

OBSERVACIBER

INDICADORES SOBRE CONFIANZA DIGITAL Y CIBERSEGURIDAD EN ESPAÑA Y LA UNIÓN EUROPEA

Octubre 2021

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

1 Introducción 3

2 Destacados 5

3 Confianza de los ciudadanos en el entorno digital 9

4 Confianza en el entorno digital en las empresas 29

5 Índice global de ciberseguridad 43

6 Conclusiones 47

7 Referencias 49

1 INTRODUCCIÓN

ObservaCiber publica el dossier de indicadores sobre la confianza y ciberseguridad en España y en la UE 27, elaborado por el ONTSI, en el que se recogen los principales indicadores que reflejan el grado de confianza de los españoles en Internet, así como el uso que los hogares y las empresas hacen de las nuevas tecnologías para protegerse en la actividad digital que llevan a cabo con mayor o menor cotidianidad.

La digitalización de la información y la conectividad de la red están creando nuevos desafíos para la protección de los datos sensibles y las comunicaciones de la red, lo que afecta la confianza de las empresas y las personas en las actividades en línea. La pandemia de COVID-19 ha afectado drásticamente el funcionamiento de las sociedades. Desde el trabajo a distancia hasta el aprendizaje remoto, la tecnología ha desempeñado un papel clave para mantener a las personas conectadas. La adopción del teletrabajo por una gran parte de las personas trabajadoras y empresas españolas ha incrementado la vulnerabilidad de los sistemas y la posible pérdida de información y los datos de la propia compañía. La pandemia en curso ha creado desconfianza, especialmente en línea, y hay un mayor reconocimiento del riesgo de ciberseguridad.

Para que la transformación digital se produzca en todos los segmentos de la economía y la sociedad, es clave crear un entorno confiable y seguro en torno a la ciberseguridad. Las personas, las empresas y los gobiernos están expuestos a una variedad de incidentes de seguridad digital que tienen como objeto las infraestructuras críticas dependientes de la tecnología digital y los servicios esenciales como la energía, el transporte, las finanzas y la salud. La competitividad empresarial, la capacidad de innovar y posicionarse en el mercado pueden estar amenazados, poniendo en riesgo el funcionamiento básico de las economías y sociedades. Para que las empresas puedan minimizar la frecuencia y el impacto negativo de estos incidentes es necesario realizar una gestión eficaz de los riesgos de seguridad digital, de forma que se pueda aprovechar los beneficios de la transformación digital (OCDE, 2019).

El presente dossier ofrece una imagen integral de la protección TIC entre los individuos y las empresas españolas durante 2020 y su evolución en los últimos años, que sirve para conocer qué colectivos y sectores de actividad son los más desprotegidos. También es útil para analizar la evolución e impacto de estas medidas de seguridad en la transformación digital de las empresas y de la población.

El informe se divide en seis capítulos, incluyendo este primero de introducción. El segundo incluye los indicadores destacados sobre confianza digital tanto en empresas como entre la población. El tercer apartado analiza los principales indicadores sobre confianza de la ciudadanía en el entorno digital, y en el cuarto se analiza la confianza en el entorno digital en las empresas. Ambos análisis se hacen desde una perspectiva nacional, en la que se muestra la situación de España y la Unión Europea, poniendo en relación la realidad de nuestro país con la del resto de los Estados miembros. El apartado quinto describe el índice global de ciberseguridad publicado por la Unión Internacional de Telecomunicaciones (UIT), que mide el compromiso de los Estados miembros con la ciberseguridad. Por último, el apartado sexto incluye las principales conclusiones del informe.

A efectos de este dossier, se entiende por seguridad de las TIC aquellas medidas, controles y procedimientos aplicados a los sistemas TIC para asegurar la integridad, autenticidad, disponibilidad y confidencialidad de datos y sistemas. Estas medidas incluyen la protección de los riesgos físicos, lógicos y por los propios usuarios que se pueden dar en el uso de las tecnologías.

Para la realización de este dossier se han utilizado los datos de la encuesta sobre el uso de TIC y comercio electrónico en las empresas del Instituto Nacional de Estadística (INE ETICCE, 2020), y la encuesta sobre equipamiento y uso de tecnologías de la información y comunicación en los hogares del INE (INE ETICH, 2020). Para la comparativa europea se han usado las mismas encuestas en el ámbito europeo que armoniza y recopila Eurostat: Community survey on ICT usage and eCommerce in Enterprises, y Community survey on ICT usage in Households and by Individuals: (Eurostat, 2021).

2 DESTACADOS

SE INCREMENTA LA DESCONFIANZA DE LA CIUDADANÍA EN EL ENTORNO DIGITAL: DOS DE CADA CINCO PERSONAS TIENEN POCA O NINGUNA CONFIANZA EN INTERNET.

- Aunque más de la mitad de la población (55,3%) tenía mucha (51,1%) o bastante (4,2%) confianza en Internet en 2020, el porcentaje con poca o ninguna confianza en internet se ha incrementado en 8,4 puntos en el último año, hasta alcanzar el 37,9%.
- Esta falta de confianza afecta negativamente a las transacciones *on-line*: en España, el 16% de las personas y en la Unión Europea el 6%, declaran que no realizan compras *on-line* debido a la preocupación por la privacidad o seguridad en el pago por Internet.
- También afecta negativamente al desarrollo de la administración electrónica. En 2020, en España el 19% y en Europa el 14% de quienes tuvieron la necesidad de enviar algún formulario y no lo hicieron, señalan como motivo su preocupación por la protección y la seguridad de sus datos personales.

MENOR PORCENTAJE DE INCIDENTES DE CIBERSEGURIDAD QUE AFECTEN A LAS PERSONAS EN ESPAÑA QUE EN LA UNIÓN EUROPEA DE MANERA GLOBAL, PERO MAYOR EN "*PHARMING*" (REDIRECCIÓN A PÁGINAS WEB FALSAS) Y EN PÉRDIDA DE DATOS EN MÓVILES COMO CONSECUENCIA DE ALGÚN VIRUS.

- El 28% de la población española sufrió algún incidente de ciberseguridad en 2019, por debajo de la media europea que se situó en el 34%.
- La recepción de mensajes fraudulentos *(phishing)* es la incidencia más destacable, el 19,2% la población española y el 26% de la europea lo sufrieron.
- Otro incidente destacable es la de ser redirigido a páginas web falsas que solicitan información personal *(pharming)*. En España afectó al 17%, por encima del 13% de la media de la UE.
- En 2020, el 8% de la población española que accede a Internet a través del móvil declaró pérdida de datos como consecuencia de un virus, por encima del 4% de la europea.

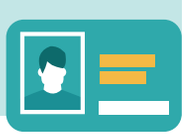
DESIGUAL USO DE SISTEMAS DE SEGURIDAD EN ORDENADORES Y MÓVILES ENTRE ESPAÑA Y LA UE.

- En España, algo más de la mitad de la población (52%) y en Europa algo menos (48%) realizaron copias de seguridad de archivos (documentos, imágenes, etc.) de sus ordenadores en 2019.
- En el móvil, el 31% de la población española y el 39% de la europea declaran disponer de algún sistema de seguridad instalado automáticamente o provisto con el sistema operativo del *smartphone* en 2020.



PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES: ELEVADO CONOCIMIENTO DE QUÉ SON LAS COOKIES (2 DE CADA 3 PERSONAS); POCAS ACCIONES PARA LIMITAR SU USO (1 DE CADA 3); Y ESCASA UTILIZACIÓN DE SOFTWARE ADICIONAL PARA LIMITAR EL SEGUIMIENTO (0,5 DE CADA 3).

- Una gran mayoría de la ciudadanía saben que las ***cookies*** se pueden utilizar para rastrear los movimientos de la gente en Internet. Así lo declara el 66% de la población española y el 69% de la europea en 2019.
- Sin embargo, no muchos realizan acciones para limitar el uso de las ***cookies***: en España lo hacen el 29% de la población, y en la UE27 el 32%.
- Son menos los que utilizan algún ***software*** que limite la capacidad de realizar un seguimiento de sus actividades de Internet, en España el 14% de las personas y en Europa el 17%.
- Respecto a la protección de datos personales, una gran mayoría (74%) de la población española realizó alguna acción para administrar el acceso a los datos personales en Internet en 2020.
- En el caso de las aplicaciones instaladas en el móvil, más de la mitad de la población española (57%) restringió o rechazó el acceso a datos personales al menos una vez en 2020, por encima de la media de la Unión Europea que se sitúa en el 52%.



PREPARACIÓN DE LAS EMPRESAS EN CIBERSEGURIDAD: AVANCES, PERO DESIGUAL PREPARACIÓN SEGÚN EL TAMAÑO DE LAS EMPRESAS.

- Más de la mitad de las empresas españolas habían definido una política de seguridad TIC en 2019, pero solo el 25% lo habían definido o revisado en los últimos 12 meses.
- El 33% de las empresas españolas disponían de documentación sobre seguridad TIC en 2019, un punto porcentual menos que la media de la UE28. Sin embargo, este porcentaje alcanza el 72% entre las grandes empresas españolas.
- El nivel de utilización de sistemas internos de seguridad TIC por las empresas españolas es muy alto, el 96,3% de las empresas declararon tener alguno en 2020.
- La medida de seguridad TIC más utilizada es disponer de *software* actualizado, el 97% adoptaron esta medida.
- Ante posibles incidencias de seguridad TIC muchas empresas disponen de un seguro para hacer frente a las mismas. En España el 18% de las empresas disponían de este tipo de seguro, por debajo de la media europea que se situó en el 24%.
- Para gestionar la seguridad TIC, las empresas españolas utilizan más recursos externos que internos: el 67% usan recursos externos frente al 38% internos.
- Mantener a las personas trabajadoras concienciadas y formadas sobre seguridad TIC es uno de los aspectos clave para reducir incidentes y afianzar la confianza digital en las empresas. En España el 21% de las empresas dan formación obligatoria de seguridad TIC, y el 41% voluntaria, valores por debajo de la media europea que se sitúa en 24 y 44% respectivamente.



INCIDENTES DE CIBERSEGURIDAD EN LAS EMPRESAS: POCOS INCIDENTES EN ESPAÑA Y EN LA UE.

- No son muchas las empresas que declaran haber sufrido incidentes de seguridad TIC. En España, el 9% de las empresas declararon que sus servicios TIC no estaban disponibles, misma proporción que en el caso de la media de la Unión Europea.

- Otro de los incidentes más habituales es que se produzca destrucción o corrupción de datos, lo que afectó en 2019 al 7% de las empresas españolas y el 5% de las empresas europeas.

ÍNDICE GLOBAL DE CIBERSEGURIDAD: ESPAÑA ENTRE LOS CUATRO PAÍSES MÁS COMPROMETIDOS CON ELEVAR EL NIVEL DE CIBERSEGURIDAD DEL PAÍS.

- España es uno de los países que exhibe un mayor compromiso con la ciberseguridad. Así lo refleja la cuarta posición que ocupa España en 2020 en el índice global de ciberseguridad elaborado por la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas para medir el compromiso de los países con la ciberseguridad.

- De todos los países analizados, solo está por detrás de EE. UU., Reino Unido, Arabia Saudí y Estonia, e iguala la posición con Corea del Sur y Singapur.

- En el contexto de la UE27, España (con una puntuación de 98,52 sobre 100) se encuentra en segunda posición, solo por detrás de Estonia (99,48 puntos).

3 CONFIANZA DE LA CIUDADANÍA EN EL ENTORNO DIGITAL

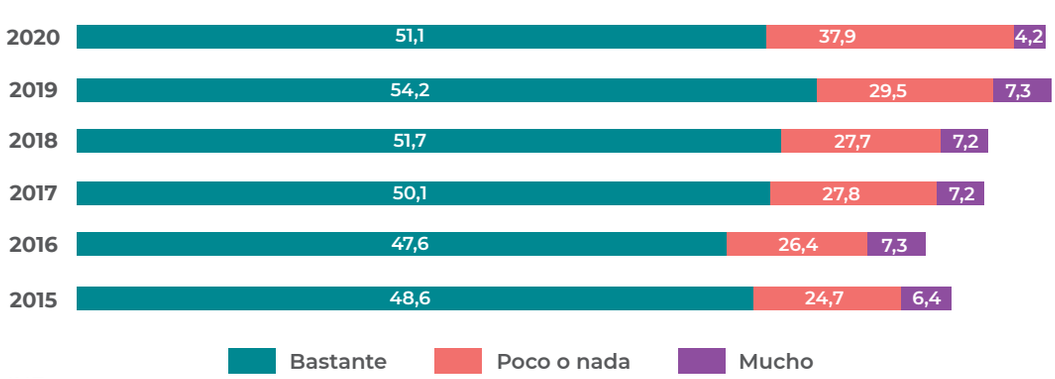
Dado que Internet impregna la mayor parte de las actividades cotidianas de las personas, la confianza en el entorno digital se ha convertido en uno de los factores clave en los que se sustenta las transacciones en la economía digital.

Los gobiernos, las empresas y las personas deben confiar y ser confiables para aprovechar todos los beneficios que ofrece la transformación digital.

La confianza en el entorno digital está directamente relacionada con la percepción que tiene la ciudadanía respecto de sus actividades en Internet, de forma que estas no le generen incidentes que acarreen perjuicios económicos, pérdida o mala utilización de la información personal, asegurando que esta se tratará con la debida privacidad, protegiendo sus datos personales.

En 2020, la mayor parte de la población española (55,3%) tenía mucha (51,1%) o bastante (4,2%) confianza en Internet. Aunque la tendencia de este indicador ha sido creciente desde 2015 a 2019, en 2020 esta ha disminuido, lo que se refleja en el porcentaje de personas que tienen poca o nada confianza en Internet, que pasó del 29,5% en 2019 al 37,9% en 2020. Con el tiempo, habrá que analizar si esta bajada en la confianza en Internet se debe a las consecuencias de la pandemia COVID-19.

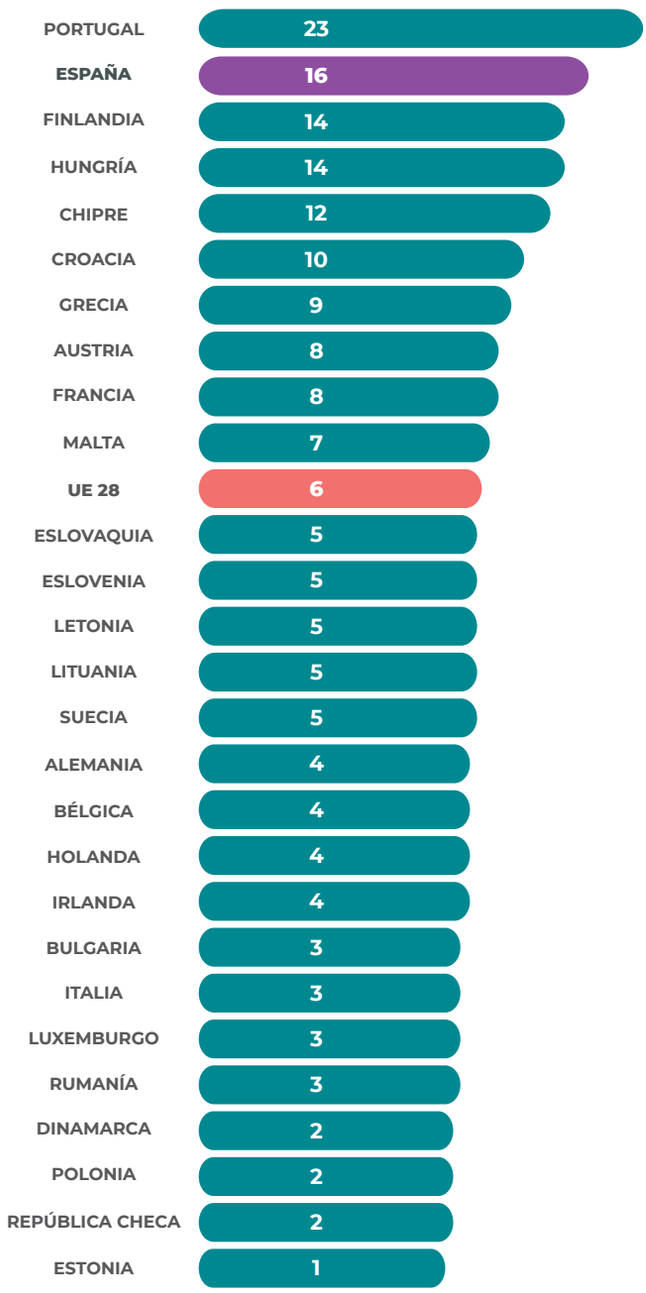
Ilustración 1. Grado de confianza en Internet en España



Fuente: **INE**

La falta de confianza en Internet tiene consecuencia directa en la disminución de las transacciones comerciales que las personas realizan por la red. La preocupación por la privacidad o seguridad en el pago por Internet es una de las razones que declara la ciudadanía para no comprar por Internet. Portugal (23%), España (16%), Finlandia (14%) y Hungría (14%) son los países en los que se da más este déficit de confianza en Internet. Sin embargo, este motivo lo aducen un porcentaje de personas significativamente menor en Dinamarca (2%), Polonia (2%), República Checa (2%) y Estonia (1%).

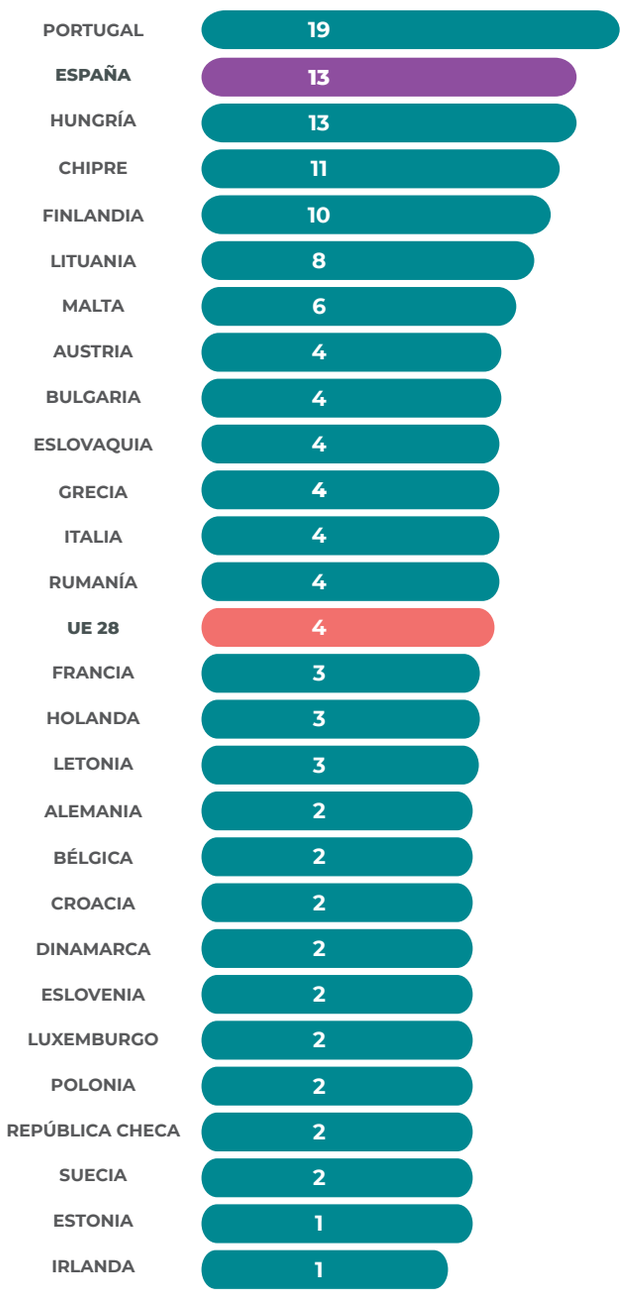
Ilustración 2. Personas que no compraron por internet porque le preocupa la privacidad o seguridad en el pago (Año 2019)



Fuente: **EUROSTAT**

Otra de las razones para no realizar compras en línea tiene que ver con la confianza respecto a los efectos posteriores a la transacción, por ejemplo, los relacionados con la recepción o devolución de productos, o inquietudes sobre reclamaciones e indemnizaciones. En 2019, estas preocupaciones afectaron al 13% de la población española, solo por debajo de los portugueses (19%). De media en Europa este motivo lo declaran el 4% de las personas para no comprar por Internet.

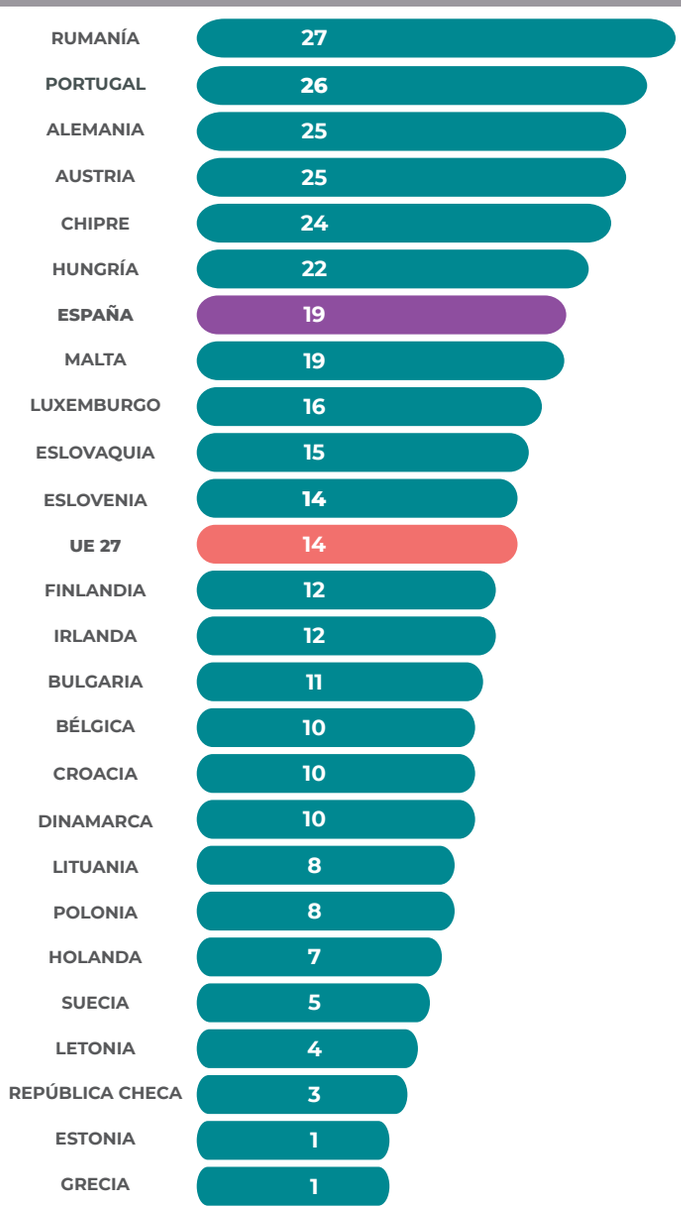
Ilustración 3. Personas que no compraron por Internet por falta de confianza en la recepción o devolución de los productos, en las reclamaciones o indemnizaciones (año 2019)



Fuente: EUROSTAT

La confianza de la ciudadanía en Internet también tiene reflejo en el desarrollo de la administración electrónica. La preocupación sobre la protección y seguridad de los datos personales es una de las razones que algunos alegan para no enviar formularios oficiales a las administraciones públicas por Internet. En 2020, el 19% de la población española y el 14% de la europea que tuvieron la necesidad de enviar algún formulario no lo hicieron por este motivo. La desconfianza es mayor en Rumanía (27%), Portugal (26%), Alemania (25%) y Austria (25%). Otras razones para no enviar formularios oficiales en España incluyen la falta de habilidades o conocimientos (35%) o por no estar disponible el servicio (12%).

Ilustración 4. Personas que no enviaron formularios cumplimentados para tratar con las AAPP a través de Internet por estar preocupadas por la protección y seguridad de los datos personales (año 2020)



Fuente: **EUROSTAT**

INCIDENTES DE CIBERSEGURIDAD EN LA CIUDADANÍA

Una parte de la percepción de la confianza de las personas en Internet tiene que ver con los incidentes sobre ciberseguridad que hayan padecido.

De media, en la UE27 el 34% de las personas experimentaron algún incidente de ciberseguridad en 2019. En España este problema es menor, afectando al 28% de la población. La percepción de incidentes es mayor en países avanzados en la transformación digital, destacando Dinamarca (50%), Francia (46%), Suecia (45%) y Países Bajos (42%). En el lado opuesto se encuentran Bulgaria (13%), Grecia (13%), Letonia (10%), Polonia (9%) y Lituania (7%).

La recepción de mensajes fraudulentos ***(phishing)*** es la incidencia más destacable. De media, el 26% de la población europea declara haber tenido este problema en 2019, con diferencias sustanciales entre los Estados miembros. Así, en Hungría el 45% de su ciudadanía declaró esta incidencia, frente al 3% en Lituania. En el caso de España este porcentaje alcanzó el 19,2%.

Otra incidencia que destaca es la de ser redirigido a páginas web falsas que solicitan información personal ***(pharming)***. En este caso, la percepción de la ciudadanía también es muy dispar entre los Estados miembros. En Malta (26%), Francia (20%), España (17%) y Suecia (16%) hay mayor percepción de este problema, por encima de la media de la UE27 (13%). Sin embargo, en Letonia (3%), Lituania (3%) y Bulgaria (2%) la percepción de este problema es muy baja.

En menor medida se detectan otros problemas o incidentes sobre ciberseguridad. Así, el acceso de los menores de edad a páginas web inapropiadas supone el 3% de los problemas detectados por la población española, y lo mismo ocurre con la europea.

También es bajo el porcentaje de personas que han experimentado pérdidas económicas debido al uso fraudulento de tarjetas de crédito, lo declaran el 3% de la población española y de la europea. Sin embargo, la percepción de este problema ha crecido desde 2010, si bien de forma ligera (2 puntos porcentuales).

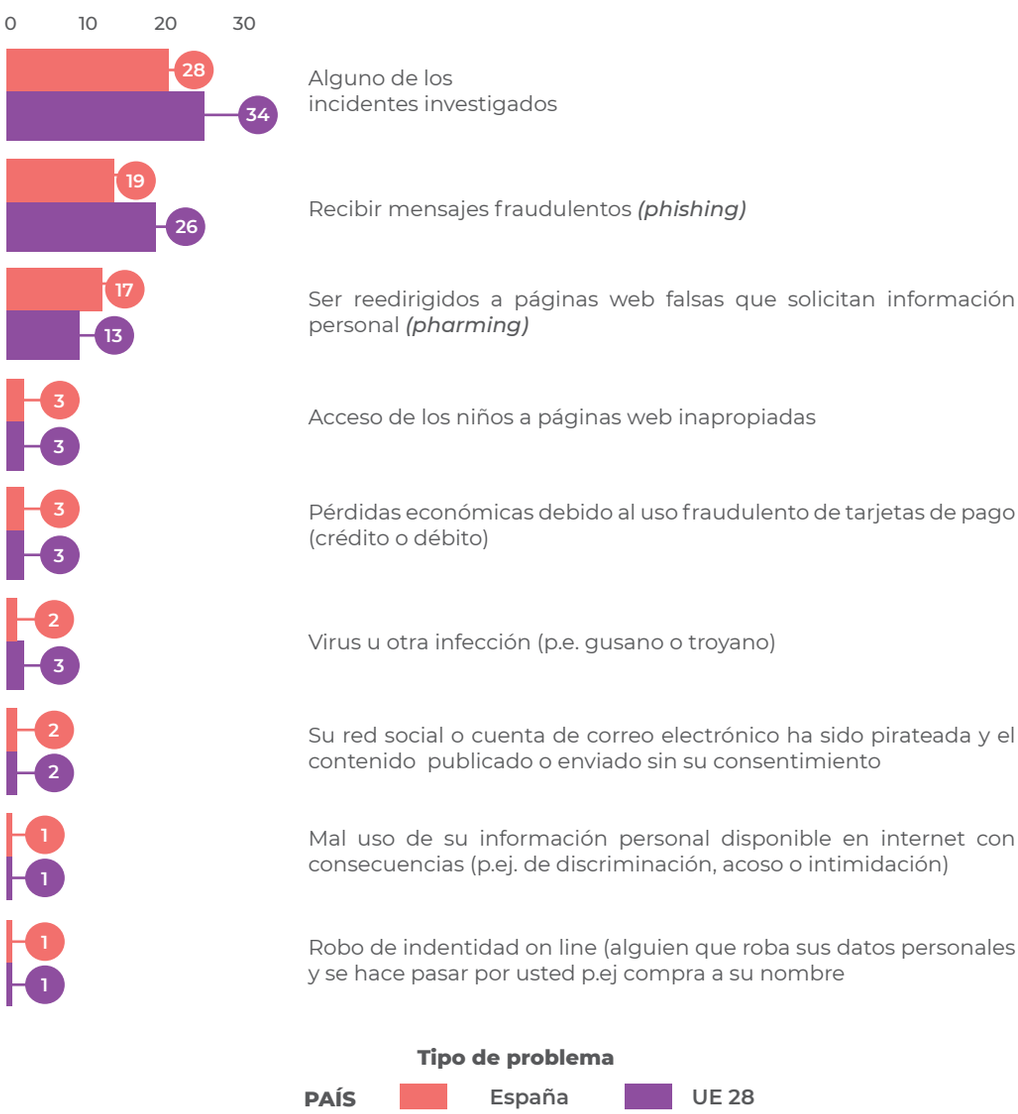
En el caso de la infección de virus u otro tipo de instalación (gusanos o troyanos, por ejemplo) la tendencia es la contraria: se ha producido un descenso notable desde 2010. Esto es debido posiblemente a la integración de software antivirus en los sistemas operativos y porque se ha incrementado el nivel de información y concienciación respecto de este tema (OCDE, 2019). Así, en España este problema lo había detectado el 22% de la población en 2010, mientras que en 2019 solo afectó al 2%. De media en la UE27 los porcentajes son similares, pasando del 22% en 2010 al 3% en 2021.

La percepción sobre el funcionamiento de las redes sociales y el correo electrónico es buena, solo el 2% de la población española declaró en 2019 que su red social o cuenta de correo electrónico había sido pirateada y su contenido publicado o enviado sin su consentimiento.

Muy poca población española y europea (1%) declaran un mal uso de su información personal disponible en Internet con consecuencias, como por ejemplo el acoso, discriminación o intimidación.

Por último, también es poca la población (1%) que declaran que habían sufrido el robo de identidad en línea.

Ilustración 5. Incidentes de seguridad en el uso de Internet en España y la UE27 (año 2019)



Fuente: **EUROSTAT**

En lo que respecta a incidentes en el uso del móvil, la pérdida de datos como consecuencia de un virus es un problema que declara el 8% de las personas españolas usuarias de Internet a través del móvil. España está entre los Estados miembros en los que este problema es mayor, después de Croacia (15%) y junto a Bulgaria (8%). De media en la UE27 la percepción de este problema es menor, solo el 4% de la población europea lo han experimentado.

Ilustración 6. Pérdida de datos en el móvil como consecuencia de un virus (año 2020)



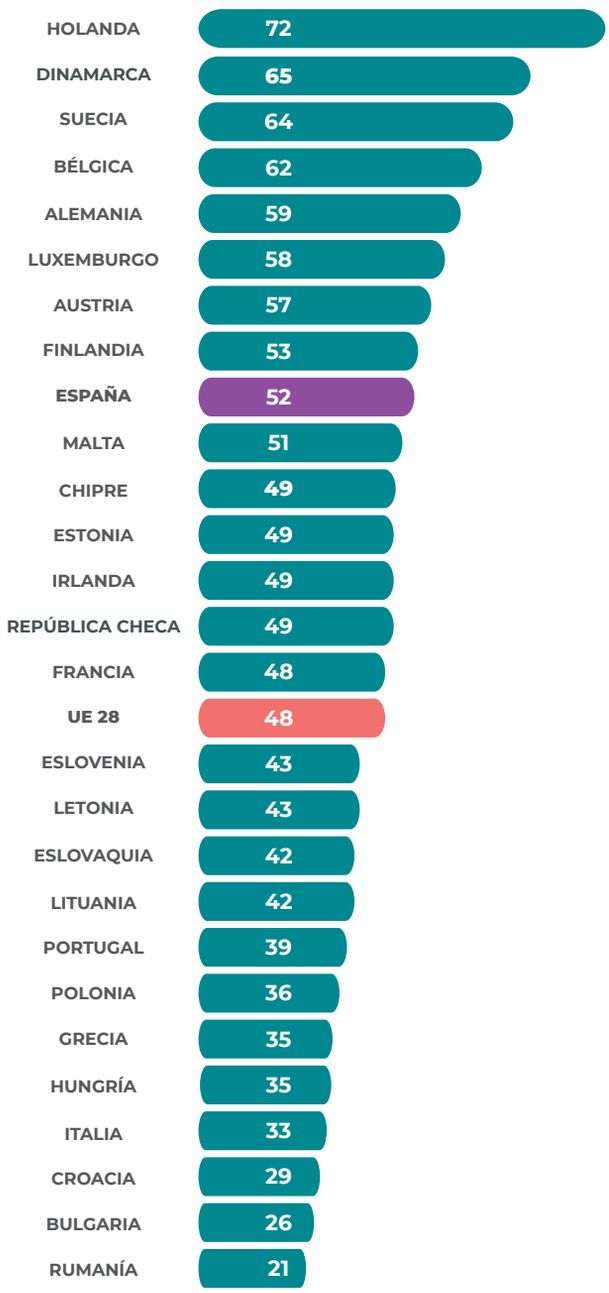
Fuente: **EUROSTAT**

PREPARACIÓN DE LA CIUDADANÍA EN CIBERSEGURIDAD

La gestión de los riesgos de seguridad digital y la privacidad es clave para fomentar la confianza en los entornos en línea entre los individuos. La conciencia de las amenazas a la seguridad y la privacidad y las competencias para prevenirlas y responder a ellas son cruciales para prosperar en la sociedad digital.

Una de las tareas más comunes para mantener la seguridad TIC entre los individuos es la realización de copias de seguridad de los datos que dispone en dispositivos electrónicos. En España, algo más de la mitad de la población (52%) realizaron copias de seguridad de los archivos (documentos, imágenes, etc.) de su ordenador en un dispositivo de almacenamiento externo (CD, DVD, disco duro externo, dispositivo de almacenamiento USB) o en un espacio de almacenamiento en Internet. El nivel de preparación de la población española en esta actividad está por encima de la media de la UE27 (48%), pero no alcanza a los países más avanzados digitalmente como Países Bajos (72%), Dinamarca (65%), Suecia (64%) o Bélgica (62%).

Ilustración 7. Personas que realizan copias de seguridad de sus archivos (año 2019)



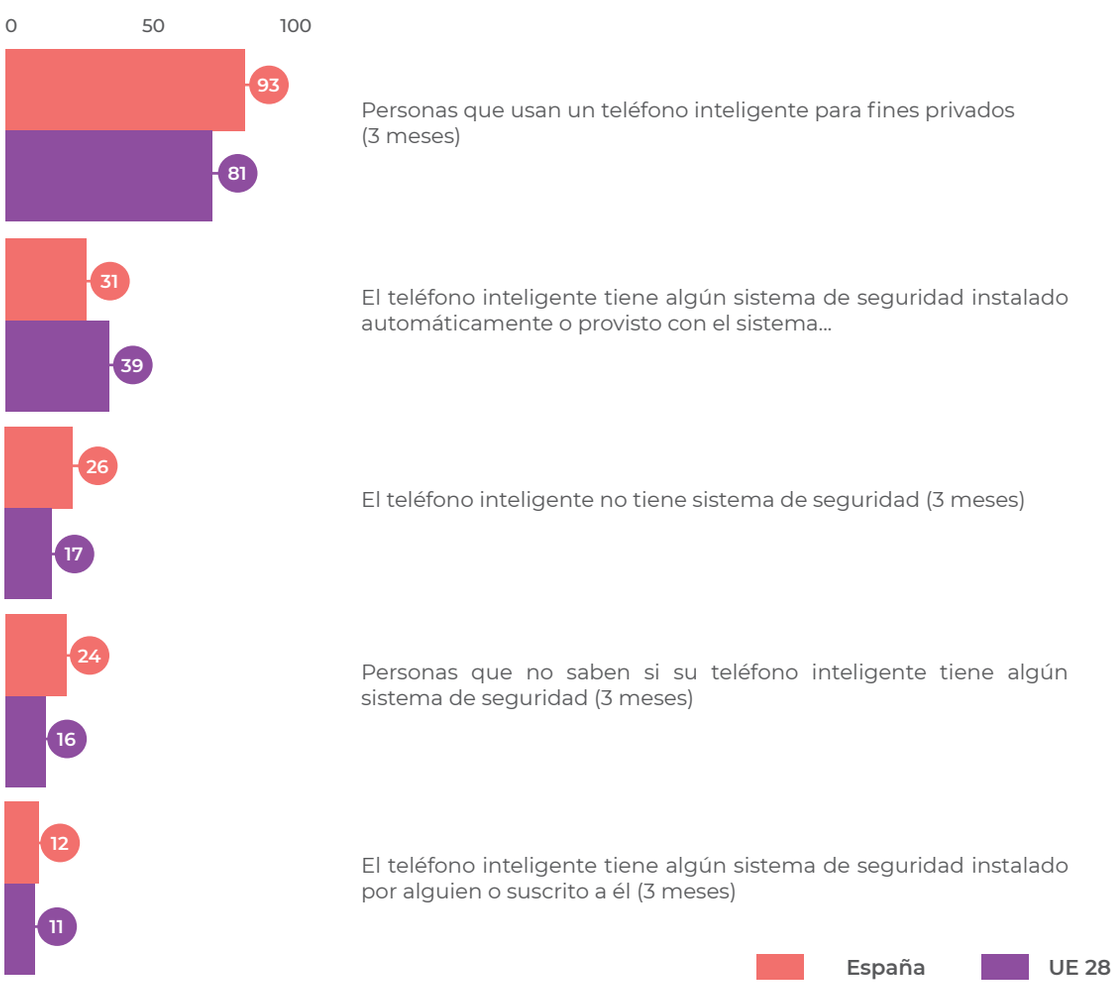
Fuente: **EUROSTAT**

La adopción casi universal de los teléfonos inteligentes y otros dispositivos de conexión a Internet en movilidad, otorgan a estos dispositivos un papel cada más importante en la vida cotidiana de las personas. El 81% de la población española y el 93% de la europea utilizaron el teléfono inteligente para fines privados. Disponer de mecanismos que sirvan para mantener la seguridad de estos dispositivos es de vital importancia para fortalecer la confianza digital.

El 31% de la población española declaran disponer de algún sistema de seguridad instalado automáticamente o provisto con el sistema operativo del ***smartphone***, y el 12% tiene algún sistema de seguridad instalado por alguien o está suscrito a él. En el caso de la población europea, estos porcentajes son del 39% y 11% respectivamente.

Sin embargo, hay un porcentaje no desdeñable de personas que declaran que no tienen un sistema de seguridad (26% en España y 12% en la UE27). Además, muchas desconocen su teléfono móvil dispone de algún sistema de seguridad (24% en España y 16% en la UE27).

Ilustración 8. Preparación sobre ciberseguridad en el uso del móvil (año 2020)



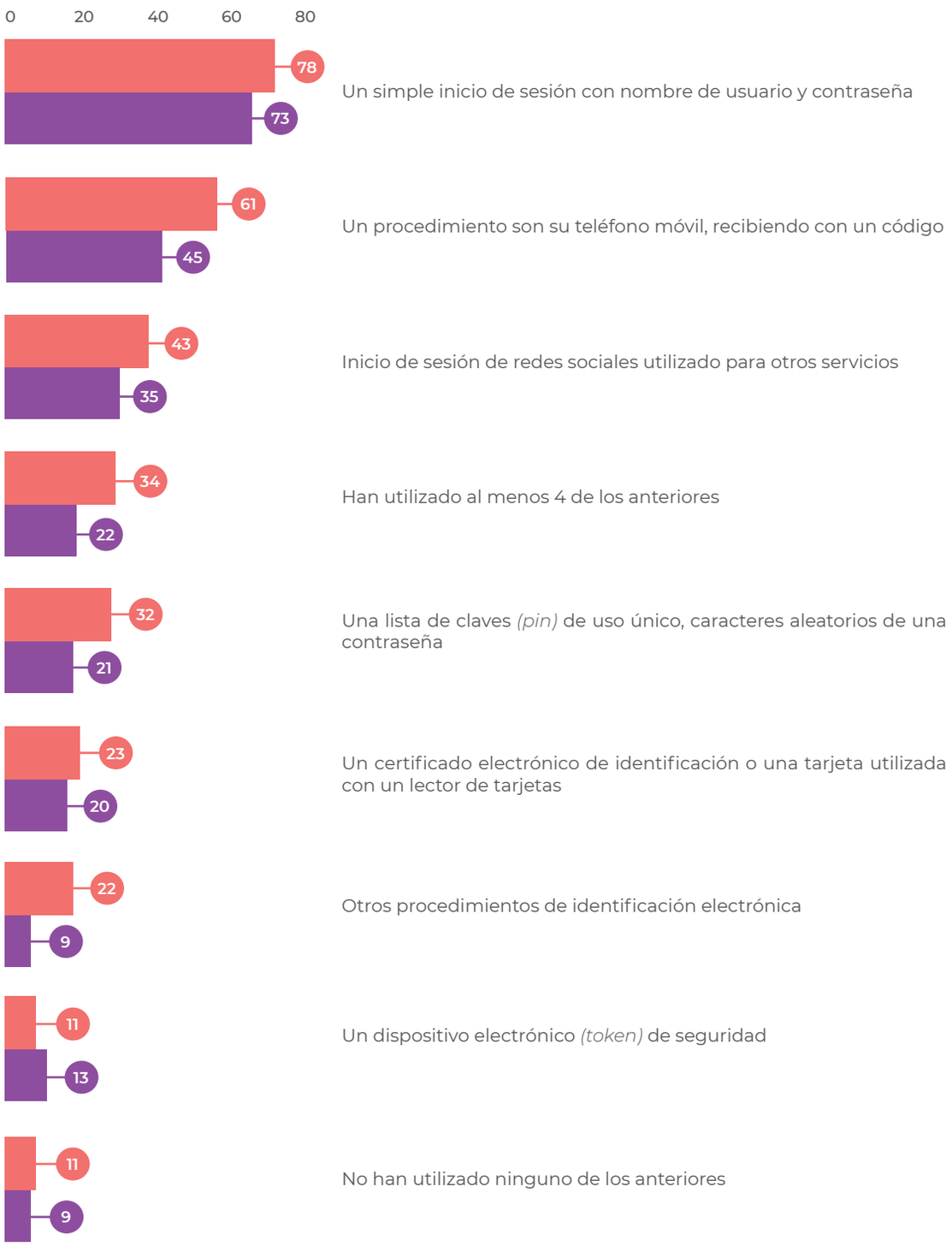
Fuente: **EUROSTAT**

La utilización de muchos servicios ***online*** disponibles en Internet exige la identificación de las personas que usan Internet para ofrecerles un servicio personalizado. La sofisticación de estos mecanismos incrementa la seguridad en el uso de estos servicios, pero a la vez exige un mayor grado de preparación de la ciudadanía, que necesitarán habilidades específicas para utilizar certificados electrónicos o dispositivos de seguridad. La capacitación permite a las personas aumentar su conciencia mientras adquieren más habilidades de privacidad y seguridad digital actualizadas en un contexto de rápidos cambios tecnológicos. Todo ello reforzará el grado de confianza de las personas en el uso de servicios ***online***, tanto en lo que se refiere al comercio electrónico como en la administración electrónica.

En Europa, los sistemas de identificación más utilizados son los más simples, y en algunas ocasiones, los menos seguros. Así, iniciar una sesión mediante usuario y contraseña lo emplean el 78% de la población española y el 73% de la europea. Le sigue en importancia los procedimientos que usan un código que ha sido enviado mediante un mensaje SMS al móvil. En España este procedimiento es más habitual que en Europa, el 61% de la población española lo usan frente al 45% de la europea. También es muy frecuente iniciar una sesión en una red social para utilizar servicios ***online*** de otros proveedores. En España lo hace el 43% de la población, y en la UE27 el 35%.

La utilización de sistemas más seguros, como los certificados electrónicos de identificación o una tarjeta utilizada con un lector de tarjetas, es menos frecuente, el 23% de la población española y el 20% de la europea lo emplean. La utilización de dispositivos electrónicos de seguridad, tipo token, (el 11% en España y 13% en la UE27) es menos habitual.

Ilustración 9. Personas que usan procedimientos de identificación para servicios *online* por tipo (año 2020)



Fuente: **EUROSTAT**

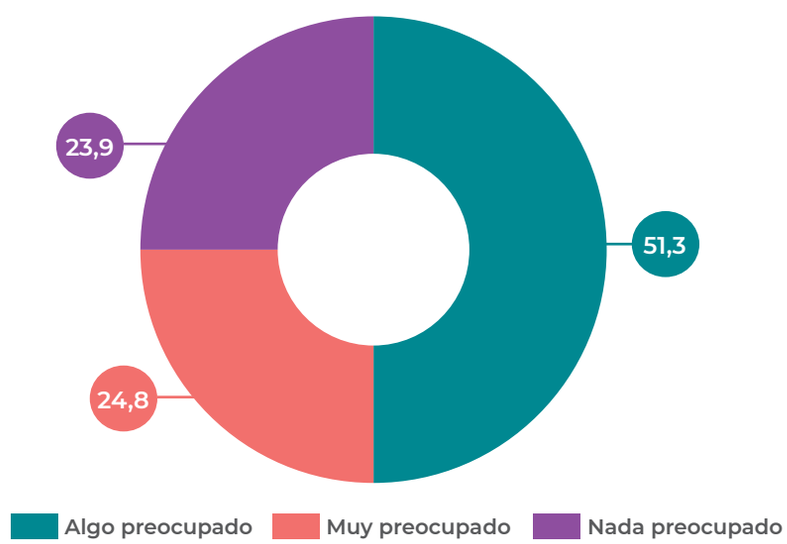
PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

La naturaleza intangible de los intercambios de datos dificulta que las personas controlen el uso y la reutilización de sus datos personales en diferentes jurisdicciones. Los datos personales se recopilan o acceden primero, luego se almacenan, agregan, procesan y finalmente se utilizan y analizan. La utilización de la inteligencia artificial permite que los datos también se puedan generar de forma automática. Cada uno de estos pasos tiene características especiales e involucra a diferentes partes interesadas. En la era digital, la confianza debe construirse entre las personas que poseen y consienten (aunque no siempre se dan cuenta de que lo han hecho) para proporcionar sus datos personales en línea, sin necesariamente controlar su uso, y las organizaciones que analizan y utilizan información de estos datos, respectando las leyes y la ética en torno a la recopilación, el almacenamiento, el análisis y el uso de los datos (OCDE, 2019).

Con la mayor disponibilidad de servicios en línea y redes sociales, las personas proporcionan cada vez más información personal, a veces sin saberlo, a proveedores de servicios y plataformas en línea.

En España, el 24% de la población está muy preocupada y el 51% algo preocupada porque las actividades que realizan en Internet estén siendo utilizadas para ofrecer publicidad.

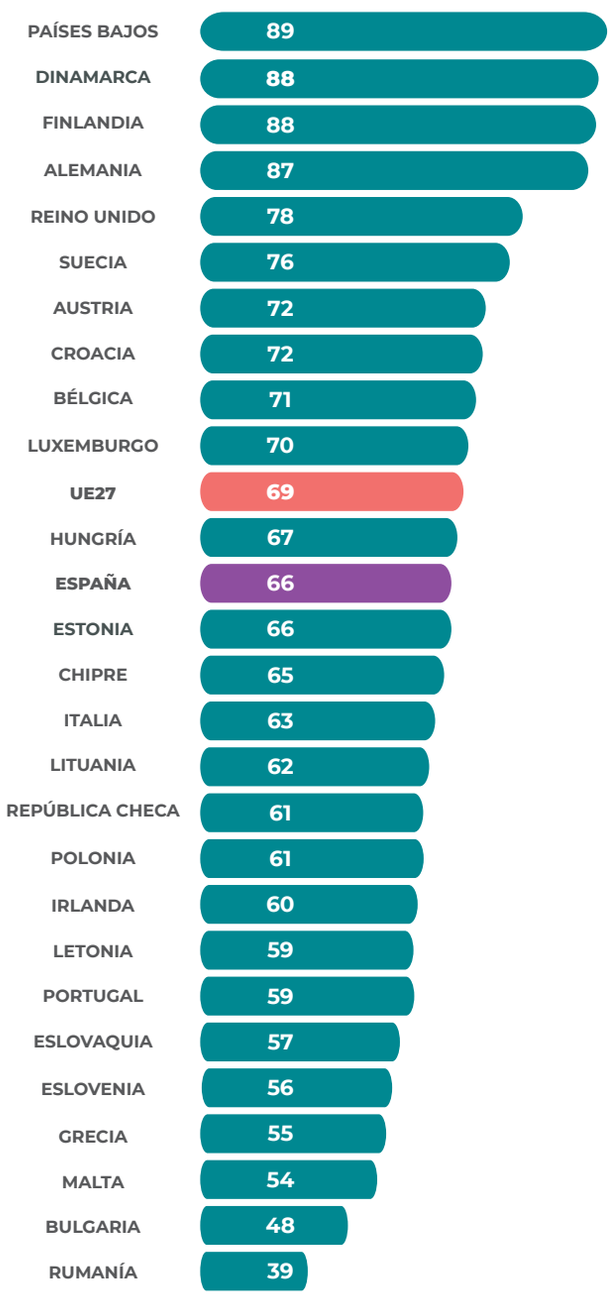
Ilustración 10. Grado de preocupación por que las actividades estén siendo registradas para ofrecer publicidad (año 2020)



Fuente: **INE**

Una gran mayoría de la ciudadanía europea sabe que las cookies se pueden utilizar para rastrear los movimientos de la gente en Internet. Así lo declaran 69% de la población europea y el 66% de la española. En Países Bajos (89%), Dinamarca (88%), Finlandia (88%) y Alemania (87%) el conocimiento es casi universal.

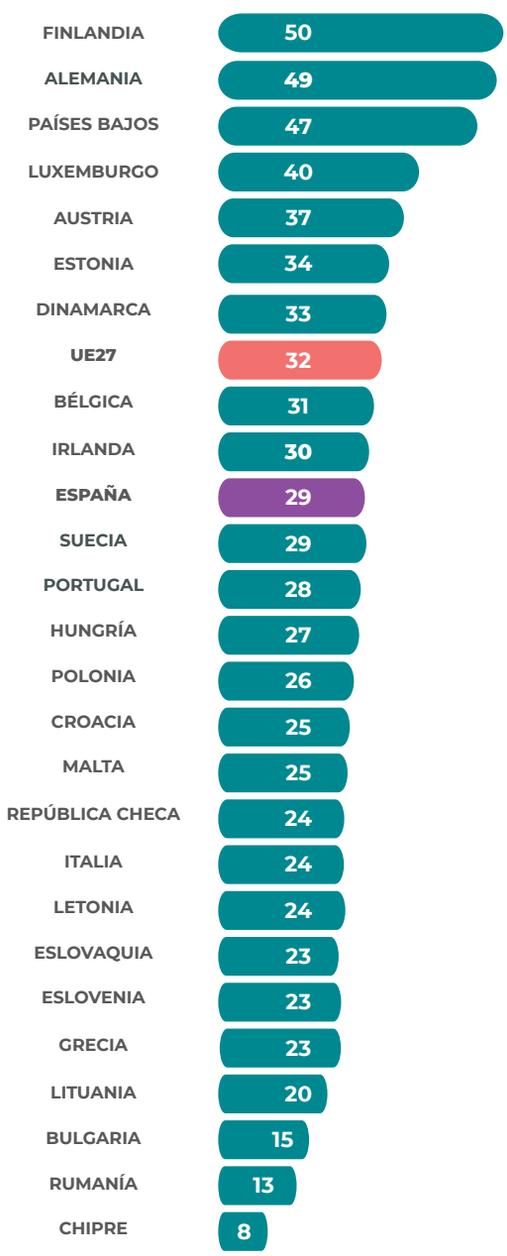
Ilustración 11. Personas que saben que las cookies se pueden utilizar para rastrear los movimientos de la gente en Internet (año 2020)



Fuente: **EUROSTAT**

Sin embargo, no muchos realizan acciones para limitar el uso de las cookies. De media, en Europa el 32% de las personas ha cambiado la configuración de su navegador de Internet para evitar o limitar las cookies en cualquiera de sus dispositivos. Esta actividad es menos frecuente en España, el 29% de los individuos lo hacen. Los países con mayor transformación digital son los que presentan mayor adopción de este tipo de acción por su ciudadanía, siendo Finlandia (50%), Alemania (49%) y Países Bajos (47%) los países con mayores porcentajes.

Ilustración 12. Personas que alguna vez han cambiado la configuración de su navegador de Internet para evitar o limitar las *cookies* en cualquiera de sus dispositivos (año 2020)

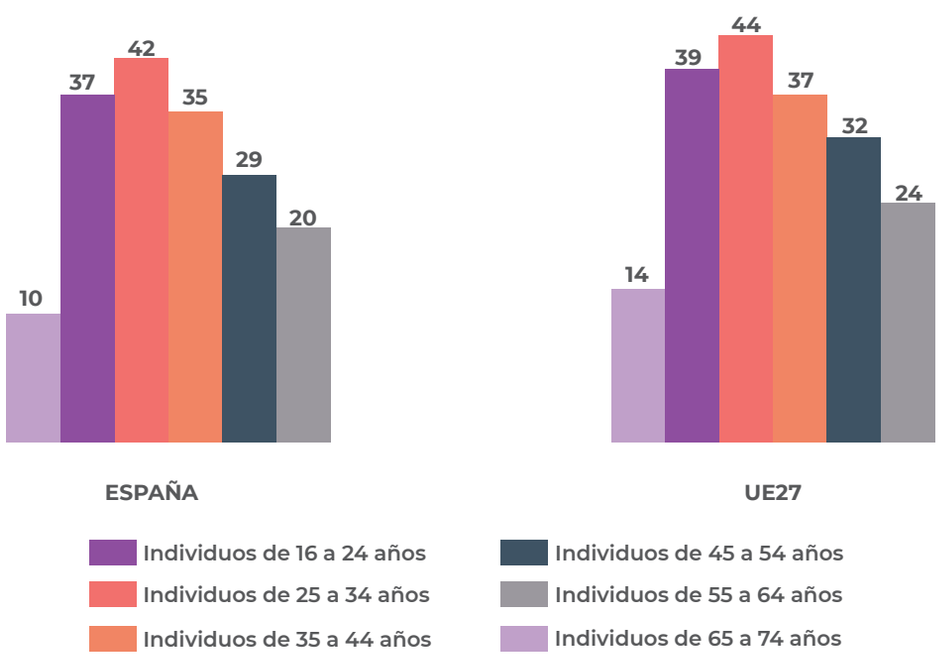


Fuente: **EUROSTAT**

Las personas con mayor formación oficial son las que realizan más este tipo de acciones, el 42% de la población española y el 46% de la europea. Estos porcentajes bajan entre las personas con formación oficial media al 31% en ambos casos. Y por último entre las personas de baja o sin formación oficial, estos porcentajes caen al 15 y 19% respectivamente.

También hay grandes diferencias entre las personas en esta actividad en función de la edad. Las personas de 25 a 34 años son los que más modifican el navegador para evitar o limitar las cookies, el 42% de las personas de esta edad lo han hecho. Esta actividad se va reduciendo a medida que tomamos segmentos de edad mayores, hasta llegar a las de 65 a 74 años, en las que solo el 10% realizan estos cambios.

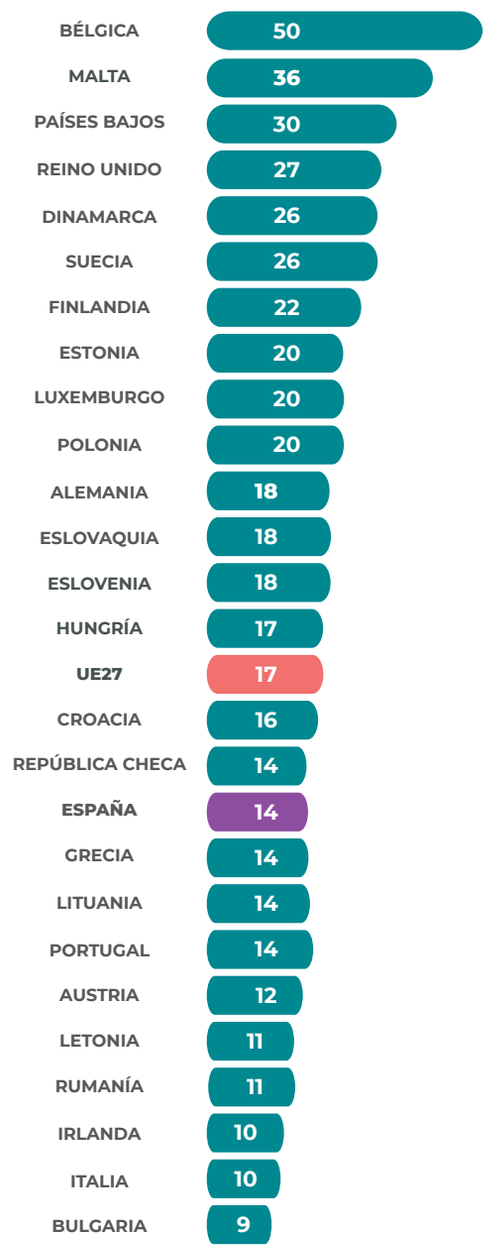
Ilustración 13. Personas que alguna vez han cambiado la configuración de su navegador de Internet para evitar o limitar las *cookies* en cualquiera de sus dispositivos por edad (año 2020)



Son aún menos las personas que utilizan algún software que limita la capacidad de realizar un seguimiento de sus actividades en Internet, en España solo el 14% de las personas, y en la UE27 el 17%.

Fuente: **EUROSTAT**

Ilustración 14. Personas que utilizan *software* que limita la capacidad de realizar un seguimiento de sus actividades en Internet (año 2020)

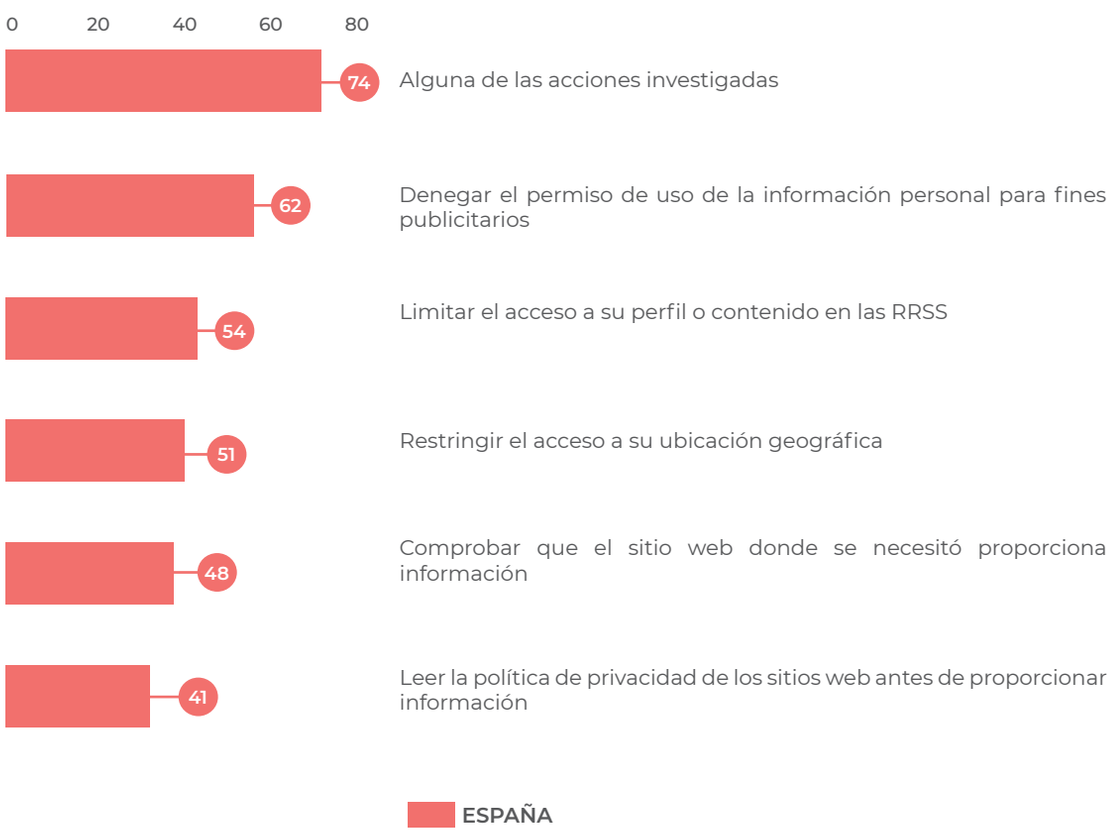


Fuente: **EUROSTAT**

La digitalización de la información y la conectividad de red mejorada crean nuevos desafíos para la protección de los datos personales, mientras que los ataques y el uso fraudulento se llevan a cabo de forma regular.

En España, el 74% de la población española realizó alguna acción para administrar el acceso a los datos personales en Internet. La acción más frecuente es la de denegar el permiso del uso de la información personal para fines publicitarios, el 62% de la población española y el 49% de la europea realizaron este tipo de acción. Países Bajos (73%) y Finlandia (70%) son los países con mayor porcentaje de personas que realizaron esta acción.

Ilustración 15. Personas que administraron el acceso a los datos personales en Internet en España (año 2020)



Fuente: **EUROSTAT**

Otra de las acciones más realizadas por las personas españolas fue la de limitar el acceso a su perfil o contenido en las redes sociales. El 54% de la población española lo realizó, siendo España uno de los países con mayor porcentaje de personas que realizan esta acción después de Países Bajos (63%), Finlandia (57%) y Austria (54%). La media europea se sitúa en torno al 38%.

El 51% de la población española restringió los enlaces a su ubicación geográfica, situándose por encima de la media de la Unión Europea, que es del 44%. En el caso de los países más avanzados digitalmente, como Países Bajos (75%), Finlandia (62%) y Dinamarca (62%), estos porcentajes son superiores.

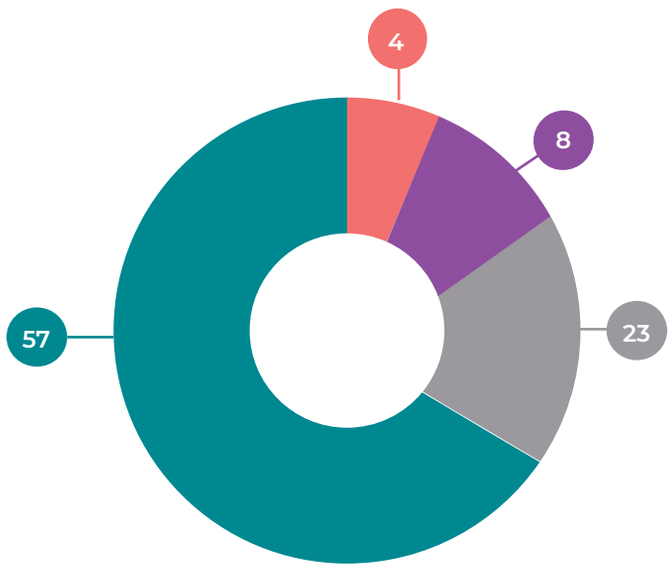
Comprobar que el sitio web donde se necesita proporcionar información personal es seguro es una actividad que realizan el 48% de la población española, muy por encima de la media europea, que es del 32%. Países Bajos (62%), Dinamarca (52%) e Irlanda (52%) son los países en los que esta práctica es más habitual.

Leer la política de privacidad de los sitios web antes de proporcionar información personal es una de las medidas que debería ser frecuente para administrar el acceso a los datos personales en Internet. Sin embargo, tanto en España (41%) como en la UE27 (40%) no es una actividad que realice una gran mayoría de la ciudadanía. El único país donde más de la mitad de la población realiza este tipo de actividades es Finlandia, con el 51%.

En el caso de las aplicaciones móviles, a menudo se solicita permiso, en el momento de uso o instalación, para acceder a los datos personales de la persona usuaria del móvil. En España, el porcentaje de población que han restringido o rechazado el acceso a datos personales al menos una vez es del 57%, por encima de la media de la Unión Europea, que se sitúa en el 52%. Los países con mayor porcentaje de población que rechazan el acceso a datos personales en las aplicaciones son Suecia (68%) y Alemania (65%).

El 23% de la población española no ha restringido o ha rechazado el acceso a datos personales cuando usa o instala una aplicación. El 8% no sabía que fuera posible restringir o rechazar el acceso a los datos personales en las aplicaciones y, por último, el 4% no usa aplicaciones con acceso a datos personales.

Ilustración 16. Individuos que usan restricciones al acceso a datos personales cuando usa o instala una aplicación en España (año 2020)



Fuente: **EUROSTAT**

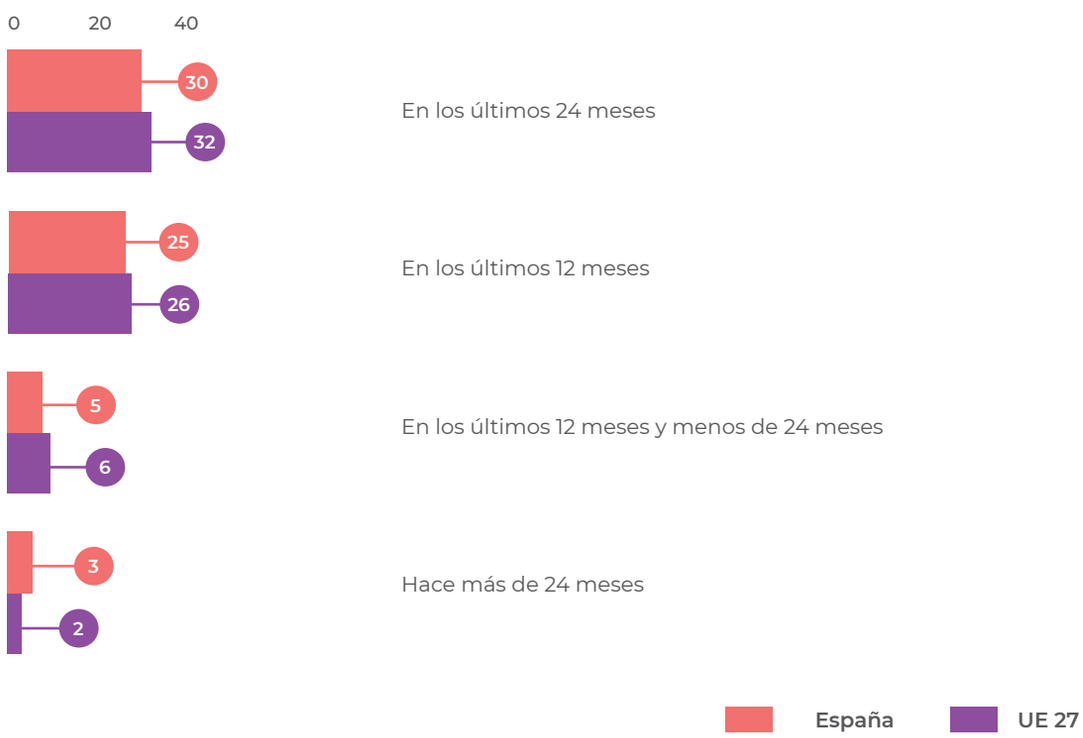
4 CONFIANZA EN EL ENTORNO DIGITAL EN LAS EMPRESAS

La capacidad de las organizaciones para gestionar los riesgos de seguridad digital y la privacidad es clave para fomentar la confianza en los entornos en línea. Desde una perspectiva empresarial, la gestión de los riesgos de seguridad digital debe integrarse en todo el proceso empresarial para que sea eficaz.

PREPARACIÓN DE LAS EMPRESAS EN CIBERSEGURIDAD

Disponer de una política formal de seguridad TIC es una señal de que una empresa es consciente de los riesgos digitales. En España, más de la mitad de las empresas habían definido una política de seguridad TIC, si bien varía el momento en el que esta se establece. El 30% de las empresas lo habían definido o revisado en los últimos 24 meses y, el 25%, en los últimos 12 meses.

Ilustración 17. Empresas que han definido formalmente una política de seguridad TIC (año 2019)

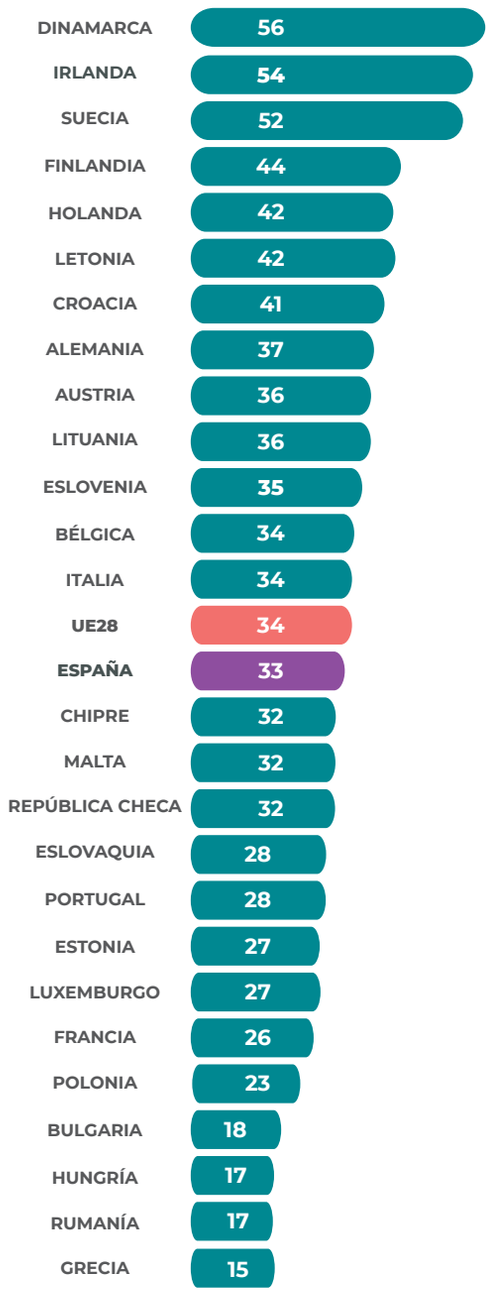


Fuente: **EUROSTAT**

Mantener documentación sobre seguridad TIC es una de las herramientas más importantes de toda política de seguridad. En 2019, el 33% de las empresas españolas disponían de documentación sobre seguridad TIC, un punto porcentual menos que la media de la UE28. Sin embargo, esta proporción varió ampliamente entre países y según el tamaño de la empresa. Mientras que, en algunos países, como Dinamarca (56%), Irlanda (54%) y Suecia (52%), más de la mitad de las empresas disponían de documentación sobre seguridad TIC, en otros, como Bulgaria (18%), Hungría (17%), Rumanía (17%) y Grecia (15%), estas no superaban el 20%.

Por tamaño de empresa, disponer de documentación sobre seguridad TIC es una práctica que realizan una gran parte de las grandes empresas españolas, el 72%, mientras que entre las pymes cae al 32% y en las pequeñas, al 30%.

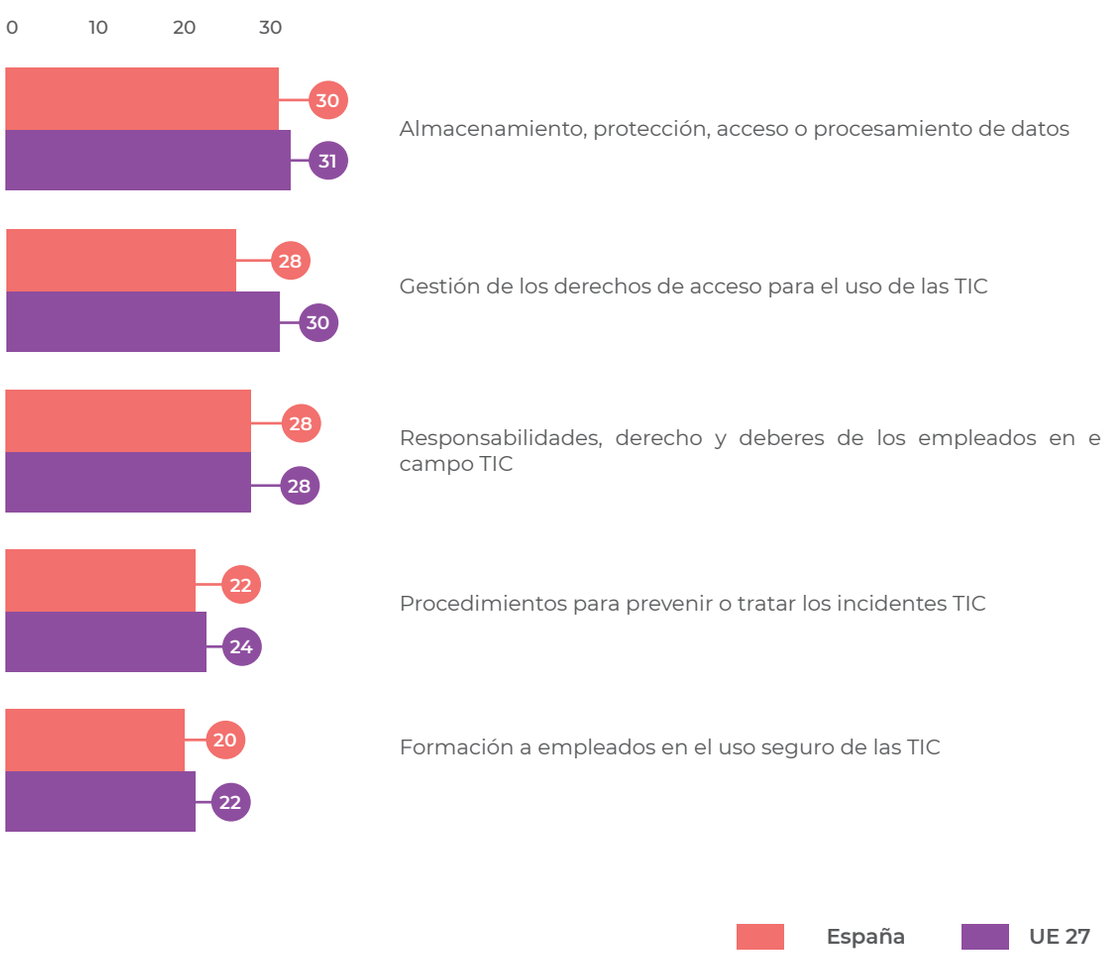
Ilustración 18. Empresas con documentación sobre seguridad TIC (año 2019)



Fuente: EUROSTAT

El tipo de documentación sobre medidas de ciberseguridad más utilizado por las empresas españolas tiene que ver con aspectos relativos al almacenamiento, protección, acceso o procesamiento de datos (30%). Le sigue la documentación sobre la gestión de los derechos de acceso para el uso de las TIC (28%) y sobre las responsabilidades, derechos y deberes de los empleados en el campo TIC (28%). Por último, los documentos sobre procedimientos para prevenir o tratar los incidentes TIC (22%) y la formación a personas empleadas en el uso seguro de las TIC (20%) son otros documentos que emplean las empresas españolas.

Ilustración 19. Empresas con documentación sobre seguridad TIC, por tipo de documentación sobre medidas de seguridad (año 2019)



Fuente: **INE**

En España, el 96,3% de las empresas utilizan sistemas internos de ciberseguridad. La medida más utilizada es la de mantener el ***software*** actualizado, el 97% de las empresas españolas declaran tenerlo. Otra de las medidas más usadas es realizar copias de seguridad de los datos en una ubicación separada, el 91% lo hacen. El 81% de las empresas españolas realizan control de acceso a la red. La autenticación mediante contraseña fuerte, es decir, con una longitud mínima de 8 valores alfanuméricos, la realizan el 76% de las empresas españolas. Además, el 52% de las empresas disponen de protocolos para el análisis de incidentes de seguridad de ciberseguridad. La red privada virtual o ***VPN*** es otra de las medidas que adoptan el 48% de las empresas. Otras medidas relevantes son la de realizar test de seguridad TIC (43%), incorporar técnicas de encriptación (43%), evaluación de riesgos TIC (39%) e identificación de usuario y autenticación mediante elementos biométricos (25%).

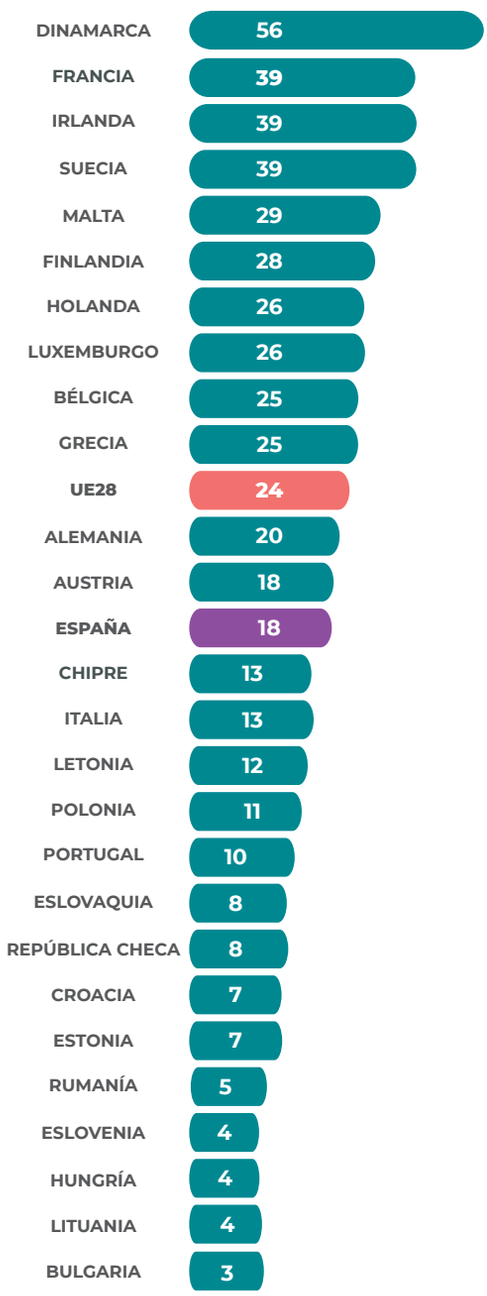
Ilustración 20. Empresas españolas que utilizan sistemas internos de seguridad por tipo (año 2020) (% / empresas que utilizan sistemas internos de seguridad TIC)



Fuente: INE

Ante posibles incidencias de seguridad TIC muchas empresas disponen de un seguro para hacer frente a las mismas. De media en Europa, el 24% de las empresas disponían de este tipo de seguro en 2019. En el caso de España este porcentaje es inferior, alcanzando el 18%. La adopción de este tipo de seguros es muy dispar entre los países de la UE. Así, mientras que en Dinamarca casi 6 de cada 10 empresas disponen de seguro, en otros países, como Rumanía (5%), Eslovenia (4%), Hungría (4%), Lituania (4%) y Bulgaria (3%), no se supera el 5%.

Ilustración 21. Empresas que tienen un seguro frente a incidencias de seguridad TIC (año 2019)

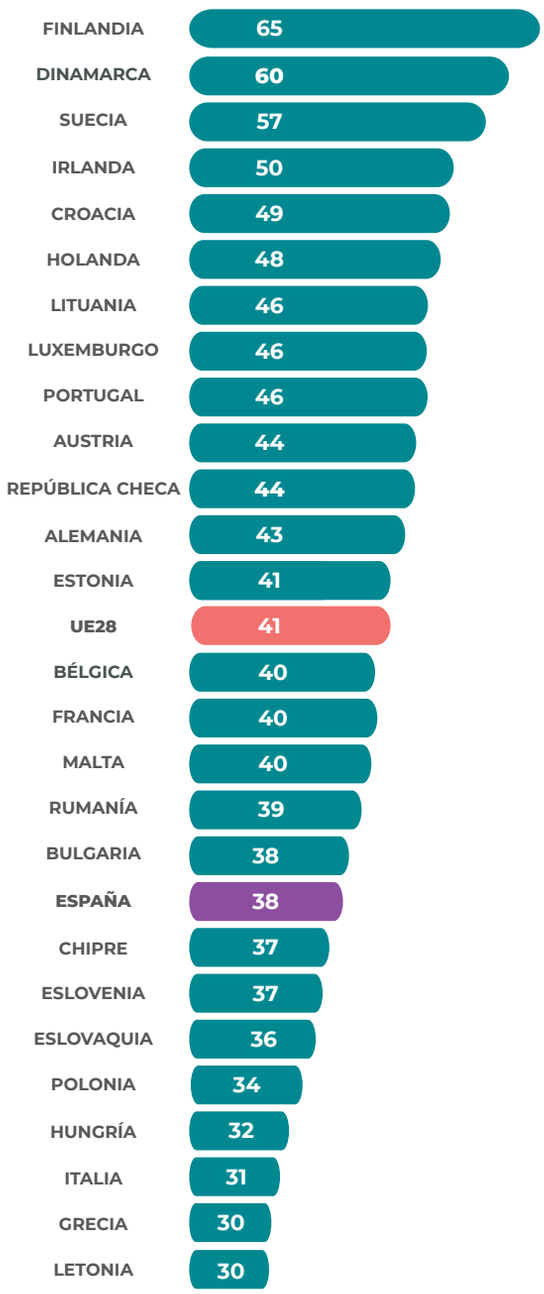


Fuente: EUROSTAT

La gestión de los riesgos de seguridad TIC puede ser realizado internamente por las personas empleadas o subcontratado según la estrategia comercial y la disponibilidad de recursos, incluidas las habilidades presentes en la fuerza laboral.

De media en la Unión Europea, en el 41% de las empresas las actividades relacionadas con la seguridad TIC son realizadas por el personal propio. En el caso de España esta proporción es menor, alcanzando el 38% de las empresas. Finlandia (65%), Dinamarca (60%) y Suecia (57%) son los países en los que más proporción de empresas usan recursos internos para gestionar la seguridad TIC. En el lado opuesto, en Grecia y en Letonia no se supera el 30%.

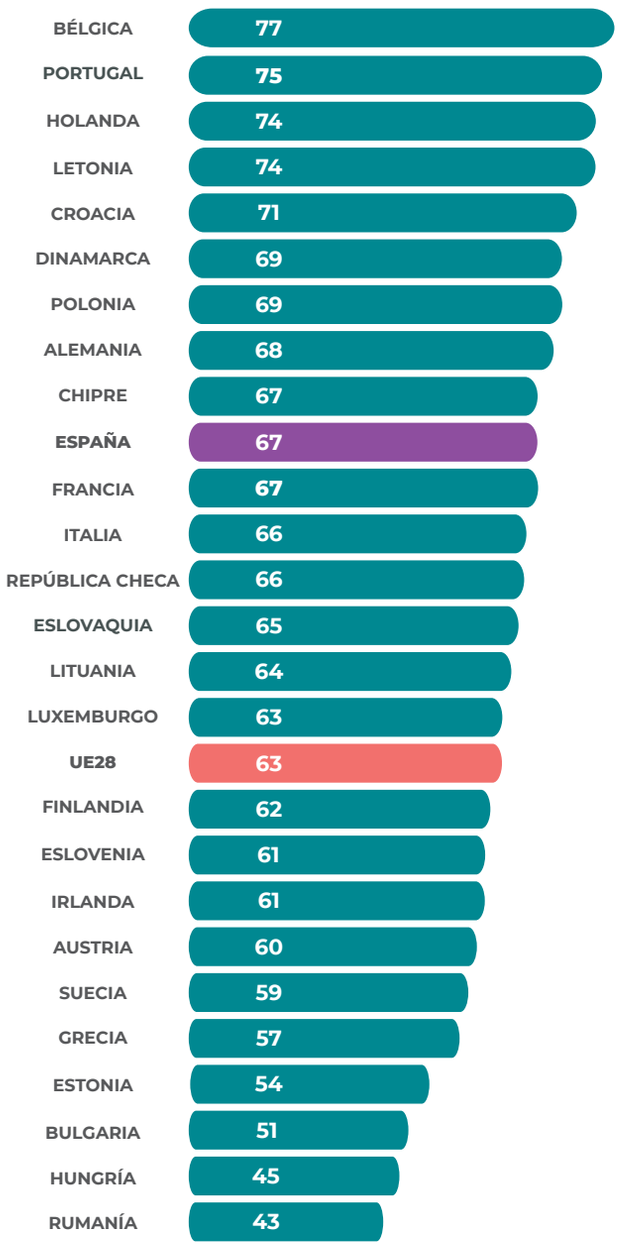
Ilustración 22. Empresas cuyas actividades relacionadas con la seguridad TIC son realizadas por los propios empleados (año 2019)



Fuente: **EUROSTAT**

Sin embargo, la mayor parte de las empresas europeas y españolas prefieren que la gestión de la seguridad TIC sea realizada por proveedores externos. En el caso de España el 67% de las empresas lo hacen, y de media en la UE 28 el 63%. Bélgica (77%), Portugal (75%), Países Bajos (74%) y Letonia (74%) son los países en los que más se adopta esta práctica, mientras que en Estonia (54%). Bulgaria (51%), Hungría (45%) y Rumanía (43%), donde menos.

Ilustración 23. Empresas cuyas actividades relacionadas con la seguridad TIC son realizadas por proveedores externos (año 2019)

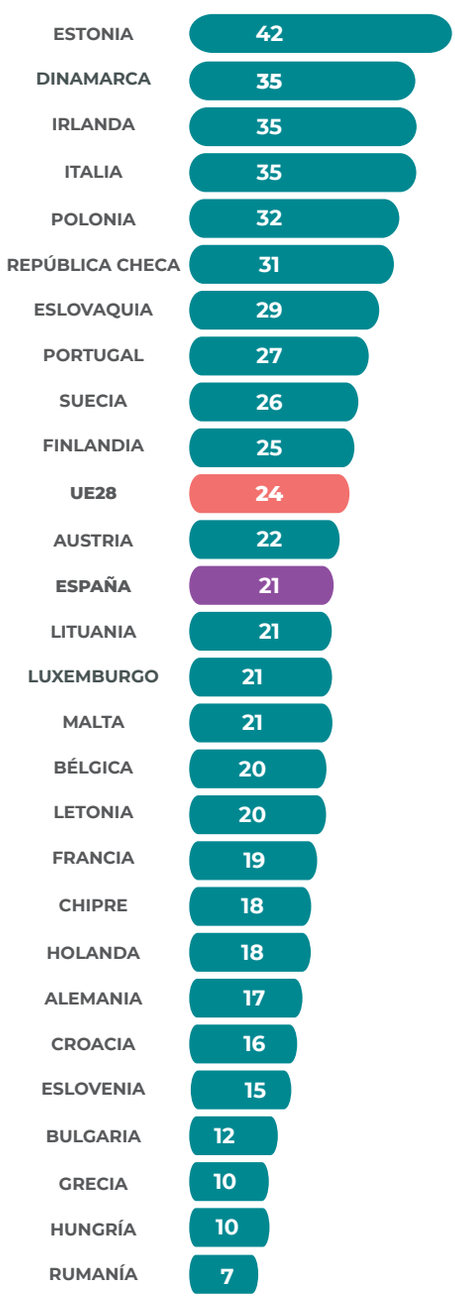


Fuente: EUROSTAT

Mantener a las personas trabajadoras concienciadas y formadas sobre seguridad TIC es uno de los aspectos clave para reducir incidentes y afianzar la confianza digital en las empresas.

Respecto a la formación, en España, el 21% de las empresas proporcionaban formación obligatoria sobre seguridad TIC, por debajo de la media de la UE que se situó en 24%. Estonia (42%), Dinamarca, Irlanda y Italia (35%) son los países en los que mayor proporción de empresas dan formación obligatoria. En cambio, en Bulgaria (12%), Grecia (10%), Hungría (10%) y Rumanía (7%) cuentan con la menor proporción.

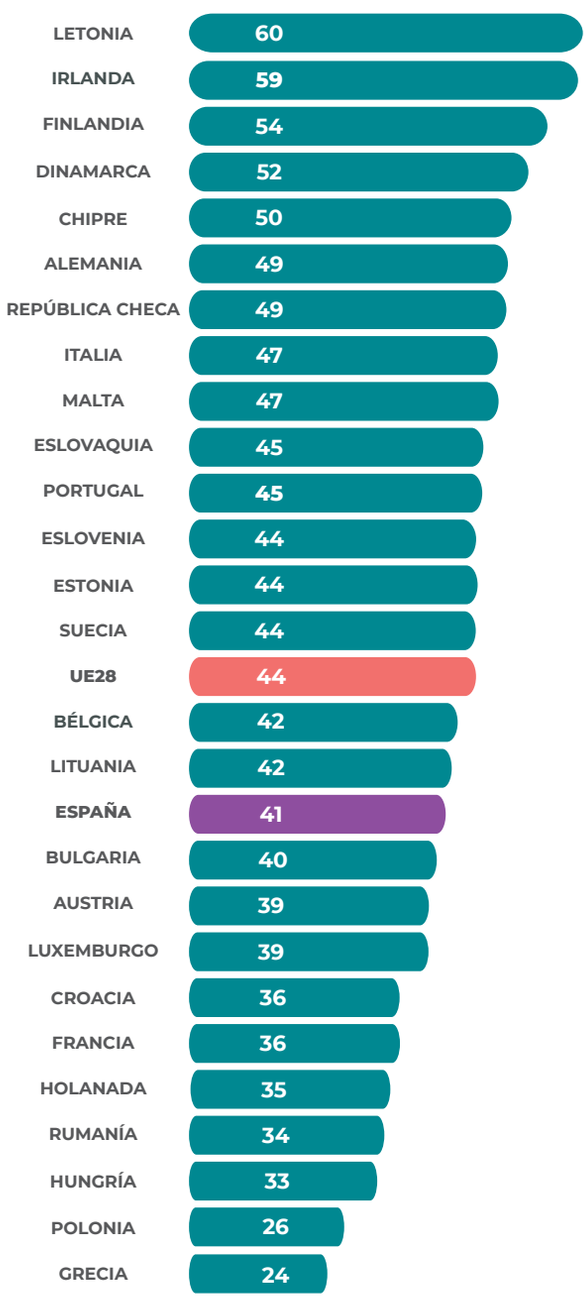
Ilustración 24. Empresas con formación obligatoria sobre seguridad TIC (año 2019)



Fuente: **EUROSTAT**

Sin embargo, la mayor parte de las empresas prefieren proporcionar a su personal formación voluntaria sobre TIC, en España (41%) estas empresas doblan a las que dan formación obligatoria. La adopción es muy dispar en la UE27, mientras que en Letonia (60%), Irlanda (59%), Finlandia (54%) y Dinamarca (52%) más de la mitad de las empresas dan formación voluntaria, en países como Polonia (26%) y Grecia (24%) no se supera el 30%. La media europea se sitúa en el 44%.

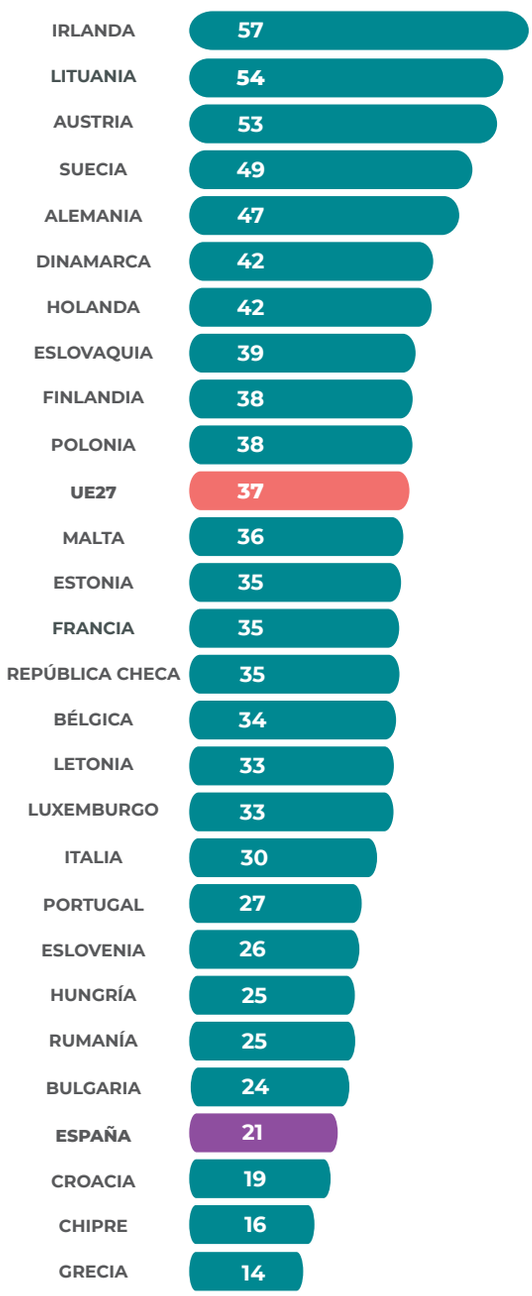
Ilustración 25. Empresas con formación voluntaria sobre seguridad TIC (año 2019)



Fuente: **EUROSTAT**

En cuanto a la concienciación del personal sobre aspectos relacionados con la seguridad TIC, solo el 21% de las empresas españolas informan a sus trabajadores de sus obligaciones en materia de seguridad TIC por contrato. Este valor sitúa a España a la cola de los países europeos en medidas para concienciar y responsabilizar a los trabajadores, junto con Croacia (19%), Chipre (16%) y Grecia (14%), lejos de la media europea, que es del 37%, y de los países con mayor adopción de esta práctica por parte de las empresas que son Irlanda (57%), Lituania (54%) y Austria (53%).

Ilustración 26. Empresas que informan a las personas empleadas de sus obligaciones en materia de seguridad de las TIC por contrato (año 2019)

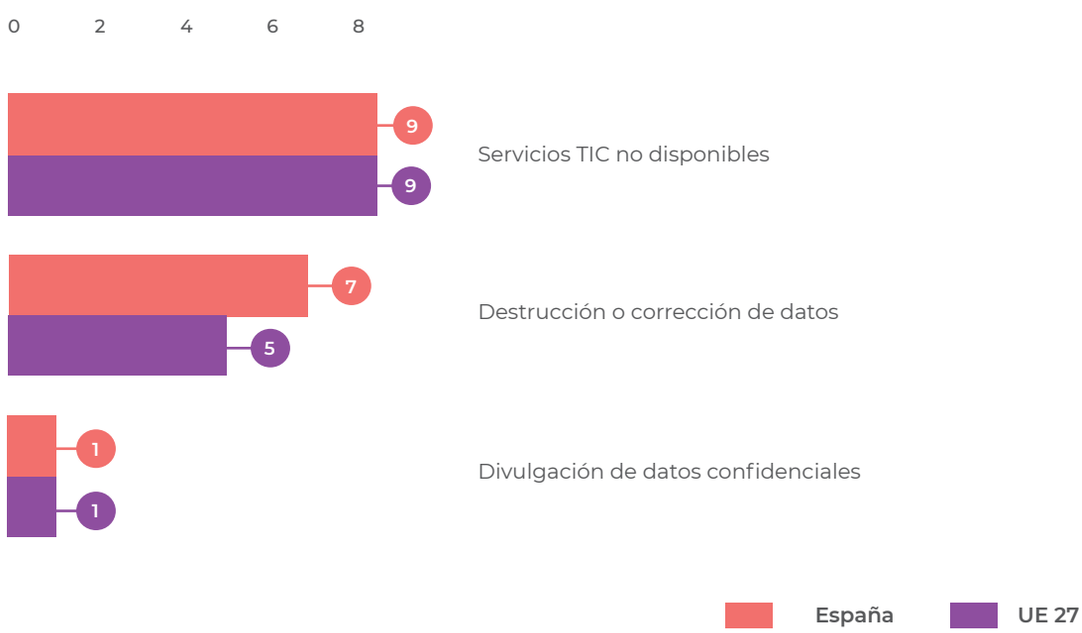


Fuente: **EUROSTAT**

INCIDENTES DE CIBERSEGURIDAD EN LAS EMPRESAS

No son muchas las empresas que declaran incidentes de seguridad TIC. En España, el 9% de las empresas declararon que sus servicios TIC no estaban disponibles, la misma proporción que en el caso de la media de la Unión Europea. Otro de los incidentes más habituales es que se produzca destrucción o corrupción de datos, lo que afectó en 2019 al 7% de las empresas españolas y el 5% de las empresas europeas. Por último, la divulgación de datos confidenciales afectó al 1% de las empresas españolas y europeas.

Ilustración 27. Incidentes de seguridad TIC en empresas (año 2019)



Fuente: **EUROSTAT**

5 ÍNDICE GLOBAL DE CIBERSEGURIDAD

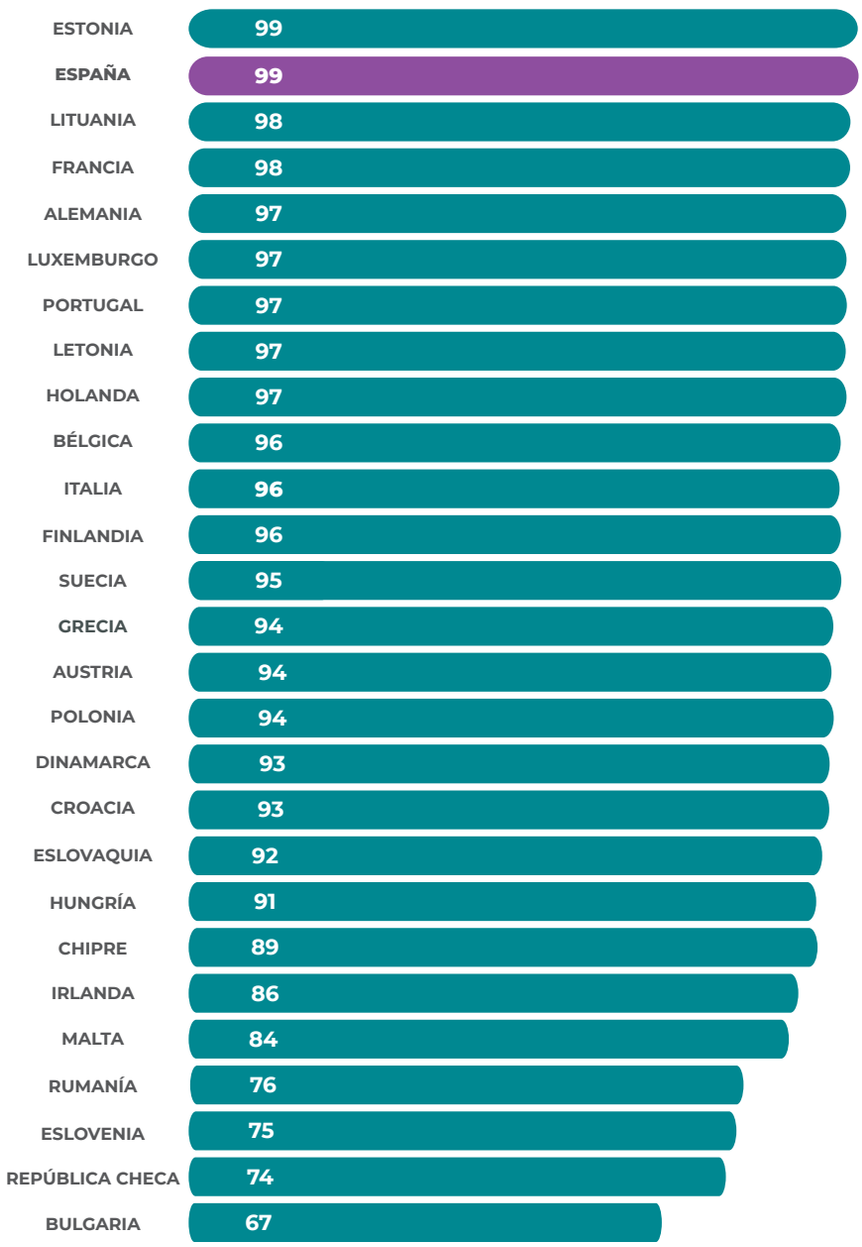
Las estrategias nacionales de seguridad digital describen cómo los países se preparan y responden a los ataques contra sus redes digitales. Pueden considerarse una dimensión importante de la preparación nacional en términos de gestión de riesgos de seguridad digital. Se trata de un marco o estrategia integral que debe ser desarrollado, implementado y ejecutado con un enfoque de múltiples partes interesadas, que aborda acciones coordinadas para la prevención, preparación, respuesta y recuperación de incidentes por parte de las autoridades gubernamentales, el sector privado y la sociedad civil (UIT, 2020).

La Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas publica periódicamente el Índice Global de Ciberseguridad (IGC) que miden el compromiso de los Estados miembros con la Agenda de Ciberseguridad Global definida por la UIT. Este informe tiene como objetivo comprender mejor el compromiso de los países con la ciberseguridad, identificar brechas, fomentar la incorporación de buenas prácticas y proporcionar información útil para que los países mejoren sus políticas sobre ciberseguridad. La edición de 2020 recoge la valoración de 194 países, que han sido evaluados con un riguroso proceso, a través de 82 preguntas, para obtener un total de 20 indicadores repartidos en 5 pilares: legal, técnico, organizativo, desarrollo de capacidades y cooperación.

De todos los países incluidos a nivel mundial en el Índice de ciberseguridad mundial de 2020 de la UIT, la mitad informó que tenía una estrategia de seguridad digital publicada, el 34% la estaba desarrollando o tenía una antigüedad superior a cinco años, y el 15% restante no tenía ninguna estrategia dedicada.

A pesar de que la mitad de los países no tienen una estrategia de seguridad digital o no está actualizad, el 70% tiene un equipo nacional de respuesta a emergencias (es decir, CIRT, CSRIT o CERT). Sin embargo, la mayoría de los países no cuentan con métricas para evaluar el riesgo asociado a la ciberseguridad a nivel nacional. La falta de estas métricas puede dificultar que los países evalúen los riesgos actuales, prioricen las intervenciones de ciberseguridad y hagan un seguimiento del progreso.

Ilustración 28. Índice global de ciberseguridad de los países de la UE27 (año 2020)



Fuente: **Unión Internacional de Telecomunicaciones**

España alcanza una puntuación de 98,52 sobre 100 en el índice global de ciberseguridad, lo que la sitúa en el cuarto puesto a nivel mundial en el IGC 2020, solo por detrás de EE. UU., Reino Unido, Arabia Saudí y Estonia, e igualada con Corea del Sur y Singapur. En el contexto de la UE27, España se encuentra en segunda posición, detrás de Estonia (99,48 puntos).

Tabla 1. Índice global de ciberseguridad (20 primeras posiciones) (año 2020)

PAÍS	ÍNDICE	POSICIÓN
EEUU	100	1,0
ARABIA SAUDÍ	99,5	2,0
REINO UNIDO	99,5	2,0
ESTONIA	99,5	3,0
ESPAÑA	98,5	4,0
COREA	99,5	4,0
SINGAPUR	99,5	4,0
EMIRATOS ARABES UNIDOS	98,1	5,0
MALASIA	98,1	5,0
FEDERACIÓN RUSA	98,1	5,0
LITUANIA	97,9	6,0
JAPÓN	97,8	7,0
CANADÁ	97,7	8,0
FRANCIA	97,6	9,0
INDIA	97,5	10,0
TURQUÍA	97,5	11,0
AUSTRALIA	97,5	12,0
LUXEMBURGO	97,4	13,0
ALEMANIA	97,4	13,0
PORTUGAL	97,3	14,0
LETONIA	97,3	15,0
HOLANADA	97,1	16,0
NORUEGA	96,9	17,0
MAURITANIA	96,9	17,0
BRASIL	96,6	18,0
BÉLGICA	96,3	19,0
ITALIA	96,1	20,0

Fuente: UIT

La evolución de España en este índice ha sido muy positiva en los últimos años, pasando de la posición 30 en 2014, a la 19 en 2016, 7 en el 2018 y 4 en 2020, lo que pone de manifiesto el compromiso de los distintos gobiernos de España con la ciberseguridad a lo largo de los últimos años.

6 CONCLUSIONES

En la medida en la que la economía y la sociedad se transforman en más digital, la gestión de los riesgos de seguridad, privacidad y protección de la ciudadanía y las empresas en el entorno digital se convierte en un uno de los factores clave de las políticas de los países. España se encuentra bien posicionada en el compromiso por dar respuesta a los problemas que surgen de la ciberseguridad, como lo demuestra la cuarta posición que ocupa en el índice global de ciberseguridad que publica la UIT.

La confianza en el entorno digital de la ciudadanía es alta, aunque se ha visto reducida en el último año, por lo que habrá que analizar en el futuro las posibles causas de este retroceso, poniendo foco en los posibles efectos de la pandemia COVID-19 y el aumento del uso de los servicios en la desconfianza de la ciudadanía en Internet.

Los incidentes de ciberseguridad se van transformando. Aunque estamos más preparados para afrontar riesgos tradicionales de Internet, como los virus, se incrementa la frecuencia y virulencia de nuevos incidentes a través de técnicas más sofisticadas, como el ***phishing*** o el ***pharming***, que a menudo se sustentan en el engaño, lo que merma la confianza en el entorno digital.

Aunque las grandes empresas y organizaciones están más preparadas para gestionar y abordar las consecuencias de riesgos de seguridad digital, los datos sugieren que este no es el caso de las pymes, y en particular de las microempresas, que puede enfrentarse a limitaciones financieras, de gestión, de habilidades y de conocimientos.

La formación y la concienciación en ciberseguridad son aspectos clave para reducir y afianzar la confianza digital. Los datos muestran que hay margen para incrementar la formación en ciberseguridad por parte de las empresas de su personal.

La concienciación de la ciudadanía española sobre el uso de los datos personales en Internet es alta, la mayor parte de las personas realizan alguna acción para administrar sus datos personales en Internet. Sin embargo, se detectan brechas digitales en las habilidades para configurar el acceso a datos personales en función de la edad y el nivel educativo de los individuos.

Por último, para afianzar la confianza en el entorno digital es clave encontrar un equilibrio entre el marco normativo y ético en torno a la recopilación y el almacenamiento de los datos, las organizaciones que los analizan y usan, y las personas que poseen y consienten (aunque no siempre se dan cuenta de que lo han hecho) sus datos personales en línea.

7 REFERENCIAS

Eurostat. (20 de 04 de 2021). Eutostat. Recuperado el 04 de 05 de 2021, de ***Population and social conditions***: https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=lfsa_ehomp&lang=en

INE ETICCE. (2020). Encuesta sobre el uso de TIC y comercio electrónico en las empresas. Obtenido de https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176743&menu=ultiDatos&idp=1254735576692

INE ETICH. (2020). Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. Obtenido de https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735576692

OCDE. (2019). ***Measuring the Digital Transformation: A Roadmap for the Future.*** Pairs: OECD Publishing.

UIT. (2020). ***Global Cibersecurity Index 2020. Unión Internacional de Telecomunicaciones.*** Ginebra: ITU Publications.

El informe “Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea. Octubre 2021” ha sido elaborado por el siguiente equipo de trabajo del Observatorio Nacional de Tecnología y Sociedad (ONTSI):

Lucía Velasco

Luis Muñoz

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.

NIPO: 094-21-115-6



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