DigitAll

Formación en
Competencias
Digitales

4
Seguridad

DigitAll

Formación en
Competencias
Digitales

Seguridad

Nivel A1

ÍNDICE

4.1. PROTECCIÓN DE DISPOSITIVOS

- *Principios de la seguridad de la información*
- *Fuentes de información sobre seguridad*

4.2. PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

- *Derechos de los ciudadanos en materia de protección de datos*

4.3. PROTECCIÓN DE SALUD Y DEL BIENESTAR

- *Principios de la salud digital*

4.4. PROTECCIÓN MEDIOAMBIENTAL

- *Consumo sostenible de tecnología*

DigitAll

Seguridad

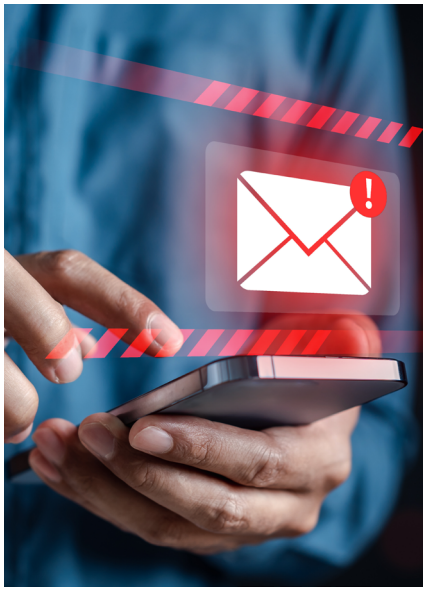
4.1 PROTECCIÓN DE DISPOSITIVOS

Seguridad

Nivel A1 4.1 Protección de dispositivos

Principios de la seguridad de la información

Principios de la seguridad de la información



La seguridad de la información en la sociedad actual juega un papel fundamental. Todos utilizamos a diario sistemas informáticos para gestionar nuestra información, ya sea a nivel personal, como en una empresa o en la administración pública. Esta migración de nuestros datos a formato digital conlleva una serie de riesgos que debemos conocer y controlar para no sufrir ningún ataque que los comprometa. En este tema vamos a definir el concepto de seguridad de la información, a presentar una serie de términos relacionados y a exponer una serie de principios que debemos seguir para proteger nuestros datos digitales.

Seguridad de la información

Dentro del mundo de la informática existen multitud de términos relacionados con la protección de los sistemas o de la información que estos gestionan. El primero de ellos es la seguridad de la información. Para entender este concepto, primero debemos definir qué significa exactamente información. La **información** es "todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma" (*CCN-STIC-431:2006*). En este sentido, la información puede encontrarse habitualmente en forma de mensajes, correos electrónicos, bases de datos, etc.

La **seguridad de la información**, por tanto, se define como la preservación de la confidencialidad, la integridad y la disponibilidad de esta información (*UNE-ISO/IEC 27000:2014*). Estos tres conceptos forman las tres dimensiones de la seguridad de la información, nombrado conjuntamente como **Tríada CIA** (del inglés, Confidentiality, Integrity and Availability). A continuación, se define brevemente cada uno de ellos:

1 | **Confidencialidad:** garantizar que la información es secreta, y solo las personas autorizadas pueden acceder a la misma y visualizarla.

2 | **Integridad:** asegurar que la información no se modifica sin permiso.

3 | **Disponibilidad:** capacidad de la información de ser accesible y estar lista para su uso cuando es demandada.

LA TRÍADA CIA: CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Se introduce el concepto de tríada CIA: Confidencialidad, Integridad y Disponibilidad. Se explican cada una de las partes que componen este concepto con ejemplos sencillos, pero reales, y se enfatiza en la importancia de este concepto dentro de la seguridad de la información.

e.digitall.org.es/A4C41A1V02

Las tres dimensiones de la seguridad de la Tríada CIA se definen como "servicios de seguridad" dentro de la *norma ISO-7498-2*. Además de la confidencialidad, la integridad y la disponibilidad, existen otros servicios de seguridad incluidos en esta norma:

1 | **Autenticación:** garantizar que alguien es quien dice ser, ya sea durante una comunicación o como autor de una información.

2 | **No repudio:** evitar que emisor o receptor nieguen la transmisión o la recepción de un mensaje, respectivamente.

3 | **Control de acceso:** evitar el acceso no autorizado a un recurso.

A la hora de pensar en diferentes medidas de protección de la seguridad de la información, debemos tener en cuenta todos los servicios de seguridad anteriores. Para comprender cada uno de los puntos vamos a ver el ejemplo de la aplicación que utilizamos en nuestra banca electrónica.

Cuando accedemos a la banca electrónica de nuestro banco a través de un navegador web, lo primero que podemos ver es información pública de los servicios que oferta. Si por cualquier error la página no estuviese accesible, la información no estaría **disponible** para su consulta. Si queremos acceder a nuestra información privada, como nuestras cuentas bancarias y los movimientos, necesitamos identificarnos. Para ello realizamos el proceso de **autenticación**, indicando nuestro nombre de usuario y contraseña. Por supuesto, si estos datos no son correctos, no podremos acceder a nuestra información, ya que existe un **control de acceso** a la misma. Una vez nos autenticado, podemos ver nuestros datos. Esta información

se envía cifrada desde los servidores del banco hasta nuestro ordenador, por lo tanto, es **confidencial**. Además, también se aplican mecanismos de control de **integridad**, para garantizar que la información que estamos visualizando es la correcta. Por último, dado que estamos autenticados, si realizamos un movimiento bancario utilizando nuestra cuenta, el banco garantiza el **no repudio** de la orden.

Seguridad informática

Además de la seguridad de la información existen otros conceptos similares que se suelen utilizar indistintamente, pero que cuentan con ciertos matices. Uno de ellos es el de **seguridad informática**, que hace referencia a los aspectos tecnológicos de la seguridad que inciden directamente en los medios informáticos donde la información es procesada, almacenada, distribuida, etc. Un ejemplo específico de este punto es utilizar cifrado para proteger los datos mientras están almacenados o en tránsito.

Por el contrario, la seguridad de la información es un término más amplio, que engloba a la seguridad informática, y que incluye aspectos sistémicos de la seguridad, como las políticas o procedimientos. Algún ejemplo de medida que se incluye dentro de la seguridad de la información, pero no en seguridad informática, son la aplicación de políticas de gestión de riesgos o la adecuación de la seguridad a la regulación vigente.

⚠ ATENCIÓN

A pesar de ser términos muy similares, la **seguridad de la información** y la **seguridad informática** no son lo mismo. La seguridad de la información es un término mucho más amplio, que engloba a la seguridad informática.

Principios de la seguridad de la información

Para garantizar un buen nivel de la seguridad de la información existen una serie de principios fundamentales que debemos seguir. Estos principios nos dan unas ideas básicas que pueden ser aplicables en múltiples escenarios. De aplicarse correctamente, podemos asegurar que dispondremos de un nivel de seguridad aceptable en nuestros sistemas.

Política de mínimos privilegios

Seguir una política de mínimos privilegios es una buena forma de enfocar la división de los permisos a la hora de poder acceder y procesar la información. En este sentido, los privilegios hacen referencia a los determinados permisos que tiene un usuario para realizar una acción específica sobre una información concreta. Por lo tanto, el principio de mínimo privilegio nos plantea que debemos configurar los permisos de la información de tal forma que se le permita realizar las acciones únicamente necesarias a cada usuario para garantizar sus actividades diarias. Lo que se pretende evitar es que un usuario, o grupo de usuarios, dispongan de más privilegios de los necesarios, lo que podría comprometer la seguridad del sistema.

Veamos un ejemplo de este principio. Imaginemos que varios usuarios de una misma organización utilizan el mismo ordenador para almacenar cierta información personal, como por ejemplo sus nóminas. En este escenario, ningún usuario debería poder consultar la nómina de otro usuario que no sea él mismo. Una posible configuración de este escenario podría ser crear una carpeta para cada usuario y configurar los permisos de tal forma que cada usuario tenga acceso únicamente a su carpeta personal. En este caso estamos aplicando el principio de mínimo privilegio, ya que estamos concediendo los permisos únicos necesarios a cada usuario para realizar sus tareas sin problema. Por el contrario, si no configurásemos los permisos correctamente, tendríamos un escenario en el que todos los usuarios dispondrían de permisos sobre todas las carpetas. En este sentido, cualquier usuario malintencionado o que haya sufrido un ataque, y cuya cuenta haya sido comprometida, supondría un potencial problema de seguridad sobre la información del sistema.

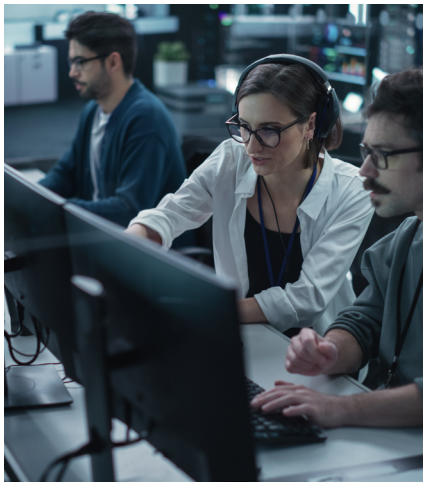
Política de control de acceso cerrado por defecto

Estrechamente relacionado con el principio anterior se encuentra el principio de control de acceso cerrado por defecto. La idea detrás de este principio es configurar los permisos de los usuarios sobre la información de forma restrictiva por defecto, de tal forma que nadie pueda tener acceso a menos que se indique específicamente. Establecer una política de control de acceso cerrado por defecto pretende

evitar el acceso indebido a cierta información de forma involuntaria y desapercibida.

Esta política se puede entender fácilmente si hablamos de los firewalls. Los firewalls son dispositivos que controlan las conexiones de la red. Por lo general, es una buena política configurar un firewall de modo que no permita ninguna conexión de red por defecto y añadir específicamente aquellas que necesitemos. Esto sucede, por ejemplo, con el firewall que viene configurado por defecto en el sistema operativo Windows. Este firewall no permite que alguien externo establezca una conexión de ningún tipo con nuestro ordenador, a menos que haya sido previamente iniciada por el propio equipo.

Segregación de funciones



En una organización es importante que las funciones estén repartidas entre los miembros de ésta. Dentro de una empresa existen, normalmente, diferentes departamentos que se encargan de diversas tareas, como el departamento de recursos humanos, el de marketing, o el de Tecnologías de la Información (TI). A la hora de utilizar los sistemas informáticos y gestionar la información de la organización se debería definir e implementar una serie de separaciones de las funciones y las responsabilidades de cada personal. Esto evita los conflictos de interés y la acumulación de privilegios en una única persona, lo que puede acarrear ciertos problemas de seguridad.

Un ejemplo claro podemos verlo en las funciones y tareas que deberían realizar el personal de cada uno de los departamentos de una empresa. No tendría sentido que el personal del departamento de finanzas pudiese realizar configuraciones en los dispositivos de red de una empresa, o que un empleado del departamento de marketing tuviese acceso a las nóminas de todos los empleados de la empresa. Al realizar una segregación de funciones entre los distintos empleados, aseguramos que los privilegios de los usuarios estén controlados y acotados a sus funciones diarias.

Defensa en profundidad

Este principio hace referencia a las medidas de seguridad de la información existentes, y su lugar de aplicación. Hoy en día, debido a la gran cantidad y diversidad de amenazas a las que estamos expuestos, no basta con aplicar una única medida de seguridad en un punto concreto de la organización. Es importante implementar diferentes niveles de seguridad en nuestros sistemas y en la información que estos gestionan.

Existen diferentes medidas o controles que pueden ser aplicados en cada nivel de seguridad. A continuación, se muestra un ejemplo para cada uno de estos niveles:

- **Políticas, procedimientos y concienciación:** disponer de una política de gestión de contraseñas en los equipos de la empresa, de tal forma que el usuario tenga que renovarla cada cierto tiempo y que cumpla con un mínimo de caracteres.
- **Seguridad física:** contar con un armario de comunicaciones, donde se encuentren los dispositivos de red, que esté cerrado con llave.
- **Perímetro:** instalar y configurar un firewall para controlar las conexiones entrantes y salientes de la empresa.
- **Red interna:** realizar una separación lógica de las redes internas de la organización utilizando redes VLAN (Virtual Local Area Network).
- **Host:** protección frente a software malicioso instalando sistemas antivirus.
- **Aplicación:** implementar un sistema de identidades a nivel corporativo.
- **Datos:** cifrar la información almacenada en los equipos.

La aplicación de una o varias medidas en uno de los niveles no nos garantiza que estemos completamente seguros. Se podría dar el caso en el que dispusiéramos de un alto nivel de seguridad física en la organización, contando con un guardia de seguridad, controlando los accesos al edificio, protegiendo los dispositivos de red en un armario de comunicaciones cerrado con llave... pero que no aplicásemos ningún otro control en el resto de los niveles de seguridad. Podríamos sufrir

Niveles de seguridad
(la imagen fue creada por el editor)

Saber más

Una VLAN es una red lógica que agrupa un conjunto de dispositivos que comparten una misma red física, aislando el tráfico de cada conjunto.

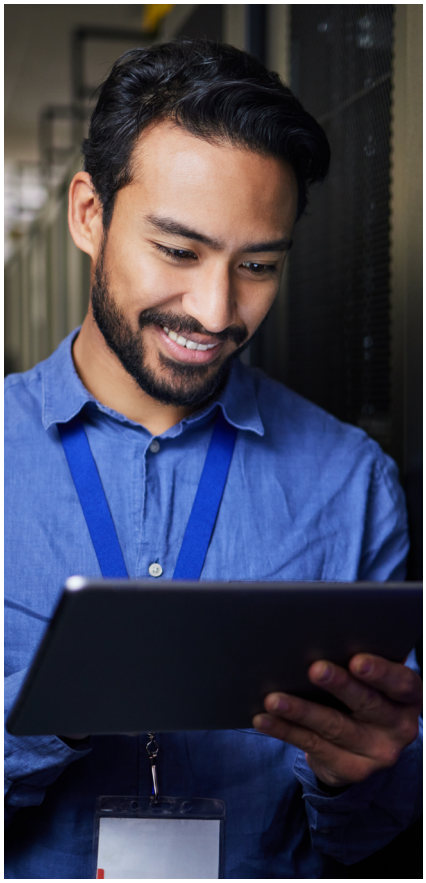
es.wikipedia.org/wiki/VLAN

en cualquier momento un ataque a través de una conexión de red desde el exterior y podrían visualizar todos los datos almacenados en nuestros equipos ya que no contamos con medidas en el resto de los niveles. En cualquier sistema informático, el nivel de seguridad del conjunto se define por el nivel de seguridad del punto más débil. Es importante por tanto tener en mente todas las capas y establecer controles en cada una de ellas, aplicando el principio de defensa en profundidad.

⚠ ATENCIÓN

En cualquier sistema informático, el nivel de seguridad del conjunto se define por el nivel de seguridad del punto más débil.

Formación en seguridad informática



Como se ha mencionado en el punto anterior, el nivel de seguridad de un sistema se define por el nivel de seguridad de su punto más débil. En este sentido, el punto más débil de cualquier sistema de información son las personas que los utilizan, los usuarios. No es suficiente con aplicar todas las medidas existentes en todos los niveles de seguridad si los usuarios no conocen las amenazas que pueden afectarles o no saben cómo actuar cuando están ante una.

Es fundamental que tanto los usuarios domésticos como los empleados de las empresas dispongan de ciertos conocimientos sobre ciberseguridad. Se sabe que la gran mayoría de los ataques que resultan exitosos no se debe a la falta de medidas o controles de seguridad, sino al desconocimiento por parte de los usuarios. Uno de los ejemplos más comunes en este sentido, y que más tasa de éxito tiene, es el phishing. Estos ataques se basan en el engaño al usuario, enviándole un mensaje haciéndose pasar por una tercera persona o entidad para que realice una acción específica. El usuario confía en el mensaje y sigue los pasos, lo que acaba en muchos casos en robos de datos, acceso a cuentas, etc.

A nivel personal, es interesante conocer las diferentes fuentes de información que existen en materia de seguridad para poder consultarlas y adquirir conocimiento en esta materia. Estos recursos disponen de información relevante, tanto para usuarios como para empresas, sobre las distintas amenazas que existen hoy en día y cómo podemos protegernos de ellas.

Además, a nivel corporativo, es interesante implementar programas de formación para todo el personal.

FUENTES DE INFORMACIÓN SOBRE SEGURIDAD

Documento referenciado: ***A4C41A1D02***

Auditorías de seguridad informática

Además de conocer las diferentes amenazas que nos pueden afectar, tanto en el ámbito personal como en el trabajo, y aplicar medidas para protegernos, también es importante conocer el nivel de seguridad del que disponen nuestros sistemas. Para ello se realizan auditorías de seguridad, que permiten conocer el estado de seguridad de un conjunto de sistemas de información.

Las auditorías de seguridad permiten comprobar que, efectivamente, las medidas de seguridad se están aplicando correctamente y cumplen su función. Estas auditorías sirven además para descubrir la existencia de vulnerabilidades que no habían sido identificadas previamente y que pueden suponer una potencial vía de entrada a ataques. Las auditorías son un punto clave para conocer el estado de seguridad de un sistema u organización.

Existen diferentes tipos de auditorías, pero en general podemos clasificarlas en auditorías internas o externas. Las auditorías internas son realizadas por personal de la organización sobre sus propios sistemas. Por otra parte, las auditorías externas son contratadas a una empresa externa. Es importante establecer las condiciones y el alcance de estas auditorías antes de su realización para evitar malentendidos o problemas imprevistos. Existen también auditorías que son certificables y que sirven para garantizar un cierto nivel de seguridad de cara a posibles clientes o proveedores.

Consecuencias de la no aplicación de los principios de la seguridad de la información

En la sociedad actual, tanto los ciudadanos en sus vidas privadas como las empresas y organizaciones públicas realizan sus tareas diarias utilizando sistemas de información. Hoy en día, la gran mayoría de negocios tiene una gran dependencia de los sistemas informáticos para llevar a cabo sus operaciones. De hecho, existe un alto valor para el negocio en todos los datos que son registrados, procesados y almacenados por las empresas.

Es fundamental, por tanto, adoptar los principios de la seguridad de la información que hemos visto para garantizar que no sufrimos ningún ataque que pueda interrumpir nuestras tareas diarias. En caso contrario, existen multitud de consecuencias negativas, tanto a nivel personal como para las empresas. Diariamente podemos ver multitud de noticias relacionadas con ataques y riesgos relacionados con la seguridad de la información. Algunos ejemplos de estas consecuencias en el entorno corporativo son:

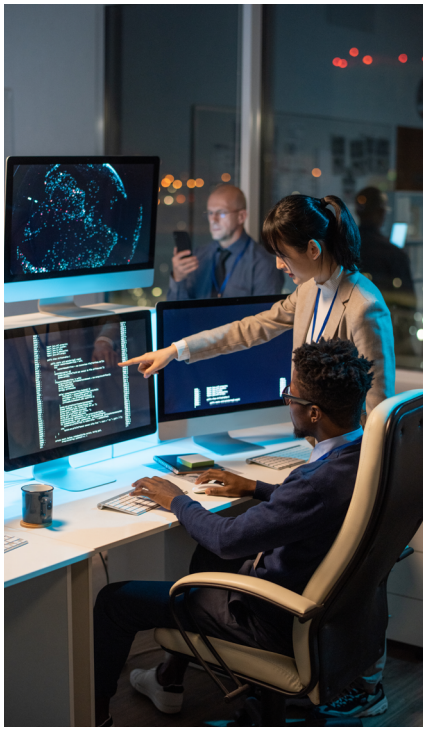
- **Pérdida de la credibilidad** y, por tanto, daños a la imagen y reputación de la organización.
- **Robo de datos** confidenciales de clientes, empleados, proveedores y socios comerciales.
- **Incumplimiento de las leyes** vigentes en la Unión Europea en materia de protección de datos personales.
- **Pérdida económica**, en el caso de que no sea posible recuperar la información extraída o eliminada de nuestros sistemas. Además, los atacantes pueden exigir el pago de una suma de dinero, utilizando un tipo de software malicioso denominado *ransomware*. Este tipo de programas suponen una de las principales amenazas existentes hoy en día.
- **Paralización de los procesos** de producción, pérdidas en ventas e impacto en la calidad del servicio.

Seguridad

Nivel A1 4.1 Protección de dispositivos

Fuentes de información sobre seguridad

Fuentes de información sobre seguridad



Para mantener un mayor nivel de seguridad y ser conscientes de los peligros a los que nos enfrentamos es necesario estar informados. Muchas veces nos enteramos de noticias sobre la ciberseguridad en la prensa o por redes sociales. En esta documentación se muestran varias fuentes fiables de información sobre ciberseguridad.

Organismos relevantes en ciberseguridad

Durante las últimas décazdas se han creado organismos especializados en ciberseguridad. Aunque existen empresas dedicadas a este ámbito, también es necesario contar con instituciones públicas que puedan dedicarse a la **vigilancia del ciberespacio**, a proporcionar **información al ciudadano, asesorar empresas** o incluso **proteger infraestructuras críticas**.

Conocer estos organismos nos permite acudir a ellos en necesidad de información o asesoramiento, al mismo tiempo que nos permite **aprender sobre nuevos conceptos** en ciberseguridad que nos pueden ser útiles como ciudadanos.

Ámbito estatal: organismos en España

En España contamos con diversos organismos, dedicados a diferentes funciones. Uno de los principales organismos es el **Centro Criptológico Nacional (CCN)** (*ccn-cert.cni.es*), dependiente del Centro Nacional de Inteligencia (CNI) español. La cara pública del CCN es su equipo de respuesta a incidentes y emergencias de ciberseguridad: el CCN-CERT. En su sitio web podemos encontrar mucha información relacionada con su labor: conseguir un ciberespacio más seguro y confiable, así como la protección de información clasificada y sensible.

Junto al CCN-CERT podemos encontrar otros organismos importantes como el **Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)** o el **Mando Conjunto del Ciberespacio (MCCE)** del Ministerio de Defensa. Por otro lado, el **Grupo de Delitos Telemáticos (GDT)** de la Guardia Civil o la **Brigada Central de Investigación Tecnológica (BCIT)** de la Policía Nacional son las unidades especiales de los cuerpos de seguridad estatal para investigar y perseguir a la delincuencia relacionada con la informática.

Existen otros organismos como la OSI o el INCIBE, que veremos a continuación en profundidad.

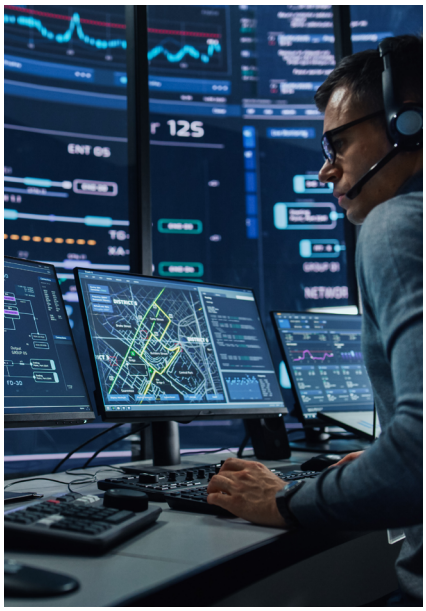
Ámbito comunitario: organismos en Europa

En los últimos años la Unión Europea ha impulsado una serie de reglamentos e iniciativas para mejorar el estado de la ciberseguridad comunitaria. En este sentido, la institución más relevante en el ámbito europeo es la **European Union Agency for Cybersecurity (ENISA)**. Esta organización vela por mantener un alto nivel de ciberseguridad común a todos los Estados Miembros de la Unión.

Además de la ENISA, existe un grupo de lucha contra el cibercrimen organizado, denominado el **European Cybercrime Centre (EC3)**. Este organismo, creado por la Europol, tiene como principal objetivo proteger a los ciudadanos, empresas y gobiernos de la Unión Europea del crimen online, fortaleciendo la respuesta ante este tipo de amenazas.

Ámbito internacional: organismos de otros países

A nivel internacional, cada estado dispone de diferentes instituciones y legislación en materia de ciberseguridad. En este contexto, una de las agencias más conocidas por su relevancia y capacidades operativas es la **National Security Agency (NSA)** de Estados Unidos. Esta agencia de inteligencia está especializada en la captación y procesamiento de información y en la inteligencia de señales. Otra de las agencias relacionadas es la **Cybersecurity & Infrastructure Security Agency (CISA)**, que cuenta con numerosos recursos en inglés en materia de ciberseguridad.



Saber más

Web del CCN-CERT: *ccn-cert.cni.es*
Web del CNPIC: *cnpic.interior.gob.es/opencms*
Web del MCCE: *e.digitall.org.es/emad*
Web del GDT: *gdt.guardiacivil.es/webgdt*
Web de la BCIT: *e.digitall.org.es/bcit*
Web del ENISA: *enisa.europa.eu*
Web del EC3: *e.digitall.org.es/EC3*
Web del NSA: *nsa.gov*
Web del CISA: *cisa.gov*

OSI: Oficina de Seguridad del Internauta

La **Oficina de Seguridad del Internauta (OSI)** forma parte del INCIBE y proporciona la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet. Su principal objetivo se centra en la concienciación y visualización de los problemas de ciberseguridad que pueden afectar al internauta. La información que nos brinda está enfocada principalmente hacia el ciudadano con conocimientos digitales básicos.

Su página web dispone de una amplia gama de recursos de información de todo tipo, herramientas, guías, etc. Algunos ejemplos de información útil para el ciudadano son:

- **Actualizaciones diarias:** la OSI proporciona información actualizada sobre noticias, avisos de ciberseguridad, artículos de blog, etc. Los ejemplos más ilustrativos de esta sección son las "Historias reales". En estos artículos podemos encontrar ejemplos reales de situaciones donde se describe un ataque o amenaza y las directrices que se deben seguir en caso de que nos suceda a nosotros. Por ejemplo, la OSI nos explica ***las amenazas de los deepfakes*** o también ***cómo actuar si han secuestrado nuestras cuentas*** (*incibe.es/ciudadania*).
- **Campañas:** este tipo de publicaciones se dividen en diferentes temáticas, como, por ejemplo: las contraseñas, los dispositivos móviles o el IoT. Dentro de cada uno de estos temas podemos encontrar una lista de recursos de la OSI relacionados con ese tema como, por ejemplo, infografías, vídeos, historias reales, etc. Un ejemplo de esto es la campaña "***Ingeniería social: que no te engañen***" (*incibe.es/ciudadania/tematicas*).
- **Manuales para aprender a protegernos:** la OSI publica diferentes manuales con recomendaciones de protección y con diferentes temáticas. Se centra en abordar problemáticas concretas, entenderlas y mostrar las medidas que debemos tomar para protegernos ante ellas. Algunas de las temáticas que se incluyen aquí son: ***cómo proteger tu red Wi-Fi*** o ***cómo cuidar tu privacidad*** (*incibe.es/ciudadania*).

Saber más

IoT son las siglas de **Internet of Things**, que en español significa Internet de las cosas. Se trata de un concepto que describe la red de objetos físicos que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet o de otras redes de comunicación.

e.digitall.org.es/iot

- **Recursos:** esta sección agrupa diferentes recursos, como son: talleres, guías, herramientas, servicios, etc.
- **Juegos educativos:** en su sitio web también podemos encontrar una serie de juegos que nos ayudan a comprender mejor los conceptos relacionados con la ciberseguridad como, por ejemplo, los ***juegos de mesa*** (*incibe.es/ciudadania*) que pueden descargarse directamente.

Cabe mencionar que, dentro de los recursos que nos ofrece la OSI, existe una iniciativa particular que se centra en la concienciación y protección de los más pequeños: **Internet Segura 4 Kids**. Esta iniciativa pretende formar tanto a menores de edad, como a sus profesores y familias, en materia de ciberseguridad.

Saber más

Web de la OSI: *osi.es*
Web de la Internet Segura 4 Kids: *is4k.es*

INCIBE: Instituto Nacional de Ciberseguridad

El **Instituto Nacional de Ciberseguridad (INCIBE)** es un organismo gubernamental dedicado completamente a la ciberseguridad, centrada en los ciudadanos, las empresas, las redes académicas o de investigación y otros sectores estratégicos.

Ya se ha mencionado la OSI, que está orientada a la ciudadanía en general. Para dotar también a las empresas de materiales útiles, el INCIBE cuenta con la iniciativa "Protege tu empresa". Con ella pretenden formar a las empresas, especialmente a las PYMES, y ofrecer recursos útiles como el ***kit de concienciación para entrenar a los empleados*** (*e.digitall.org.es/kit-incibe*). Además, el instituto tiene recursos orientados a fomentar el emprendimiento en el sector de la ciberseguridad, con iniciativas como INCIBE Emprende.

Saber más

Web del INCIBE: *incibe.es*
Iniciativa "Protege tu empresa": *incibe.es/protege-tu-empresa*
Iniciativa "INCIBE Emprende": *incibe.es/emprendimiento*

El INCIBE también cuenta con un sitio web interactivo para que los emprendedores y PYMES se introduzcan en conceptos relacionados con la ciberseguridad. Para ello, presentan a dos personajes animados que acompañan al espectador en su formación. Esta formación está adaptada a diferentes sectores empresariales o itinerarios.

ITINERARIOS DE CIBERSEGURIDAD INCIBE

itinerarios.incibe.es

UN PASO MÁS ALLÁ: GESTIÓN DE LA CIBERSEGURIDAD

La ciberseguridad se gestiona, tanto en las PYMES como en las grandes empresas. En este vídeo, se introducen conceptos como el impacto y el riesgo, que ayudan a gestionar las amenazas a una empresa.

e.digitall.org.es/A4C41A2V02

CCN-CERT

El **Centro Criptológico Nacional (CCN-CERT)** es una de las principales fuentes de información para mantenerse actualizados en materia de ciberseguridad y su legislación asociada en España. Este organismo es el encargado de desarrollar diferentes herramientas de ciberseguridad usadas por muchas empresas. Una de las más interesantes para la formación específica y técnica en ciberseguridad es ***Ángeles*** (***e.digitall.org.es/angeles***), una herramienta con multitud de recursos de diferentes niveles orientados a las empresas, como "ciberconsejos" o informes de buenas prácticas.

El CCN cuenta con numerosas guías técnicas e informes de seguridad periódicos, como el informe anual "Ciberamenazas y Tendencias", publicado a finales de cada año con un análisis del panorama de ciberseguridad nacional.

Saber más

Web sobre el Esquema Nacional de Ciberseguridad (ENS): *ens.ccn.cni.es/es*
Web Informes CCN-CERT públicos: *e.digitall.org.es/informes-cert*
Web de Guías del CCN-CERT: *e.digitall.org.es/guias-cert*

ENISA

La **European Union Agency for Cybersecurity (ENISA)** es un organismo europeo que proporciona multitud de recursos en inglés sobre ciberseguridad. Al igual que el CCN-CERT, esta agencia europea cuenta con informes periódicos como el "Cyber Europe", que se publica a finales de año con un resumen de las tendencias de ciberseguridad europeas.

Su sitio web (*enisa.europa.eu*) es muy útil para encontrar información organizada por temáticas.

DigitAll

Seguridad

4.2 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD

Seguridad

Nivel A1 4.2 Protección de los datos personales y la privacidad

Derechos de los ciudadanos en materia de protección de datos

Derechos de la ciudadanía en materia de protección de datos personales

El derecho a la información

Los derechos que recoge la Constitución Española se clasifican en distintas categorías según su relevancia. Los más importantes son los denominados Derechos Fundamentales. El derecho a la protección de los datos personales es un Derecho Fundamental. A partir de ahí, el legislador da contenido a ese derecho por distintas vías: impone deberes a los sujetos que tratan o manipulan datos personales, reconoce derechos más concretos a la ciudadanía o establece mandatos de actuación a los poderes públicos. Este documento desarrolla esos derechos de la ciudadanía en los que se desgaja el derecho a la protección de los datos personales.

LOS DERECHOS DE LA CIUDADANÍA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES (I)

e.digitall.org.es/A4C42A2V08

El primero de ellos es el derecho a la información. Sus manifestaciones son muy amplias y variadas (por ejemplo, el derecho de acceso que se trata un poco más adelante se puede considerar una concreción del derecho a la información).

Una de las manifestaciones para garantizar este derecho es la imposición al responsable del tratamiento del deber de facilitar determinada información al interesado. La normativa prevé que esa información se pueda facilitar por capas o niveles:

- Primera capa, una información básica.
- Segunda capa, una información detallada.

El contenido de la información varía según los datos personales se obtengan directamente del interesado (por ejemplo, se introducen datos al abrir una cuenta en Facebook o YouTube) o de un tercero (por ejemplo, una cadena hotelera cede ciertos datos personales a una agencia de viajes para la realización de una campaña de publicidad).

Información que debe facilitarse cuando los datos personales se obtengan del interesado

En la primera capa (información básica), la Agencia Española de Protección de Datos recomienda facilitar la siguiente información:

- La identidad del responsable del tratamiento.
- Una descripción sencilla de los fines del tratamiento, incluyendo la elaboración de perfiles si existiese.
- La base jurídica del tratamiento.
- Si se prevé que los datos puedan ser cedidos a terceros. Previsión o no de transferencias a terceros países.
- La posibilidad de ejercer los derechos que se exponen en este documento.
- Una dirección electrónica u otro medio (por ejemplo, la descarga de un documento pdf) que permita acceder de forma sencilla e inmediata a la restante información.

En la segunda capa (información detallada), se recomienda incluir la siguiente información:

- Datos de contacto del responsable. Identidad y datos del representante (si existiese). Datos de contacto del delegado de protección de datos (si existiese).
- Descripción ampliada de los fines del tratamiento. Plazos o criterios de conservación de los datos. Decisiones automatizadas, perfiles y lógica aplicada.
- Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. Obligación o no de facilitar datos y consecuencias de no hacerlo.
- Destinatarios o categorías de destinatarios. Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.
- Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de los datos, y la limitación u oposición a su tratamiento. Derecho a retirar el consentimiento prestado. Derecho a reclamar ante la Autoridad de Control.

⚠ ATENCIÓN

Cuando los datos personales se recogen directamente de los interesados, la información debe facilitarse con carácter previo a esa recogida.

Información que debe facilitarse cuando los datos personales no se obtengan del interesado

Cuando los datos personales no han sido obtenidos del interesado, **además de la información que se indica en el apartado anterior**, se debe facilitar la siguiente:

En la primera capa (básica):

- La fuente de los datos, esto es, su procedencia

En la segunda capa (detallada):

- La información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. Son fuentes de acceso público, por ej., los diarios y boletines oficiales, los medios de comunicación social, las páginas web, etc.
- La categoría de datos que se traten (por ejemplo, datos identificativos generales como el nombre o teléfono; o datos sensibles como el origen racial o las opiniones religiosas).

⚠ ATENCIÓN

Cuando los datos personales no se recaban del interesado, el responsable del tratamiento debe informarle de esa recogida en el plazo de un mes y, a más tardar, en la primera comunicación al interesado.

Saber más

Grupo de trabajo sobre protección de datos del artículo 29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 (WP 260). *e.digitall.org.es/articulo29*

El derecho de acceso

Consiste en el derecho del interesado a obtener del responsable del tratamiento confirmación de si se está tratando o no datos personales que le conciernen.

En ese caso, el responsable debe facilitar dos cosas:

- Una copia de esos datos o un sistema de acceso remoto, directo y seguro a ellos
- Una serie de información que coincide con la expuesta en la sección anterior (fines del tratamiento, categorías de datos personales, destinatarios, plazo de conservación, etc.)

⚠ ATENCIÓN

El ejercicio del derecho de acceso permite al interesado averiguar qué saben las empresas sobre él, esto es, qué datos personales tratan y controlar su licitud y exactitud.

Este derecho tiene una serie de limitaciones materiales y formales. En cuanto a los materiales, son dos:

- No debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual.
- Ciertos intereses públicos (seguridad del Estado; defensa; seguridad pública; ...).

En cuanto a la limitación formal, cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte, el responsable podrá solicitarle que especifique los datos o actividades de tratamiento a los que se refiere.

Saber más

Comité Europea de Protección de Datos. Directrices 1/2022 sobre el derecho de acceso. *e.digitall.org.es/directrices*

El derecho de rectificación

El derecho de rectificación tiene dos manifestaciones:

- Por un lado, obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. El interesado debe indicar a qué datos se refiere y la corrección que haya de realizarse.
- Por otro, teniendo en cuenta los fines del tratamiento, el derecho a que se completen los datos personales que sean incompletos. Supone que en aquellos casos en los que la información que aporte el interesado se adecúe a los fines del tratamiento y complete los datos que trata el responsable, éste vendrá obligado a admitirla y a incluirla en su tratamiento (por ej., piénsese en el tratamiento de datos sobre solvencia crediticia).

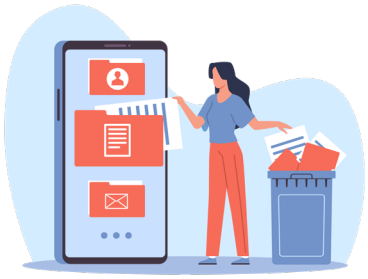
ATENCIÓN

El derecho de rectificación puede ejercitarse cuando se estén tratando datos inexactos o incompletos.

En el supuesto de que sea necesario, el interesado deberá acompañar a la solicitud la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

En cualquier caso, el responsable tiene el deber de garantizar la exactitud en los datos que trata, esto es, que es algo que debe hacer incluso de oficio sin solicitud alguna.

El derecho de supresión y el derecho al olvido



El derecho de supresión supone el derecho a obtener sin dilación indebida del responsable del tratamiento la eliminación de los datos personales que le conciernan. Puede ejercerse respecto de la totalidad de los datos que se tratan o sólo sobre alguno de ellos.

Esta supresión es obligatoria cuando concurran algunas de las siguientes circunstancias:

1 | Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados.
2 | El interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.
3 | El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para dicho tratamiento.
4 | Los datos personales hayan sido tratados ilícitamente.
5 | Los datos personales deban suprimirse para el cumplimiento de una obligación legal.
6 | Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información relativos a los niños.

⚠ ATENCIÓN

Cuando el responsable haya hecho públicos los datos personales y esté obligado a suprimirlos, adoptará las medidas razonables para informar a otros responsables que estén tratando esos datos personales para que también procedan a su supresión. Esto es el **derecho al olvido**.

Cuando el derecho de supresión se ejerce sobre datos que se hayan hecho públicos, se habla del derecho al olvido. Por tanto, el derecho al olvido sólo se exige frente al responsable que haya publicado los datos personales y no alcanza a los supuestos de mera comunicación de datos, esto es, cuando esos datos se hayan facilitado a personas o entidades singulares.

NOTA

El Tribunal Supremo ha declarado que no cabe ejercer el derecho de supresión frente a los datos del libro de bautismo.

NOTA

Desde 2014 hasta 2020, Google ha recibido peticiones para retirar más de 4 millones de enlaces. En España, el porcentaje de peticiones aceptadas ronda el 40 %.

En cualquier caso, el derecho de supresión no es absoluto y la normativa prevé una serie de supuestos en los que no procede, aunque con determinadas condiciones. Los más relevantes:

1 | Para ejercer el derecho a la libertad de expresión e información (piénsese, por ej., en las noticias publicadas en prensa digital).
2 | Para el cumplimiento de una obligación legal que requiera el tratamiento de datos y que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable (por ej., ciertos datos de investigaciones policiales o penales).
3 | Por razones de interés público en el ámbito de la salud pública.
4 | Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
5 | Para la formulación, el ejercicio o la defensa de reclamaciones.

Saber más

Comité Europeo de Protección de Datos. Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD. *e.digitall.org.es/directrices*

El derecho a la limitación del tratamiento

LOS DERECHOS DE LA CIUDADANÍA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES (II)

e.digitall.org.es/A4C42B1V08

Es el derecho a obtener del responsable el marcado de los datos personales conservados con el fin de limitar su tratamiento de manera provisional cuando proceda alguna de las siguientes circunstancias:

- El interesado impugne la exactitud de los datos, mientras el responsable la verifica.
- El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso. En este caso, lo que se pretende

fundamentalmente es evitar que se destruyan las pruebas acreditativas de la infracción cometida por el responsable.

- El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para el ejercicio o la defensa de reclamaciones.
- El interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos invocados por el responsable para continuar el tratamiento prevalecen sobre los del interesado.

Mientras dure esa limitación, los datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, por una serie de motivos tasados: consentimiento del interesado, formulación de reclamaciones, protección de los derechos de otra persona y razones de interés público.

Como acaba de exponerse, esta limitación se regula como un derecho del interesado y no como un deber del responsable del tratamiento. Esto es, el responsable del tratamiento no tiene el deber de proceder de oficio a la limitación del tratamiento cuando concurran algunas de las circunstancias expuestas, sino que para que ello ocurra el interesado habrá de ejercer expresamente este derecho.

⚠ ATENCIÓN

La limitación del tratamiento es de carácter provisional mientras concurren o se verifican determinadas circunstancias.

El derecho a la portabilidad de los datos

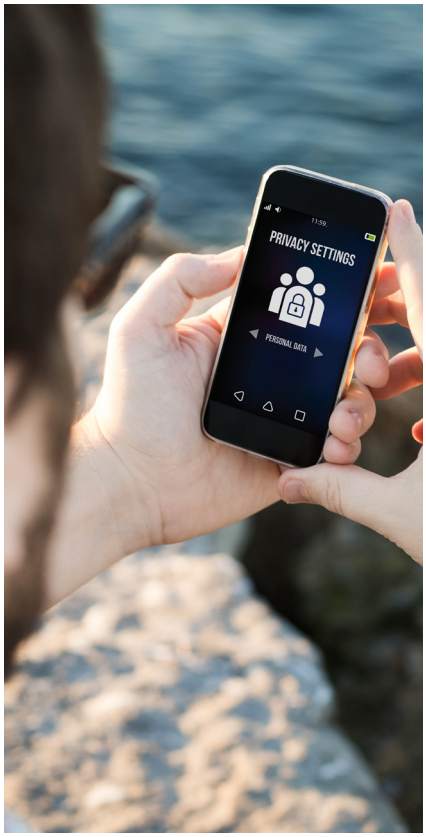
Consiste en el derecho del interesado a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.

Los datos sobre los que se puede ejercer este derecho son aquellos que el interesado haya facilitado. Estos no son solo aquellos que de manera consciente y activa entregó la persona interesada (por ejemplo, a través de un formulario), sino que también están incluidos en esta noción aquellos obtenidos a partir de la actividad del usuario en el uso de un servicio o de un dispositivo, para los que no se produce realmente una entrega activa de los mismos (por ejemplo, el historial de actividad física de un usuario registrado en una app de entrenamiento). Se excluyen los datos creados por el

responsable del tratamiento (por ejemplo, las puntuaciones o estadísticas que esa app genere a partir de esos datos).
Este derecho está sometido a dos condiciones:

1 | Que el tratamiento esté basado en el consentimiento o en un contrato. Si las causas de licitud del tratamiento son otras (por ejemplo, una obligación legal), los datos no podrán ser objeto de este derecho.

2 | Que el tratamiento se efectúe por medios automatizados.



Al ejercer este derecho, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. Por ejemplo, la portabilidad de los datos de los recibos domiciliados que una persona tiene en una entidad bancaria a otra entidad bancaria.

Son evidentes las implicaciones y dificultades de orden práctico y técnico que puede conllevar el ejercicio de este derecho. Piénsese, en la extensión de los datos de carácter personales, de todo tipo y en diferente formato, que se mueven por las diferentes redes sociales, blogs, servicios de *cloud computing*, de correo electrónico, etc. A todos estos servicios se les confía el almacenamiento y tratamiento masivo de datos de carácter personal. De lo que se trata es de establecer mecanismos jurídicos que impidan, bajo el argumento de dificultades técnicas, que los interesados quedan cautivos digitales de por vida de un concreto proveedor. Además, ello origina un efecto beneficioso para la promoción de la competencia.

Por estos motivos, es necesario elaborar un conjunto de normas y formatos comunes que sean interoperables a fin de responder a los requisitos del derecho a la portabilidad de datos. No obstante, es inmenso el camino que queda por recorrer.

En cuanto a la diferencia entre este derecho y el derecho de acceso, la portabilidad garantiza al interesado la obtención de una copia de la información susceptible de ser procesada fácilmente por otro sujeto, mientras que el acceso se limita a garantizar la información en sí misma. Esta diferencia tiene también consecuencias en cuanto a la forma de cumplir con la solicitud de ejercicio del derecho. En el derecho de acceso, los datos deben facilitarse al interesado en un formato de lectura accesible, que le permita conocer y entender la información.

En el derecho a la portabilidad, los datos se pueden facilitar en un formato incomprensible para el ser humano, pero sí para el tratamiento informatizado. También puede establecerse alguna diferencia entre ambos derechos en cuanto a su alcance. Por ejemplo, un sujeto tiene derecho de acceso a su historia clínica en un hospital privado. Eso incluye las pruebas médicas y el diagnóstico. Pero si el interesado solicita la portabilidad a otro hospital privado, se puede limitar a los resultados de las pruebas en bruto -los datos-, sin incluir los diagnósticos médicos -que es información generada por el responsable-.

ATENCIÓN

El derecho a la portabilidad implica que los datos personales de un usuario puedan transmitirse directamente de una entidad o empresa a otra, sin necesidad de ser entregados al propio usuario, siempre que ello sea técnicamente posible.

NOTA

La normativa bancaria permite la portabilidad de las cuentas, migrando de un banco a otro todos los servicios y datos personales, como las transferencias periódicas o las domiciliaciones.

Saber más

Grupo de Autoridades europeas de protección de datos. Directrices sobre el derecho a la portabilidad de datos (WP 242). *e.digitall.org.es/wp-242*

El derecho de oposición

El derecho de oposición atribuye al interesado la facultad para impedir el tratamiento de sus datos personales. Hay dos supuestos:

- Cuando el tratamiento tenga por objeto la mercadotecnia directa (publicidad) o la elaboración de perfiles relacionados con dicha mercadotecnia, el interesado podrá oponerse sin necesidad de justificación alguna y debe necesariamente aceptarse por el responsable.
- Cuando el tratamiento tenga como fundamento el interés público, el ejercicio de poderes públicos o el interés legítimo del responsable o de un tercero, deberá motivar esa oposición en función de su situación particular.

Por ejemplo, una Universidad pública, sobre la base de su misión realizada en interés público, impone a sus alumnos que enciendan las cámaras en la docencia *on line*. No obstante, un alumno, por su especiales circunstancias personales y familiares (sólo pudiera conectarse en lugares donde hay otros miembros de la familia), puede ejercer su derecho de oposición a este tratamiento.

En este segundo supuesto, el responsable puede seguir tratando los datos si acredita motivos legítimos que prevalezcan sobre los del interesado. Por ejemplo, posiblemente la Universidad podría imponer la medida anterior si fuera para verificar la identidad del alumno a la hora de efectuar un examen.

En cualquier caso, es necesario que el responsable responda al interesado expresando los motivos por los que rechaza su solicitud de oposición.

⚠ ATENCIÓN

El derecho de oposición no puede ejercerse ante muchos tratamientos de datos que realizan las Administraciones públicas (Hacienda, policía, Seguridad Social, etc.)

Saber más

Agencia Española de Protección de Datos. Conoce tus derechos.
e.digitall.org.es/conoce-tus-derechos

DigitAll

Seguridad

4.3 PROTECCIÓN DE LA SALUD Y EL BIENESTAR

Seguridad

Nivel A1 4.3 Protección de la salud y el bienestar

Principios de la salud digital

Principios de la salud digital

En el presente documento se aborda el concepto de salud digital, la e-salud y sus diferencias y similitudes. Aunque son conocidos los beneficios que pueda aportar la tecnología a la salud y el bienestar, se identifican las principales diferencias, a un nivel básico, entre los riesgos y amenazas relacionadas con la salud digital a nivel psicológico, físico y/o social.

Introducción al concepto de salud digital

En los temas relacionados con la salud y el mundo digital, existe poca evidencia acerca de los beneficios y daños que tienen las soluciones digitales sobre la salud y el bienestar de las personas. Sin embargo, en el presente documento intentaremos facilitar la identificación de las repercusiones que la tecnología pueda tener sobre nuestra salud.

La **salud digital** es un concepto creado para relacionar el impacto positivo o negativo que tienen las tecnologías de la información y las comunicaciones (TIC) (desde ordenadores portátiles, inteligencia artificial hasta dispositivos ponibles) sobre la salud y el bienestar de las personas. Según la Organización Mundial de la Salud (OMS), en el año 2012 se ha conceptualizado del término de salud digital, que incluye el uso de tecnología para mejorar la salud y otros campos relacionados con la misma. Según la OMS, la salud digital comprende desde los consumidores digitales hasta la robótica, considera dispositivos inteligentes y conectados y abarca diferentes usos de las tecnologías para la salud, como el internet de las cosas, el aprendizaje automático, la inteligencia artificial, la informática avanzada y el análisis de grandes volúmenes de datos.

> **NOTA**
>
> **Salud digital**: concepto que abarca el impacto que tiene el uso y empleo de las TIC sobre la salud y el bienestar.

La salud digital no sólo se caracteriza por aplicar diferentes herramientas tecnológicas en la salud, sino que también implica un cambio en la práctica sanitaria y asistencial. Por ello, su objetivo es promover y potenciar una mejor asistencia sanitaria mediante el uso de la tecnología. Así, podemos decir que este concepto ha supuesto la transformación digital de los sistemas de salud, provocando reformas a nivel legal, administrativo y financiero.

La digitalización de la salud nos permitirá prevenir enfermedades, e incluso detectarlas en fases tempranas, mantener una atención más efectiva y de calidad, reducir los costes de la atención sanitaria y hacer un seguimiento personalizado de la salud de las personas, ya sea por el médico de cabecera o por la propia autogestión de la salud.

Desde la Comisión Europea se espera que la salud digital promueva la participación de las personas en la gestión de su propia salud, haciendo énfasis en el estilo de vida y en la prevención y conectando los diferentes agentes y sectores del sistema de salud y la asistencia social para mejorar las situaciones de emergencia, las epidemias, los procedimientos y, sobre todo, para reducir las deficiencias de la atención sanitaria actual.

En esta línea, aproximadamente desde el año 1999, ha existido un término relacionado con la salud digital que ha generado confusión, usándose de manera errónea como sinónimo; hablamos del concepto de la e-salud o e-health.

La **e-salud** se define como una rama dentro de la salud digital. Abarca las TIC como herramientas empleadas en el entorno sanitario en materia de prevención, diagnóstico, tratamiento y seguimiento, así como en la gestión de la salud, ahorrando costes al sistema sanitario y mejorando la eficacia de este. La principal diferencia entre ambas es que las iniciativas de la e-salud no se originan desde el paciente, como ocurre en la salud digital. Además, las categorías dentro de la e-salud están más relacionadas con el tratamiento informático de datos sanitarios, incluyendo en el término herramientas como:

- El registro médico electrónico o historial de la clínica electrónica.
- La telesalud (incluida la telemedicina).
- El aprendizaje o formación digital a distancia, también conocido como e-Learning.
- La educación continua en tecnologías de la información y la comunicación.

Sin embargo, a pesar de todos los beneficios que nos pueda a aportar la tecnología, también puede tener un impacto negativo sobre la salud y el bienestar, ya sea de forma directa o indirecta sobre su uso diario.

⚠ ATENCIÓN

E-salud y salud digital no son sinónimos, sino que la primera es una rama dentro de la segunda.

Dentro de los diferentes riesgos y amenazas que puede provocar el uso de la tecnología, nos encontramos con los conceptos de adicción digital y ciberacoso. Sin embargo, también se tratarán otras amenazas digitales relacionados con la e-salud y el tratamiento de datos.

Amenazas digitales relacionadas con la e-salud

La rápida evolución de las TIC ha provocado una serie de cambios a los que hay que adaptar el sistema sanitario. Uno de ellos es la privacidad de las personas usuarias, ya que el tratamiento de esta información es un aspecto altamente sensible. Por ello, cada vez más, los gobiernos y entidades públicas relacionadas con la salud y la seguridad trabajan en un almacenamiento más seguro para los datos de la población. En esta línea, el uso de las nuevas tecnologías y el almacenamiento de los datos en la nube es una mejora de la salud digital, ya que permite y promueve la salud participativa en la ciudadanía mediante la visualización y la compartición de los datos de su salud, facilitando la atención y la gestión sanitaria.

Saber más

Las principales amenazas consideradas se enfocan en la adicción digital y el ciberacoso.

ATENCIÓN

La privacidad con respecto a los datos de salud de las personas usuarias es un tema altamente sensible y necesario de tratar.

La incorporación de tecnologías que interactúan con el medio físico y que pueden ser monitorizadas y controladas remotamente (parches "inteligentes" de insulina, marcapasos programables a través de redes inalámbricas, prótesis para compensar discapacidades físicas, etc.) han posicionado la salud y la afectación directa a la vida de las personas como un riesgo mucho más preocupante. Algunos ejemplos recientes, como el hackeo de marcapasos y bombas de insulina, así lo demuestran.

NOTA

Estos avances también suponen un reto para la seguridad, ya que estos sistemas deben de hacer frente a la lucha de hackeos o fugas que puedan provocar que información personal relacionada con el estado de salud de una persona sea pública. Por ello, a nivel nacional y europeo, se trabaja en leyes que protejan la información personal. Así la salud digital debe someterse al Reglamento Europeo de Protección de Datos y a la Ley de Protección de Datos y Garantía de Derechos Digitales, que afectan a los profesionales sanitarios, hospitales, clínicas, y centros médicos que manejan toda esta información. Esta normativa se relaciona con la confidencialidad de los datos médicos, mejorar la calidad de los datos, hacer uso del consentimiento del paciente en todo momento, mantener informado al paciente sobre su diagnóstico y tratamiento.

La complejidad del nuevo contexto tecnológico hace que el número de actores involucrados en el ciclo de vida de los nuevos procesos digitales sea tan extenso que algunos de ellos ni siquiera son conscientes de su influencia e interacción con estos procesos y, consecuentemente, no están incorporando los controles de seguridad suficientes en sus funciones ni en las tecnologías que proporcionan.

A las carencias existentes en las tecnologías del internet de las cosas hay que añadir que algunos de los nuevos servicios de teleasistencia o de monitorización remota de las personas contemplan el uso de los teléfonos móviles particulares de los consumidores/clientes como fuente de información (biometrías, geoposicionamiento, generación de alertas, etc.), sin calibrar adecuadamente el que no sean dispositivos de precisión especializados ni fiables.

Saber más

Las tecnologías englobadas en el internet de las cosas incluyen la teleasistencia o la monitorización remota de la salud de las personas.

Además, a la complejidad y carencias anteriores, hay que sumar las carencias existentes en los edificios desde los que se prestan estos servicios, bien sean fábricas donde se construye tecnología médica, farmacéuticas donde se producen medicamentos, centros de atención sanitaria o cualquier otro tipo de instalación relacionada con servicios de medicina y salud en general. Buena parte de esas instalaciones han incorporado tecnologías inteligentes conectadas a internet para optimizar sus recursos (calefacción, iluminación, control de accesos, ascensores, video vigilancia, mantenimiento preventivo, etc.) y esas tecnologías pueden tener, a su vez, vulnerabilidades que pueden ser explotadas remotamente. Vulnerabilidades que, además de afectar al funcionamiento del edificio, pueden facilitar el acceso a personas no autorizadas que incluso alteren los procesos que allí se desempeñan, llegando a impactar en la salud de los consumidores finales.

Riesgos y amenazas de la tecnología en la salud digital

Riesgos y amenazas a nivel físico

Un uso inadecuado de la tecnología puede afectar en gran medida a nuestra salud física. Esta afectación se debe, principalmente, a tiempos de uso excesivos o a mantener una postura inadecuada. Esta situación puede producirse tanto en entornos laborales como en nuestro hogar o en espacios de ocio. Algunos de los problemas que podemos sufrir son:

- **Daño en la vista:** la utilización de pantallas durante periodos muy largos de tiempo puede causar problemas en nuestros ojos como ardor, lagrimeo o enrojecimiento. Esto es debido, en gran parte, a la luz azul de los LED que forman la pantalla, cuya exposición afecta a la retina. También cabe destacar otro gran problema como es la fatiga ocular, que es ocasionada por una disminución en la frecuencia con la que parpadeamos. Así mismo, estos problemas relacionados con la vista pueden, a su vez, ocasionar dolor de cabeza.
- **Espalda y cervicales:** el uso prolongado de dispositivos tecnológicos provoca que los hombros estén habitualmente inclinados hacia delante y que las

NOTA

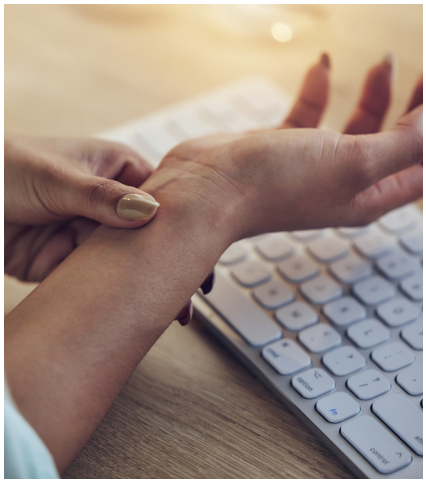
Además, las infraestructuras como los edificios no están preparados para los avances tecnológicos, ya sea por la conectividad ya sea por Wi-Fi, Bluetooth u otras alternativas.

ATENCIÓN

Un uso inadecuado de los dispositivos tecnológicos puede dar lugar a diferentes riesgos y amenazas a nivel físico, social y psicológico.

cervicales se mantengan en tensión durante largos periodos de tiempo, lo que provoca la aparición de contracturas.

- **Síndrome del túnel carpiano:** un uso prolongado del teclado y el ratón puede provocar este síndrome. Sucede cuando el nervio que va desde el antebrazo a la mano se comprime a su paso por el túnel carpiano, una zona de ligamentos que se encuentra bajo la palma de la mano. Dicha afección suele provocar adormecimiento, entumecimiento o pérdida de fuerza y movilidad en la muñeca afectada, entre otros.



Los problemas anteriores afectan directamente a diferentes partes de nuestro cuerpo, pero también debemos tener en cuenta que un abuso en el uso de la tecnología también puede derivar en un **estilo de vida sedentario**. Esto puede suponer un riesgo para nuestra salud a nivel general, siendo la causa de múltiples enfermedades como la **obesidad, problemas de corazón o el colesterol elevado**.

Riesgos y amenazas a nivel social

El empleo de las nuevas tecnologías a nivel social puede ser positivo siempre que no se dejen de lado las actividades de la vida cotidiana como estudiar, hacer deporte, salir con amigos y estar en familia, entre otros. Cuando su uso es desmedido y descontrolado, puede dar lugar a una serie de riesgos:

- **Aislamiento social:** la adicción a redes sociales, videojuegos o diversas aplicaciones puede generar que el usuario acabe aislándose del mundo; lo que le afectará en sus relaciones interpersonales con amigos, familiares, compañeros... En casos de adolescentes puede llegar a influir negativamente en el desarrollo de sus habilidades sociales. Por ejemplo, con la pérdida del contacto físico o la dificultad para apreciar emociones y gestos.
- **Falta de relación con el mundo real:** el uso desmesurado de las TIC puede llevar al individuo a abstraerse totalmente del mundo en el que vive, creando una desconexión total con su entorno. En muchos casos, la mayor parte de la realidad que perciben se correspondería con la realidad digital.

⚠ ATENCIÓN

Un uso desmedido de las nuevas tecnologías puede dar lugar a una serie de riesgos sociales como el aislamiento social o la falta de relación con el mundo real.

Riesgos y amenazas a nivel psicológico

La tecnología también presenta un gran impacto en la población a nivel psicológico. Los riesgos y trastornos psicológicos derivados de la tecnología son más comunes en la población adolescente. Entre los diferentes riesgos y amenazas destacan:

- **Nomofobia:** es un problema cada vez más habitual en la sociedad. Se define como el miedo irracional a estar sin el dispositivo móvil, ya que muchas personas presentan una dependencia total hacia su dispositivo. Esta situación puede provocar dolor de cabeza o estómago, ansiedad, estrés y, en casos más graves, puede provocar el desarrollo de trastornos mentales como trastornos obsesivos.
- **Síndrome de la llamada imaginaria:** este problema hace referencia a la sensación de que el teléfono está vibrando y sonando, aunque no sea así, provocando el impulso de tener que mirar el dispositivo. Este problema se debe a que el cerebro relaciona cualquier impulso que recibe con el móvil.
- **Dependencia de internet:** este tipo de dependencia viene provocada por el uso continuo que se le da a esta red informática por el contenido que nos aporta y que nos permite utilizar nuestro smartphone, las redes sociales, los chats, las páginas de contactos, etc. Esta dependencia puede provocar el desarrollo de problemas de ansiedad, estrés, alteraciones de conducta o aislamiento.
- **Problemas de inseguridad:** el uso frecuente de dispositivos móviles para hacer uso de redes sociales puede provocar que las personas comiencen a compararse con otras personas, o quieran aparentar una vida ideal a través de estas plataformas, pudiéndose exponer a críticas, así como la necesidad de obtener un feedback de las redes sociales como los “Me gusta”. Todos estos factores pueden provocar en las personas daños psicológicos como malestar que promuevan el desarrollo de ansiedad, depresión o trastornos alimenticios.

- **Tecnoestrés:** otro riesgo que puede provocar el uso de la tecnología en la población es el tecnoestrés. Este problema es la falta de habilidades para tratar con la tecnología de forma saludable. Esto puede provocar altos niveles de ansiedad y frustración en la persona y también el desarrollo de actitudes negativas hacia la tecnología. Algunas personas también pueden presentar cierto miedo a estos dispositivos, resistencia a hablar e incluso pensar en ella, y tener pensamientos hostiles y agresivos hacia el mundo de las TIC.

⚠ ATENCIÓN

La dependencia , la nomofobia o el síndrome de la llamada, son algunos de los riesgos psicológicos por el uso excesivo de la tecnología.

Los profesionales de la salud también refieren otros riesgos de la tecnología que pueden influir en la vida diaria de una persona, como son: problemas de sueño, necesidad de las TIC para sentirse conforme con uno mismo/a, falta de concentración, problemas de comunicación o aumento descontrolado del tiempo de uso.

Saber más

Principio Activa. Qué es la salud digital y la e-salud.
principioactiva.com

Salud Digital. Fundación Carlos Slim.
saluddigital.com

DigitAll

Seguridad

4.4
PROTECCIÓN DEL MEDIO AMBIENTE

Seguridad

Nivel A1 4.4 Protección del medio ambiente

Consumo sostenible de tecnología

Consumo sostenible de tecnología

Introducción: consumo de energía de la tecnología digital

El consumo de materiales y energía asociado a la fabricación y uso de dispositivos tecnológicos se encuentra en continuo crecimiento a nivel mundial, incrementado incluso después de la pandemia de la COVID-19.

Como vimos en el vídeo 2 de la serie ("***¿Necesitamos los recursos tecnológicos que fabricamos?***"), algunos datos son contundentes a la hora de ilustrar el fenómeno. Según los informes de *GSMA Intelligence*, plataforma que representa los intereses del sector de la telefonía móvil, desde el año 2017 ya hay más dispositivos móviles en uso que personas en el planeta. En ese momento, según GSMA, se estaba a punto de llegar a los 8.092 millones de conexiones móviles, mientras que el total de población en todo el mundo era de 7.373 millones (GSMA, 2017). En su nuevo informe añaden, además, los datos de personas que tienen al menos un dispositivo móvil y muestran que, a finales de 2021, 5.300 millones de personas estarán abonadas a servicios móviles, lo que representa el 67% de la población mundial (GSMA, 2022).

¿NECESITAMOS LOS RECURSOS TECNOLÓGICOS QUE FABRICAMOS?

e.digitall.org.es/A4C44A1V02

⚠ ATENCIÓN

Según los informes de *GSMA Intelligence*, plataforma que representa los intereses del sector de la telefonía móvil, desde el año 2017 ya hay más dispositivos móviles en uso que personas en el planeta.

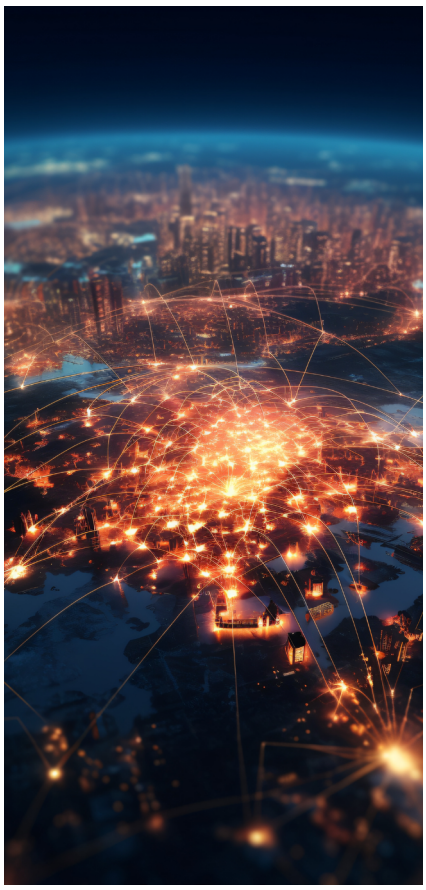
El mismo informe detalla cómo, con el 95% de la población mundial cubierta por una red de banda ancha móvil, el principal reto es abordar la brecha de uso, es decir, el 40% de la población mundial cubierta por una red de banda ancha móvil pero que aún no utiliza Internet. Por tanto, es más que probable que estos datos de uso de conexiones y dispositivos móviles se vayan incrementando a corto plazo.

Precisamente, este incremento de uso de internet también se puede representar con datos realmente llamativos. Según el Informe *Clicking Clean* de Greenpeace (2017), se calcula que la huella energética del sector de las tecnologías de la

información equivale ya a un consumo de aproximadamente el 7% de la electricidad mundial y sigue en aumento. Más allá de este dato, el mismo informe nos detalla cómo Internet genera cuatro áreas principales de demanda de energía: centros de datos, redes de comunicación, dispositivos de los usuarios y la energía para fabricar los equipos necesarios para los tres anteriores.

El consumo creciente de tecnología digital está impulsando la creación de la infraestructura necesaria, en concreto una gran cantidad de nuevos centros de datos que consumen mucha energía para servir como elementos indispensables de la nueva economía digital. En estos centros de datos se sitúan los servidores que sirven para almacenar nuestros mensajes, fotos y demás archivos que se intercambian entre dispositivos móviles y ordenadores. La tendencia es que estos centros vayan creciendo cada vez más en tamaño y recursos necesarios, pero hoy en día las instalaciones más grandes ya necesitan consumir tanta energía como una ciudad de tamaño mediano, principalmente para refrigerarse (Greenpeace, 2017:2).

La forma en que se construya y se alimente de energía la infraestructura digital global va a determinar cómo se pueden encarar algunos de los desafíos socioambientales más relevantes a los que se enfrentan las sociedades actuales, incluyendo la crisis climática. De hecho, si los centros de datos e infraestructuras digitales se alimentan con energías renovables, la creciente dependencia y necesidad de tecnología digital puede liderar y acelerar la transición hacia un modelo económico más sostenible y con menor huella de carbono.



Distintos informes de evaluación de la sostenibilidad de las infraestructuras digitales ponen el foco en la necesidad de que las grandes corporaciones en el sector de la tecnología digital apuesten decididamente por la generación de la energía necesaria para sus desarrollos a partir de fuentes renovables y que no emitan o minimicen sus emisiones de dióxido de carbono. De hecho, estamos viendo un aumento significativo en la priorización del uso de energías renovables entre algunas de las mayores empresas de internet. No solo por las necesidades vinculadas a la reducción de emisiones para combatir la crisis climática, sino por el horizonte de agotamiento de combustibles fósiles en el futuro.

En este mismo sentido, la descarbonización se ha instaurado como meta clave en la lucha contra el cambio climático, motivo por el que la Comisión Europea ha incluido el gas y la energía nuclear en la taxonomía verde, es decir, incluirá en la lista de actividades económicas medioambientalmente sostenibles.

Corporaciones líderes en el sector como Apple, Facebook y Google se comprometieron hace ya 10 años a una transición total a la generación 100% de origen renovable, y a lo largo de la última década se han sumado a ese compromiso más de 20 compañías del sector. Estas empresas están motivadas por distintas razones de peso, ya que sus propios clientes empiezan a estar preocupados por la sostenibilidad de la tecnología digital. Pero, además, las energías renovables empiezan a ser más rentables que ciertos combustibles fósiles para producciones a gran escala, especialmente en contratos a largo plazo, además de proporcionar más seguridad de suministro relacionada con aspectos geopolíticos.

Pero si bien es cierto que cada vez más empresas se están sumando a la apuesta por un consumo de energía 100% de origen renovable, hay que vigilar que las apuestas por un modelo transformador sean firmes, y no una simple fachada o método de *greenwashing* para las corporaciones. Por tanto, la actitud crítica de las personas consumidoras y asociaciones resulta imprescindible para vigilar el cumplimiento de esas apuestas.

Saber más

El término "greenwashing" se refiere al proceso de transmitir una falsa impresión o información engañosa sobre el grado de sostenibilidad o ecología de los productos o servicios de una empresa. Es una forma de marketing que busca aprovechar la creciente demanda de los consumidores por opciones más respetuosas con el medio ambiente.

es.wikipedia.org/wiki/Ecoblanqueo

Demanda de materiales para la tecnología digital

Además de la demanda de energía que hemos visto en el punto anterior, la industria de la tecnología digital también requiere una alta demanda de materiales para la producción de dispositivos y la construcción de infraestructuras. Por poner un ejemplo, se calcula que cada smartphone necesita de más de 60 componentes para su proceso de fabricación y entre ellos se encuentran materiales como aluminio, oro, cobre o cobalto que se extraen de la naturaleza en cantidades considerables desde hace décadas, pero también otros como litio o silicio cuya extracción se está multiplicando para cubrir las necesidades de la tecnología digital, como ya vimos en el video 3 del nivel "***Procesos de fabricación de recursos tecnológicos***".

PROCESOS DE FABRICACIÓN DE RECURSOS TECNOLÓGICOS

e.digitall.org.es/A4C44A1V03

Precisamente el litio es un material cada vez más demandado por ser el componente fundamental de la mayoría de las baterías. Básicamente, una batería está formada por dos o más celdas electroquímicas y dos electrodos para convertir energía química en energía eléctrica. En una batería de ion-litio, el electrodo positivo de la batería funciona principalmente con un compuesto de litio, mientras que el electrodo negativo de la batería emplea carbono en forma de grafito. Además, debe estar cubierta por una carcasa de aluminio en la que también se puede encontrar cobalto.

Por otro lado, componentes microelectrónicos y el cableado del teléfono están fabricados fundamentalmente con metales como el cobre, la plata y el oro que son muy buenos conductores de la electricidad, aunque se también se pueden encontrar platino, estaño, plomo y paladio. La electrónica de los dispositivos se fundamenta en chips de silicio puro, que se bombardean con elementos semiconductores como fósforo, antimonio, arsénico, boro, galio o indio para mejorar sus propiedades eléctricas.

Tanto para los condensadores de los dispositivos como para las lentes de las cámaras se necesita del tántalo, elemento presente en el coltán, que es una abreviatura comercial utilizada en partes de África para nombrar la "Columbita - Tantalita". El coltán es conocido responsable indirecto de los

conflictos bélicos que sufre la República Democrática del Congo, donde se hallan las mayores reservas mundiales, pero también se encuentra en China, Rusia u otros países africanos como Etiopía, Mozambique, Nigeria y Ruanda. El nivel de producción en estos países varía en función de los depósitos, pues muchos son de explotación artesanal. Un concentrado de tantalio puede contener de 10% a 40% Ta2O5, su valor comercial se calcula sobre el concentrado de óxido de tántalo.

Tanto el micrófono como el altavoz de un dispositivo digital están formados por imanes, que contienen aleaciones de neodimio, hierro y boro, además de disprosio y praseodimio. Estos dos últimos elementos pertenecen a las llamadas "tierras raras", 17 elementos de la tabla periódica, 15 de los cuales pertenecen a los lantánidos. Sus propiedades más destacables son de índole química, óptica y magnética, y resultan críticos para la transición energética y la tecnología digital. Además del disprosio y el praseodimio, el itrio, lantano, terbio, europio y el gadolinio se utilizan para las pantallas de dispositivos digitales; y el neodimio para la electrónica de los mismos.

Y, por último, las carcasas metálicas de nuestros dispositivos están compuestas por aleaciones de magnesio, además de poder encontrar níquel, que evitará las interferencias electromagnéticas, y compuestos de bromo que, debido a sus propiedades ignífugas, hacen que el dispositivo sea más resistente al calor.

Después de este repaso, podemos elaborar un **listado no exhaustivo de 30 elementos necesarios para la fabricación de dispositivos móviles** (a la derecha).

Al coste económico y energético que se requiere para la extracción de estos elementos químicos, hay que sumar el impacto ambiental de las actividades mineras. Además, todos estos recursos naturales son limitados, es decir, que se van agotando y los yacimientos que quedan disponibles cada vez son más difíciles de explotar. Se calcula que antes de 2050, ya podrían haberse agotado los principales materiales imprescindibles para la fabricación de tecnología digital, y esto será debido al aumento exponencial de su consumo a nivel mundial.

Asimismo, cada año se generan más de 46 millones de toneladas de residuos electrónicos por los smartphones,

1 | Cobre
2 | Plata
3 | Oro
4 | Platino
5 | Paladio
6 | Silicio
7 | Fósforo
8 | Antimonio
9 | Arsénico
10 | Estaño
11 | Plomo
12 | Aluminio
13 | Cobalto
14 | Boro
15 | Galio
16 | Indio
17 | Tántalo
18 | Neodimio
19 | Hierro
20 | Boro
21 | Disprosio
22 | Praseodimio
23 | Itrio
24 | Lantano
25 | Terbio
26 | Europio
27 | Gadolinio
28 | Magnesio
29 | Níquel
30 | Bromo

30 elementos necesarios para la fabricación de dispositivos móviles.

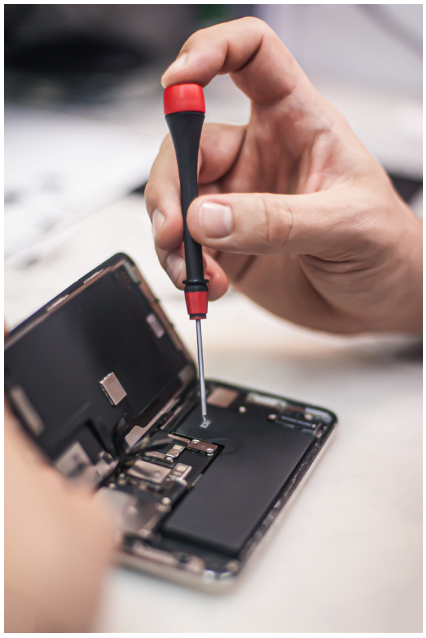
ordenadores, entre otros aparatos que se desechan y con ellos se pierde una enorme cantidad de minerales y materiales preciosos.

Hábitos de consumo sostenible de tecnología

Ante este panorama, se hace imprescindible plantear nuevos enfoques para optimizar la sostenibilidad de la producción y el consumo de tecnología digital. Como hemos visto en el video 4 de la serie, titulado "***Consumo sostenible de tecnología***", en primer lugar, debemos centrarnos en las 3 R clásicas de la sostenibilidad, es decir, Reducir nuestro consumo, tanto de dispositivos como de energía; Reutilizar dispositivos y componentes en la medida de lo posible; y, por último, Reciclar los materiales que se utilizan en la fabricación.

CONSUMO SOSTENIBLE DE TECNOLOGÍA
e.digitall.org.es/A4C44A1V04

En cuanto a la reutilización y el reciclaje, es necesario tener en cuenta que todos los dispositivos utilizados y desechados hasta la fecha, la llamada "basura electrónica" o residuos de aparatos eléctricos y electrónicos (RAEE), pueden ser una fuente indispensable de materiales cada vez más escasos, en la medida que se consigan reutilizar o reciclar. El reciclaje y la reutilización de la basura electrónica no sólo permite darle más "vidas" a un mismo recurso natural, sino que también supone un importante ahorro desde el punto de vista energético, ya que es mucho más rentable reacondicionar un material que extraerlo desde su fuente natural y transformarlo.



En cuanto a la reducción de nuestro consumo de dispositivos, no sólo es una cuestión de voluntad personal. Además de tener en cuenta las opciones de reutilizar o reacondicionar dispositivos disponibles antes de adquirir uno nuevo, también es necesario hacer incidencia política y reclamar a las administraciones competentes una mayor regulación a la hora de limitar las obsolescencias que operan sobre este tipo de dispositivos desde sus diseños y sus procesos de comercialización, tanto la obsolescencia programada, como las obsolescencias percibidas o de especulación.

De este modo, se debería favorecer el "derecho a reparar" los dispositivos digitales y electrónicos a partir de diseños que posibiliten su reparación y la adquisición de repuestos durante varios años. Ya existen ejemplos en este sentido, como el *Fairphone* o "teléfono justo", una iniciativa que prioriza la

extensión de la vida útil de los dispositivos a partir de un diseño modular que facilita las reparaciones fáciles; además de favorecer la reducción de residuos electrónicos a través de la reutilización y la reparación, sino también incrementando el uso de materiales reciclados en su fabricación. Por último, es una iniciativa que también garantiza que los materiales utilizados no provienen de zonas de conflicto y que las personas que trabajan en su fabricación lo hacen con unas condiciones justas.

En cuanto al consumo energético ligado a la tecnología digital, lo más sencillo es comenzar por hábitos y gestos cotidianos para reducir nuestra huella digital. Un informe de la *Agence de la transition écologique* francesa afirma que el 43% de las personas nunca apaga la caja de su televisión o el *router*. Son detalles que pueden marcar la diferencia a nivel global, como apagar los interruptores, no dejar la televisión, la impresora o la consola en *stand by*, no dejar el ordenador suspendido, así como colocar regletas con interruptor de apagado ya que, si el equipo está conectado directamente a la red, seguirá consumiendo.

La Comisión Europea, en su programa "La Década Digital de Europa: metas digitales para 2030," expone literalmente que "los dispositivos digitales deben favorecer la sostenibilidad y la transición ecológica, siendo imprescindible que los usuarios, no solo deben conocer el impacto medioambiental y el consumo de energía de sus dispositivos", sino que también "deben poder participar en el proceso democrático a todos los niveles y tener el control sobre sus propios datos".

Saber más

Agence de la transition écologique, (2022). Evaluation environnementale des équipements et infrastructures numériques en France. (Evaluación ambiental de los equipamientos e infraestructuras digitales en Francia). *e.digitall.org.es/evaluacion-ambiental*

Greenpeace (2017) "Clicking Clean". *e.digitall.org.es/clicking-clean*

National Geographic (2022). Tierras raras. *e.digitall.org.es/tierras-raras*

Observatorio Nacional de Tecnología y Sociedad (ONTSI), (2021) "Tendencias en el uso de dispositivos tecnológicos" *e.dgitall.org.es/ontsi*

Parlamento Europeo (2022). Derecho a reparar: el PE quiere productos más duraderos y fáciles de reparar. *e.digitall.org.es/derecho-reparar*

Comisión Europea (2021). La Década Digital de Europa: metas digitales para 2030. *e.digitall.org.es/metas-2030*

DigitAll

Formación en
Competencias
Digitales

https://www.digitall.org.es/

DigitAll

Coordinación General

Universidad de Castilla-La Mancha
Carlos González Morcillo
Francisco Parreño Torres

Coordinadores de área

Área 1. Búsqueda y gestión de información y datos

Universidad de Zaragoza
Francisco Javier Fabra Caro

Área 2. Comunicación y colaboración

Universidad de Sevilla
Francisco Javier Fabra Caro
Francisco de Asís Gómez Rodríguez
José Mariano González Romano
Juan Ramón Lacalle Remigio
Julio Cabero Almenara
María Ángeles Borrueco Rosa

Área 3. Creación de contenidos digitales

Universidad de Castilla-La Mancha
David Vallejo Fernández
Javier Alonso Albusac Jiménez
José Jesús Castro Sánchez

Área 4. Seguridad

Universidade da Coruña
Ana M. Peña Cabanas
José Antonio García Naya
Manuel García Torre

Área 5. Resolución de problemas

UNED
Jesús González Boticario

Coordinadores de nivel

Nivel A1

Universidad de Zaragoza
Ana Lucía Esteban Sánchez
Francisco Javier Fabra Caro

Nivel A2

Universidad de Córdoba
Juan Antonio Romero del Castillo
Sebastián Rubio García

Nivel B1

Universidad de Sevilla
Francisco de Asís Gómez Rodríguez
José Mariano González Romano
Juan Ramón Lacalle Remigio
Montserrat Argandoña Bertran

Nivel B2

Universidad de Castilla-La Mancha
María del Carmen Carrión Espinosa
Rafael Casado González
Víctor Manuel Ruiz Penichet

Nivel C1

UNED
Antonio Galisteo del Valle

Nivel C2

UNED
Antonio Galisteo del Valle

Maquetación

Universidad de Salamanca
Fernando De la Prieta Pintado
Pilar Vega Pérez
Sara Alejandra Labrador Martín

Creadores de contenido

Área 1. Búsqueda y gestión de información y datos

1.1 Navegar, buscar y filtrar datos, información y contenidos digitales

Universidad de Huelva
Ana Duarte Hueros (coord.)
Arantxa Vizcaíno Verdú
Carmen González Castillo
Dieter R. Fuentes Cancell
Elisabetta Brandi
José Antonio Alfonso Sánchez
José Ignacio Aguaded
Mónica Bonilla del Río
Odiel Estrada Molina
Tomás de J. Mateo Sanguino (coord.)

1.2 Evaluar datos, información y contenidos digitales

Universidad de Zaragoza
Ana Belén Martínez Martínez
Ana María López Torres
Francisco Javier Fabra Caro
José Antonio Simón Lázaro
Laura Bordonaba Plou
María Sol Arqued Ribes
Raquel Trillo Lado

1.3 Gestión de datos, información y contenidos digitales

Universidad de Zaragoza
Ana Belén Martínez Martínez
Francisco Javier Fabra Caro
Gregorio de Miguel Casado
Sergio Ilarri Artigas

Área 2. Comunicación y colaboración

2.1 Interactuar a través de tecnología digitales

Iseazy

2.2 Compartir a través de tecnologías digitales

Universidad de Sevilla
Alién García Hernández
Daniel Agüera García
Jonatan Castaño Muñoz
José Candón Mena
José Luis Guisado Lizar

2.3 Participación ciudadana a través de las tecnologías digitales

Universidad de Sevilla
Ana Mancera Rueda
Félix Biscarri Triviño
Francisco de Asís Gómez Rodríguez
Jorge Ruiz Morales
José Manuel Sánchez García
Juan Pablo Mora Gutiérrez
Manuel Ortigueira Sánchez
Raúl Gómez Bizcocho

2.4 Colaboración a través de las tecnologías digitales

Universidad de Sevilla
Belén Vega Márquez
David Vila Viñas
Francisco de Asís Gómez Rodríguez
Julio Barroso Osuna
María Puig Gutiérrez
Miguel Ángel Olivero González
Óscar Manuel Gallego Pérez
Paula Marcelo Martínez

2.5 Comportamiento en la red

Universidad de Sevilla
Ana Mancera Rueda
Eva Mateos Núñez
Juan Pablo Mora Gutiérrez
Óscar Manuel Gallego Pérez

2.6 Gestión de la identidad digital

Iseazy

Área 3. Creación de contenidos digitales

3.1 Desarrollo de contenidos

Universidad de Castilla-La Mancha
Carlos Alberto Castillo Sarmiento
Diego Cordero Contreras
Inmaculada Ballesteros Yáñez
José Ramón Rodríguez Rodríguez
Rubén Grande Muñoz

3.2 Integración y reelaboración de contenido digital

Universidad de Castilla-La Mancha
José Ángel Martín Baos
Julio Alberto López Gómez
Ricardo García Ródenas

3.3 Derechos de autor (copyright) y licencias de propiedad intelectual

Universidad de Castilla-La Mancha
Gabriela Raquel Gallicchio Platino
Gerardo Alain Marquet García

3.4 Programación

Universidad de Castilla-La Mancha
Carmen Lacave Rodero
David Vallejo Fernández
Javier Alonso Albusac Jiménez
Jesús Serrano Guerrero
Santiago Sánchez Sobrino
Vanesa Herrera Tirado

Área 4. Seguridad

4.1 Protección de dispositivos

Universidade da Coruña
Antonio Daniel López Rivas
José Manuel Vázquez Naya
Martiño Rivera Dourado
Rubén Pérez Jove

4.2 Protección de datos personales y privacidad

Universidad de Córdoba
Aida Gema de Haro García
Ezequiel Herruzo Gómez
Francisco José Madrid Cuevas
José Manuel Palomares Muñoz
Juan Antonio Romero del Castillo
Manuel Izquierdo Carrasco

4.3 Protección de la salud y del bienestar

Universidade da Coruña
Javier Pereira Loureiro
Laura Nieto Riveiro
Laura Rodríguez Gesto
Manuel Lagos Rodríguez
María Betania Groba González
María del Carmen Miranda Duro
Nereida María Canosa Domínguez
Patricia Concheiro Moscoso
Thais Pousada García

4.4 Protección medioambiental

Universidad de Córdoba
Alberto Membrillo del Pozo
Alicia Jurado López
Luis Sánchez Vázquez
María Victoria Gil Cerezo

Área 5. Resolución de problemas

5.1 Resolución de problemas técnicos

Iseazy

5.2 Identificación de necesidades y respuestas tecnológicas

Iseazy

5.3 Uso creativo de la tecnología digital

Iseazy

5.4 Identificar lagunas en las competencias digitales

Iseazy

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia