FORO NACIONAL DE CIBERSEGURIDAD

BRÚJULA DE LA CIBERSEGURIDAD DEL CIUDADANO

Propuestas para afrontar los principales riesgos en diez ámbitos

Hacia un Plan estratégico de ciberseguridad ciudadana

2023

LA BRÚJULA DE LA CIBERSEGURIDAD DEL CIUDADANO

La **Estrategia Nacional de Ciberseguridad** de 2019 señala la necesidad de una mayor implicación de toda la sociedad, mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que **el ciudadano es corresponsable de la ciberseguridad nacional**.

Asimismo, como indica la **Carta de Derechos Digitales, los poderes públicos deben velar por el derecho a la ciberseguridad de los ciudadanos**, además de promover la sensibilización y formación en materia de ciberseguridad, para lo que podrán contar con la colaboración de la sociedad civil.

Con el objetivo de abordar desde ambas perspectivas la necesidad de aumentar la concienciación de la sociedad sobre los ciberriesgos que implica el uso de la tecnología, **la Brújula para la ciberseguridad del ciudadano** se concibe como un instrumento orientativo en el que se **analizan diez ámbitos que el Foro Nacional de Ciberseguridad ha considerado que están entre los que representan en la actualidad un riesgo mayor** para la ciudadanía o que necesitan una especial atención.

Para cada ámbito analizado se ha incluido: una introducción a los retos planteados, las necesidades percibidas que pueden tener los ciudadanos en ese ámbito; algunas iniciativas existentes de referencia, a modo de ejemplo, para ayudar a afrontar los riesgos y finalmente, una selección de propuestas dirigidas a los agentes impulsores de la cultura de la ciberseguridad.

Complementando lo anterior, de manera visual a través de un código de semáforo, se presentan, para cada ámbito y por segmentos de la población que se han considerado más vulnerable, el estado de la situación y las recomendaciones principales. Finaliza la Brújula con unas conclusiones y recomendaciones dirigidas a las Administraciones Públicas, con la propuesta de elaboración de un **Plan estratégico de ciberseguridad ciudadana y una Estrategia de protección de menores online.**

Los ámbitos objeto de análisis han sido los siguientes:

1. Redes sociales
2. Contraseñas y credenciales
3. Ingeniería Social
4. Primer acceso a las TIC
5. Trámites y compras online
6. Privacidad e información personal
7. Internet de las cosas
8. Protección del dispositivo
9. Inteligencia artificial
10. Denuncia, soporte y ayuda

Esperamos que esta Brújula cumpla su misión y sirva de orientación en el camino hacia una mayor cultura en ciberseguridad en España.

PORQUE LA CIBERSEGURIDAD ES RESPONSABILIDAD DE TODOS

FORO NACIONAL DE CIBERSEGURIDAD

Autores

Coordinadora sociedad civil:

Ana Isabel Borredá Caballero (Presidenta de la Fundación Borredá)

Coordinadora institucional:

Elena de la Calle Vian (Departamento de Seguridad Nacional)

Autores y colaboradores:

Adrián Capdevila Dueñas

Félix Gómez Mármol

Enrique González Herrero

Eugenia Hernández Sánchez

Mar López Gil

Juan José Martínez Pagán

Casimiro Nevado Santano

Ramón Ortiz González

Antonio Ramos García

Arturo Ribagorda Garnacho

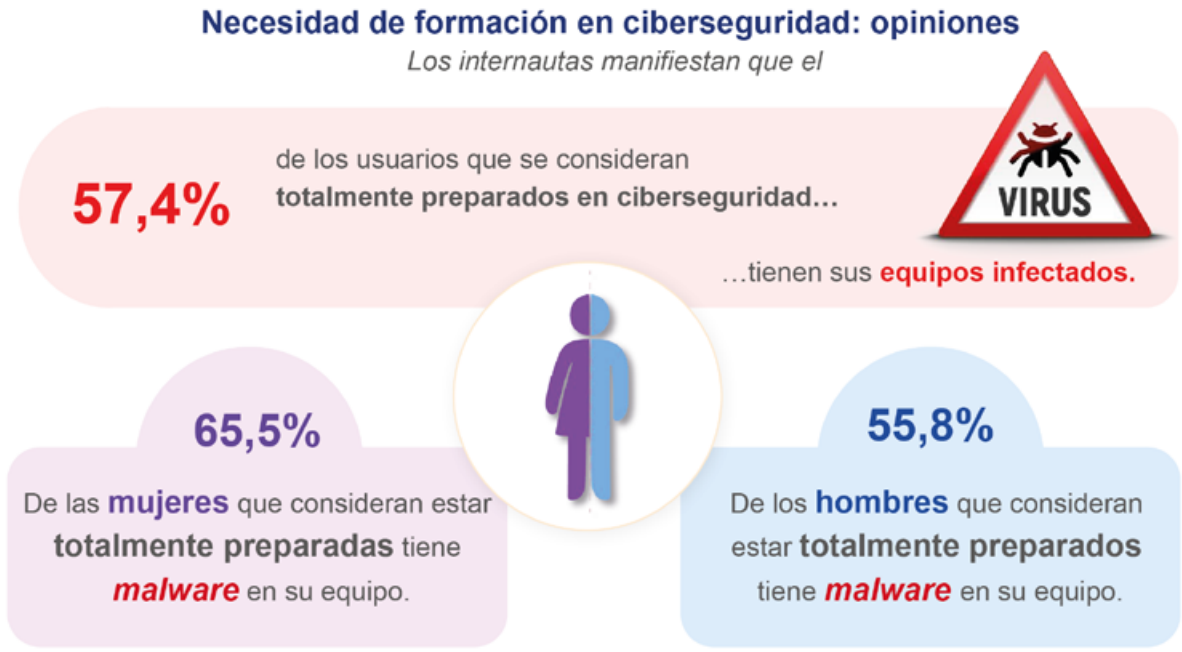
ÍNDICE

1. LA CIBERSEGURIDAD: UN DESAFÍO PARA LA CIUDADANÍA

La tecnología forma parte de la realidad cotidiana de toda la ciudadanía. Especialmente en los últimos años asistimos a una verdadera transformación digital de nuestra sociedad que ha contribuido, sin duda, a mejorar la vida de la población. El desarrollo de nuevas tecnologías permite hoy, por ejemplo, conectar a las personas a grandes distancias, solicitar multitud de servicios desde un teléfono móvil, recibir información de interés en tiempo real o desempeñar acciones cotidianas en el hogar de manera más confortable.

Sin embargo, a pesar de esos avances, es indudable que el **uso de la tecnología también entraña grandes retos, entre los cuales destaca la ciberseguridad**. En este sentido, la implicación del propio usuario resulta imprescindible para poder hacer frente a los riesgos, amenazas y vulnerabilidades que pueden derivarse de los dispositivos y servicios digitales que utiliza. **Conocimientos y habilidades como el establecimiento de medidas de seguridad básicas o el uso responsable de los dispositivos deberían ser cuestiones asumidas por los ciudadanos de manera mayoritaria,** como ocurre en la actualidad en otros ámbitos, por ejemplo, en el de la seguridad vial, **pero la realidad muestra que no es así en términos generales**.

Esa falta de concienciación y corresponsabilidad se aprecia en estudios como el que lleva a cabo periódicamente el **Observaciber**, el observatorio de ciberseguridad dependiente de la Secretaria de Estado de Digitalización e Inteligencia Artificial, cuyo objetivo es fomentar la cultura de la ciberseguridad en España. En su informe titulado ***Cómo se protege la ciudadanía de los ciberriesgos*** (en su edición de abril de 2022) señala que el 41,1% de los participantes declara realizar conscientemente alguna conducta de riesgo en el empleo de sus dispositivos. Por ejemplo, el 39,6% navega sin tener las actualizaciones al día, el 33% pulsa en enlaces de Internet que no saben a dónde le dirigen o el 34,6% descarga aplicaciones de *markets* o páginas no oficiales.



> También resulta reveladora la cantidad de usuarios que consideran estar suficientemente protegidos sin que así sea (según el citado estudio, un 57,4% de los participantes que afirma sentirse totalmente preparado tienen sus equipos infectados) y el desconocimiento que existe de los vectores de ataque o los riesgos reales a los que se enfrentan cuando navegan por Internet o utilizan dispositivos conectados. En consecuencia, desconocen cómo deben actuar ante las diferentes amenazas que existen en este ámbito.

Dada esta carencia de concienciación y conocimientos en torno a los riesgos que existen en el ciberespacio, **los expertos del Grupo de Cultura de Ciberseguridad del Foro Nacional de Ciberseguridad** han llevado a cabo un análisis de algunos de los principales ámbitos en los que los riesgos y amenazas asociados a las tecnologías, o servicios más extendidos o en desarrollo, requieren una especial concienciación y corresponsabilidad por parte de la sociedad, así como de los segmentos de la población más vulnerables a ellos.

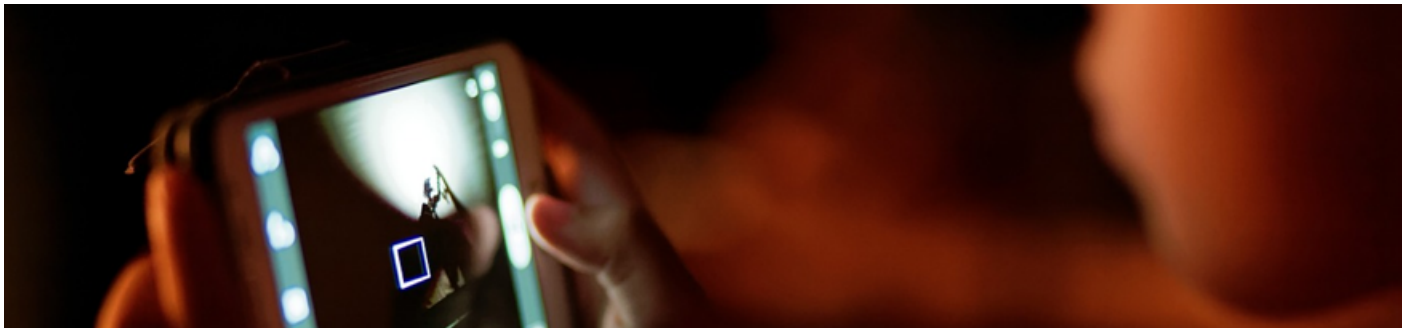
2. SEGMENTOS DE POBLACIÓN MÁS VULNERABLES

En cuanto al perfil y los segmentos de población que se pueden considerar más vulnerables a los riesgos y amenazas que conlleva el uso de la tecnología, en relación con la ciberseguridad destacan los siguientes:

Menores de edad

Los menores de edad constituyen uno de los segmentos más vulnerables, especialmente, a partir del momento en el que tienen independencia en el uso de sus propios dispositivos y consumo de contenidos. Es entonces cuando comienzan a registrarse en diferentes servicios, juegos, redes sociales, etc., sin la madurez suficiente y sin el conocimiento apropiado de los riesgos y peligros que existen en el ámbito digital. Coincide, además, con un momento vital en el que puede que cuestionen la autoridad de los adultos y, además, tengan cierta disponibilidad de recursos económicos propios que pueden gastar, por ejemplo, en compras o juegos online.

Dentro de este conjunto de población, es de vital importancia centrarse en los **adolescentes:** menores que empiezan a utilizar la tecnología como vehículo social, académico, laboral, de ocio y económico y que, frecuentemente, pueden mostrar comportamientos impulsivos, inmadurez o poca cultura de ciberseguridad. En este caso, es fundamental que la familia y los educadores, con el apoyo de las autoridades, les ayuden a tomar conciencia del potencial de la tecnología, tanto para lo bueno como para lo malo, hacerles partícipes de los auténticos riesgos a los que están expuestos y acompañarlos en la adquisición de criterio, conocimientos y habilidades.



Personas mayores

Las personas de edad avanzada suelen presentar mayores dificultades a la hora de acceder y utilizar las tecnologías, si bien muchas de ellas se ven abocadas a emplearlas en actividades cotidianas para las que no siempre están capacitadas (por ejemplo, banca online o trámites administrativos en general). Son vulnerables porque, aunque suelen ser muy precavidas, muchas veces son víctimas de estafas por desconocimiento de las técnicas empleadas por los ciberdelincuentes. Otras muchas rechazan directamente la tecnología precisamente porque no la consideran segura y les "da miedo", a pesar de que para ciertas actividades no tengan otra alternativa. Son especialmente vulnerables a acciones en las que se combina una acción cibernética maliciosa con un contacto personal, por ejemplo, a través de una llamada telefónica.

Este segmento no se define exclusivamente por la edad, sino también por la falta de conocimiento y de personas en su entorno familiar en las que apoyarse y a las que poder consultar en caso de necesidad.

Población en edad laboral no concienciada

Este segmento se refiere a las personas que disponen de los conocimientos mínimos necesarios para desenvolverse con la tecnología, sin llegar a ser usuarios avanzados, ni ser plenamente conscientes de los riesgos a los que se enfrentan. El uso de la tecnología tiene un impacto en su vida personal, pero también en el **ámbito laboral,** sea presencial o teletrabajo, dado que algunas acciones individuales pueden tener repercusión en su empresa. Es el caso de los usuarios que no son conscientes de las vulnerabilidades de sus dispositivos y de su red doméstica, pero los utilizan para teletrabajar y conectarse a la red corporativa, con el riesgo de que pueda afectar a su organización si el usuario descarga *malware*, le roban las credenciales, etc. En este marco se encuentran los trabajadores de cualquier organismo, organización y empresa, siendo de particular importancia la atención especial a aquellos que trabajan en infraestructuras críticas y para operadores de servicios esenciales.

Colectivos en riesgo de exclusión

Se han identificado tres colectivos considerados en riesgo de exclusión tecnológica. Sería el caso de los desconectados por su imposibilidad de acceso a la tecnología (sea por cuestiones económicas, escasez de infraestructuras en su lugar de residencia, etc.), las personas con discapacidad y la población extranjera e inmigrantes.

- **Desconectados:** Personas habitualmente desconectadas o sin recursos. En este sentido, es especialmente relevante el subsegmento de habitantes de **zonas rurales** por no estar tan familiarizados, a priori, con nuevas tecnologías, que suelen tener más presencia en las ciudades, y viven en lugares donde existe brecha digital.

- **Personas con discapacidad:** Las personas con discapacidad merecen una atención especial por el efecto multiplicador del riesgo que puede suponer la dificultad de uso si la tecnología no reúne las características de accesibilidad necesarias. Asimismo, las personas con discapacidad intelectual presentan una mayor vulnerabilidad para las acciones de ingeniería social.

- **Población extranjera e inmigrantes**: La falta de concienciación en este caso estaría favorecida por dificultades relacionadas con el idioma, así como por el distinto contexto cultural.


CANADA
WORLD

3. RIESGOS DE CIBERSEGURIDAD PARA EL CIUDADANO

TOP 1: REDES SOCIALES

Las redes sociales forman ya parte del día a día de millones de personas. Sin embargo, la elevada frecuencia de su uso no siempre viene acompañada de una mayor concienciación sobre los riesgos a las que están expuestas, en especial, el relacionado con la pérdida de la privacidad.

Compartir una publicación, subir una foto o un vídeo, comentar una noticia, crear nuevas amistades, pasar tiempo en ciertos entornos de conexión en tiempo real... Todas estas acciones deberían estar acompañadas de comportamientos ciberseguros, pero no todos los usuarios lo consideran imprescindible hasta que experimentan, de alguna u otra manera, las consecuencias de no haberle dado la importancia debida. En ocasiones, incluso, se difuminan y llegan a traspasarse los límites del entorno personal hacia el mundo laboral.

Cuanto más tiempo pasan las personas en las redes sociales más expuestas están a sus riesgos, y dado que está tendencia sigue aumentando, es necesaria una mayor concienciación sobre las prácticas y comportamientos ciberseguros en estos entornos.

Retos y amenazas que plantea

Esta conexión cada vez más permanente es, en términos de ciberseguridad, un vector de incidentes y exposición de privacidad y, en numerosos casos, también de actividades fraudulentas y criminales. Su utilización constante expone información sobre la vida en el ámbito personal y profesional.

Por otro lado, las redes sociales se extienden como uno de los mecanismos más utilizados para ataques relacionados con la ingeniería social y otras conductas delictivas como el ciberacoso o el *ciberbullying*.

Necesidades de los ciudadanos

- Una formación más específica sobre los temas relacionados con los riesgos existentes en el uso de las redes sociales, tanto en lo que se refiere al control de la información publicada, como a la configuración de la privacidad.

- Una mayor exigencia normativa sobre el aspecto más técnico de la configuración de privacidad.

- Un control más exhaustivo del acceso para los menores de edad, haciendo respetar las condiciones de uso de cada red social y activando mecanismos en otros portales (juego, cripto, banca) para verificar la documentación acreditativa de edad antes del acceso.

- Crear conciencia sobre los riesgos inherentes que supone la utilización de redes sociales. Por ejemplo:

    - Qué supone compartir información (usuarios, claves, contraseñas, pin, claves de la Seguridad Social, Clave Tokens, DNI o identificaciones oficiales, teléfono, correo, mensajes).

    - Vulnerabilidades a las que se expone al navegar en equipos públicos, o de terceras personas, wifis y redes no autorizadas.

    - La importancia de crear contraseñas seguras, actualizar software, usar antivirus.

    - Cómo detectar perfiles legítimos y falsos, enlaces fraudulentos, técnicas de ingeniería social, estafas virtuales.

- Dotar al usuario de hábitos y recursos para incorporarlos en todos los niveles: desde cómo proteger la privacidad de sus datos personales, información

confidencial profesional o cualquier dato sensible, hasta cómo adoptar buenas prácticas para el uso de redes sociales, sitios y plataformas digitales.

Algunas iniciativas de referencia

- Curso presencial para personas con discapacidad y nuevos usuarios sobre el manejo básico de las redes sociales y aplicaciones de videollamada[1].

- Talleres online gratuitos de ciberseguridad, que incluyen un curso específico sobre riesgos y fraudes en redes sociales[2]. Buenas prácticas. Políticas de seguridad para las pymes desarrolladas por el Instituto Nacional de Ciberseguridad. Proporciona las herramientas de seguridad adecuadas para proteger las redes sociales, así como concienciar sobre la necesidad de formar a los administradores antes de desempeñar esta labor[3]:

Propuestas a los actores impulsores de la cultura de la ciberseguridad

Algunas de las actuaciones en las que deben trabajar los actores impulsores de la cultura de ciberseguridad para promocionar un uso más seguro de las redes sociales deberían apoyarse en mensajes más contundentes tales como:

- Clarificación sobre las opciones de privacidad ofrecidas por las redes sociales y el establecimiento de opciones restrictivas en el uso del perfil personal.

- Concienciación y uso del sentido común en el comportamiento ante los desconocidos y sus planteamientos de enlace (*match*) en la red del mismo modo que lo haríamos en el mundo real.

- La no publicación ni facilitación de datos propios que abran la puerta a la identificación de conductas o hábitos que puedan derivar en caer víctimas de un delito.

- Atención a la publicación de imágenes o contenidos de terceros y, especialmente, en el caso de menores.

- Impulsar la implantación efectiva de controles de acceso para los menores de edad.

---

[1] https://plenainclusionmadrid.org/formacion/formacion-redes-sociales-y-videollamada/

[2] https://www.osi.es/es/talleres-ciberseguridad

[3] https://www.incibe.es/protege-tu-empresa/blog/buenas-practicas-redes-sociales-aumenta-tu-popularidad-sacrificar-seguridad

TOP 2: CREDENCIALES Y CONTRASEÑAS

Las credenciales son documentos físicos o digitales que garantizan nuestra identidad. Tienen una relación estrecha con la autenticación, que es el proceso de comprobar nuestras credenciales y gracias al cual es posible verificar que somos quien decimos ser. Las contraseñas, por su parte, son uno de los tipos de credenciales más frecuentes que se usan para comprobar nuestra identidad en los medios digitales.

El uso de contraseñas como único mecanismo de autenticación está desaconsejado en determinados entornos. Son numerosos los métodos que pueden utilizar los actores maliciosos en Internet para conseguirlas[4] y, por ello, para autenticarnos de manera segura, se suele utilizar una combinación de, al menos, dos tipologías diferentes de credenciales, dando lugar a la llamada autenticación de dos factores o a autenticación de factor múltiple. Por ejemplo: una contraseña más una clave única enviada a mi dispositivo; una contraseña más un dispositivo o el reconocimiento facial (característica biométrica) más dispositivo, etc.

La autenticación de usuarios es el primer proceso básico en la cadena de la ciberseguridad de los usuarios. Es de vital importancia, ya que un actor malintencionado que consiguiera nuestras credenciales podría suplantar nuestra identidad a todos los efectos, desde el acceso a nuestras cuentas bancarias, hasta cometer un delito con nuestro nombre[5].

[4] MITRE ATTCK matrix: Credential Access (*The adversary is trying to steal account names and passwords*) https://attack.mitre.org/tactics/TA0006/

[5] Fiscalía general del Estado. Unidad de criminalidad informática. Comunicación usurpación identidad https://www.fiscal.es/documents/20142/fa2280e1-e5ed-b37f-dc3f-6fc3aa3dd6b7

Retos y amenazas que plantea

El primer reto que se plantea es la concienciación de los usuarios. Los procesos de autenticación de factor múltiple, y con tiempos de caducidad de sesión por inactividad, no son percibidos por los usuarios como mecanismos beneficiosos que ayudan a proteger sus activos digitales, sino más bien como mecanismos perturbadores, ante los cuales sienten incomodidad. Es por ello que existe la tendencia a sortearlos por cualquier método y a usar contraseñas inseguras que, en la práctica, vienen a ser lo mismo que no utilizar ninguna[6].

El segundo reto se produce como consecuencia de la alta cantidad de aplicaciones y servicios digitales que utiliza el ciudadano medio que, según recientes estudios, es de 30 diferentes en un mes[7]. El desafío consiste en la dificultad para crear y custodiar de manera segura tantas contraseñas, diferentes para cada una de las aplicaciones o servicios, que además hay que actualizar periódicamente.

Otro reto es la compartición de credenciales con terceras personas. Suele producirse por una causa puntual y, una vez compartida, no se tiene la precaución de cambiar la contraseña.

Además, el *phishing,* junto con el SMS *spoofing* son dos métodos utilizados habitualmente por los ciberdelincuentes para robar credenciales y controlar dispositivos, que a su vez pueden ser usados como credencial. Por ello, la concienciación y el entrenamiento de los usuarios para que sepa reconocerlos y evitar caer en ellos es un reto adicional.

Necesidades de los ciudadanos

La complejidad para el usuario en la gestión segura de credenciales, unida a la sofisticada ingeniería de los cibercriminales, convierten a la gran mayoría de los ciudadanos en personas altamente vulnerables a este riesgo.

Por ello, una parte importante de la responsabilidad de proteger la identificación de los ciudadanos cuando acceden a servicios digitales debe recaer en aquellos que tienen los recursos para implementar los mecanismos adecuados de control de acceso. Por ejemplo, la adopción de mecanismos de autenticación multifactorial y de contraseñas complejas, el uso de la biometría, etc[8]. Esto debe ser considerado como una responsabilidad

[6] https://unaaldia.hispasec.com/2022/12/las-contrasenas-mas-utilizadas-de-2022.html

[7] Mobile App Download Statistics & Usage Statistics (2022) https://buildfire.com/app-statistics/

[8] Four user authentication issues developers and admins struggle with (solved). https://www.smseagle.eu/2020/01/27/4-user-authentication-issues-developers-and-admins-struggle-with-solved/

importante de las empresas que ofrecen servicios críticos al ciudadano y también de las administraciones públicas.

En este sentido, cabe destacar como ejemplo el uso del certificado digital y el DNI electrónico, que proporcionan a los ciudadanos accesos de alto nivel de seguridad a los servicios públicos. En este sentido, sería conveniente facilitar más tutoriales y guías de ayuda a los usuarios, como las que ofrece la página del DNI electrónico[9] para configurar el uso de dichos mecanismos.

Asimismo, sería necesario el incremento de tutoriales y contenidos audiovisuales para concienciar a los usuarios y enseñarles cómo configurar factores de autenticación múltiple en los servicios digitales que utilizan.

Algunas iniciativas de referencia

- INCIBE, la opción de documentos para el empleado de la sección "Protege tu empresa" ofrece una guía muy completa y detallada sobre la gestión de contraseñas[10].

- La Oficina de Seguridad del Internauta (OSI) ha lanzado una campaña con el nombre "Contraseñas seguras", que presenta una serie de artículos sobre las contraseñas. En ellos cubre aspectos como la concienciación, buenas prácticas y el uso de gestores de contraseñas[11].

- El CCN-PYTEC ofrece una guía completa sobre autenticación multifactor en la que se definen los requisitos mínimos para cumplir con el Esquema Nacional de Seguridad (ENS)[12].

---

[9]Ejemplo de uso del DNI electrónico: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1079&id_menu=%5B17

[10]https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

[11]https://www.osi.es/es/campanas/contrasenas-seguras

[12]https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/353-pildorapytec-oct2020-autenticacion-multifactor/file

Propuestas a los actores impulsores de cultura de ciberseguridad

- Programas de concienciación y educación en ciberseguridad. Con eslóganes como “tu contraseña es la llave de tu casa, ¿la dejarías en un lugar donde cualquiera la pudiera coger?”.

- Cybervoluntarios en las escuelas, asociaciones de vecinos y centros de mayores que ayuden a las personas con pocos conocimientos a utilizar el certificado digital.

- Facilitar el acceso a gestores de contraseñas, con una subvención si fuera necesario (al igual que existe una subvención para el Kit Digital).

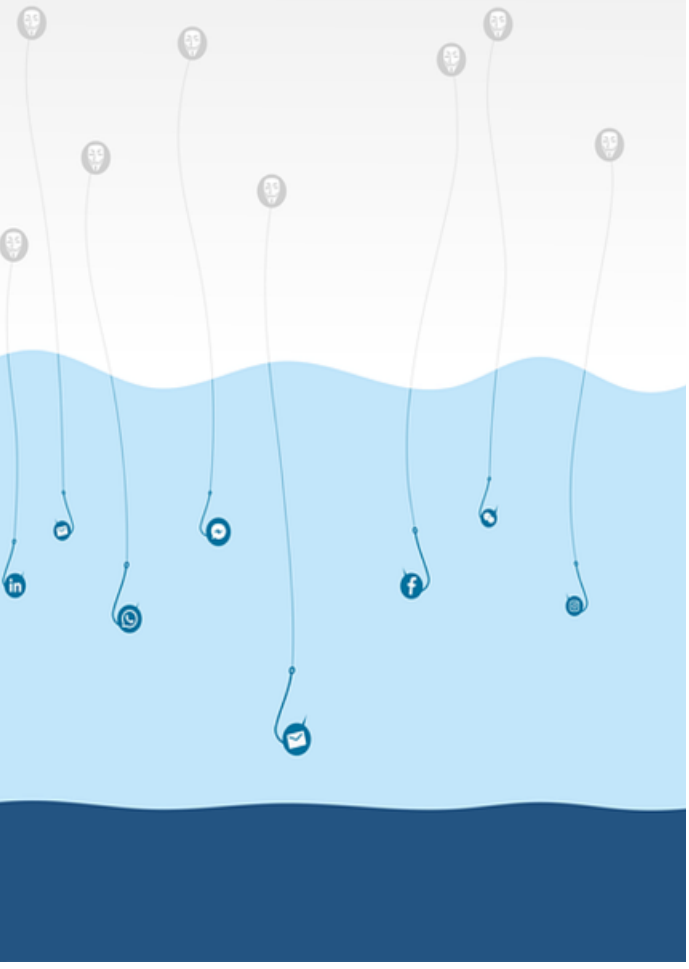
- Impulso del uso de biometría como mecanismo de autenticación, sin menoscabo de su consideración como dato personal sensible.

- Fomento de la responsabilidad compartida entre proveedores y usuarios en el uso de credenciales y la gestión de la autenticación, para evitar las malas prácticas de los dueños de los sistemas si, por ejemplo, no disponen de autenticación de factor múltiple o permiten contraseñas débiles.

TOP 3: ATAQUES DE INGENIERÍA SOCIAL

La ingeniería social consiste en la manipulación psicológica de los usuarios para acceder a sus datos sensibles. Incluye la suplantación, el engaño, la manipulación y, en general, el abuso de la confianza de las personas para que revelen información o realicen acciones perjudiciales para ellas mismas o para terceros sin que sean conscientes de ello. Entre estas acciones se incluye el acceso a las cuentas bancarias de la víctima, el robo de su identidad en redes sociales, el acceso a información privada, como fotos y vídeos, el uso de su dispositivo para atacar a otras víctimas, etc.

Cualquier persona puede ser víctima de un ataque de ingeniería social, pero las personas con menos dominio de la tecnología están más expuestas, tardan más tiempo en darse cuenta y, en muchas ocasiones, no saben a quién recurrir si son víctimas de este tipo de ataque.



La ingeniería social puede entrar en la vida de los ciudadanos por varias vías:

- A través del teléfono, haciéndose pasar por una persona o entidad de confianza y pidiendo que se entreguen contraseñas, dinero o acceso remoto al ordenador. En los casos de v*ishing,* los ciberdelincuentes imitan voces mediante el uso de Inteligencia Artificial.

- Por email, a través de un correo con un enlace o un archivo adjunto malicioso, dando lugar al *ransomware* o secuestro de datos.

- A través de un dispositivo externo como un USB que, entregado como obsequio, contenga *malware* con el objetivo de entrar en sistemas de la competencia y poder espiarles.

- Por Internet, a través de la nueva técnica *deep-fake*, que es como se conoce a las alteraciones en el rostro y la voz de una persona mediante el uso de un software con Inteligencia Artificial.

Retos y amenazas que plantea

La ingeniería social sirve para llevar a cabo diversos tipos de ataques, que suponen el verdadero reto de esta amenaza:

- *Phishing*: consiste en el envío de correos electrónicos o mensajes de texto falsos que simulan provenir de instituciones, bancos, tiendas online, etc., proporcionando enlaces a páginas no oficiales que emulan perfectamente la estética de las páginas oficiales de dichas entidades donde se le solicita ingresar credenciales como nombres de usuario y contraseñas.

- Duplicación de la tarjeta SIM: consiste en la solicitud al operador de telecomunicaciones de una nueva tarjeta, suplantando la identidad de la víctima y así utilizarla para validar transacciones bancarias.

- Interceptación de mensajes SMS: es la interceptación mediante ingeniería de comunicaciones de los mensajes SMS enviados a un número de teléfono, para validar transacciones bancarias y robar dinero.

- Lectura de códigos QR: consiste en insertar un archivo infectado o una URL maliciosa en un código QR con la finalidad de llevarnos a una página de pagos falsa que emule a la del comercio u organismo oficial al que están suplantando, o descargue el archivo malicioso en nuestro dispositivo.

Necesidades de los ciudadanos

Es necesario empoderar a los ciudadanos a través del **autoconocimiento y la formación** en esta temática. Son los sesgos cognitivos y tipo de personalidad que tenemos los que están al mando de la mayor parte de nuestros pensamientos y acciones. Los cibercriminales conocen esos sesgos cognitivos y analizan los tipos de personalidad que existen, saben a qué reacciona cada cual, qué les llama la atención, a qué les resulta irresistible dar click. Nuestra personalidad nos hace vulnerables.

Para formar adecuadamente (en cantidad y calidad) a los usuarios en materia de ciberseguridad, es necesario reducir la vulnerabilidad que podría encarnar cada elemento humano en la sociedad, precisamente por la impredecibilidad que tienen las personas en su comportamiento. La **neurociberseguridad** es una forma de empoderar a los usuarios a través del autoconocimiento, donde se debe facilitar un diálogo entre la neurociencia a través de los procesos cognitivos y la seguridad en el ámbito digital. Así entenderán y serán conscientes de los procesos cognitivos que explican el éxito de los ciberataques y podrán evitarlos.

También se requiere **concienciación y divulgación atractiva a través de campañas de comunicación masivas** para generar nuevos hábitos en el ámbito digital en la ciudadanía:

Algunas iniciativas de referencia

Phishing:

- INCIBE protege tu empresa. Sección dedicada al *phishing* con ejemplos y descripciones detalladas y consejos para evitarlo[13].
- El CCN-CERT, en la sección de su web "Defensa contra amenazas", ofrece dos *hashtags* de Twitter en los que publica regularmente información y alertas actualizadas sobre campañas de *phishing* y *malware*[14]:
- La Universidad Veracruzana (México) ha creado una página de concienciación a la que llegas después de clicar en un enlace engañoso originado por ellos mismos. Sirve como entrenamiento[15].

SIM-Swaping:

- La Oficina de Seguridad del Internauta ofrece en su blog un artículo muy detallado con instrucciones precisas para evitarlo y un video explicativo[16].

Códigos QR:

- INCIBE, en la sección de su web "Protege tu empresa", cuenta con una página explicando los riesgos y ofrece consejos a las empresas para evitar que sus códigos QR sean manipulados o suplantados con fines maliciosos[17].

---

[13] https://www.incibe.es/protege-tu-empresa/tematicas/phishing

[14] #NoTeinfectesConElMail y #CiberCOVID19

[15] https://www.uv.mx/csirt/concientizacion-phishing/

[16] https://www.osi.es/es/actualidad/blog/2022/06/09/sim-swapping-como-evitar-esta-estafa

[17] https://www.incibe.es/protege-tu-empresa/blog/protege-los-codigos-qr-y-no-pongas-riesgo-seguridad-tus-clientes

Propuestas a los actores impulsores de cultura ciberseguridad

- Lanzamiento de enlaces engañosos que lleven a una página que sirva como concienciación y educación a los ciudadanos, como lo hace la Universidad Veracruzana, o lo hacen algunas empresas con sus empleados.

- Campañas de concienciación masivas basadas en el autoconocimiento para el empoderamiento de la ciudadanía, aportando más valor e información, más allá de los hábitos.

- Aplicaciones gratuitas para lectura de código QR, que permitan visualizar la URL antes de acceder a ella.

- Mensajes más contundentes sobre la amenaza del *phishing*, de los QR maliciosos y cómo darnos cuenta de que hemos sido víctimas.

TOP 4: PRIMER ACCESO A LAS TIC

La iniciación a las TIC se produce a edades cada vez más tempranas, hasta el punto de que utilizamos el apelativo de nativos digitales para describir las destrezas de las nuevas generaciones.

En paralelo, hay personas que comienzan a aprovechar las posibilidades que ofrecen las tecnologías conectadas a edades tardías, lo que requiere un esfuerzo importante de capacitación para poder utilizar con confianza y seguridad los servicios digitales.

En ambos casos, el primer acceso a las TIC es un proceso que merece especial atención, así como mayores esfuerzos de concienciación y formación.

Retos y amenazas que plantea

El uso de las TIC supone un reto para toda la sociedad debido a los riesgos y amenazas que existen en el ámbito digital, pero más si cabe para las personas que comienzan a utilizar dispositivos conectados, como podrían ser los teléfonos móviles, las tabletas o los ordenadores. Los riesgos a los que se enfrentan los colectivos de menores y personas de avanzada edad que comienzan a utilizar las TIC son comunes con el resto de los ciudadanos, con el añadido de un acentuado desconocimiento, *a priori*, tanto del uso de los dispositivos como de las amenazas que habitan en la red.

El robo de información personal, la suplantación de identidad, el fraude, el acoso en sus diferentes modalidades o la difamación en redes sociales son algunas de las amenazas más comunes para los menores y, en su mayor parte, también para los ciudadanos de edad avanzada. En el caso de los menores, debido a la inmadurez propia de la edad, el uso de la tecnología les vuelve más vulnerables a la adicción o futura ludopatía.

Necesidades de los ciudadanos

En el caso de los menores y adolescentes, que van introduciéndose en el uso de dispositivos móviles, vemos cómo utilizan especialmente los teléfonos o las tabletas para acceder a servicios como las redes sociales, aplicaciones de comunicación o a los juegos en línea. Esta iniciación requiere una educación adaptada a los más pequeños para que hagan un uso responsable de dichos servicios y estén preparados para detectar y evitar los riesgos y amenazas que afectan a su uso. Es importante sensibilizar a los adultos de la necesaria supervisión en virtud del especial deber de vigilancia, como pueden ser los padres o tutores respecto de sus hijos o pupilos o los titulares de un centro docente respecto de los alumnos.

Igualmente, las personas mayores que hasta ahora estaban desconectadas se ven abocadas al uso de tecnologías para llevar a cabo determinadas operaciones de la Administración o de las entidades financieras, que les obligan a hacer uso de dispositivos y procesos informáticos hasta entonces desconocidos para ellos. Por ello, es necesario que también los mayores que están aprendiendo a utilizar estas herramientas conozcan y tomen conciencia de los riesgos que entraña su utilización.

Algunas iniciativas de referencia

- La extinta Agencia de Protección de Datos de la Comunidad de Madrid puso en marcha hace dos décadas charlas para adolescentes en los colegios en las que estaban involucrados los propios profesores de informática.

- Internet Segura 4 Kids (is4K): esta iniciativa de INCIBE es el Centro de Seguridad en Internet para menores de edad en España[18].

- Experiencia Senior: se trata de un programa de concienciación para mayores de 60 años, también lanzado por INCIBE. Su objetivo es impulsar y potenciar las habilidades digitales de los usuarios mayores de 60 años con materiales específicos y formativos, que les permitan adquirir las nociones básicas necesarias para desenvolverse con confianza y seguridad cuando naveguen por Internet[19].

Propuestas a los actores impulsores de cultura de la ciberseguridad

- Elaborar una hoja de ruta de formación que se plasme en iniciativas de todo tipo adaptadas a la edad de los más jóvenes, como pueden ser la grabación de contenidos audiovisuales infantiles, charlas en los centros educativos, aplicaciones o juegos que les permitan aprender mientras se entretienen. En definitiva, es necesario adaptar formatos y mensajes a los menores para poder llegar a ellos de manera eficaz. En ese sentido, es fundamental contar con los educadores, quienes realmente conocen esas necesidades.

- Por otro lado, son los padres quienes tendrán que desempeñar un papel principal en la educación y el cuidado del acceso a las TIC de sus hijos. En ese sentido, han de ser conscientes y transmitir la corresponsabilidad que supone utilizar las tecnologías. El primer acceso a las TIC requiere también acciones orientadas a

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

[19] https://www.osi.es/es/experiencia-senior

los padres, como puedan ser campañas de sensibilización o actividades lúdico-educativas que puedan llevar a cabo conjuntamente progenitores y menores.

- El ámbito educativo también debe estar implicado en la formación y concienciación de los menores cuando comienzan a utilizar las tecnologías. Convendría alcanzar acuerdos y convenios al más alto nivel para que los colegios incorporen actividades destinadas a dicho fin, en las que estén involucrados tanto los educadores, como los padres, expertos en la materia y, evidentemente, los menores.

- En el caso de las personas mayores, igualmente requiere que los mensajes y contenidos que contribuyan a su formación estén adaptados a su edad e intereses. Uno de los aspectos clave al respecto es evitar provocar miedo a la hora de utilizar sus dispositivos, sino todo lo contrario, confianza y herramientas para que estos usuarios sepan reaccionar ante los retos que se les planteen.

- Las campañas de concienciación son una herramienta muy útil, pero insuficiente si no van acompañadas de otras acciones. En este sentido, se deben identificar las vías de acceso a ese segmento de población, localizando sus centros de encuentro, en ciudades y zonas rurales, o los medios de comunicación más populares entre los mayores, para que las actividades formativas lleguen al público objetivo.

- Al igual que los jóvenes, resultaría interesante involucrar a los descendientes de las personas mayores, ya sean sus hijos, nietos, sobrinos o cualquier otro familiar que pueda ayudarles, por ejemplo, mediante actividades compartidas lúdico-formativas.

- Las entidades financieras, la Administración y todas aquellas organizaciones que requirieran el uso de la tecnología para poder beneficiarse de sus servicios, deberían participar en iniciativas que ayudasen a entender y conocer cómo protegerse en la Red.

TOP 5: TRÁMITES Y COMPRAS ONLINE

La tecnología digital nos ha traído grandes beneficios, pero también ha generado nuevos riesgos para los usuarios en el comercio electrónico, la navegación web y la realización de gestiones online. El fraude en el comercio electrónico ha aumentado más rápido que la cifra de ventas, alcanzando un importe a nivel mundial de 41.400 millones de euros[20].

El fraude puede producirse de muchas maneras, como la suplantación de identidad, el robo de credenciales de una tarjeta de crédito o la publicación de ofertas falsas por las que el usuario nunca recibirá el producto adquirido. Es perjudicial tanto para los usuarios finales, como para las empresas, siendo particularmente sensibles las pymes por su menor capacidad de inversión para dotarse de los medios de protección.

Retos y amenazas que plantea

Los vectores de ataque y métodos utilizados por los ciberdelincuentes para perpetrar sus ataques son múltiples. Citamos algunos:

- Observación visual si introducimos nuestras claves en un lugar público.
- Interceptación del tráfico para robar contraseñas si estamos en una WiFi pública y no estamos utilizando una VPN.
- Introducción de las claves de mi tarjeta de crédito en un sitio web o una pasarela de pagos fraudulenta, si no somos capaces de verificar el grado de confianza del sitio.
- Interceptación de nuestras claves y de nuestra tarjeta de crédito por *malware* que se haya introducido en nuestro equipo si no tenemos actualizado el antivirus.
- Interceptación de nuestras claves y nuestra tarjeta de crédito por *malware* que se haya introducido en un sitio de *e-commerce* si la empresa que gestiona el sitio no ha parcheado las vulnerabilidades.

[20] Juniper Research: Online payment fraud: markets forecast, emerging threats & Segment analysis 2022-2027 https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report

- Ciberanzuelos o *phishing* vía *email*, SMS o ingeniería social. Un engaño mediante el cual nosotros mismos estamos facilitando nuestras claves al cibercriminal sin ser conscientes de ello.

- Duplicación fraudulenta de nuestro módulo SIM por el ciberdelincuente para interceptar los códigos de validación SMS.

- Falta de disciplina en la custodia de nuestras contraseñas, registrándolas en algún sitio desde donde puedan ser robadas, no actualizándolas periódicamente o utilizando una misma contraseña para varios servicios.

- Introducir nuestras credenciales en un sitio web que no tiene implementado el protocolo https (el candadito verde del navegador), permitiendo así que la comunicación pueda ser interceptada por un ciberdelincuente.

Con tantas posibles vías de ataque, el mayor reto es la concienciación y formación del ciudadano, para que sea capaz de elaborar sus propias estrategias y rutinas, adaptadas a las circunstancias personales que le permitan utilizar los servicios de la manera más segura posible.

El segundo reto es la disponibilidad y conocimiento del uso de herramientas, siendo imprescindibles los antivirus o EDR en todos los dispositivos, y su correcta configuración y actualización.

Necesidades de los ciudadanos

El ciudadano de a pie necesita conocer aspectos básicos de ciberseguridad como, por ejemplo, saber identificar si un sitio web es seguro y quién es el titular de este; las recomendaciones básicas de seguridad y buenas prácticas para operar en la red y realizar compras y gestiones; los riesgos a que se enfrenta y sus posibles consecuencias; los métodos de ataque o engaño más comunes y evitarlos. Si es una pyme o un autónomo, además necesita conocer qué tiene que hacer para ofrecer sus servicios digitales de manera segura para sus clientes y para sí mismo. En cualquier caso, en consonancia con lo anterior, la necesidad más primordial del ciudadano como consumidor o profesional es la formación en ciberseguridad.

Por otro lado, es necesario contar con una normativa clara que delimite las responsabilidades entre proveedores y usuarios de servicios digitales en caso de ataque cibernético o fraude.

Finalmente, cabe destacar que incluso con la mejor concienciación y educación se hace difícil gestionar todas las prácticas necesarias para una ciberseguridad personal sin apoyarse en herramientas. El ciudadano necesita una caja de herramientas de

ciberseguridad, a ser posible integrada y de fácil acceso, que incluya como mínimo lo más básico: antivirus o EDR, verificador de URL y gestor de contraseñas, además de un lector para el DNI electrónico.

Iniciativas de referencia

- La Asociación Española de Banca dispone de un portal con contenido formativo para usar de forma segura sus plataformas[21].
- OSI-INCIBE: Compra segura en internet[22].
- Guía de Ciberseguridad en el comercio electrónico[23].
- Cursos y tutoriales sobre compras online[24].

Propuestas a los actores impulsores de cultura ciberseguridad

- Inclusión de la ciberseguridad personal como materia en los ciclos de enseñanza obligatoria.
- Creación de una caja de herramientas de seguridad digital, conteniendo, al menos, los elementos mencionados en la sección anterior. Esto se podría proveer como un Kit Digital gratuito para los ciudadanos.
- Promover la elaboración de guías de consejos y seguridad para el uso de aplicaciones comerciales de pagos online, para que los ciudadanos puedan utilizarlas de forma segura.
- Promover la elaboravión de Kit de Consejos y configuración en las entregas de tarjetas y/o integración de medios de pagos en móviles (tecnología NFC) por parte las entidades financieras.
- Promover la emisión y popularización, por parte de los bancos y entidades de crédito, de tarjetas de crédito con numeración virtual o tarjetas de pago recargables.

---

[21] https://www.aebanca.es/category/ciberseguridad/

[22] https://www.osi.es/sites/default/files/docs/guia_compra_segura_internet_web_vfinal.pdf

[23] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad.pdf

[24] https://concienciat.gva.es/cursos/compras-online-seguras/; https://www.osi.es/es/pagos-online

- Promover el aprovechamiento de los recursos de los fabricantes de sistemas operativos de los principales móviles para ofrecer consejos de seguridad a los usuarios.
- Divulgar el conocimiento de los sellos de confianza de las páginas web y su significado.
- Delimitar las responsabilidades en caso de fraude, así como las consecuencias si no se han adoptado las medidas de seguridad necesarias por las distintas partes.

TOP 6: PRIVACIDAD E INFORMACIÓN PERSONAL

Desde la antigüedad, los individuos han percibido el valor de sus datos personales, pero no es hasta que el uso de las tecnologías de la información y las comunicaciones se generaliza cuando esta percepción se torna en preocupación por las capacidades de estas tecnologías para capturar, procesar, almacenar y transmitir datos e información personal.

Este derecho a la privacidad está regulado por el *Reglamento europeo 679/2016* de protección de datos personales y su adaptación a nuestro entramado legal, *la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales Personales.*

Estas disposiciones instituyen, entre otras, un conjunto de deberes para los responsables del tratamiento de estos datos, otorgan unos derechos a las personas físicas, prevén para cada Estado miembro una o varias autoridades de control independientes y establecen un conjunto de sanciones administrativas para los responsables en caso de incumplimiento.

Retos y amenazas que plantea

El principal reto es concienciar a las personas físicas en la importancia de sus datos personales y la necesidad de ser muy cautelosos cuando se ceden a terceros ante la enorme capacidad de las tecnologías de la información para recopilar, procesar, almacenar, transmitir datos, en especial en lo referente a datos sensibles, como los

relativos a la salud, ideología, opiniones políticas, vida u orientación sexual, origen étnico o racial, convicciones religiosas o filosóficas, la afiliación sindical, etc.

Mención aparte merecen las *cookies* que almacenan los datos de navegación en una web para transmitirlos después al responsable de esta, lo que puede permitirle conocer nuestros hábitos, preferencias, aficiones, idioma, etc.

Necesidades de los ciudadanos

Para afrontar estos retos y desafíos, los ciudadanos precisan, básicamente, conocer:

- Qué es un dato de carácter personal.
- Los derechos que les asisten según las disposiciones legales: acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos.
- Las condiciones de licitud del tratamiento de sus datos:
    - El interesado dio su consentimiento expreso, informado, libre, específico e inequívoco (consentimiento que debe poder ser retirado en cualquier momento tan fácilmente como se otorgó).

Que dicho tratamiento sea necesario para:

    - La ejecución de un contrato.
    - El cumplimiento de una obligación legal.
    - Proteger intereses vitales del interesado o de terceros.
    - El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.
    - La satisfacción de intereses legítimos del responsable del tratamiento o de un tercero.
- Ante quién y cómo proceder si considera conculcados sus derechos, el tratamiento de sus datos no se ha ejecutado bajo los principios de protección de datos o sin una base legitimadora adecuada.

Algunas iniciativas de referencia

- Educar en seguridad y privacidad digital: Curso organizado por la AEPD, el INCIBE y el INTEFP[25].

Propuestas a los actores impulsores de cultura ciberseguridad

- Identificar a los colectivos cuyos miembros están especialmente expuestos y realizar acciones de divulgación dirigidas específicamente a ellos.

- Impulsar acciones de divulgación en los colegios a través de las asociaciones de padres y madres (CEAPA, CONCAPA, AMPA, etc.) y las consejerías de educación de las comunidades autónomas.

- En el caso de personas mayores, canalizar las acciones a través de asociaciones de pensionistas, uniones de jubilados, asociaciones de mayores, etc., y las consejerías con competencias en el bienestar de los mayores. Así como ONGs como Cruz Roja, Cáritas, etc.

- Fomentar la corresponsabilidad de los ciudadanos, que pasa por conocer en primer lugar qué se entiende por datos personales, las categorías especiales de datos personales, los derechos que le asisten y los canales de denuncia, además del seguimiento de una serie de consejos en su navegación por internet. Por lo que respecta a los consejos en la navegación por Internet, se encuentran, entre otros:

    - No facilite información personal salvo que sea informado, al menos, de la identidad del responsable o encargado del tratamiento, la finalidad del tratamiento, los derechos que le asisten y ante quién ejercitarlos, la dirección electrónica u otro medio donde acceder al resto de informaciones obligadas por la normativa de protección de datos.

    - No proporcione información personal de terceros excepto que se haya obtenido su consentimiento.

    - Revise periódicamente la configuración de privacidad de sus cuentas en redes sociales.

    - Sea muy cauto con las informaciones personales que publique procurando que sean las mínimas, así como con las informaciones personales almacenadas en el móvil.

[25] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-incibe-e-intef-lanzan-un-nuevo-curso-de-formacion

- Desconfíe de los correos de desconocidos con faltas de ortografía, de ofertas muy atractivas que transmitan premura, *phishing*, ya que suelen solicitar datos personales como números de cuentas bancarias o instan al usuario a conectarse a páginas web con el mismo propósito.

- Si guarda información personal en la nube, configure adecuadamente las opciones de privacidad, asegurándose de que el canal de transferencia de datos trabaje bajo https, cifrando sus datos (aunque ya lo haga el proveedor del servicio) y manteniendo copias de seguridad en un soporte convencional.

- Si usa un sensor para monitorizar su actividad física, compruebe los ajustes del dispositivo para preservar su privacidad y no comparta la información registrada en las redes sociales.

TOP 7: INTERNET DE LAS COSAS

Hoy en día existen multitud de dispositivos cotidianos que están conectados a Internet y que recaban, tratan, almacenan y transmiten información del usuario, que puede ser de carácter básico o, incluso, en algunos casos de especial protección, como los datos relacionados con la salud. Se trata de tecnologías que tienen el objetivo de hacer más sencillas y eficientes determinadas actividades y que proporcionan, además, información de valor al usuario. Por ejemplo, a la hora de cocinar, hacer deporte, ver la televisión, etc. Es lo que conocemos como Internet de las Cosas (IOT).

El 16 de julio de 2020, la Comisión puso en marcha una investigación sectorial sobre el Internet de las Cosas de consumo[26] en la UE. Las conclusiones de la investigación confirmaron que, en general, cada vez más dispositivos y servicios se están convirtiendo

[26] https://competition-policy.ec.europa.eu/system/files/2022-01/internet-of-things_final_report_2022_es.pdf

en «inteligentes», lo que permite a los usuarios acceder a una gama cada vez más amplia de dispositivos y servicios interconectados dentro y fuera de sus hogares.

Según la Comisión Europea se espera el despliegue de más de 41.000 millones de dispositivos IoT para 2025. Uno de los principales retos del IoT tiene que ver con la capacidad de manejar volúmenes diversos y muy grandes de dispositivos conectados, así como con la necesidad de identificarlos de forma segura para que puedan conectarse a las redes de IoT[27].

En este sentido, se hace una especial alusión a los asistentes de voz que permiten a los usuarios acceder a una amplia gama de funciones, como reproducir música, escuchar la radio, noticias o podcasts, controlar dispositivos domésticos inteligentes, brindar información o ayudar en la planificación y ejecución de rutinas diarias, así como a las aplicaciones móviles inteligentes o las aplicaciones complementarias, interfaces de usuario para acceder a dispositivos inteligentes y servicios de IoT para consumidores.

Las soluciones de IoT se utilizan también dentro del contexto de las llamadas ciudades inteligentes o *smart cities*, con el objetivo de crear un entorno interconectado en las ciudades en el que se mejore el uso de los recursos y se proporcionen servicios de manera más inteligente, tanto en el transporte urbano como en el suministro de agua o en los sistemas de calefacción, entre otros muchos ámbitos.

Retos y amenazas que plantea

Los dispositivos asociados al IOT pueden contener vulnerabilidades, ya sea por su configuración, infraestructura o características. Teniendo en cuenta que esta tecnología recoge y procesa información de los usuarios, es fundamental poner atención en su protección y uso.

A esto hay que sumar que los dispositivos IoT están relacionados o conectados cada vez más con otras tecnologías como el Big Data, 5G o la Inteligencia Artificial, lo que incremente los riesgos a los que están sujetos estos dispositivos.

Los usuarios deben conocer los riesgos y las medidas de seguridad básicas cuando adquieren dispositivos que tengan la capacidad de conectarse a Internet para evitar que los ciberdelincuentes se hagan con su control, invadiendo la privacidad del usuario o generando situaciones de riesgo. En este sentido, es destacable lo señalado por la propuesta de Reglamento Europeo de Ciberresiliencia[28] , en el que se pone de manifiesto la insuficiente comprensión de la información y del acceso a ella por parte de los usuarios

[27] https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy

[28] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0454&from=ES

lo que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.

Tal y como apunta el INICIBE[29], a menudo el usuario no es consciente del tratamiento de datos llevado a cabo por los dispositivos sensorizados. Los mecanismos convencionales utilizados para obtener el consentimiento de los usuarios son considerados consentimientos de baja calidad debido a que en muchos casos se basan en la falta de información que recibe el usuario sobre el posterior tratamiento de los datos personales que está proporcionando. Además, esta información puede llegar a manos de terceros sin que el usuario sea consciente de su difusión.

En el día a día pueden encontrarse con la inutilización de los dispositivos conectados, la perdida de privacidad, vigilancia no autorizada, problemas para la salud o participación en actividades ilícitas por la utilización de los dispositivos conectados para formar parte de una red zombi para lanzar ciberataques a gran escala.

Necesidades de los ciudadanos

Conocer:

- Qué es el IoT, para qué sirve y en que les afecta desde el punto de vista de la seguridad.
- Aspectos relativos a la protección de datos y a la privacidad en el uso del IoT.
- Configuraciones de seguridad que pueden implementarse en dispositivos conectados.

Algunas iniciativas de referencia

- La Oficina de Seguridad del Internauta del Instituto Nacional de Seguridad, contempla un espacio específico sobre el IoT, los riesgos de un mundo hiperconectado[30].
- Informe de buenas prácticas en el IoT del CCN CERT[31].

---

[29] https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

[30] https://www.osi.es/es/campanas/iot-los-riesgos-de-un-mundo-hiperconectado

[31] https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-internet-de-las-cosas/file.html

Propuestas a los actores impulsores de cultura ciberseguridad

- **Guía Básica de Seguridad IoT**: las guías actuales están orientadas a las empresas, pero no tanto a la concienciación y buen uso por parte de la sociedad en general.

- **Concienciar sobre las obligaciones existentes** de informar a los consumidores de los riesgos de los dispositivos conectados a Internet si no se toman medidas de seguridad y se hace un uso responsable de ellos.

- **Acciones de concienciación** sobre un uso higiénico de los dispositivos IoT, para que los usuarios implementen medidas básicas necesaria, como las siguientes: cambiar las contraseñas por defecto que traen de fábrica estos dispositivos; crear contraseñas seguras para el acceso a las aplicaciones de los dispositivos IoT; instalación de antivirus o la configuración adecuada de la red doméstica, entre otras.

TOP 8: PROTECCIÓN DEL DISPOSITIVO

La capacidad de procesamiento y conexión con la que cuentan los dispositivos actuales (ordenadores, móviles, tabletas, *wearables*, aparatos conectados, etc.) tiene como consecuencia que los usuarios estén cada vez más expuestos a los riesgos que entraña el mal uso o funcionamiento incorrecto de los mismos.

Las consecuencias de esta situación pueden ir desde una simple molestia (por ejemplo, no saber cuántos pasos ha contabilizado nuestro *smartwatch* esta semana) hasta restricciones operativas muy serias, como robos de información, suplantación de identidad, sustracción de dinero y un largo etcétera.

Por este motivo, es esencial que los usuarios implementen medidas de protección de sus dispositivos y de la información que contienen, de manera que se minimicen en lo posible las amenazas a las que están sujetos. A esto se une la necesidad de hacer un uso correcto de los dispositivos, evitando prácticas que faciliten que los riesgos mencionados se materialicen.

Retos y amenazas que plantea

Nuestra sociedad tiene una cada vez mayor dependencia de los dispositivos conectados, especialmente, de teléfonos móviles, equipos informáticos y tabletas. Dicha dependencia es tal que estos aparatos se han vuelto en muchas ocasiones imprescindibles para realizar algunas actividades cotidianas, tanto en el ámbito personal como en el profesional.

El principal reto es proteger adecuadamente tanto los dispositivos en sí como la información que contienen. Es preciso concienciar de que es necesario implementar en los dispositivos medidas de seguridad tales como establecer claves de acceso al aparato, instalar antivirus, actualizar el software periódicamente, realizar copias de seguridad, utilizar aplicaciones de detección en caso de pérdida, mantener activo el *firewall*, navegar a través de VPN y así hasta cubrir las distintas necesidades en función del uso que haga de ellos. De lo contrario, el usuario estará dejando la puerta abierta a accesos no deseados que no solo socaven su privacidad, sino que les causen un perjuicio significativo como pudiera ser el robo de claves o acceso a información sensible.

Evitar las amenazas conlleva asumir la responsabilidad de aplicar medidas como las mencionadas y además llevar a cabo buenas prácticas durante la utilización de sus dispositivos. Esto supone, en muchos casos, aplicar el sentido común y la cautela para evitar situaciones –lamentablemente habituales– como escribir las claves de acceso o contraseñas y pegarlas al propio dispositivo, descargar archivos de páginas web no verificadas como seguras, dejar acceso libre a sus ordenadores o móviles, conectarse a redes abiertas sin protección, etc. En definitiva, otro de los retos actuales es concienciar a la población de la importancia de emplear la tecnología de manera adecuada, esto es, minimizando los riesgos de manera activa.

Necesidades de los ciudadanos

La protección de los dispositivos implica una participación proactiva de los usuarios, pues son ellos quienes habrán de adoptar la mayor parte de medidas destinadas a su seguridad. No obstante, es necesario que los propios dispositivos incorporen medidas de seguridad de la información y las comunicaciones, y además permitan una configuración sencilla para obtener un nivel de protección óptimo.

Los usuarios hoy en día son conocedores de la existencia de algunas soluciones que proporcionan seguridad a sus dispositivos, como, por ejemplo, los antivirus. Sin embargo, se produce una doble necesidad en cuanto que, por un lado, desconocen otras muchas herramientas destinadas a mejorar su protección y, por otro, no las instalan por desconfianza o por pensar que su configuración puede ser compleja. En ese sentido, los ciudadanos necesitan concienciarse sobre la importancia de las soluciones y configuraciones de seguridad y, a la vez, hace falta facilitarles la tarea a la hora de implementarlas.

Los ciudadanos también han de comprender que las medidas de seguridad, incluso cuando suponen un coste económico, son tan necesarias como lo son en otros ámbitos de la vida, véase la vivienda. Han de entender que las amenazas de la Red pueden ser tan peligrosas como algunas del ámbito físico, por ejemplo, un robo de claves bancarias puede suponer el robo de dinero de la cuenta.

Algunas iniciativas de referencia

- Oficina de Seguridad del Internauta de INCIBE: la OSI proporciona información y soporte al usuario final para evitar y resolver los problemas de seguridad que le pueden surgir al navegar por Internet, sobre todo, en sus primeros pasos en las nuevas tecnologías. Esta página cuenta, por un lado, con una sección de herramientas gratuitas[32] que los usuarios pueden descargar para instalar en sus dispositivos del tipo que sean. Por otro lado, contiene campañas para,

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

por ejemplo, saber configurar dispositivos móviles[33] para establecer unas capacidades mínimas de seguridad.

- El CSIRT-GV ha puesto en marcha una campaña[34] centrada en la protección de los dispositivos móviles frente a ciberataques. En ella se facilitan consejos prácticos, orientaciones e incluso la descarga de antivirus para que los usuarios tomen conciencia y establezcan medidas mínimas de seguridad.

Propuestas a los actores impulsores de cultura ciberseguridad

- Impulso de la fabricación de soluciones y dispositivos con ciberseguridad por diseño, de manera que aumente el nivel de protección mínimo adecuado para el usuario.

- Involucración de los propios fabricantes de tecnologías en la protección de los dispositivos que ponen a la venta, ya sea fomentando campañas conjuntas con organismos de concienciación al ciudadano o elaborando materiales con contenidos que ayuden al usuario a proteger esos dispositivos o soluciones.

- Desarrollar actividades de vigilancia tecnológica junto con el Ministerio de Consumo para comunicar a los fabricantes los problemas de seguridad en sus dispositivos, con la finalidad de que estos las subsanen a través de actualizaciones y para futuros desarrollos.

- Promocionar los programas de *bug bounty* (recompensas por encontrar vulnerabilidades) para dispositivos dirigidos al consumo mayoritario (y en especial para los públicos más desprotegidos).

- Enfatizar el enfoque de responsabilidad compartida de los propios usuarios, con el objetivo de que adopten las medidas oportunas para proteger sus dispositivos. En este sentido, tanto los conocimientos como los mensajes han de estar adaptados a los diferentes perfiles poblacionales y mediante los medios de comunicación más utilizados por dichos segmentos.

- Facilitar herramientas gratuitas de ciberseguridad a los ciudadanos, promocionando iniciativas similares o impulsando la que lleva a cabo la OSI.

- Subvenciones para dispositivos con seguridad por diseño.

---

[33] https://www.osi.es/es/campanas/dispositivos-moviles

[34] https://concienciat.gva.es/tips_de_seguridad/protege-tu-movil-de-ciberataques/

TOP 9: INTELIGENCIA ARTIFICIAL

La Estrategia Nacional de Inteligencia Artificial (ENIA)[35] señala que, del mismo modo que la inteligencia humana es muy compleja de definir, no existe aún una definición formal y universalmente aceptada de inteligencia artificial (IA), y se remite a la definición dada por la Comisión Europea que se ha referido a la IA como "sistemas de software (y posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital: percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado". La inteligencia artificial incluye el aprendizaje automático y el procesamiento del lenguaje natural[36].

El estudio elaborado por el Observatorio Nacional de Tecnología y Sociedad[37] (ONTSI), dirigido a analizar analiza la percepción de la opinión pública en relación con la implantación de elementos de IA, expone que "la población valora positivamente la aplicación de la IA en todas aquellas aplicaciones que suponen una ayuda en muchas actividades cotidianas y contribuyen a mejorar o facilitar nuestra vida". En este sentido, la IA puede aportar múltiples aplicaciones y oportunidades en diversos campos como la salud, la educación, el transporte y la gestión de la movilidad, el apoyo a la toma de decisiones o en el ámbito de la ciberseguridad para prevenir y detectar ciberataques o ayudarnos a la detección de noticias falsas y de patrones de comportamiento manipulativos.

Retos y amenazas que plantea

En cuanto a los riesgos relacionados con el uso de la IA para los ciudadanos, existen numerosos documentos que alertan sobre la necesidad de evaluar el posible impacto para los derechos humanos, tal y como asevera también la Comisión Europea. En este sentido, se debe considerar el posible sesgo de los algoritmos utilizados por la IA, que se puede producir cuando los datos manejados para su entrenamiento no son representativos en el contexto en el que se aplican. Además, se ha de ser consciente de que la inteligencia artificial puede utilizarse para la modificación de imágenes y videos con el objetivo de generar contenidos falsos

[35] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf

[36] ¿Qué es la inteligencia artificial? | Accenture

[37] Estudio sobre aplicación de la inteligencia artificial (ontsi.es)

o amplificar artificialmente determinadas informaciones, así como para facilitar la suplantación de la identidad a través de los denominados *deep fakes*.

Dado que la inteligencia artificial se basa en tener una gran cantidad de datos de los usuarios para poder entrenar a los algoritmos, uno de los mayores retos es la privacidad. Así, la IA combinada con Internet de las cosas (IoT) podría detectar patrones de comportamiento en el hogar o hábitos de navegación y compras por internet, a través de la captura y procesamiento de audio, video u otra información disponible a través de dispositivos conectados.

Nuestro país, sin duda, ha hecho una apuesta decidida por el desarrollo de la IA como parte de la *Estrategia España Digital 2025*, de la cual han derivado distintas medidas, como la publicación de la citada Estrategia Nacional de Inteligencia Artificial , que incluye como una de sus líneas de actuación la creación de confianza en la IA. Sin embargo, la IA está aún lejos de la ciudadanía, sin que esta sea consciente de los beneficios, que esta tecnología aporta ni de los riesgos[38].

Necesidades de los ciudadanos

Es necesario que los ciudadanos conozcan qué es la IA y para qué sirve, de una manera clara, concisa y sencilla.

En la misma línea, los ciudadanos deben conocer los riesgos y amenazas derivados de esta tecnología, en especial, aquellos aspectos relativos a la protección de datos.

Asimismo, los ciudadanos deben prestar atención a la configuración de seguridad de los dispositivos conectados que utilicen técnicas de IA.

Algunas iniciativas de referencia

- La Agencia de Protección de Datos en el documento de "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial"[39] hace referencia a los derechos que tienen los ciudadanos con relación a la toma de decisiones automatizadas.

- En el marco de la planificación del Programa Nacional de Inteligencia Artificial de Finlandia, AuroraAI es un programa que aglutina es una serie de cursos gratuitos en línea creados por Reaktor y la Universidad de Helsinki. Los cursos combinan la teoría con ejercicios prácticos. En la iniciativa también ha participado el Gobierno

[38] Una inteligencia artificial ética y confiable para la ciudadanía europea - Retina (https://retinatendencias.com/)

[39] https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

de España y su contenido (una introducción a la Inteligencia Artificial, en línea y gratis, para no expertos) se encuentra en español[40] .

- La Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad (INCIBE), en el espacio Ponte al Día, incluye un artículo sobre los **riesgos que pueden suponer los asistentes inteligentes**[41]. Además, proporciona un espacio sobre cómo realizar configuraciones seguras para altavoces inteligentes con el asistente Alexa[42].

- Asimismo, Amazon y Google, por su parte, han diseñado espacios específicos dirigidos a ayudar a implementar la seguridad de Alexa[43] y de Google Nest[44].

- Destacar también Hackers vs. Cybercrook[45], una aventura gráfica de la OSI en la que el usuario debe ayudar a un personaje a proteger su casa inteligente, amenazada por Cybercrook. El jugador debe ir resolviendo los problemas que le plantea el juego para poder avanzar en la aventura.

Propuestas a los actores impulsores de la cultura de la ciberseguridad

- Actualización de los recursos existentes e implementación de otros nuevos más concretos para impulsar las previsiones contempladas la *Ley 15/2022*, de 12 de julio, integral para la igualdad de trato y la no discriminación, en los que se alerte sobre los riesgos de la IA.

- Concienciar a la ciudadanía sobre el funcionamiento básico de la IA y cómo puede afectarles, en especial, en cuanto a la protección de sus datos personales, como establece la Estrategia Nacional de Inteligencia Artificial en su Línea de Actuación 6.1–Crear confianza en la IA.

- Implicar a fabricantes y desarrolladores, inclusive científicos y centros de investigación, para el desarrollo de acciones conjuntas de concienciación sobre la IA, sus usos y riesgos y, específicamente, sobre la utilización segura de los asistentes personales.

- Estas acciones deberían desarrollarse de manera articulada y conjunta a fin de alcanzar un mayor impacto a través de mensajes contundentes.

---

[40] https://www.elementsofai.com/es

[41] https://www.osi.es/es/actualidad/blog/2018/05/30/que-riesgos-pueden-suponer-los-asistentes-inteligentes

[42] https://www.osi.es/es/actualidad/blog/2020/07/24/configuraciones-seguras-para-altavoces-inteligentes-con-el-asistente

[43] https://www.amazon.es/Portal-de-privacidad-de-Alexa/b?node=17136920031

[44] https://landing.google.com/advancedprotection/

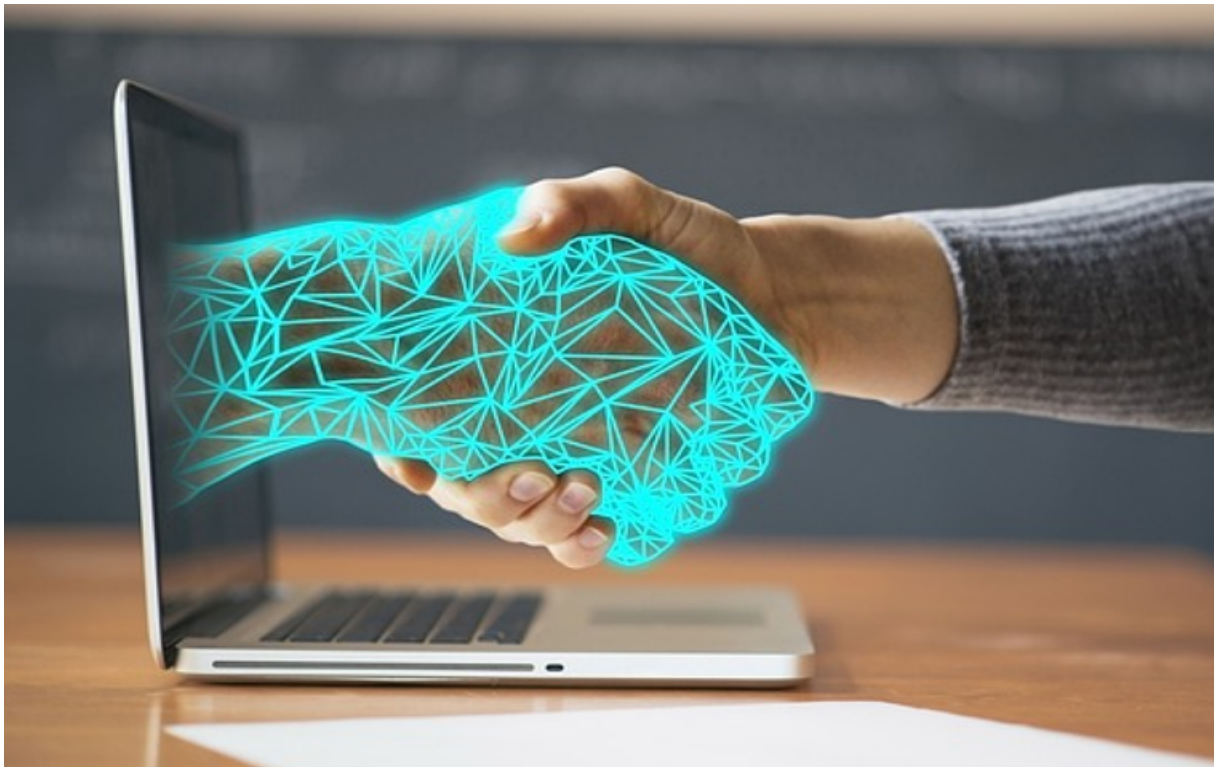
[45] https://www.osi.es/es/hackers

TOP 10: DENUNCIA, SOPORTE Y AYUDA

Saber a quién acudir para consultar dudas de ciberseguridad y recibir ayuda, así como conocer los canales de denuncia existentes si se ha sido víctima de un ciberdelito, constituyen necesidades esenciales para todos los ciudadanos que, en muchos casos, desconocen a quien dirigirse para recibir información, o cómo poner en conocimiento de las autoridades competentes los fraudes o ciberdelitos de los que han sido víctimas.

El soporte y la ayuda de terceros tienen un efecto tanto preventivo como reactivo, capacitando al ciudadano para hacer frente a las ciberamenazas, así como ayudando a la recuperación tras sufrir un ciberincidente.

Por otra parte, la denuncia del hecho delictivo es esencial para avanzar en la lucha contra la cibercriminalidad, que en los últimos años ha alcanzado un gran crecimiento[46].



[46] https://www.europapress.es/nacional/noticia-cibercriminalidad-mantiene-tendencia-alza-subir-89-pandemia-20230122112547.html

Retos y desafíos que plantea

A pesar de que el conocimiento y el recurso a los canales de ayuda ha ido aumentado progresivamente, se constata que aún no serían conocidos por la mayoría de la población, como pone de manifiesto el estudio "Cómo se protege la ciudadanía ante los ciberriesgos" [47], en el que se indica que el servicio proporcionado por el INCIBE a través del teléfono 017, en el que se brinda ayuda sobre ciberseguridad a la ciudadanía y empresas, es conocido por el 15,4% de las personas encuestadas.

Por otro lado, es importante que el ciudadano sepa que, a pesar de que todo intercambio de información u operatividad en Internet deja un rastro digital, los datos son volátiles, susceptibles de ser duplicados, fácilmente modificables e incluso eliminados, por lo que, ante la presencia de un posible delito o incidente, hay que actuar y ponerlo en conocimiento de las autoridades a la mayor brevedad, facilitándole el conocimiento de los canales de denuncia y su acceso. En este sentido, la posibilidad de la denuncia online, particularmente, ampliando la posibilidad de hechos delictivos que se pueden denunciar, facilitaría que el ciudadano pusiera en conocimiento los hechos de manera más rápida y eficiente.

Necesidades de los ciudadanos

Conocer los canales de ayuda, tanto los ofrecidos por las Administraciones Públicas como los que ponen a su disposición otras entidades con las que se relacionan de manera telemática, como los bancos.

Conocer y facilitar el acceso a los canales de denuncia proporcionados por las Fuerzas y Cuerpos de Seguridad del Estado y la Agencia Española de Protección, entre otros.

Concienciación sobre qué medidas tomar si se está siendo o se ha sido víctima de un ciberdelito. Por ejemplo[48]:

- Cómo hacer una denuncia y qué documentación se debe aportar.
- Acciones para evitar la progresión del ataque y para tratar de bloquear operaciones fraudulentas, alertando rápidamente, en su caso, al banco.
- Acciones para facilitar la investigación:

[47] https://observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

[48] Información más detallada en el ANEXO

- información que se ha de recopilar, cómo hacerlo y cómo conservarla (correos electrónicos, conversaciones, páginas web, videos, perfiles de redes sociales etc.);

- uso de los servicios de terceros de confianza o testigos online, que certifican el contenido publicado y público en la Red y pueden garantizar su validez en un proceso penal;

- acudir a un notario, a un perito forense o a las autoridades policiales que puedan certificar el contenido en cuestión.

Algunas iniciativas de referencia

- Concurso lanzado por INCIBE para dar a conocer el teléfono 017 entre todos los centros educativos de España[49].

- Campaña Europol EC3 sobre cómo hacer de tu hogar un lugar ciberseguro[50].

- Campaña de Policía Nacional destinada al uso seguro de Internet por parte de menores, en colaboración con Telefónica[51].

- Campaña "YO DENUNCIO" de la Guardia Civil (iniciativa de 2010).

- Campaña de la Agencia Española de Protección de Datos y del Ministerio de Consumo con consejos para actuar ante una suplantación de identidad en redes sociales, incluyendo la denuncia[52].

Propuestas a los actores impulsores de cultura ciberseguridad

- Explicar mediante mensajes más claros y contundentes las diferentes vías y canales disponibles de ayuda para la ciudadanía, respuesta a incidentes, soporte especializado y denuncia. En el caso de la denuncia los canales serían los siguientes:

---

[49] https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-concurso-dar-conocer-el-telefono-017-todos-los-centros

[50] https://www.europol.europa.eu/cms/sites/default/files/documents/safe-at-home_es.pdf

[51] ttp://www.ciberexperto.org/

[52] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-ministerio-consumo-campana-suplantacion-identidad

    - Brigada Central de Investigación Tecnológica (BCIT) de la Policía Nacional; Grupo de Delitos Telemáticos (DT) de la Guardia Civil; Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza; Unidad Central de Delitos Informáticos de los Mossos y Grupo de Apoyo Tecnológico de la Policía Foral de Navarra.

    - En el caso concreto de contenidos sensibles, la Agencia Española de Protección de datos pone a disposición de la ciudadanía un canal prioritario de retirada de contenidos sensibles.

    - Fiscal de Sala de Criminalidad Informática.

    - Defensor del Pueblo.

- Sería positivo que existiera una forma alternativa y segura de presentar las denuncias para optimizar el tiempo de atención al ciudadano, que incluyese, por ejemplo, la firma electrónica con doble factor de autenticación en las Sedes Electrónica de la Guardia Civil y de la Policía Nacional.

- Nuevas campañas en prensa y medios de comunicación para difundir estos canales.

- Repositorio común con las vías de denuncia y canales públicos puestos a disposición de los ciudadanos.

ANEXO

DECÁLOGO DE RECOMENDACIONES SI VAS A DENUNCIAR

La investigación tecnológica se basa en datos, muchas veces, intangibles. No obstante, todo intercambio de información u operatividad en Internet deja un rastro digital.

> Todos los datos en la Red son volátiles, susceptibles de ser duplicados, fácilmente modificables e incluso eliminados, por lo que, ante la presencia de un posible delito o incidente, hay que actuar y ponerlo en conocimientos de las autoridades a la mayor brevedad.

Por todo ello, es recomendable que sigas los siguientes pasos:

1. Si se han realizado pagos a terceros o se han ejecutado transferencias fraudulentas, además de denunciarlo, debes contactar y alertar rápidamente a tu banco para tratar de bloquear la operación si fuera posible.

2. Si estás sufriendo un delito en ese momento y no puedes controlar el dispositivo, se te ha bloqueado, ves que se mueve el ratón por su cuenta o aparecen ventanas o caracteres raros de bloqueo, desenchufa el cable de alimentación del ordenador y del router y apaga el móvil. De esta manera, sin conexión, si están actuando de forma remota, no podrán seguir operando.

3. Si ya hemos sufrido el delito, no alteres el soporte original: no toques las aplicaciones que ya puedan estar abiertas, no sigas interactuando con los autores del delito si has mantenido conversaciones con ellos por algún medio como Whatsapp, correo electrónico u otras aplicaciones de intercambio de información.

4. Recopila conserva y no borres toda la información disponible que tengas sobre el hecho: correos electrónicos conversaciones, páginas web donde hayas operado, documentación como supuestas facturas, justificantes de pago, así como las cuentas de usuario que puedas tener. Ten en cuenta que si borras o pierdes alguna de la información de la que dispones, nunca se podrá volver a recuperar.

5. Si has sufrido un cargo fraudulento o inesperado que no has realizado, tienes que acudir a tu banco para que verifique la operación y te aporte un comprobante sobre la operaciones fraudulentas que deberás adjuntar en el momento de la denuncia.

6. No modifiques claves ni contraseñas. Imagínate que cierras la cuenta de una red social, por ejemplo, Facebook, y estuviste hablando por mensaje privado con un sospechoso. Ya no se podrá acceder a sus contenidos salvo que tenga la contraseña guardada en el dispositivo.

7. Los pantallazos no tienen validez en un proceso penal. Es habitual presentar capturas de pantalla mal detalladas, impresas en un papel o pantallazos imprecisos de la información. Las capturas de pantalla son fácilmente modificables y no serán admitidas en un proceso judicial. Si tienes que recoger cualquier comentario, perfil en redes o páginas web existen los denominados terceros de confianza o testigos online, webs que certifican automáticamente el contenido publicado y público en la Red. Estos servicios te permiten realizar una copia exacta del contenido de la página que te interese reportar y certifican que no ha sido alterado. Solo tienes que introducir la URL (la dirección en la Red que te he mostrado) de la página que desees y posteriormente te lo envían al correo que desees en formato PDF.

   Si no sabes emplearlos o los contenidos son de carácter privado, como mensajes directos en redes sociales o sistemas de mensajería, será necesario que acudas a un notario, a un perito forense o a las autoridades policiales que puedan certificar el contenido en cuestión.

8. Si dispones de información como cuentas de perfiles en redes sociales, emails, conversaciones en plataformas de segunda mano, etc. debes ser muy cauteloso porque puedes aportar esa información de forma parcial, incompleta o ilocalizable.

9. Si tienes que reportar o denunciar perfiles, no es suficiente con el *nick* o seudónimo. Debes saber que cada uno de los usuarios de las redes sociales tiene su propio identificador. Si no sabes cómo obtenerlo, puedes ir a la página principal o de inicio del perfil o cuenta que te interese reportar y copiar la URL (nombre de la página web) de la barra de direcciones que estés visionando del perfil. No obstante, el *nick* también es fundamental (aunque ya venga implícito en el identificador).

10. Si has comprado en un anuncio sospechoso, los datos clave que deberás aportar son, como mínimo, la URL de la barra de direcciones del navegador y todos los datos que puedan ayudar a situar el anuncio: sección, usuario/referencia de publicación, fecha y hora y cualquier otro dato concreto.

11. Si tienes que denunciar o aportar la referencia a algún vídeo que esté publicado, no aportes capturas a modo de fotograma. Lo ideal sería, si sabes, que descargues inmediatamente el vídeo y lo aportes como un archivo por separado. Existen programas gratuitos que te permiten descargarte el archivo de vídeo. SI no sabes

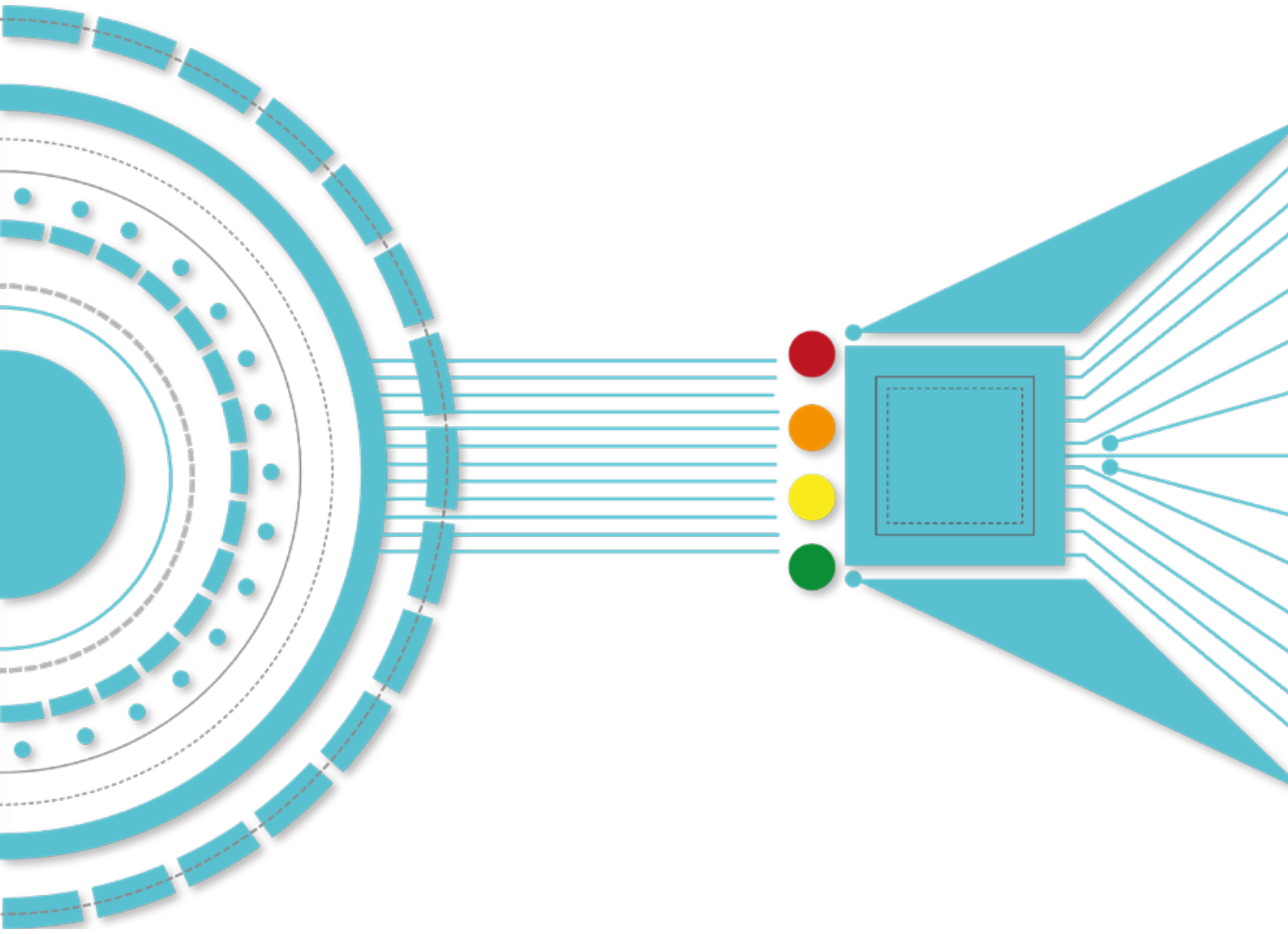
realizar este proceso, es suficiente con que aportes la URL o la dirección web del vídeo y el nombre del canal del usuario que lo publica.

12. Si ha sido tu empresa la que ha sufrido un ataque, sería conveniente que realizaras un informe pericial informático forense de cara a presentar las evidencias del ataque sufrido y hacerlo valer en un juicio para asumir las responsabilidades que correspondan frente a otros u los clientes.

13. Conserva toda la información y las evidencias digitales que hayas aportado o se te hayan solicitado hasta el final del proceso.

14. Debes saber que puedes ampliar la información de la que dispones en cualquier momento ante las autoridades si dispones de nuevos datos o de nueva documentación.

4. SEMÁFORO DE RIESGOS Y SECTORES MÁS VULNERABLES



	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
REDES SOCIALES	🔴	🟠	🔴	🔴	• Clarificación sobre las opciones de privacidad ofrecidas por las redes sociales y el establecimiento de opciones restrictivas en el uso del perfil personal. • Concienciación y uso del sentido común en el comportamiento ante los desconocidos y sus planteamientos de enlace (match) en la red del mismo modo que lo haríamos en el mundo real. • La no publicación ni facilitación de datos propios que abran la puerta a la identificación de conductas o hábitos que puedan derivar en caer víctimas de un delito. • Atención a la publicación de imágenes o contenidos de terceros y especialmente en el caso de menores. • Impulsar la implantación efectiva de controles de acceso para los menores de edad.
	Se trata de uno de los medios más utilizados para ataques de ingeniería social y otras conductas delictivas como el ciberacoso o el ciberbullying Es una puerta de entrada para incidentes y exposición de privacidad y, en numerosos casos, también de actividades fraudulentas y criminales				
USO DE CONTRASEÑAS Y CREDENCIALES	🟠	🔴	🔴	🔴	• Programas de concienciación y educación en ciberseguridad. Con eslóganes como “Tu contraseña es la llave de tu casa, ¿la dejarías en un lugar donde cualquiera la pudiera coger?” • Cybervoluntarios en las escuelas, asociaciones de vecinos y centros de mayores que ayuden a las personas con pocos conocimientos a utilizar el certificado digital. • Facilitar el acceso a gestores de contraseñas, con una subvención si fuera necesario (al igual que existe una subvención para el Kit Digital). • Impulso del uso de la biometría como mecanismo de autenticación, sin menoscabo de su consideración como dato personal sensible. • Fomento de la responsabilidad compartida entre proveedores y usuarios en el uso de credenciales y la gestión de la autenticación, para evitar las malas prácticas de los dueños de los sistemas si, por ejemplo, no disponen de autenticación de factor múltiple o permiten contraseñas débiles.
	El robo de contraseñas es un vector de ataque habitual y muy exitoso para todo tipo de atacantes				
ATAQUES DE INGENIERÍA SOCIAL	🟠	🔴	🔴	🔴	• Lanzamiento de links engañosos que lleven a una página que sirva como concienciación y educación a los ciudadanos, como lo hace la Universidad Veracruzana, o como lo hacen algunas empresas con sus empleados. • Campañas de concienciación masivas basadas en el autoconocimiento para el empoderamiento de la ciudadanía, aportando más valor e información, más allá de los hábitos. • Aplicaciones gratuitas para lectura de código QR, que permitan visualizar la URL antes de acceder a ella. • Mensajes más contundentes sobre la amenaza del *phishing*, de los QRs maliciosos y cómo darnos cuenta de que hemos sido víctimas.
	Se trata de medios no técnicos para conseguir de manera fraudulenta el acceso a información o sistemas o para llevar a cabo un fraude.	Incluye la suplantación, el engaño, la manipulación y, en general, el abuso de la confianza de las personas para que revelen información o realicen acciones perjudiciales sin buscar esos efectos o ser conscientes de ellos.			

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
PRIMER ACCESO A LAS TIC					• Elaborar una hoja de ruta de formación que se plasme en iniciativas de todo tipo adaptadas a la edad de los más jóvenes, como pueden ser la grabación de contenidos audiovisuales infantiles, charlas en los centros educativos, aplicaciones o juegos que les permitan aprender mientras se entretienen. En definitiva, es necesario adaptar formatos y mensajes a los menores para poder llegar a ellos de manera eficaz. En ese sentido, es fundamental contar con los educadores, quienes realmente conocen esas necesidades. • Los padres deben desempeñar un papel principal en la educación y el ciudadano del acceso a las TIC de sus hijos. En ese sentido, han de ser conscientes y transmitir la corresponsabilidad que supone utilizar las tecnologías. El primer acceso a las TIC requiere también acciones orientadas a los padres, como puedan ser campañas de sensibilización o actividades lúdico-educativas que puedan llevar a cabo conjuntamente progenitores y menores. • El ámbito educativo también debe estar implicado en la formación y concienciación de los menores cuando comienzan a utilizar las tecnologías. Convendría alcanzar acuerdos y convenios al más alto nivel para que los colegios incorporen actividades destinadas a dicho fin, en las que estén involucrados tanto los educadores, como los padres, expertos en la materia y, evidentemente, los menores. • En el caso de las personas mayores, igualmente requiere que los mensajes y contenidos que contribuyan a su formación estén adaptados a su edad e intereses. Uno de los aspectos clave al respecto es evitar provocar 'miedo' a la hora de utilizar sus dispositivos, sino todo lo contrario, confianza y herramientas para que estos usuarios sepan reaccionar ante los retos que se les planteen. • Las campañas de concienciación son una herramienta muy útil, pero insuficiente si no van acompañadas de otras acciones. En este sentido, se deben identificar las vías de acceso a ese segmento de población, localizando sus centros de encuentro, en ciudades y zonas rurales o los medios de comunicación más populares entre los mayores, para que las actividades formativas lleguen al público objetivo. • Al igual que los jóvenes, resultaría interesante involucrar a los descendientes de las personas mayores, ya sean sus hijos, nietos, sobrinos o cualquier otro familiar que pueda ayudarles, por ejemplo, mediante actividades compartidas lúdico-formativas. • Las entidades financieras, la Administración, y todas aquellas organizaciones de cualquier tipo que requirieran el uso de la tecnología para poder beneficiarse de sus servicios, deberían participar en iniciativas que ayudasen a entender y conocer cómo protegerse en la Red.
	Se produce, por un lado, a edades cada vez más tempranas y, por otro, a edades tardías en las que los ciudadanos se ven obligados a utilizar herramientas que nunca habían empleado enfrentándose a riesgos y amenazas para los que no están preparados ni formados.				

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN
				
TRÁMITES Y COMPRAS ON LINE	Durante el acceso online a plataformas de compras, adquisición de servicios o trámites con las administraciones, los ciudadanos se enfrentan a situaciones de riesgo para los que no siempre han recibido una formación que les permita proteger sus datos y su patrimonio.			

RECOMENDACIONES

- Inclusión de la ciberseguridad personal como materia en los ciclos de enseñanza obligatoria.
- Creación de una caja de herramientas de seguridad digital. Esto se podría proveer como un Kit Digital gratuito para los ciudadanos.
- Promover la elaboración de guías de consejos y seguridad para el uso de aplicaciones comerciales de pagos online, para que los ciudadanos puedan utilizarlas de forma segura.
- Promover la elaboración de Kit de Consejos y configuración en las entregas de tarjetas y/o integración de medios de pagos en móviles (tecnología NFC) por parte las entidades financieras.
- Promover la emisión y popularización, por parte de los bancos y entidades de crédito, de tarjetas de crédito con numeración virtual o tarjetas de pago recargables.
- Promover el aprovechamiento de los recursos de los fabricantes de sistemas operativos de los principales móviles para ofrecer consejos de seguridad a los usuarios.
- Divulgar el conocimiento de los sellos de confianza de las páginas web y su significado.
- Delimitar las responsabilidades en caso de fraude, así como las consecuencias si no se han adoptado las medidas de seguridad necesarias por las distintas partes.

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES

PRIVACIDAD E INFORMACIÓN PERSONAL	●	●	●	●	• Identificar a los colectivos cuyos miembros están especialmente expuestos y realizar acciones de divulgación dirigidas específicamente a cada colectivo.
					• Impulsar acciones de divulgación en los colegios a través de las asociaciones de padres y madres (CEAPA, CONCAPA, AMPA, etc.) y las consejerías de educación de las comunidades autónomas.
					• En el caso de personas mayores, canalizar las acciones a través de asociaciones de pensionistas, uniones de jubilados, asociaciones mayores, etc., y las consejerías con competencias en el bienestar de los mayores. Así como ONGs como Cruz Roja, Caritas.
					• Fomentar la corresponsabilidad de los ciudadanos, que pasa por conocer en primer lugar qué se entiende por datos personales, las categorías especiales de datos personales, los derechos que le asisten y los canales de denuncia, además del seguimiento de una serie de consejos en su navegación por internet. Por lo que respecta a los consejos en la navegación por internet, se encuentran, entre otros:
					  • No facilite información personal salvo que sea informado, al menos, de: la identidad del responsable o encargado del tratamiento, la finalidad del tratamiento, los derechos que le asisten y ante quien ejercitarlos, la dirección electrónica u otro medio donde acceder al resto de informaciones obligadas por la normativa de protección de datos.
					  • No proporcione información personal de terceros excepto que se haya obtenido su consentimiento.
					  • Revise periódicamente la configuración de privacidad de sus cuentas en redes sociales.
					  • Sea muy cauto con las informaciones personales que publique procurando que sean las mínimas, así como con las informaciones personales almacenadas en el móvil.
					  • Desconfíe de los correos de desconocidos con faltas de ortografía, de ofertas muy atractivas, que transmiten premura, etc. (*phising*), pues a menudo solicitan datos personales, como números de cuentas bancarias, o instan a conectarse a páginas web con los mismos propósitos.
					  • Si guarda información personal en la nube, configure adecuadamente las opciones privacidad, asegurándose de que el canal de transferencia de datos trabaje bajo https, cifrando sus datos (aunque ya lo haga el proveedor del servicio) y manteniendo copias de seguridad en un soporte convencional.
					  • Si usa un sensor para monitorizar su actividad física, compruebe los ajustes del dispositivo para preservar su privacidad y no comparta la información registrada en las redes sociales.

Preocupación por las capacidades de la tecnología para capturar, procesar, almacenar y transmitir datos e información personal.

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
INTERNET DE LAS COSAS					• Guía Básica de Seguridad IoT: las guías actuales están orientadas a las empresas, pero no tanto a la concienciación y buen uso por parte de la sociedad en general. • Concienciar sobre las obligaciones existentes de informar a los consumidores de los riesgos de los dispositivos conectados a Internet si no se toman medidas de seguridad y se hace un uso responsable de ellos. • Acciones de concienciación sobre un uso higiénico de los dispositivos IoT, para que los usuarios implementen las medidas básicas necesaria como las siguientes: cambiar las contraseñas por defecto que traen de fábrica estos dispositivos; crear contraseñas seguras para el acceso a las aplicaciones de los dispositivos IoT; instalación de antivirus o la configuración adecuada de la red doméstica, entre otras.
	Existen multitud de dispositivos cotidianos que están conectados a Internet y que recaban, tratan, almacenan y transmiten información del usuario, que puede ser básica o de especial protección Estos dispositivos suelen contener vulnerabilidades, ya sea por su configuración, infraestructura o características				
PROTECCIÓN DE LOS DISPOSITIVOS					• Impulso de la fabricación de soluciones y dispositivos con ciberseguridad por diseño, de manera que aumente el nivel de protección mínimo adecuado para el usuario. • Involucración de los propios fabricantes de tecnologías en la protección de los dispositivos que ponen a la venta, ya sea fomentando campañas conjuntas con organismos de concienciación al ciudadano o elaborando materiales con contenidos que ayuden al usuario a proteger esos dispositivos o soluciones. • Desarrollar actividades de vigilancia tecnológica junto con el Ministerio de Consumo para comunicar a los fabricantes los problemas de seguridad en sus dispositivos, con la finalidad de que estos las subsanen a través de actualizaciones y para futuros desarrollos. • Promocionar los programas de *bug bounty* (recompensas por encontrar vulnerabilidades) para dispositivos dirigidos al consumo mayoritario (y en especial para los públicos más desprotegidos). • Enfatizar el enfoque de responsabilidad compartida de los propios usuarios, con el objetivo de que adopten las medidas oportunas para proteger sus dispositivos. En este sentido, tanto los conocimientos como los mensajes han de estar adaptados a los diferentes perfiles poblacionales y mediante los medios de comunicación más utilizados por dichos segmentos. • Facilitar herramientas gratuitas de ciberseguridad a los ciudadanos, promocionando iniciativas similares o impulsando la que lleva a cabo la Oficina de Seguridad del Internauta. • Subvenciones para dispositivos con seguridad por diseño.
	La capacidad de procesamiento y de conexión con la que cuentan los dispositivos actuales (teléfonos inteligentes y tabletas, más allá de los típicos portátiles, y a los que podemos sumar todo tipo de wearables) hace que las personas estemos, cada vez, más expuestas a los riesgos de un mal uso o un mal funcionamiento de los mismos.				

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
INTELIGENCIA ARTIFICIAL	🟠	🟠	🔴	🟠	• Actualización de los recursos existentes e implementación de otros nuevos más concretos para impulsar las previsiones contempladas la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, en los que se alerte sobre los riesgos de la IA. • Concienciar a la ciudadanía sobre el funcionamiento básico de la IA y cómo puede afectarles, en especial, en cuanto a la protección de sus datos personales, como establece la Estrategia Nacional de Inteligencia Artificial en su Línea de Actuación 6.1 Crear confianza en la IA . • Implicar a fabricantes y desarrolladores, inclusive científicos y centros de investigación, para el desarrollo de acciones conjuntas de concienciación sobre la IA, sus usos y riesgos y, específicamente, sobre la utilización segura de los asistentes personales. • Estas acciones deberían desarrollarse de manera articulada y conjunta a fin de alcanzar un mayor impacto a través de mensajes contundentes.
	Esta tecnología no presenta una flexibilidad como la de la inteligencia humana, que permite adaptarse a cualquier situación, lo que puede llevar a un comportamiento erróneo que podría conllevar una vulneración de la protección de datos e incluso suplantar la identidad de una persona.				

DENUNCIA, SOPORTE Y AYUDA	🔴	🔴	🔴	🔴	• Explicar mediante mensajes más claros y contundentes las diferentes vías y canales disponibles de ayuda para la ciudadanía, respuesta a incidentes, soporte especializado y denuncia. En el caso de la denuncia, los canales serían los siguientes:
					  • Brigada Central de Investigación Tecnológica (BCIT) de la Policía Nacional; Grupo de Delitos Telemáticos (DT) de la Guardia Civil; Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza; Unidad Central de Delitos Informáticos de los Mossos y Grupo de Apoyo Tecnológico de la Policía Foral de Navarra.
					  • En el caso concreto de contenidos sensibles, la Agencia Española de Protección de Datos pone a disposición de la ciudadanía un canal prioritario de retirada de contenidos sensibles.
					  • Fiscal de Sala de Criminalidad Informática.
					  • Defensor del Pueblo.
					• Sería positivo que existiera una forma alternativa y segura de presentar las denuncias para optimizar el tiempo de atención al ciudadano, que incluyese, por ejemplo, la firma electrónica con doble factor de autenticación en las Sedes Electrónica de la Guardia Civil y de la Policía Nacional.
					• Nuevas campañas en prensa y medios de comunicación para difundir estos canales.
					• Repositorio común con las vías de denuncia y canales públicos puestos a disposición de los ciudadanos.

	Actualmente, se pueden realizar múltiples trámites con las Administraciones Públicas a través de las TIC, principalmente haciendo uso del certificado electrónico o de otros mecanismos, esto no se ve reflejado cuando el ciudadano tiene la necesidad de presentar una denuncia ante las Fuerzas y Cuerpos de Seguridad, ya que esta únicamente puede presentarse en casos concretos, siendo obligatorio el desplazamiento físico.				

5. CONCLUSIONES Y RECOMENDACIONES

La **transformación digital** de nuestra sociedad se orienta en gran medida a mejorar la vida de la población. Sin embargo, el uso de la tecnología también entraña grandes peligros y retos, entre los cuales destaca la ciberseguridad. El establecimiento de determinadas **medidas de seguridad**, el **uso responsable** de los dispositivos o la **formación**, son algunos de los requerimientos mínimos que deben asumir los ciudadanos.

Entre ellos, **menores de edad, personas mayores, población en edad laboral o colectivos en riesgo de exclusión**, como discapacitados o inmigrantes, constituyen grupos que requieren una especial atención por su vulnerabilidad en cuanto al buen uso de la tecnología y la ciberseguridad.

Con independencia de las recomendaciones propuestas en cada uno de los ámbitos analizados en esta Brújula, existe un **denominador común a todos ellos que es la falta de conocimiento y concienciación de la ciudadanía** sobre los peligros inherentes a un mal uso de la tecnología. A esto hay que añadir la falta de una infraestructura y dispositivos seguros.

Para avanzar en la corresponsabilidad, los ciudadanos deben tener acceso a información y la Administración debe promover fórmulas, utilizando todos los recursos a su alcance, para explicar los riesgos a los que aquellos están sometidos, así como las recomendaciones sobre las medidas adecuadas para combatirlos. Si bien es cierto que existen muchas actuaciones en este sentido, los datos muestran que queda mucho por hacer, no tanto quizá en cuanto a número de iniciativas, sino más bien desde la **perspectiva de la unidad de acción y coordinación a través de una visión estratégica**.

En definitiva, sería necesario acometer el diseño e implantación de un **Plan estratégico de ciberseguridad ciudadana,** que contenga la descripción de las acciones a ejecutar sobre cada colectivo de riesgo y sus modalidades: formación a todos los niveles, concienciación mediante campañas dirigidas a cada público objetivo, mejora de la regulación de aquellos aspectos que facilitan la progresión de los riesgos, promoción de acuerdos con diseñadores y fabricantes de *software* y dispositivos para incorporar desde el diseño inicial medidas de seguridad adecuadas en los dispositivos, impulso y facilitación del acceso a los servicios de denuncia y ayuda ante incidentes, y todo cuanto contribuya a mejorar la

capacidad de respuesta frente a los riesgos por parte de la población. En este sentido, es particularmente importante poner el foco en los menores, mediante una **Estrategia de protección de menores online**[53] unitaria, y dotarse de los recursos necesarios para su implementación. Como viene señalando la Fiscalía General del Estado en su Memoria Anual[54] "la endémica carencia de medios personales y materiales en la lucha contra la ciberdelincuencia tiene en este ámbito unas consecuencias especialmente graves".

La consecución de un objetivo tan ambicioso exige realizar una detallada planificación de las acciones, un compromiso y una involucración de los niveles políticos y una sensibilización de los ciudadanos, para dotar a la sociedad en su conjunto de las herramientas necesarias para enfrentar los crecientes riesgos de ciberseguridad.

Para ello, el Plan definiría las áreas y los objetivos estratégicos, así como los indicadores para medir su consecución, entre los que se incluirían los siguientes:

- Educación y formación, con la implantación de la formación obligatoria en materia de ciberseguridad en el currículo escolar.
- Concienciación de ciberseguridad responsable que consiga un cambio de comportamiento de los usuarios.
- Seguridad por diseño de los dispositivos para facilitar su uso confiable.

En el pasado, hemos asistido a la puesta en marcha de planes de este tipo con notable éxito: campañas para promover la práctica del deporte o el ejercicio de hábitos saludables. En particular, **la Estrategia de Seguridad Vial 2011-2020 constituye un excelente modelo de referencia** a los fines que se pretenden por el paralelismo de las acciones a acometer.

[53] España ocupa el cuarto puesto en el índice global de la ciberseguridad de la Unión Internacional de Telecomunicaciones. Para poder seguir avanzando en el compromiso con la ciberseguridad que mide el índice, sería necesario poder responder con una Estrategia unitaria a la pregunta incluida en su cuestionario: ¿Hay una estrategia nacional de Protección de la Infancia en Línea? https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_Spanish.pdf

[54] https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/recursos/pdf/MEMFIS21.pdf

PLAN ESTRATÉGICO DE SEGURIDAD VIAL	PLAN ESTRATÉGICO DE CIBERSEGURIDAD
Educación Vial	Educación en Internet
Protección a los usuarios más vulnerables	Protección a los usuarios más vulnerables
Cumplimiento normas circulación	Elaboración y cumplimiento normas tráfico en la red
Mejora infraestructuras viarias	Internet segura
Vehículos más seguros	Dispositivos más seguros
Promoción del uso de las tecnologías modernas para aumentar la seguridad vial	Promoción del uso de las tecnologías para aumentar la ciberseguridad
Mejora de los servicios de emergencia y atención tras las lesiones	Mejora de los servicios de emergencia y atención tras los incidentes

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

NIPO (edición online): 089-23-012-3
Fecha de edición: junio 2023

FORO
NACIONAL DE
CIBERSEGURIDAD

2023