OBSERVACIBER

CÓMO SE PROTEGE LA CIUDADANÍA ANTE LOS CIBERRIESGOS

ESTUDIO SOBRE PERCEPCIÓN Y NIVEL DE CONFIANZA EN ESPAÑA

Edición Junio 2021

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
ontsi | incibe_ | OBSERVACIBER

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

CÓMO SE PROTEGE LA CIUDADANÍA ANTE LOS CIBERRIESGOS. ESTUDIO SOBRE PERCEPCIÓN Y NIVEL DE CONFIANZA EN ESPAÑA

El Observatorio Nacional de Tecnología y Sociedad (ONTSI) realiza semestralmente el estudio "Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España" (anteriormente denominado "Estudio sobre la ciberseguridad y confianza del ciudadano en la red") 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 segundo 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 se mantiene tanto en los equipos informáticos como en 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 70 motores antivirus.

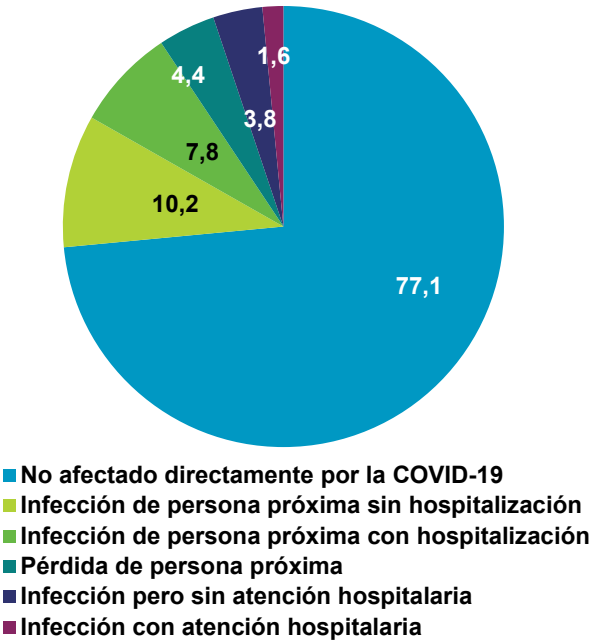
1 Contexto del estudio

Este estudio se realiza sobre una base de datos recogidos desde julio hasta diciembre de 2020, ambos meses inclusive. En esos meses, la sociedad española ha experimentado cambios significativos en su rutina, y parte del objetivo de este análisis es determinar el efecto de estos cambios en los hábitos de ciberseguridad.

Como primer punto a tener en cuenta para la interpretación de los datos del estudio se encuentra la situación experimentada por los panelistas frente a la COVID-19.

En concreto el 22,9% de los panelistas afirma haber sido afectado por una de las siguientes causas: infección (ya sea propia o de una persona próxima), requiriendo en el 9,4% ingreso hospitalario (1,6% casos propios, 7,8% casos de personas próximas) y pérdida de personas próximas (4,4%).

FIGURA 1. SITUACIONES VIVIDAS POR LOS PANELISTAS DURANTE LA COVID-19



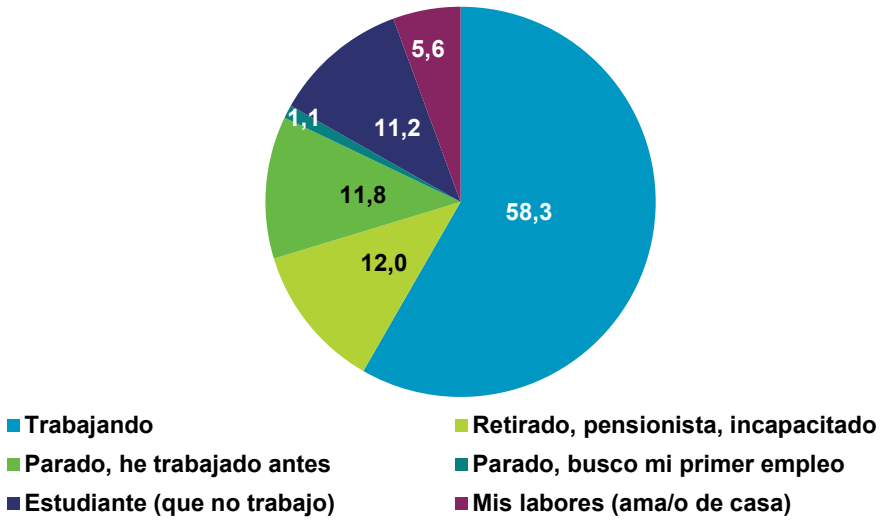
Base: Total usuarios
Fuente: Panel hogares, ONTSI
**datos recogidos durante julio y agosto de 2020*

Además, debe considerarse nuevamente la situación laboral de los panelistas, dado que las diversas restricciones territoriales han limitado la movilidad y ello ha dado pie a que muchas empresas mantuviesen la situación de teletrabajo. Este hecho, unido con factores personales como los mencionados con anterioridad e incluso otros propios del alejamiento social, influye indiscutiblemente a la rutina profesional. Es por ello que las empresas suelen integrar como parte de sus planes de incorporación cursos de concienciación e incorporación progresiva al trabajo.

En adelante se considera la población formada por los trabajadores, dado que interesa particularmente conocer las variaciones en las conductas digitales frente al teletrabajo de los mismos, para muchos prolongado. En este semestre en torno al 58,3% de los participantes son trabajadores, frente al 41,7% que forma parte de la población no trabajadora. Cabe preguntarse si los hábitos han variado para el conjunto de la muestra, y por ello a lo largo del estudio se mantendrá la distinción entre población trabajadora y no trabajadora para las comprobaciones puntuales que se estimen oportunas.

De igual forma, las restricciones territoriales han podido impulsar el hábito digital en todos los participantes, acompañado, en algunos casos, de la adopción de buenas prácticas en ciberseguridad.

FIGURA 2. CONTEXTO LABORAL DE LOS PANELISTAS

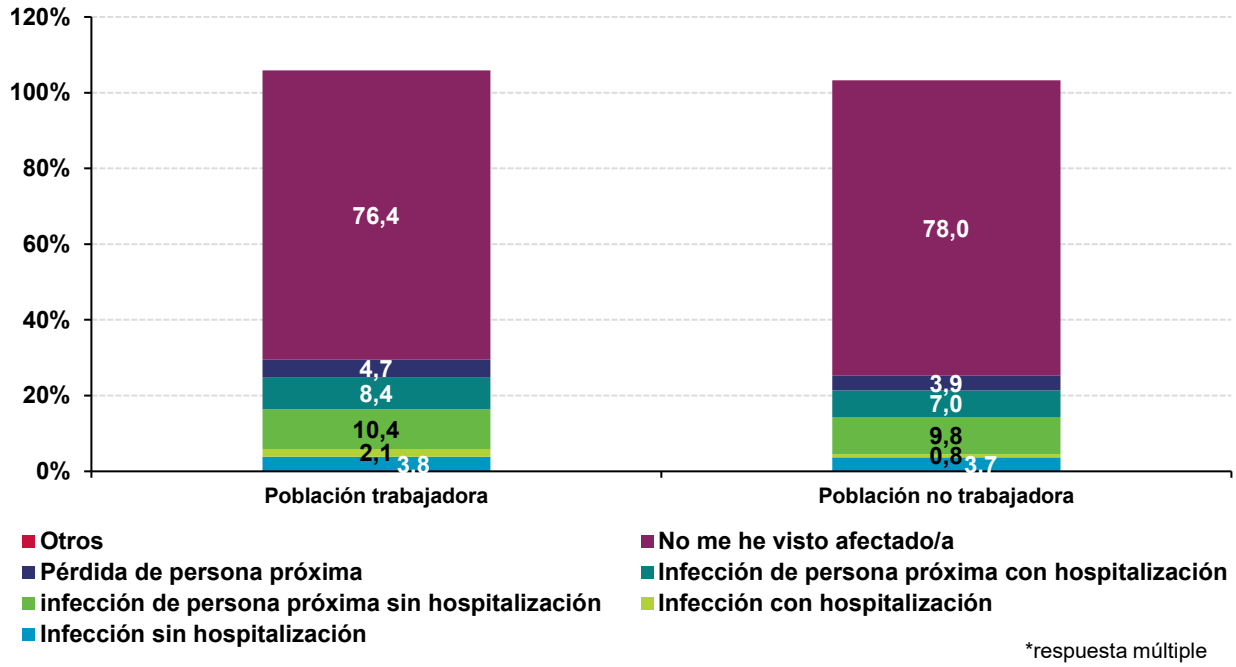


Base: Total usuarios
Fuente: Panel hogares, ONTSI

Finalmente, si desglosamos las situaciones de influencia respecto a la COVID-19 atendiendo a los conjuntos de población trabajadora o no trabajadora, comprobamos que los porcentajes son muy similares.

Por lo tanto, dichas variables relacionadas con la COVID-19 afectan por igual a ambos conjuntos para este estudio.

FIGURA 3. AFECCIONES DE LOS PANELISTAS POR TIPO DE POBLACIÓN



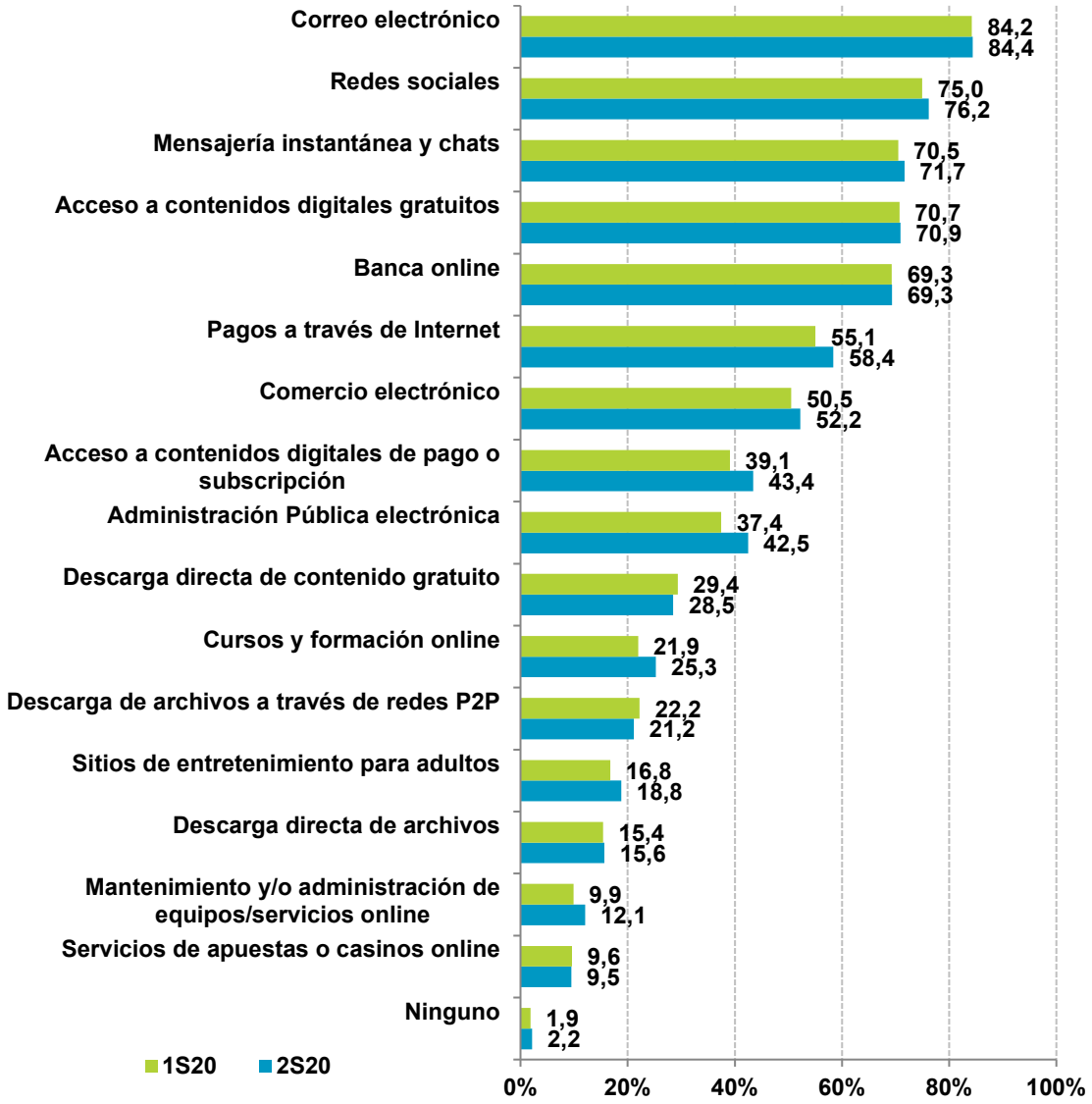
*respuesta múltiple

Base: Total usuarios
Fuente: Panel hogares, ONTSI

2 Usos de Internet

Durante este semestre siguen predominando los servicios de correo electrónico, redes sociales y mensajería instantánea. Como se aprecia en el gráfico de uso declarado de servicios en Internet, las diferencias no son significativas respecto a semestres anteriores, aumentando una vez más la mensajería instantánea y los chats. Se destaca no obstante el aumento de los pagos a través de Internet, que pasa a un 58,4% (3,3 puntos porcentuales más que el semestre anterior-en adelante p.p.-), el acceso a los contenidos digitales de pago, un 43,4% (4,3 p.p.), los trámites a través de la administración pública electrónica, un 42,5% (5,1 p.p.), el mantenimiento de los equipos online, un 12,1% (2,2 p.p.) y finalmente la formación online, 25,3% (3,4 p.p.).

FIGURA 4. USO DECLARADO DE SERVICIOS DE INTERNET (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

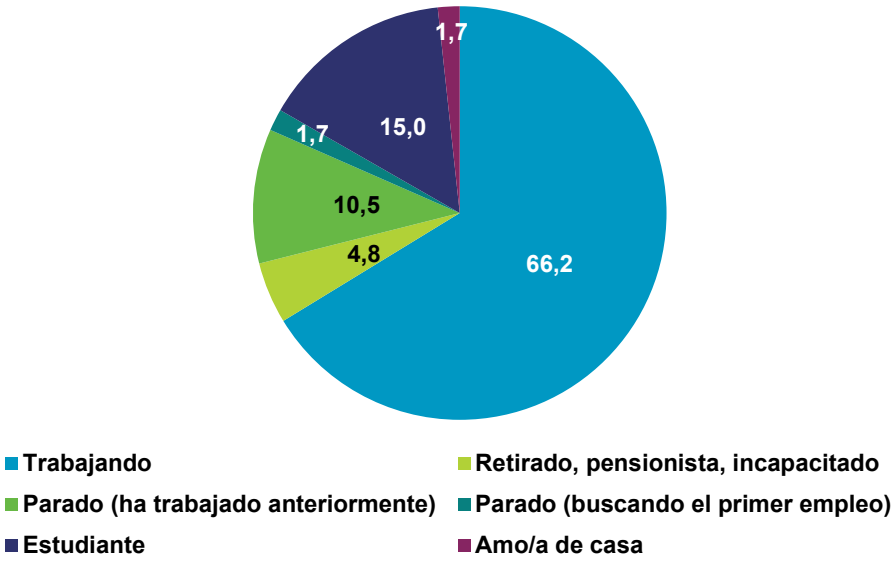
Se observa un incremento en los trámites con la administración (a través principalmente de certificados digitales de firma electrónica).

En algunos casos, estos trámites han podido adaptarse a las circunstancias para emplear otras vías de autenticación para los usuarios.

Se aprecia también un ligero descenso, de las descargas a través de redes P2P y la descarga de contenido gratuito. Estos datos se alinean con los resultados del semestre anterior, donde ya se veía reflejado el crecimiento del consumo en plataformas digitales de pago como Netflix [1], HBO y Disney+ entre otras [2]. Muy probablemente el hábito en el uso de este tipo de servicios pueda traer consigo una clara bajada en el acceso a webs fraudulentas y de piratería.

Por otra parte, de los usuarios que han realizado cursos y formación online, la mayoría de ellos se encuentran trabajando o son estudiantes. En este semestre se ha considerado también el acceso a cursos por parte de amo/a de casa, siendo dicho porcentaje equivalente al de parados que buscan su primer empleo (1,7%).

FIGURA 5. ACCESO A CURSOS Y FORMACIÓN ONLINE SEGÚN LA ACTIVIDAD REALIZADA POR LOS USUARIOS (%)



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

ACCESO A CURSOS Y FORMACIÓN ONLINE (DATO DECLARADO)

66,2%
TRABAJADORES

15%
ESTUDIANTES

12,2%
PARADOS

6,5%
OTROS

Con respecto a datos del semestre anterior cabe destacar que se reduce la participación en cursos del conjunto de retirados, pensionistas y/o incapacitados. En concreto baja 8 p.p., situándose en el 4,8%. Como dato positivo, el número de estudiantes involucrado en cursos online aumenta al 15% (crecimiento de 11,2 p.p.).

[1] https://www.elperiodico.com/es/economia/20201021/netflix-gana-un-188-mas-en-tercer-trimestre-8166612

[2] https://www.elespanol.com/invertia/medios/20200925/netflix-hbo-disney-disparan-pandemia-millones-espana/523198772_0.html

Sin embargo en diversos centros educativos se ha optado por la modalidad semipresencial, pudiendo afectar este hecho a los resultados.

3 Medidas de seguridad

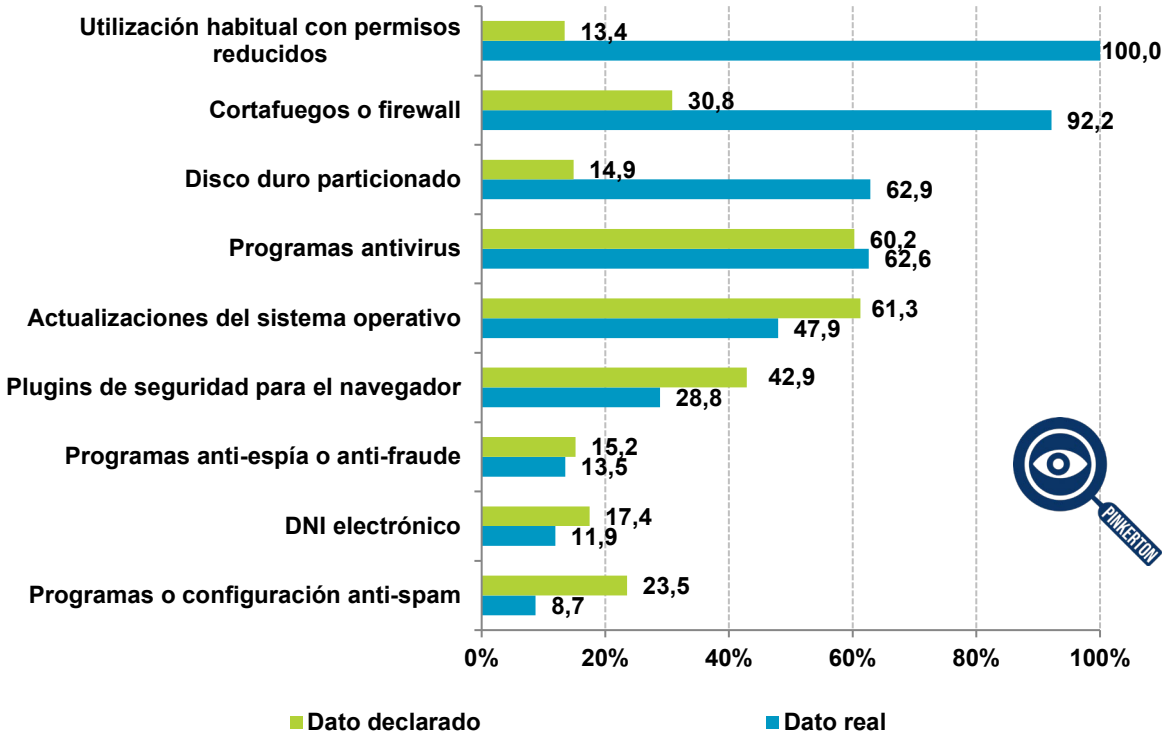
En esta sección se analizan las medidas de seguridad utilizadas por los panelistas españoles durante el segundo semestre de 2020.

Esta parte del estudio recoge tanto los resultados de las encuestas como la información recopilada mediante el análisis real de los ordenadores del hogar y los dispositivos Android (tabletas y teléfonos inteligentes), obtenida por medio de la herramienta Pinkerton.

3.1 Ordenadores en el hogar

En esta oleada se contrasta el uso declarado de medidas de seguridad con el uso real identificado durante el escaneo.

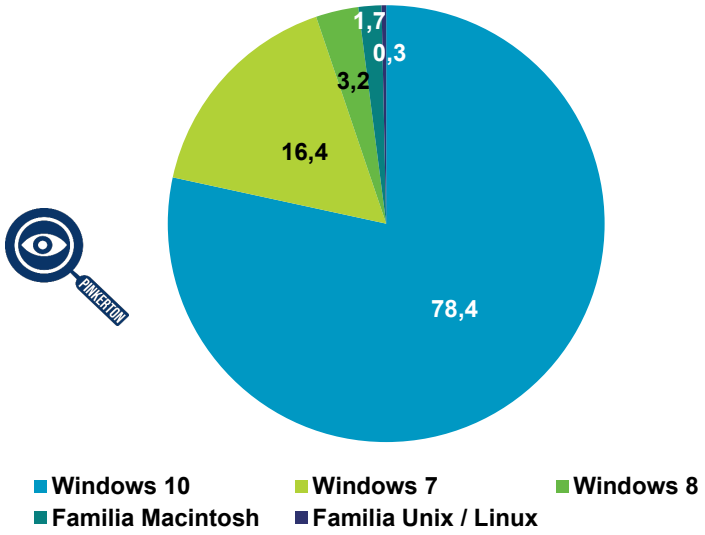
FIGURA 6. USO DECLARADO VS REAL DE MEDIDAS DE SEGURIDAD EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

Destacan claramente tres medidas: la utilización de permisos reducidos, el uso de cortafuegos y el particionado de disco duro. Dichas medidas pueden ser imperceptibles para muchos usuarios, ya que vienen integradas en los sistemas operativos modernos, y habitualmente activadas por defecto. Es el caso por ejemplo de los sistemas operativos Windows, plataforma predominante en el estudio, siendo escogida por el 98% de los panelistas, frente al 1,7% y 0,3% que ocupan las familias Macintosh y Unix/Linux, respectivamente.

FIGURA 7. SISTEMAS OPERATIVOS EN LOS ORDENADORES DEL HOGAR (%) – DATO REAL



Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

De igual forma se da la situación opuesta: medidas que el usuario entiende utilizadas pero que sin embargo no se encuentran en el equipo escaneado. Es el caso, por ejemplo, de los programas antifraude, anti-espía, anti-spam o antivirus. Probablemente sean términos que aún hoy día causan confusión a muchos usuarios, pese a que hay numerosa información disponible para el ciudadano a través del portal de la Oficina de Seguridad del Internauta (OSI)[3].

Respecto a la variación entre el dato declarado del uso del DNIe y el dato real recabado de los equipos, puede deberse a varios factores, entre los que se encuentran: la posible utilización de otro equipo para los trámites que involucren el DNI electrónico, la posible confusión entre DNIe y certificado digital, o bien la instalación incompleta/incorrecta del software empleado para el DNIe por parte del usuario. Este software podría haber sido configurado parcialmente y no usado finalmente.

3.2 Dispositivos Android

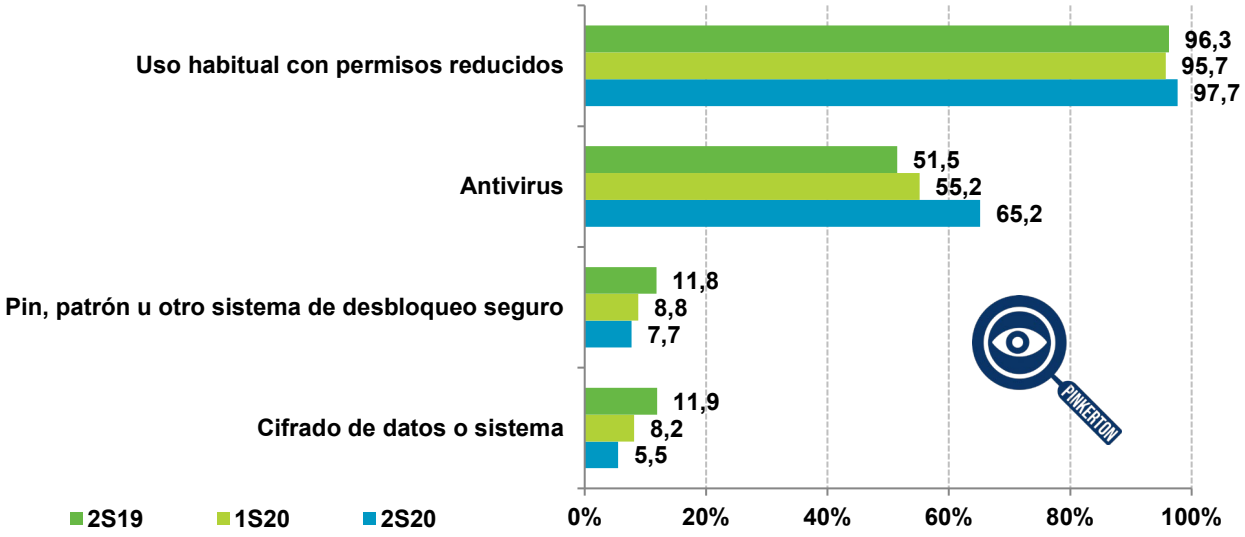
Se mantiene en este semestre el análisis del uso real de medidas de seguridad en dispositivos Android considerando cuatro bloques principales: uso habitual con permisos reducidos, uso de antivirus, la utilización de pin, patrón u otro sistema de desbloqueo seguro y el cifrado de datos o sistema.

Durante este semestre se ha observado una mejoría en el uso habitual con permisos reducidos. No obstante dicho valor ya era alto, superando el 90% en las últimas oleadas. Los últimos datos reflejan que el 97,7% de los usuarios de Android tienen permisos reducidos. Recordemos que en el caso PC se llega al 100%, pero que, no obstante, los resultados de la seguridad para los

[3] Guía para aprender a identificar fraudes online: https://www.osi.es/es/guia-fraudes-online

dispositivos móviles siguen aventajando a los de PC, como veremos más adelante en este mismo informe.
En general la mejoría de seguridad en los dispositivos Android se observa en el uso habitual con permisos reducidos y también en el uso de antivirus. Sin embargo el uso de mecanismos de control de acceso (pin, patrón, desbloqueo seguro) o el cifrado de los datos continúan en descenso. Estos dos últimos bloques son muy importantes para proteger la privacidad, como se indica desde la Agencia Española de Protección de Datos (AEPD), en su catálogo de medidas preventivas y herramientas para proteger la privacidad[4].

FIGURA 8. USO REAL DE MEDIDAS DE SEGURIDAD EN DISPOSITIVOS ANDROID (%)



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

Entre los mecanismos de control de acceso más populares para dispositivos móviles destacan aquellos basados en biometría (rasgos únicos del individuo, como la huella dactilar). No solo son fáciles de usar (p.ej. el reconocimiento facial sólo requiere que miremos la cámara del dispositivo), sino que, además, se basan en una característica propia de la persona, no en un PIN/contraseña que podríamos olvidar o que nos podrían robar.

Estos mecanismos, bien configurados, permiten facilitar el uso de tecnologías digitales con seguridad a personas que podrían olvidar o extraviar fácilmente los códigos de acceso[5].

Finalmente, la última versión de Android hasta la fecha (Android 11), incorpora mejoras de seguridad y privacidad[6]. Por ejemplo, permite que los usuarios proporcionen permisos a las aplicaciones por sesiones, en lugar de mantenerlos durante el tiempo de vida de la aplicación. Esta característica hace que el usuario sea más consciente de los permisos que necesita la aplicación, aunque puede darse igualmente el efecto contrario, y es que se normalice el aceptar los permisos sin prestarles demasiada atención.

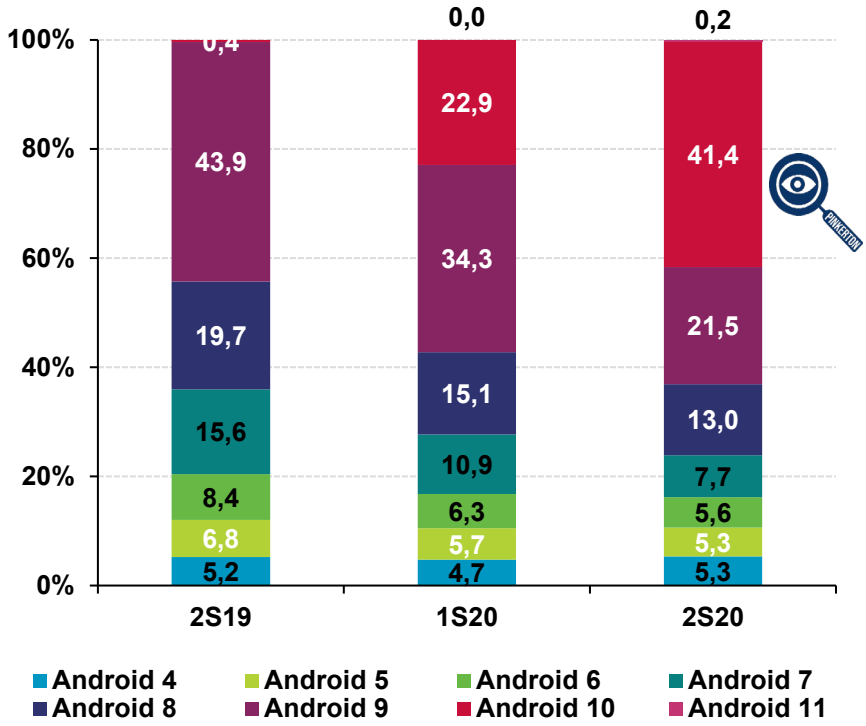
[4] https://www.aepd.es/es/areas-de-actuacion/recomendaciones/medidas

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

[6] https://www.android.com/safety/

Otra característica interesante es que Android 11 resetea aquellas aplicaciones que no se usan en un tiempo, incluyendo los permisos concedidos a aplicaciones que no se usen. Por lo que aumenta el control sobre los recursos del dispositivo.

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



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

Google lanzó Android 11 en septiembre de 2020, por lo que en el momento del estudio sólo un 0,2% de los panelistas disponía de Android 11.

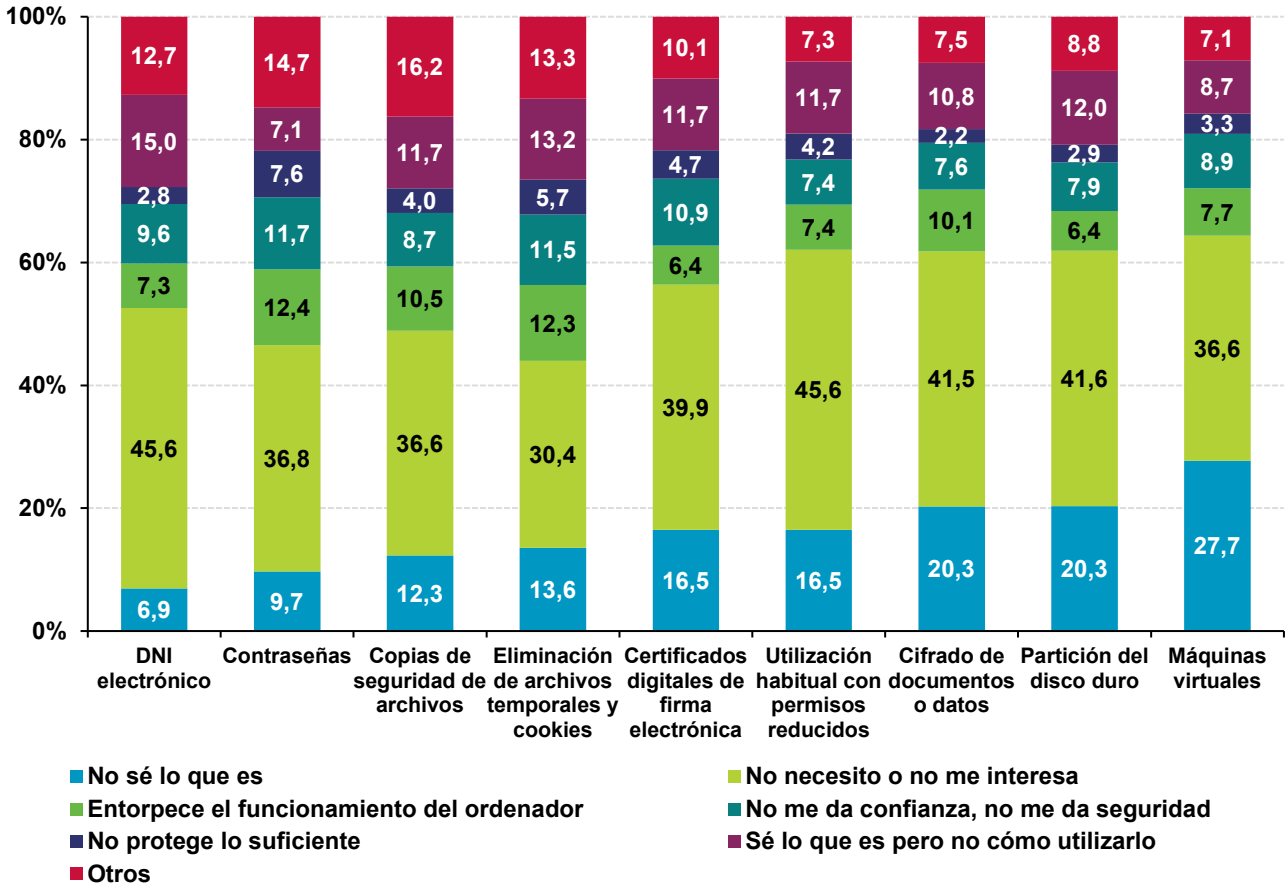
Esto coincide con la situación actual, en la que la cuota de mercado de Android 10 se sitúa en torno al 44,47%[7], rondando en este estudio el 41,4%. Por lo tanto las características mencionadas no afectan significativamente a los resultados del informe.

3.3 No utilización de medidas de seguridad

En este apartado se analizan los motivos de la no utilización de las medidas de seguridad sujetas al estudio. Las declaraciones de los panelistas se recogen a continuación.

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

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

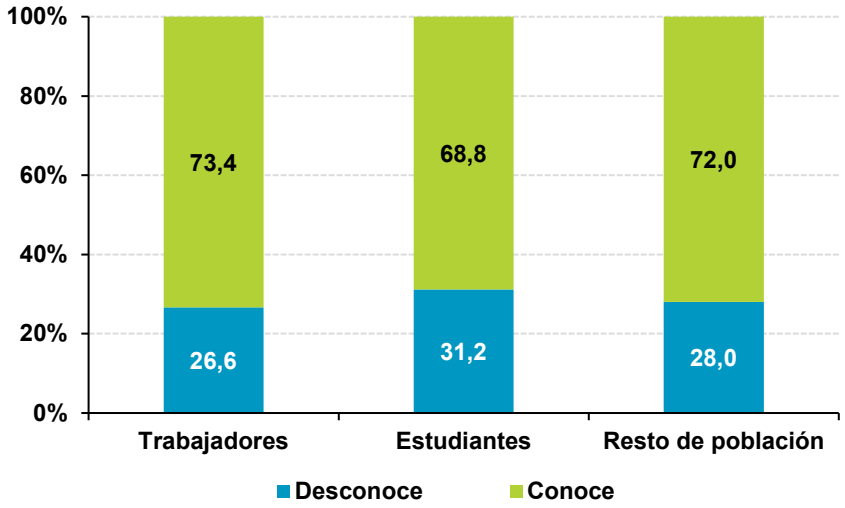
Comenzando por los motivos de no utilización por desconocimiento (no saber qué es), al igual que ya ocurría en el semestre anterior las máquinas virtuales siguen siendo un recurso desconocido para un porcentaje significativo de usuarios (27,7%), aunque la diferencia porcentual disminuye un 1,8 p.p. Cabría pensar que tal vez la única vía para paliar este hecho sea a través de la formación, dado que es un concepto que por lo general es difícil de asimilar para personas cuyo ámbito se aleja del uso habitual de TIC.

La siguiente figura desgrana el porcentaje de panelistas que ha indicado no emplear una máquina virtual argumentando como motivo el no saber lo que es, atendiendo a tres sectores: trabajadores, estudiantes y resto de población.

Resulta muy llamativo que el grado de desconocimiento de la población de estudiantes respecto a las máquinas virtuales sea mayor que el que tiene la población trabajadora.

Aunque el porcentaje de trabajadores que desconoce el concepto es menor respecto al resto de la población, siguen siendo cifras altas. Más teniendo en cuenta que tanto los trabajadores como los estudiantes podrían verse muy beneficiados por el uso de máquinas virtuales, no sólo desde el punto de vista de la seguridad.

FIGURA 11. PANELISTAS QUE DESCONOCEN QUÉ ES UNA MÁQUINA VIRTUAL (%)

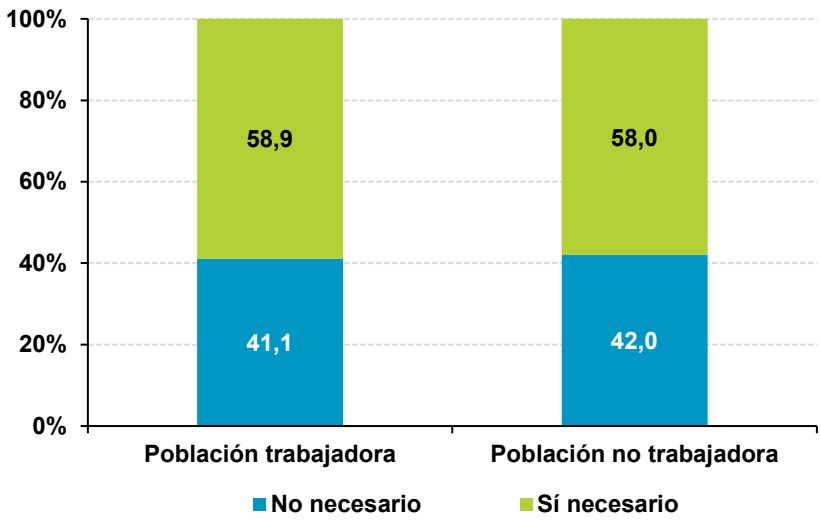


Base: Usuarios que no utilizan máquinas virtuales
Fuente: Panel hogares, ONTSI

Volviendo a la FIGURA 10, se percibe un descenso general del desconocimiento de las medidas de seguridad como motivo de no uso, aumentando sólo en el caso de la partición del disco duro, que sube un 1,9 p.p. respecto al semestre anterior.

El motivo más frecuente de la no utilización de las medidas continúa siendo el no considerarlas necesarias.

FIGURA 12. PANELISTAS QUE CONSIDERAN NECESARIO EL CIFRADO (%)



Base: Usuarios que no utilizan cifrado
Fuente: Panel hogares, ONTSI

Por ejemplo, el 41,5% de los panelistas creen innecesario el cifrado de documentos o datos. En este caso si analizamos los datos para las poblaciones trabajadora y no trabajadora, vemos que en cada conjunto poblacional el desconocimiento es casi equivalente (0,9 p.p. de diferencia). En este caso era de esperar que entre el grupo de trabajadores se identificase mayor unanimidad en cuanto a la necesidad del cifrado.

Este hecho podría resultar preocupante en cuanto a que es un requisito para la adecuación de la norma ISO 27001 (Gestión de seguridad de la información), y que precisamente pretende proteger a las organizaciones en caso de fugas/brechas de información. Cifrar los datos es una medida preventiva destinada a dificultar su comprensión y análisis en caso de acceso por parte de terceros no autorizados.

También el Esquema Nacional de Ciberseguridad (ENS) recoge los criterios para el uso del cifrado como parte del Anexo II (Medidas de seguridad)[8]. En particular, mientras que para los niveles bajo-medio no aplica, para el nivel alto sí es requisito. Existen guías de seguridad, como la CCN-STIC 807[9], que detallan extensamente tanto los requisitos de cifrado como los mecanismos y los algoritmos de cifrado recomendados.

Las medidas de cifrado aplican tanto a plataformas PC como a dispositivos móviles, y de hecho ya se encuentran presentes de forma nativa en múltiples plataformas. No obstante, para aquellas plataformas que dependan de la instalación de herramientas adicionales, desde la Oficina de Seguridad del Internauta (OSI) se indican varios consejos y procedimientos para cifrar los datos[10].

3.4 Medidas automatizables y activas

Una forma de clasificar las medidas de seguridad es atendiendo a su posible automatización o intervención del usuario en su configuración. Así, consideramos que las medidas automatizables son aquellas que, por lo general, no requieren de ninguna acción por parte del usuario (pasivas), o cuya configuración permite una puesta en marcha automática. Por otro lado, consideramos las medidas no automatizables o activas como aquellas que requieren una intervención por parte del usuario para su correcto funcionamiento.

Para el estudio se considera la naturaleza de las medidas, aunque la seguridad mejorada de las últimas versiones de las plataformas PC y móviles incluyan algunas de las medidas no automatizables de forma nativa (por ejemplo la utilización de permisos reducidos).

En este último semestre el uso de medidas automatizables ha disminuido en el ordenador del hogar (FIGURA 13). A excepción de la actualización del sistema operativo (tal vez la más automatizable), y el uso de programas o configuración de bloqueo de pop-up y publicidad (tal vez acompañando a la actualización), el resto de medidas experimenta un descenso. Desafortunadamente, como ya adelantaba la FIGURA 6, la percepción de los usuarios es incluso positiva comparada con los datos reales de uso.

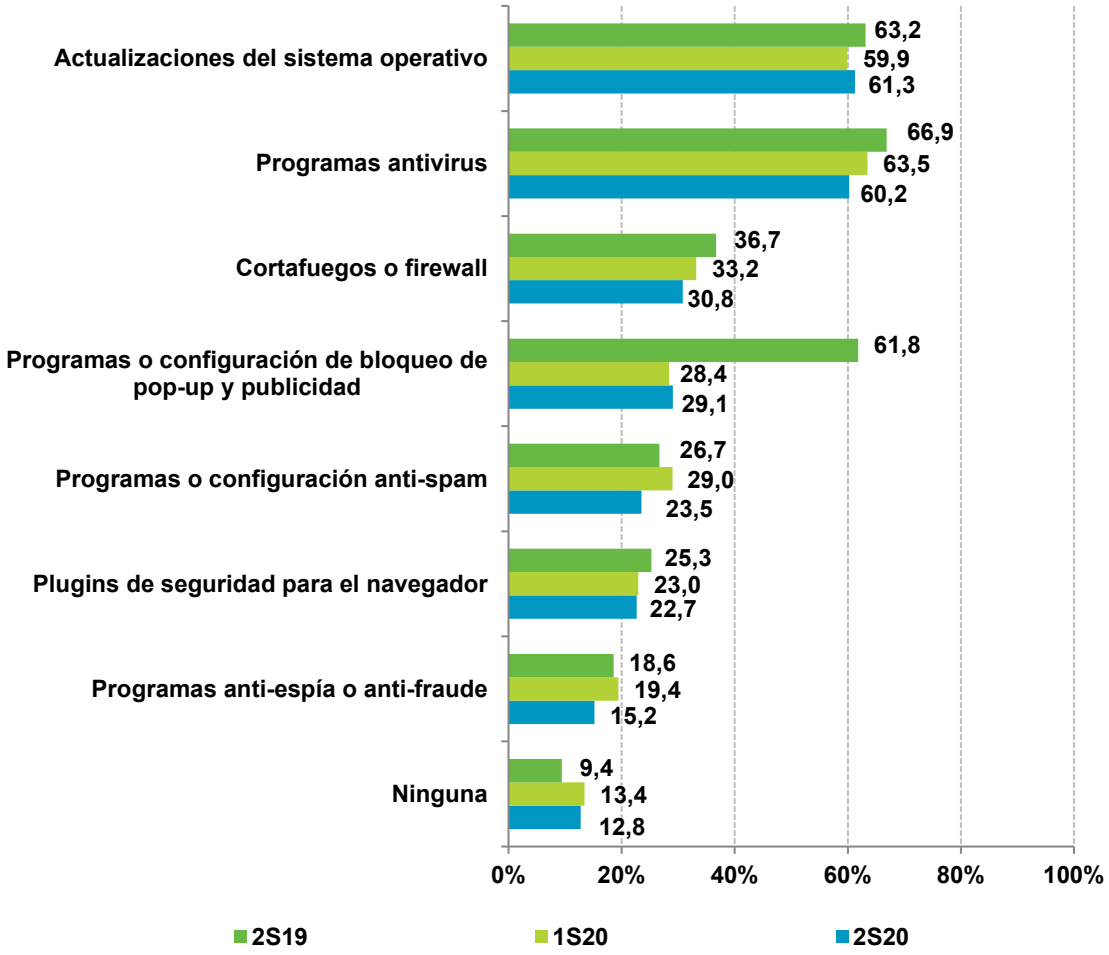
[8] https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1156

[9] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

[10] https://www.osi.es/es/actualidad/blog/2019/05/29/cifrado-y-almacenamiento-seguro-de-ficheros-paso-paso

De igual forma las medidas de seguridad activas no muestran diferencias notables respecto a los resultados del semestre anterior.

FIGURA 13. MEDIDAS DE SEGURIDAD AUTOMATIZABLES EN EL ORDENADOR DEL HOGAR (DATOS DECLARADOS)



Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

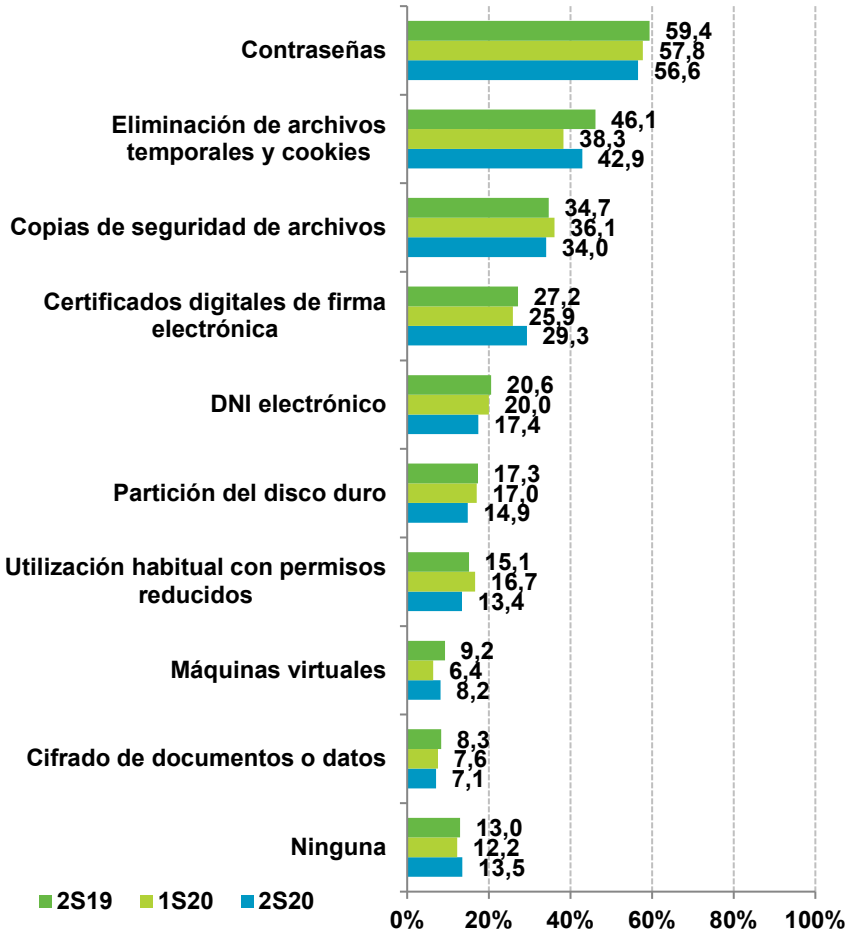
Sí destaca la percepción por parte de los usuarios de un mayor uso de certificados digitales para la firma electrónica y el uso de herramientas de eliminación de archivos temporales y cookies.

El uso declarado de máquinas virtuales se incrementa 1,8 puntos porcentuales, aunque como ya se adelantó en la sección 3.3 sería necesario fomentar el uso de esta herramienta, en especial entre trabajadores y estudiantes.

Algunos conceptos básicos sobre la virtualización se describen en el artículo "La virtualización puede ser la solución a tus problemas" de INCIBE [11]. En dicho artículo se explica en detalle cómo la virtualización puede ayudar a mejorar la seguridad de las empresas.

[11] https://www.incibe.es/protege-tu-empresa/blog/virtualizacion-puede-ser-solucion-tus-problemas

FIGURA 14. MEDIDAS DE SEGURIDAD ACTIVAS EN EL ORDENADOR DEL HOGAR (%)



Base: Usuarios de PC
Fuente: Panel hogares, ONTSI

4 Hábitos de comportamiento en la navegación y usos de Internet

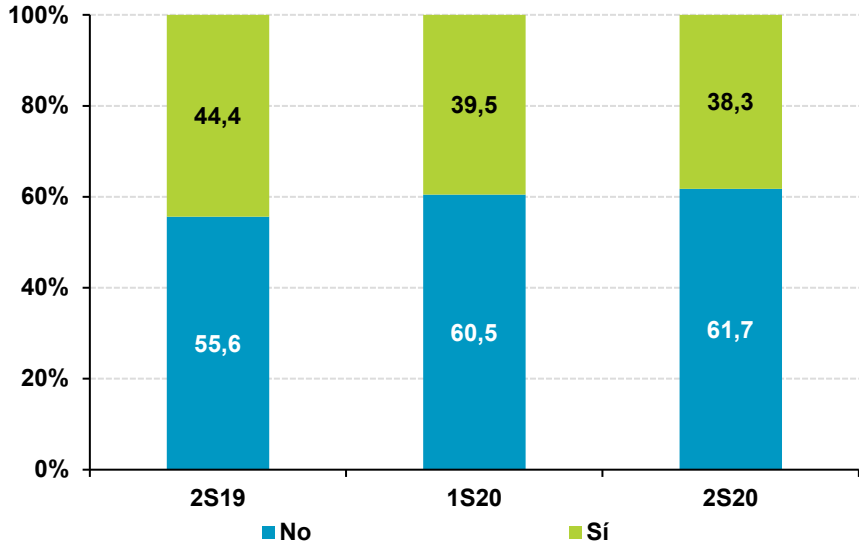
Estudiar el comportamiento en la red, las conductas de riesgo asumidas y el grado de conocimiento de sus repercusiones es fundamental para identificar puntos de mejora para futuras guías y campañas de concienciación.

4.1 Evolución de las conductas de riesgo

La evolución de las conductas de riesgo experimenta una mejoría leve respecto al semestre anterior.

En concreto el 61,7% de los usuarios declaran no realizar conductas de riesgo de forma consciente, lo que supone una mejora porcentual de 1,2 p.p., y manteniendo por lo tanto su progresión ascendente.

FIGURA 15. EVOLUCIÓN DE LA ADOPCIÓN CONSCIENTE DE CONDUCTAS DE RIESGO (%)

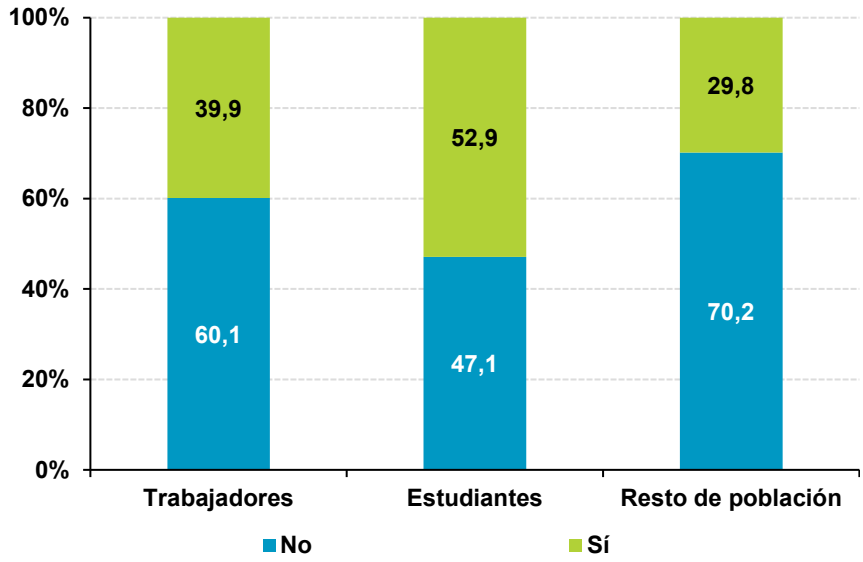


Base: Total usuarios
Fuente: Panel hogares, ONTSI

En particular, los trabajadores asumen menos riesgo que el semestre anterior, disminuyendo el porcentaje del 41,2% al 39,9% (1,3 p.p.). En dicho caso se ha querido diferenciar de la parte no activa la conducta de riesgo de los estudiantes, observándose que más de la mitad sí asume conductas de riesgo conscientes.

El resto de la población resulta, en este caso, más prudente, con un 70,2% de casos declarados en los que no se realizan conductas de riesgo.

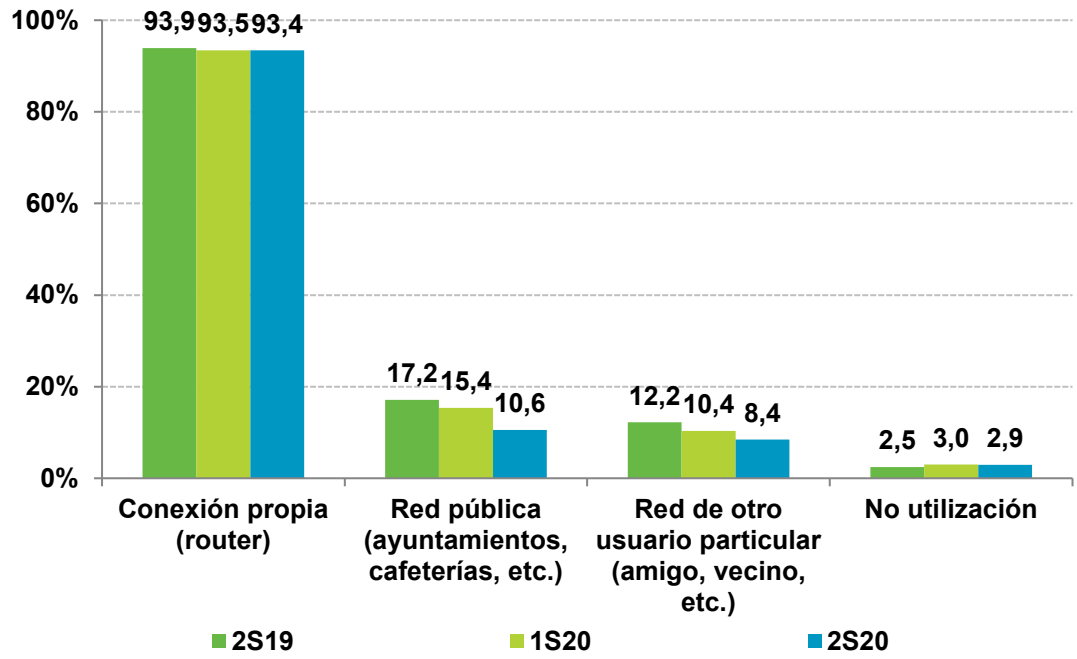
FIGURA 16. REALIZACIÓN CONSCIENTE DE ALGUNA CONDUCTA DE RIESGO SEGÚN PERSONAS TRABAJADORAS, ESTUDIANTES Y RESTO DE POBLACIÓN NO ACTIVA (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

Por último, la siguiente figura muestra la utilización declarada de redes Wi-fi públicas y privadas.

FIGURA 17. UTILIZACIÓN DE REDES WI-FI PRIVADAS Y PÚBLICAS (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

En este caso cabe destacar que las conductas de riesgo se reducen visiblemente al disminuir al 10,6% la conexión a la red pública que suele estar por lo general abierta y desprotegida.

4.2 Descargas e instalación de programas en el ordenador

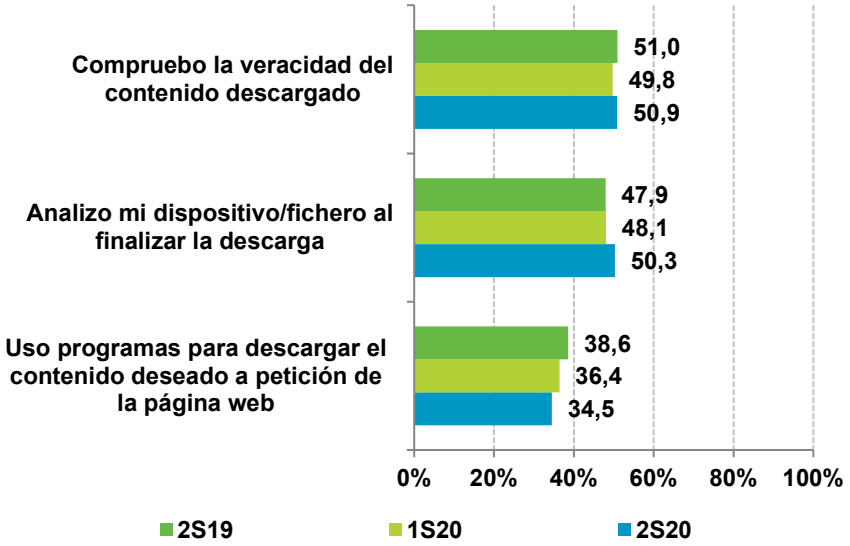
Las descargas de los programas e instalación consciente de los mismos es un punto crítico en la evaluación de los hábitos de ciberseguridad.

En particular, entre los servicios ofrecidos en Internet (ver FIGURA 4) que han sido utilizados por el usuario en el último semestre encontramos la descarga directa de archivos (incluimos las descargas gratuitas), y la descarga de archivos a través de redes P2P.

Los hábitos en la descarga directa de archivos han experimentado ciertas mejoras respecto al semestre anterior. Los panelistas comprueban más la veracidad del contenido descargado y analizan los ficheros. Desde la página de la OSI se informa a los usuarios sobre diferentes herramientas gratuitas que permiten el análisis de ficheros[12].

[12] https://www.osi.es/es/herramientas

FIGURA 18. USO DE DESCARGA DIRECTA DE ARCHIVOS, PROGRAMAS, DOCUMENTOS, ETC. (%)



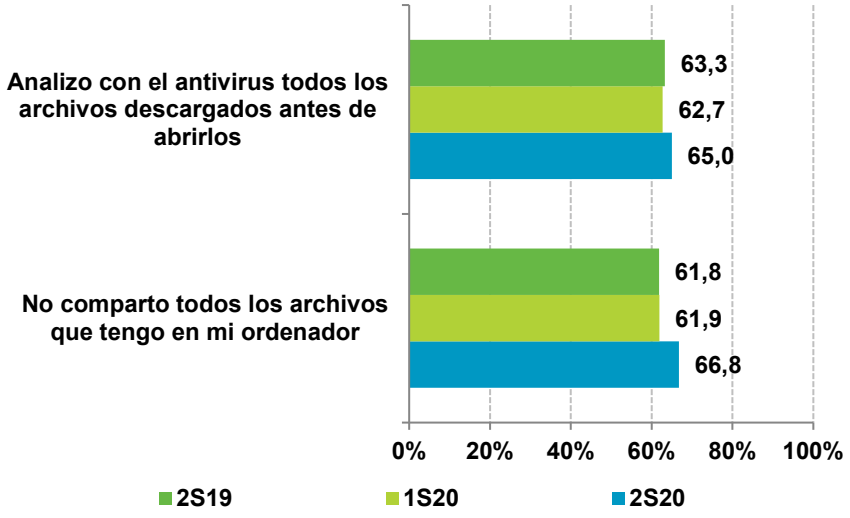
Base: usuarios de redes P2P
Fuente: Panel hogares, ONTSI

El uso de las redes P2P también se toma con mayor cautela. Se adelantaba en la sección 2 que el hábito de acceder a contenido digital de pago (p.ej. plataformas Netflix, HBO, etc.) había propiciado un descenso en el uso de las redes P2P.

Los resultados recabados muestran que los panelistas demuestran ser más conscientes del riesgo de las descargas por dicho medio.

También ofrecen una conducta más comedida sobre la compartición de archivos propios de sus equipos, aumentando 4,9 p.p. la no compartición respecto del primer semestre.

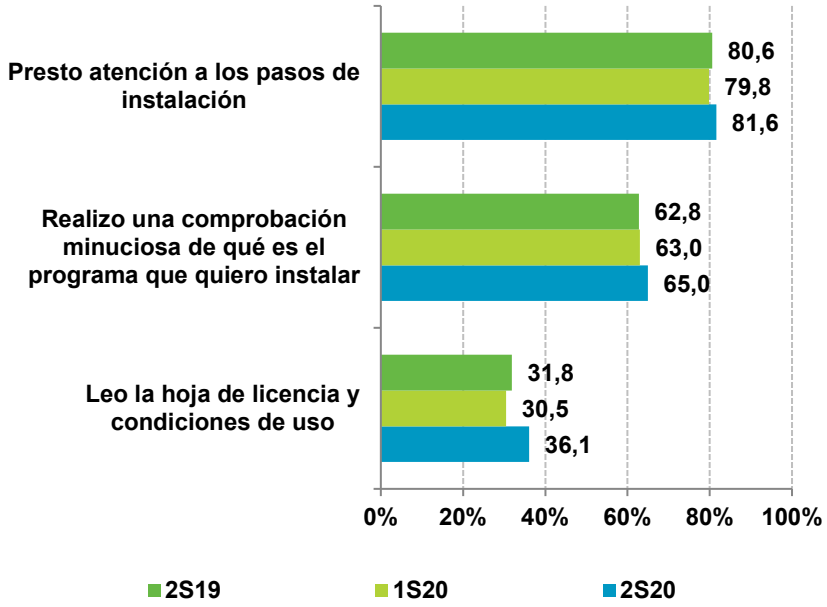
FIGURA 19. HÁBITOS DE COMPORTAMIENTO EN EL USO DE REDES P2P (%)



Base: usuarios de redes P2P
Fuente: Panel hogares, ONTSI

La instalación de programas también mejora sus buenas prácticas, en especial la atención de los usuarios a la lectura de la hoja de licencia y condiciones de uso.

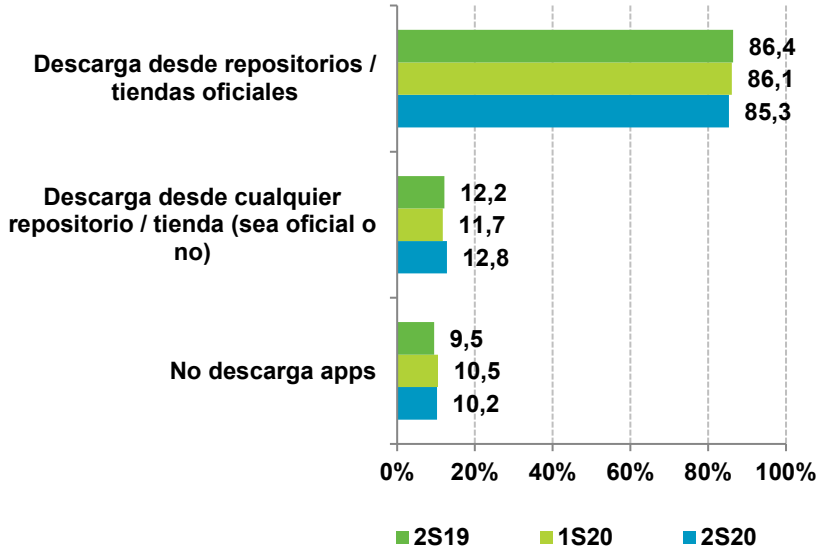
FIGURA 20. INSTALACIÓN DE PROGRAMAS (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

Sin embargo, los hábitos de descarga de los usuarios con dispositivos móviles sí han experimentado variaciones negativas. Se declaran menos descargas de repositorios oficiales y más desde sitios no oficiales (ver FIGURA 21).

FIGURA 21. DESCARGA DE APLICACIONES EN DISPOSITIVOS ANDROID (%)



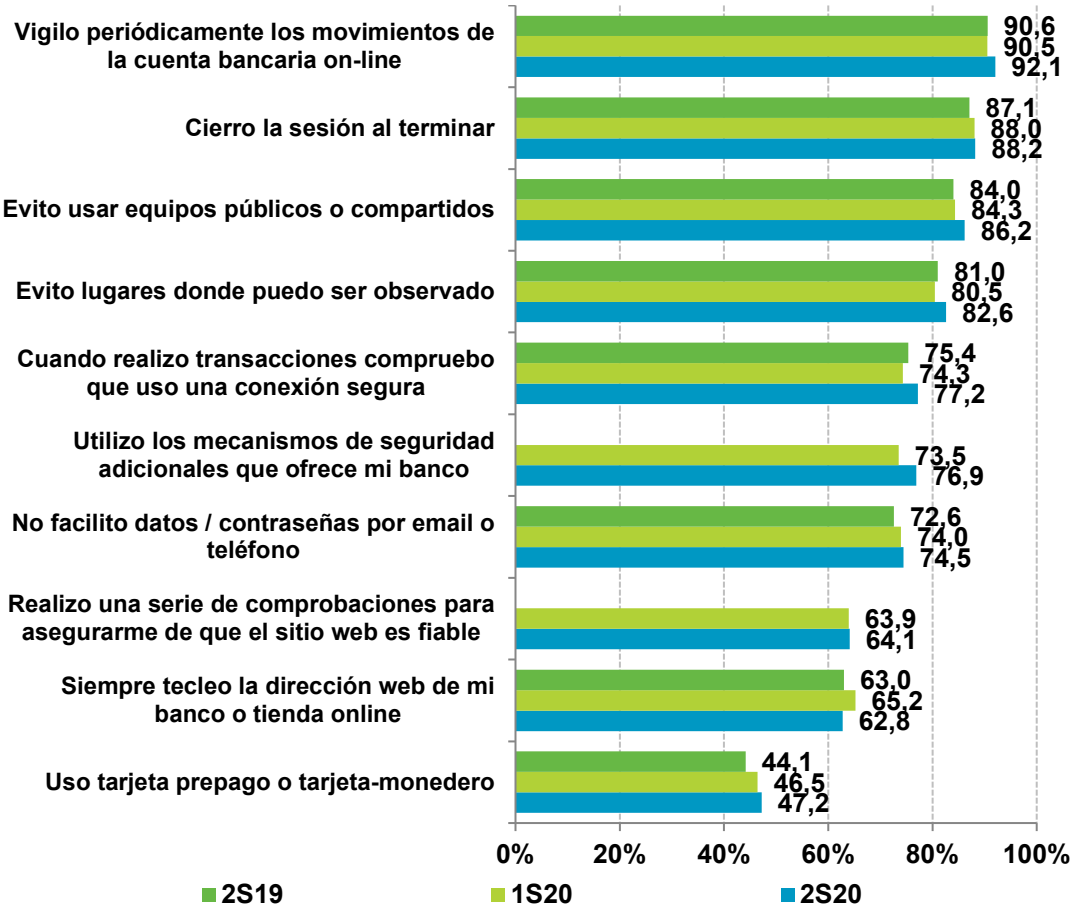
Base: total usuarios
Fuente: Panel hogares, ONTSI

4.3 Evolución de los hábitos en los servicios de banca online y comercio electrónico

Entre la evolución de los hábitos generales cabe destacar el uso de servicios de banca online o comercio electrónico, y en particular el aumento del uso de mecanismos de seguridad adicionales ofrecidos por los bancos.

Las entidades bancarias están introduciendo nuevas medidas de seguridad y forzando a los usuarios a emplearlas, algo que se ve reflejado también en los resultados de las encuestas. La última de las medidas que se ha forzado desde la Comisión Europea, como parte de la directiva de servicios de pago (PSD2 [13]), es la Autenticación Reforzada de Cliente (SCA), que debía estar implementada antes del 1 de enero de 2021. Estas medidas están dirigidas a reforzar la seguridad de los pagos con tarjeta en comercio electrónico.

FIGURA 22. HÁBITOS DE COMPORTAMIENTO EN EL USO DE SERVICIOS DE BANCA ONLINE O COMERCIO ELECTRÓNICO (%)



Base: usuarios que utilizan la banca online y/o comercio electrónico
Fuente: Panel hogares, ONTSI

[13] Aprobada en 2015, la PSD2 entró en vigor en España en 2018. Entre sus medidas incluye la SCA. Más información en https://www.osi.es/es/actualidad/blog/2019/09/17/informate-lo-que-debes-saber-si-quieres-hacer-pagos-online-partir-de

Son medidas que se implantan sin duda en muy buen momento, dado que los ataques sobre el sector financiero siguen en aumento y todo indica que seguirá así en 2021.

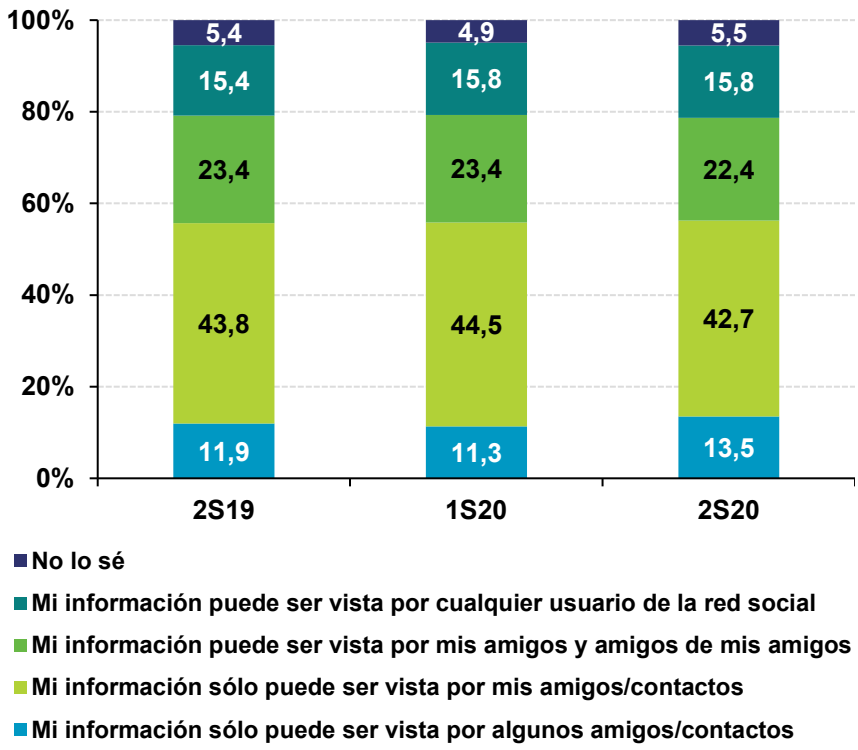
Las restricciones de movilidad por la COVID-19 también han facilitado evitar el uso de equipos públicos o lugares donde el panelista pueda ser observado.

Durante 2020 se vieron aumentados los casos de phishing y en particular smishing y vishing[14], por lo que la mejora de la conducta de los panelistas en relación a proporcionar datos o contraseñas por email o teléfono es muy buena noticia, aunque la diferencia respecto al semestre anterior sea casi imperceptible.

En cuanto a las redes sociales, éstas han sido (y continúan siéndolo para muchas personas) el único vínculo con familiares y allegados.

En el último semestre de 2020 la precaución de cara a la visualización restringida del contenido publicado en las redes sociales aumentó en 2,2 p.p. respecto al primer semestre del año. Así, en torno al 13,5% de los panelistas declaran que la información de su perfil sólo puede ser vista por algunos amigos y/o contactos.

FIGURA 23. HÁBITOS DE COMPORTAMIENTO EN EL USO DE REDES SOCIALES (%)



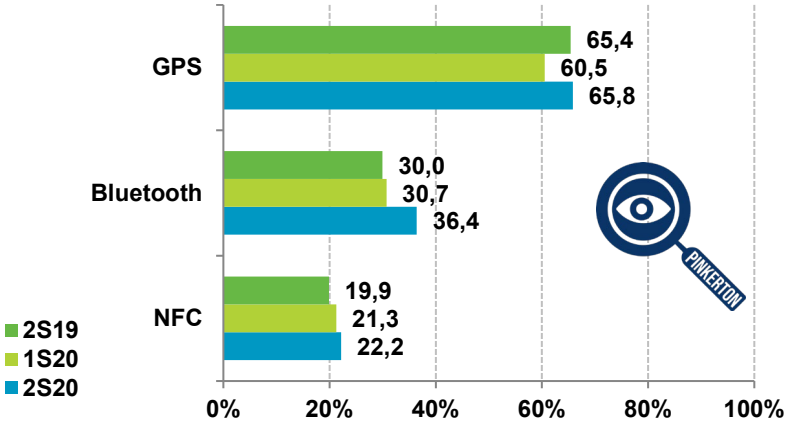
Base: total usuarios
Fuente: Panel hogares, ONTSI

Como incremento destacado en el ámbito de los dispositivos Android está por ejemplo el aumento del uso de tecnologías como GPS, Bluetooth y NFC. De hecho, el incremento en los dos primeros

[14] https://unaaldia.hispasec.com/2020/12/un-ano-diferente-salvo-por-el-fraude-que-sigue-en-aumento.html

ha podido ser motivado por el uso de aplicaciones de rastreo de la COVID-19, mientras que el incremento en el uso de NFC sigue un ritmo más progresivo en concordancia con los semestres anteriores.

FIGURA 24. TECNOLOGÍAS ACTIVAS EN DISPOSITIVOS ANDROID (%)



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

5 Incidentes de seguridad

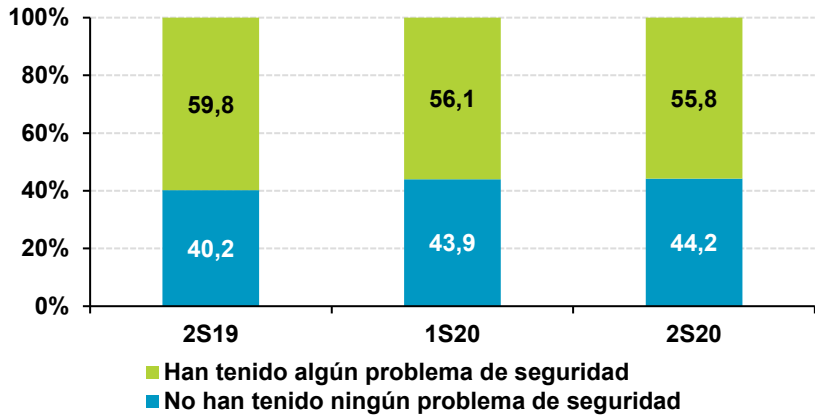
Las medidas de seguridad y los buenos hábitos reducen la probabilidad de sufrir un incidente de seguridad. Sin embargo, aun siguiendo las buenas prácticas, existe el riesgo de exposición a los ciberataques, que han continuado evolucionando para sortear las medidas de seguridad en 2020.

Esta sección se centra en el análisis de los incidentes de seguridad identificados por los panelistas y aquellos que han sido verificados por los escaneos de los dispositivos.

5.1 Evolución de las incidencias

El 55,8% de los panelistas afirma haber tenido ningún problema de ciberseguridad durante este semestre, por lo que estaríamos ante una disminución de los incidentes declarados.

FIGURA 25. EVOLUCIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



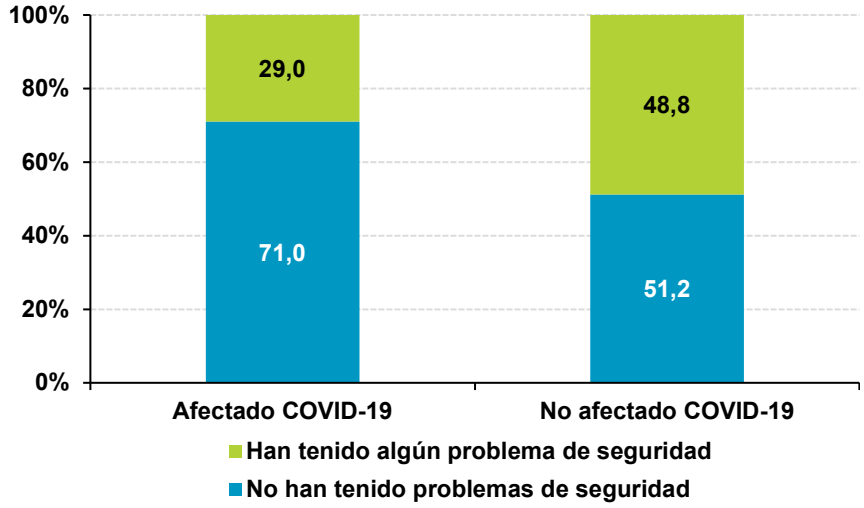
Base: total usuarios
Fuente: Panel hogares, ONTSI

Este hecho puede deberse a la mejoría experimentada en los hábitos de comportamiento, o incluso a temporadas de inactividad del panelista debido a las incidencias por la COVID-19. Aunque la FIGURA 1 indicaba que la mayoría de los panelistas no se habían visto afectados de forma directa por la enfermedad de la COVID-19, sí puede ser interesante comprobar en qué grado afectan las incidencias de seguridad según la afección de la enfermedad.

La FIGURA 26 muestra las incidencias de seguridad en este semestre considerando dos grupos: panelistas afectados directa o indirectamente por la COVID-19 y no afectados. Del primer grupo sólo el 29% declara haber sufrido algún problema de seguridad, frente al 48,8% declarado por el segundo grupo.

Tanto los periodos de inactividad como la variación de prioridades o incluso de atención pueden ser también causas de esta diferencia.

FIGURA 26. INCIDENCIAS DE SEGURIDAD POR GRUPOS DE POBLACIÓN AFECTADOS Y NO AFECTADOS POR LA COVID-19 (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

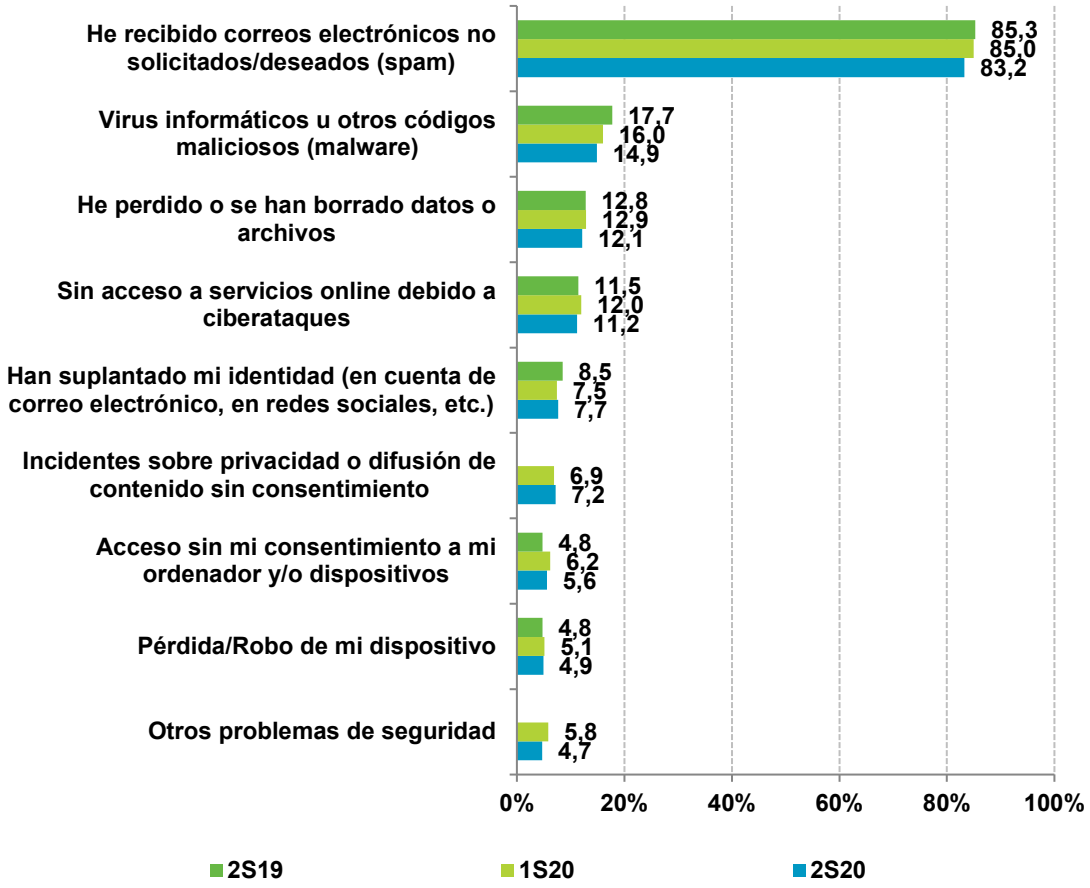
Por otro lado, la evolución de las incidencias de seguridad se mantiene con pocos cambios respecto a los semestres previos.

La recepción de correos indeseados continúa siendo la principal incidencia declarada por los usuarios, seguida de los virus informáticos. Los incidentes que aumentan –aunque muy levemente- respecto al semestre previo son la suplantación de identidad y los incidentes sobre la privacidad o difusión de contenido sin consentimiento.

Esto último hace más importante, si cabe, el destacado papel del cifrado de datos como buena práctica, que podría paliar este tipo de situaciones, así como establecer mecanismos que ayuden a mejorar la privacidad de los usuarios.

Algunas guías y recomendaciones sobre privacidad pueden encontrarse en las páginas web de la OSI[15], que ofrece un listado, además de herramientas, que pueden emplearse para la navegación segura[16]. También en Internet Segura *for Kids* (IS4K)[17], espacio dedicado a los más jóvenes que ofrece información de carácter general.

FIGURA 27. EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)



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

En particular, ante el problema que representa el aumento de casos de suplantación de identidad, hay un artículo reciente de la OSI que se centra en esta problemática, con el fin de asesorar a los usuarios sobre cómo protegerse y actuar en caso de suplantación de cuentas[18]. Entre los mecanismos de protección se encuentran la correcta configuración de las opciones de privacidad de las cuentas, evitar aceptar solicitudes de amistad de desconocidos, minimizar la publicación de contenido susceptible de ser empleado para la identificación en nuestras cuentas, emplear gestores de contraseñas y generación de las mismas para cada red social.

[15] https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

[16] https://www.osi.es/es/herramientas-gratuitas/categoria/privacidad-y-seguridad-de-datos/privacidad-y-navegacion-segura

[17] https://www.is4k.es/necesitas-saber/privacidad

[18] https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar

Además, para los casos de SIM *swapping* –duplicación de la tarjeta SIM– deberemos contactar con nuestra compañía telefónica, y emplear siempre servicios de confianza.

Los atacantes pueden mejorar sus ataques de ingeniería social con toda la información que recaban de los objetivos, y además ganarse la confianza de nuestro entorno por medio del vínculo que establecen con nuestra cuenta[19]. Cuando aceptamos a contactos en nuestra red social sin conocerlos personalmente estamos además dando acceso al contenido que publicamos –caso de tener la cuenta privada– pero además podemos estar facilitando el acceso a datos publicados por terceros, nuestro entorno directo.

Así mismo, es importante conocer que a día de hoy las principales redes sociales cuentan con sus propios mecanismos para notificar suplantaciones o robos de cuenta, a veces llamados "hackeos" de cuentas.

5.2 Infecciones por malware

ORDENADORES QUE ALOJAN MALWARE Y SU PELIGROSIDAD

59,2%
DE LOS ORDENADORES ESCANEADOS CON PINKERTON ALOJAN MALWARE

72,0%
DEL MALWARE DETECTADO PRESENTA UN NIVEL DE RIESGO ALTO

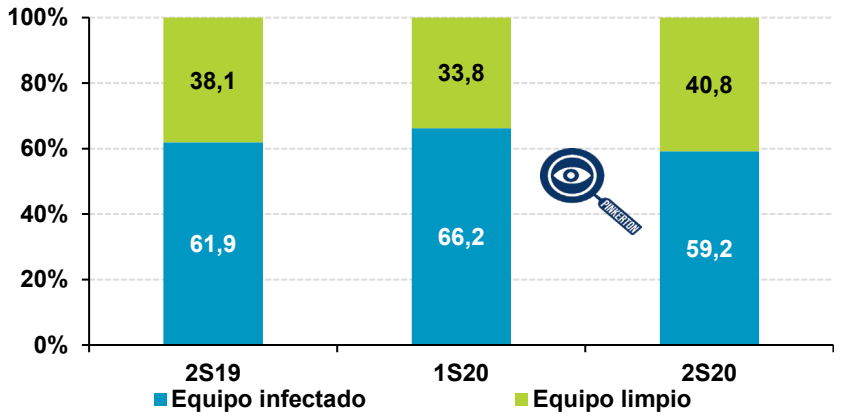
Esta sección describe los resultados del estudio para los casos de infecciones por malware. Se dedica un apartado para este tipo de incidente dado que un equipo infectado con malware es un elemento no confiable en nuestro entorno, un intruso no deseado en nuestro hogar.

Los datos analizados en esta parte del informe corresponden a datos reales recabados por la herramienta Pinkerton.

5.2.1 Malware en el ordenador del hogar

La percepción de la disminución de incidencias de malware por parte de los usuarios (FIGURA 27) se asocia con los datos recogidos de los dispositivos.

FIGURA 28. ESTADO REAL DE INFECCIÓN EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

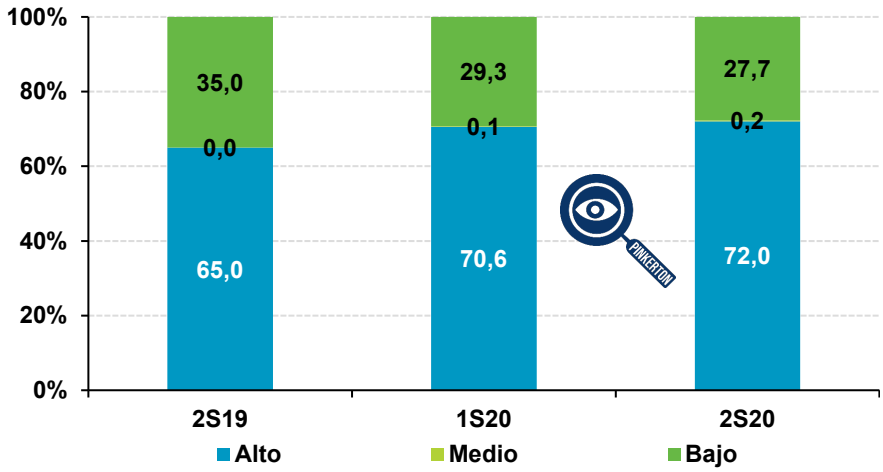
[19] https://www.diariosur.es/tecnologia/funcionan-fabricas-troles-20200116200217-nt.html

En el caso de los ordenadores del hogar, el número de equipos infectados se reduce al 59,2% este semestre, aunque continúa siendo un valor elevado, más de la mitad de los equipos escaneados.

Sin embargo, pese a la disminución de infecciones, la peligrosidad alta del malware detectado aumenta al 72%, 1,4 p.p. respecto al primer semestre, como muestran los datos de la FIGURA 29. También aumenta ligeramente el malware de peligrosidad media.

En la categoría de peligrosidad alta se encuentra el malware cuya operativa afecta a la integridad del sistema de forma notable, permitiendo incluso en algunos casos el acceso remoto por parte del atacante, acceso a información confidencial o afectando a la funcionalidad crítica. Un ejemplo es el ransomware y también los rootkits. Un atacante con acceso remoto y con control sobre el equipo puede emplearlo como arma para lanzar otros ataques coordinados contra otras redes. La preesencia de troyanos es habitual, por ejemplo en el caso de malware bancario, destinado a obtener las credenciales de los usuarios.

FIGURA 29. PELIGROSIDAD DEL MALWARE EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

El malware de peligrosidad media incluye muestras en las que se ha identificado un comportamiento no necesariamente perjudicial para el funcionamiento crítico, o que no realiza control explícito de terceros no autorizados sobre el entorno. Por ejemplo, el adware entraría en esta clasificación. Puede configurar partes de los servicios con el fin de de mostrar información publicitaria a la víctima, o afectar al rendimiento, pero no introducir pérdidas de recursos. Idealmente este tipo de malware querrá coexistir con el usuario para seguir mostrando recomendaciones de compra según sus preferencias.

Por último, el malware de peligrosidad baja puede incluir incluso herramientas empleadas para hacking, que pueden servir para realizar escaneos por ejemplo u otras utilidades, sin que llegue a interferir en el funcionamiento del propio equipo.

No obstante, pueden facilitar el trabajo del atacante si logra acceso al equipo con dichas utilidades, dado que no tendrá que instalar nada adicional para poder hacer uso de los kits de escaneo.

Son por lo tanto los casos de peligrosidad media-alta los que más peligro inmediato presentan, por comprometer directamente al equipo víctima. La FIGURA 30 muestra la evolución del malware considerando adwares, troyanos y espías. Bajan los porcentajes de casos respecto al semestre anterior, en el que destacaba el aumento de troyanos.

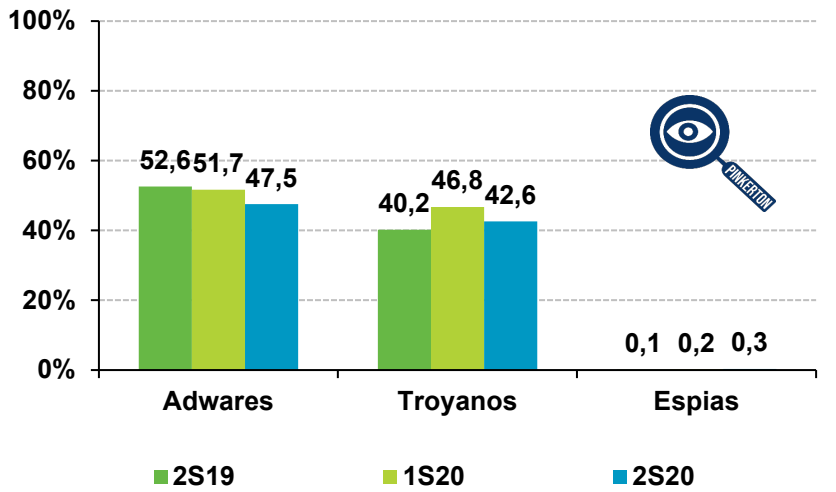
En este caso, no obstante, se observa que la proporción de software espía sigue en aumento, aunque muy paulatinamente.

En el sector de los troyanos podemos encontrar diverso tipos de malware, entre ellos los troyanos bancarios, que afectan directamente a la economía de las personas físicas. Mediante el robo de credenciales, permiten a los atacantes tomar control de las cuentas de las víctimas.

Por los resultados del análisis de hábitos de los internautas, y en particular aquellos que afectan a los servicios bancarios (ver sección 4.3), se percibe mayor consciencia del control de las cuentas bancarias, aunque también puede estar motivado por la situación de crisis que la COVID-19 ha generado para muchas personas.

En cualquier caso, un mayor control sobre las operaciones bancarias también permite la rápida identificación de este tipo de malware, en el caso de haber pasado desapercibido para el resto de controles y medidas pasivas y activas.

FIGURA 30. EVOLUCIÓN DEL MALWARE EN EL ORDENADOR DEL HOGAR (%)



Base: Total ordenadores
Fuente: Panel hogares, ONTSI

La siguiente tabla muestra un resumen de las incidencias de malware en el ordenador del hogar, las declaradas frente a las reales.

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

Declaran tener malware en PC	Su PC presenta malware		
	Sí	No	Total
Sí	6	3,6	11,5
No	53,2	37,2	88,5
Total	59,1	33,9	100

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

Disminuye el número de usuarios que no se percatan de tener malware en su ordenador en 6,1 p.p., llegando al 53,2%. No obstante continúa siendo una cifra alta. Estos usuarios están empleando su ordenador sin ser conscientes de que está comprometido, por lo que probablemente estén relajando sus conductas.

Pese a estas cifras, sujetas a las condiciones particulares de la muestra, sus hábitos y también a la situación provocada por el confinamiento y las restricciones territoriales, hay que tener presente que los casos de malware en general están aumentando.

Mientras que diversos informes apuntan a que 2020 fue un año similar a 2019, también añaden la aparición de nuevas familias de malware no sólo para ordenadores, sino también dirigidas a dispositivos móviles[20].

En el caso de estos últimos y siguiendo la tendencia de los últimos semestres, se han identificado menos muestras de malware en los dispositivos sujetos al estudio.

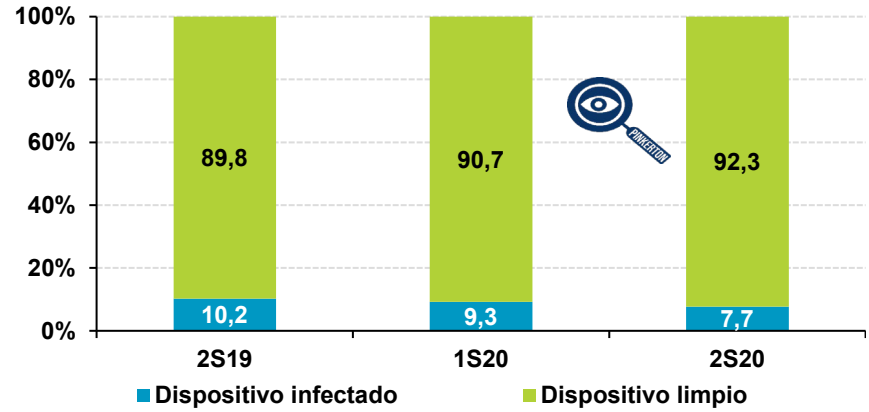
5.2.2 Malware en dispositivos Android

Este semestre el software de rastreo utilizado en este estudio -Pinkerton- ha vuelto a registrar el descenso de los casos de infecciones por malware en dispositivos Android. Las mejoras en las actualizaciones contribuyen también a este descenso, así como la implementación de cada vez más medidas activas adicionales a las pasivas nativas de la seguridad de los dispositivos.

Ya se indicó no obstante que las mejoras de Android 11 (ver sección 3.2) no afectan significativamente al estudio debido al bajo porcentaje de usuarios con este terminal, pero sí aumentan el número de dispositivos con Android 10, que traía consigo también mejoras de seguridad.

[20] https://www.buguroo.com/es/laboratorio/informe-malware-bancario-2020

FIGURA 31. ESTADO REAL DE INFECCIÓN EN DISPOSITIVOS ANDROID (%)



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

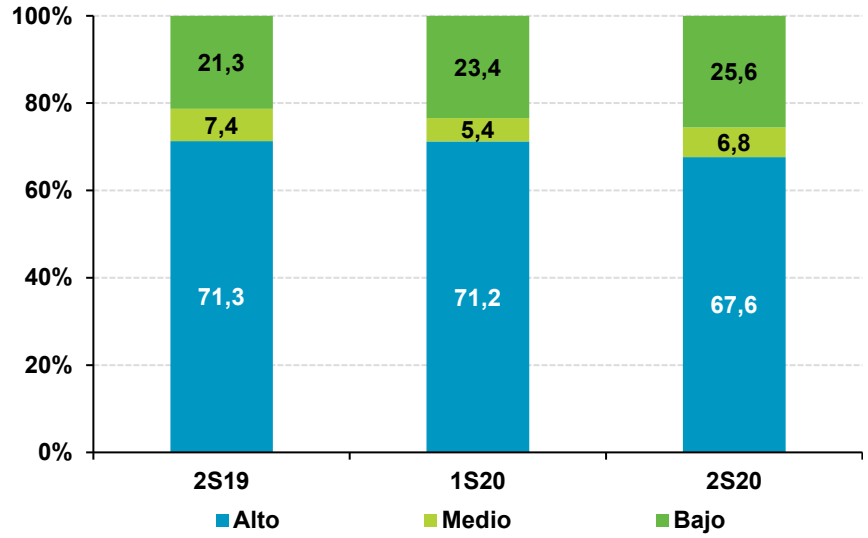
Mientras que en el caso de los ordenadores el número de equipos infectados bajaba pero aumentaba el porcentaje de peligrosidad alta, para los dispositivos Android la peligrosidad sigue bajando también este semestre.

De hecho, la diferencia es mayor respecto a los dos semestres anteriores (3,6 p.p.), situándose en el 67,6% de equipos infectados con malware de peligrosidad alta.

Respecto a los equipos infectados con malware de peligrosidad media, en este caso se hacen notar más que en el caso de los ordenadores, siendo del 6,8%. Ambas cifras (media y alta) suman el 74,4%, un valor que está lejos de ser bajo.

Se analizará en los próximos semestres cómo evolucionan estos valores, considerando las mejoras de seguridad de las últimas versiones de Android, unido a la adquisición paulatina de buenos hábitos.

FIGURA 32. PELIGROSIDAD DEL MALWARE EN DISPOSITIVOS ANDROID (%)



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

EVOLUCIÓN DEL MALWARE EN PC Y ANDROID PARA 2S20

Adware

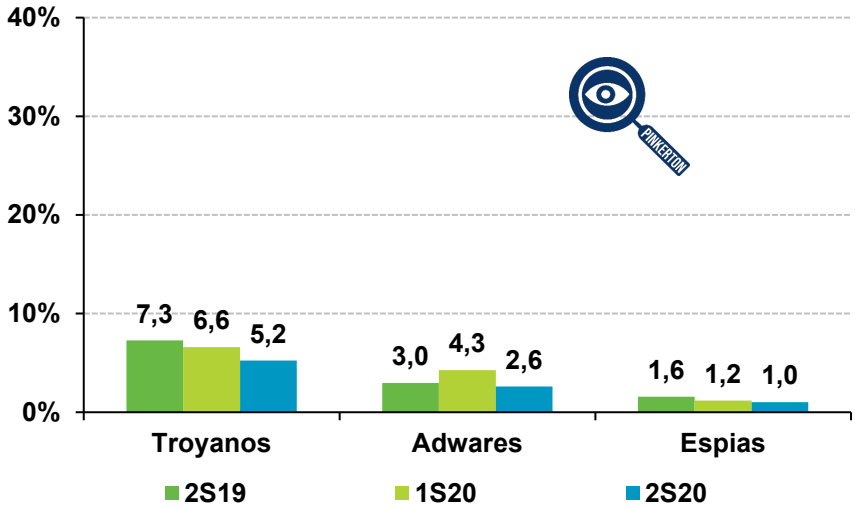
ES EL TIPO DE MALWARE MÁS PRESENTE EN LOS ORDENADORES

Troyano

ES EL TIPO DE MALWARE MÁS PRESENTE EN LOS DISPOSITIVOS ANDROID

Respecto a los semestres anteriores se percibe también un descenso en la infección de los dispositivos por los tipos troyano, adware y espías, manteniéndose los troyanos como el malware más presente en este tipo de plataformas.

FIGURA 33. EVOLUCIÓN DEL MALWARE EN DISPOSITIVOS ANDROID (%)



Base: Total dispositivos Android
Fuente: Panel hogares, ONTSI

Este hecho enlaza con el aumento de malware bancario para dispositivos Android, malware que se apoya principalmente en el uso de troyanos para su descarga e instalación en el equipo.

La siguiente tabla resume las incidencias de malware, declaradas frente a las reales, en dispositivos Android. Destacar que un 7,3% de los usuarios que creen no tener malware, sí tienen el dispositivo comprometido. Desciende la cifra en torno a 1,4 p.p. respecto del 8,7% que se obtenía en la anterior oleada.

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

Declaran tener malware en el dispositivo Android	Su dispositivo Android presenta malware		
	Sí	No	Total
Sí	0,4	5	94,6
No	7,3	87,3	5,4
Total	7,7	92,3	100

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

Las mejoras en la versión de Android 10 podrían haber ayudado significativamente a este descenso, al igual que los hábitos de mejora adquiridos por los panelistas.

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

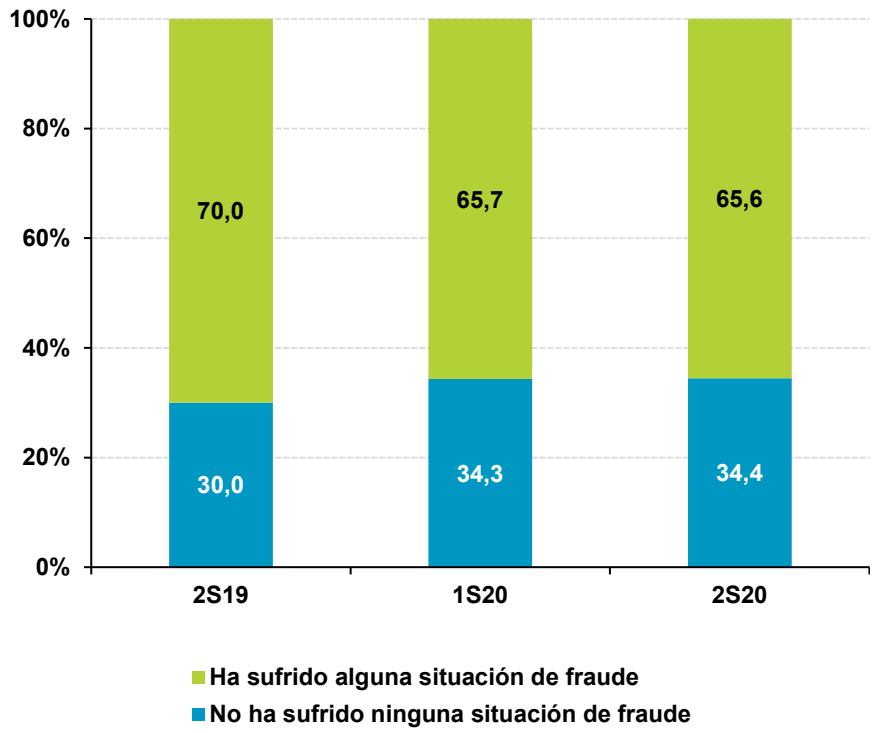
Los incidentes de seguridad traen consigo consecuencias para los panelistas, algunas de ellas perceptibles por los mismos. Las más directas o perceptibles están vinculadas al fraude, que es uno de los aspectos analizados a continuación.

Además, se analizan los cambios de hábitos realizados por los panelistas tras los incidentes de ciberseguridad.

6.1 Evolución de los intentos de fraude

La percepción de los intentos de fraude se mantiene prácticamente igual que en el primer semestre, con muy poca variación (0,1 p.p. menos).

FIGURA 34. EVOLUCIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



Base: Total usuarios
Fuente: Panel hogares, ONTSI

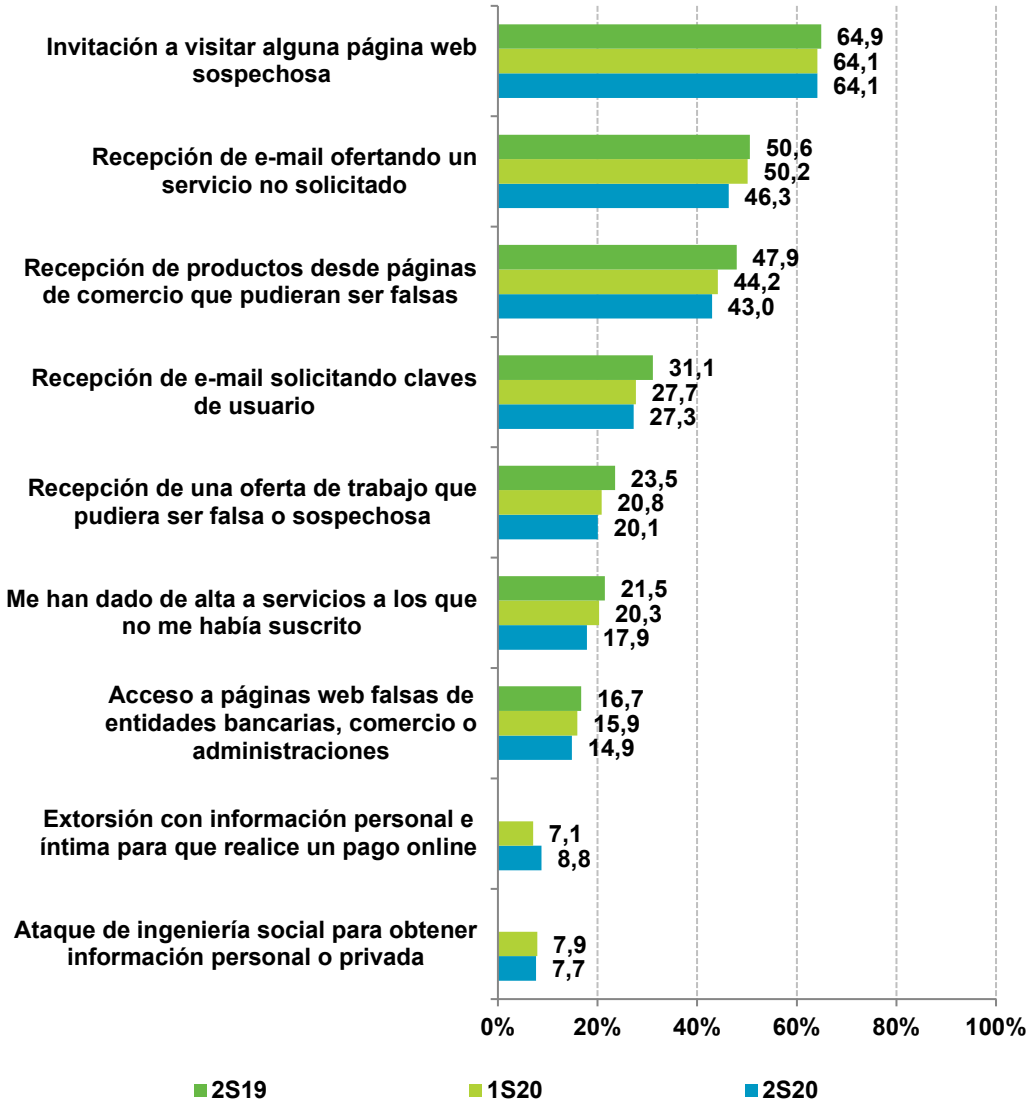
De las manifestaciones de fraude que han percibido los panelistas destaca la de extorsión con información personal e íntima para que se realice un pago online. Esto podría tener relación con la presencia de troyanos en los equipos, pero también con la exposición de los datos personales.

NO TE LO GUARDES, ¡NOTIFICA!

PUEDES NOTIFICAR CASOS DE FRAUDE ONLINE O SITIOS WEB QUE ALOJAN MALWARE REPORTANDO EN:

INCIDENCIAS@INCIBE-CERT.ES

FIGURA 35. EVOLUCIÓN DE LA MANIFESTACIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



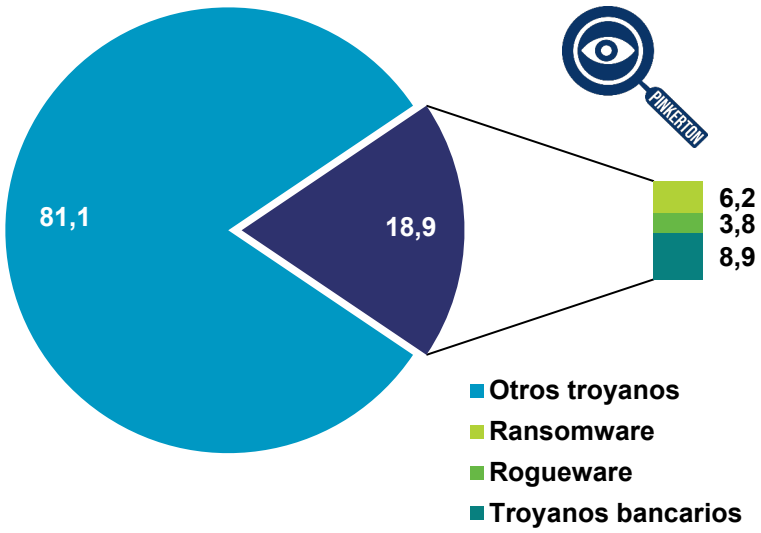
Base: Usuarios que han sufrido un intento de fraude
Fuente: Panel hogares, ONTSI

Entre los tipos de malware vinculados con el fraude online destacan los troyanos bancarios, el ransomware y el rogueware. En los ordenadores del hogar el porcentaje de infecciones de estos grupos es de un 18,9%, destacándose los troyanos bancarios que suponen un 8,9%.

Estas cifras pueden consultarse en la FIGURA 36, donde además vemos que hay un 81,1% que corresponde a otros tipos de malware dentro de la categoría troyanos.

Estos otros troyanos podrían servir también para la esconder la presencia de este malware en sus primeras fases, o bien para ataques dirigidos a otros sectores. Cabe destacar que los creadores de malware cada vez combinan más técnicas, incluyendo características de varios tipos de malware en uno solo.

FIGURA 36. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN EL ORDENADOR DEL HOGAR (%)



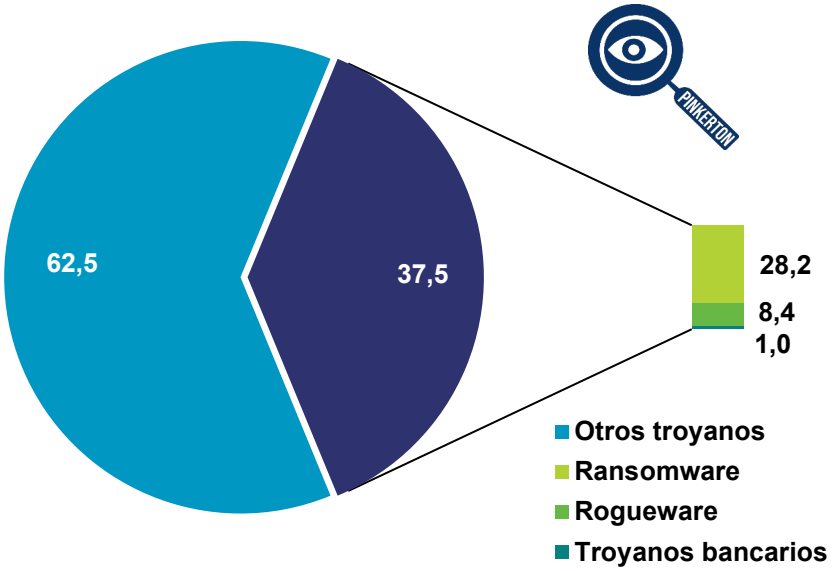
Base: total ordenadores con troyanos detectados
Fuente: Panel hogares, ONTSI

En los dispositivos Android el 28,2% del malware vinculado al fraude corresponde a muestras de ransomware, seguido por el tipo rogueware (8,4%) y los troyanos bancarios (1%).

FIGURA 37. TROYANOS BANCARIOS, RANSOMWARE Y ROGUEWARE EN DISPOSITIVOS ANDROID (%)

FRAUDE ONLINE EN ANDROID

28,2%
DEL MALWARE DIRIGIDO A FRAUDE CORRESPONDE A
RANSOMWARE



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

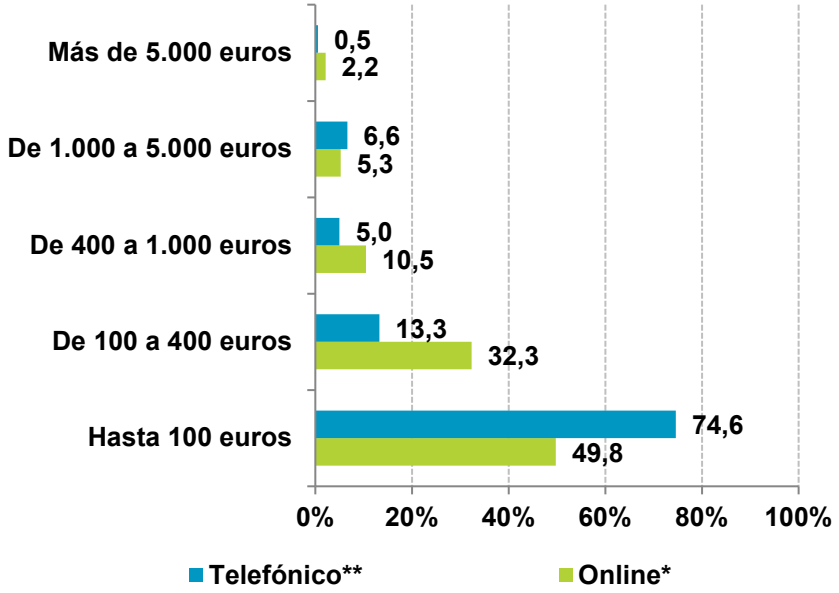
Las diferencias entre los resultados de los ordenadores del hogar y las plataformas Android, apoyan los estudios sobre el aumento del malware para las plataformas Android dirigido a fraude, y en especial el uso de ransomware para estos dispositivos, que es un tipo vinculado de forma más natural con las plataformas PC.

Mientras que las familias de troyanos bancarios para Android siguen apareciendo y evolucionando [21], aprovechándose de que los usuarios emplean cada vez más sus dispositivos personales para los trámites bancarios (impulsado también por soluciones como Bizum que naturalizan este uso), los troyanos bancarios siguen manteniendo su nicho en las plataformas PC.

6.2 Repercusión económica

En la siguiente figura se describen las cantidades monetarias estafadas declaradas por los panelistas.

FIGURA 38. DISTRIBUCIÓN DEL PERJUICIO ECONÓMICO DEBIDO A FRAUDES TELEFÓNICOS Y ONLINE (%)



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

El 74,6% de los usuarios afectados por fraude declaran pérdidas de hasta 100 euros por medio de un fraude telefónico (*vishing*), frente al 49,8% que declara la misma cantidad en el caso de fraude online. Para cantidades que oscilan entre 1000 y 5000 euros el fraude telefónico vuelve a superar al fraude online, aunque la diferencia no es tan significativa.

El fraude online puede resultar más fácil de realizar y también menos costoso en términos de recursos. Ambos dependen de las capacidades de ingeniería social del atacante o las personas contratadas para perpetrar el engaño. Como parte de su labor de difusión INCIBE ha preparado un conjunto de vídeos explicando diferentes tipos de fraude, entre los que se encuentra el *vishing*, la modalidad telefónica del *phishing*[22].

[21] https://www.welivesecurity.com/la-es/2020/11/26/informe-de-amenazas-de-eset-para-el-tercer-trimestre-de-2020/

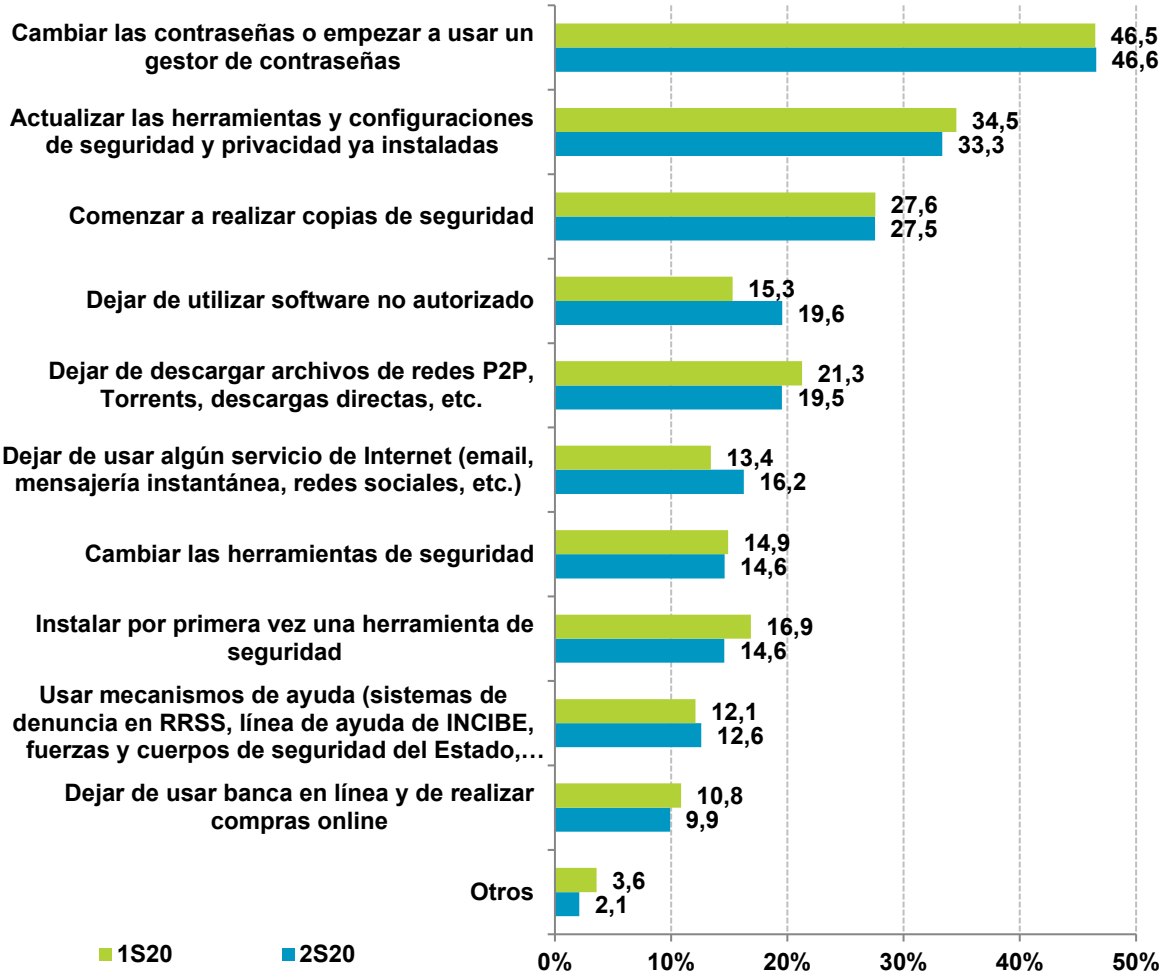
[22] https://www.incibe.es/aprendeciberseguridad/vishing

Para defenderse ante este y otros tipos de fraude es imprescindible mantenerse informado, la concienciación y actuar con cautela siempre desde el paraguas de la información. Siempre debemos evitar proporcionar datos confidenciales, nuestra entidad bancaria (de ser el caso) tiene ya nuestros datos. Ante la duda, finalizar la llamada y contactar directamente con la entidad bancaria es lo más recomendable.

6.3 Cambios de hábitos tras un incidente de seguridad

Al igual que ocurriría con un accidente en el plano no virtual, sufrir un incidente de seguridad puede motivar el cambio de hábitos de cualquier persona. La FIGURA 39 muestra los cambios de hábitos declarados por los panelistas tras sufrir un incidente de seguridad.

FIGURA 39. 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

Destaca el aumento del porcentaje de aquellos que dejan de usar software no autorizado, que estaría relacionado con la disminución de las descargas en redes P2P y el pago de servicios que proporcionan contenidos digitales (ver sección 2).

También señalan el 16,2% de los panelistas que han optado por dejar de usar algún servicio de Internet. Esto podría tener relación con los incidentes de suplantación o con la necesidad de minimizar la exposición de información personal.

El cambio de contraseñas continúa siendo uno de los hábitos más señalados tras un incidente de seguridad, junto con la actualización de las herramientas del equipo. La percepción sobre la necesidad del cambio de herramientas de seguridad continúa siendo la misma que en la oleada anterior, lo que indica que no se haya considerado, por parte de un mayor número de panelistas, la necesidad de nuevas herramientas para enfrentarse a nuevos problemas o mejorar la detección.

El 12,6% de los usuarios ya aprovecha los Mecanismos de Ayuda

La utilización de los mecanismos de ayuda sigue creciendo (12,6%), aunque la diferencia respecto de la oleada anterior es tan sólo de 0,5 p.p. No obstante es muy buena noticia y cabe esperar que sea un hábito que cada vez se inculque más en la sociedad.

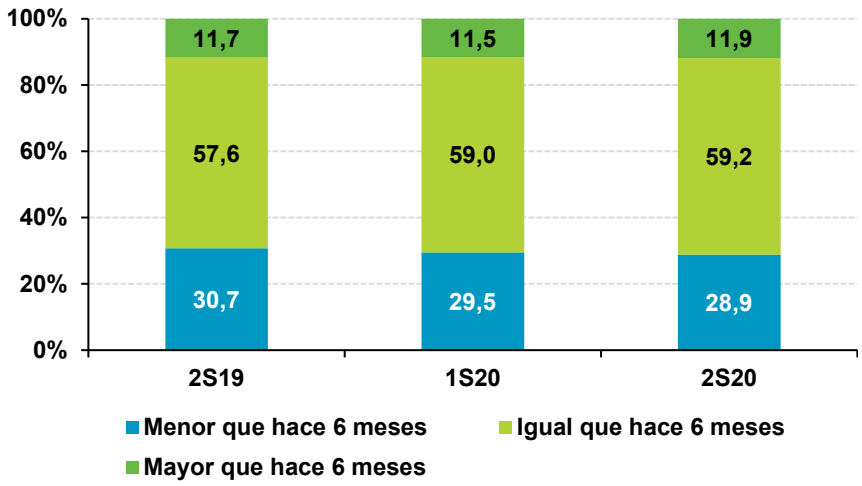
7 Confianza en el ámbito digital en los hogares españoles

Se recogen a continuación las declaraciones de los internautas sobre los riesgos que perciben al navegar por la red, así como sus opiniones sobre la seguridad en Internet.

7.1 Evolución de la percepción de las incidencias y el riesgo

La percepción de la cantidad de incidencias de ciberseguridad es muy similar a la de los semestres anteriores. Tan sólo el 11,9% de los usuarios estima que las incidencias hayan aumentado más que hace seis meses, aumentando este valor sólo 0,4 p.p. respecto del semestre anterior.

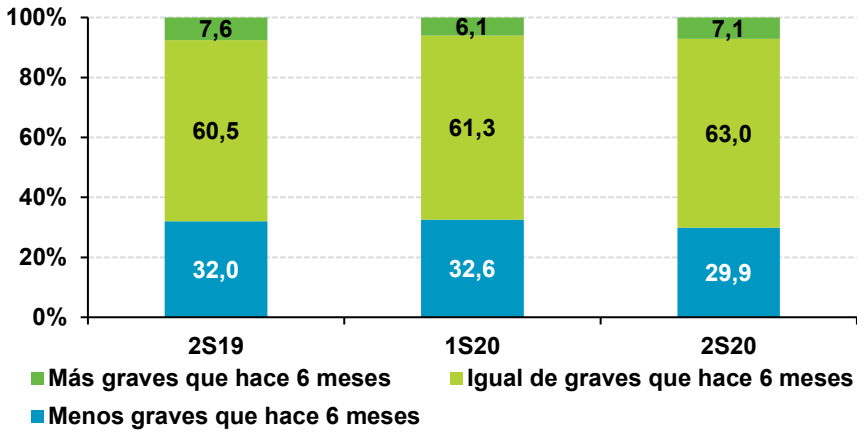
FIGURA 40. EVOLUCIÓN DE LA PERCEPCIÓN DE LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

La percepción de la gravedad de las incidencias también se incrementa ligeramente, considerando el 7,1% de los usuarios que los incidentes que ocurren son más graves que hace seis meses. Esto se puede asociar al aumento del nivel de peligrosidad en el malware identificado en los ordenadores del hogar, aunque no así en el caso de los dispositivos Android. No obstante, no hay que olvidar que en este caso las incidencias no van sólo referidas al malware, sino también a fraudes y otros incidentes identificados por los usuarios en apartados anteriores.

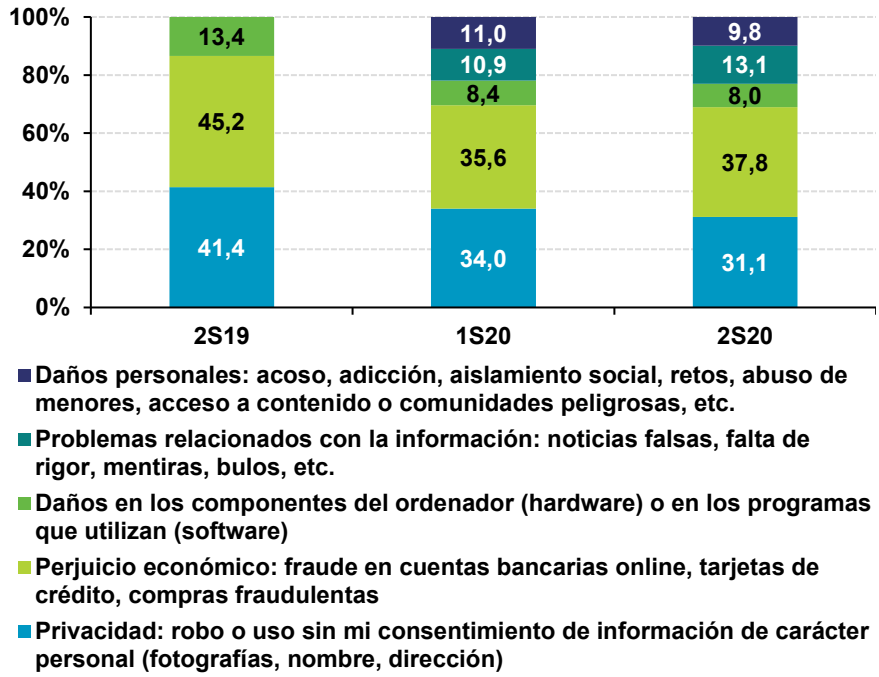
FIGURA 41. EVOLUCIÓN DE LA PERCEPCIÓN DE LA GRAVEDAD DE LAS INCIDENCIAS DE SEGURIDAD (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

La percepción del fraude con perjuicio económico y también de las noticias falsas ha aumentado en este último semestre (2,2 p.p. en ambos casos).

FIGURA 42. EVOLUCIÓN DE LA PERCEPCIÓN DE LOS RIESGOS EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

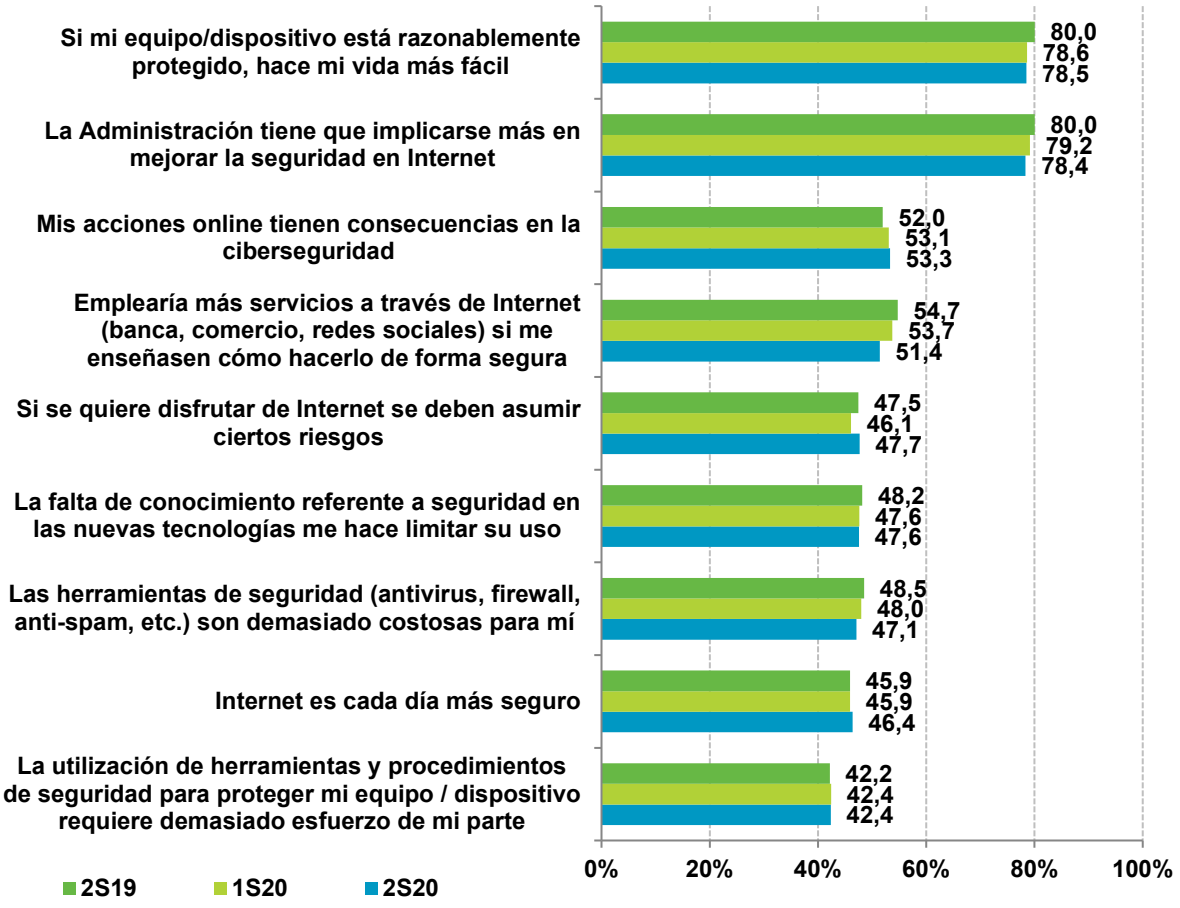
Para detectar noticias falsas (*fake news*) se recomienda, entre otros hábitos[23]: comprobar siempre la fuente, verificar al autor y al medio de la noticia. Como buena práctica siempre hay que evitar divulgar noticias de las que no estemos completamente seguros, y contrastar las noticias siempre. Una de las comprobaciones también puede ser verificar si la fuente es un *bot*, es decir, un perfil falso creado para dar veracidad a noticias falsas[24].

Por otra parte también cabe destacar que disminuye la percepción de problemas de privacidad, aunque con escasa diferencia respecto del primer semestre. Esta percepción podría influir en la creencia por parte de los panelistas de que los mecanismos de cifrado no serían necesarios. Sin embargo, también se ha visto a lo largo del informe cómo se han dado más incidentes de suplantación de identidad que el semestre anterior (ver sección 5.1).

7.2 Opiniones sobre la seguridad en Internet

La siguiente figura ofrece el punto de vista de los usuarios sobre la evolución de la seguridad en Internet.

FIGURA 43. EVOLUCIÓN DE OPINIONES SOBRE LA SEGURIDAD EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

[23] https://www.osi.es/es/campanas/bulos-fake-news-fraudes

[24] https://www.osi.es/es/guia-fraudes-online

Los resultados son similares a los de los semestres anteriores, con algunos matices a destacar.

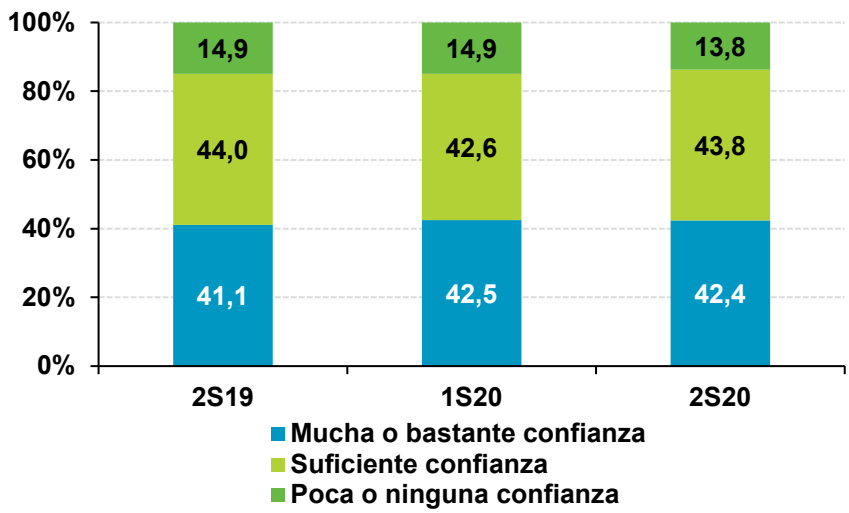
El 47,1% de los usuarios indica que las herramientas de seguridad son costosas, y sin embargo la FIGURA 6 ofrece una visión que contrasta los datos declarados de herramientas versus los datos reales de uso en la que se muestra que muchos usuarios creen no estar empleando herramientas que finalmente sí usan.

Por un lado podemos extraer la lectura de que tal vez los ciudadanos no conozcan la seguridad que proporciona sus ordenadores y dispositivos móviles de forma nativa, o las ventajas de seguridad que presentan las actualizaciones. Puede que ya intuyan que es necesario tener los equipos y dispositivos actualizados para minimizar las vulnerabilidades, pero no conozcan plenamente las ventajas de seguridad que ofrecen y de las que hacen uso sin saberlo.

Por otro lado hay herramientas gratuitas de seguridad, y páginas de confianza donde podemos conocerlas como la OSI[25], en las que además se ofrece información desinteresada sobre su uso.

El efecto de las mejoras de seguridad en las últimas versiones de las plataformas más usadas del estudio (Windows y Android) puede que influya en la percepción de que Internet es cada día más seguro, y motive a los usuarios a querer asumir más riesgos para disfrutar de la red.

FIGURA 44. EVOLUCIÓN DEL NIVEL DE CONFIANZA EN INTERNET (%)



Base: total usuarios
Fuente: Panel hogares, ONTSI

Respecto a la evolución del nivel de confianza, los porcentajes se mantienen prácticamente sin variaciones desde el semestre anterior disminuyendo ligeramente (-0,1 p.p.). Podría deberse a los casos de fraude identificados por los usuarios, aunque estas situaciones han compensado con otros factores la visión general que tienen los internautas de la confianza en la red de redes.

[25] https://www.osi.es/es/herramientas

8 Conclusiones

Este estudio corresponde al segundo semestre de 2020, aún marcado por la pandemia de la COVID-19, donde las restricciones de movilidad y también situaciones de enfermedad y otras causas han quedado reflejadas y han influido en el contexto del análisis.

Una de las primeras conclusiones que se extraen del informe es que aún hay importantes reticencias por resolver en materia de concienciación y formación dirigida a la ciudadanía. Pese a que es cierto que se realizan numerosas campañas muy bien enfocadas y dirigidas a diversos públicos, aún cuesta que los ciudadanos comprendan del todo qué herramientas tienen ya a su alcance en sus propios dispositivos. El concepto de "seguridad nativa" podría ser una asignatura pendiente en el mapa de estrategias para la concienciación ciudadana.

Más aún, la utilidad del cifrado de los datos parece no percibirse completamente, tampoco en colectivos tan importantes como la comunidad de usuarios trabajadores. Estas soluciones también las incorporan hoy día numerosas plataformas de forma nativa. Otras soluciones de seguridad, como las máquinas virtuales, resultan muy útiles en entornos corporativos y de educación, y sin embargo siguen siendo grandes desconocidas para un porcentaje importante de usuarios.

Además de las mejoras de seguridad en las propias plataformas, encontramos que los usuarios declaran haber disminuido sus conductas de riesgo. Esto también es muy positivo y se ha demostrado que tanto este como otros factores han mejorado los resultados, como el auto-confinamiento o la reducción de exposición, al minimizar por ejemplo la conexión a redes Wi-fi públicas.

No obstante los incidentes relacionados con la suplantación de identidad han destacado a lo largo del estudio, así como las precauciones que hay que tomar frente a dichas situaciones y cómo actuar en el caso de que seamos víctimas de este tipo de ataques.

Por otro lado, los datos reales indican que en este semestre hubo una reducción –aunque no demasiado marcada– de los casos de infecciones en los ordenadores del hogar y los dispositivos Android. Es una buena noticia que no obstante debe tomarse con cautela por el contexto social del estudio, en el que aún nos encontramos en una situación de pandemia global, y donde parte de los integrantes del estudio se han visto afectados directamente.

Los intentos de fraude declarados se mantienen casi como en el semestre anterior, aunque la repercusión económica de éstos se ha hecho notar. El 2,2% de los panelistas destacó pérdidas superiores a los 5000 euros debidas al fraude online, frente al 0,5% que indicaba las mismas cantidades pero para el fraude telefónico. Los ataques de *vishing* (phishing telefónico) se han intensificado en el último año aprovechando la situación generada por la pandemia. El perfil reflejado en este estudio sugiere que el foco principal del *vishing* son estafas de hasta 100 euros, aunque esto podría variar en el futuro.

Por último, la confianza de los panelistas en la red de redes ha mejorado en el último semestre, aunque no de forma notable. Podría haber contribuido a esta mejoría la percepción no equivocada del conjunto de la muestra de la reducción de infecciones y amenazas durante el último semestre.

Se analizará en siguientes oleadas si tras la situación de pandemia en la que aún nos encontramos la percepción sobre la ciberseguridad en el hogar continúa mejorando de cara a la opinión de los ciudadanos.

Índice de figuras

FIGURA 1. situaciones vividas por los panelistas durante la covid-19 4
FIGURA 2. Contexto laboral de los panelistas 5
FIGURA 3. Afecciones de los panelistas por tipo de población 5
FIGURA 4. Uso declarado de servicios de Internet (%) 6
FIGURA 5. Acceso a cursos y formación online según la actividad realizada por los usuarios (%) 7
FIGURA 6. Uso declarado vs real de medidas de seguridad en el ordenador del hogar (%)..... 8
FIGURA 7. Sistemas operativos en los ordenadores del hogar (%) – Dato real **¡Error! Marcador no definido.**
FIGURA 8. Uso real de medidas de seguridad en dispositivos Android (%)..... 10
FIGURA 9. Versiones de android en dispostivos móviles (%) 11
FIGURA 10. Motivos de no utilización de medidas de seguridad (%) 12
FIGURA 11. Panelistas que desconocen qué es una máquina virtual (%) 13
FIGURA 12. Panelistas que consideran necesario el cifrado (%) 13
FIGURA 13. Medidas de seguridad automatizables en el ordenador del hogar (datos declarados) 15
FIGURA 14. Medidas de seguridad activas en el ordenador del hogar (%) 16
FIGURA 15. Evolución de la adopción consciente de conductas de riesgo (%) 17
FIGURA 16. Realización consciente de alguna conducta de riesgo según personas trabajadoras, estudiantes y resto de población no activa (%) 17
FIGURA 17. Utilización de redes Wi-fi privadas y públicas (%) 18
FIGURA 18. Uso de descarga directa de archivos, programas, documentos, etc. (%) 19
FIGURA 19. Hábitos de comportamiento en el uso de redes p2p (%) 19
FIGURA 20. Instalación de programas (%) 20
FIGURA 21. Descarga de aplicaciones en dispositivos Android (%) 20
FIGURA 22. Hábitos de comportamiento en el uso de servicios de banca online o comercio ELECTRÓNICO (%) 21
FIGURA 23. Hábitos de comportamiento en el uso de Redes sociales (%)..... 22
FIGURA 24. Tecnologías activas en dispositivos ANdroid (%)..... 23
FIGURA 25. Evolución de las incidencias de seguridad (%)..... 23
FIGURA 26. Incidencias de seguridad por grupos de población afectados y no afectados por la covid-19 (%) 24
FIGURA 27. Evolución de la clasificación de las incidencias de seguridad (%)..... 25
FIGURA 28. Estado real de infección en el ordenador del hogar (%)..... 26
FIGURA 29. Peligrosidad del malware en el ordenador del hogar (%)..... 27
FIGURA 30. Evolución del malware en el ordenador del hogar (%) 28
FIGURA 31. Estado real de infección en dispositivos Android (%) 30
FIGURA 32. Peligrosidad del malware en dispositivos Android (%) 30
FIGURA 33. Evolución del malware en dispositivos Android (%) 31
FIGURA 34. Evolución de los intentos de fraude online (%) 32
FIGURA 35. Evolución de la manifestación de los intentos de fraude online (%) 33
FIGURA 36. Troyanos bancarios, ransomware y rogueware en el ordenador del hogar (%) 34
FIGURA 37. Troyanos bancarios, ransomware y rogueware en dispositivos Android (%) 34
FIGURA 38. Distribución del perjuicio económico debido a fraudes telefónicos y online (%)..... 35
FIGURA 39. Evolución de los cambios de hábitos tras sufrir un incidente de seguridad (%)..... 36
FIGURA 40. Evolución de la percepción de la cantidad de incidencias de seguridad (%)..... 37
FIGURA 41. Evolución de la percepción de la gravedad de las incidencias de seguridad (%)..... 38
FIGURA 42. Evolución de la percepción de los riesgos en Internet (%)..... 38
FIGURA 43. Evolución de opiniones sobre la seguridad en Internet (%) 39
FIGURA 44. Evolución del nivel de confianza en Internet (%) 40

El informe del *"Cómo se protege la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España"* ha sido elaborado por el siguiente equipo de trabajo del Observatorio Nacional de Tecnología y Sociedad (ONTSI):

Lucía Velasco
Alberto Urueña
Raquel Castro García-Muñoz
Santiago Cadenas Villaverde
José Antonio Seco Arnegas

Estudio realizado con asistencia técnica de:

NIPO: 094-21-113-5

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.

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

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