentaje de ordenadores del hogar infectados por malware, pese a seguir mostrando cifras altas. En concreto el análisis muestra que el 40,8% de los equipos analizados contiene adware, el 33,3% troyanos y el 0,1% espías.

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario.

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

Tipos de malware:
https://www.osi.es/es/actualidad/blog/2020/05/06/principales-tipos-de-virus-y-como-protegernos-frente-ellos



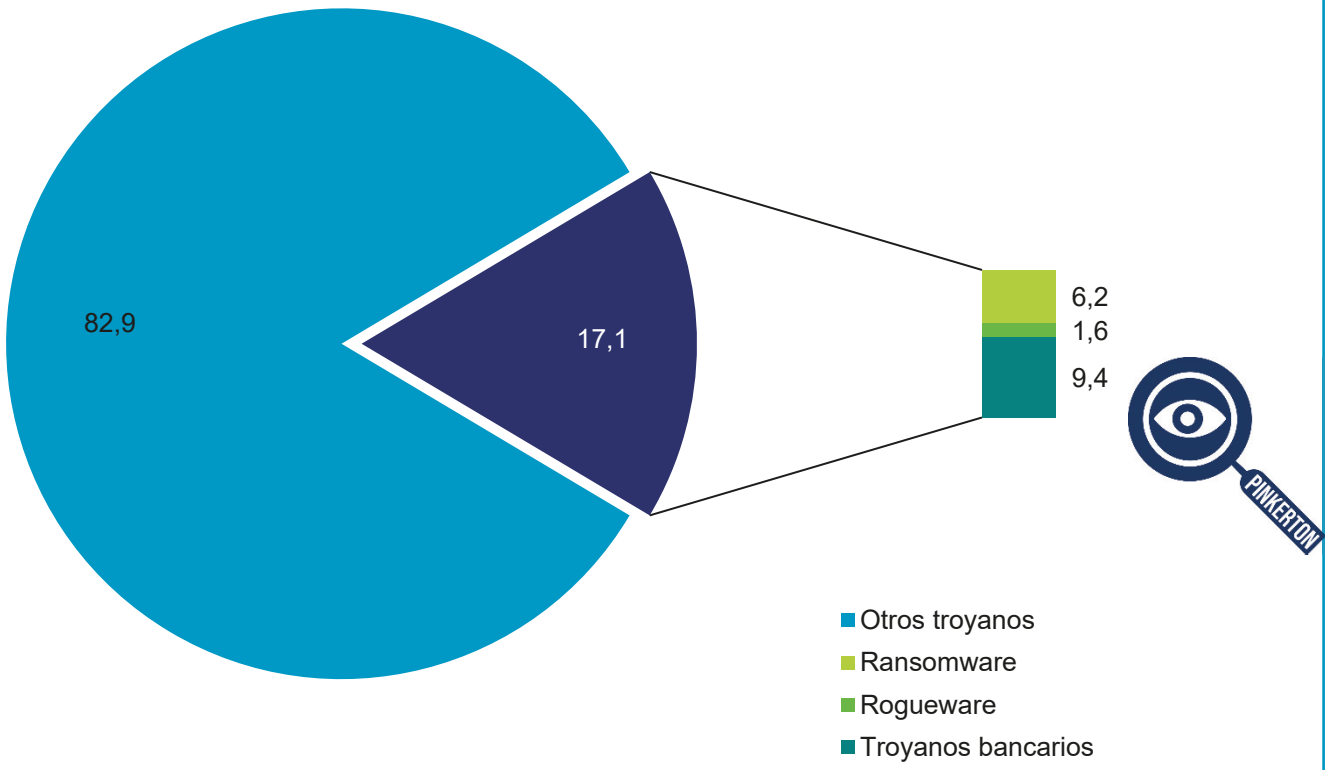
BASE: Total ordenadores

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Clasificación de troyanos detectados en el ordenador del hogar

De los troyanos identificados, el 17,1% corresponde a troyanos bancarios, rogueware o ransomware, con un 9,4%, 1,6% y 6,2% respectivamente.

Cabe destacar que los troyanos relacionados con ransomware corresponden a muestras identificadas en sus primeras fases.

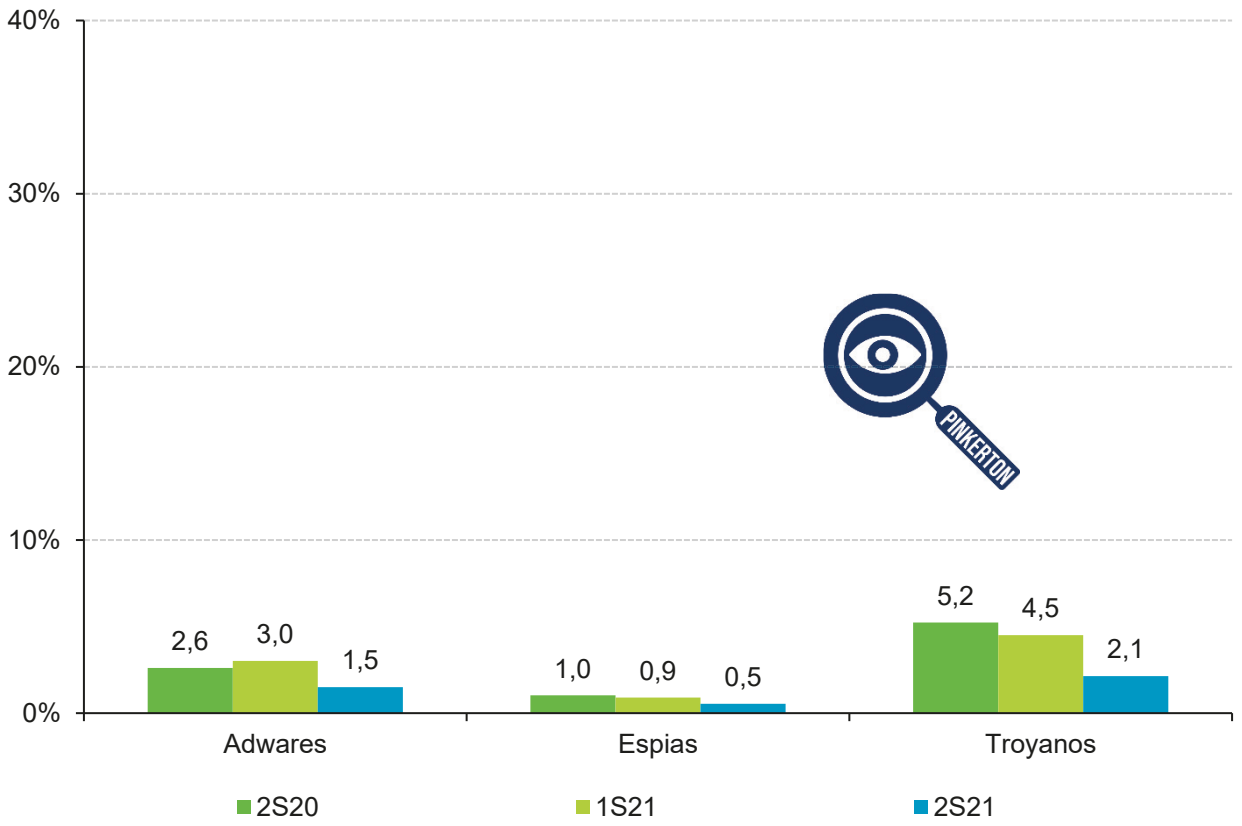


BASE: Total ordenadores con troyanos detectados

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Tipología del malware detectado en dispositivos Android

Desciende nuevamente el número de troyanos en dispositivos Android, encontrándose comprometidos con este tipo de malware el 2,1% de los dispositivos analizados. Los dispositivos infectados con adware y espías descienden al 1,5% y 0,5% respectivamente.



Guía de ciberataques:
https://www.osi.es/es/guia-ciberataques

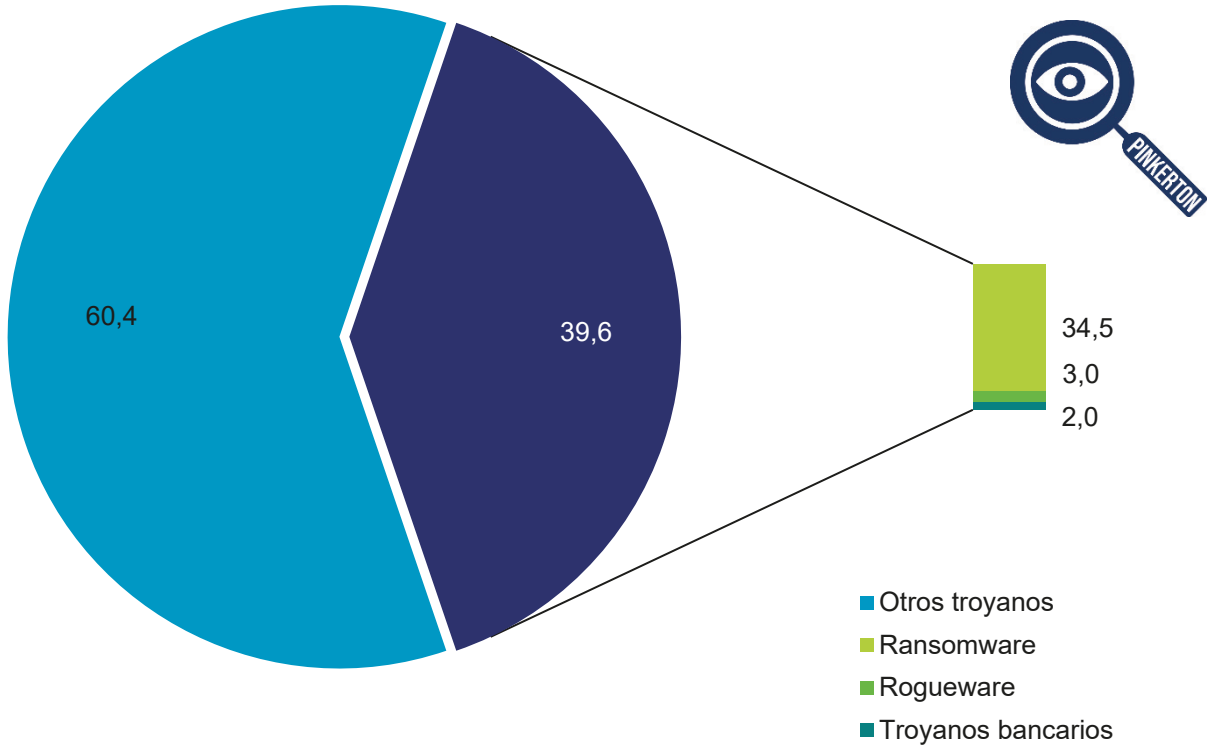
BASE: Total dispositivos Android

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Clasificación de troyanos detectados en dispositivos Android

El 34,5% de los troyanos identificados en dispositivos Android corresponde a ransomware, seguido de rogueware (3%) y los troyanos bancarios (2%).

Los troyanos que desencadenan ransomware se destacan significativamente de esta forma del resto de troyanos en los dispositivos.



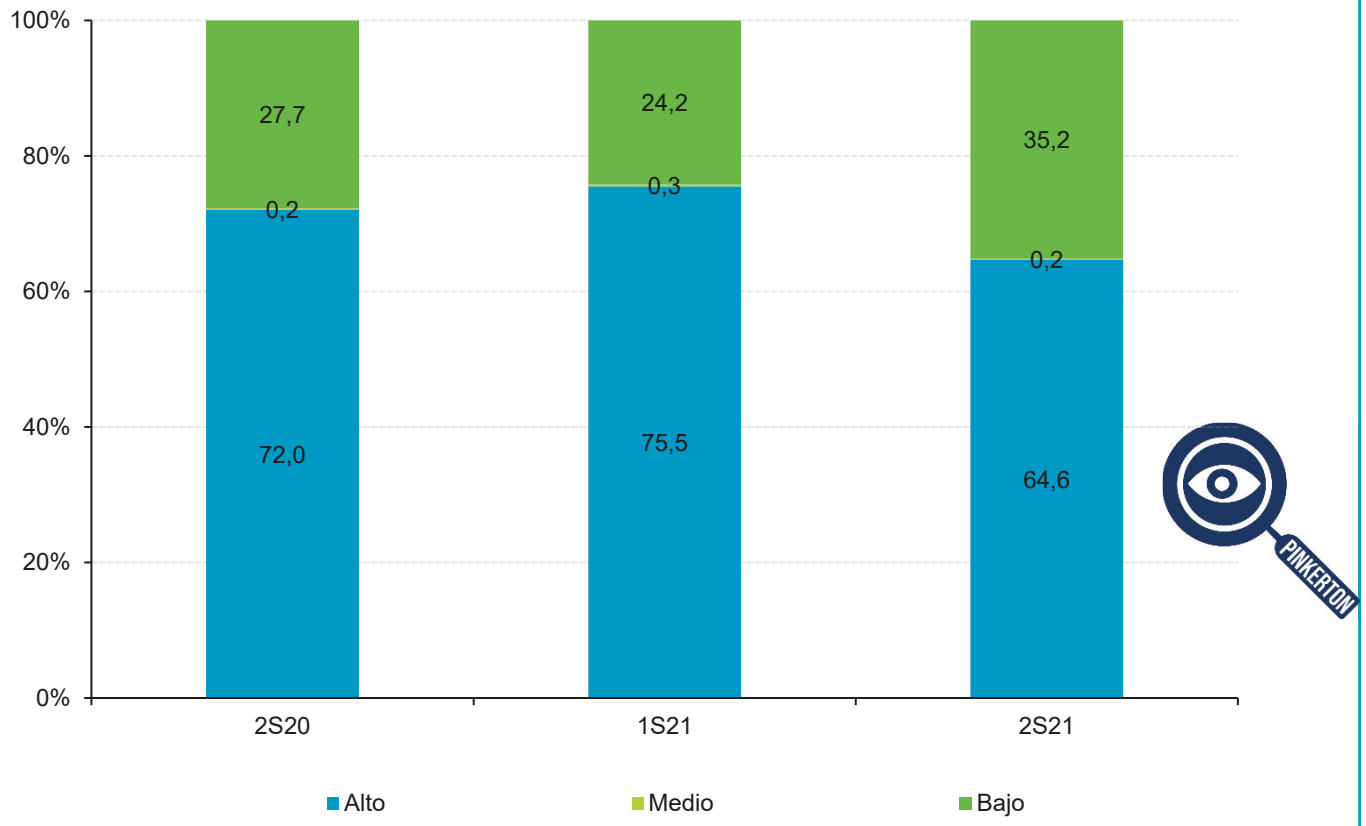
BASE: Total dispositivos Android con troyanos detectados

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Peligrosidad del malware detectado y riesgo en el ordenador del hogar

El 64.6% de los dispositivos analizados por el software Pinkerton están infectados con malware de peligrosidad alta. No obstante, aunque el porcentaje haya disminuido respecto a los dos semestres anteriores, sigue siendo peligroso para los usuarios en los dispositivos del hogar porque basta con que un equipo se infecte para comprometer toda la red, en tanto a que los mecanismos de propagación del malware cada vez están mejor diseñados para aprovecharse de la conectividad de los dispositivos.

Guía de ciberataques:
https://www.osi.es/es/guia-ciberataques



Nota: la clasificación de peligrosidad del tipo de malware se define en la introducción del estudio

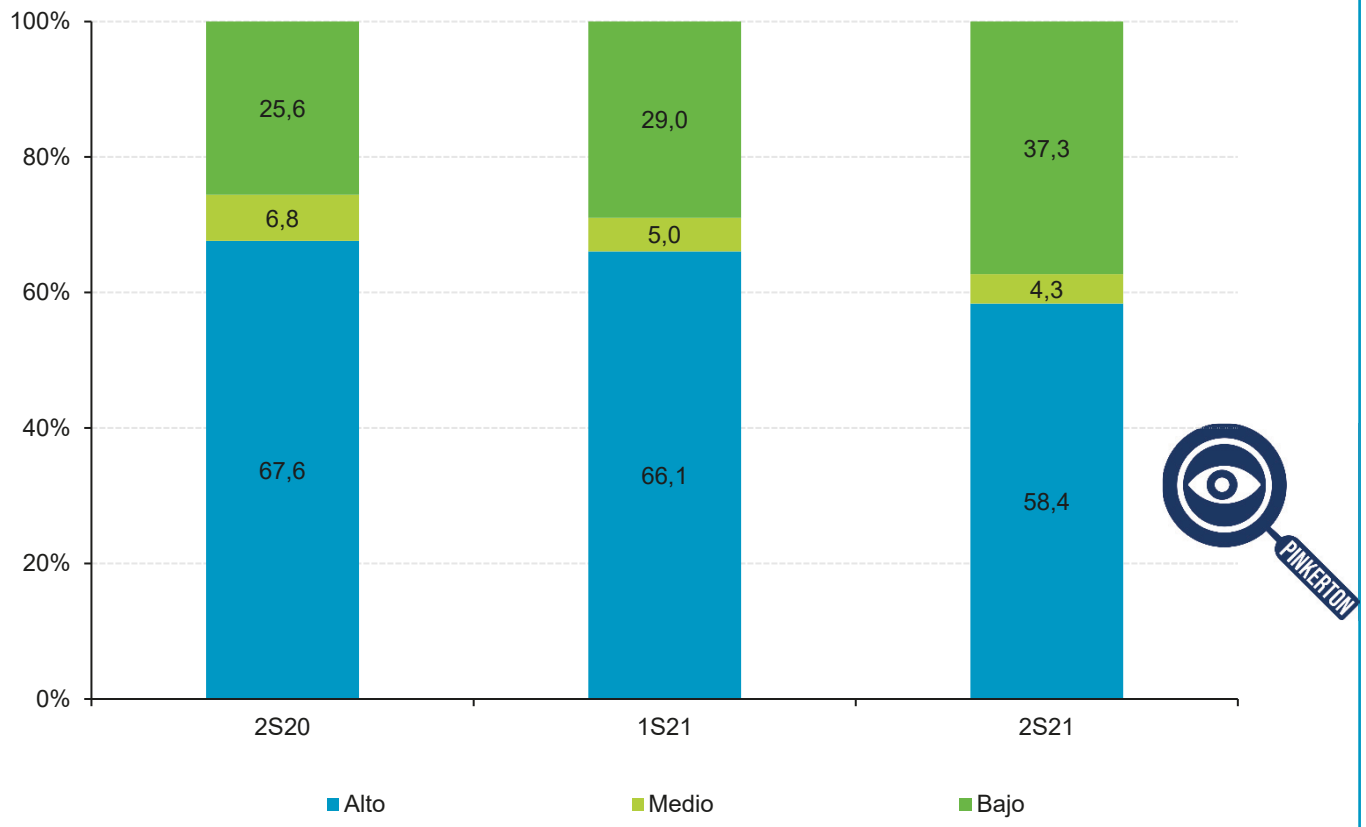
BASE: Total ordenadores infectados

Módulo VIII: Datos reales procedentes de los análisis realizados por Pinkerton

Peligrosidad del malware detectado y riesgo de los dispositivos Android

Respecto al malware detectado en dispositivos Android, la cantidad de malware altamente peligroso para el propio dispositivo y para la privacidad del usuario, también ha disminuido respecto al semestre anterior, en concreto en 7,7 p.p.. Sin embargo, el porcentaje continúa siendo alto, con el 58,4% de los equipos analizados conteniendo malware de peligrosidad alta.

Tipos de malware:
https://www.osi.es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus



Nota: la clasificación de peligrosidad del tipo de malware se define en la introducción del estudio

BASE: Total Dispositivos Android infectados

Metodología

Introducción al estudio

El Observatorio Nacional de Tecnología y Sociedad (ONTSI) de Red.es, ha diseñado y promovido el:

Estudio sobre la Ciberseguridad y Confianza en los hogares españoles

Esta investigación es referente en el diagnóstico sobre el estado de la ciberseguridad en los hogares digitales españoles, analizando la adopción de medidas de seguridad y el nivel de incidencia de situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que los hogares españoles depositan en la Sociedad de la Información.

Los datos presentados en este informe han sido extraídos siguiendo diferentes metodologías:

- Dato declarado: Obtenido de las encuestas online realizadas a los 3.400 hogares que han conformado la muestra del estudio.
- Dato real: Para ello se utiliza el software **Pinkerton** desarrollado por Hispasec Sistemas, que analiza los dispositivos recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas. **Pinkerton** también detecta la presencia de malware en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 70 motores antivirus. Los datos así extraídos se representan en el presente informe con la siguiente etiqueta:

Los datos reflejados en **este informe abarcan el análisis desde julio hasta diciembre de 2021**.

Introducción al estudio

El actual estudio recoge información concerniente a datos presentados en estudios sobre la ciberseguridad y confianza en los hogares españoles realizados con anterioridad.

El objetivo es poder contrastar dicha información con la obtenida en el presente estudio, y de este modo determinar la evolución experimentada en el ámbito de la ciberseguridad y confianza digital.

Para designar a cada estudio se han utilizado las nomenclaturas que se exponen a continuación:

- **1S19**, estudio realizado en el primer semestre de 2019 (enero - junio).
- **2S19**, estudio realizado en el segundo semestre de 2019 (julio - diciembre).
- **1S20**, estudio realizado en el primer semestre de 2020 (enero - junio).
- **2S20**, estudio realizado en el segundo semestre de 2020 (julio – diciembre).
- **1S21**, estudio realizado en el primer semestre de 2021 (enero - junio).
- **2S21**, estudio realizado en el segundo semestre de 2021 (julio - diciembre).

Introducción al estudio

El **objetivo general** de este estudio es hacer un **análisis del estado real** de la **ciberseguridad y confianza digital** entre los usuarios españoles de Internet y, al mismo tiempo, contrastar el nivel real de incidentes que sufren los equipos y dispositivos móviles con las percepciones de los usuarios además de mostrar la evolución temporal de estos indicadores.

Además se trata de **impulsar** el **conocimiento especializado y útil** en materia de **ciberseguridad y privacidad**, para mejorar la implantación de medidas por parte de los usuarios.

Así mismo se pretende reforzar la **adopción de políticas y medidas** por parte de la Administración, orientando iniciativas y políticas públicas tanto en la generación de confianza en la Sociedad de la Información, como en la mejora individual de la seguridad, sustentadas en una percepción realista de los beneficios y riesgos de las mismas.

Introducción al estudio

Medidas de seguridad[1]

Son programas o acciones utilizadas por el usuario para proteger el ordenador y los datos que se encuentren en este. Estas herramientas y acciones pueden ser realizadas con la intervención directa del usuario **(automatizables y no automatizables)** y pueden ser también medidas anteriores o posteriores a que ocurra la incidencia de seguridad **(proactivas, reactivas o ambas).**

Medidas automatizables

Son aquellas medidas de **carácter pasivo** que, por lo general, no requieren de **ninguna acción por parte del usuario**, o cuya configuración permite una puesta en marcha automática.

Medidas no automatizables

Son aquellas medidas de **carácter activo** que, por lo general, **sí requieren una actuación específica por parte del usuario** para su correcto funcionamiento.

Medidas proactivas

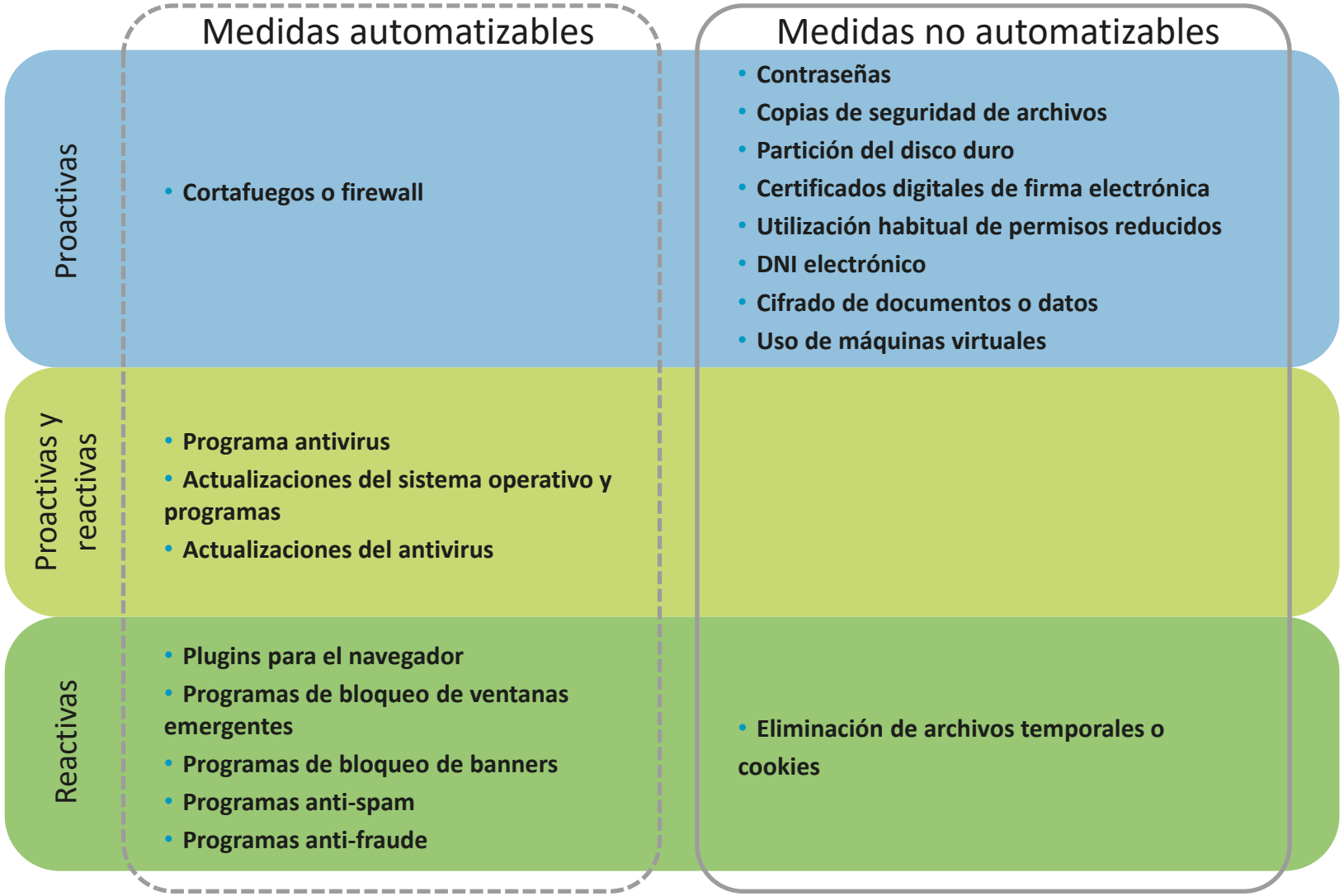
Son aquellas medidas utilizadas para **prevenir y evitar**, en la medida de lo posible, la ocurrencia de incidencias de seguridad y minimizar las posibles **amenazas desconocidas y conocidas**.

Medidas reactivas

Son aquellas medidas que son utilizadas para **subsanar** una incidencia de seguridad, es decir, son las medidas que se utilizan para eliminar **amenazas conocidas y /o incidencias ocurridas**.

[1] Existen medidas de seguridad que, por su condición, se pueden clasificar en varias categorías, tal es el caso de los programas antivirus y sus actualizaciones, o las del sistema operativo. Un programa antivirus, por su naturaleza, puede detectar tanto las amenazas existentes en el equipo como aquellas que intenten introducirse en él.

Introducción al estudio



Introducción al estudio

Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un PC/portátil o dispositivo móvil (tablet, smartphone, relojes inteligentes, etc.) sin el consentimiento del propietario. Comúnmente se conocen como virus, en realidad se trata de un término más amplio que engloba otras tipologías.

Troyanos o caballos de Troya. *Bankers* o troyanos bancarios, *Backdoors* o puertas traseras, *Keyloggers* o capturadores de pulsaciones, *Dialers* o marcadores telefónicos, *Rogueware*

***Adware* o software publicitario**

Herramientas de intrusión

Virus

Archivos sospechosos detectados heurísticamente. Técnica empleada por los antivirus para reconocer códigos maliciosos que no se encuentran en la base de datos de virus del antivirus

***Spyware* o programas espía**

Gusano o *worm*

Otros. *Exploit, Rootkits, Scripts, Lockers* o *Scareware*, *Jokes* o bromas

Mas información: https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

Introducción al estudio

Para determinar el nivel de riesgo[3] de los equipos analizados, se establece la peligrosidad del malware detectado en función de las posibles consecuencias sufridas. La clasificación se realiza en base a los siguientes criterios:

- **Peligrosidad alta**: se incluyen en esta categoría los especímenes que, potencialmente: permiten el acceso remoto por parte de un atacante al sistema víctima; pueden suponer un perjuicio económico para el usuario; facilitan la captura de información confidencial o sensible de la víctima; se emplean como pasarelas para atacar otros equipos (pudiendo acarrear consecuencias legales para la víctima); o minan el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.
- **Peligrosidad media**: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema: no perjudican de forma notoria su rendimiento; abren ventanas no deseadas al navegar; incrustan publicidad en páginas web legítimas que realmente no contienen publicidad; o facilitan la captura de información no sensible de la víctima (por ejemplo, patrones de navegación para crear perfiles de publicidad dirigida, etc.).
- **Peligrosidad baja**: se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, *hacking tools*, etc.). En la mayoría de los casos son herramientas instaladas por el usuario de forma intencionada, para listar y matar procesos, o conectarse remotamente a su equipo, etc. Por otra parte, también se consideran especímenes de baja peligrosidad los programas "broma" (por ejemplo aquellos que despliegan una ventana que se va moviendo y resulta imposible cerrarla con el ratón) y los virus exclusivos para plataformas móviles, ya que estos no son capaces de ejecutarse sobre los equipos de los usuarios.

[3] Se establece como el nivel de riesgo de cada equipo el de mayor nivel de entre el malware que aloje. Es decir, un equipo en el que se detecte un software malicioso de peligrosidad alta y otro de peligrosidad media, siempre será incluido en el grupo de equipos con un nivel de riesgo alto.

Alcance del estudio

Alcance del estudio

El "*Estudio sobre la Ciberseguridad y Confianza del ciudadano en la Red*" se realiza a partir de una metodología basada en el panel online dedicado y compuesto por aquellos hogares con conexión a Internet repartidos por todo el territorio nacional.

Los datos extraídos de la encuesta, realizada con una periodicidad semestral, permiten obtener la percepción sobre la situación de la seguridad en Internet y nivel de e-confianza de los usuarios.

Ficha técnica

Universo: Usuarios españoles de Internet mayores de 15 años con acceso a Internet desde el hogar (al menos una vez al mes).

Tamaño Muestral: 3.400 hogares encuestados y equipos/dispositivos Android escaneados (software instalado en 680 PCs y 2.210 smartphones y 510 tablets Android).

Ámbito: Península, Baleares y Canarias.

Diseño Muestral: Para cada CC.AA., estratificación proporcional por tipo de hábitat, con cuotas de segmento social y número de personas en el hogar.

Trabajo de Campo: El trabajo de campo ha sido realizado entre noviembre y diciembre de 2021 mediante entrevistas online a partir de un panel de usuarios de Internet.

Error Muestral: Asumiendo criterios de muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5, y para un nivel de confianza del 95,5%, se establece que al tamaño muestral n=3.400 le corresponde una estimación del error muestral igual a ±1,68%.

Growth from Knowledge

HISPASEC

¡Gracias!

El informe del *"Estudio sobre la Ciberseguridad y Confianza del ciudadano en la Red"* ha sido elaborado por el siguiente equipo de trabajo del Observatorio Nacional de Tecnología y Sociedad (ONTSI) de Red.es:

Lucía Velasco
Luis Muñoz López
José María Zavala Pérez
Belén Kayser

Agradecer la colaboración en la realización de este estudio a:

Asimismo se quiere también agradecer la colaboración de:

ISSN: 2660-423X
doi: 10.30923/CiCoCiRed-2020-2
NIPO: 094-20-095-8

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

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