Estudio sobre la ciberseguridad y confianza del ciudadano en la RED

NOVIEMBRE 2020

Oleada enero - junio 20

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

1 CONTEXTO DEL ESTUDIO

2 USOS DE INTERNET

3 MEDIDAS DE SEGURIDAD

4 HÁBITOS DE COMPORTAMIENTO EN LA NAVEGACIÓN Y USOS DE INTERNET

5 INCIDENTES DE SEGURIDAD

6 CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD Y REACCIÓN DE LOS USUARIOS

7 CONFIANZA EN EL ÁMBITO DIGITAL EN LOS HOGARES ESPAÑOLES

8 CONCLUSIONES

ESTUDIO SOBRE LA CIBERSEGURIDAD Y CONFIANZA DEL CIUDADANO EN LA RED

Red.es en colaboración con Hispasec Sistemas y GFK realiza semestralmente un estudio para analizar la adopción de medidas de seguridad y evaluar las incidencias de situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que los hogares españoles depositan en el uso de las nuevas tecnologías de la información. Este resumen ejecutivo corresponde al estudio realizado en el primer semestre de 2020.

El objetivo de este estudio es el análisis del estado de los hogares españoles a través de indicadores de seguridad basados en la percepción de los usuarios sobre la misma, así como el nivel de confianza de estos respecto a la seguridad y su evolución, haciendo un contraste comparativo con el nivel real de seguridad que mantienen tanto los equipos informáticos como los dispositivos Android.

Se pretende impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe tiene como finalidad, entre otras, informar del comportamiento y utilización segura y privada de las nuevas tecnologías, además de servir como apoyo para solucionar incidencias por parte de los usuarios y la adopción de medidas por parte de la Administración.

El estudio se realiza a través de dos vías: el análisis de seguridad real de los equipos informáticos y dispositivos Android, mediante el escaneo con la herramienta Pinkerton y el análisis de las declaraciones aportadas por los internautas encuestados.

Los datos declarados son obtenidos de las encuestas online realizadas a los hogares que han conformado la muestra del estudio, mientras que para los datos reales se utiliza el software Pinkerton. Este software analiza los sistemas de PC's y dispositivos Android recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas, a la vez que detecta la presencia de *malware* en los equipos y dispositivos móviles gracias a la utilización conjunta de más de 50 motores antivirus.

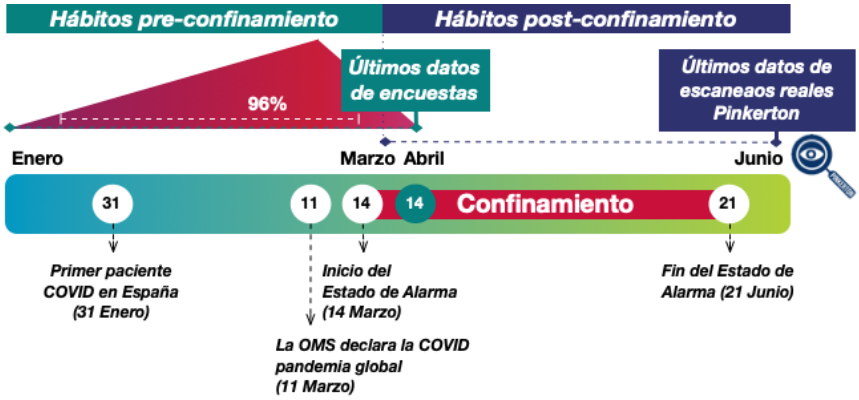
1 Contexto del estudio

Para realizar la interpretación de los datos analizados en este estudio debe tenerse en cuenta el contexto en el que éstos fueron recabados. La situación histórica en la que todo el conjunto de la población se ha visto envuelta debido a la alarma y posterior confinamiento debido a la pandemia mundial provocada por el Coronavirus SARS-CoV-2, en adelante COVID-19[1], ha condicionado el análisis e interpretación de los datos.

[1] COVID-19 es el nombre dado a la enfermedad que causa el virus conocido como Coronavirus SARS-CoV-2.

En concreto, en torno al 96% de las encuestas realizadas a los usuarios sobre sus hábitos corresponden al primer trimestre del año, antes de que se proclamase el Estado de Alarma, mientras que los datos recabados de los dispositivos más recientes corresponden al segundo trimestre, entre el 1 de Abril y el 31 de Junio, por lo que contaríamos con datos reales sobre los cambios realizados en los equipos por parte de los usuarios durante el confinamiento.

FIGURA 1. LINEA DE TIEMPO REPRESENTATIVA DEL CONTEXTO DEL SEMESTRE



Por lo tanto, esta nueva oleada es de gran interés, dado que se analizan datos de la percepción de la seguridad de los usuarios justo antes del confinamiento, cuando la amenaza de la COVID-19 comenzaba a materializarse y los datos de los dispositivos de los usuarios durante el confinamiento. Es por ello que este informe es el primero que mostrará la influencia real del confinamiento y el teletrabajo en la ciberseguridad y confianza de los hogares españoles.

2 Usos de Internet

Es primordial conocer cuáles son los servicios más demandados por los usuarios en Internet, puesto que en estos mismos servicios se centrarán la mayor parte de los vectores de ataque de los ciberdelincuentes.

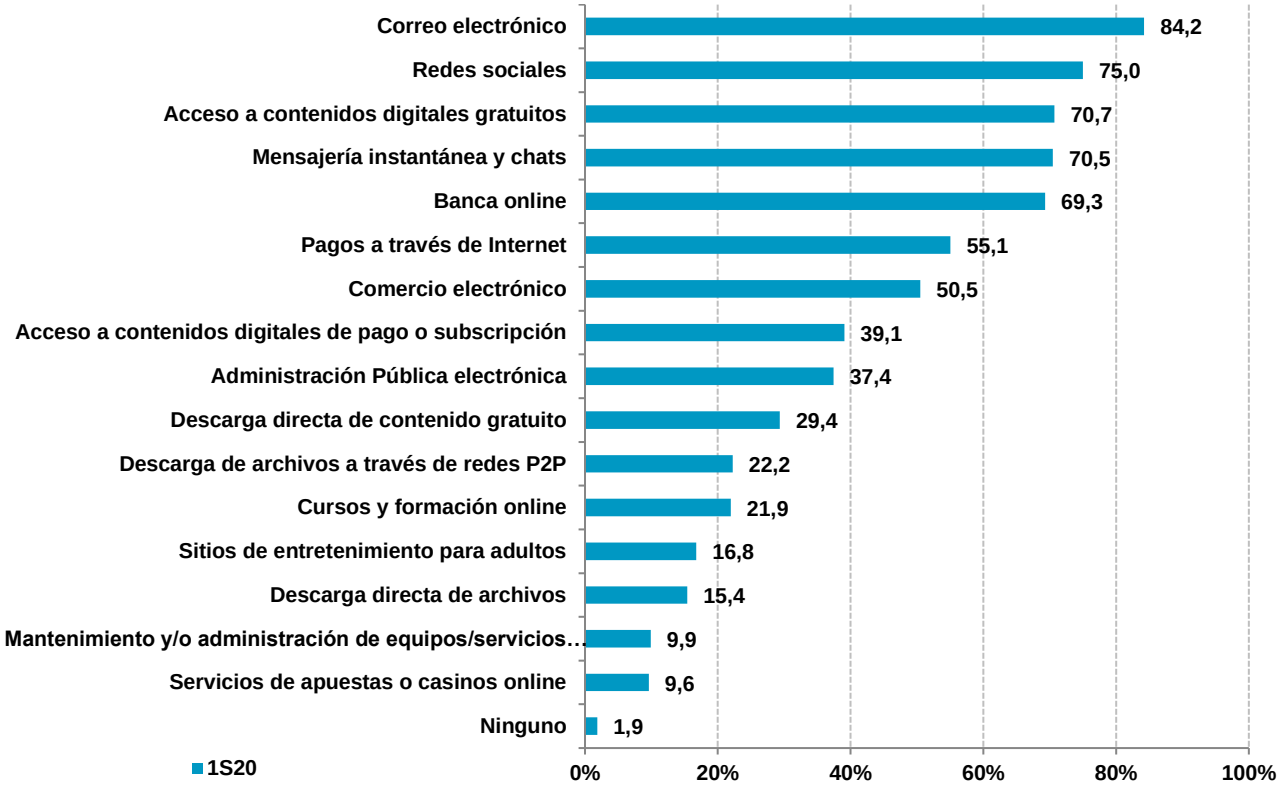
A este respecto, el siguiente gráfico muestra el uso de servicios declarado por los usuarios justo antes de decretarse el Estado de Alarma, pero con la amenaza del mismo ya presente.

Se ha detectado un aumento significativo, de hasta 15 p.p., en el uso de herramientas de comunicación, socialización y ocio, aún antes de decretarse el Estado de Alarma[2]. El correo electrónico (84,2%), las redes sociales (75,0%), la mensajería instantánea (70,5%) y la banca online (69,3%) han sido los servicios más utilizados por los usuarios. Aunque en la actualidad, el mayor consumo de contenido digital de ocio procede principalmente de plataformas gratuitas (70,7%), como por ejemplo el caso de la plataforma *YouTube*, que vio crecer sus visitas en torno al 55%

[2] https://iabspain.es/estudio/informe-de-nielsen-espana-digital-consumer-24-hours-indoors-covid19/

respecto a meses anteriores[3]; el consumo de plataformas digitales de pago como Netflix, HBO, Prime Video o Disney+ son empleados por el 39,1% de los encuestados y han visto un incremento en el número de suscriptores muy superior al esperado inicialmente antes de conocerse la pandemia[4]. Por ejemplo, en el caso de Netflix[5] se registró un incremento de casi el doble de suscriptores y vieron crecer su tráfico un 210% de media[6]. Incluso fue necesaria la intervención de la Administración para solicitar la reducción del ancho de banda consumido por estas plataformas consideradas como no imprescindibles para evitar el colapso de la red[7]. Los cibercriminales han aprovechado esta situación para incrementar el uso de los *kits* de *phishing* y fraude asociados a este tipo de servicios durante el confinamiento.

FIGURA 2. USO DECLARADO DE SERVICIOS DE INTERNET (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

[3] https://www.europapress.es/portaltic/internet/noticia-consumo-video-youtube-aumenta-55-confinamiento-espana-20200408121152.html

[4] https://www.elespanol.com/invertia/medios/20200306/netflix-amazon-hbo-cadenas-hacen-fuertes-coronavirus/472453569_0.html

[5] https://www.eluniverso.com/entretenimiento/2020/04/21/nota/7819755/netflix-aumento-158-millones-clientes-primer-trimestre-ano

[6] https://www.businessinsider.es/coronavirus-hbo-vs-netflix-vs-disney-ven-espanoles-619557

[7] https://elpais.com/sociedad/2020-03-18/bruselas-pide-a-netflix-que-limite-su-servicio-para-evitar-el-colapso-de-internet.html

Los pagos a través de Internet o el comercio electrónico se sitúan en una posición reseñable, ya que al menos 1 de cada 2 encuestados hace uso de ellos. En concreto, en la segunda semana del confinamiento se vieron incrementados hasta 73,7 p.p. respecto a la misma semana del 2019[8].

Otro servicio que ha obtenido un gran protagonismo ha sido el acceso a la Administración Pública de forma electrónica (37,4%), que ha visto incrementado su uso de forma telemática. Este incremento supone una buena noticia dado que refleja que un porcentaje significativo de la población ya estaba adaptándose al uso de medios telemáticos antes de que fuesen obligatorios por el confinamiento.

USO DECLARADO DE SERVICIOS ANTES DEL CONFINAMIENTO

84,2%
CORREO ELECTRÓNICO

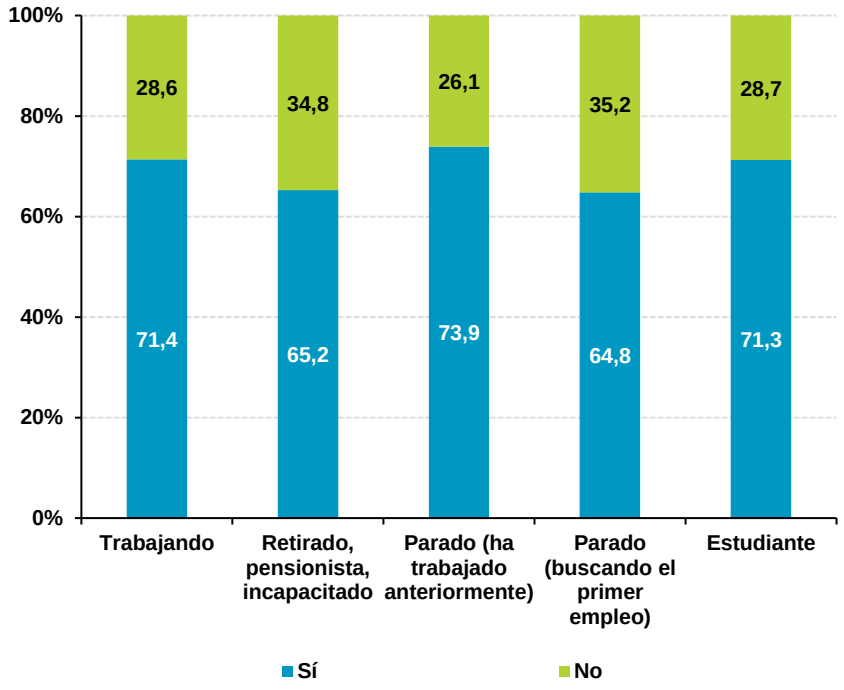
75%
USO DE REDES SOCIALES

70,5%
MENSAJERÍA INSTANTÁNEA Y CHAT

37,4%
REALIZAN TRÁMITES TELEMÁTICOS CON LA ADMINISTRACIÓN

El uso de mensajería instantánea continúa siendo muy habitual entre los encuestados, independientemente de su situación laboral (entre un 64,8% y un 73,9%), siendo uno de los medios de comunicación oficial más común en la actualidad. De hecho, las campañas de *phishing* también están adaptándose para aprovechar esta tendencia. En el contexto de los mensajes de texto (SMS) y mensajería instantánea, el *phishing* recibe el nombre de *smishing*.

FIGURA 3. USO DE MENSAJERÍA INSTANTÁNEA Y CHAT SEGÚN LA ACTIVIDAD REALIZADA POR LOS USUARIOS (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

Por lo tanto, cabe destacar que ya sea por medio del correo electrónico (84,2%) o por vía de la mensajería instantánea (70,5%) hay un alto porcentaje de usuarios expuestos a dicho tipo de engaño.

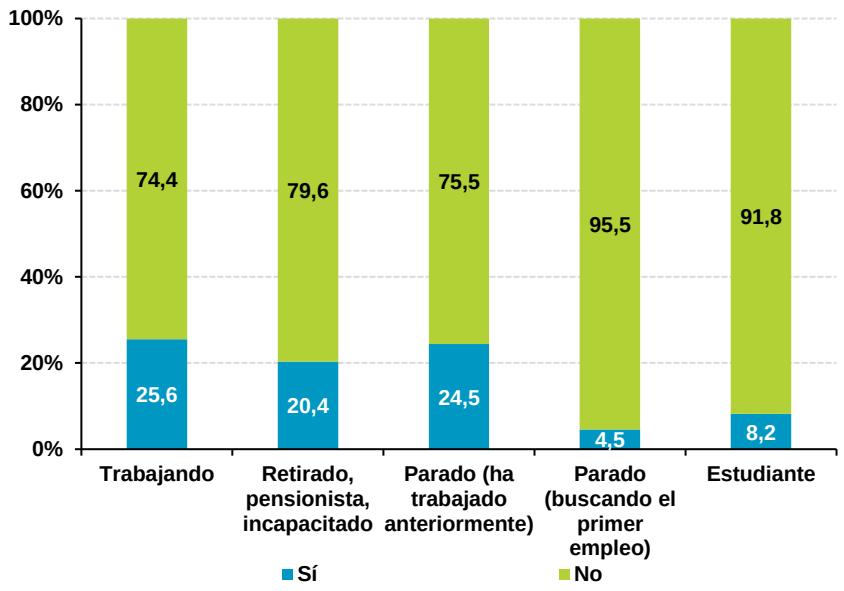
[8] https://iabspain.es/estudio/informe-de-nielsen-espana-digital-consumer-24-hours-indoors-covid19/

Otro factor que podría pasar desapercibido pero que es fundamental en este contexto es el uso de redes sociales declarado antes del confinamiento.

En concreto, un 70,5% de los panelistas usan redes sociales, y esto implica exposición a posibles campañas de desinformación. Este será otro punto clave a tratar en posteriores estudios post-confinamiento.

También se ha observado que prácticamente uno de cada cuatro encuestados que está trabajando o en búsqueda de un nuevo empleo opta por la formación en línea, a diferencia de los estudiantes o aquellos desempleados que están buscando su primer empleo (8,2% y 4,5% respectivamente).

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



Base: Total usuarios
Fuente: Panel hogares, ONTSI

Resulta interesante conocer la predisposición de los usuarios a la realización de cursos online puesto que a través de ellos es posible ampliar o profundizar sobre el conocimiento de herramientas de seguridad, establecer hábitos prudentes, concienciar de los potenciales riesgos de la Red y aprender a protegerse de ellos o cómo actuar en caso de sufrir una incidencia de este tipo, etc.

3 Medidas de seguridad

El aumento del teletrabajo a causa de la pandemia pone de manifiesto la gran importancia de emplear medidas de seguridad de forma adecuada, puesto que un mal uso de las mismas podría poner en riesgo tanto al usuario como a la propia empresa.

La interacción entre usuario y dispositivo es una de las fases más delicadas de la seguridad de la información. En la actualidad, las personas usuarias disponen de muchas herramientas para controlar y proteger sus dispositivos móviles, ordenadores y otros equipos de incidencias de seguridad y ataques de terceros.

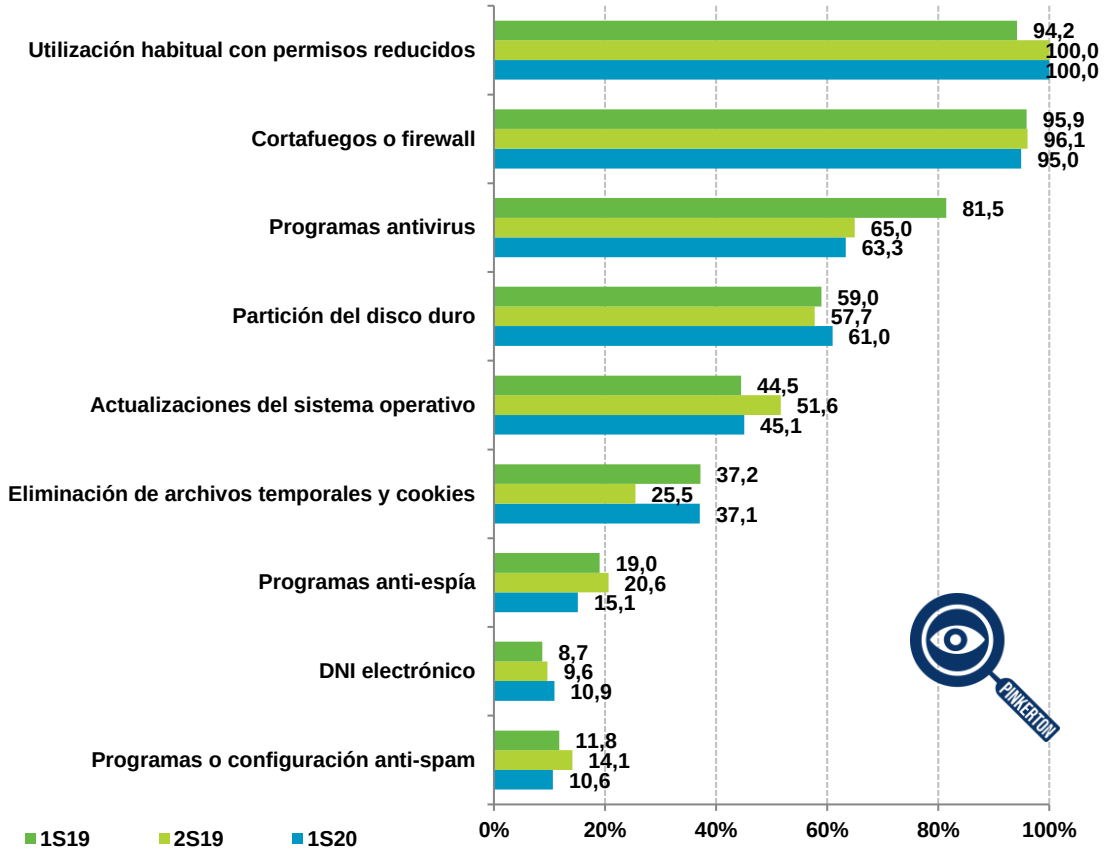
En este apartado se analizan las medidas de seguridad utilizadas por los panelistas españoles durante el primer semestre de 2020.

Los datos que se muestran a continuación se han obtenido a partir de las declaraciones de aquellas personas de nacionalidad española que han participado en las encuestas y de la información recopilada mediante el análisis real de sus sistemas (ordenadores del hogar y dispositivos móviles) realizado por la herramienta Pinkerton.

3.1 Ordenadores del hogar

Las principales medidas de seguridad usadas por los panelistas en el ordenador del hogar se mantienen respecto al segundo semestre de 2019. Estas medidas son: la utilización habitual con permisos reducidos, utilizada por la totalidad de los usuarios y el uso de cortafuegos o firewall (95%).

FIGURA 5. USO REAL DE MEDIDAS DE SEGURIDAD EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

No es de extrañar que el uso del ordenador del hogar se haga con permisos reducidos, ya que el principal sistema operativo utilizado por los usuarios –y con una cuota de mercado mundial del 58,9%– es Windows 10[9].

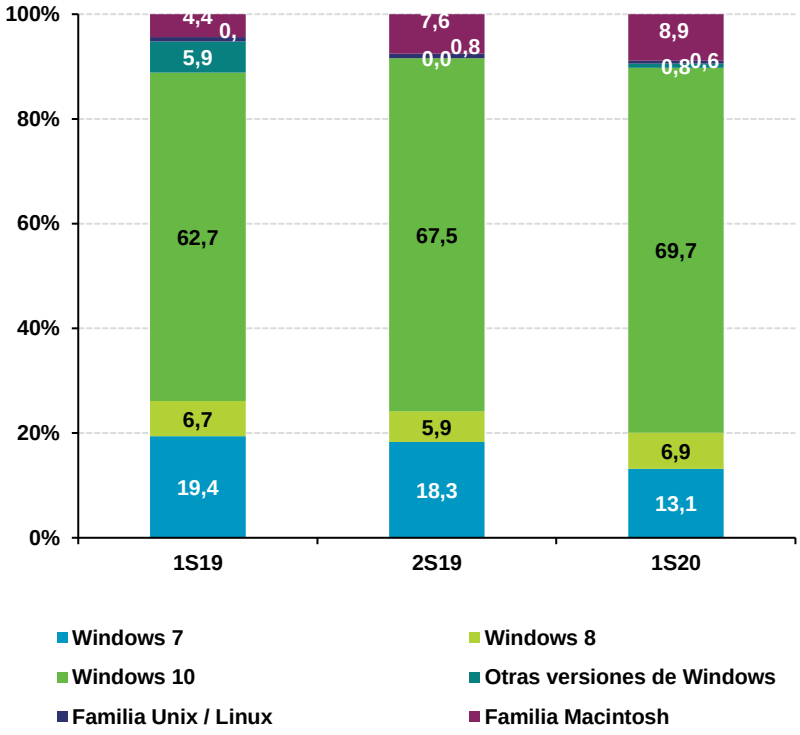
[9] https://netmarketshare.com/operating-system-market-share.aspx?

En concreto, como muestra la figura siguiente, más del 69% de los panelistas declara Windows 10. En dicho sistema operativo se aplican por defecto las cuentas de usuario con permisos reducidos. De este modo, cuando una acción requiere un mayor nivel de privilegios, el sistema solicita las credenciales para elevar los mismos de manera puntual.

La finalización del servicio de soporte para Windows 7, uno de los sistemas operativos más emblemáticos de Microsoft el pasado 14 de enero, hará incrementar aún más si cabe la cuota de mercado de Windows 10. De hecho, es interesante remarcar que, pese a que Microsoft anunció que la actualización a Windows 10 era gratuita antes del Estado de Alarma, los datos no reflejan una variación de sistema operativo más significativa.

Por lo tanto estos resultados también podrían indicar la necesidad de mejorar las campañas de información para que los usuarios actualicen sus equipos domésticos.

FIGURA 6. SISTEMAS OPERATIVOS DECLARADOS EN LOS ORDENADORES DEL HOGAR (%)



Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

Otro dato significativo corresponde al particionado del disco duro, que sube 3,3 p.p. respecto a la anterior oleada. Este dato va en concordancia con la cuota de mercado que ocupa Windows 10 mencionada antes, puesto que dicho sistema operativo particiona por defecto el disco duro en su instalación.

La medida de seguridad que acusa un mayor descenso, es la actualización del sistema operativo, con 6,5 p.p. menos respecto al segundo periodo de 2019.

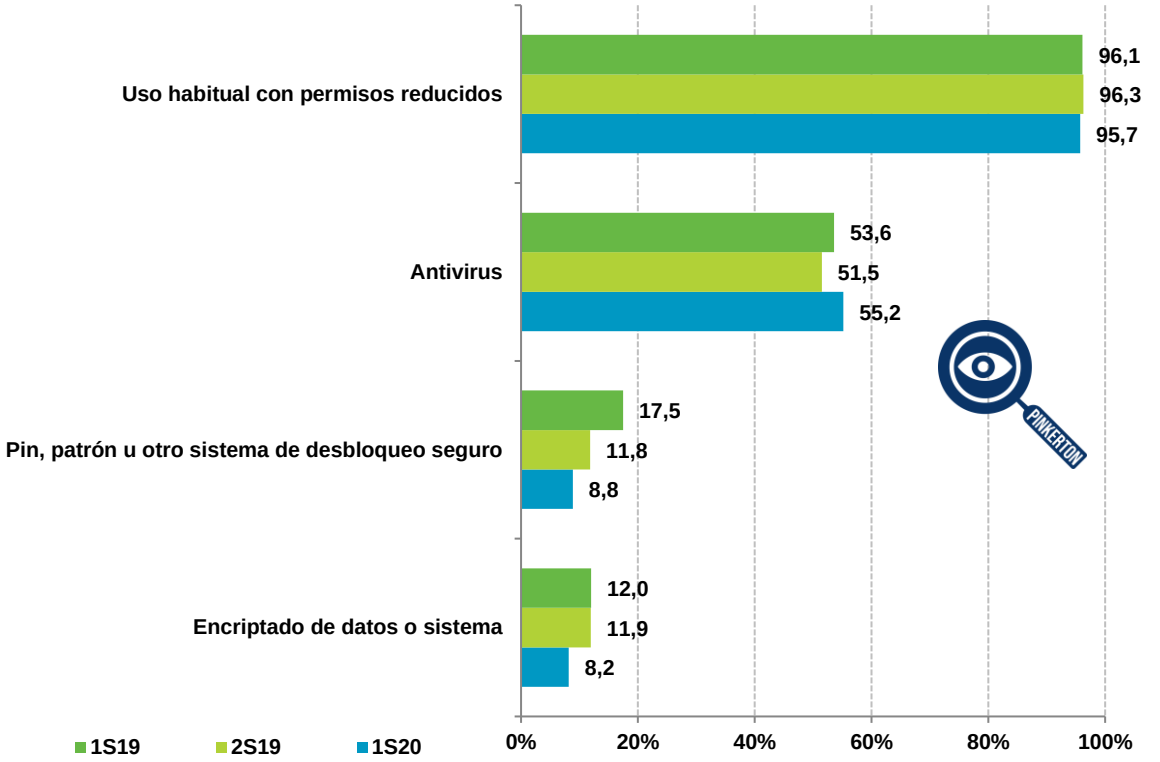
A consecuencia del coronavirus, el pasado 24 de marzo Microsoft anunciaba la paralización de las actualizaciones opcionales para Windows 10 y Windows Server con el fin de evitar cualquier potencial problema en los ordenadores de las personas que se encontrasen teletrabajando a raíz de ellas[10]. Sin embargo, las actualizaciones de seguridad sí han continuado liberándose a lo largo de todo el periodo de aislamiento social ya que su objetivo es el de proteger los equipos solucionando problemas de seguridad detectados o conocidos que los ciberdelincuentes podrían aprovechar.

Finalmente, el uso del DNI electrónico sigue creciendo a un ritmo constante desde principios de 2019, con una subida de 1 p.p. de media por semestre. El teletrabajo y el cierre de las Administraciones Públicas de cara al público, han incentivado su uso entre la población.

3.2 *Dispositivos Android*

Para esta parte del análisis se consideran cuatro bloques principales, concernientes a los permisos reducidos, el uso de antivirus, la utilización de contraseñas o sistemas de desbloqueo seguro y el encriptado de datos o sistema.

FIGURA 7. USO REAL DE MEDIDAS DE SEGURIDAD EN DISPOSITIVOS ANDROID (%)



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

En base a los resultados obtenidos, el uso del terminal móvil con permisos reducidos (no *root*), es la principal medida de seguridad que se observa en los dispositivos Android (95,7%).

[10] https://docs.microsoft.com/en-us/windows/release-information/windows-message-center

La

FIGURA 8, en la que se entrará en detalle más adelante, ofrece un desglose de esta medida observada en las diferentes versiones de Android. Se trata de una medida de seguridad pasiva, ya que es una característica establecida por defecto en casi la totalidad de estos dispositivos.

Si un *malware* infectase un móvil que contase con privilegios elevados (*root)*, este podría hacerse con el control total del terminal. Es por ello que resulta totalmente desaconsejable la elevación de privilegios de manera permanente en los dispositivos móviles.

La instalación de antivirus es la principal medida de seguridad activa que se encuentra en los terminales móviles. Esta medida ha visto incrementar su uso ligeramente respecto al anterior semestre (+3,7 p.p.) situándose en un 55,2%, cada vez más cerca del uso de programas antivirus en el ordenador del hogar con un 63,3% (**FIGURA 5**).

En ello se puede encontrar una connotación negativa debido al hecho de que no se debe únicamente a un aumento del uso en dispositivos móviles sino a la pronunciada tendencia decreciente que ha venido siguiendo el uso del software antivirus entre los usuarios de ordenador desde la segunda mitad de 2018.

USO HABITUAL CON PRIVILEGIOS REDUCIDOS EN ANDROID (DATO REAL)

99,6%
CON PERMISOS REDUCIDOS EN ANDROID 10

99,7%
CON PERMISOS REDUCIDOS EN ANDROID 9

99,0%
CON PERMISOS REDUCIDOS EN ANDROID 8

95,3%
CON PERMISOS REDUCIDOS EN ANDROID 7

Aun así cabe destacar que el uso de esta herramienta ha crecido 3,7 p.p. entre los usuarios de dispositivos Android, lo cual resulta bastante positivo ya que el sistema operativo Android no incluye esta herramienta de seguridad y es el propio usuario el que debe instalarla.

A pesar de que los programas antivirus no resultan infalibles[11], continúan constituyendo una medida de seguridad básica que todo usuario debería tener instalada en sus equipos y dispositivos.

Por último, el cifrado de datos del sistema es usado por tan solo un 8,2% de los panelistas, siendo a su vez, una de las medidas más desconocidas por los usuarios (23,3%) como se podrá observar más adelante en la **FIGURA 10**.

3.2.1 Nivel de privilegios real en versiones de Android

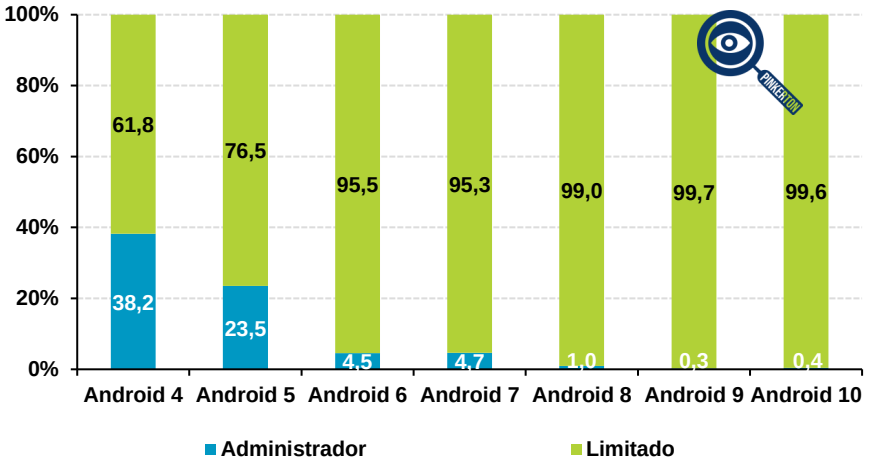
Como se ha mencionado anteriormente, el uso de perfiles de administrador (*root)* está totalmente desaconsejado por el elevado riesgo que supone sufrir una incidencia con este tipo de perfil activo. Es por ello que se toma en consideración este factor para estudiarlo en detalle.

Si se analiza qué versiones de Android cuentan con perfil de tipo administrador, se puede observar que va en total consonancia con

[11] https://www.av-comparatives.org/wp-content/uploads/2019/03/avc_android_201903_en.pdf

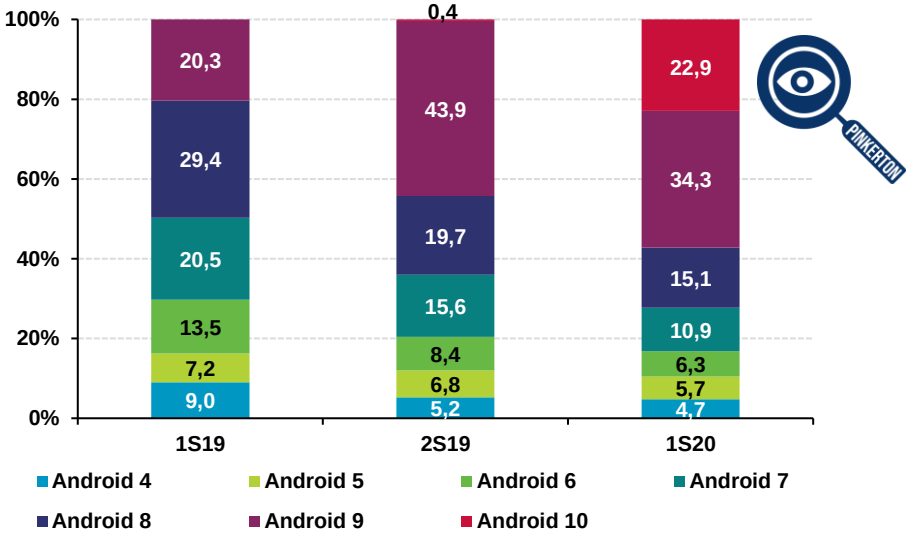
la antigüedad de la versión de Android que utiliza el usuario.

FIGURA 8. NIVEL DE PRIVILEGIOS REAL EN PERFILES EN DISPOSITIVOS ANDROID (%)



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

FIGURA 9. VERSIONES DE ANDROID EN DISPOSTIVOS MÓVILES (%)



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

Mientras que en aquellos terminales que disponen de alguna de las últimas versiones disponibles, la mayoría de los usuarios suelen operarlos con los permisos que por defecto establece el sistema, en las versiones de Android 4 y 5 se observa que más del 20% de los dispositivos han sido modificados para elevar sus privilegios.

No obstante, este hecho no debe ser preocupante puesto que la cuota de mercado de estas versiones de Android apenas alcanza el

5% en la actualidad[12], en consonancia con los datos recogidos por Pinkerton que indican un 4,7% y un 5,7% respectivamente para las versiones mencionadas y están próximas a caer en desuso (**FIGURA 9**).

Que los usuarios requieran en su dispositivo de un perfil de tipo administrador, podría responder a la necesidad de modificar aquellos que han dejado de tener soporte oficial por parte del fabricante para continuar disfrutando de novedades y actualizaciones gracias a módulos libres creados por la comunidad de desarrolladores, aplicaciones que precisan de algún requisito especial, o para modificar de alguna manera el rendimiento o incluso la apariencia del terminal.

También se debe considerar que los dispositivos más recientes suelen cubrir las necesidades del usuario, cuestión que las versiones anteriores, posiblemente, no hagan debido a haberse quedado obsoletas.

Por último, destacar que para obtener permiso de administrador es necesario realizar acciones no triviales en el dispositivo que podría ponerlo en riesgo y perder la garantía. Por lo que, una vez pasado el periodo de garantía, es más factible que el usuario opte por manipular el dispositivo.

3.3 *No utilización de medidas de seguridad*

El principal dato a destacar sobre la no utilización de medidas de seguridad, es que entre un 29,1% y un 44,7% de los usuarios opinan que no necesitan alguna de ellas. Sin embargo, un 56,1% de los usuarios han afirmado sufrir una incidencia de seguridad en los últimos seis meses (**FIGURA 21**), la cual quizás podría haberse evitado o minimizado sus consecuencias, gracias al uso de alguna de dichas medidas de seguridad.

Al analizar con más detalle los motivos de un usuario para decidir no emplear una determinada medida de seguridad, se observan diferentes casuísticas dependiendo de la medida de seguridad en cuestión (**FIGURA 10**).

Un 7,8% de los usuarios afirman desconocer qué es el DNI electrónico y un 17% los certificados digitales. Estas medidas de seguridad son las principales herramientas para realizar trámites digitales con las Administraciones Públicas, ya que permiten acceder a aplicaciones y documentos con un alto nivel de seguridad.

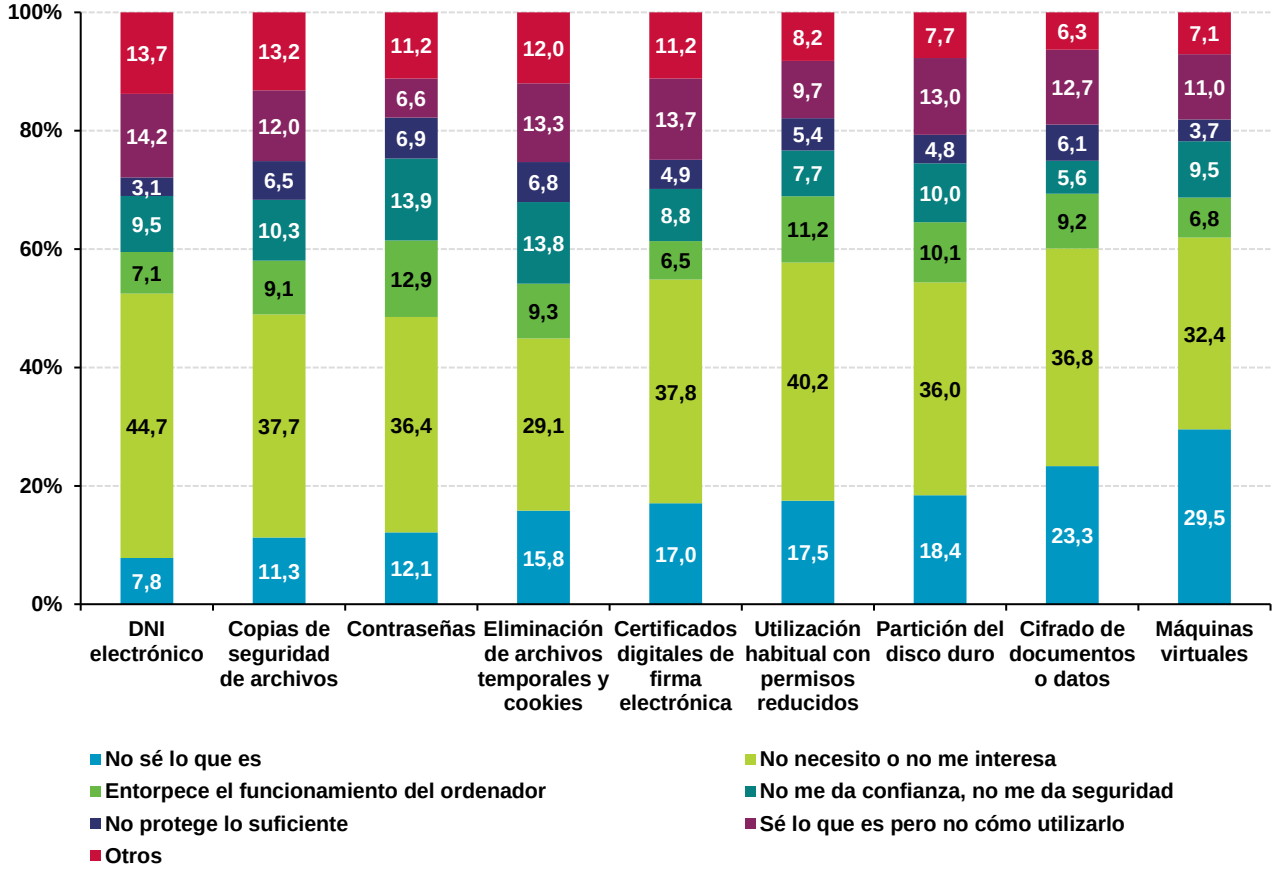
Las medidas de seguridad que más desconocen los usuarios son: las máquinas virtuales (29,5%), el cifrado de documentos o datos (23,3%) y la partición del disco duro (18,4%).

Por otro lado, las medidas de seguridad consideradas menos necesarias o carentes de interés por parte de los usuarios son: el DNI electrónico (44,7%), el empleo de usuarios con permisos reducidos en sus equipos y dispositivos (40,2%) y la realización de copias de seguridad (37,7%).

[12] https://gs.statcounter.com/os-version-market-share/android/mobile-tablet/worldwide

Esta última de gran importancia ya que puede reducir significativamente el riesgo de perder datos sensibles tras sufrir la pérdida o robo del dispositivo, borrado accidental de archivos, fallos en físicos en el equipo, un ataque de *ransomware* o cualquier otro tipo de problema de seguridad.

FIGURA 10. MOTIVOS DE NO UTILIZACIÓN DE MEDIDAS DE SEGURIDAD (%)



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

3.4 *Medidas automatizables y activas*

La utilización de medidas de seguridad automatizables permite que los equipos estén protegidos aún sin que el usuario deba actuar directamente sobre las opciones de seguridad, o tenga que configurar muy pocas opciones.

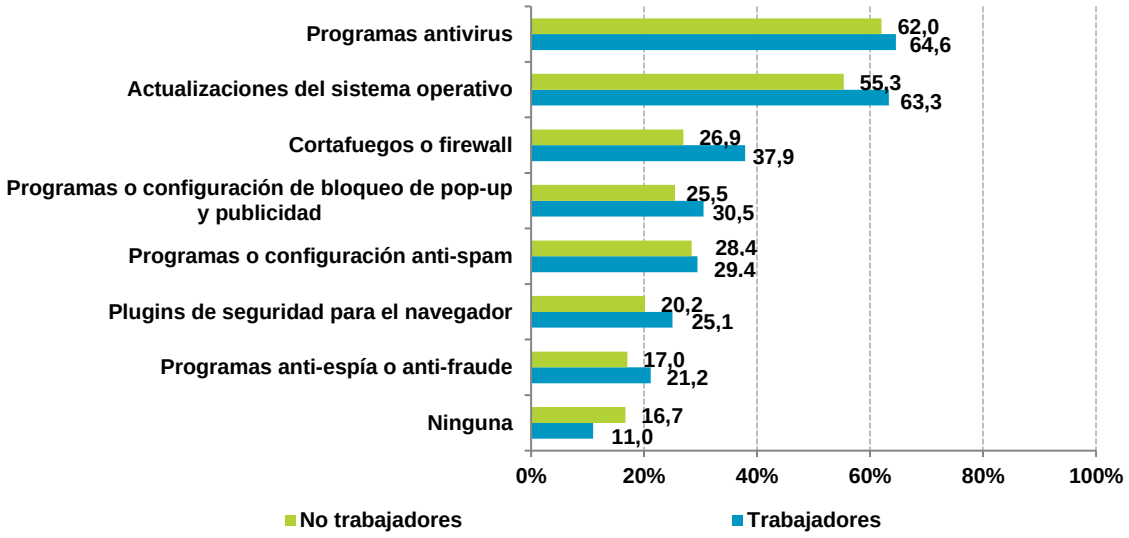
Por otra parte, las medidas activas requieren de mayor interactuación por parte del usuario. Algunas medidas de seguridad pueden encontrarse influenciadas por los hábitos laborales de los usuarios, por lo que en esta sección se considera el perfil trabajador de los usuarios.

Resulta necesario comprender el contexto de partida en cuanto al uso de las medidas de seguridad anterior a la declaración del Estado de Alarma. Los datos mostrados a continuación reflejan dicho contexto, en el que la situación generada por la pandemia del

COVID-19 pudo motivar el uso de medidas de seguridad automatizables aún antes del confinamiento.

Cabe destacar que los datos obtenidos reflejan que las medidas de seguridad, tanto automatizables como activas, son considerablemente más utilizadas por las personas que se encuentran trabajando.

FIGURA 11. MEDIDAS DE SEGURIDAD AUTOMATIZABLES EN EL ORDENADOR DEL HOGAR SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%)

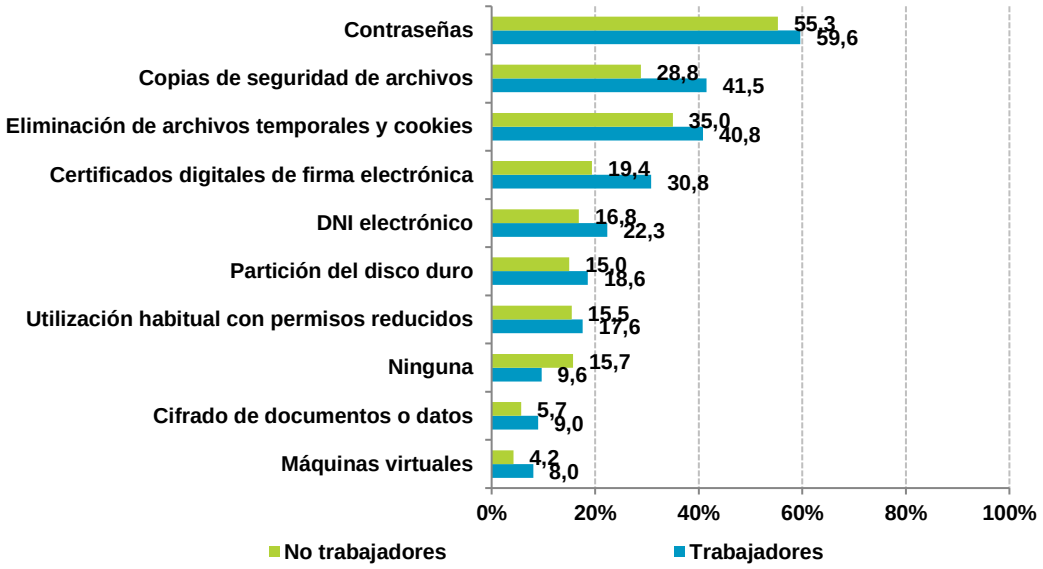


Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

En cuanto a las medidas de seguridad automatizables usadas por las personas trabajadoras respecto a las desempleadas destacan: las actualizaciones del sistema operativo (+8 p.p.), el uso de cortafuegos (+11 p.p.) o el uso de *plugins* de seguridad para el navegador (+4,9 p.p.).

Respecto a las medidas de seguridad activas destacan: la copia de seguridad de archivos (+12,7 p.p.), el uso de certificados digitales y DNI electrónico (+11,4 p.p. y +5,5 p.p. respectivamente). Estas medidas son de vital importancia si las empresas quieren que los usuarios hagan uso del teletrabajo de forma segura. Por lo tanto, resulta muy positivo que antes del confinamiento ya se estuviesen aplicando estas medidas.

FIGURA 12. MEDIDAS DE SEGURIDAD ACTIVAS EN EL ORDENADOR DEL HOGAR SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%)



Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

Una de las causas que puede explicar la mayor responsabilidad en cuanto al uso de medidas de seguridad por parte de los trabajadores, son las recomendaciones, guías y campañas de concienciación llevadas a cabo tanto por las empresas como por los organismos públicos[13].

4 Hábitos de comportamiento en la navegación y usos de Internet

Conocer la evolución de los hábitos diarios de los usuarios se torna imprescindible para identificar puntos de mejora, así como predecir posibles rutinas que pongan en riesgo la seguridad del hogar. En especial, el primer semestre de 2020 ha implicado una variación forzosa en el comportamiento de todo el conjunto de la población. Cabe destacar que las declaraciones de los panelistas corresponden a fechas anteriores al Estado de Alarma, y aun así se aprecia una variación respecto al comportamiento del usuario a la hora de navegar por Internet y utilizar su equipo. El hecho de permanecer en casa –ya sea por precaución o por imposición- podría causar un relajamiento de los hábitos prudentes entre aquellos empleados que han contado con la posibilidad de continuar realizando su actividad laboral de manera remota.

Cabe recordar, que estos hábitos suponen una parte tan importante en la seguridad como las medidas y herramientas analizadas en el apartado anterior. Por tanto, resulta de interés comprobar qué hábitos prudentes son utilizados por los usuarios españoles.

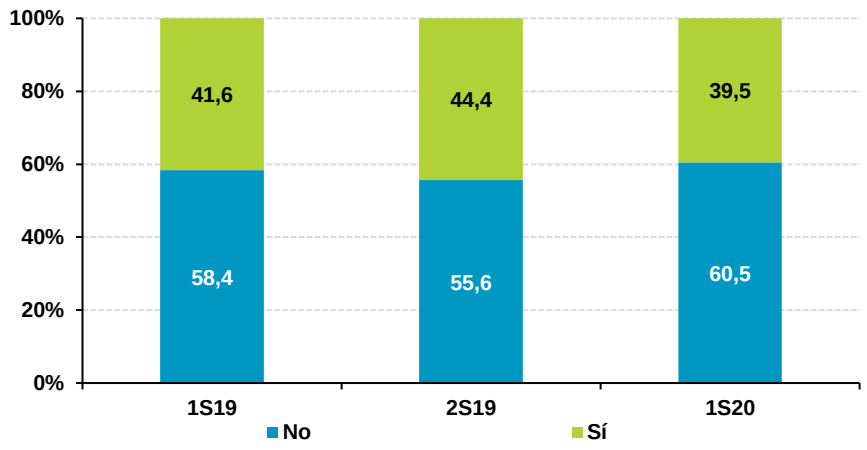
4.1 *Evolución de las conductas de riesgo*

Durante este semestre se ha apreciado un decremento en el porcentaje de usuarios que declaran la adopción de conductas de riesgo de forma consciente (-4,9 p.p.), lo que indica un perfil de usuario cada vez más prudente a la hora de hacer uso de Internet;

[13] https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

aunque en menor medida entre los usuarios que trabajan, como se puede observar en la **FIGURA 14**.

FIGURA 13. EVOLUCIÓN DE LA ADOPCIÓN CONSCIENTE DE CONDUCTAS DE RIESGO (%)



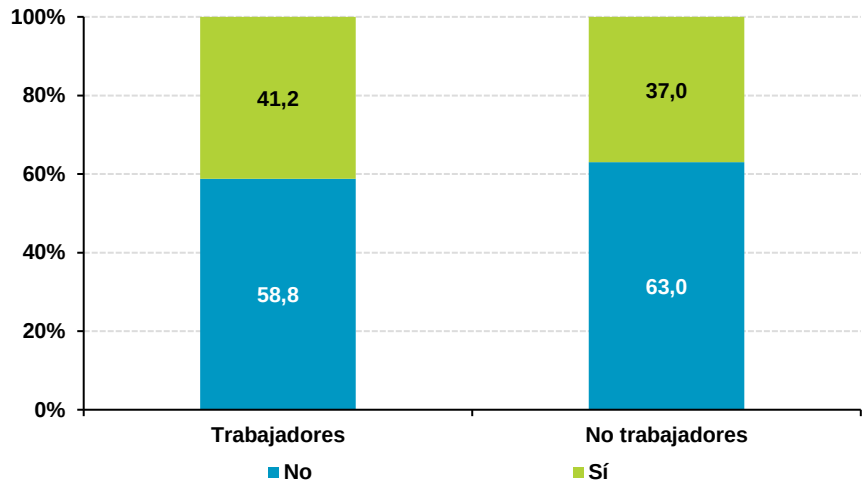
Base: Total usuarios
Fuente: Panel hogares, ONTSI

Aunque la tendencia mejora respecto al anterior semestre, son cuatro de cada diez usuarios los que realizan algún tipo de conducta de riesgo cuando navega por Internet.

Se puede observar en la siguiente gráfica que, si se compara a las personas con empleo con la población no trabajadora, las primeras realizan conductas de riesgo de forma consciente 4,2 p.p. más que la población no trabajadora.

Por tanto, se deben considerar estos datos como un indicador para corroborar que aún quedan pasos que dar para tener una población con plena cultura en seguridad.

FIGURA 14. REALIZACIÓN CONSCIENTE DE ALGUNA CONDUCTA DE RIESGO SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

Es importante destacar que, para que se produzca una incidencia de seguridad, únicamente es necesario realizar alguna acción de

riesgo puntual: por ejemplo, abrir un fichero adjunto a un correo de un remitente que no es de confianza, instalar *cracks* para poder utilizar software sin licencia, o deshabilitar el software antivirus para eludir el bloqueo a un fichero o sitio web que se ha detectado como alguna amenaza.

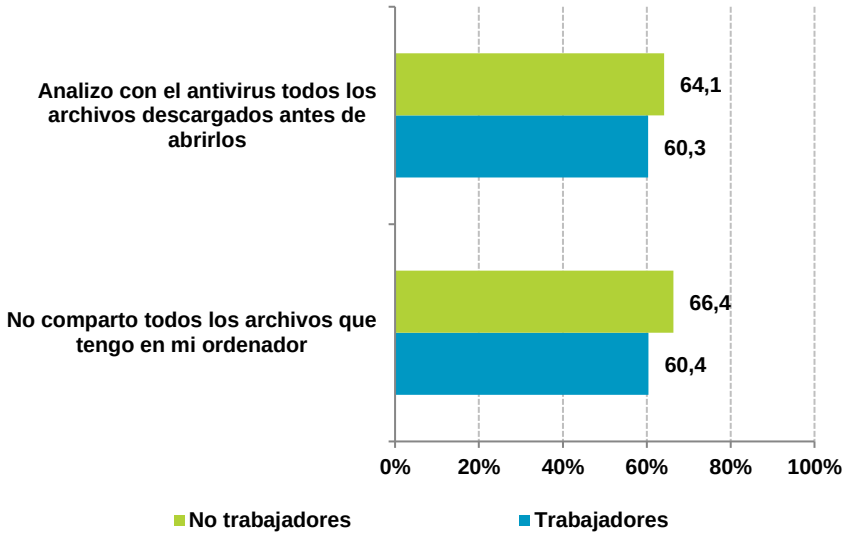
4.2 *Descargas e instalación de programas en el ordenador*

Es común que la infección de un equipo se produzca por la descarga de archivos desde plataformas no confiables o sitios de terceros que no cuentan con suficientes medidas de seguridad. Para conocer el grado de exposición de los usuarios a este tipo de problema, se ha analizado la interacción del usuario con respecto a la descarga a través de redes P2P y la descarga de archivos.

En este caso también se tiene en cuenta para el análisis si el usuario tiene un empleo remunerado en el momento de la encuesta. En concreto, los resultados apuntan a que la proporción de panelistas que analiza los archivos descargados en redes P2P con antivirus se mantiene en torno a los dos tercios (64,1%) para la población no trabajadora y algo menos (60,3%) para los usuarios trabajadores.

Sin embargo, cabe destacar que más de uno de cada tres usuarios no trabajadores exponen todo el contenido de su equipo en las redes P2P. Este hecho se agrava cuando se observan los datos porcentuales de usuarios trabajadores que realizan dicha práctica, pues casi un 40% comparte todos los archivos de su ordenador personal. Si estos trabajadores utilizasen el mismo ordenador para teletrabajar, podrían estar exponiendo información sensible y privada de la empresa.

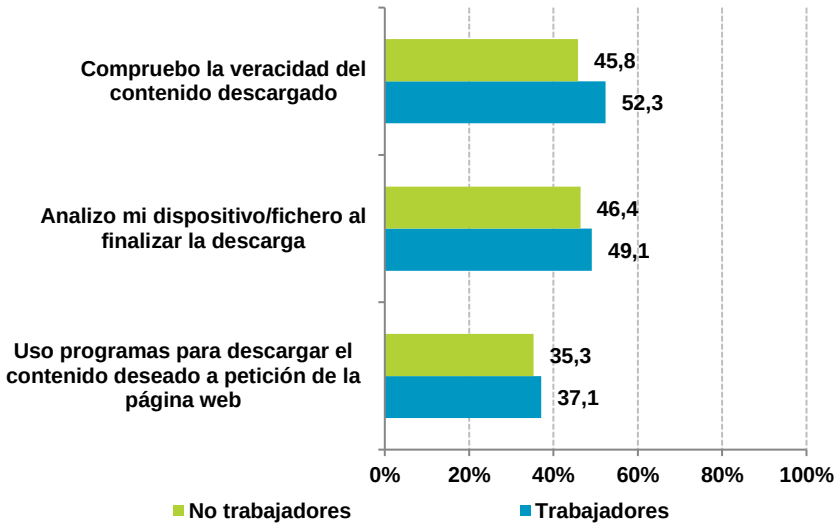
FIGURA 15. DESCARGAS EN REDES P2P SEGÚN TRABAJADORES Y NO TRABAJADORES (%)



Base: usuarios que realizan descargas P2P
Fuente: Panel hogares, ONTSI

Con respecto al comportamiento de los usuarios en relación a las descargas en Internet, éste varía notablemente entre los trabajadores y la población no trabajadora.

FIGURA 16. DESCARGAS EN INTERNET SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Los usuarios que trabajan, comprueban la veracidad del contenido descargado 6,5 p.p. más que la población no trabajadora y analizan los dispositivos al finalizar la descarga 2,7 p.p. más. En este aspecto, parece que los usuarios trabajadores realizan comportamientos más prudentes que el resto de la población.

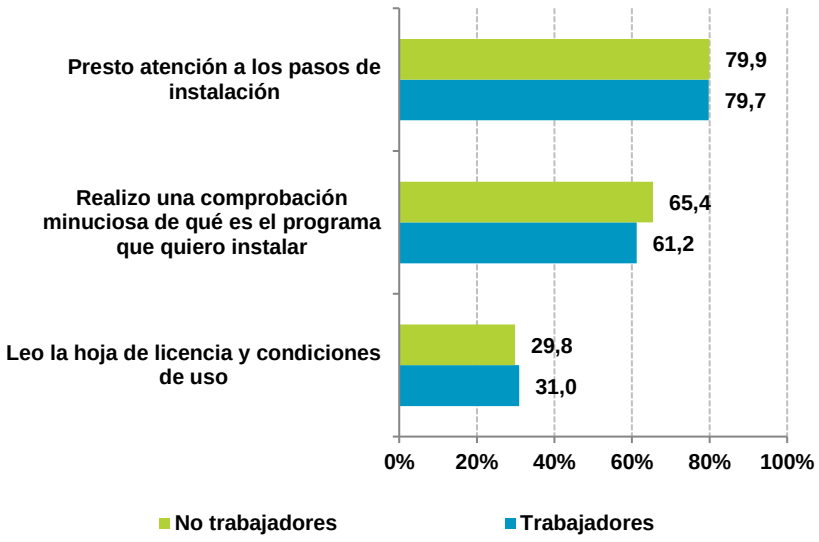
Independientemente del análisis de los ficheros descargados, siempre es recomendable comprobar también la autenticidad de los archivos con algún tipo de *hash* (o resumen), para contrastarlo con la información disponible en la web oficial desde la que se han bajado.

A pesar de que el 63,3% de panelistas tiene un antivirus instalado en su ordenador del hogar con sistema Windows (**FIGURA 5**), menos del 50% se preocupa por analizar los archivos descargados desde Internet, pese a que es una práctica bastante común distribuir *malware* mediante esta vía.

Cabe destacar que, atendiendo a los resultados desglosados en la

FIGURA 17, no se aprecia ninguna variación significativa en los hábitos que tienen los panelistas trabajadores y los que no trabajan respecto a los programas que instalan en el ordenador.

FIGURA 17. INSTALACIÓN DE PROGRAMAS EN EL ORDENADOR DEL HOGAR SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

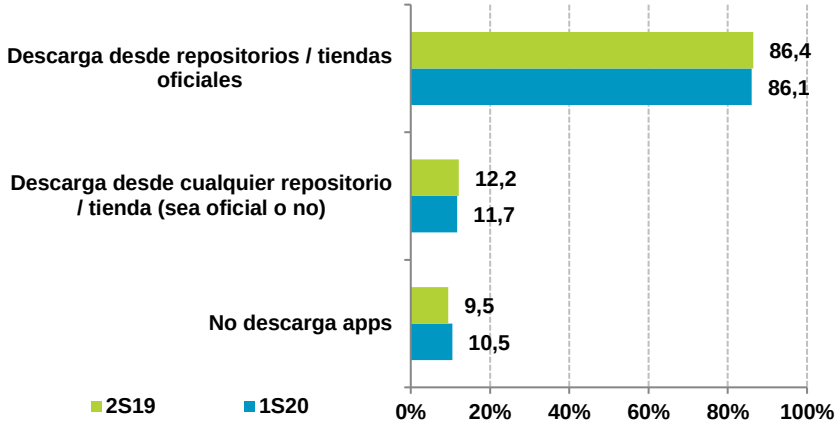
En torno al 80% de los panelistas afirman prestar atención a los pasos de instalación. Este hábito es de vital importancia puesto que durante la instalación de determinados programas o versiones gratuitas o de prueba de los mismos se solicita, y aparece marcada por defecto su aceptación, la opción de instalar software de terceros a modo de financiación. De forma que al no prestar la debida atención, se instalará software no deseado en el sistema. En algunos casos, se instala software de terceros que tiene como propósito el minado de *bitcoins* mediante los recursos del ordenador, con la consecuente pérdida de rendimiento que esto conlleva.

El porcentaje de usuarios que realizan una comprobación minuciosa sobre el programa que desean instalar es del 61,2% para los usuarios trabajadores y del 65,4% para la población no empleada, presentándose aquí la mayor diferencia entre estos dos grupos. Por último, tan solo el 29,8% de los panelistas no trabajadores y el 31,0% que sí trabaja, afirman leer la hoja de licencia y condiciones.

4.3 Evolución de los hábitos en dispositivos Android

La mayoría de los usuarios que disponen de un dispositivo Android hacen uso de los repositorios oficiales para la descarga de aplicaciones, este porcentaje sigue manteniéndose por encima del 86% de los panelistas (**FIGURA 18**). Por otro lado, el porcentaje de usuarios que también descargan de repositorios no oficiales baja 0,5 p.p. respecto al pasado semestre.

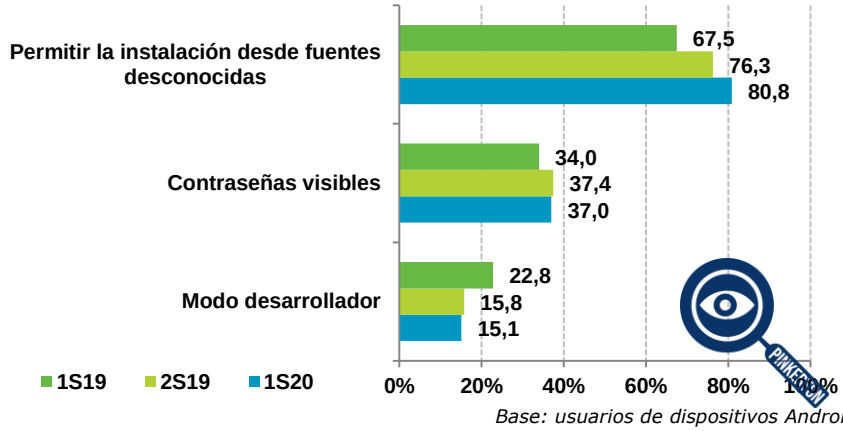
FIGURA 18. DESCARGA DE APLICACIONES EN DISPOSITIVOS ANDROID (%)



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

El hecho de que repositorios oficiales (véase Google Play) estén integrados en los dispositivos Android de fábrica, es el principal motivo de que su uso sea tan elevado, resultando más cómodo y sencillo para el usuario utilizarlos.

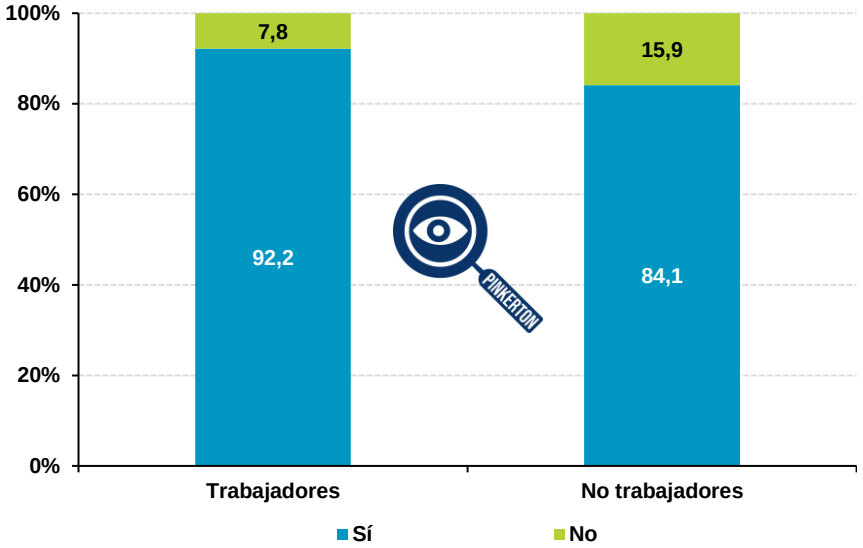
FIGURA 19. EVOLUCIÓN DEL ESTADO DE OPCIONES DE SEGURIDAD EN DISPOSITIVOS ANDROID (%)



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

La opción de permitir la instalación desde fuentes desconocidas (80,8%) sigue creciendo a un ritmo continuo, experimentando un incremento de 4,5 p.p. desde el anterior semestre, y de 13,3 p.p. desde inicios de 2019. Es necesario mencionar que, por defecto, dicha opción viene desactivada en el sistema Android debiendo el usuario modificarla. Cabe matizar que en versiones anteriores a Android 8.0, la instalación de aplicaciones desde fuentes desconocidas era un ajuste único en las opciones del dispositivo. A partir de dicha versión, este hecho cambió y el usuario debe activar una a una las aplicaciones que quiere que hagan uso de este permiso, lo que añade algo más de seguridad.

FIGURA 20. ESTADO DE LA OPCIÓN DE INSTALACIÓN DESDE FUENTES DESCONOCIDAS ENTRE USUARIOS QUE DESCARGAN APLICACIONES DESDE REPOSITORIOS NO OFICIALES SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%)



Base: usuarios que descargan apps desde repositorios no oficiales
Fuente: Panel hogares, ONTSI

Sin embargo, llevar a cabo instalaciones de aplicaciones desde tiendas o repositorios no oficiales supone un riesgo para el dispositivo y la integridad de otras aplicaciones. En dichos repositorios o tiendas, por lo general, no se controla la procedencia de las aplicaciones que en ellas se almacenan. Además, en ocasiones, no se realizan análisis para comprobar la existencia de *malware*, e incluso puede no ser posible comprobar el certificado con el que se ha firmado la aplicación, al contrario que en los *markets* oficiales.

Una aplicación descargada desde un sitio no oficial podría incluir algún tipo de *malware*. Por ejemplo los *droppers*, que se encargan de descargar otros códigos maliciosos en el sistema infectado, o *bankbots*, que manipulan aplicaciones bancarias instaladas en el sistema realizando una suplantación de la pantalla de inicio del banco, y en ocasiones de la tarjeta de coordenadas en el momento en el que el usuario abre la aplicación.

Por último, la opción de contraseñas visibles y modo desarrollador apenas experimentan variaciones respecto al anterior semestre, siendo activadas dichas opciones por el 37% y 15,1% de los usuarios respectivamente.

Que más de un tercio de los panelistas tenga activada la opción de contraseñas visibles en su dispositivo móvil supone un gran riesgo ante una posible pérdida o robo del mismo, ya que un tercero podría tener acceso a información sensible y privada del usuario.

Si se disgrega entre usuarios que actualmente trabajan y la población trabajadora, es posible hallar ligeras diferencias entre el porcentaje de los usuarios que descargan aplicaciones desde repositorios no oficiales y tienen activa la opción de instalar aplicaciones desde fuentes desconocidas: +8,1 p.p. en el primer grupo.

Como punto positivo, se observa que entre los usuarios que realizan descargas desde repositorios no oficiales, existe un pequeño grupo más prudente (7,8% entre los trabajadores y 15,9% entre los no

trabajadores) que deshabilita la opción de instalar desde fuentes desconocidas tras realizar la descarga.

5 Incidentes de seguridad

La utilización de las diferentes medidas de seguridad y la práctica de hábitos prudentes adquieren un papel de gran importancia al reducir significativamente el riesgo de que las amenazas de seguridad se tornen en incidencias reales. Más si cabe aún, estas medidas deben priorizarse al máximo en entornos de teletrabajo.

Sin embargo, no existe un método que resulte infalible y, además, dichas amenazas se encuentran en continua evolución en su afán de tratar de eludir las posibles barreras tanto a nivel de usuario como de sistema, e incluso, pasar desapercibidas ante los diferentes programas de seguridad.

En este apartado se analizan los incidentes de seguridad sufridos por los panelistas en el periodo comprendido entre enero y junio de 2020. Al igual que en las secciones anteriores los datos declarados por los panelistas corresponden al primer trimestre del año 2020, mientras que los datos reales recabados de los dispositivos reflejan el estado de los mismos durante el segundo trimestre, al final del primer semestre.

5.1 Evolución de las incidencias

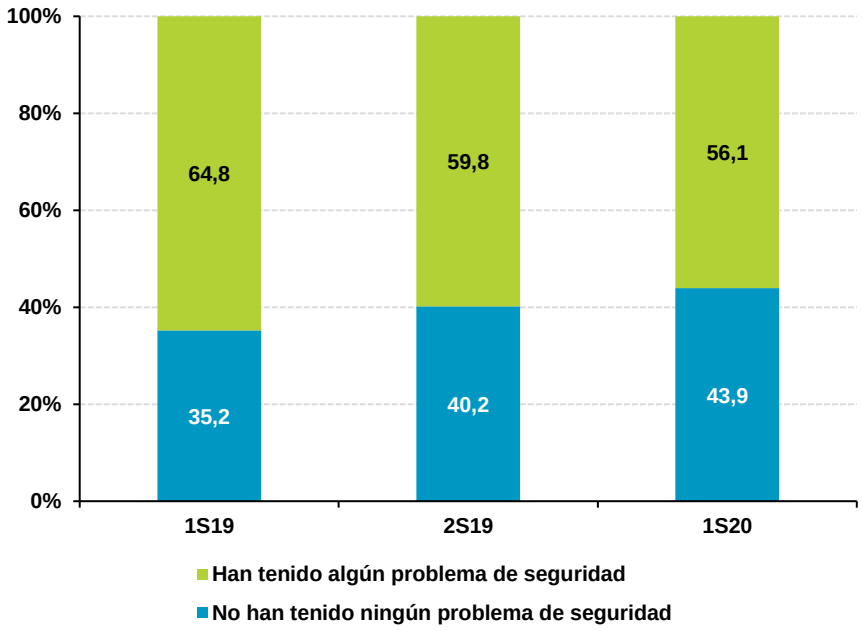
El número de usuarios que han informado de algún problema de seguridad en los últimos 6 meses sigue reduciéndose (-3,7 p.p.), continuando con la tendencia decreciente iniciada en la segunda mitad del año 2018.

Teniendo en cuenta que el número de ciberataques durante los últimos años sigue creciendo considerablemente, registrándose hasta 218.302 ciberdelitos[14] en España en 2019 y, que el 71% de trabajadores IT de seguridad han percibido un aumento de ciberataques[15] desde el inicio de la pandemia del SARS-CoV-2, se podría considerar que las cifras seguirán creciendo.

FIGURA 21. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)

[14] https://oedi.es/estadisticas/

[15] https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/



Base: total usuarios
Fuente: Panel hogares, ONTSI

No obstante, más de la mitad de los panelistas (56,1%), afirman haber sufrido algún problema de seguridad en el último semestre. Aunque esta cifra disminuye ligeramente respecto al segundo semestre de 2019, no debemos olvidar que, de hecho, son incidentes declarados – aquellos de los que se ha percatado el usuario, que podrían ser falsos positivos o negativos – y por tanto los datos reales que se verán más adelante serán determinantes para conocer el estado real de los dispositivos.

Se pueden encontrar numerosos motivos para que más de la mitad de los usuarios hayan sufrido algún problema de seguridad. Entre los usuarios que no utilizan alguna de las medidas de seguridad (**FIGURA 10**), que en gran medida pueden prevenir y evitar este tipo de incidencias, hay entre un 29% y un 45% de los usuarios que opinan que no son necesarias. Un gran porcentaje de los usuarios no hacen uso de medidas activas como los programas antivirus (36,7%) o anti-spam (89,4%). La actualización del sistema operativo, realizada por el 45,1% de los panelistas, queda un tanto alejada de valores ideales de lo que debería ser la utilización de esta medida de seguridad.

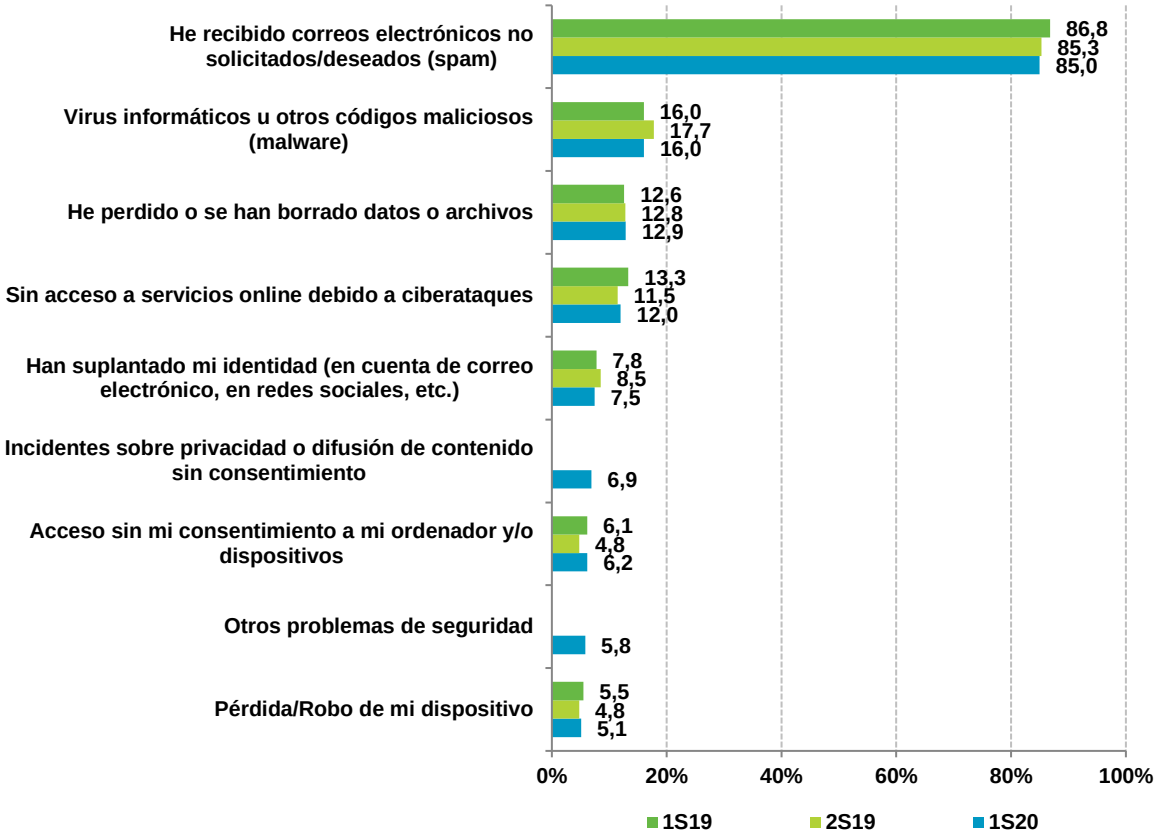
En cuanto a dispositivos móviles que usan el sistema operativo Android (**FIGURA 7**), el 44,8% no tiene instalado ningún software antivirus. Por tanto, el escaso uso de medidas como el sistema de desbloqueo seguro (8,8%), el encriptado de datos (8,2%), o la elevada tasa de panelistas que permiten la instalación desde fuentes desconocidas (80,8%) (**FIGURA 19**).

Por otro lado, si bien ha disminuido el número de usuarios que afirman realizar conductas de riesgo en Internet (**FIGURA 13**), sigue siendo un dato bastante elevado (39,5%).

Todos estos aspectos constituirían las principales medidas a incentivar para tratar de reducir aún más las incidencias de seguridad.

Respecto a las incidencias que afectan a los usuarios se mantienen estables respecto a los anteriores semestres (**FIGURA 22**). La recepción de correo electrónico no deseado, que afecta a un 85% de los panelistas, es la incidencia más acusada, permaneciendo como uno de los principales vectores de ataque para la difusión de *malware* o las campañas de *phishing* para el robo de credenciales bancarias, por ejemplo. En segundo lugar, encontramos las incidencias relacionadas con virus informáticos u otros códigos maliciosos (*malware*) que se mantiene estable entorno al 16%.

FIGURA 22. EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



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

Si bien estas campañas de ataques a usuarios a través de la Red han estado siempre presentes, desde el inicio de la pandemia los ciberdelicuentes han usado como gancho la COVID-19 y noticias derivadas de ello como por ejemplo, suplantaciones del Ministerio de Trabajo[16] con motivo de los ERTEs masivos que se han producido en España, para llevar a cabo este tipo de ataques[17].

La suplantación de identidad en redes sociales o correo electrónico (7,5%) cobra especial relevancia, ya que debido al teletrabajo, una vulneración de los datos del usuario podría afectar directamente a la empresa. El objetivo de los atacantes suele ser, principalmente, listados de usuarios y contraseñas.

[16] https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-correos-maliciosos-suplantando-al-ministerio-trabajo

[17] http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/11791400

Estos datos podrían ser aprovechados para suplantar identidades, realizar campañas de *spam*, o incluso, lograr acceso a otros servicios relacionados con los usuarios y las empresas afectadas debido a que en numerosas ocasiones se utiliza la misma contraseña [18] en servicios diferentes con el peligro que esto conlleva.

El resto de tipos de incidencias no presenta grandes variaciones, o muestran pequeños incrementos, como en el caso de la pérdida de acceso a Internet debido a ciberataques (+0,5 p.p.), o el acceso sin consentimiento al ordenador o dispositivo móvil (+1,4 p.p.).

Incidentes relacionados con la privacidad y la difusión de contenido sin consentimiento alcanzan el 6,9%. Con el auge de las redes sociales y la mensajería instantánea es cada vez más común sufrir este tipo de incidentes.

Los vectores por los que se producen son numerosos. Como ejemplos, la autorización por parte del usuario a terceras aplicaciones que puede considerar útiles, pero que en determinadas ocasiones requieren acceso a datos personales del usuario (de ahí la importancia de leer las condiciones de uso), que los usuarios compartan demasiados datos personales en sus perfiles públicos, o los *bots* que se hacen pasar por usuarios reales podrían ser utilizados para recabar información personal sin que el usuario fuese consciente de ello.

Debido a que este tipo de incidencias se están volviendo cada vez más comunes y lo valioso que resultan dichos datos personales para determinadas empresas, Facebook, con el objetivo de mitigar la difusión de contenido sin consentimiento, ha lanzado la plataforma "No sin mi consentimiento"[19], donde se puede denunciar de forma rápida dichas difusiones no autorizadas.

5.2 Infecciones por malware

El *malware* hallado en los ordenadores de los panelistas categorizado como de riesgo alto se ve incrementado 5,6 p.p. respecto al pasado semestre, quedándose cerca de los registros del primer semestre de 2019.

Además de aumentar el porcentaje de infecciones categorizadas como de alto riesgo, también ha habido un aumento en el porcentaje de equipos infectados (4,3 p.p.).

FIGURA 23. ESTADO REAL DE INFECCIÓN EN EL ORDENADOR DEL HOGAR (%)

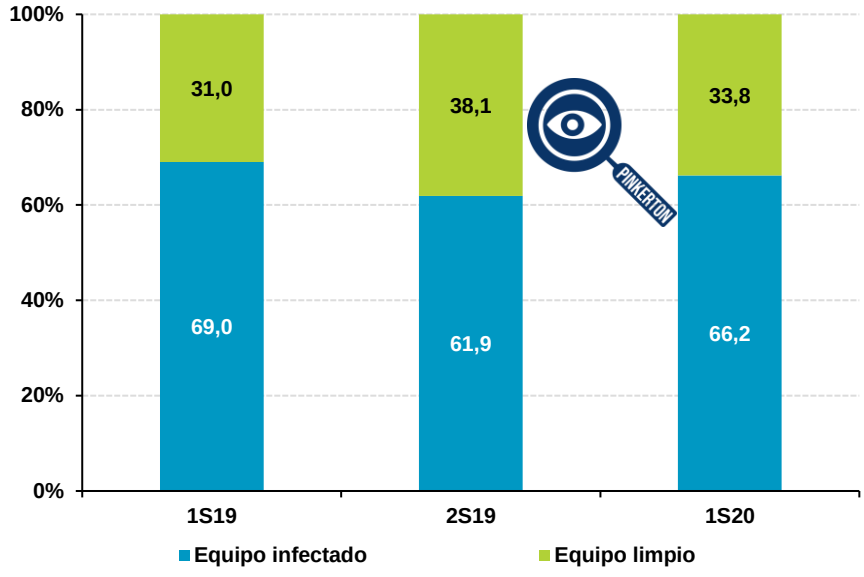
[18] https://www.pandasecurity.com/spain/mediacenter/notas-de-prensa/misma-contrasena/#:~:text=Panda%20Dome%20Passwords%3A%20varias%20cuentas,al%20ingenio%20de%20un%20ciberdelincuente.

[19] https://www.facebook.com/safety/notwithoutmyconsent

ORDENADORES QUE ALOJAN MALWARE Y SU PELIGROSIDAD

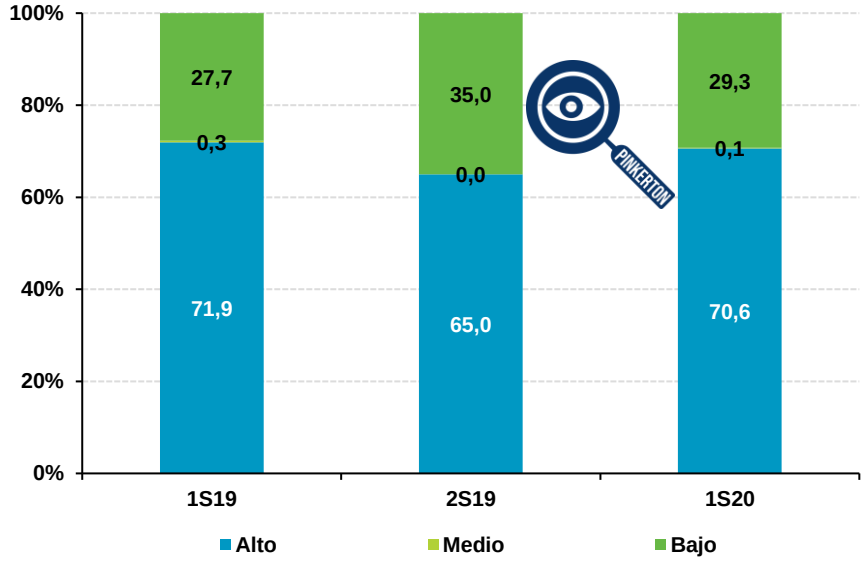
66,2%
DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE

70,6%
DEL MALWARE DETECTADO PRESENTA UN NIVEL DE RIESGO ALTO



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

FIGURA 24. PELIGROSIDAD DEL MALWARE EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

Con estos datos se concluye que el *malware* de al menos siete de cada diez ordenadores infectados presenta un riesgo alto, lo cual podría suponer: el acceso remoto por parte de un atacante al sistema de la víctima, el perjuicio económico para el usuario, o la captura de información confidencial o sensible de la víctima entre otros.

Son datos obtenidos a lo largo del primer semestre de 2020, incluido el confinamiento, por lo que parte de los usuarios podrían estar haciendo uso de estos equipos para teletrabajar exponiendo no sólo la seguridad de su hogar, sino la de su empresa.

Las empresas de soluciones antivirus están constantemente actualizando sus sistemas de detección de amenazas, desarrollando

técnicas nuevas que puedan servir tanto para las familias de *malware* ya conocidas, como para que las de nuevo desarrollo puedan ser también rápidamente reconocidas y neutralizadas. Es por ello que el uso de este tipo de software es básico para proteger un equipo frente a este tipo de incidencias.

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

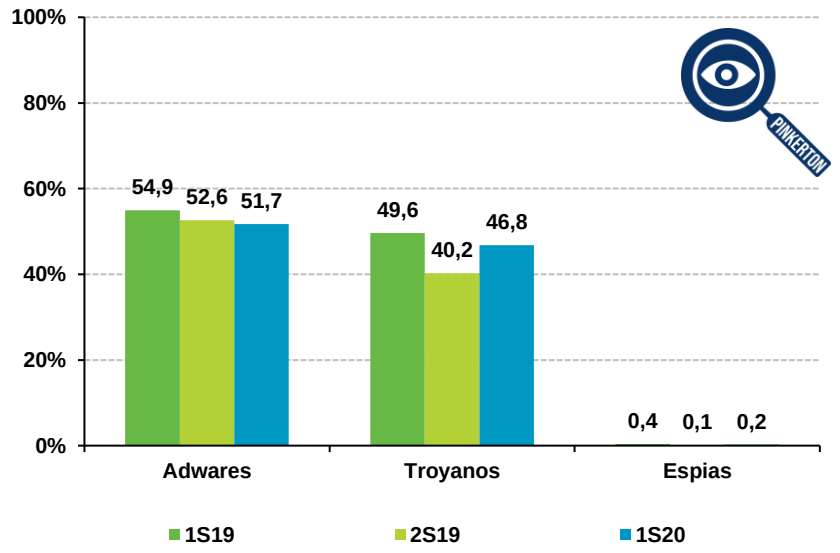
Declaran tener malware en PC	Su PC presenta malware		
	Sí	No	Total
Sí	6,8	4,7	11,5
No	59,3	29,2	88,5
Total	66,1	33,9	100

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

Los troyanos han sido el tipo de *malware* que más ha crecido en este último semestre marcado por el confinamiento.

El porcentaje de usuarios que no se percatan de que su ordenador del hogar está infectado por *malware* asciende hasta el 59,3%, lo que supone un aumento de 7,3 p.p. respecto al anterior semestre. Este dato crece proporcionalmente al porcentaje de equipos infectados, y podría suponer una mayor ofuscación de las infecciones de *malware* de cara al usuario. Esta situación es un tanto preocupante puesto que un usuario que no es consciente de que ha sido infectado con *malware* no tomará las medidas oportunas para mitigar y solventar dicha infección. Además, podría crear una falsa sensación de seguridad llevando a una relajación de los hábitos prudentes utilizados o un incremento de las conductas de riesgo al no percibir el usuario la relación causa-efecto entre ellas.

FIGURA 25. EVOLUCIÓN DEL MALWARE EN EL ORDENADOR DEL HOGAR (%)



Base: Total ordenadores
Fuente: Panel hogares, ONTSI

A continuación se analizan los tipos de *malware* que la herramienta Pinkerton ha hallado en los ordenadores de los panelistas.

Los troyanos presentan un notable repunte (+6,6 p.p.) respecto a la oleada previa, llegando a niveles próximos a los del primer semestre de 2019. Este considerable aumento de los troyanos va en total consonancia con el mayor porcentaje de *malware* de alto riesgo detectado (

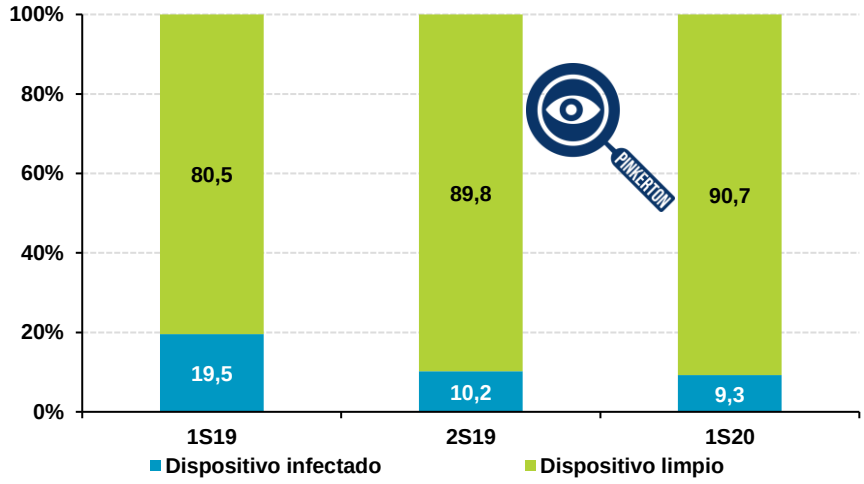
FIGURA 24).

Por otro lado, los *adwares* confirman la tendencia a la baja que presentaron en el segundo semestre de 2019, acumulando un descenso de 3,2 p.p. desde inicios del mismo año.

Por último, la presencia de *malware* espía en el ordenador del usuario es virtualmente nula. El motivo puede ser que este tipo de *malware* suele ser más sofisticado y las infecciones están enfocadas a objetivos muy concretos, mientras que el adware y los troyanos podrían obtener beneficios prácticamente de cualquier sistema infectado.

5.3 Malware en dispositivos Android

FIGURA 26. ESTADO REAL DE INFECCIÓN EN DISPOSITIVOS ANDROID (%)

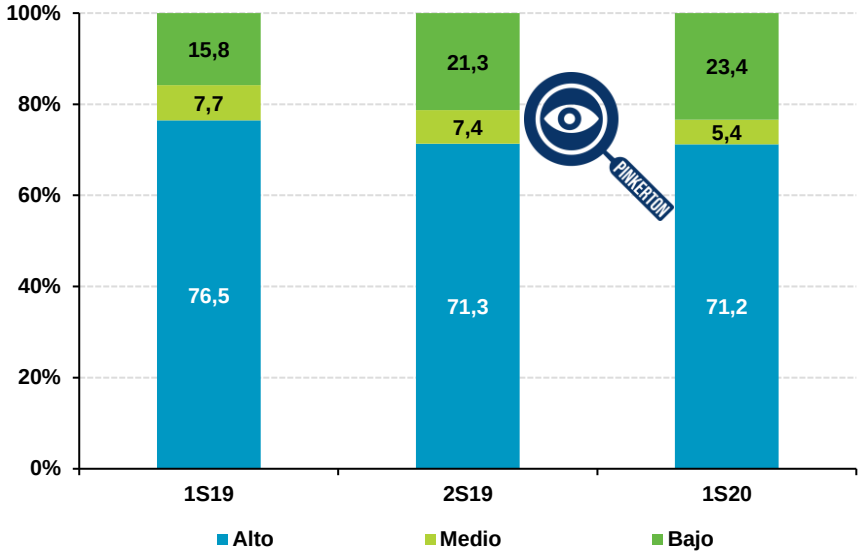


Base: total de dispositivos Android
Fuente: Panel hogares, ONTSI

En cuanto a los dispositivos móviles, la tendencia es opuesta a la vista en los ordenadores del hogar. Las infecciones siguen bajando, situándose en el 9,3%, lo que supone 0,9 p.p. menos que el segundo semestre de 2019. Se podía esperar que, al igual que en los ordenadores, el porcentaje de dispositivos móviles infectados aumentase.

Cabe la posibilidad de que esta reducción se deba en parte a que los atacantes hayan percibido que durante el confinamiento los usuarios iban a hacer más uso del ordenador del hogar en detrimento del móvil, y por ello hayan enfocado sus ataques al ordenador en mayor medida. Otra opción podría estar relacionada con el hecho de que, al contrario que con el ordenador del hogar, el usuario cambia con cierta frecuencia de dispositivo móvil e incluso si llega a percibir un bajo rendimiento (quizás causado por una infección de *malware*) en lugar de investigar la causa y buscar una solución, opta por sustituir el dispositivo por uno más actual.

FIGURA 27. PELIGROSIDAD DEL MALWARE EN DISPOSITIVOS ANDROID (%)



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

No se observa ningún cambio significativo respecto a la peligrosidad del *malware* hallado en los dispositivos móviles. La peligrosidad caracterizada como alta apenas varía un 0,1 p.p., la media 2,0 p.p. y la baja 2,1 p.p.

Si se compara la tasa de variación de infecciones de peligrosidad alta (+5,6 p.p.) que se ha visto en los ordenadores del hogar (

FIGURA 24), frente a la de los dispositivos móviles que no ha presentado una variación significativa, es factible la suposición de que se ha puesto mayor foco de atención en atacar el ordenador.

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

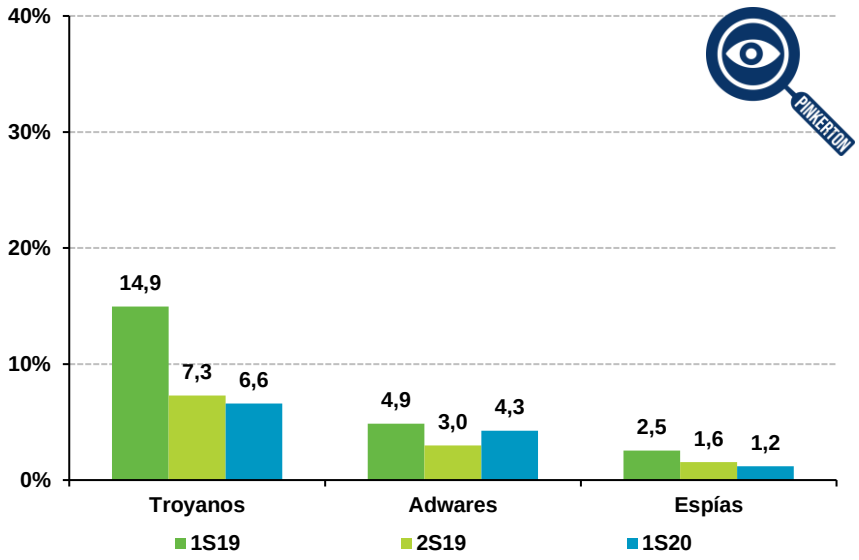
Declaran tener malware en el dispositivo Android	Su dispositivo Android presenta malware		
	Sí	No	Tota
Sí	0,6	4,7	5,3
No	8,7	86	94,7
Total	9,3	90,7	100

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

La Tabla 2 refleja los datos acerca de las incidencias de *malware* detectadas y declaradas en los dispositivos móviles. Aunque la incidencia es baja, con tan solo un 9,3% de dispositivos infectados, tan solo el 0,6% percibe que ha sufrido un incidente por *malware.*

Que el sistema operativo Android cuente con un *market* de aplicaciones oficiales que es usado por el 86,1% de los usuarios (**FIGURA 18**), puede ser el punto que marca la diferencia entre estos datos y los obtenidos en el PC.

FIGURA 28. EVOLUCIÓN DEL MALWARE EN DISPOSITIVOS ANDROID (%)



Base: Total dispositivos Android
Fuente: Panel hogares, ONTSI

Si bien en el ordenador de los usuarios se apreciaba un repunte notable de los troyanos, en los dispositivos móviles siguen en línea descendente, con una reducción de 0,7 p.p. respecto al semestre anterior.

El objetivo más habitual de los troyanos en dispositivos móviles suele ser la obtención de acceso a cuentas bancarias o contenido sensible con el que poder chantajear a los usuarios para que paguen una determinada cantidad, generalmente en *bitcoins* o en alguna moneda electrónica para evitar el rastreo del pago.

El *adware* aumenta ligeramente (1,3 p.p.) y el *malware* espía se reduce, presentando una incidencia del 1,2%.

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

Cuando se produce un incidente de seguridad, lleva consigo una serie de acciones a posteriori. Las víctimas suelen tratar de evitar que se repita modificando sus hábitos prudentes y las medidas de seguridad utilizadas (o comenzando a utilizarlas), buscando información en Internet, recibiendo formación o contratando a empresas dedicadas a la seguridad, entre otras.

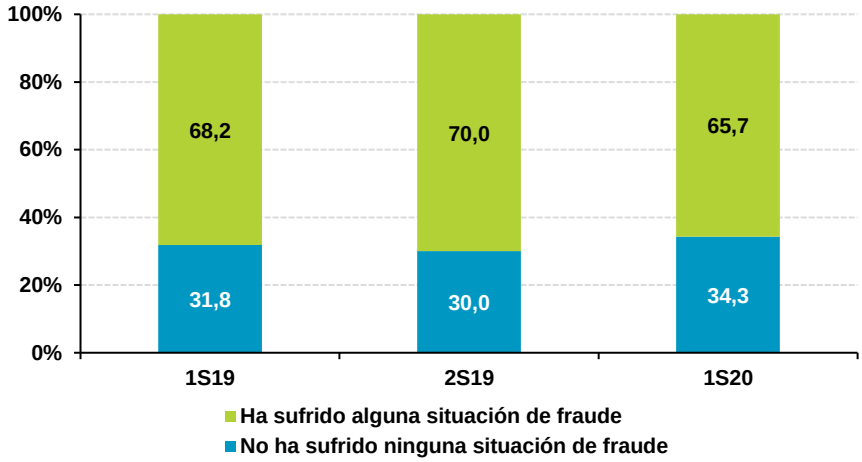
En consecuencia, el usuario va adquiriendo conciencia de los peligros que supone navegar por Internet si no se hace un uso responsable del mismo.

En el siguiente apartado se analizan las reacciones experimentadas por los usuarios después de haber padecido un incidente de seguridad.

6.1 Evolución de los intentos de fraude

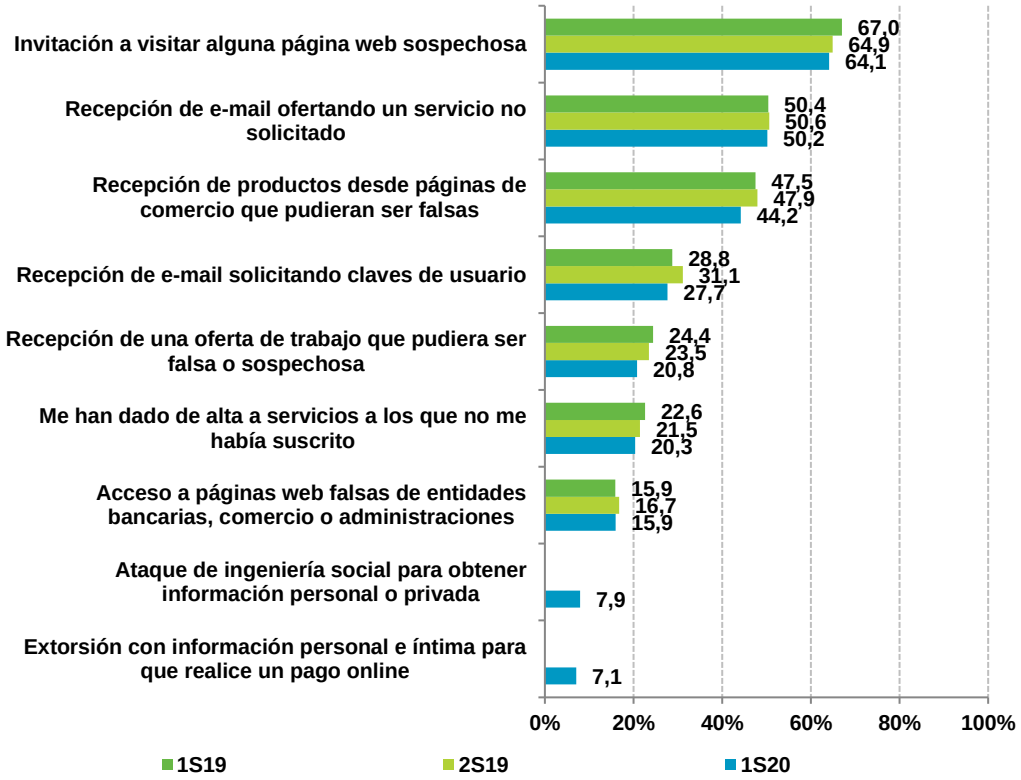
La ocurrencia de alguna situación de fraude en los últimos seis meses ha experimentado un considerable descenso (-4,3 p.p.). Esto va en concordancia con el menor reporte de incidencias de seguridad que han percibido los panelistas (**FIGURA 21**) y por tanto corrobora que, pese al incremento notable de ciberataques (según los expertos) en este último semestre, los usuarios están más concienciados y han dado un mejor uso a las herramientas de seguridad.

FIGURA 29. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

FIGURA 30. EVOLUCIÓN DE LA MANIFESTACIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



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

Las manifestaciones de los intentos de fraude están siguiendo una tendencia descendente desde inicios de 2019. No obstante, la tendencia a la baja refuerza el hecho de que el usuario cada vez es más consciente de las incidencias que puede sufrir al hacer uso de Internet y a su vez, las herramientas están siendo más precisas a la hora de evitar que los fraudes tales como spam o páginas fraudulentas, lleguen al usuario final.

Como novedad, los usuarios han reportado ataques de ingeniería social para obtener información personal o privada (7,9%). Los atacantes utilizan el *phishing*, *vishing* (llamadas telefónicas), *smishing* (mensajes de texto) o las redes sociales para realizar este tipo de ataques. Con dicha información los ciberdelincuentes podrían realizar ataques, ya no solo contra el propio usuario, sino contra la empresa de la que son empleados, con las graves consecuencias que esto podría suponer.

Para evitar este tipo de ataques se recomienda no compartir información personal por teléfono o mail, no abrir los ficheros adjuntos si provienen de remitentes desconocidos y la actualización del software antivirus.

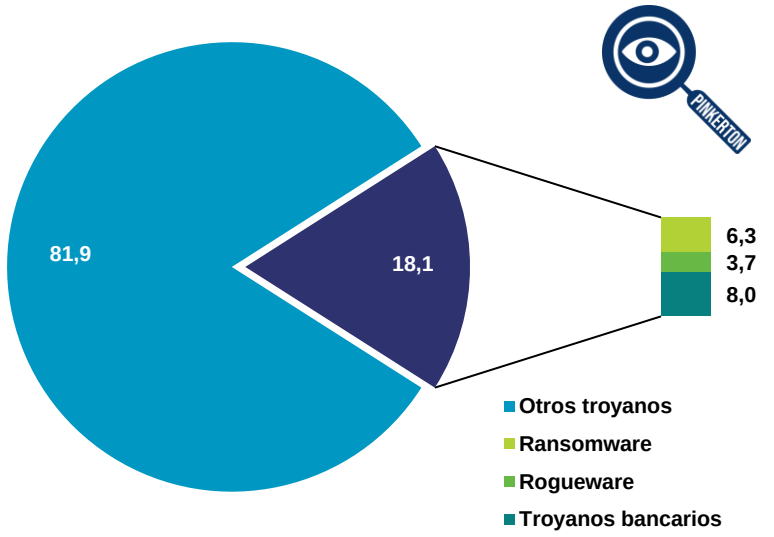
Por otro lado, estos ataques de ingeniería social también pueden derivar en extorsiones con información personal e íntima, reportadas por un 7,1% de los panelistas. La propia Policía Nacional advirtió del gran incremento de sextorsión en plena pandemia por el coronavirus[20].

La invitación a visitar alguna página web sospechosa sigue siendo el fraude más percibido con un 64,1%, mientras que la recepción de e-mail ofertando servicios no solicitados o la recepción de productos desde páginas de comercio que pudieran ser falsas son percibidas por un 50,2% y 44,2% respectivamente.

Tipología del malware analizado

- Troyano bancario: *malware* que roba información confidencial a los clientes de banca y/o plataformas de pago online.
- *Rogueware* o rogue: *malware* que hace creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto del pago suele ser la compra de un falso antivirus, que resulta ser en realidad el *malware* en sí.
- *Ransomware*: *malware* que se instala en el sistema tomándolo como "rehén" y solicita al usuario el pago de una cantidad monetaria como rescate (*ransom* en inglés).

FIGURA 31. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN EL ORDENADOR DEL HOGAR (%)



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

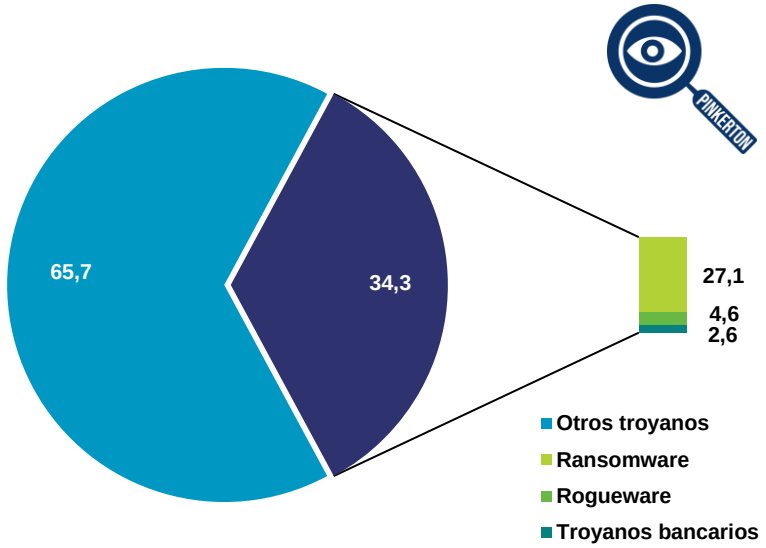
[20] https://elpais.com/sociedad/2020-04-14/la-policia-alerta-de-una-oleada-de-correos-electronicos-de-sextorsion.html

Los troyanos bancarios y los *ransomware* llevan siendo, durante un tiempo, las amenazas más rentables. Si bien estos ataques llevan produciéndose entre los usuarios mucho tiempo, en estos últimos meses se ha empleado la COVID-19 como gancho para producir las infecciones. Un ejemplo de ellos es el troyano Ginp[21], que engañaba a la víctima con un buscador de infectados por coronavirus.

Por norma general, el *ransomware* se incluye dentro de algún troyano, como una herramienta que desplegará el atacante una vez haya recopilado los datos de interés.

Esto hace que, a través del *ransomware,* se consigan maximizar las ganancias llevando a cabo el cifrado de archivos en los dispositivos infectados para después pedir un rescate por los mismos.

FIGURA 32. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN DISPOSITIVOS ANDROID (%)



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

Anteriormente se pudo ver que el porcentaje de dispositivos móviles infectados por troyanos era muy inferior al sufrido en ordenadores (**FIGURA 25**). Sin embargo, los vectores de ataque en los dispositivos Android están mucho más focalizados en el uso de *ransomware* (+20,8 p.p.) que en el ordenador.

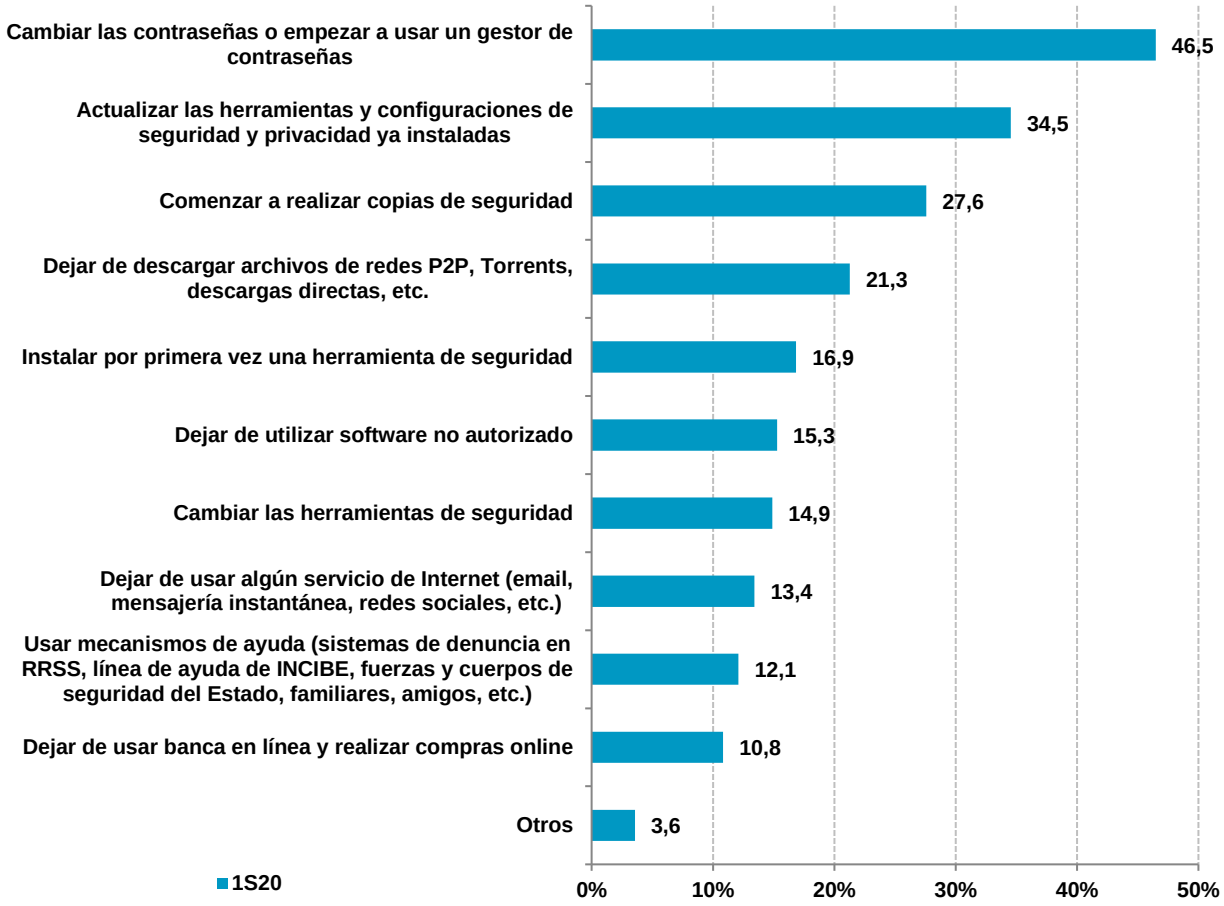
Esta diferencia deja entrever la importancia que le dan los cibercriminales a los datos de los dispositivos móviles y el valor que éstos pueden tener tanto personal como empresarialmente. Por ello el uso de cifrados de datos (**FIGURA 7**) y las copias de seguridad cobran más importancia que nunca.

6.2 Cambios de hábitos tras incidente

El cambio más frecuente entre los usuarios tras sufrir un incidente de seguridad es la modificación de sus contraseñas (46,5%). Sin embargo, otros cambios a realizar por el usuario después de sufrir un incidente resultan igualmente destacables.

[21] https://www.itdigitalsecurity.es/endpoint/2020/03/el-troyano-ginp-se-vale-del-coronavirus-para-atacar-a-usuarios-espanoles

FIGURA 33. EVOLUCIÓN DE LOS CAMBIOS DE HÁBITOS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%)



Base: Usuarios que realizan algún cambio de hábitos tras sufrir un incidente de seguridad
Fuente: Panel hogares, ONTSI

Por ejemplo, actualizar las herramientas y configuraciones de seguridad y privacidad ya instaladas (34,5%), instalar por primera vez una herramienta de seguridad (16,9%) o cambiar las existentes (14,9%). Estas acciones denotan a un usuario más concienciado en hacer un uso de las herramientas de seguridad, ya que determinadas acciones, o en este caso, la pasividad del usuario al instalar o actualizar dichas herramientas tras sufrir un incidente podría conducir a nuevos incidentes.

Una de las medidas más demandas por las empresas a sus empleados a la hora de teletrabajar es la realización de copias de seguridad. El 27,6% de los usuarios ha comenzado a realizar copias de seguridad.

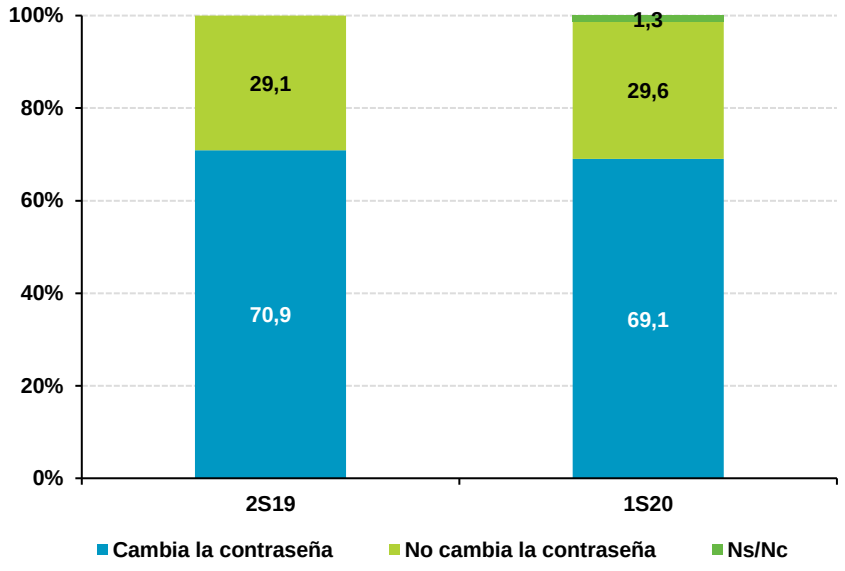
El 12,1% de los usuarios ya aprovecha los Mecanismos de Ayuda

Que hasta un 21,3% de los panelistas hayan dejado de realizar descargas en redes P2P, torrents, o descargas directas tras sufrir un incidente, puede deberse al gran auge que han tenido, por ejemplo, los servicios de *streaming*.

Tras verse en la tesitura de sufrir algún incidente de seguridad a la hora de descargar este tipo de contenido vía P2P, el usuario ha podido considerar con mayor motivo la suscripción a servicios de *streaming*, como se ha mencionado anteriormente.

Además, cabe destacar que un 12,1% de los usuarios ha hecho uso de mecanismos de ayudas, tales como realizar una denuncia en redes sociales o utilizar la línea telefónica gratuita[22] de ayuda en ciberseguridad (017) que INCIBE pone a disposición de empresas, ciudadanos, padres, menores y educadores ofreciendo un apoyo operativo ante la ocurrencia de ciberincidentes o ciberamenazas.

FIGURA 34. MODIFICACIÓN DE LA CONTRASEÑA DE LA RED INALÁMBRICA DEL HOGAR TRAS SOPECHAR DE UNA INTRUSIÓN WI-FI (%)



Base: Usuarios con conexión Wi-Fi propia que sospechan haber sufrido una intrusión en su red
Fuente: Panel hogares, ONTSI

Cambiar la contraseña por defecto de la red Wi-Fi es una de las medidas más recomendadas para su protección.

Uno de los primeros pasos que podría dar un atacante que se encontrase en las inmediaciones de la víctima, sería comprobar la seguridad del router Wi-Fi desde el cual el usuario se conecta a Internet. Si consigue vulnerar la contraseña de la red, podría suponer también el acceso a las carpetas y recursos compartidos en dicha red, como documentos privados, fotos y otra información de carácter personal.

El atacante podría analizar los dispositivos que se encuentran conectados en busca de nuevas vulnerabilidades en los mismos, e incluso realizar ataques desde dicha red amparándose en el hecho de que cualquier investigación posterior conducirían al dueño de la red como el perpetrador de las actividades ilegales realizadas. Por todo ello la contraseña de la red Wi-Fi debe ser lo más robusta que sea posible.

Como norma general es recomendable cambiar la contraseña de la red Wi-Fi y no utilizar aquella configurada por defecto. Esta recomendación se torna imprescindible si se ha sufrido una intrusión en la red del hogar, o se sospecha de ella.

Otra de las recomendaciones es la desactivación de la conexión vía WPS sino se va a hacer uso de ella o sustituir el pin por defecto, ya que uno de los vectores de ataque más empleados es el hallazgo del mismo mediante ataques de fuerza bruta.

[22] https://www.incibe.es/linea-de-ayuda-en-ciberseguridad

En la **FIGURA 34** se puede observar que el porcentaje de usuarios que no cambian la contraseña tras sospechar de una intrusión en su red (29,6%) apenas varía de un semestre a otro. Que un usuario no realice dicho cambio puede deberse a que desconoce el procedimiento a seguir para cambiar la contraseña o porque no son ellos mismos quienes administran la red Wi-Fi.

Sin embargo, ante la más mínima sospecha se debe cambiar la misma. Existen diversas *app* en el mercado con las que, de forma sencilla, el usuario puede identificar cuáles son los dispositivos conectados en su red y poder hallar fácilmente aquellos ilegítimos. Otra herramienta útil para evitar intrusiones en la red es la creación de listas blancas en la configuración del router. En dichas listas se especifica las direcciones físicas (MAC) de los dispositivos que tienen acceso a la red, negando el acceso a todos aquellos que no estén listados.

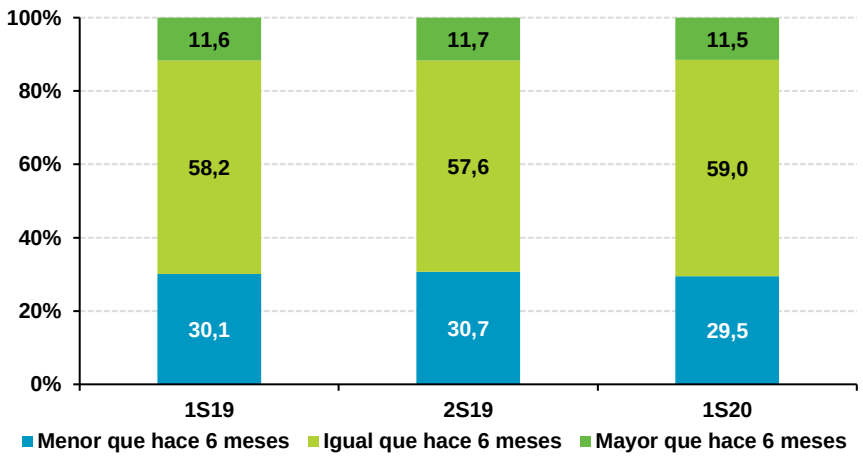
7 Confianza en el ámbito digital en los hogares españoles

En este último apartado se han recogido las valoraciones propias de los usuarios en cuanto a los riesgos que se corren al navegar por el mundo digital, la responsabilidad que conlleva estar conectado a la Red, y la confianza depositada en Internet y las Administraciones.

7.1 Evolución de la percepción de las incidencias y el riesgo

La percepción de los usuarios en cuanto a la cantidad y gravedad de incidencias de seguridad acontecidas en los últimos 6 meses se mantiene más o menos constante. Se observa un pequeño incremento en los usuarios que perciben que el número de incidencias es igual o mayor que hace 6 meses (+1,2 p.p.), lo cual va en sintonía con la percepción de los expertos de ciberseguridad[23] en relación con el aumento de incidencias en los últimos meses.

FIGURA 35. EVOLUCIÓN DE LA PERCEPCIÓN DE LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD (%)

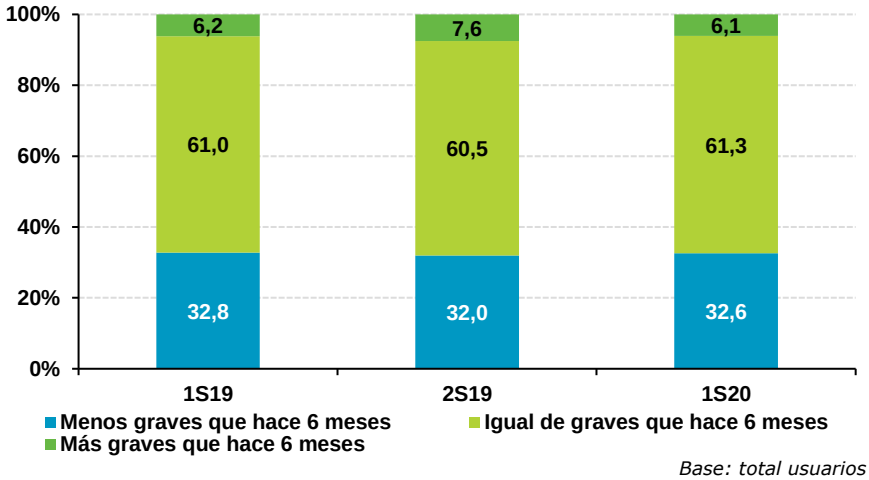


Base: total usuarios
Fuente: Panel hogares, ONTSI

[23] https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

Cabe destacar nuevamente que esta percepción es anterior al confinamiento, en un periodo en el cual aún los trámites online aún no eran imprescindibles para continuar con la rutina diaria, y antes también de que numerosos actores aprovechasen este hecho para la preparación de campañas dirigidas. A esto hay que sumar la preocupación de la sociedad por la COVID-19 y los cambios sociales introducidos durante este periodo. Este hecho puede afectar también a disminución de la sensación de riesgo e identificación de incidencias.

FIGURA 36. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

En cuanto a la gravedad de las incidencias, no se observan variaciones significativas, lo cual refuerza el hecho de que si bien la gravedad de las incidencias no se ha visto alterada durante dicho periodo, si lo han hecho los vectores de ataques por las que se producen las mismas, como se mencionaba anteriormente.

El perjuicio económico (35,6%) y la pérdida de privacidad (34,0%) siguen presentándose como los principales riesgos percibidos por los usuarios.

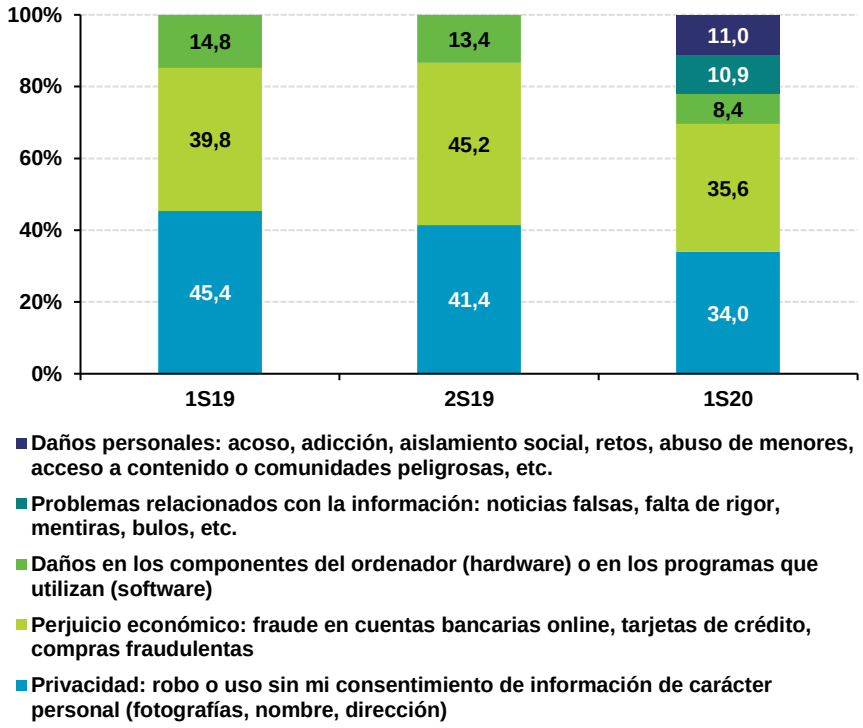
Cabe reseñar que un 11% de los usuarios perciben los daños personales, tales como el acoso, un riesgo a la hora de navegar en Internet. La adicción, especialmente al juego[24], es otro de los grandes problemas que pueden sufrir los usuario de Internet, acarreando consigo aislamiento social, problemas de salud y económicos, estos últimos repercutiendo en muchas ocasiones a sus propias familias. Por último, la adhesión a comunidades peligrosas, tales como sectas, también se han visto en aumento[25], usando la pandemia como reclamo para la captación.

En cuanto a los problemas relacionados con la información o *fake news*, son percibidos por el 10,9% de los internautas. Recordemos que el uso de redes sociales se situaba en torno al 75% y la mensajería instantánea en 70% (**FIGURA 2**). Son cifras que indican que un alto porcentaje de los panelistas emplea medios habitualmente usados de desinformación.

[24] https://www.heraldo.es/noticias/nacional/2020/04/01/el-gobierno-detecta-un-incremento-del-juego-online-durante-el-confinamiento-1367376.html

[25] https://www.elperiodico.com/es/sociedad/20200322/sectas-religion-gurus-aprovechan-coronavirus-7895498

FIGURA 37. EVOLUCIÓN DE LA PERCEPCIÓN DE LOS RIESGOS EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

En estos últimos meses, ha aparecido una ingente cantidad de bulos y noticias falsas sobre el coronavirus. Entre el 26 de febrero y el 26 de marzo fueron registrados en la red social Twitter más de 100.000 tuits (y 35 millones de impresiones) acerca del coronavirus que contenían información falsa[26]. Cabe destacar la importancia que tiene el hecho de contrastar la información que le llega al usuario, asegurándose de que esta venga de fuentes fidedignas. Esta información puede afectar al usuario en su ámbito social y económico, pudiendo sufrir estafas con dichos bulos, y aún más grave si cabe, podría poner en riesgo su salud cuando las *fake news* llevan consigo información sobre cómo prevenir o curar enfermedades utilizando remedios caseros muy peligrosos.

Nuevas campañas dirigidas a concienciar aún más a los usuarios de esta problemática podrían ser muy beneficiosas para aumentar el porcentaje de usuarios que sea capaz de identificar las noticias falsas.

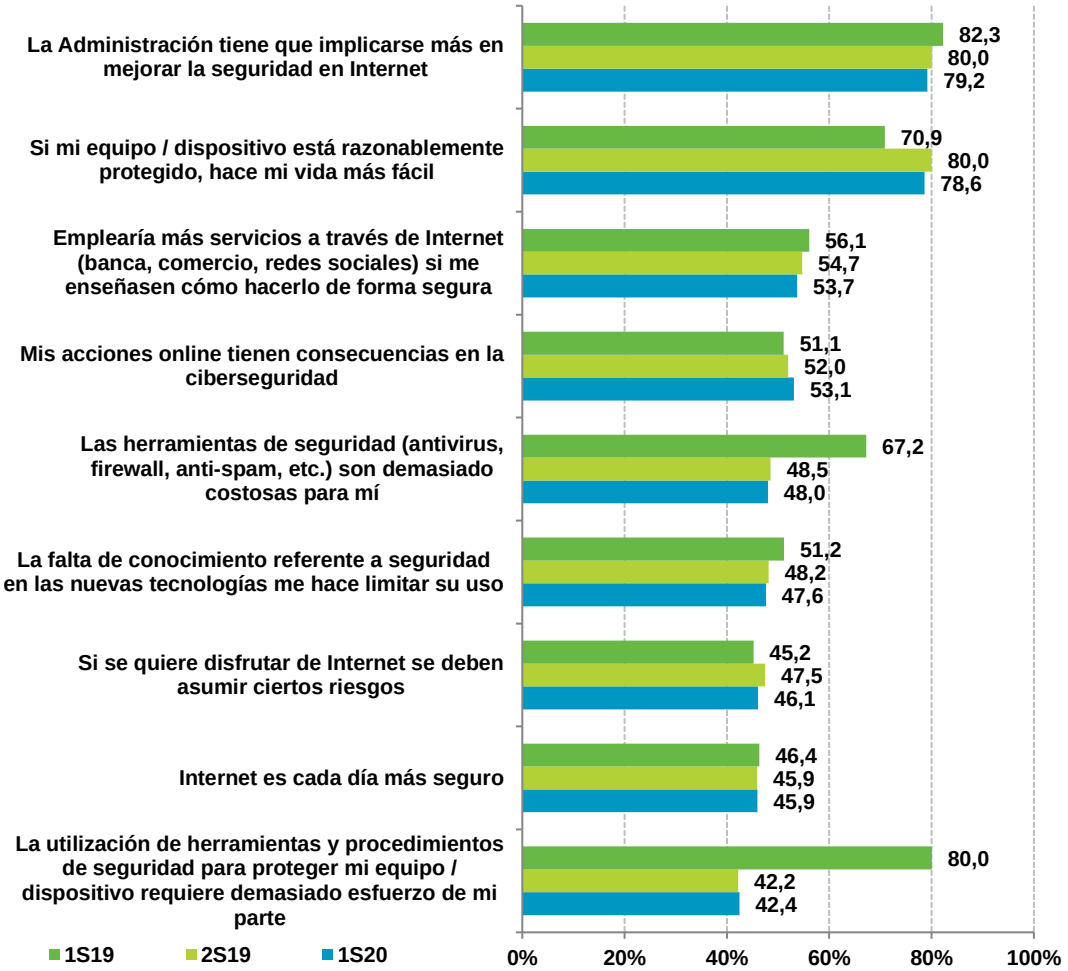
7.2 Opiniones sobre la seguridad en Internet

La opinión que pone de acuerdo a casi el 80% de los internautas es que la Administración debe implicarse más en la mejora de la seguridad en Internet, como podría ser mediante la impartición de cursos en línea sobre medidas y herramientas de seguridad, y su instalación, configuración y utilización, o sobre las principales amenazas de Internet y cómo prevenirlas y solventarlas.

[26] https://saludsinbulos.com/wp-content/uploads/2020/02/Informe-final-bulos-coronavirus.pdf.pdf

Otras formas de implicación podrían ser el desarrollo de aplicaciones gratuitas para analizar los equipos y dispositivos, mediante el envío de mensajes de concienciación sobre seguridad en línea, con artículos en los medios, o con la adaptación de leyes a los nuevos delitos tecnológicos. Si bien la tendencia es a la baja desde inicios de 2019, sigue siendo un dato muy elevado.

FIGURA 38. EVOLUCIÓN DE OPINIONES SOBRE LA SEGURIDAD EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Si se relacionan estos datos con los motivos que alegan los usuarios para no emplear determinadas medidas de seguridad (**FIGURA 10**), donde, de media, un 36,7% las considera no necesarias, un 17% no saben lo que son y un 12% no saben utilizarlas. Cada vez hay disponibles más herramientas gratuitas que son de gran utilidad para evitar incidencias, disponiendo la mayoría de ellas de tutoriales guiados para su configuración o uso, bien incrustado en la propia herramienta, o bien en la página de la empresa desarrolladora; por lo que las Administraciones solo deberían ocuparse de darles difusión en el caso de considerar interesante su implicación.

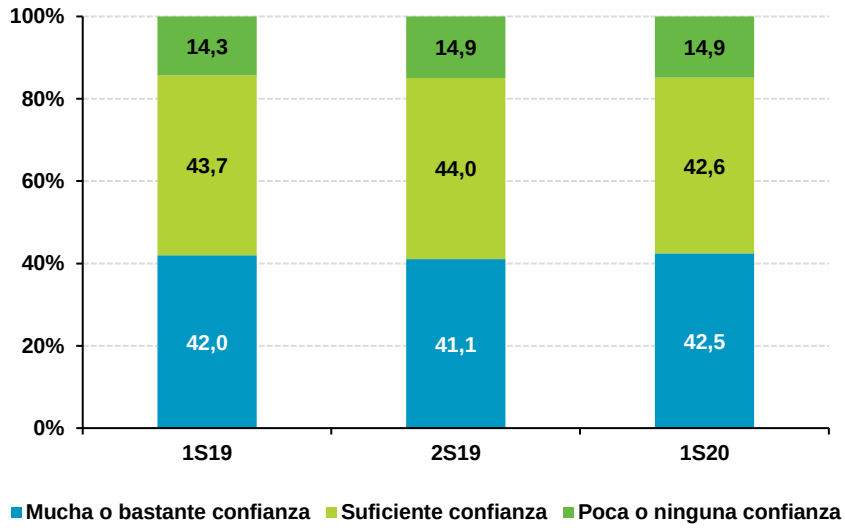
Por otro lado, hasta un 42,4% de los panelistas afirman que la utilización de herramientas y procedimientos de seguridad requieren demasiado esfuerzo por su parte, o achacan una falta de conocimiento que les limita su uso (47,6%).

Todo ello confirma el hecho de que hace falta una mayor implicación por parte de la Administración a la hora de fomentar y formar sobre las distintas medidas de seguridad, ya sean activas o pasivas, de las que el usuario puede disponer para hacer uso más seguro de Internet.

La concienciación del usuario sobre las repercusiones de sus acciones sobre la seguridad ha aumentado 2 p.p. desde principios del pasado año, lo que corrobora el incremento constante de usuarios que cada día están más sensibilizados. Un uso responsable de Internet evita, en mayor medida, sufrir un incidente de seguridad.

Por último, el 78,6% de los usuarios afirman que si su equipo está debidamente protegido le hace la vida más fácil y el porcentaje de usuarios que piensa que Internet es cada vez más seguro se estanca en el 45,9%.

FIGURA 39. EVOLUCIÓN DEL NIVEL DE CONFIANZA EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

El porcentaje de usuarios que tienen mucha o bastante confianza en Internet (42,5%) mantiene unos valores constantes desde el inicio de 2019, apreciándose un ligero estancamiento.

Si bien es cierto que Internet está dando pasos constantes en ser un lugar cada vez más seguro (como por ejemplo la reducción del uso de servicios más propensos a vulnerabilidades como SMB o Telnet),[27] no se debe perder de vista que los ciberdelincuentes también continúan adaptándose e ideando nuevos métodos para lograr llevar a cabo sus intereses.

A pesar de ello, tan solo el 14,9% de los usuarios presentan una confianza baja o inexistente en Internet.

[27] https://www.rapid7.com/research/report/nicer-2020/

8 Conclusiones

La pandemia mundial provocada por la COVID-19 ha generado un impacto sin precedentes tanto a nivel económico como social. Este informe cubre tanto la percepción de los usuarios antes del confinamiento como el estado de los ordenadores del hogar y dispositivos móviles tras el mismo. Es por ello por lo que es el primer estudio en el que queda reflejado este contexto en cuanto al uso de servicios, medidas de seguridad, hábitos prudentes y tipos de incidentes que puede sufrir un usuario en Internet.

Durante este pasado semestre se han apreciado algunos cambios significativos en los hábitos de consumo de los usuarios, como por ejemplo, las plataformas de *streaming* o el uso de servicios en línea que previamente se realizaban presencialmente, como las gestiones bancarias.

Las medidas de seguridad han variado sustancialmente. Ya sea como preludio y posterior cambio a la modalidad de teletrabajo - incluso previo a la declaración del Estado de Alarma – o a consecuencia de la modernización de los trámites electrónicos por parte también de la Administración Pública, se ha percibido el aumento del uso del DNI electrónico y certificados digitales. En concreto los datos reflejarían que la Administración Pública ha impulsado significativamente el uso de los certificados digitales y el uso de la administración electrónica en numerosos ayuntamientos.

Las incidencias de seguridad percibidas por los usuarios (excepto algunas infecciones por *malware*) se han mantenido constantes respecto anteriores semestres según la percepción de los usuarios. Dado que estos datos corresponden al estado previo al confinamiento – durante el cual estudios externos corroboran que hubo un aumento considerable de las incidencias de seguridad - una posible explicación a esta menor percepción de incidencias de seguridad podría ser la pequeña mejora en cuanto a la concienciación y responsabilidad del usuario, como se ha hecho hincapié a lo largo de todo el estudio. Cabe destacar que los vectores de ataque de dichas incidencias de seguridad han variado durante el último semestre, priorizándose las campañas de *phishing* para el robo de credenciales y los fraudes. En ambas, los ciberdelincuentes han usado la COVID-19 como reclamo.

La invitación a páginas webs sospechosas o la recepción de *spam* siguen siendo los principales incidentes de seguridad; también los usuarios reportan ataques a su información personal mediante ingeniería social o sextorsión.

La confianza en el ámbito digital también se ve alterada. Los usuarios perciben más riesgo contra sus datos personales y la proliferación de *fake news* a razón del coronavirus, lo que hace que usuario no tenga la plena confianza que debería tener a la hora de navegar por la red.

Por otro lado, los usuarios demandan más implicación por parte de la Administración. Si bien se ha destacado el hecho de que el usuario, en líneas generales, está más concienciado de hacer un uso más responsable de Internet, y esto en parte puede deberse a la acción de formación por parte de las empresas o la propia Administración, una parte notable de los usuarios alegan un

completo desconocimiento sobre el uso de determinadas herramientas o incluso desconocen la existencia de las mismas. Es ahí, donde la Administración debería centrar sus esfuerzos para corregir este desequilibrio impartiendo cursos y *webinars* sobre las herramientas de seguridad y su uso.

Muchas empresas se han visto forzadas a implementar la modalidad de teletrabajo con premura debido a la situación devenida. Gracias a esta modalidad de trabajo han podido proseguir con su actividad económica. Sin embargo, también ha podido acarrear una falta de previsión y el establecimiento de protocolos en las mismas para que sus empleados usen las redes corporativas desde equipos seguros y de forma remota. El efecto de estas medidas se ha podido observar en los datos reales recabados de los dispositivos de los usuarios por el sistema Pinkerton.

Algunas recomendaciones para un correcto desempeño del teletrabajo son: el uso exclusivo de equipamiento de la empresa, contraseñas para iniciar sesión y desbloquear el equipo, cuentas de usuarios con el nivel de privilegios adecuado, software antivirus y firewall, evitar la instalación de programas o aplicaciones ajenas al entorno laboral, el cifrado de los dispositivos de almacenamiento para evitar el acceso a la información en caso de robo o pérdida y el cifrado de las comunicaciones y conexiones a recursos de la empresa entre otras.

A lo largo de los próximos meses tanto las empresas como la Administración Pública se enfrentan a grandes retos. Si la modalidad de teletrabajo ha llegado para quedarse, resulta necesario invertir en formación tanto a empresas como a empleados para que la experiencia sea satisfactoria y segura. Además, esta necesidad puede provocar que se den pasos hacia delante para que la Transformación Digital se implante con mayor brevedad en las empresas.

Índice de figuras

FIGURA 1. LINEA DE TIEMPO REPRESENTATIVA DEL CONTEXTO DEL SEMESTRE 3
FIGURA 2. USO DECLARADO DE SERVICIOS DE INTERNET (%) 4
FIGURA 3. USO DE MENSAJERÍA INSTANTÁNEA Y CHAT SEGÚN LA ACTIVIDAD REALIZADA POR LOS USUARIOS (%) 5
FIGURA 4. ACCESO A CURSOS Y FORMACIÓN ONLINE SEGÚN LA ACTIVIDAD REALIZADA POR LOS USUARIOS (%) 6
FIGURA 5. USO REAL DE MEDIDAS DE SEGURIDAD EN EL ORDENADOR DEL HOGAR (%) 7
FIGURA 6. SISTEMAS OPERATIVOS DECLARADOS EN LOS ORDENADORES DEL HOGAR (%) 8
FIGURA 7. USO REAL DE MEDIDAS DE SEGURIDAD EN DISPOSITIVOS ANDROID (%) 9
FIGURA 8. NIVEL DE PRIVILEGIOS REAL EN PERFILES EN DISPOSITIVOS ANDROID (%) 11
FIGURA 9. VERSIONES DE ANDROID EN DISPOSTIVOS MÓVILES (%) 11
FIGURA 10. MOTIVOS DE NO UTILIZACIÓN DE MEDIDAS DE SEGURIDAD (%) 13
FIGURA 11. MEDIDAS DE SEGURIDAD AUTOMATIZABLES EN EL ORDENADOR DEL HOGAR SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%) 14
FIGURA 12. MEDIDAS DE SEGURIDAD ACTIVAS EN EL ORDENADOR DEL HOGAR SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%) 14
FIGURA 13. EVOLUCIÓN DE LA ADOPCIÓN CONSCIENTE DE CONDUCTAS DE RIESGO (%) 15
FIGURA 14. REALIZACIÓN CONSCIENTE DE ALGUNA CONDUCTA DE RIESGO SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%) 16
FIGURA 15. DESCARGAS EN REDES P2P SEGÚN TRABAJADORES Y NO TRABAJADORES (%) ... 17
FIGURA 16. DESCARGAS EN INTERNET SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%) 17
FIGURA 17. INSTALACIÓN DE PROGRAMAS EN EL ORDENADOR DEL HOGAR SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%) 18
FIGURA 18. DESCARGA DE APLICACIONES EN DISPOSITIVOS ANDROID (%) 19
FIGURA 19. EVOLUCIÓN DEL ESTADO DE OPCIONES DE SEGURIDAD EN DISPOSITIVOS ANDROID (%) 19
FIGURA 20. ESTADO DE LA OPCIÓN DE INSTALACIÓN DESDE FUENTES DESCONOCIDAS ENTRE USUARIOS QUE DESCARGAN APLICACIONES DESDE REPOSITORIOS NO OFICIALES SEGÚN PERSONAS TRABAJADORAS Y NO TRABAJADORAS (%) 20
FIGURA 21. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%) 22
FIGURA 22. EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%) 23
FIGURA 23. ESTADO REAL DE INFECCIÓN EN EL ORDENADOR DEL HOGAR (%) 25
FIGURA 24. PELIGROSIDAD DEL MALWARE EN EL ORDENADOR DEL HOGAR (%) 25
FIGURA 25. EVOLUCIÓN DEL MALWARE EN EL ORDENADOR DEL HOGAR (%) 26
FIGURA 26. ESTADO REAL DE INFECCIÓN EN DISPOSITIVOS ANDROID (%) 27
FIGURA 27. PELIGROSIDAD DEL MALWARE EN DISPOSITIVOS ANDROID (%) 28
FIGURA 28. EVOLUCIÓN DEL MALWARE EN DISPOSITIVOS ANDROID (%) 29
FIGURA 29. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%) 30
FIGURA 30. EVOLUCIÓN DE LA MANIFESTACIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%) . 30
FIGURA 31. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN EL ORDENADOR DEL HOGAR (%) 31
FIGURA 32. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN DISPOSITIVOS ANDROID (%) 32
FIGURA 33. EVOLUCIÓN DE LOS CAMBIOS DE HÁBITOS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD (%) 33
FIGURA 34. MODIFICACIÓN DE LA CONTRASEÑA DE LA RED INALÁMBRICA DEL HOGAR TRAS SOPECHAR DE UNA INTRUSIÓN WI-FI (%) 34
FIGURA 35. EVOLUCIÓN DE LA PERCEPCIÓN DE LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD (%) 35
FIGURA 36. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%) 36
FIGURA 37. EVOLUCIÓN DE LA PERCEPCIÓN DE LOS RIESGOS EN INTERNET (%) 37
FIGURA 38. EVOLUCIÓN DE OPINIONES SOBRE LA SEGURIDAD EN INTERNET (%) 38
FIGURA 39. EVOLUCIÓN DEL NIVEL DE CONFIANZA EN INTERNET (%) 39

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 las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es:

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

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

Se quiere agradecer su colaboración en la relación de este estudio a:

HISPASEC GfK

Asimismo, se quiere también agradecer la colaboración de:

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Reservados todos los derechos. Se permite su copia y distribución por cualquier medio siempre que se mantenga el reconocimiento de sus autores, no se haga uso comercial de las obras y no se realice ninguna modificación de las mismas.

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

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