Estudio sobre la ciberseguridad y confianza del ciudadano en la RED Noviembre 2020

Oleada enero - junio 2020

Colección Ciberseguridad y Confianza

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

ÍNDICE

Introducción al estudio

Introducción al estudio

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (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 3.659 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 50 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 enero hasta junio de 2020**.

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:

- **1S18**, estudio realizado en el primer semestre de 2018 (enero - junio).
- **2S18**, estudio realizado en el segundo semestre de 2018 (julio - diciembre).
- **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 segundo semestre de 2020 (enero - junio).

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

	Medidas automatizables	Medidas no automatizables
Proactivas	• Cortafuegos o firewall	• Contraseñas • Copias de seguridad de archivos • Partición del disco duro • Certificados digitales de firma electrónica • Utilización habitual de permisos reducidos • DNI electrónico • Cifrado de documentos o datos • Uso de máquinas virtuales
Proactivas y reactivas	• Programa antivirus • Actualizaciones del sistema operativo y programas • Actualizaciones del antivirus	
Reactivas	• Plugins para el navegador • Programas de bloqueo de ventanas emergentes • Programas de bloqueo de banners • Programas anti-spam • Programas anti-fraude	• Eliminación de archivos temporales o cookies

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.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

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.

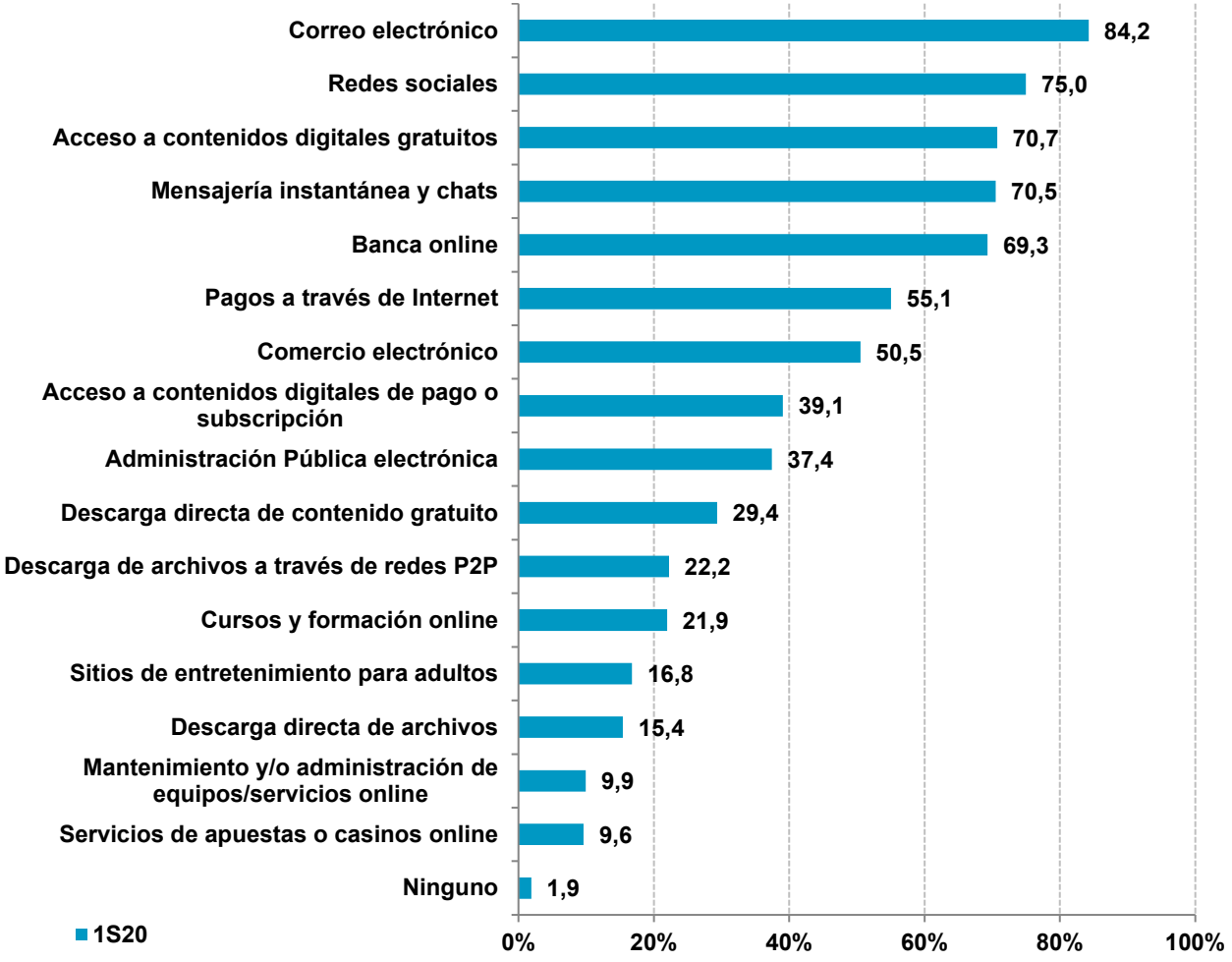
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

Módulo I:
Servicios usados en Internet

Módulo I: Servicios usados en Internet

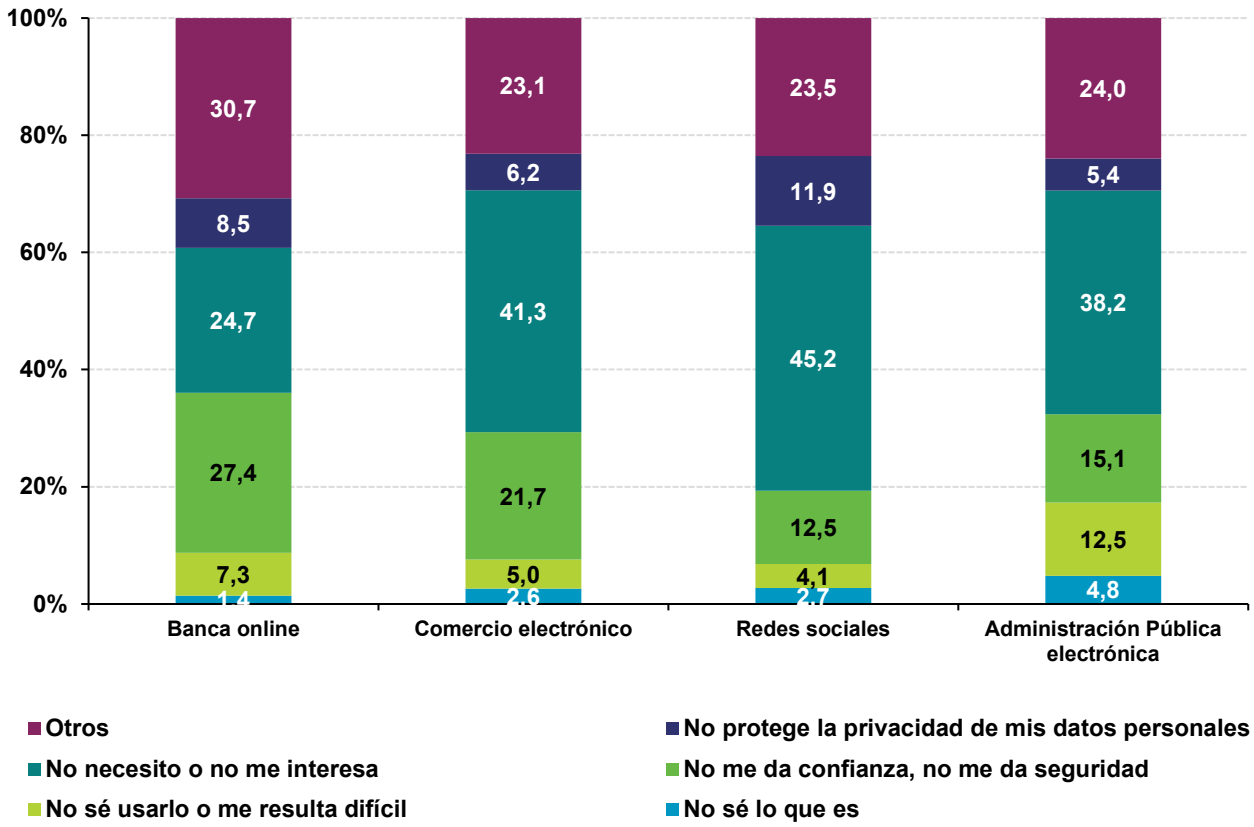
Servicios ofrecidos por Internet que han sido utilizados por el usuario en el último semestre



Base: Total usuarios

Módulo I: Servicios usados en Internet

Motivos de no utilización de los servicios ofrecidos por Internet



Base: Usuarios que no utilizan alguno de los servicios

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

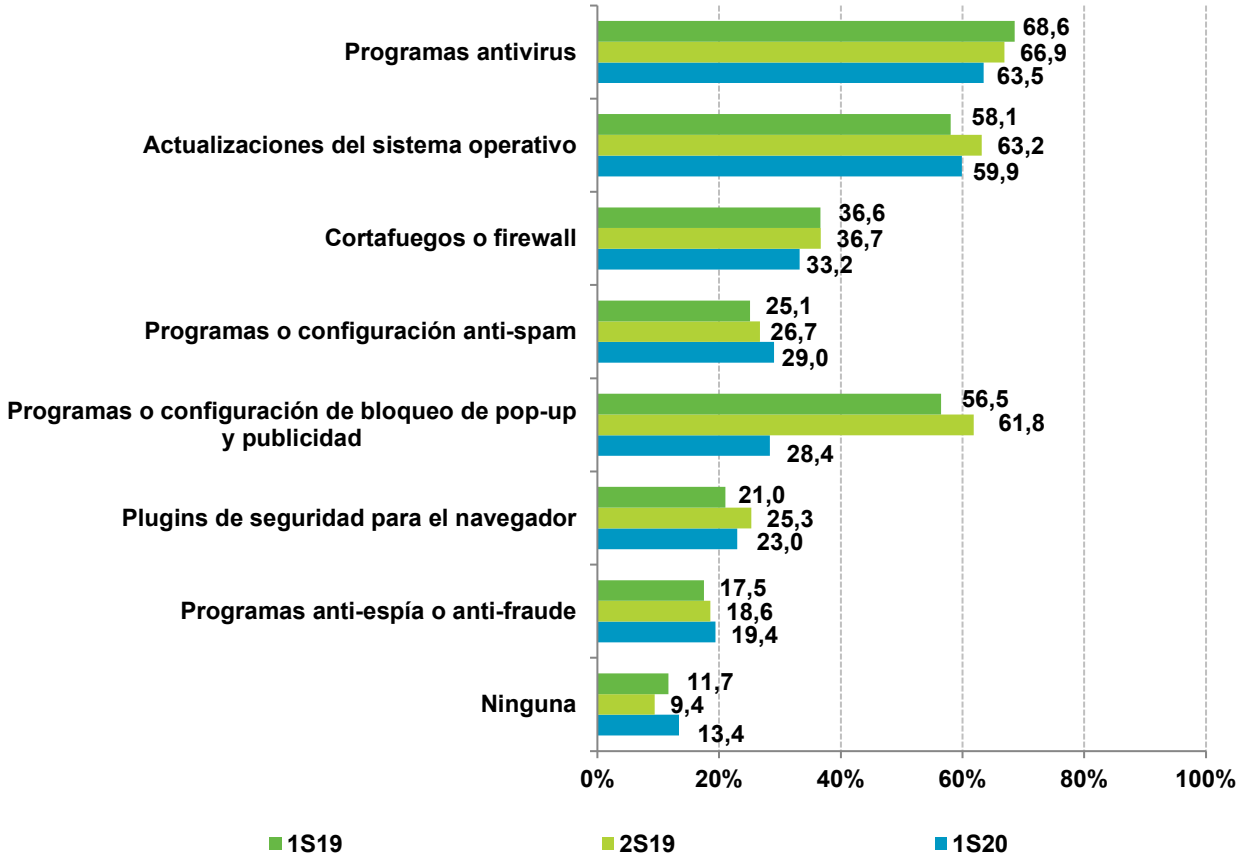
Módulo II:
Medidas y hábitos de seguridad en Internet

Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad automatizables en el ordenador del hogar

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



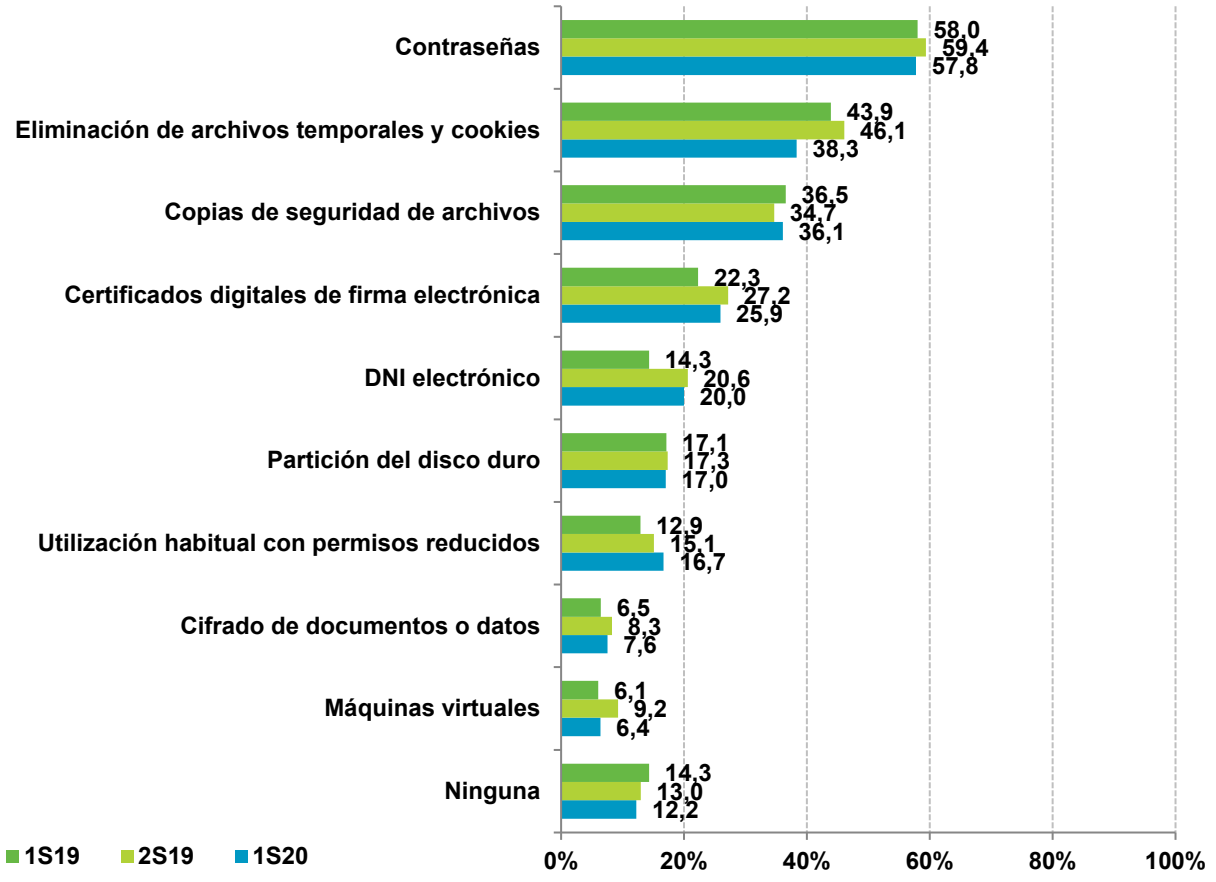
Base: Usuarios de PC

Módulo II: Medidas y hábitos de seguridad en Internet

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

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:

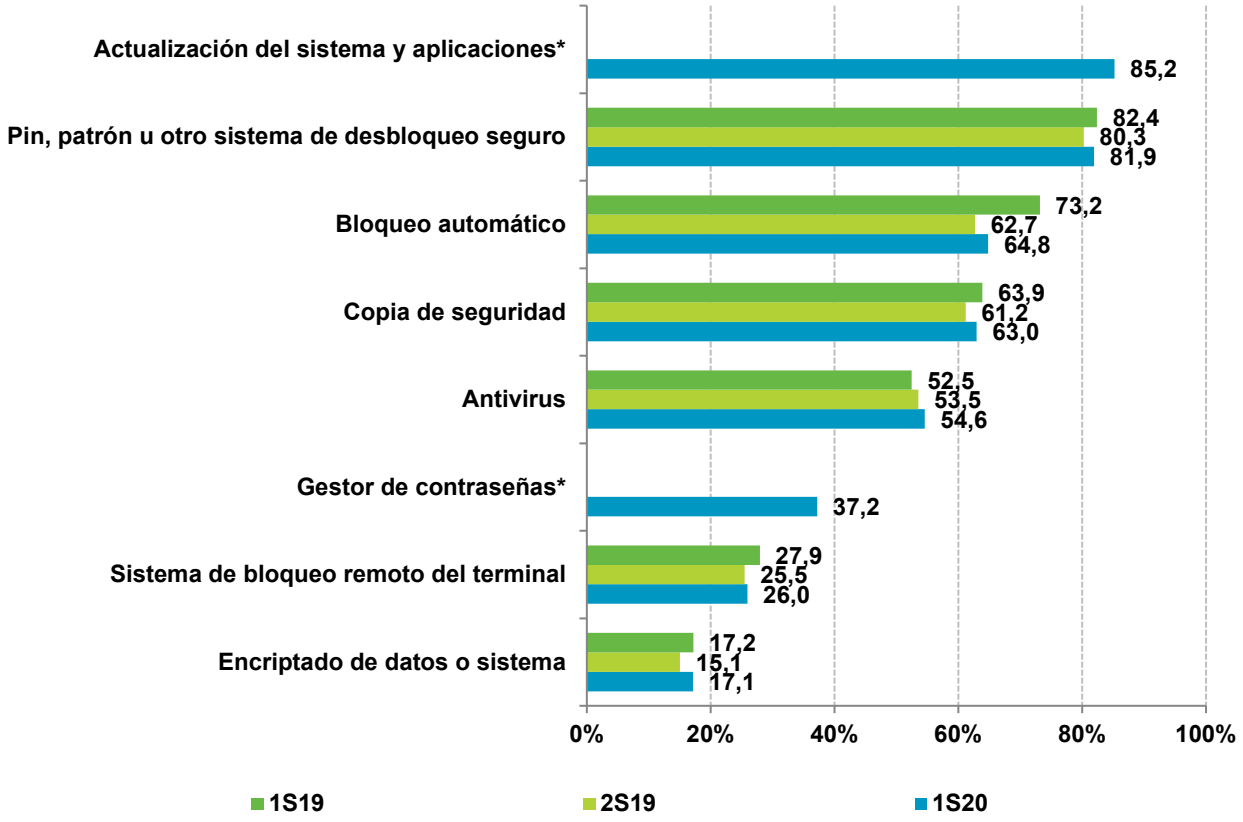
- ✓ ***Contraseñas:*** *https://www.osi.es/es/campanas/contrasenas-seguras*
- ✓ ***Copias de seguridad:*** *https://www.osi.es/es/campanas/copias-cifrado-informacion*



Base: Usuarios de PC

Módulo II: Medidas y hábitos de seguridad en Internet

Medidas de seguridad en dispositivos Android

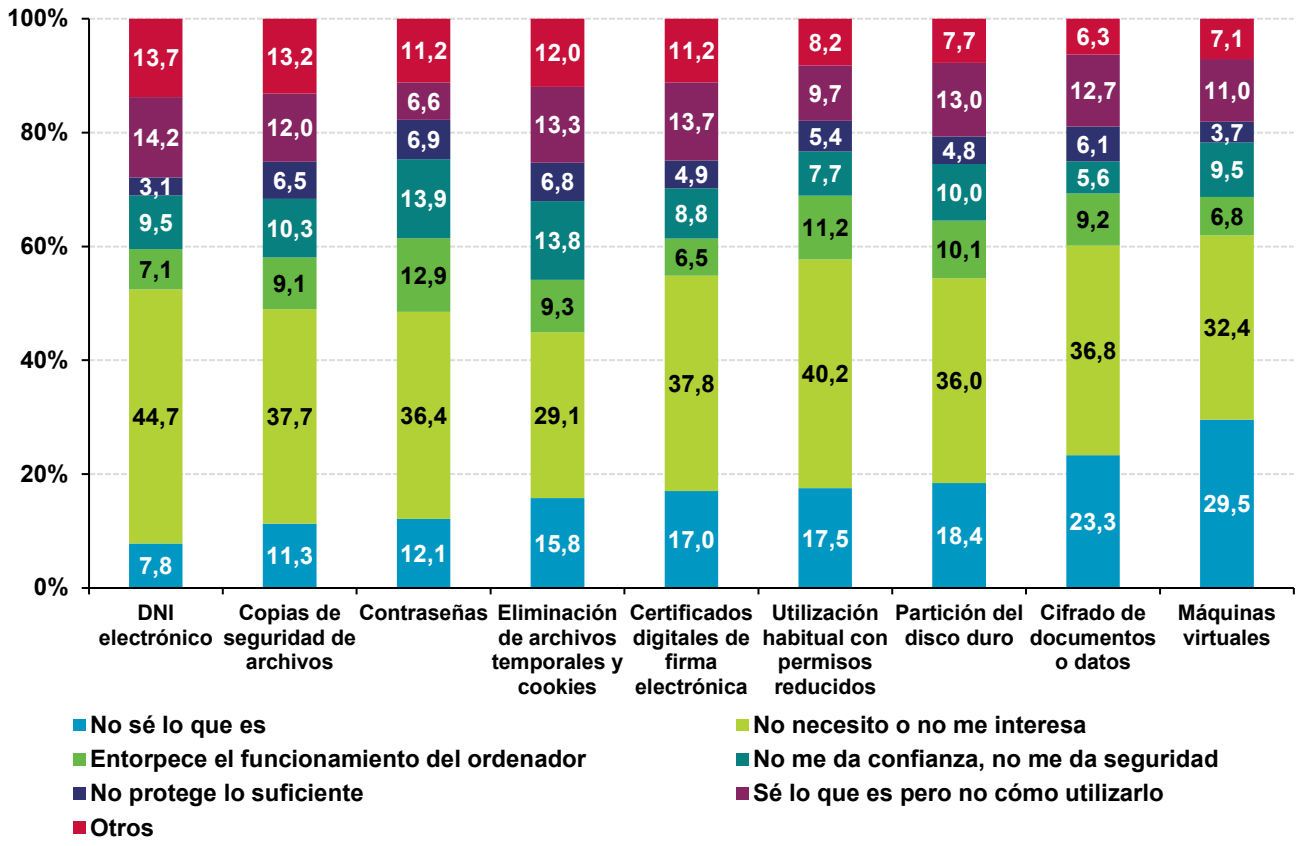


*nuevas categorías

Base: Usuarios que disponen de dispositivo Android

Módulo II: Medidas y hábitos de seguridad en Internet

Motivos de no utilización de medidas de seguridad



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

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

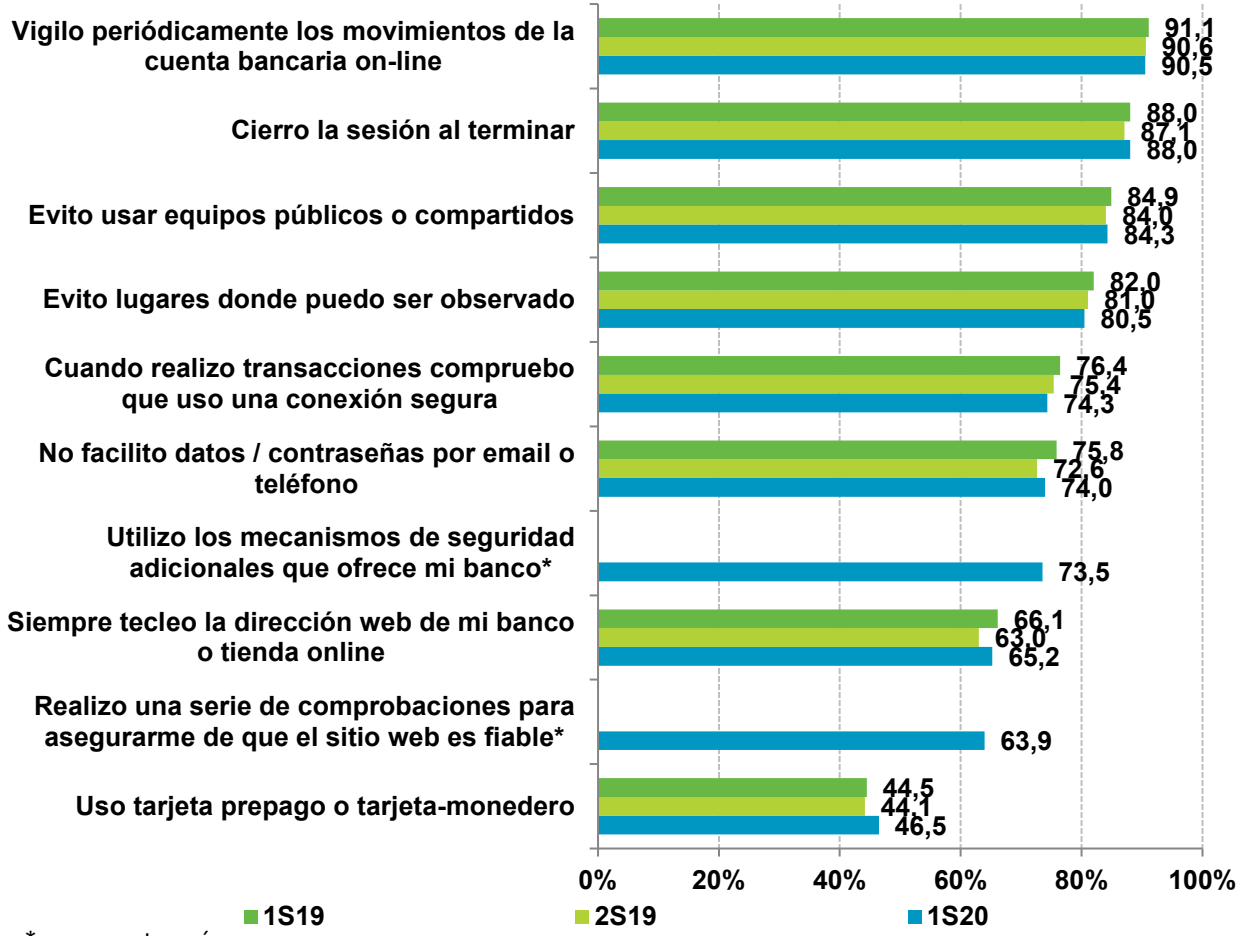
ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

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

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.



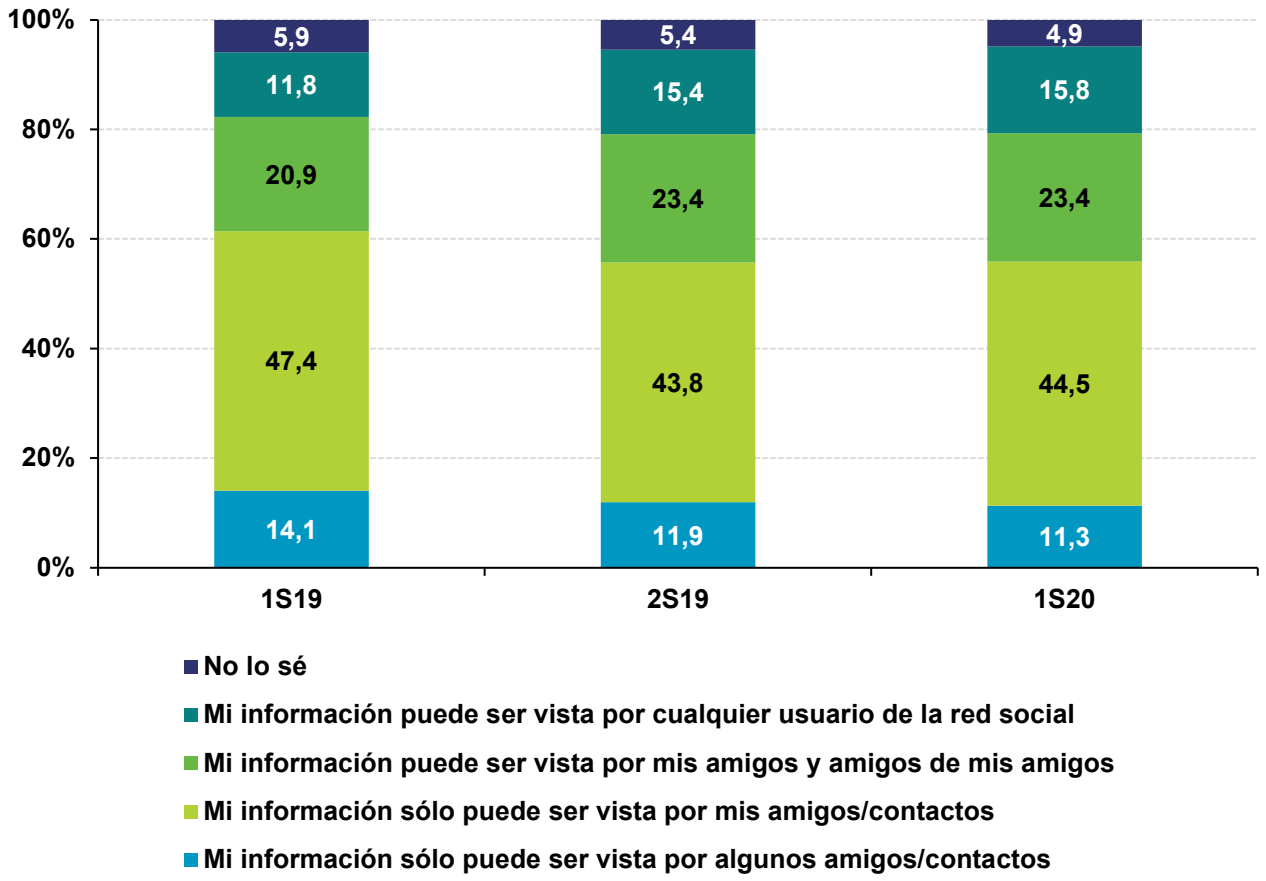
*nuevas categorías

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

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

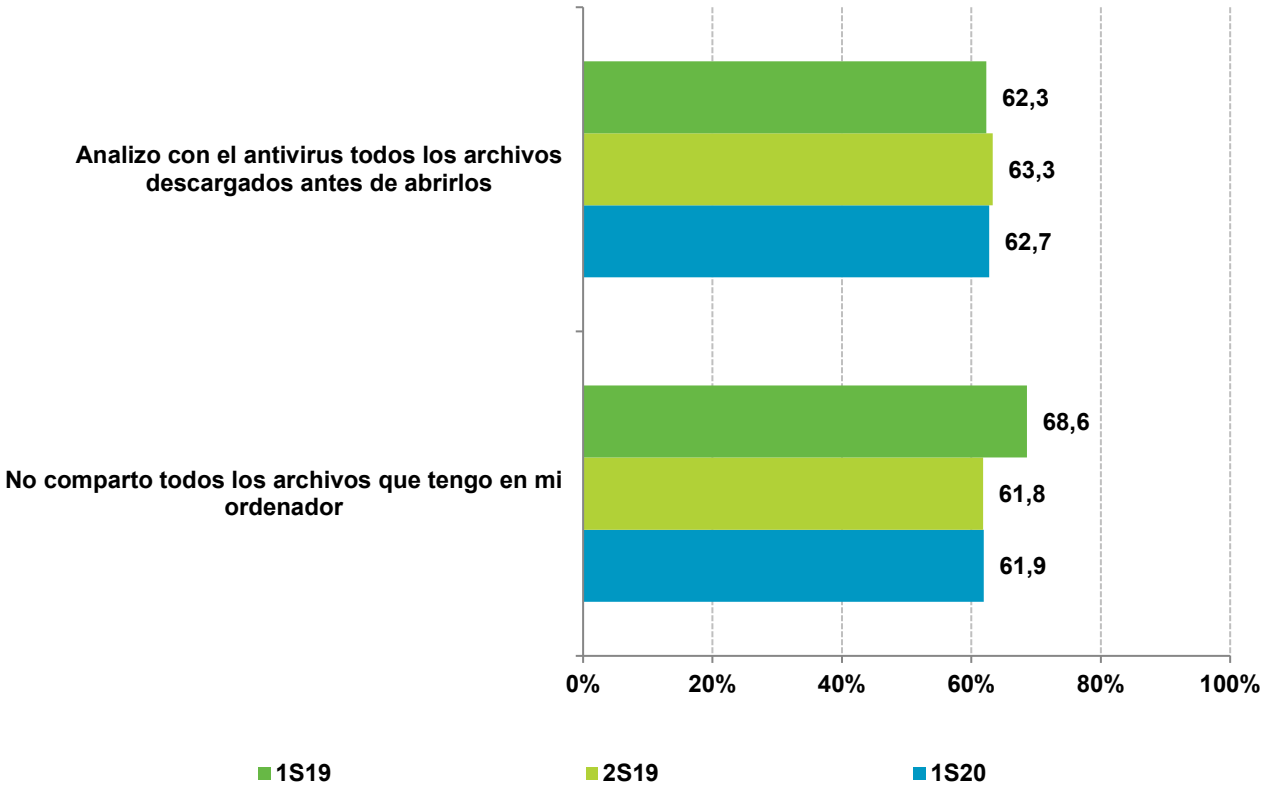


BASE: Usuarios de redes sociales

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

Hábitos de comportamiento en el uso de redes P2P

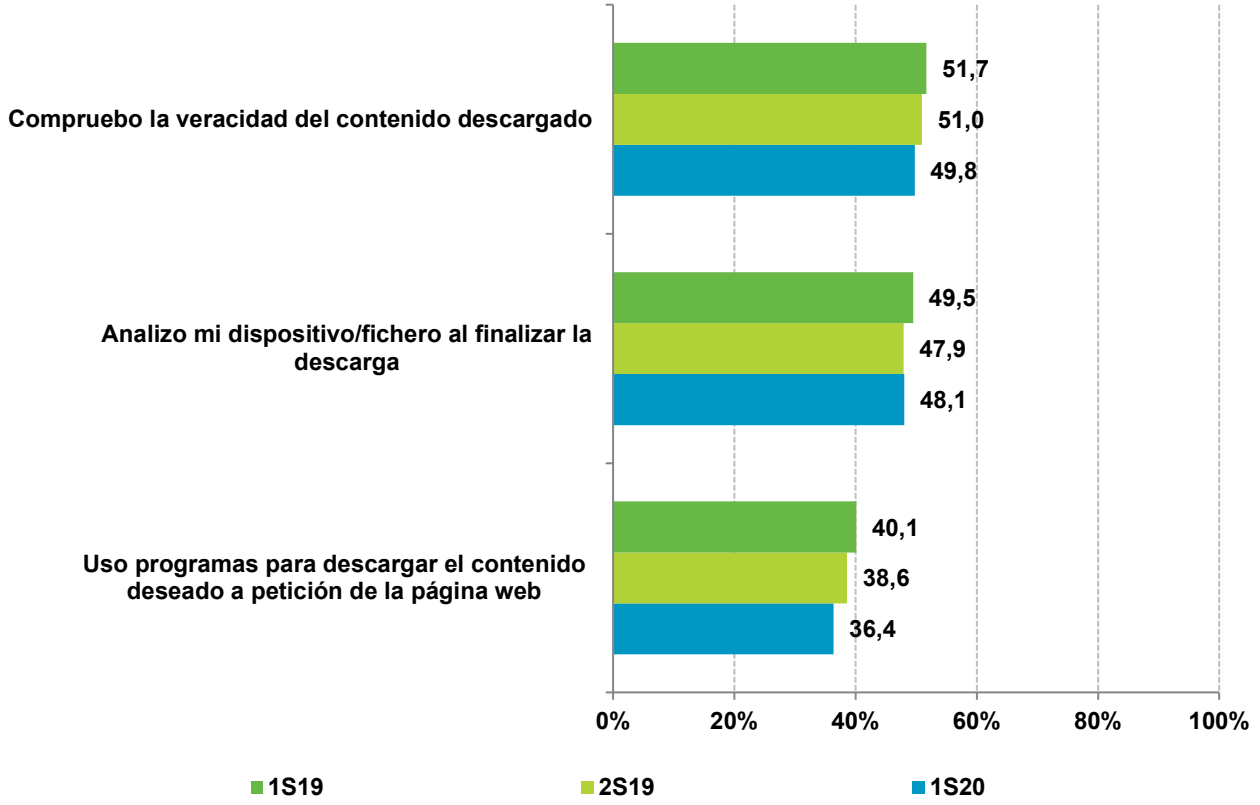
Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de malware. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como por ejemplo novedades de software, cinematográficas, musicales, etc.) logran el objetivo de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

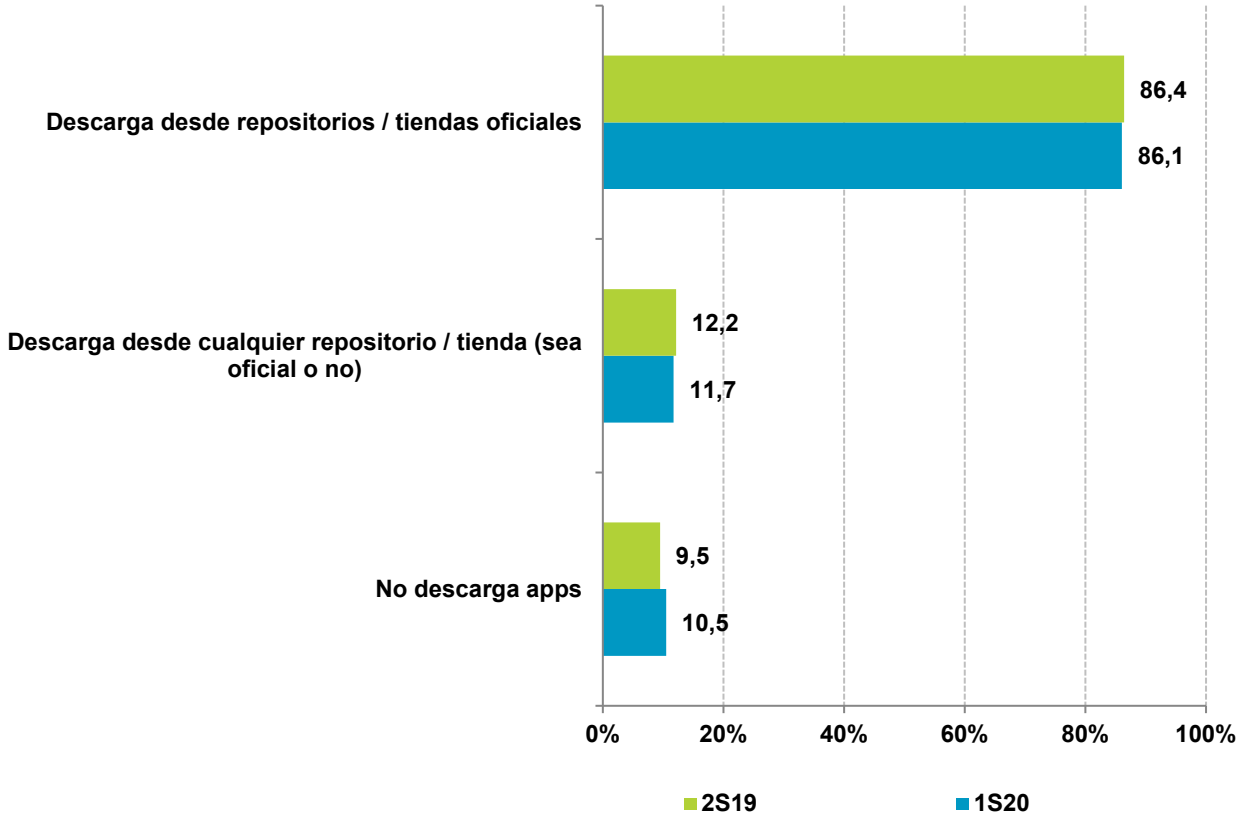
Hábitos de comportamiento en el uso de descarga directa de archivos, programas, documentos, etc.



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

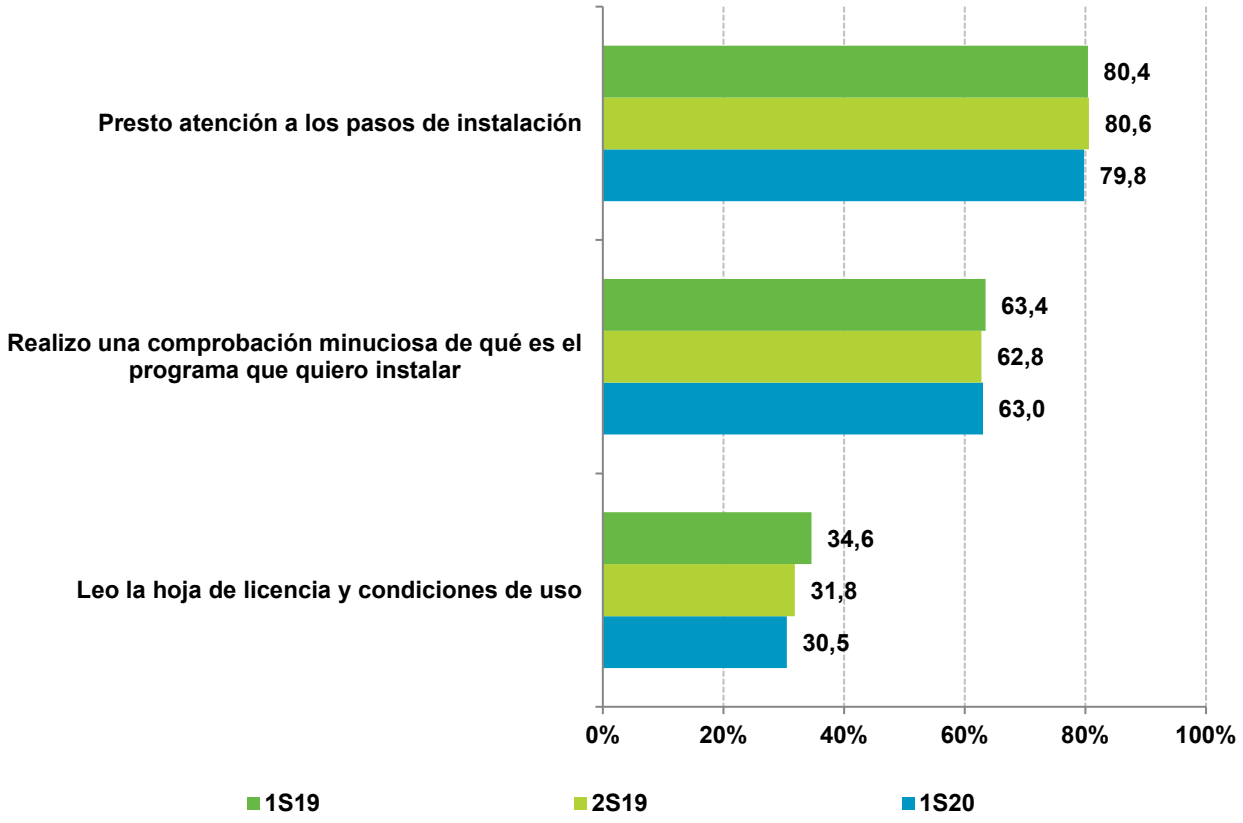


¡Ayuda! Instalé una app no fiable
https://www.osi.es/es/campanas/dispositivos-moviles/instale-app-no-fiable

BASE: Usuarios que disponen de dispositivo Android

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

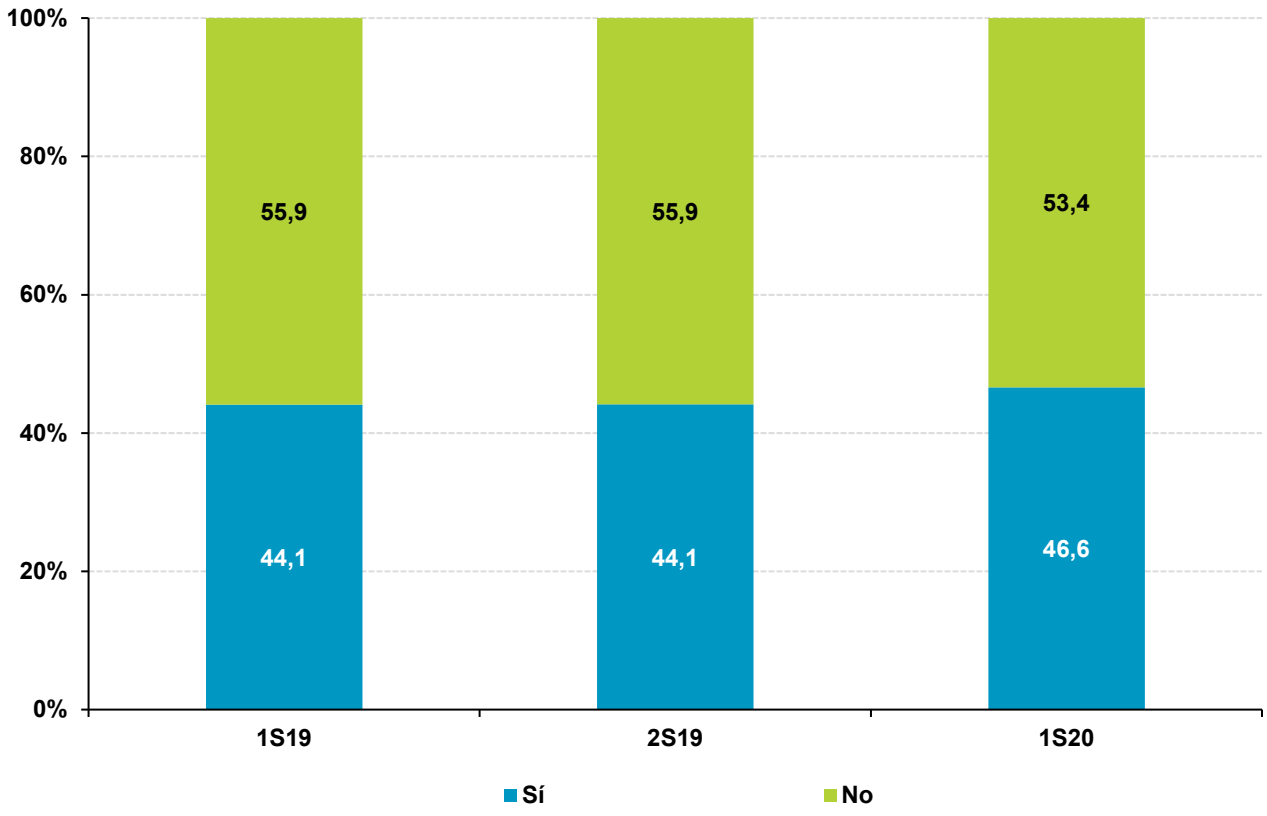
Hábitos de comportamiento en la instalación de programas



BASE: Usuarios de PC

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

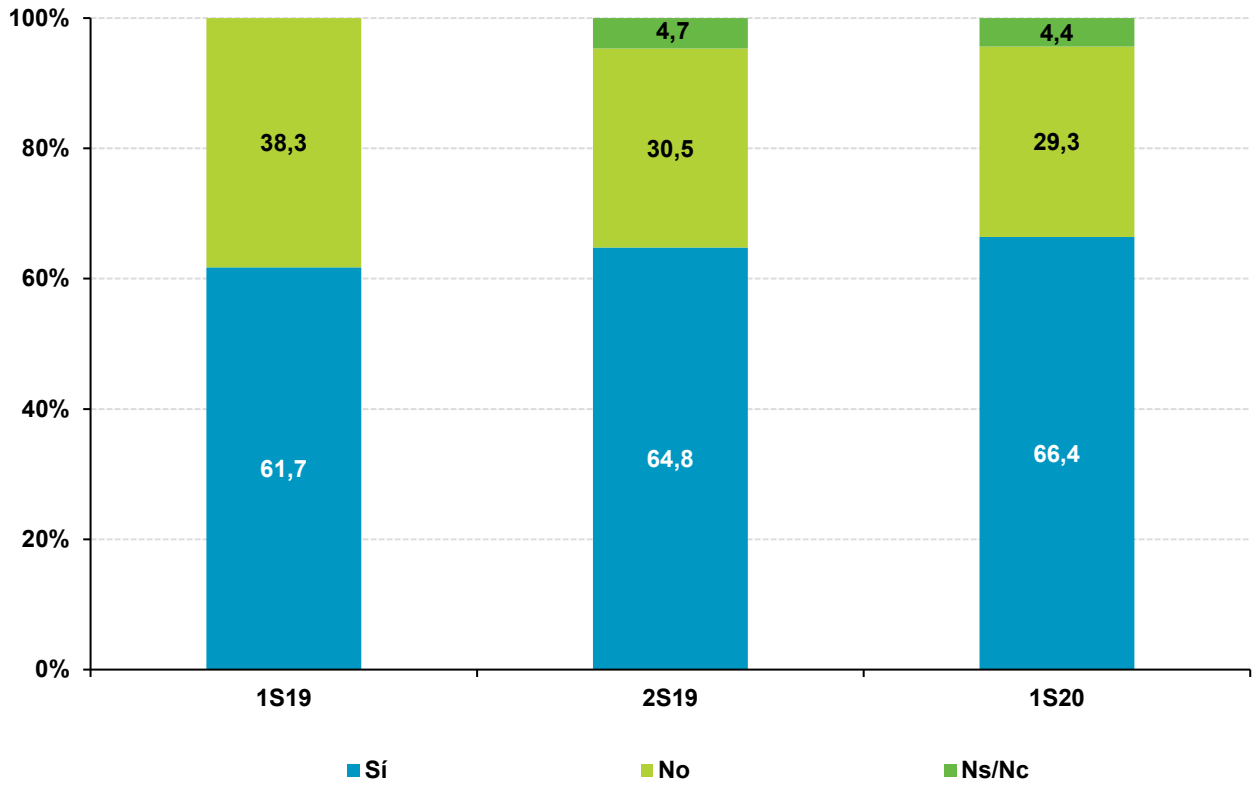
Lectura y aceptación de la información legal al registrarse o darse de alta en proveedores de servicios en Internet (redes sociales, comercio electrónico, etc.)



BASE: Total usuarios

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

Comprobación de permisos al instalar apps

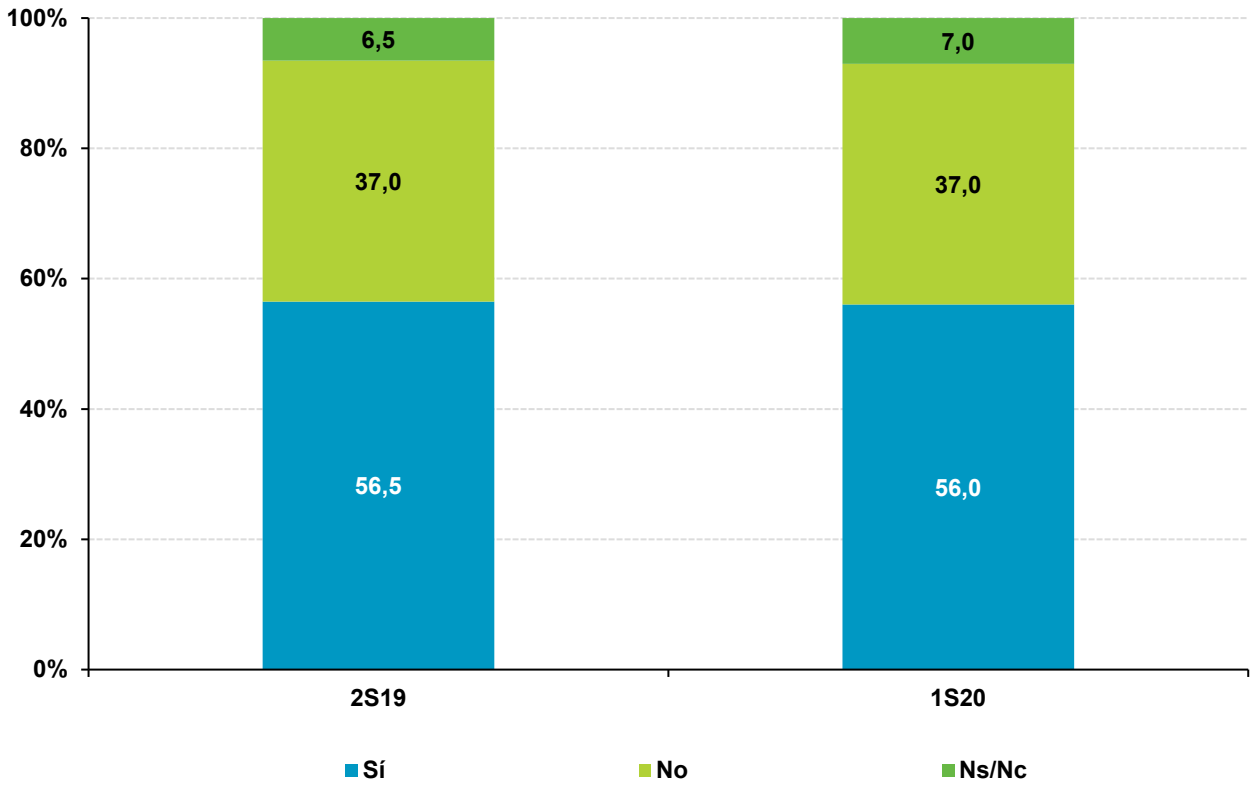


Permisos de apps y riesgos para tu privacidad
https://www.osi.es/es/permisos-de-apps-y-riesgos-para-tu-privacidad

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



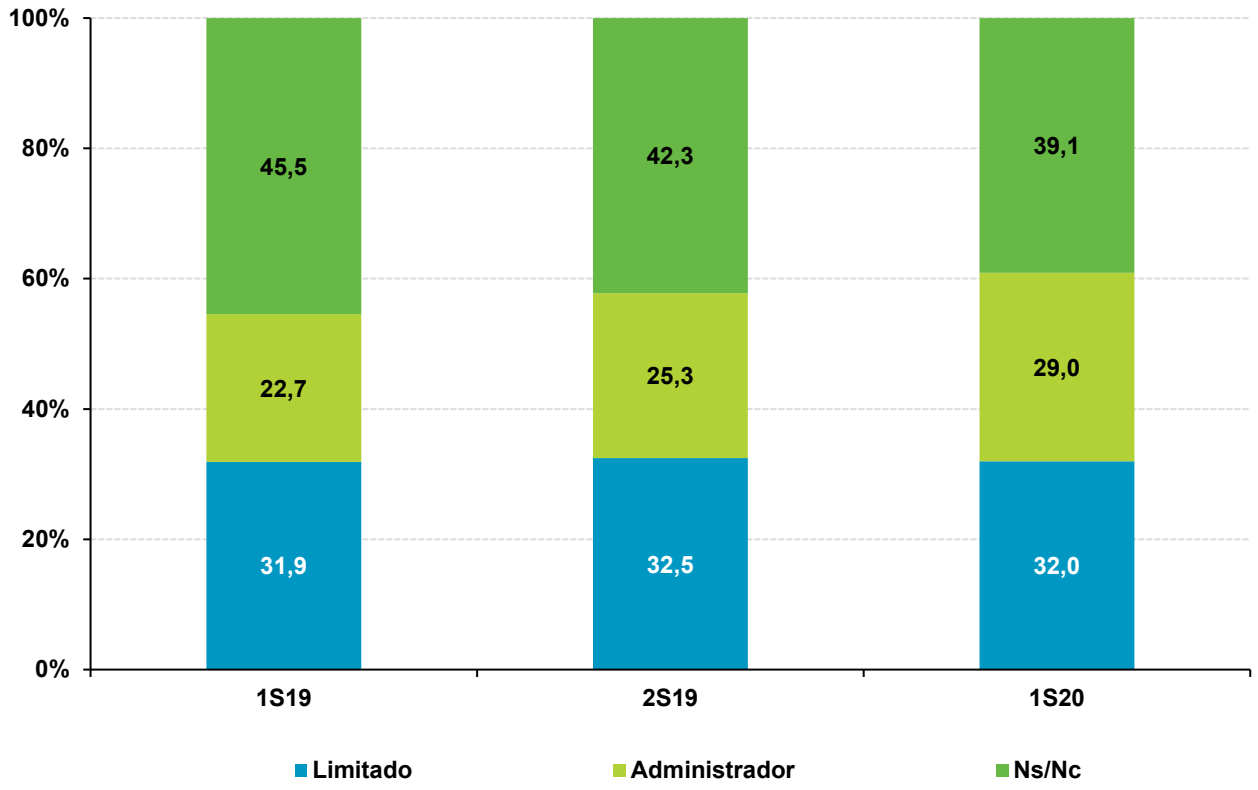
BASE: Usuarios que disponen de dispositivo Android y descargan apps

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

Privilegios del usuario en el dispositivo Android

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.

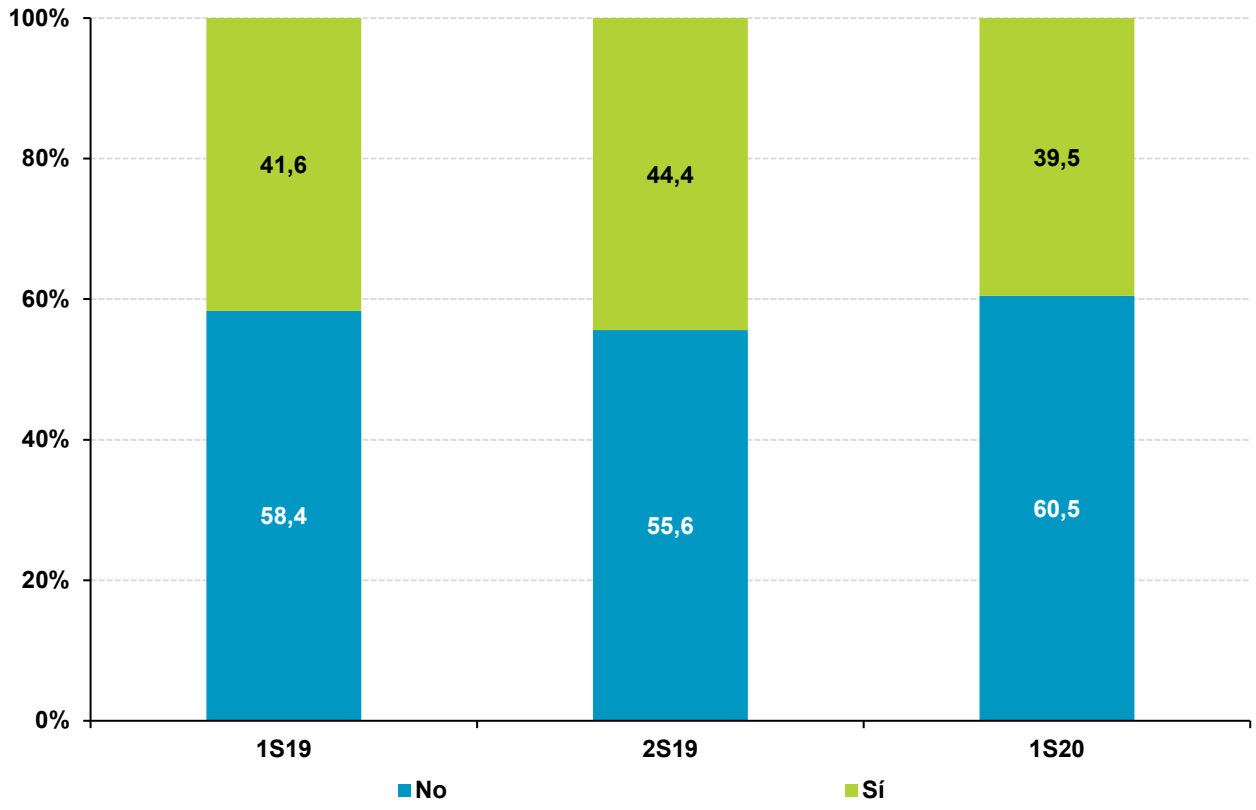
Más información:
https://www.osi.es/es/actualidad/blog/2019/04/24/conocias-el-termino-jailbreaking-o-rooting



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



BASE: Total usuarios

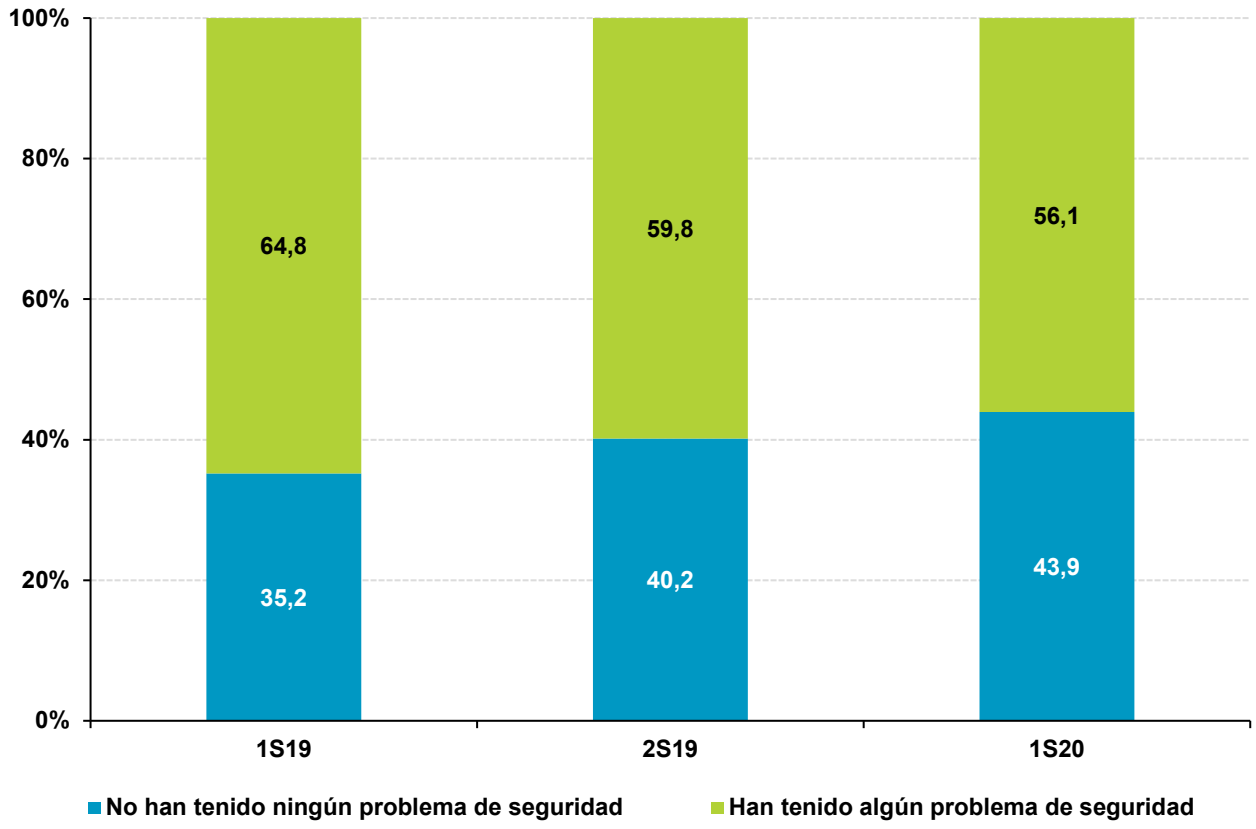
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

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



BASE: Total usuarios

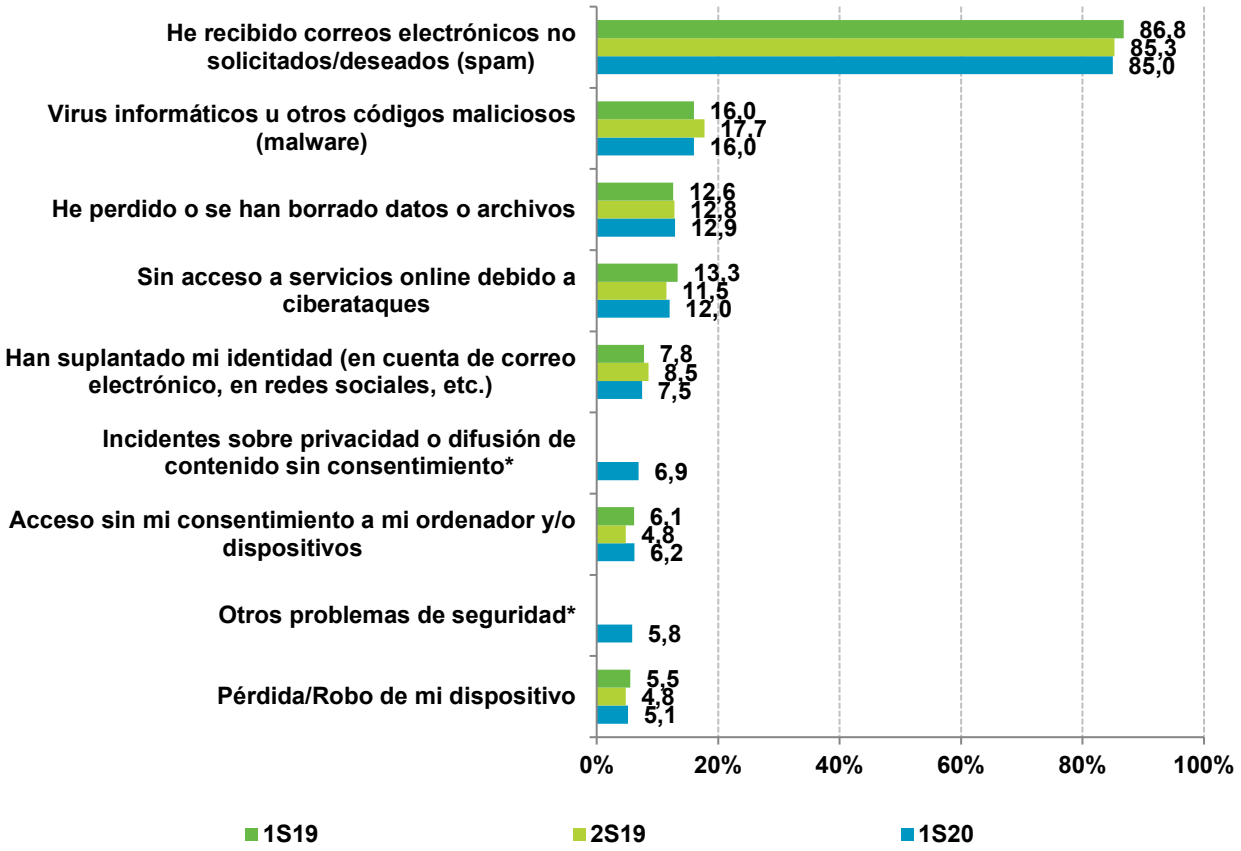
Módulo IV: Incidencias de seguridad

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

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.

Más información: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

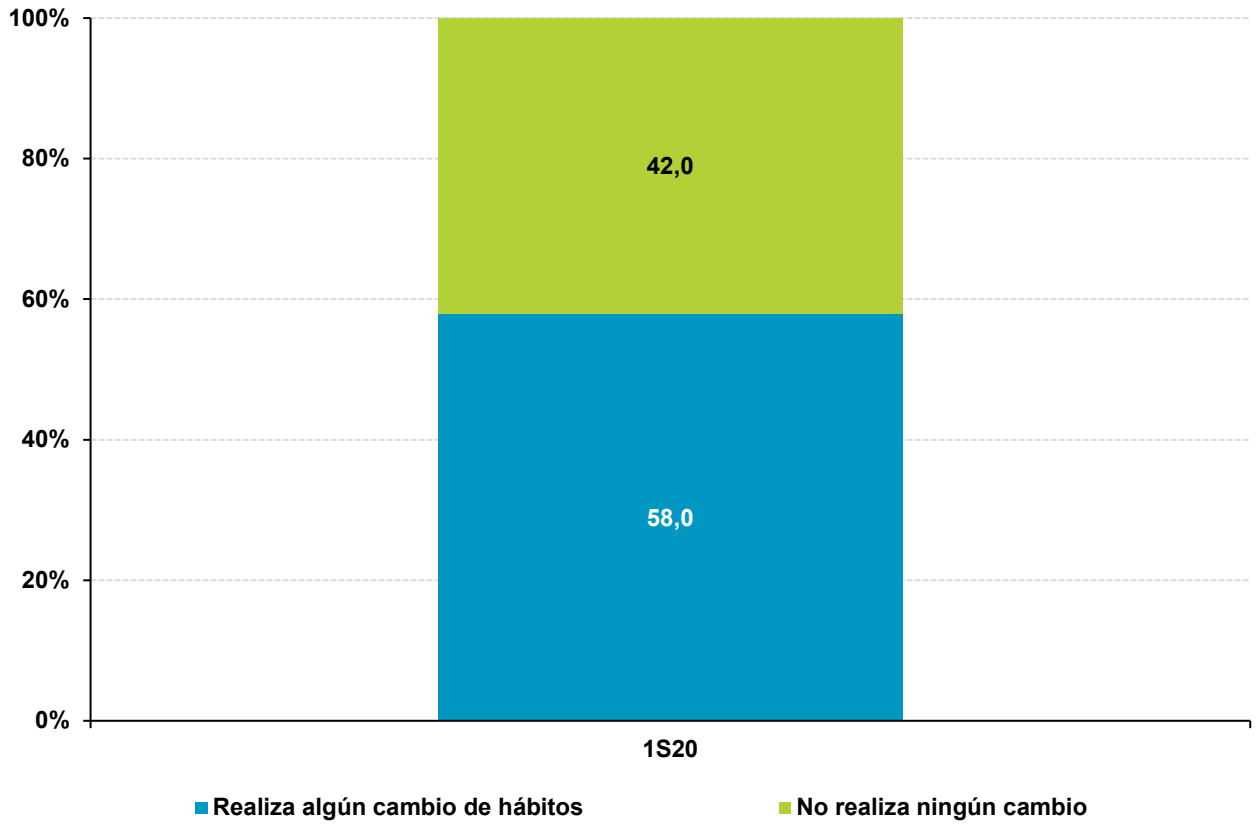


*nuevas categorías

BASE: Usuarios que han sufrido alguna incidencia de seguridad

Módulo IV: Incidencias de seguridad

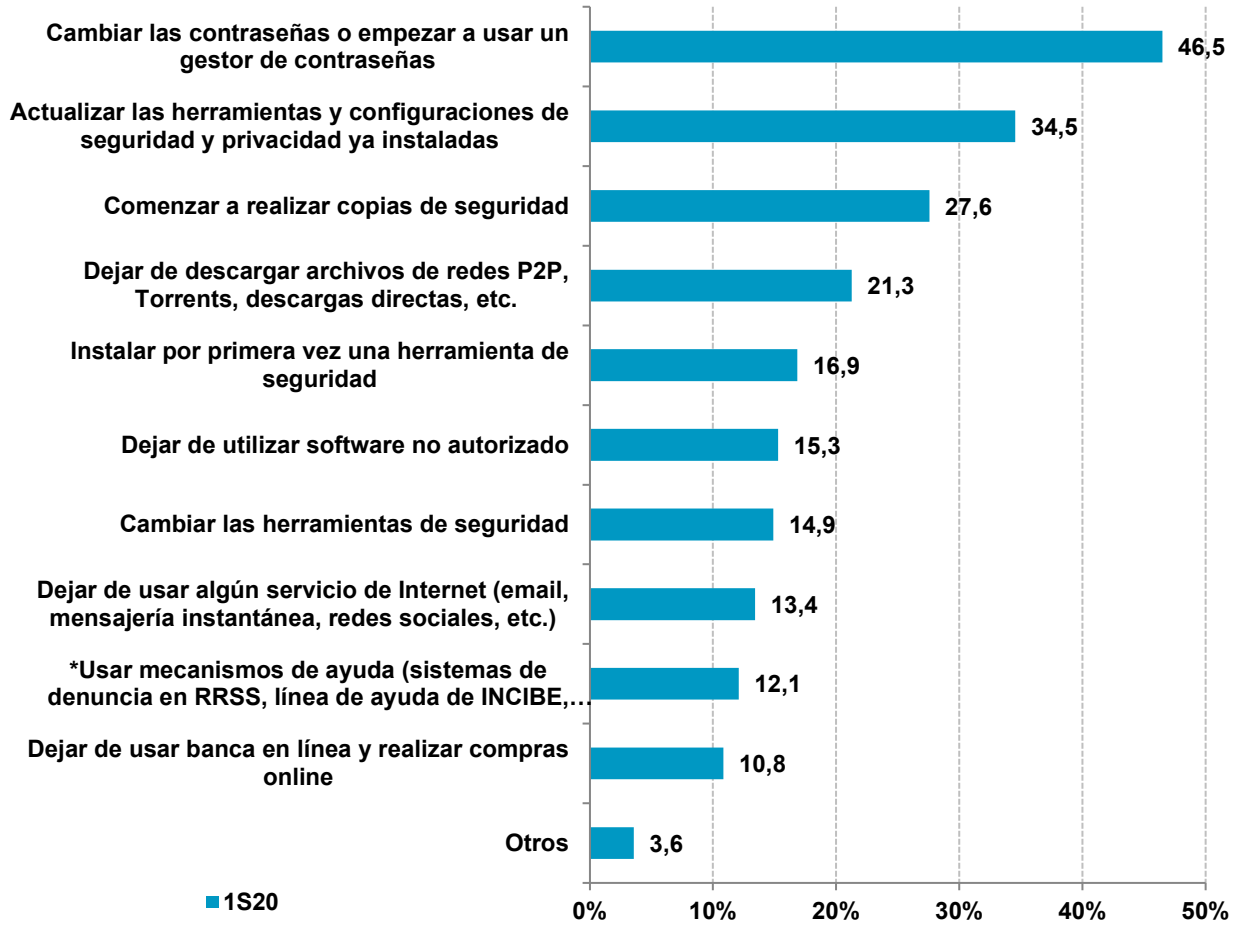
Realización de cambio de hábitos en Internet motivados por las incidencias de seguridad experimentadas durante los últimos seis meses



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

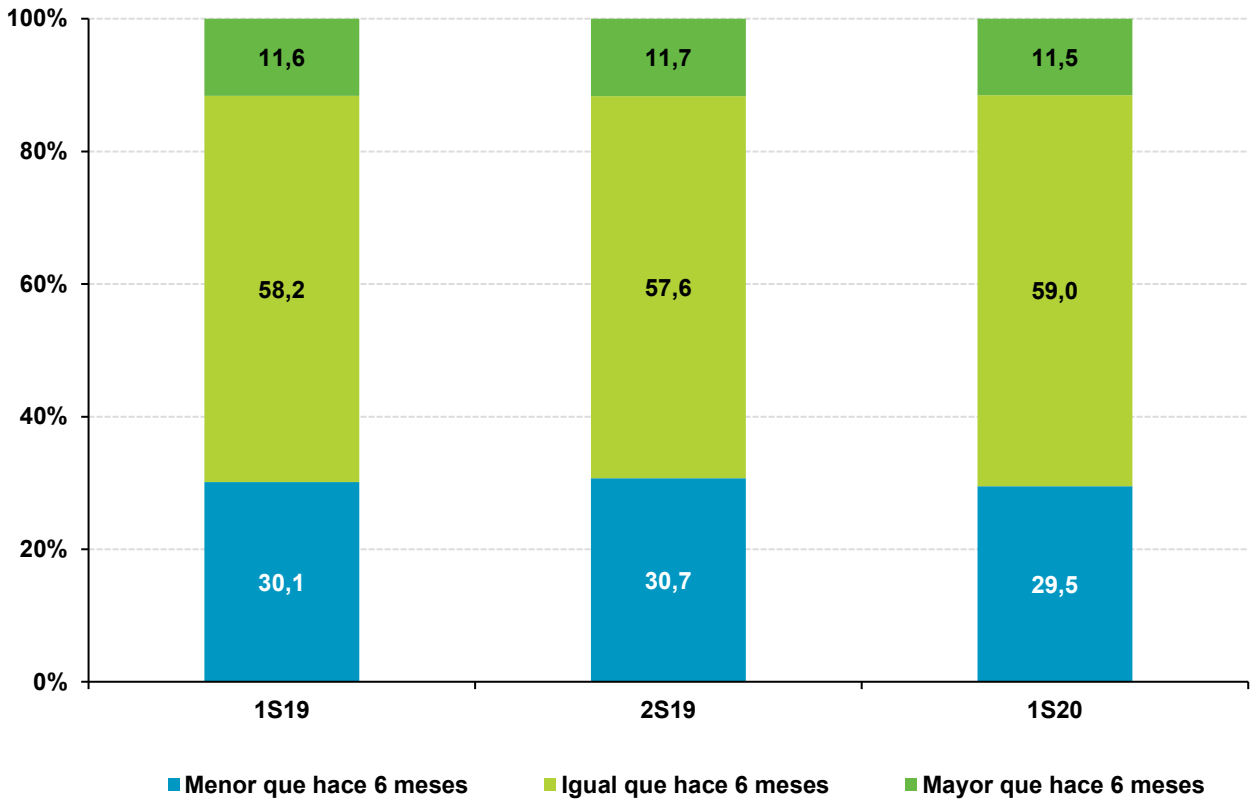


*nueva categoría

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

Módulo IV: Incidencias de seguridad

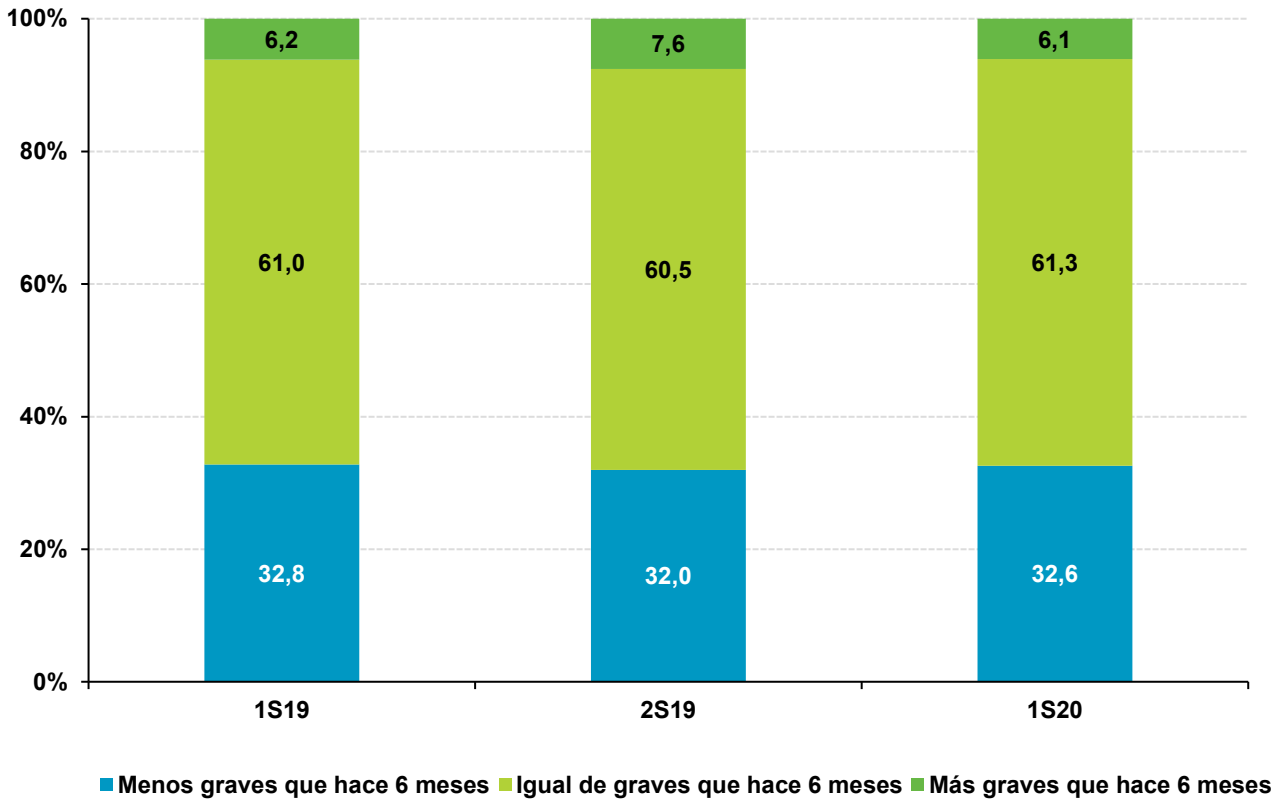
Percepción del usuario respecto al número de incidentes de seguridad que ha sufrido



BASE: Total usuarios

Módulo IV: Incidencias de seguridad

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



BASE: Total usuarios

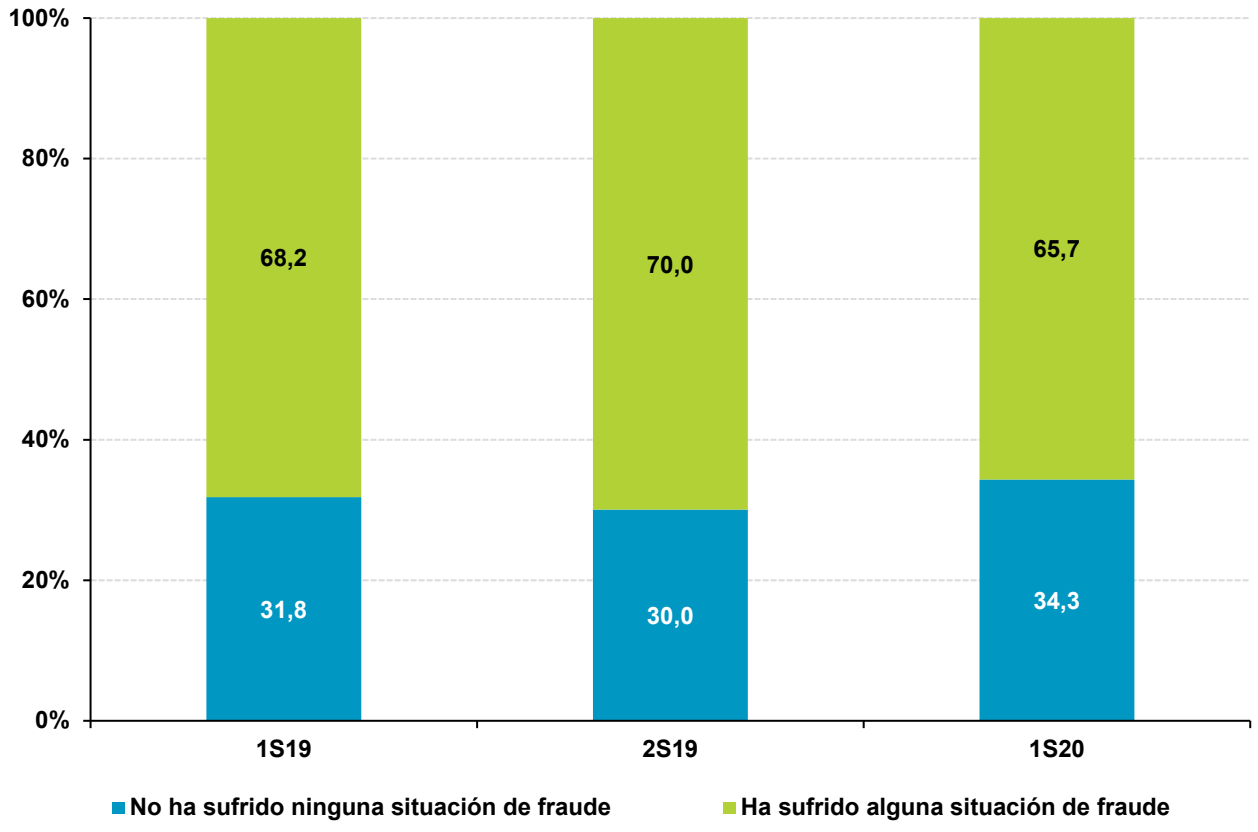
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

Módulo V: Fraude

Módulo V: Fraude

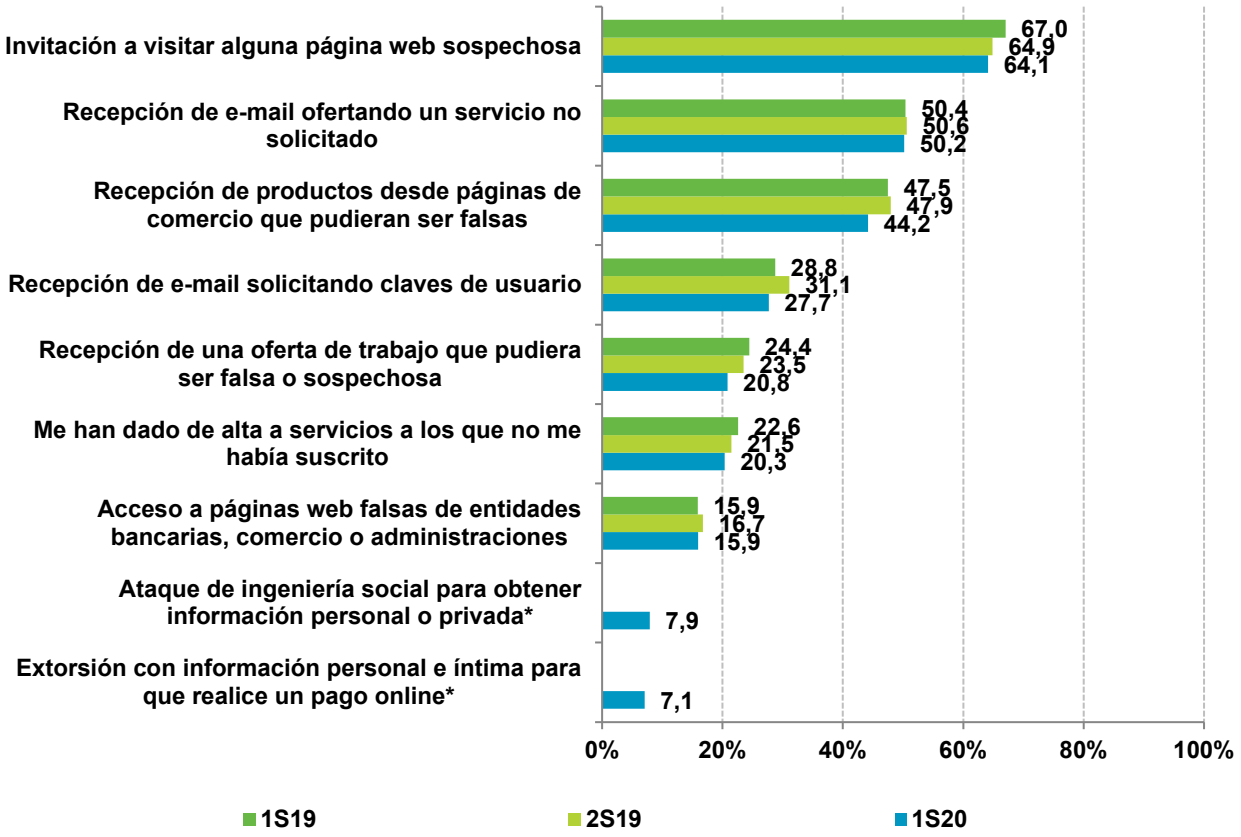
Ocurrencia de alguna situación de fraude en los últimos seis meses



BASE: Total usuarios

Módulo: Fraude

Situaciones de fraude ocurridas en los últimos seis meses



*nuevas categorías

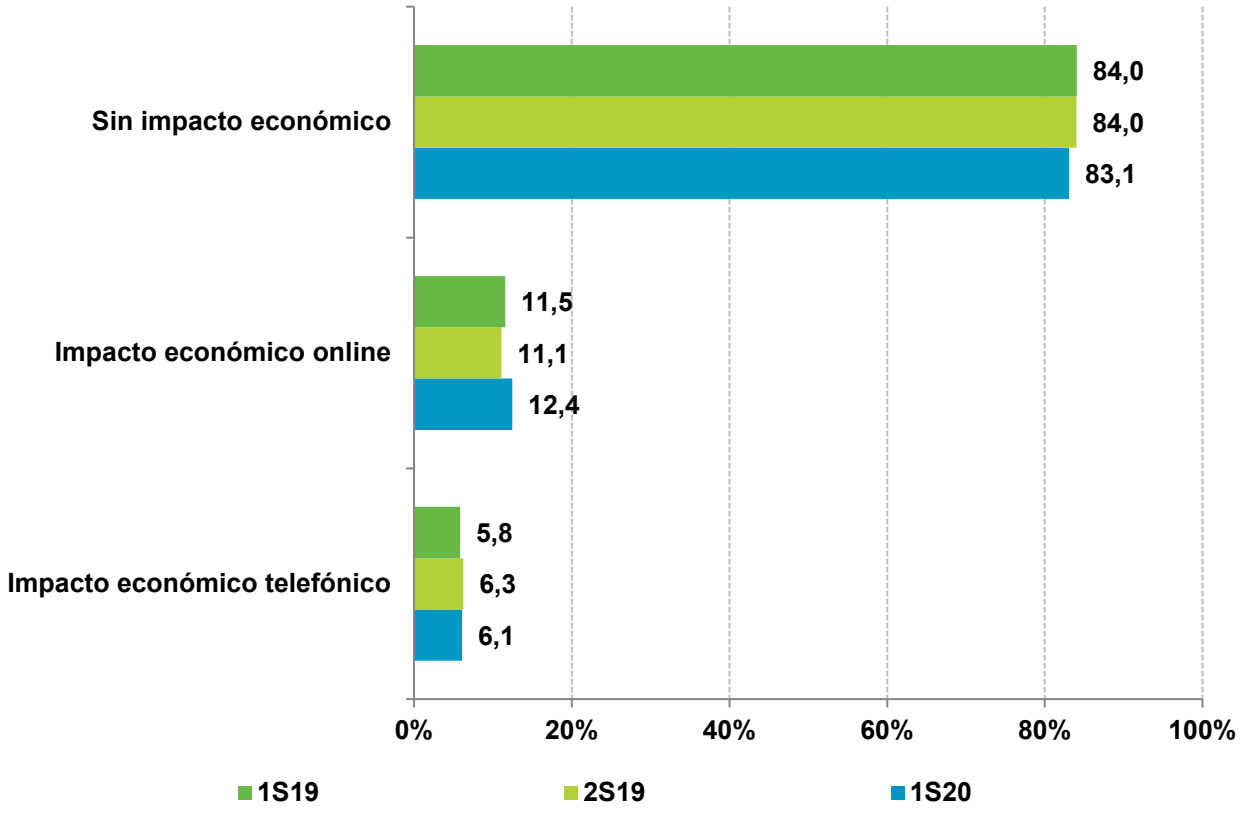
BASE: Usuarios que han sufrido alguna situación de fraude

¿Sabes como identificar el fraude online?

https://www.osi.es/es/guia-fraudes-online

Módulo V: Fraude

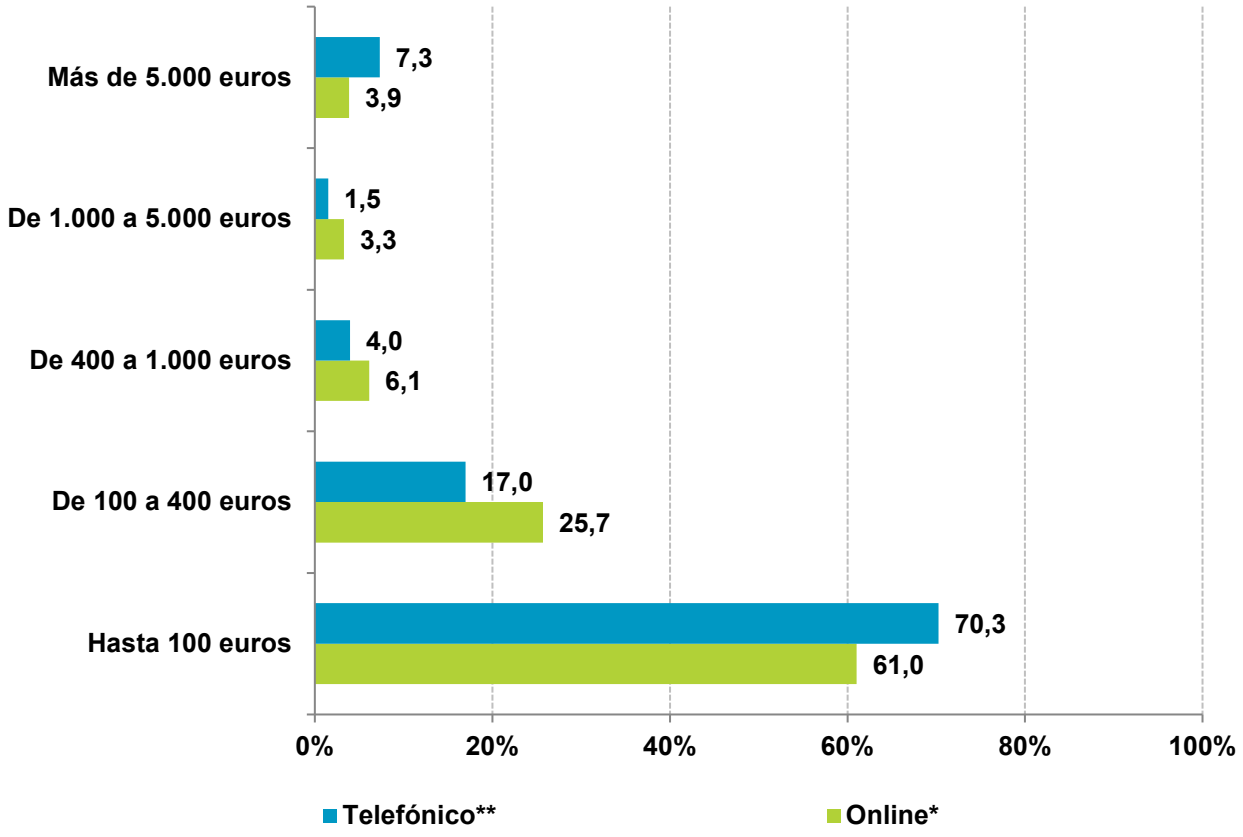
Perjuicio económico debido a posibles fraudes



BASE: Usuarios que han sufrido alguna situación de fraude

Módulo V: Fraude

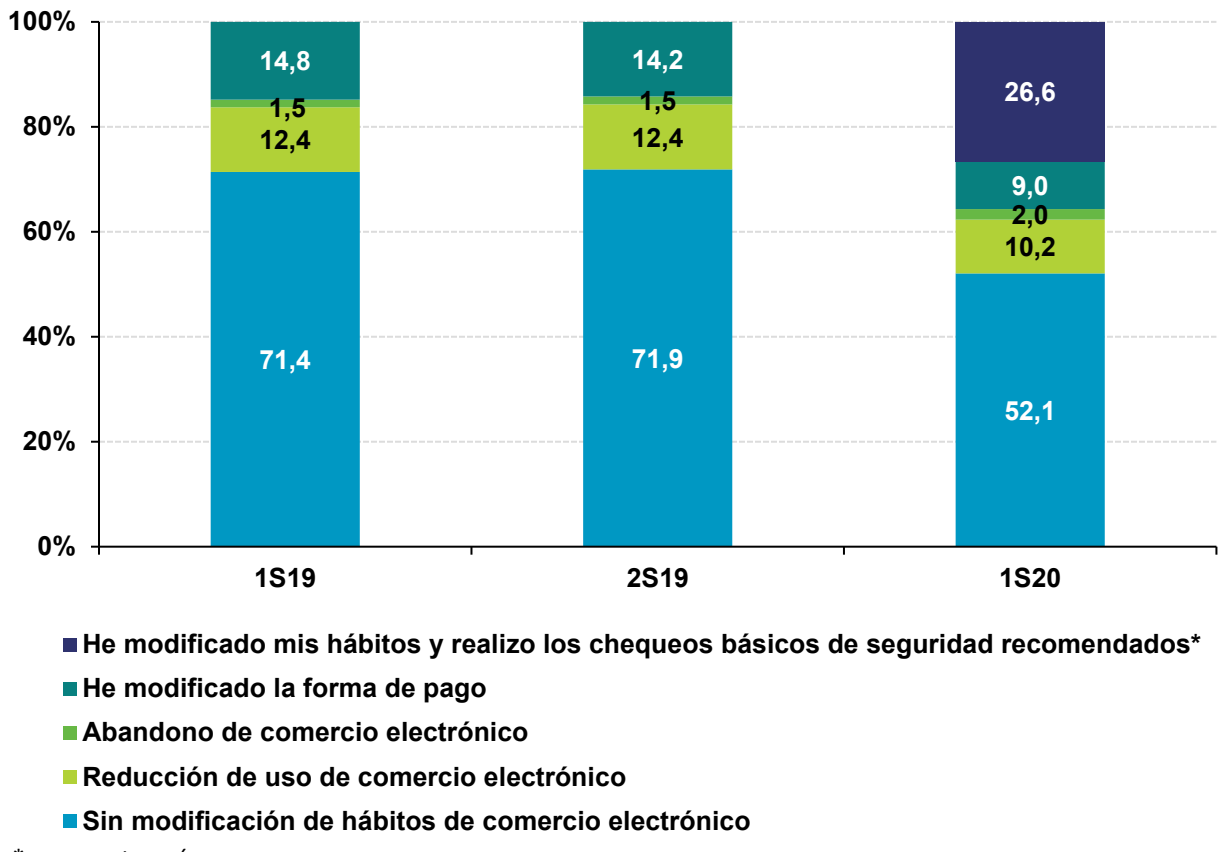
Distribución del perjuicio económico debido a posibles fraudes



* 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

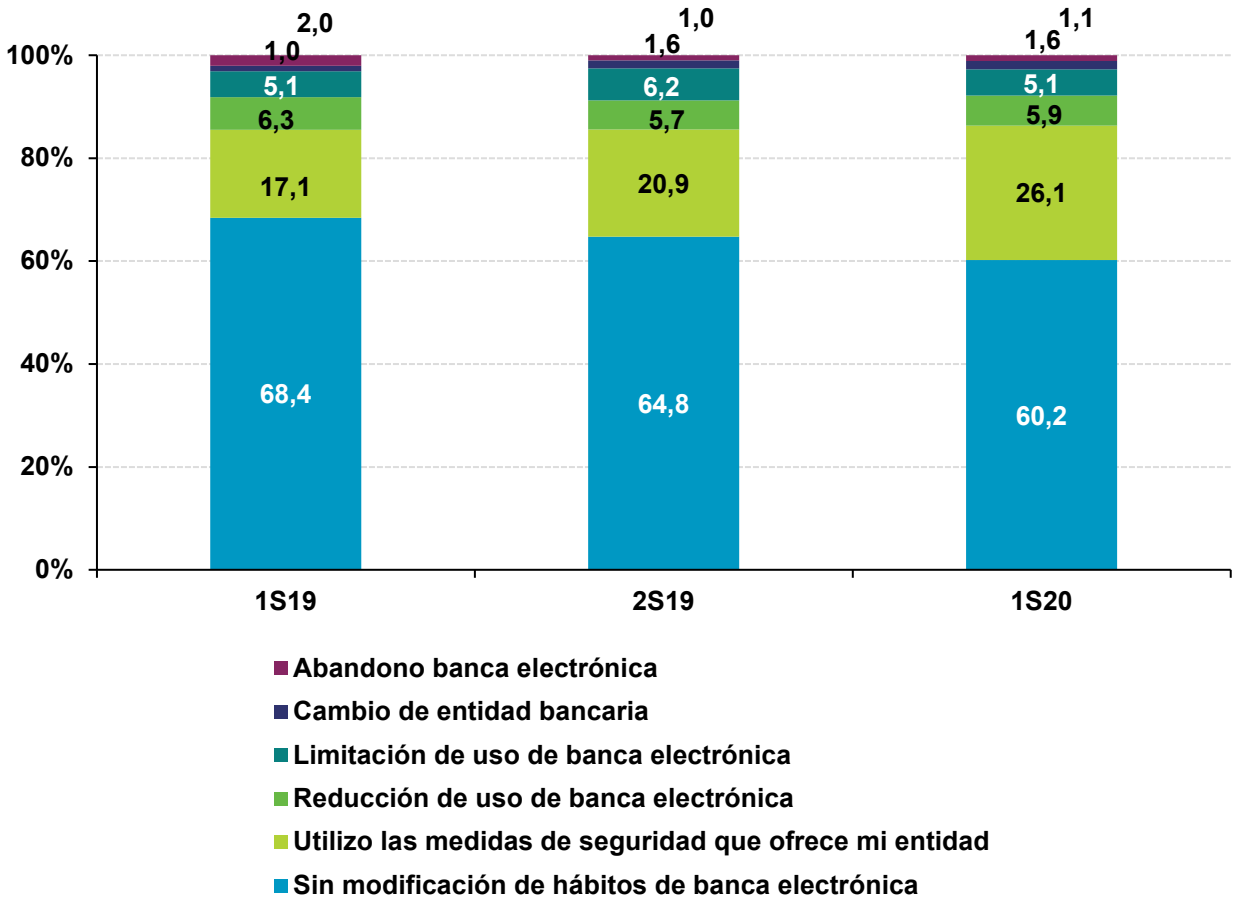


*nueva categoría

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



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

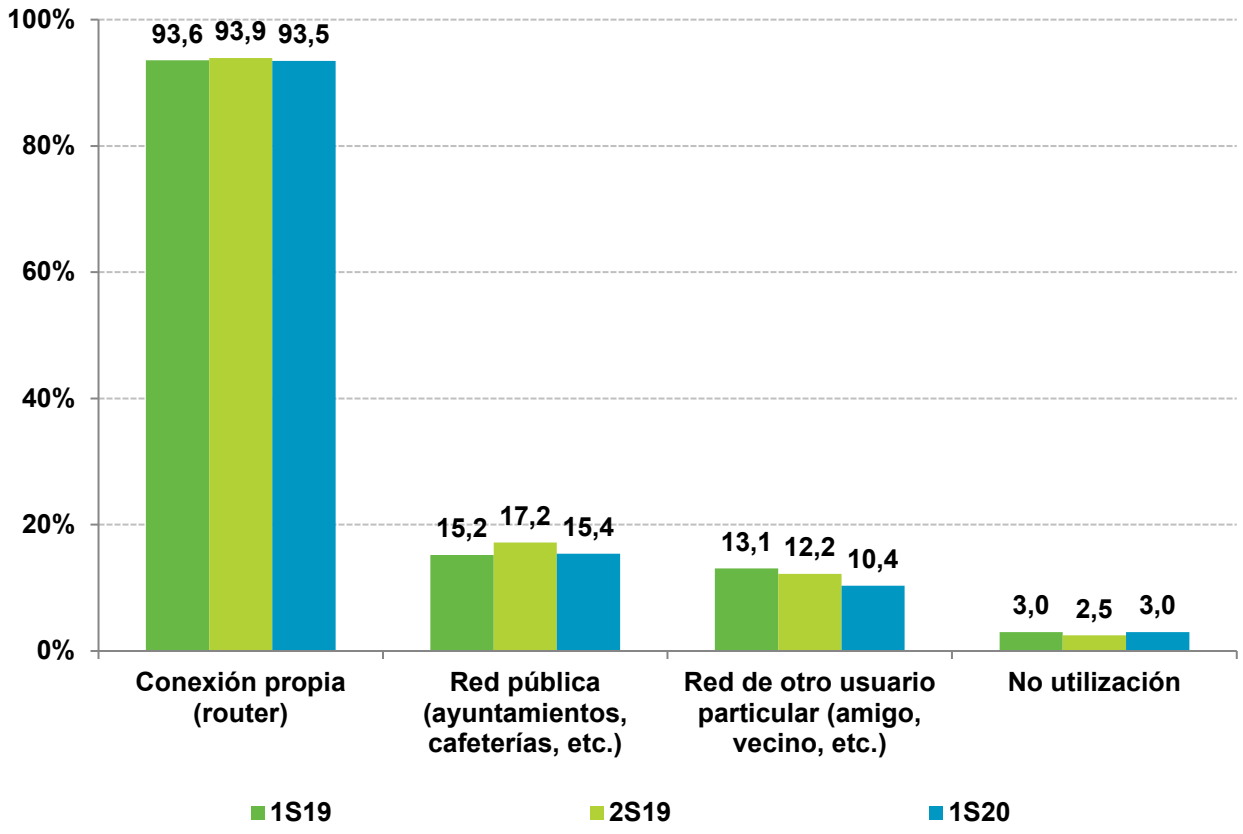
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

Módulo VI:
Seguridad en Wi-Fi

Módulo VI: Seguridad en Wi-Fi

Punto de acceso a Internet mediante redes inalámbricas Wi-Fi

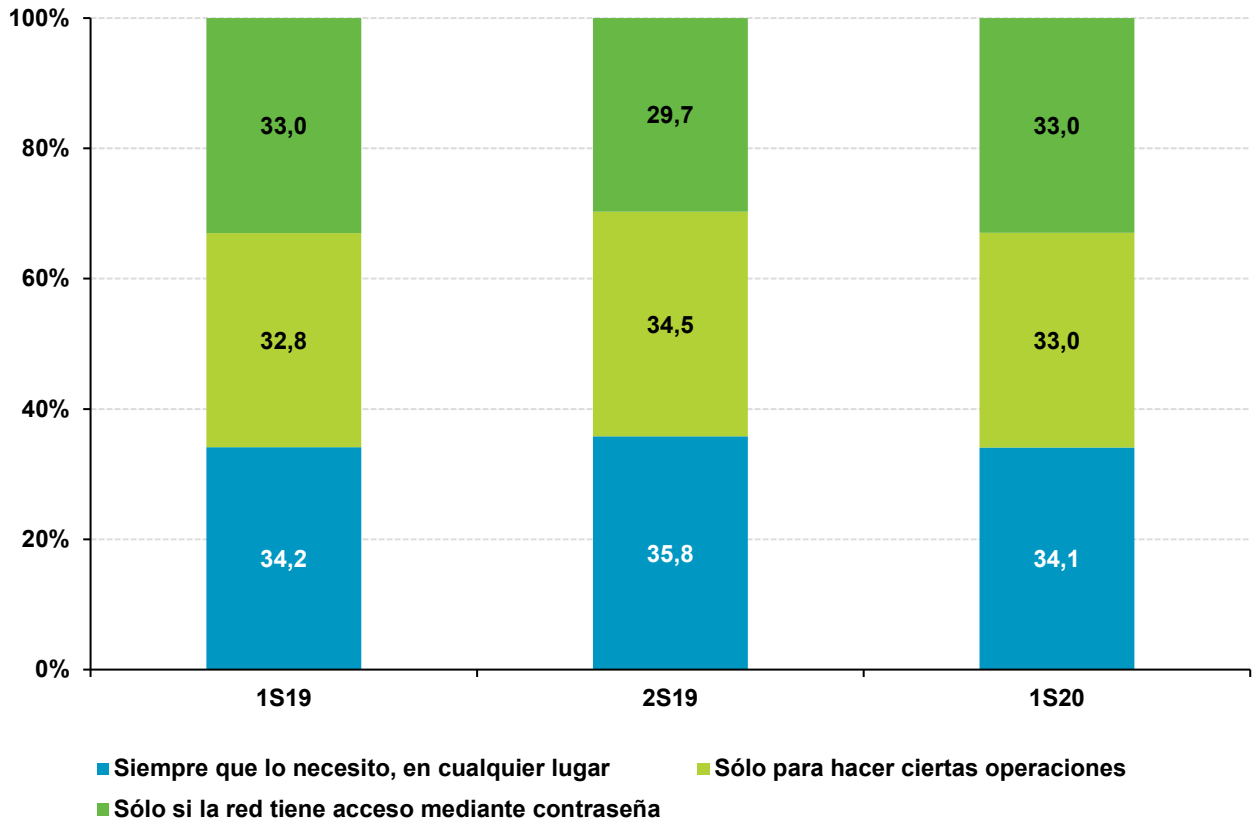


BASE: Total usuarios

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

Módulo VI: Seguridad en Wi-Fi

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

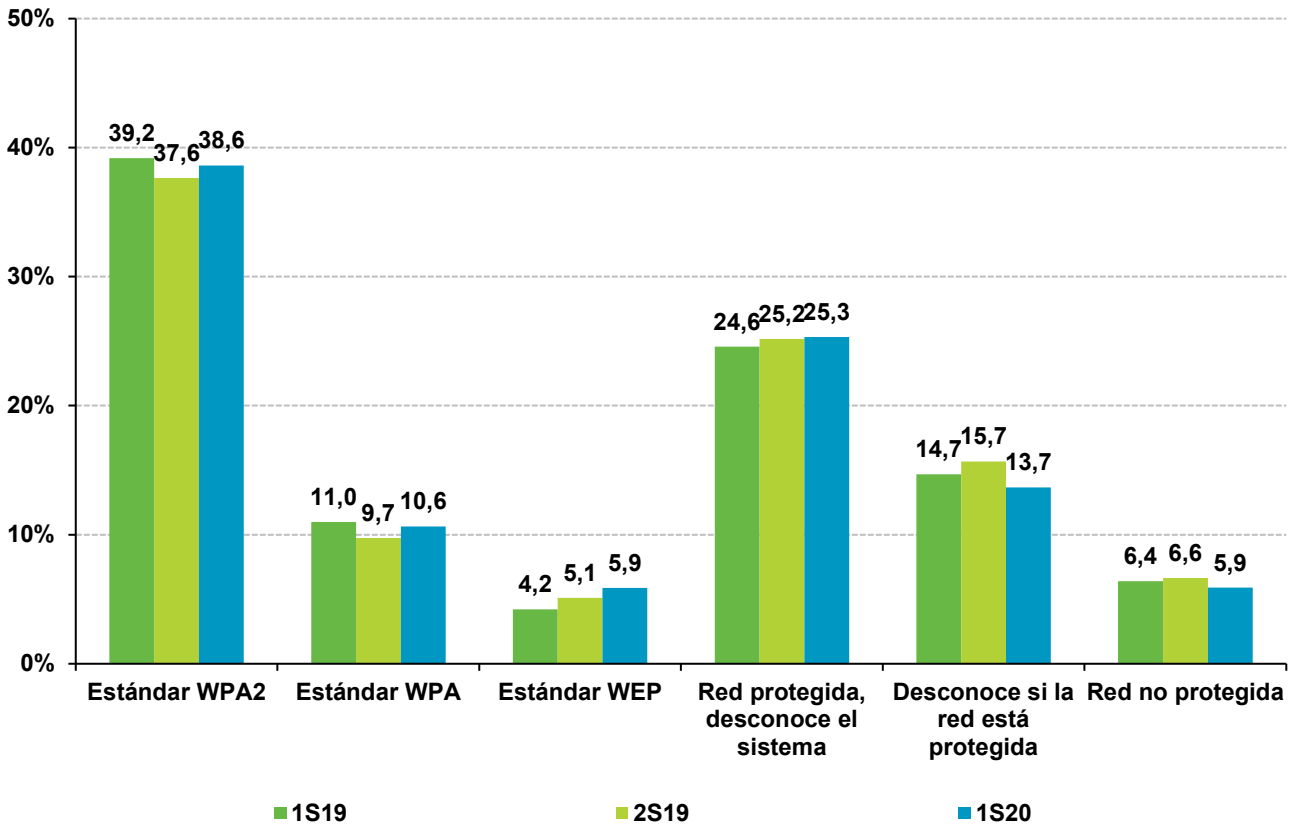


Cómo conectarte a redes Wi-Fi públicas de forma segura: https://www.osi.es/es/actualidad/blog/2019/05/02/conexion-gratis-la-vista-conecto-mi-movil

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

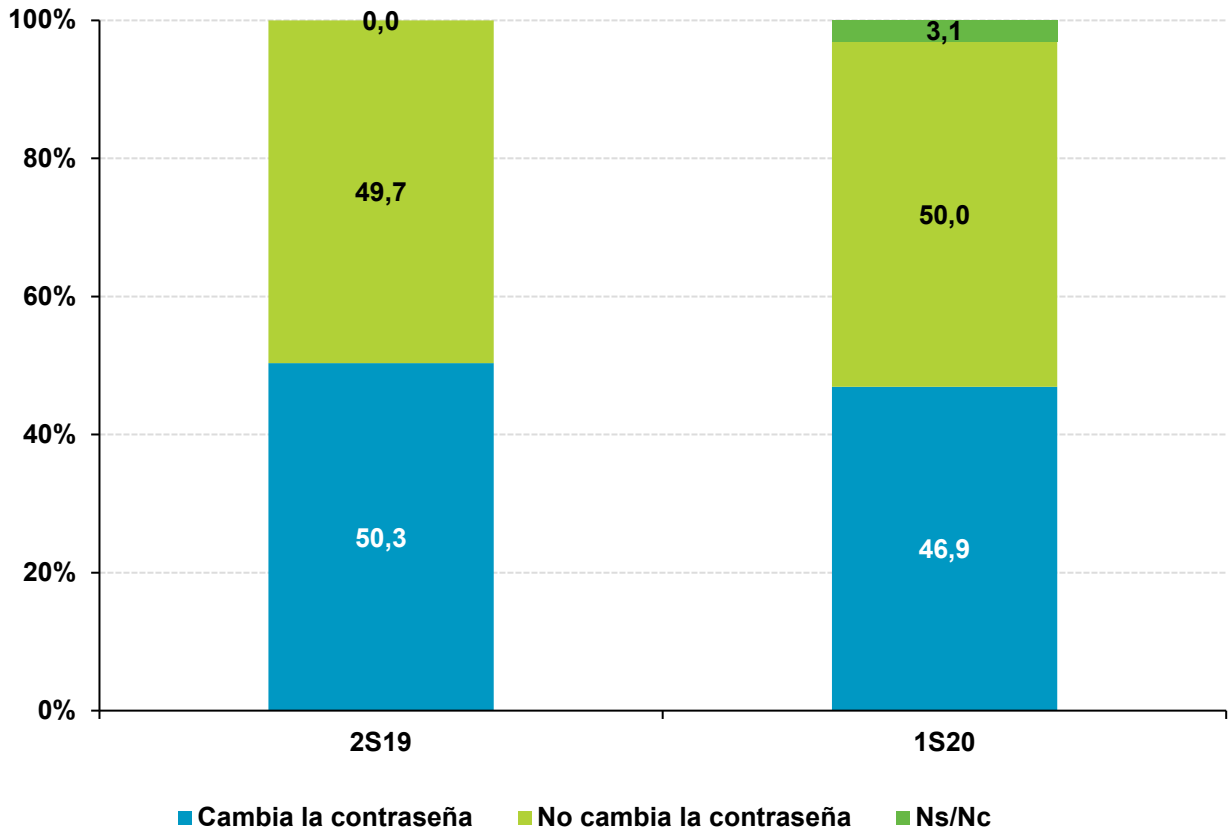


Cómo configurar tu red Wi-Fi de modo seguro: *https://www.osi.es/protege-tu-wifi*

BASE: Usuarios con conexión Wi-Fi propia

Módulo VI: Seguridad en Wi-Fi

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



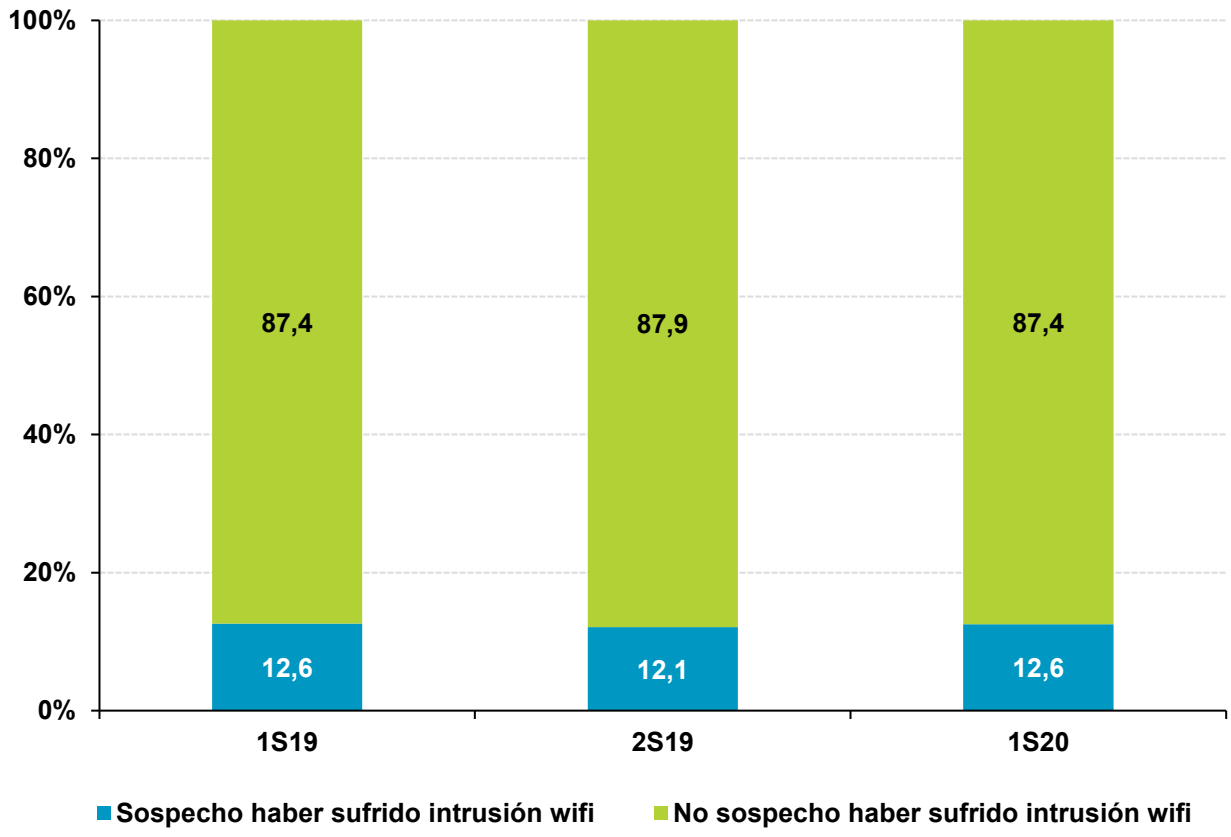
BASE: Usuarios con conexión Wi-Fi propia y sistema de seguridad

Módulo VI: Seguridad en Wi-Fi

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

¿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

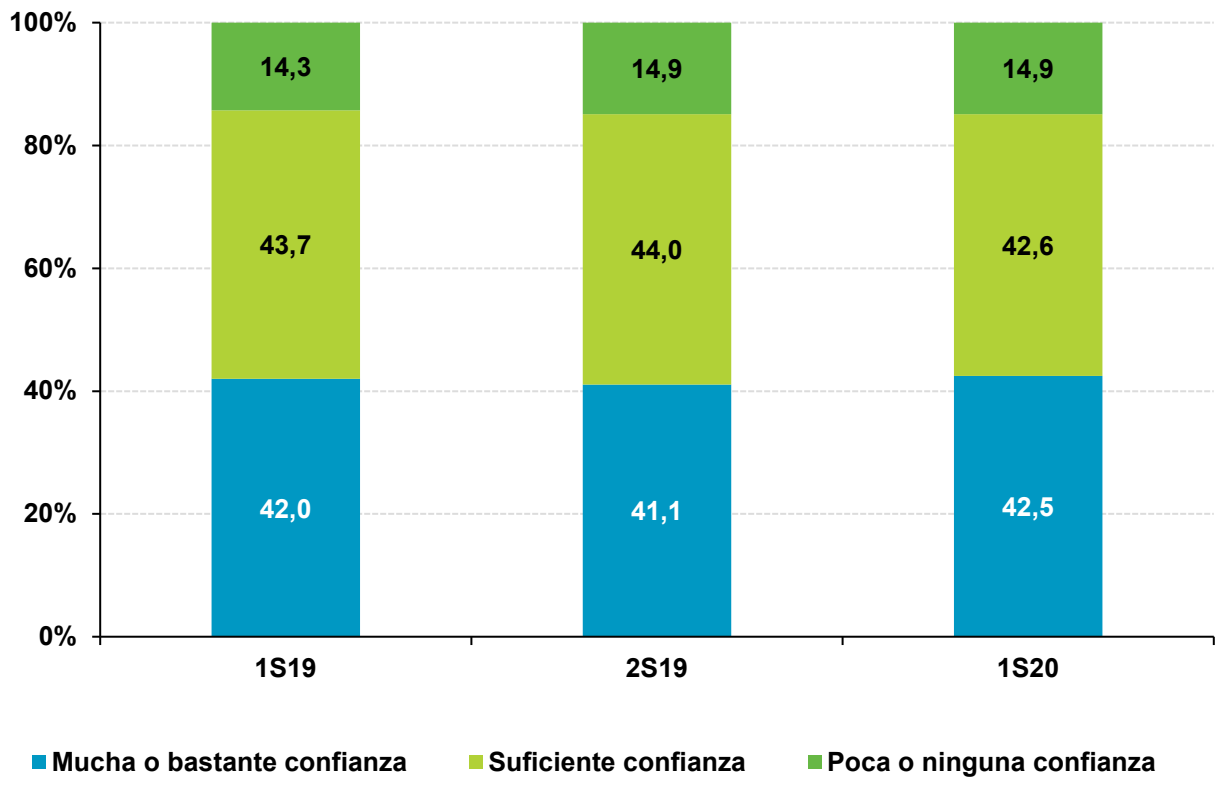
GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

Módulo VII: Opinión

Módulo VII: Opinión

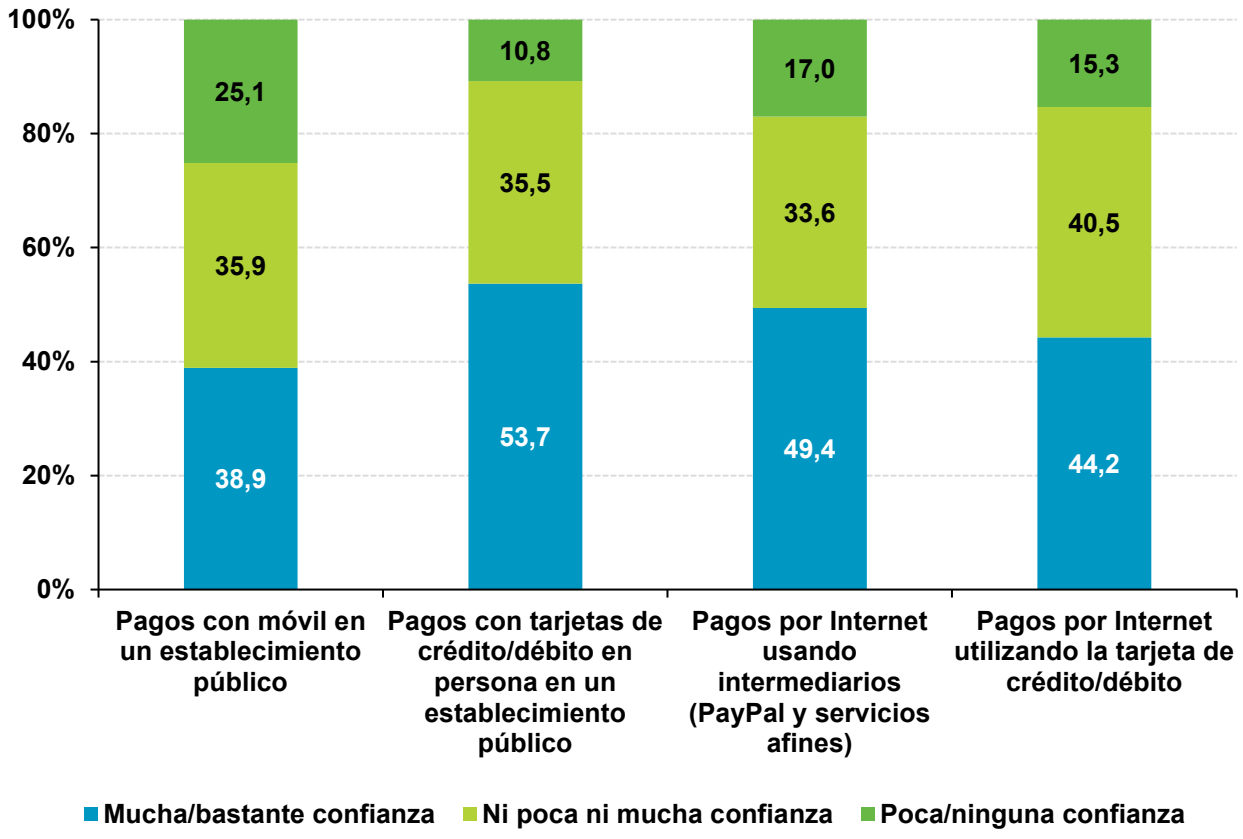
Nivel de confianza en Internet



BASE: Total usuarios

Módulo VII: Opinión

Nivel de confianza al realizar pagos (online y offline)



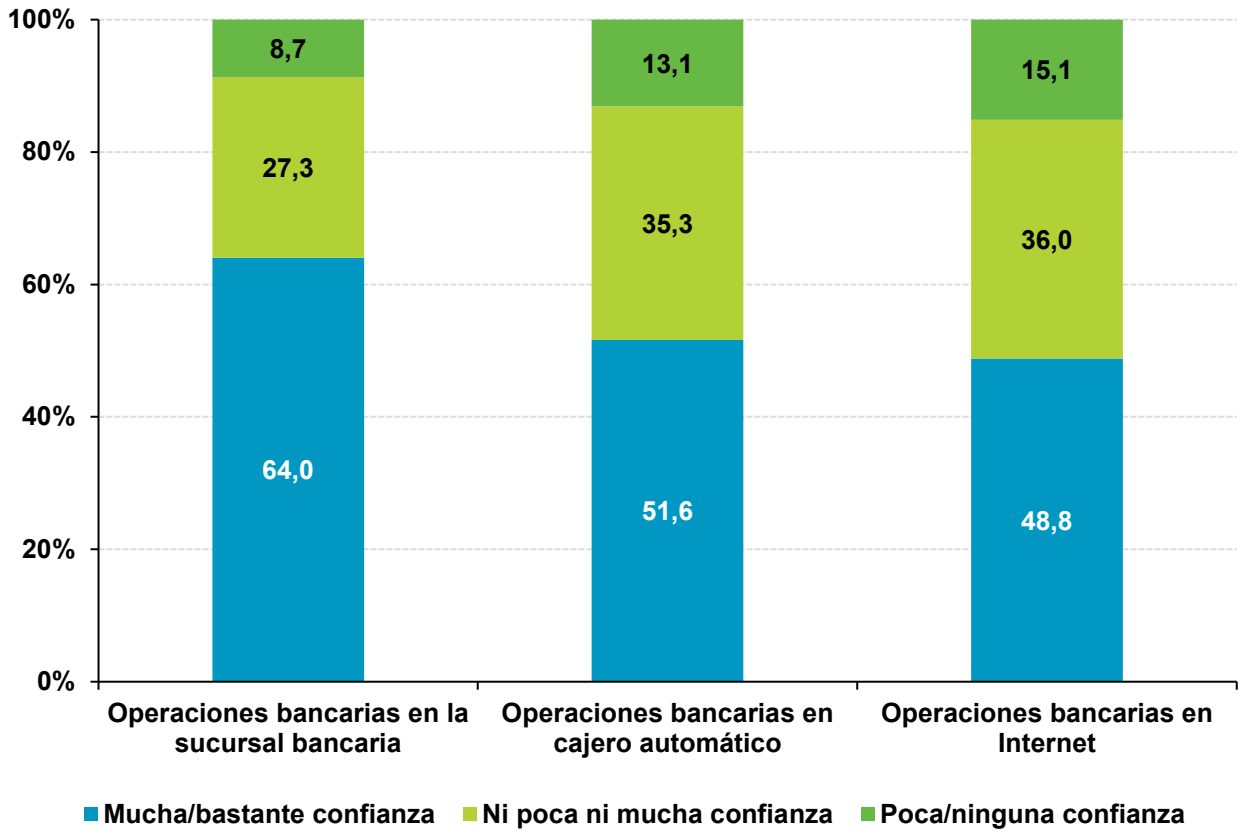
¿Sabes qué precauciones debes tener en cuenta para evitar caer en un engaño al realizar compras online?

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

BASE: Total usuarios

Módulo VII: Opinión

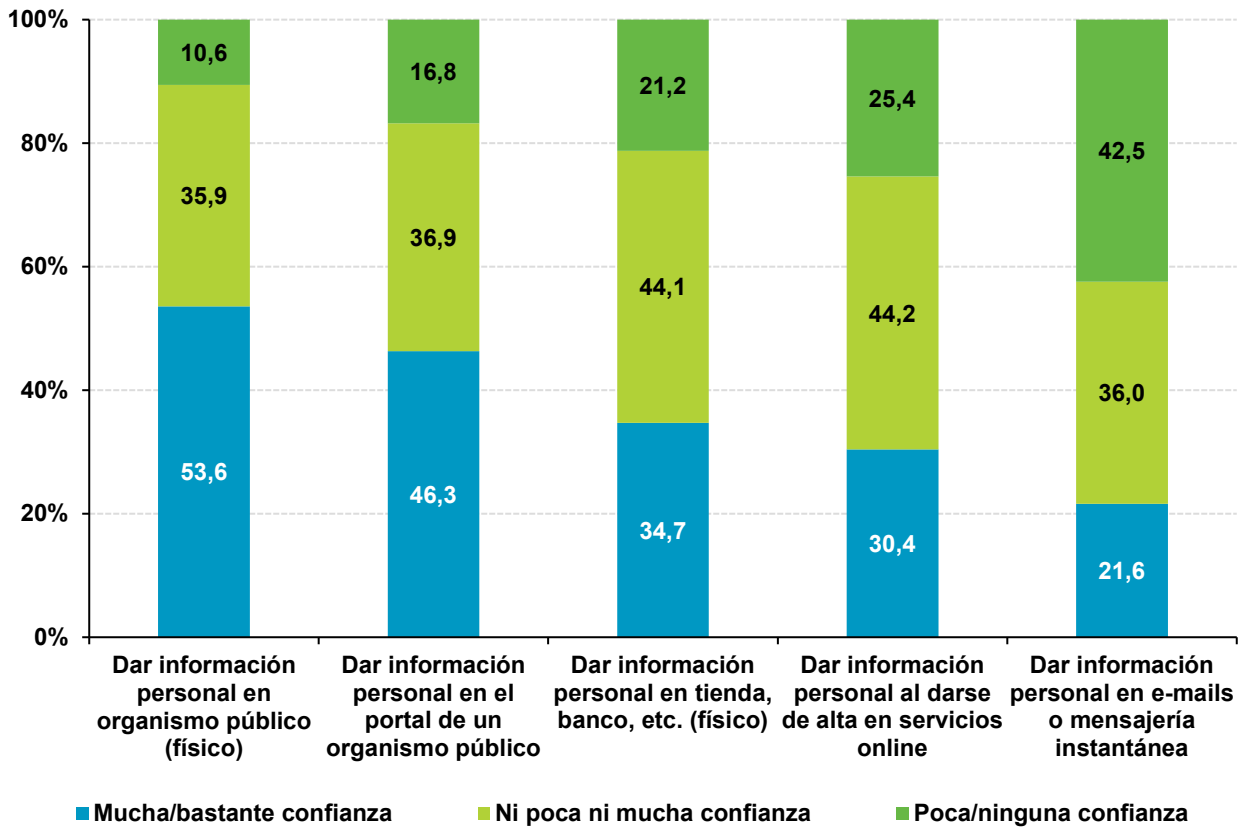
Nivel de confianza al realizar operaciones bancarias (online y offline)



BASE: Total usuarios

Módulo VII: Opinión

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

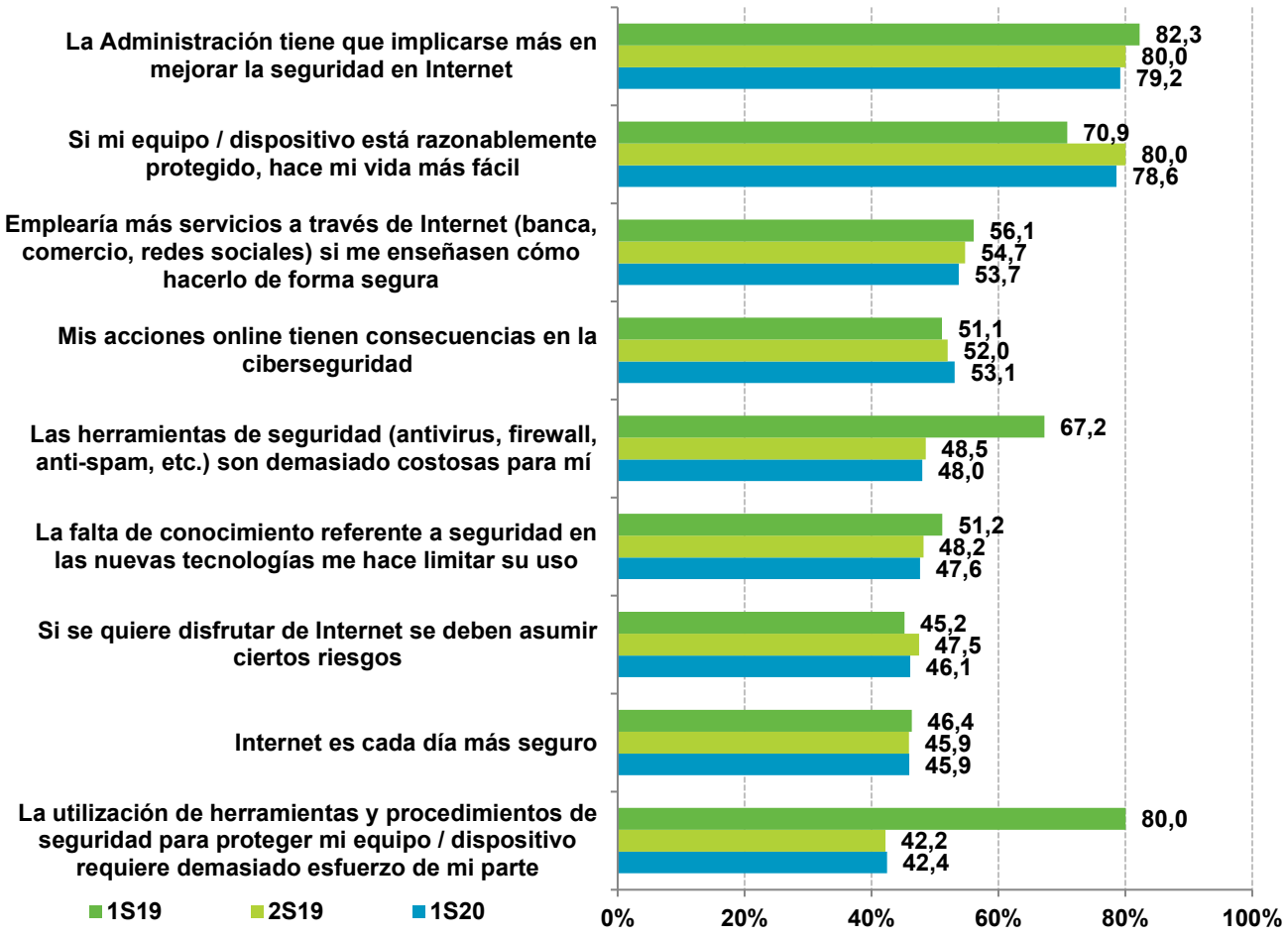


BASE: Total usuarios

Módulo VII: Opinión

Opiniones sobre la seguridad en Internet

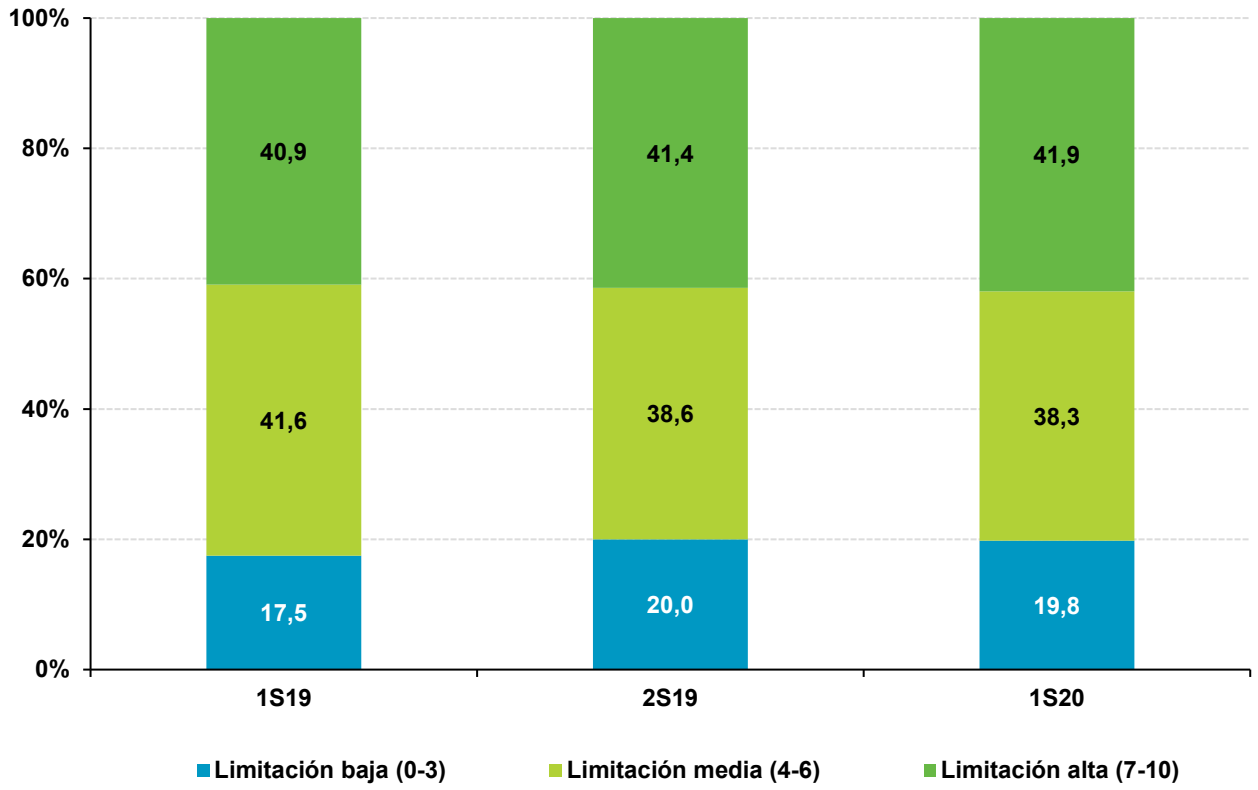
(de acuerdo o totalmente de acuerdo)



BASE: Total usuarios

Módulo VII: Opinión

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



BASE: Total usuarios

Módulo VII: Opinión

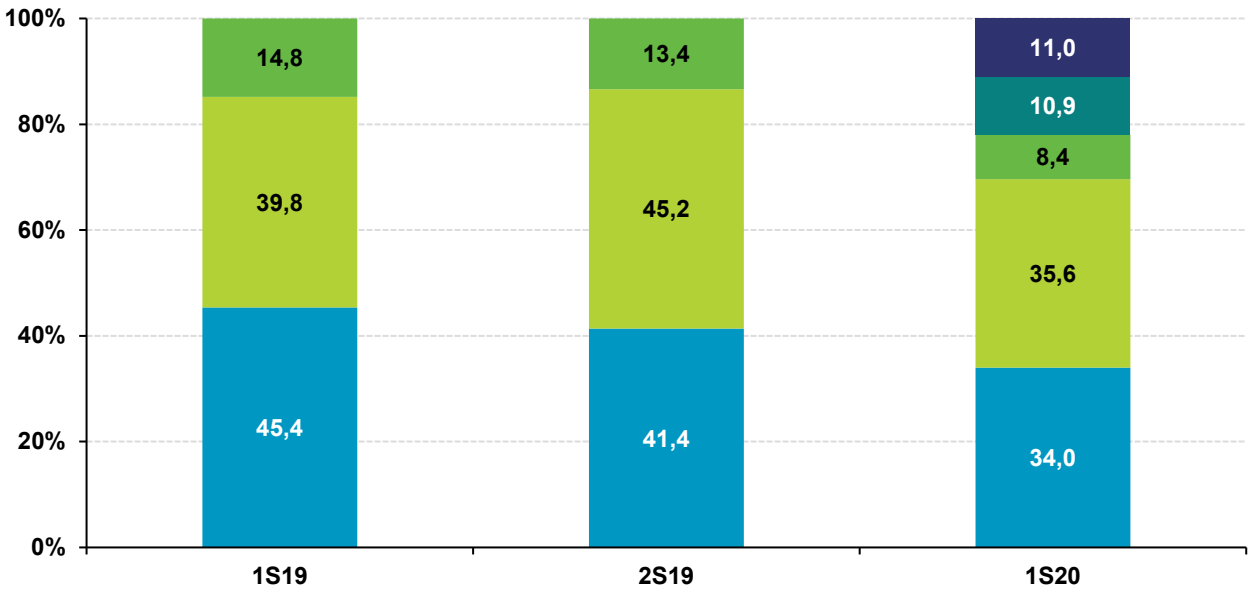
Percepción de los riesgos a los que se está más expuesto al navegar por Internet

¿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*



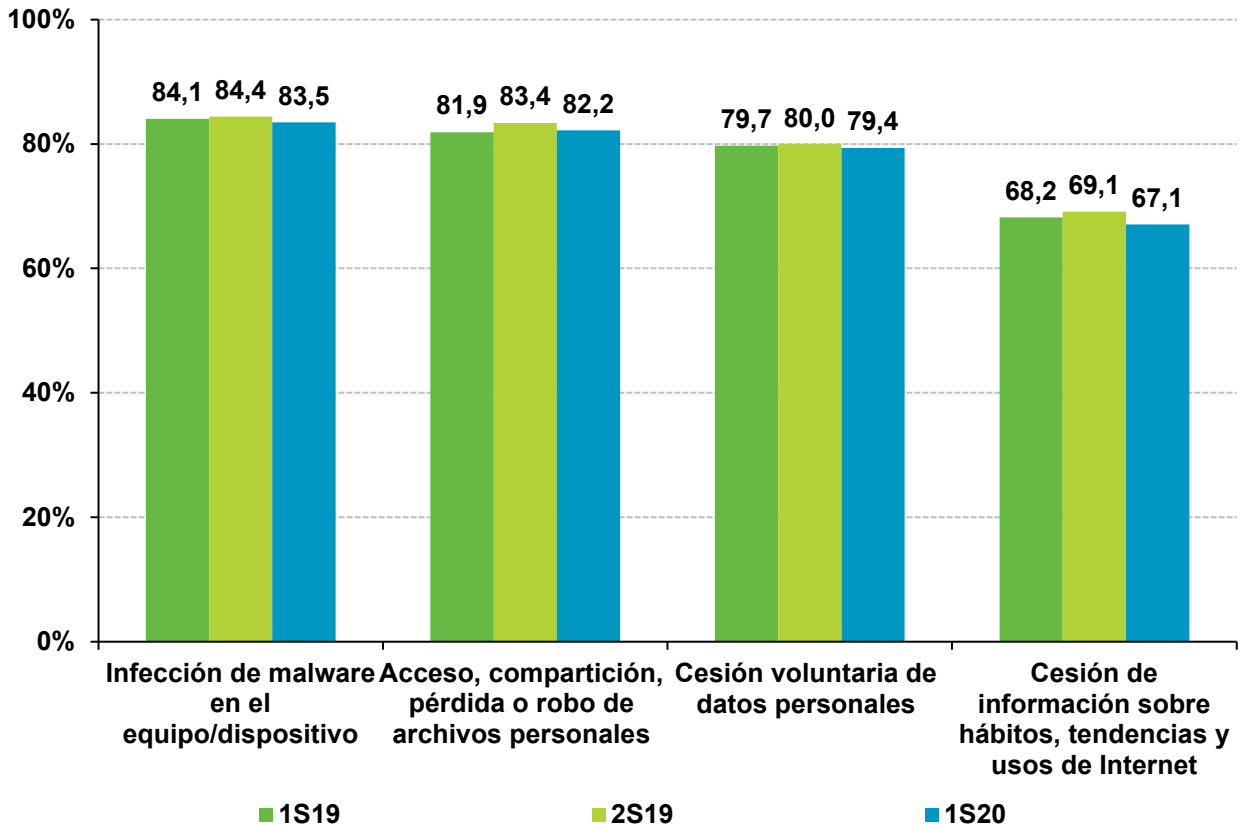
*nuevas categorías

BASE: Total usuarios

Módulo VII: Opinión

Valoración de los peligros al navegar por Internet

(bastante o muy importante)



BASE: Total usuarios

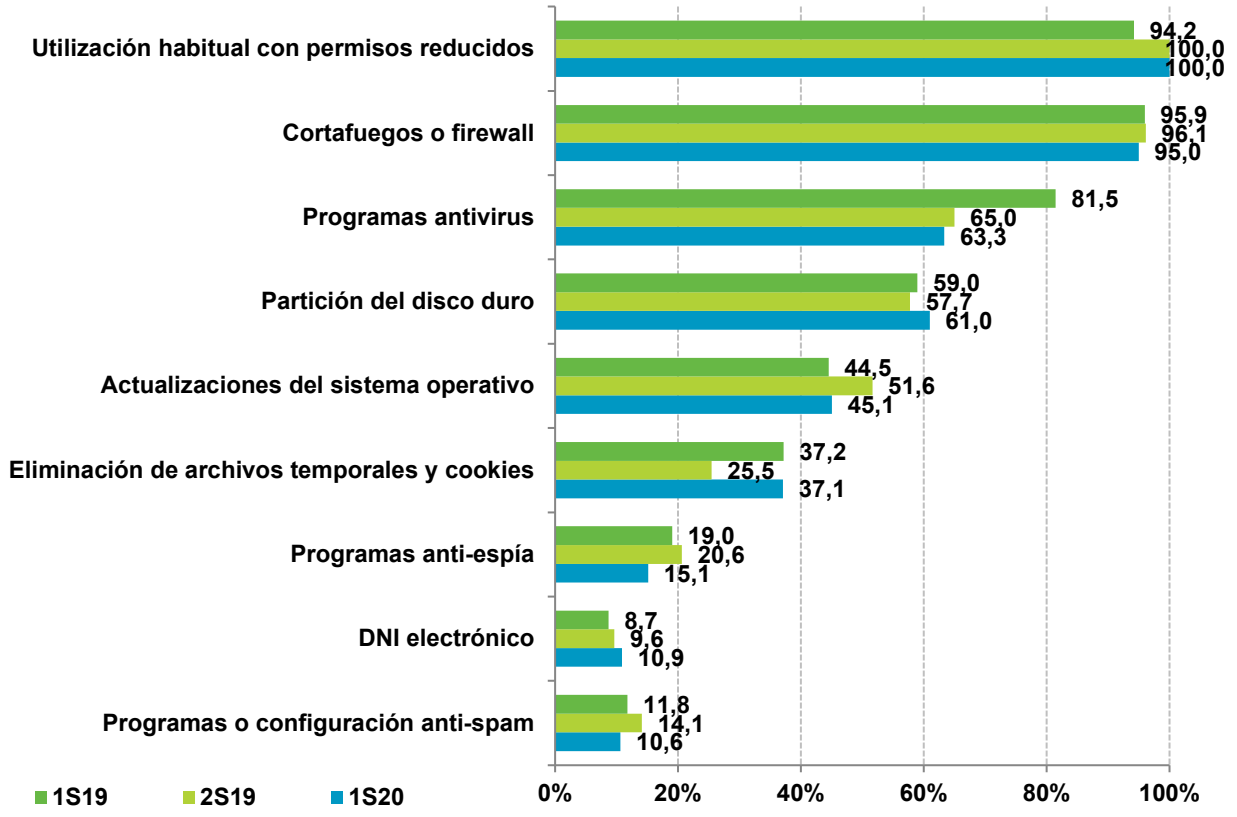
Módulo VIII:

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

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

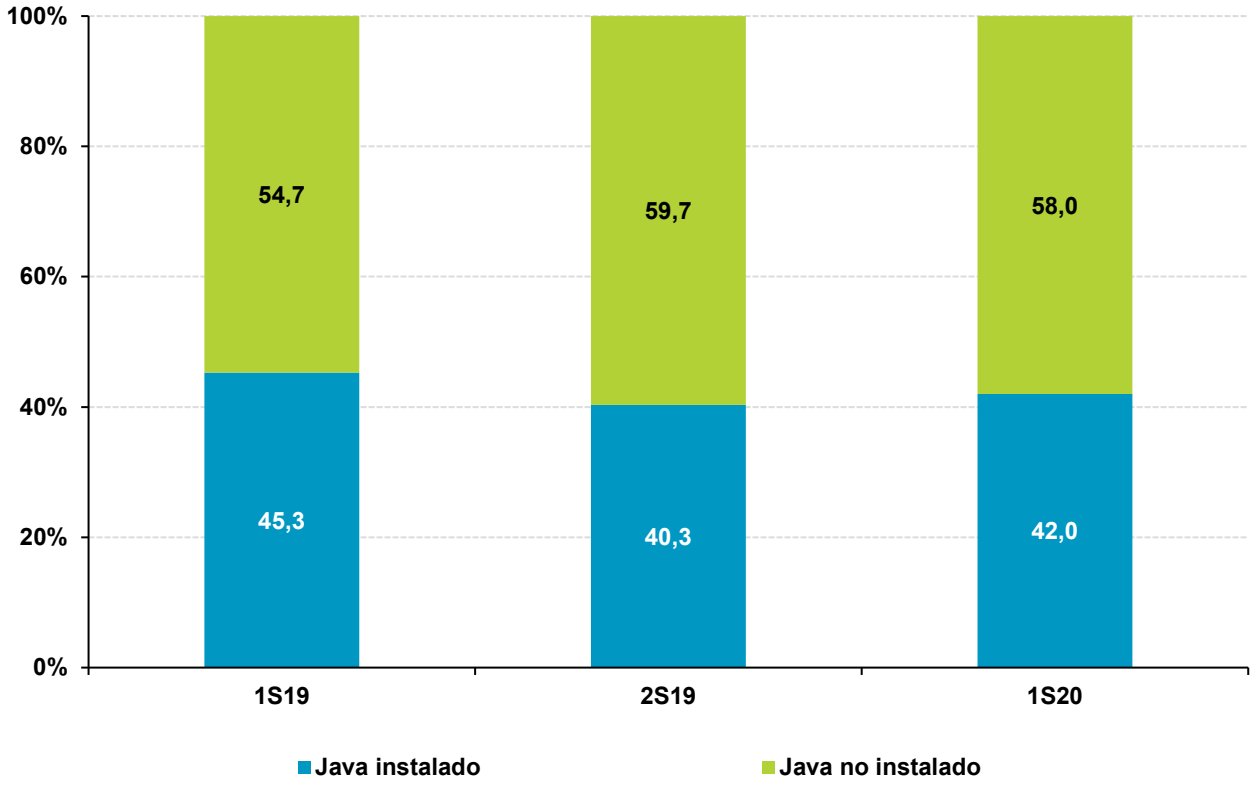


Base: Usuarios de PC

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

Entorno Java en el ordenador del hogar

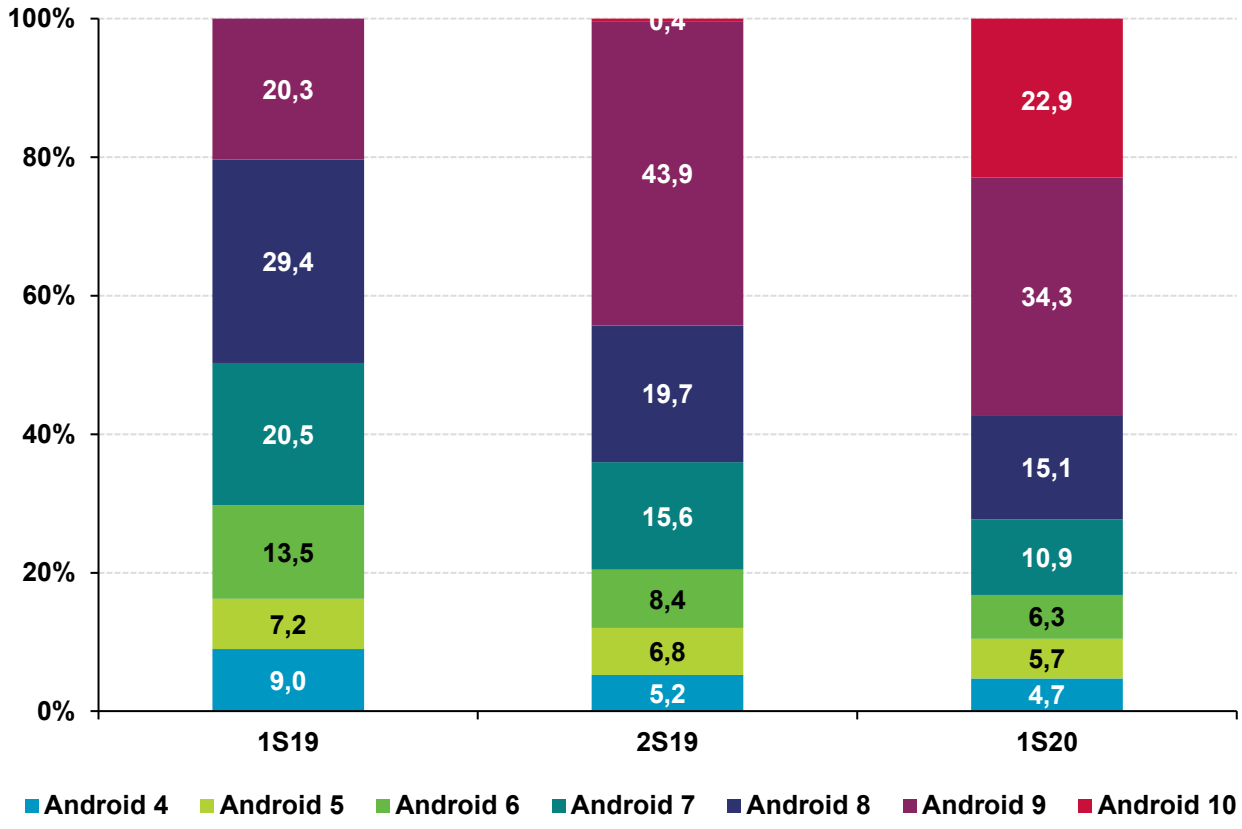
El aprovechamiento y explotación de vulnerabilidades en Java ha sido, a lo largo de los últimos años, uno de los vectores de entrada más utilizados por el malware para infectar equipos con una versión de este software desactualizada.



Base: Usuarios de Microsoft Windows

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

Versiones de Android



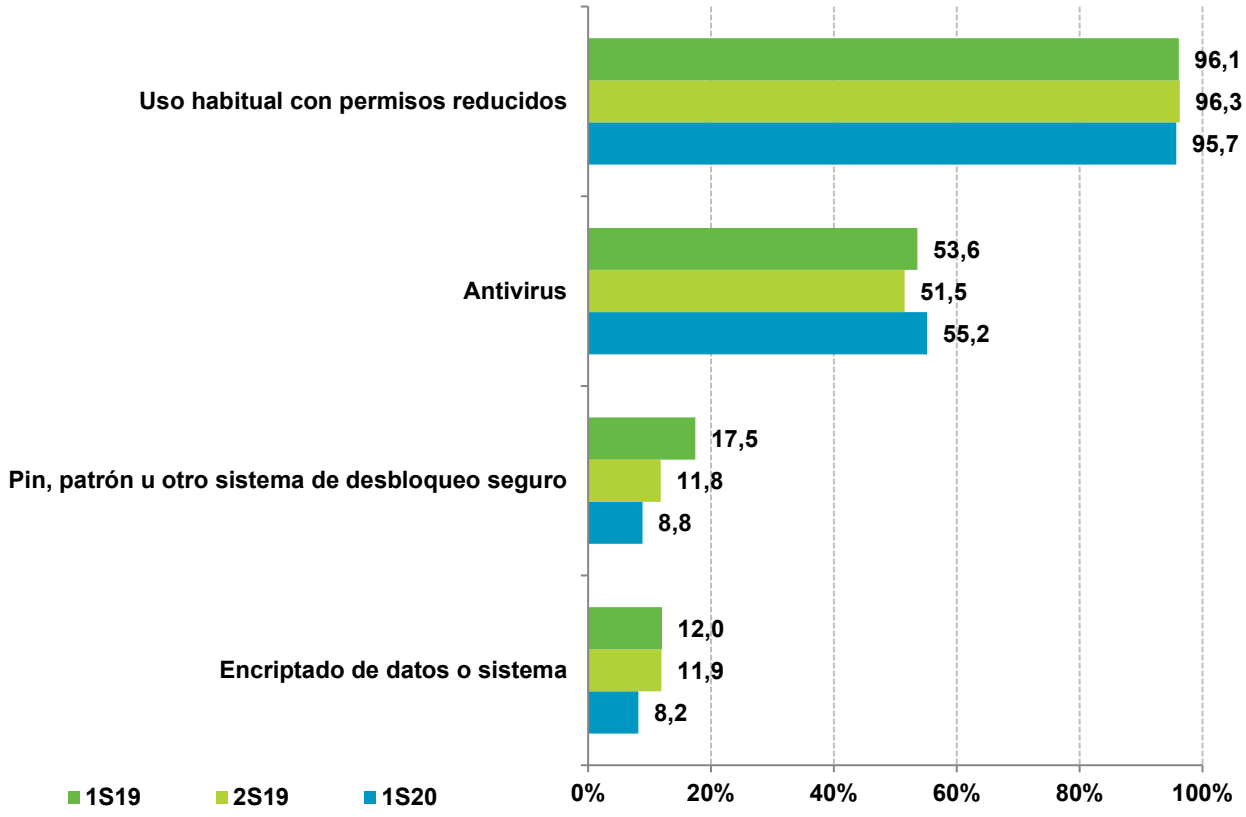
Base: Usuarios de dispositivos Android

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

Uso real de medidas de seguridad en dispositivos Android

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****.*

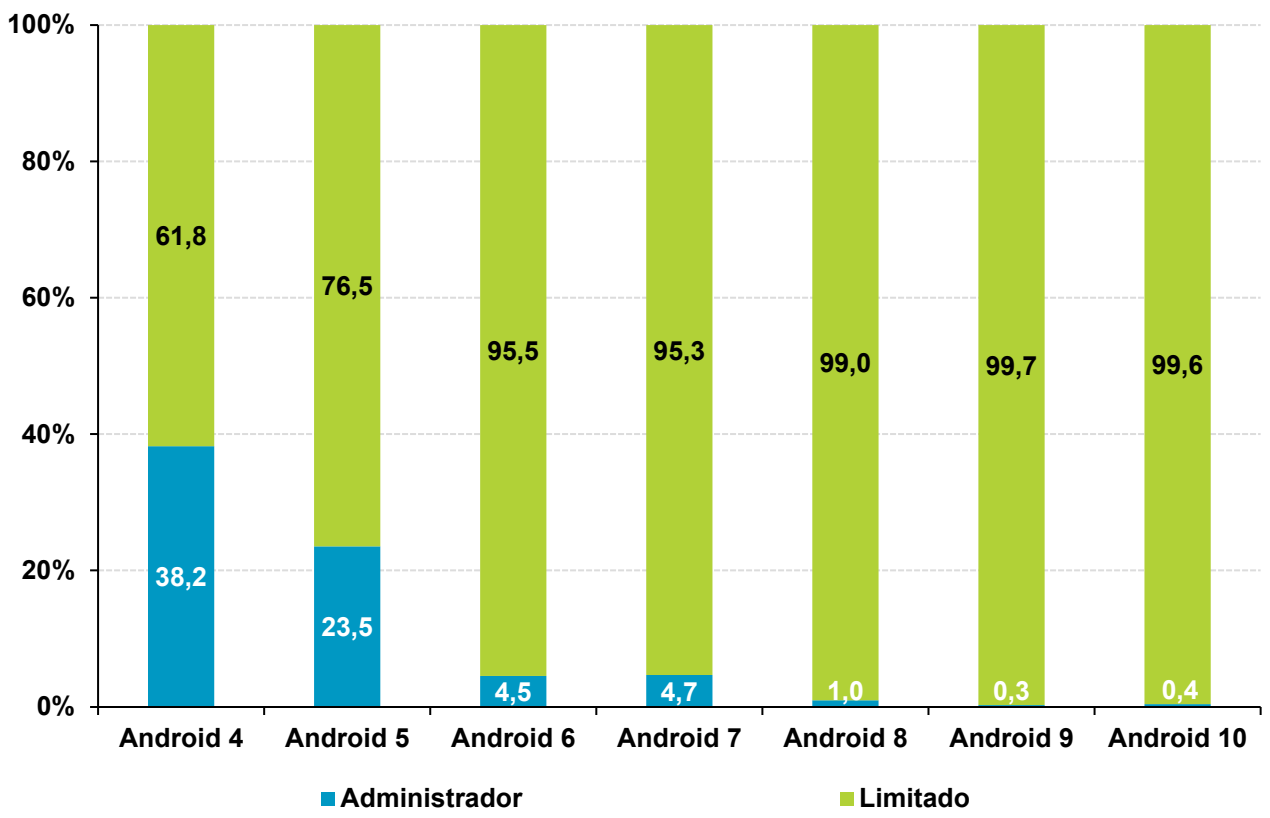
Más información:
https://www.osi.es/es/actualidad/blog/2020/10/23/bloquear-dispositivo-android-ios-biometria



Base: Usuarios de dispositivos Android

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

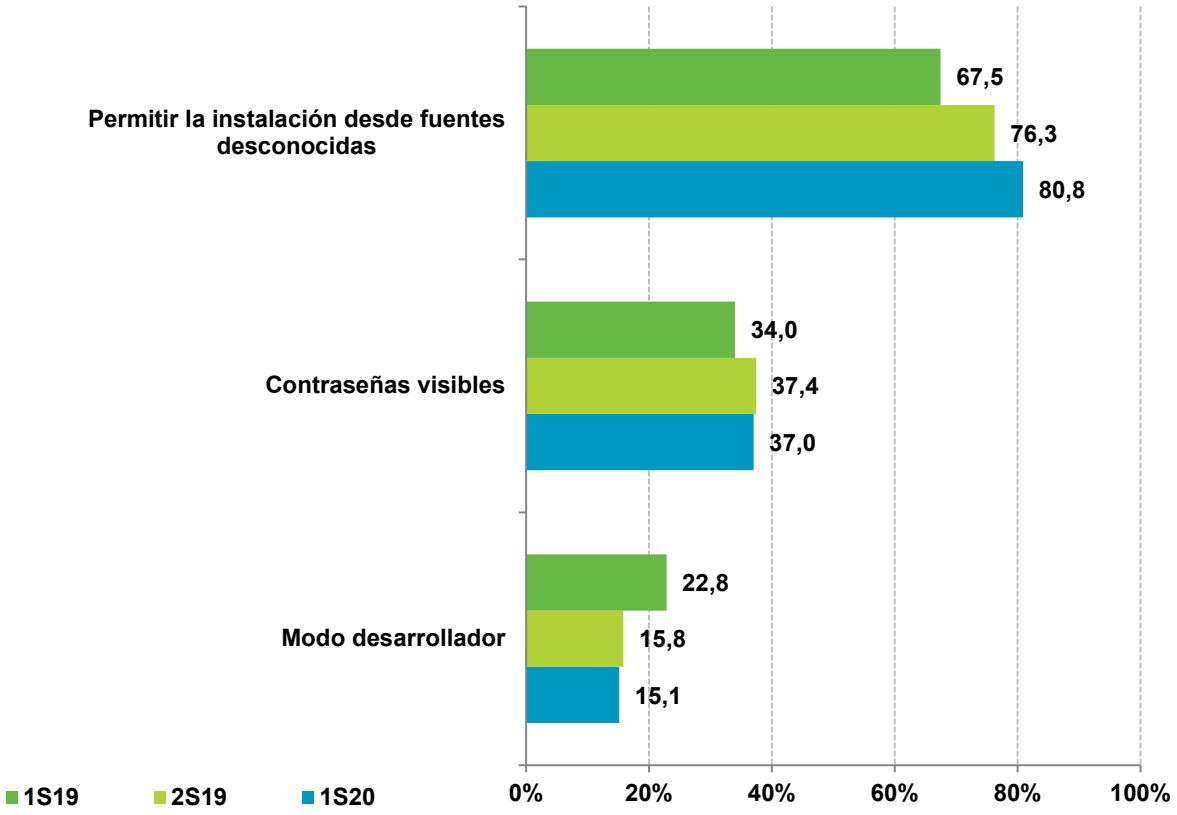
Nivel real de privilegios en los perfiles de usuario de dispositivos Android



Base: Usuarios de dispositivos Android

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

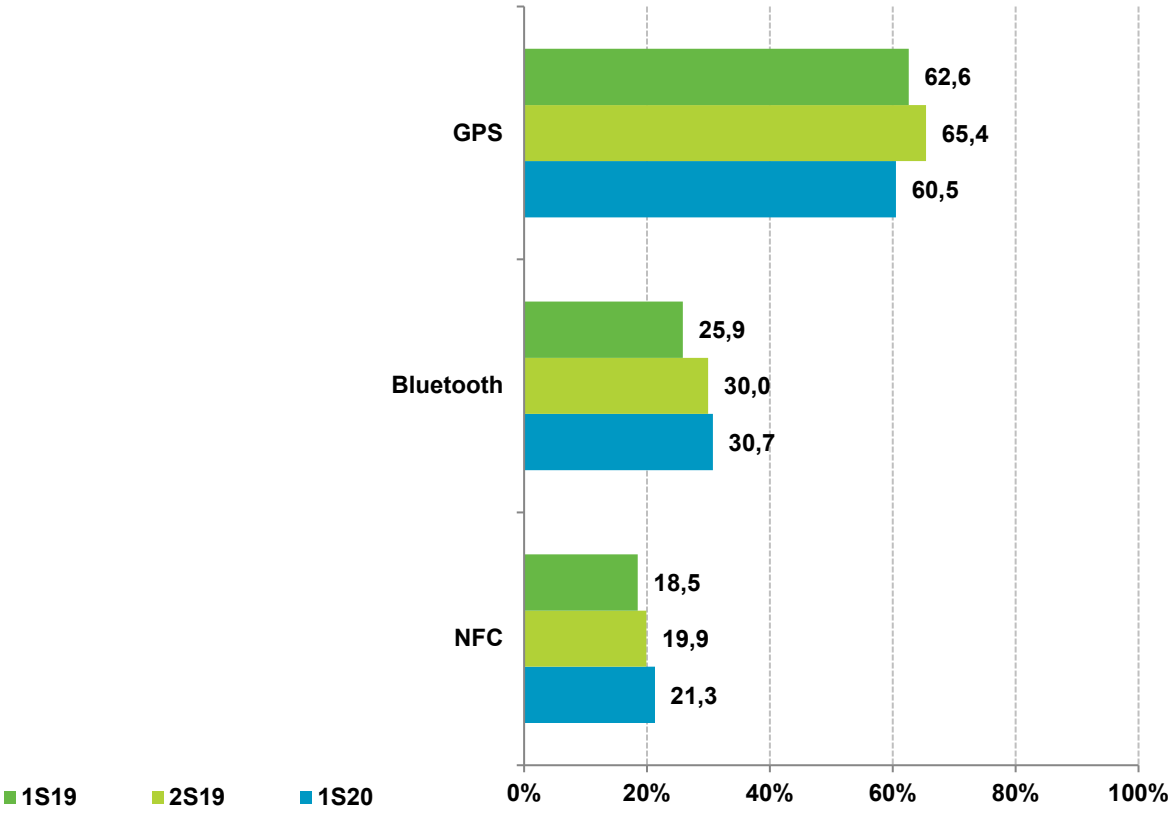
Configuraciones activas en dispositivos Android



Base: Usuarios de dispositivos Android

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

Tecnologías activas en dispositivos Android

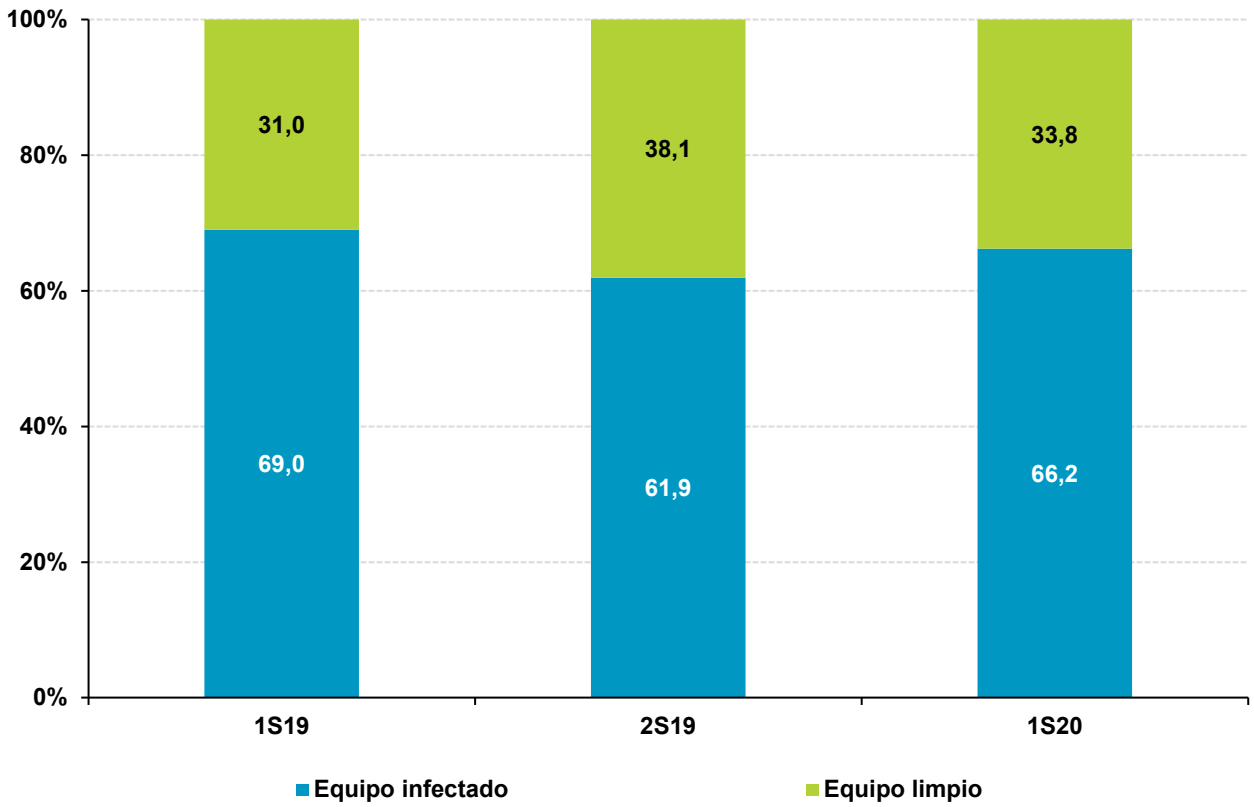


Base: Usuarios de dispositivos Android

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

Estado de infección real del ordenador del hogar

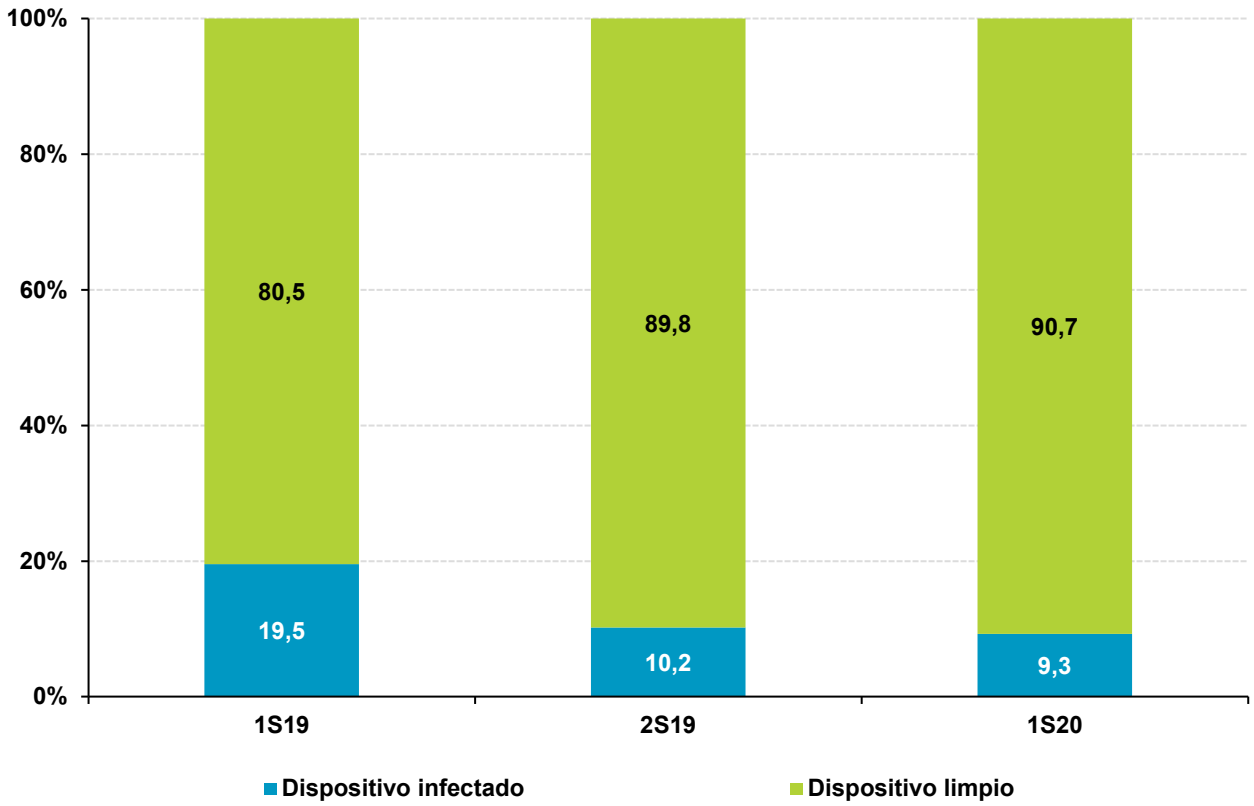
Aprende los pasos que debes dar para la eliminación de los virus de tu equipo: https://www.osi.es/es/desinfecta-tu-ordenador



BASE: Total ordenadores

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

Estado de infección real de los dispositivos Android

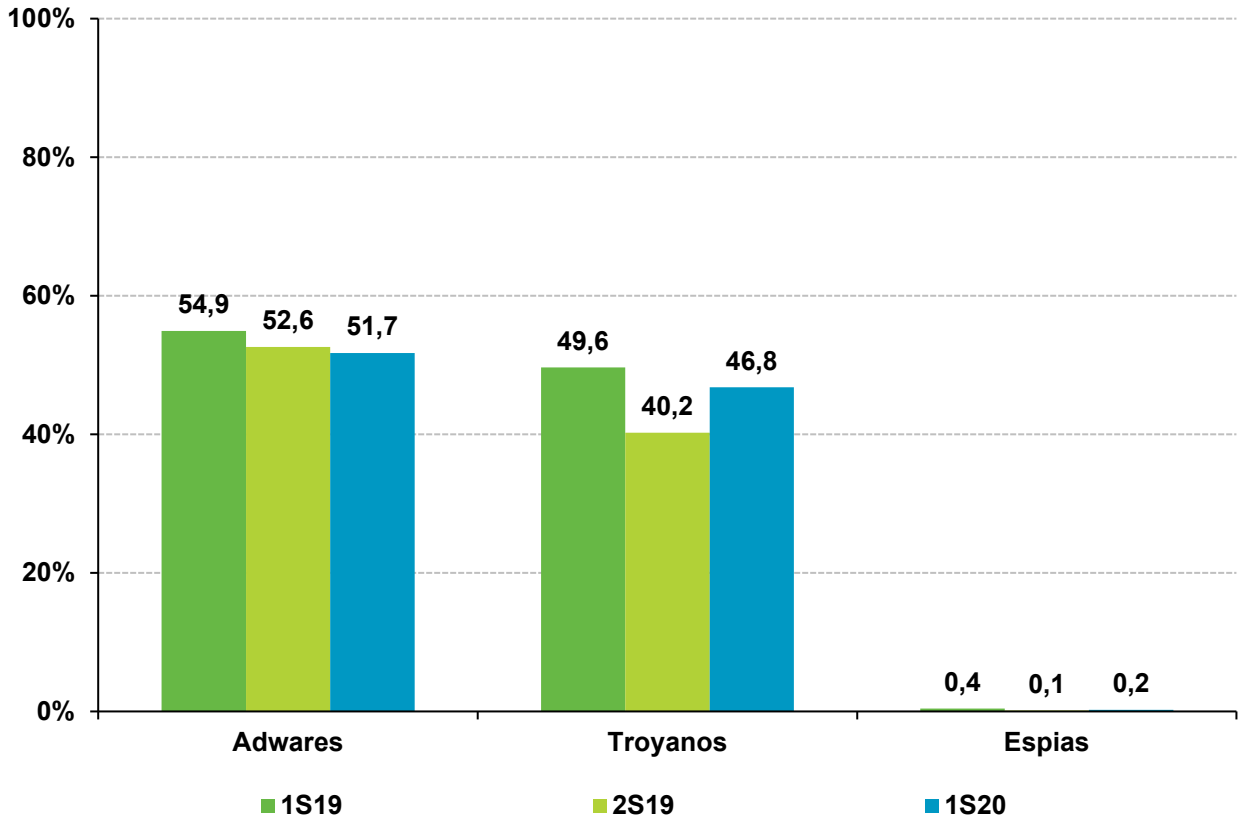


BASE: Total dispositivos Android

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

Tipología del malware detectado en el ordenador del hogar

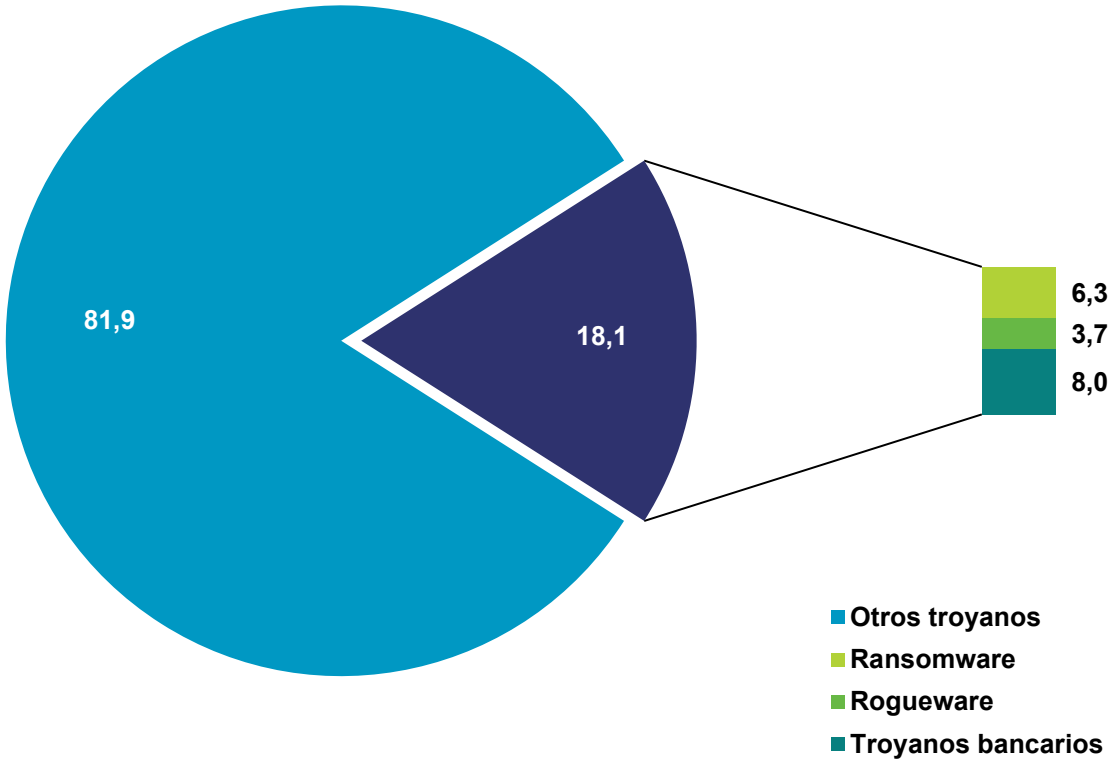
Tipos de malware: *https://www.osi.es/es/actualidad/blog/2020/05/06/principales-tipos-de-virus-y-como-protegernos-frente-ellos*



BASE: Total ordenadores

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

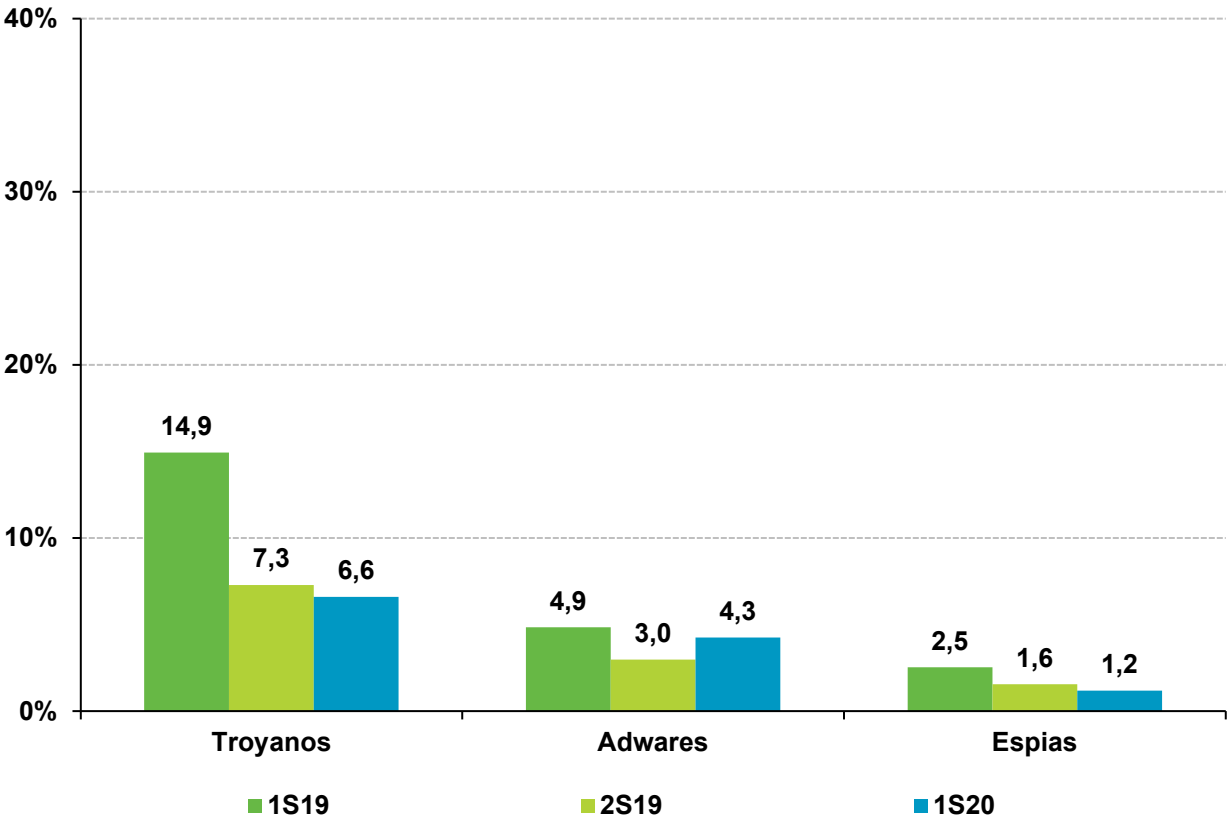
Clasificación de troyanos detectados en el ordenador del hogar



BASE: Total ordenadores con troyanos detectados

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

Tipología del malware detectado en dispositivos Android

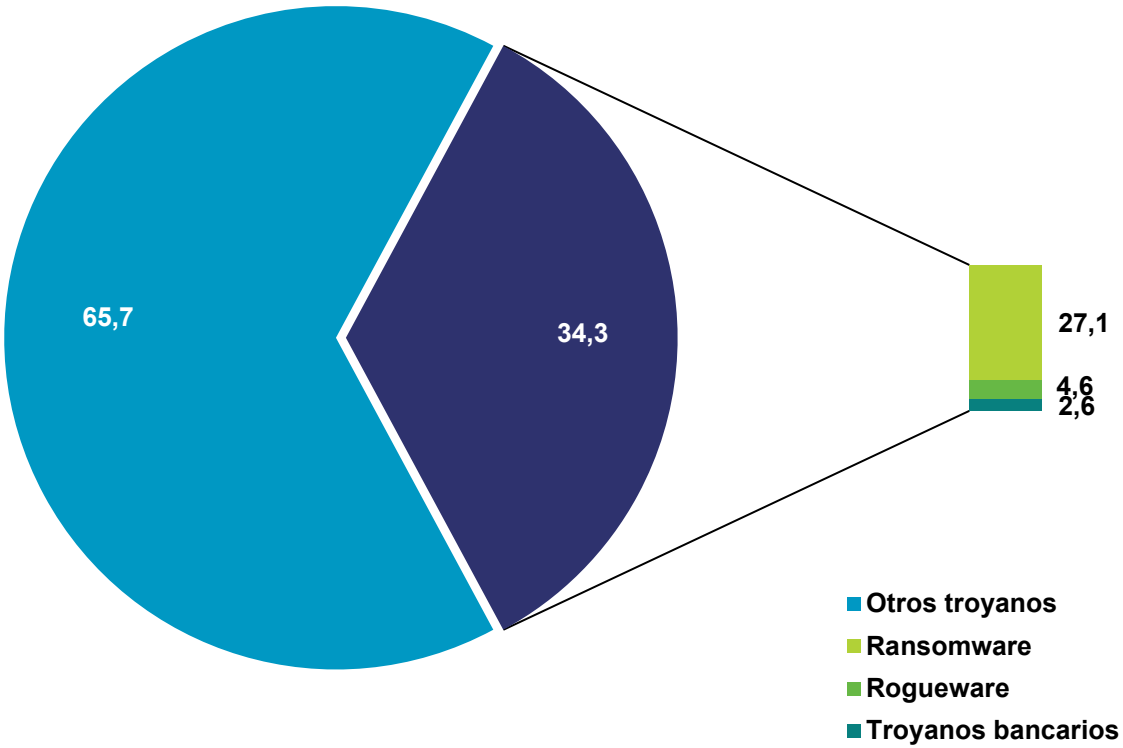


Guía de ciberataques: https://www.osi.es/es/guia-ciberataques

BASE: Total dispositivos Android

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

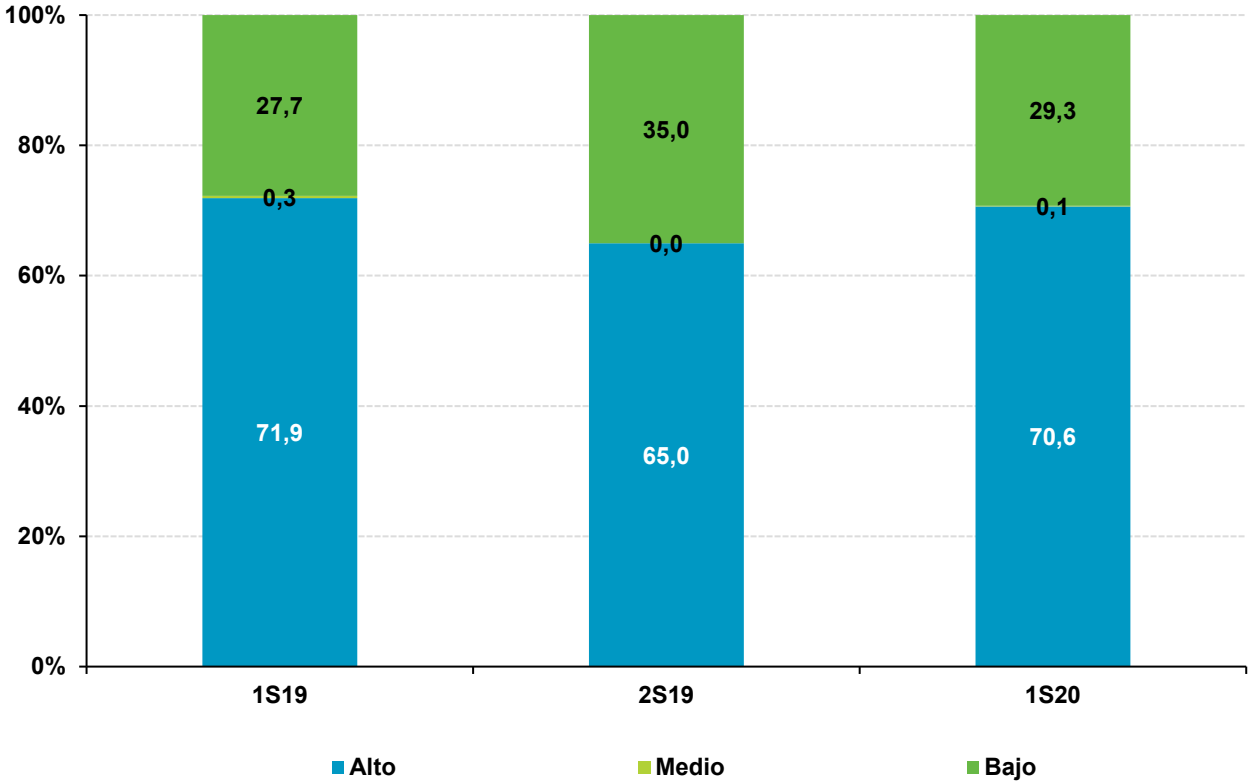
Clasificación de troyanos detectados en dispositivos Android



BASE: Total dispositivos Android con troyanos detectados

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

Peligrosidad del malware detectado y riesgo del ordenador en el ordenador del hogar



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

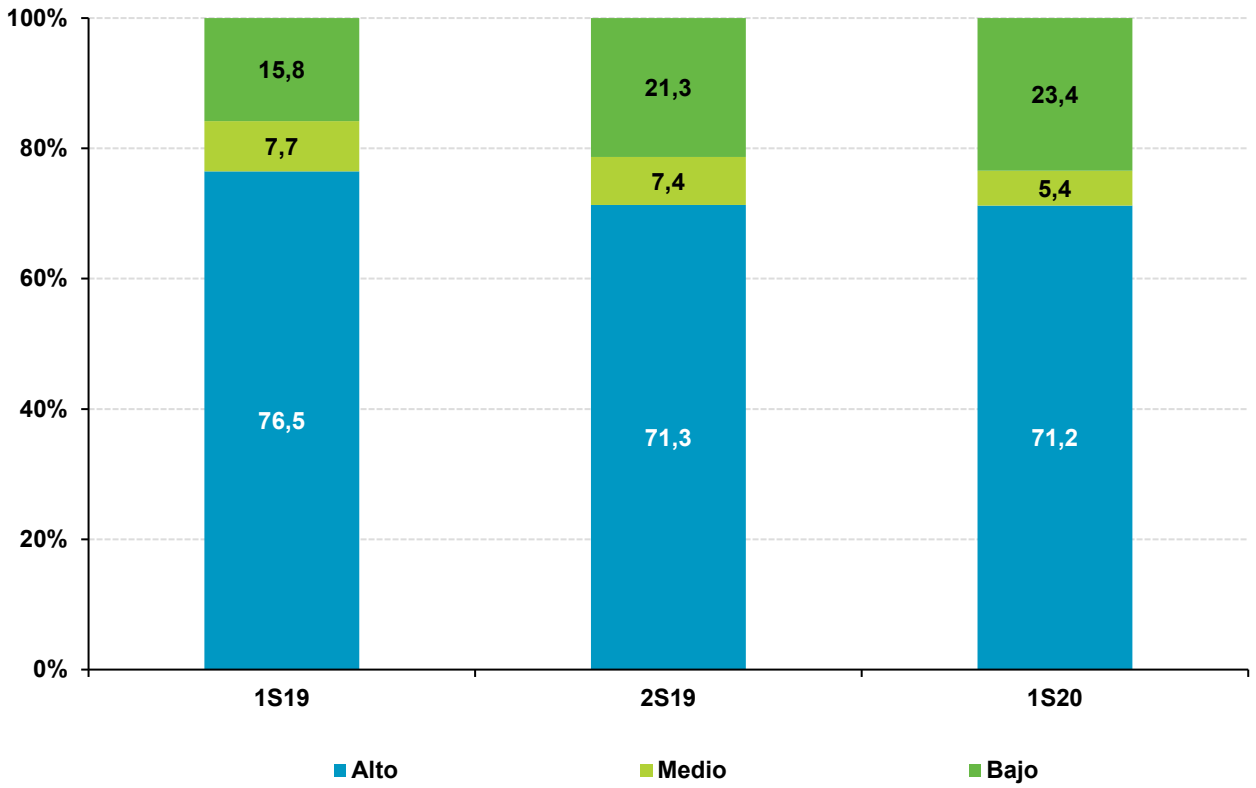
BASE: Total ordenadores infectados

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

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

Peligrosidad del malware detectado y riesgo de los dispositivos Android

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

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

Alcance del estudio

Alcance del estudio

El *"Estudio sobre la Ciberseguridad y Confianza de los hogares españoles"* 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: 3.659 hogares encuestados y equipos/dispositivos Android escaneados (software instalado en 789 PCs y 2.256 smartphones y 614 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 enero y junio de 2020 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 95,0%, se establece que al tamaño muestral n=3.659 le corresponde una estimación del error muestral igual a ±1,61%.

El informe del *"Estudio sobre la Ciberseguridad y Confianza de los hogares españoles"* ha sido elaborado por el siguiente equipo de trabajo del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es:

Dirección: Alberto Urueña López
Equipo técnico:
Raquel Castro García-Muñoz
Santiago Cadenas Villaverde
Jose Antonio Seco Arnegas

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-2020-1
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