DigitAll

Formació en
Competències
Digitals

# 4

# Seguretat

DigitAll

Formació en
Competències
Digitals

Seguretat

# Nivell A1

# ÍNDEX

DigitAll

Seguretat

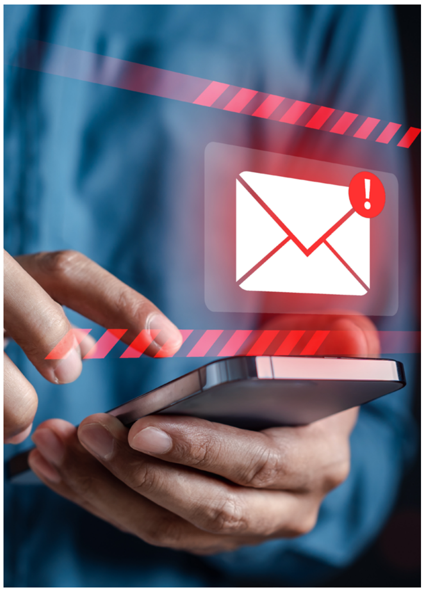
# 4.1
# PROTECCIÓ DE DISPOSITIUS

Seguretat

Nivell A1 4.1 Protecció de dispositius

# Principis de la seguretat de la informació

# Principis de la seguretat de la informació



La seguretat de la informació a la societat actual juga un paper fonamental. Tots fem servir diàriament sistemes informàtics per gestionar la nostra informació, ja sigui personalment, com en una empresa o en l'administració pública. Aquesta migració de les nostres dades a format digital comporta una sèrie de riscos que hem de conèixer i controlar per no patir cap atac que els comprometi. En aquest tema definirem el concepte de seguretat de la informació, presentarem una sèrie de termes relacionats i exposarem una sèrie de principis que hem de seguir per protegir les nostres dades digitals.

## Seguretat de la informació

Dins del món de la informàtica hi ha multitud de termes relacionats amb la protecció dels sistemes o de la informació que aquests gestionen. El primer és la seguretat de la informació. Per entendre aquest concepte, primer hem de definir què vol dir exactament informació. La **informació** és "tot coneixement que pot ser comunicat, presentat o emmagatzemat de qualsevol manera" (*CCN-STIC-431:2006*). En aquest sentit, la informació es pot trobar habitualment en forma de missatges, correus electrònics, bases de dades, etc.

La **seguretat de la informació,** doncs, es defineix com la preservació de la confidencialitat, la integritat i la disponibilitat d'aquesta informació (*UNE-ISO/IEC 27000:2014*). Aquests tres conceptes formen les tres dimensions de la seguretat de la informació, anomenat conjuntament com a tríada CIA (de l'anglès, *Confidentiality, Integrity and Availability*). A continuació, es defineixen breument:

1 | **Confidencialitat:** garantir que la informació és secreta, i només les persones autoritzades poden accedir-hi i visualitzar-la.

2 | **Integritat:** assegurar que la informació no es modifica sense permís.

3 | **Disponibilitat:** capacitat de la informació de ser accessible i estar llesta per al seu ús quan és demanada.

**LA TRÍADA CIA: CONFIDENCIALITAT, INTEGRITAT I DISPONIBILITAT**

*S'introdueix el concepte de tríada CIA: confidencialitat, integritat i disponibilitat. S'expliquen cadascuna de les parts que componen aquest concepte amb exemples senzills, però reals, i s'emfasitza la importància d'aquest concepte dins la seguretat de la informació.*

e.digitall.org.es/A4C41A1V02

Les tres dimensions de la seguretat de la tríada CIA es defineixen com a "serveis de seguretat" dins de la *norma ISO-7498-2*. A més de la confidencialitat, la integritat i la disponibilitat, hi ha altres serveis de seguretat inclosos en aquesta norma:

1 | **Autenticació:** s'ha de garantir que algú és qui diu que és, sigui durant una comunicació o com a autor d'una informació.

2 | **No repudi:** cal evitar que l'emissor o el receptor neguin la transmissió o la recepció d'un missatge, respectivament.

3 | **Control d'accés:** heu d'evitar l'accés no autoritzat a un recurs.

A l'hora de pensar en diferents mesures de protecció de la seguretat de la informació, cal tenir en compte tots els serveis de seguretat anteriors. Per comprendre cadascun dels punts veurem l'exemple de l'aplicació que utilitzem a la nostra banca electrònica.

Quan accedim a la banca electrònica del nostre banc a través d'un navegador web, el primer que podem veure és informació pública dels serveis que ofereix. Si per qualsevol error la pàgina no estigués accessible, la informació no estaria **disponible** per consultar. Si volem accedir a la nostra informació privada, com els nostres comptes bancaris i els moviments, ens cal identificar-nos. Per fer-ho realitzem el procés d'**autenticació**, indicant el nostre nom d'usuari i contrasenya. Per descomptat, si aquestes dades no són correctes, no podrem accedir a la nostra informació, ja que hi ha un control d'accés. Un cop ens autenticam, podem veure les nostres dades. Aquesta informació s'envia xifrada des dels servidors del banc fins al nostre ordinador; per tant, és **confidencial**. A més, també s'apliquen mecanismes de control d'**integritat** per garantir que la informació que estem visualitzant és la correcta. Finalment, una vegada autenticats, si fem un moviment bancari utilitzant el nostre compte, el banc garanteix el **no repudi** de l'ordre.

### Seguretat informàtica

A més de la seguretat de la informació hi ha altres conceptes similars que se solen utilitzar indistintament, però que tenen certs matisos. Un és el de **seguretat informàtica**, que fa referència als aspectes tecnològics de la seguretat que incideixen directament en els mitjans informàtics on la informació és processada, emmagatzemada, distribuïda, etc. Un exemple específic d'aquest punt és utilitzar xifrat per protegir les dades mentre estan emmagatzemades o en trànsit.

Per contra, la seguretat de la informació és un terme més ampli, que engloba la seguretat informàtica, i que inclou aspectes sistèmics de la seguretat, com ara les polítiques o els procediments. Alguns exemples de mesura que s'inclou dins de la seguretat de la informació, però no en seguretat informàtica, són l'aplicació de polítiques de gestió de riscos o l'adequació de la seguretat a la regulació vigent.

**ATENCIÓ**

Tot i ser termes molt similars, la **seguretat de la informació** i la **seguretat informàtica** no són el mateix. La seguretat de la informació és un terme molt més ampli, que engloba la seguretat informàtica.

## Principis de la seguretat de la informació

Per garantir un bon nivell de la seguretat de la informació hi ha una sèrie de principis fonamentals que hem de seguir. Aquests principis ens donen unes idees bàsiques que poden ser aplicables a múltiples escenaris. Si s'aplica correctament, podem assegurar que disposarem d'un nivell de seguretat acceptable en els nostres sistemes.

## Política de mínims privilegis

Seguir una política de privilegis mínims és una bona manera d'enfocar la divisió dels permisos a l'hora de poder accedir i processar la informació. En aquest sentit, els privilegis fan referència als determinats permisos que té un usuari per fer una acció específica sobre una informació concreta. Per tant, el principi de mínim privilegi ens planteja que hem de configurar els permisos de la informació de manera que se'ls permeti realitzar les accions únicament necessàries a cada usuari per garantir les seves activitats diàries. El que es pretén evitar és que un usuari o grup d'usuaris disposin de més privilegis dels necessaris, cosa que podria comprometre la seguretat del sistema.

Vegem-ne un exemple. Hem d'imaginar que diversos usuaris d'una mateixa organització utilitzen el mateix ordinador per emmagatzemar certa informació personal, com ara les nòmines. En aquest escenari, cap usuari no hauria de poder consultar la nòmina d'un altre usuari que no sigui ell mateix. Una possible configuració d'aquest escenari podria ser crear una carpeta per a cada usuari i configurar els permisos de manera que cada usuari tingui accés únicament a la carpeta personal. En aquest cas acomplim el principi de mínim privilegi, ja que concedim els permisos únics necessaris a cada usuari per fer les seves tasques sense problema. Per contra, si no configuréssim els permisos correctament, tindríem un escenari on tots els usuaris disposarien de permisos sobre totes les carpetes. En aquest sentit, qualsevol usuari malintencionat o que hagi patit un atac, i el compte del qual hagi estat compromès, suposaria un potencial problema de seguretat sobre la informació del sistema.

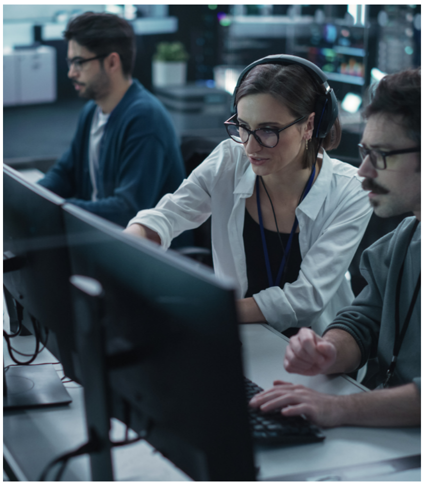
## Política de control d'accés tancat per defecte

Estretament relacionat amb el principi anterior hi ha el principi de control d'accés tancat per defecte. La idea darrere aquest principi és configurar els permisos dels usuaris sobre la informació de manera restrictiva per defecte, per la qual cosa ningú pot tenir accés llevat que s'indiqui específicament. Establir una política de control d'accés tancat per defecte pretén evitar l'accés indegut a certa informació de manera involuntària i desapercebuda.

Aquesta política es pot entendre fàcilment si parlam dels tallafocs. Els tallafocs són dispositius que controlen les connexions de la xarxa. En general, és una bona política configurar un tallafoc de manera que no permeti cap connexió de xarxa per defecte i afegir específicament les que necessitam. Això passa, per exemple, amb el tallafoc que ve configurat per defecte al sistema operatiu Windows. Aquest tallafoc no permet que algú extern estableixi una connexió de cap tipus amb el nostre ordinador, tret que hagi estat prèviament iniciada pel mateix equip.

## Segregació de funcions

En una organització és important que les funcions estiguin repartides entre els seus membres. Dins d'una empresa existeixen, normalment, diferents departaments que s'encarreguen de diverses tasques, com ara el departament de recursos humans, el de màrqueting, o el de Tecnologies de la Informació (TI). A l'hora d'utilitzar els sistemes informàtics i gestionar la informació de l'organització caldria definir i implementar una sèrie de separacions de les funcions i responsabilitats de cada personal. Això evita els conflictes d'interès i l'acumulació de privilegis en una única persona, cosa que pot comportar certs problemes de seguretat.



Un exemple clar el podem veure en les funcions i les tasques que haurien de realitzar el personal de cadascun dels departaments d'una empresa. No tindria sentit que el personal del departament de finances pogués fer configuracions als dispositius de xarxa d'una empresa, o que un empleat del departament de màrqueting tingués accés a les nòmines de tots els empleats de l'empresa. En realitzar una segregació de funcions entre els diferents empleats, assegurem que els privilegis dels usuaris estiguin controlats i acotats a les funcions diàries.

## Defensa en profunditat

Aquest principi fa referència a les mesures de seguretat de la informació existents i al lloc d'aplicació. Avui dia, a causa de la gran quantitat i diversitat d'amenaces a què estam exposats, no n'hi ha prou amb aplicar una única mesura de seguretat en un punt concret de l'organització. És important implementar diferents nivells de seguretat als nostres sistemes i a la informació que aquests gestionen.

Hi ha diferents mesures o controls que poden ser aplicats a cada nivell de seguretat. A continuació, es mostra un exemple per a cadascun d'aquests nivells:

- **Polítiques, procediments i conscienciació:** disposar d'una política de gestió de contrasenyes als equips de l'empresa, de manera que l'usuari l'hagi de renovar cada cert temps i que compleixi amb un mínim de caràcters.
- **Seguretat física:** disposar d'un armari de comunicacions, on es trobin els dispositius de xarxa, que estigui tancat amb clau.
- **Perímetre:** instal·lar i configurar un tallafoc per controlar les connexions entrants i sortints de l'empresa.
- **Xarxa interna:** fer una separació lògica de les xarxes internes de l'organització utilitzant xarxes VLAN (Virtual Local Area Network).
- ***Host*:** protecció davant de programari maliciós instal·lant sistemes antivirus.
- **Aplicació:** implementar un sistema d'identitats en el marc corporatiu.
- **Dades:** xifrar la informació emmagatzemada als equips.

L'aplicació d'una o més mesures en un dels nivells no ens garanteix que estiguem completament segurs. Es podria donar el cas en què disposéssim d'un alt nivell de seguretat física a l'organització, tenint un guàrdia de seguretat, controlant els accessos a l'edifici, protegint els dispositius de xarxa en un armari de comunicacions tancat amb clau... però que no apliquem cap altre control a la resta dels nivells de seguretat. Podríem patir en qualsevol moment un atac a través d'una connexió de xarxa des de l'exterior i podrien visualitzar totes


Nivells de seguretat
(la imatge va ser creada per l'editor)

**Saber-ne més**

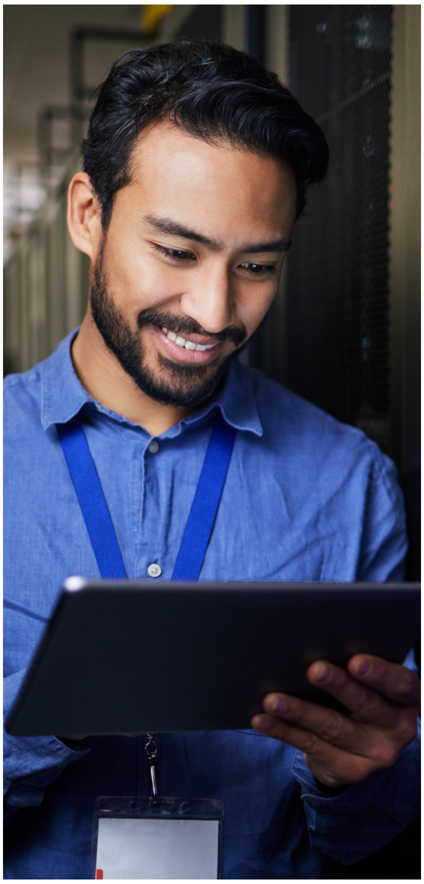
Una VLAN és una xarxa lògica que agrupa un conjunt de dispositius que comparteixen una mateixa xarxa física, aïllant el trànsit de cada conjunt.

[es.wikipedia.org/wiki/VLAN](es.wikipedia.org/wiki/VLAN) les dades emmagatzemades als nostres equips, ja que no tenim mesures a la resta dels nivells. A qualsevol sistema informàtic, el nivell de seguretat del conjunt es defineix pel nivell de seguretat del punt més feble. És important, per tant, tenir present totes les capes i establir controls en cadascuna, aplicant el principi de defensa en profunditat.

**ATENCIÓ**

A qualsevol sistema informàtic, el nivell de seguretat del conjunt es defineix pel nivell de seguretat del punt més feble.

### Formació en seguretat informàtica



Com s'ha esmentat al punt anterior, el nivell de seguretat d'un sistema es defineix pel nivell de seguretat del punt més feble. En aquest sentit, el punt més feble de qualsevol sistema d'informació són les persones que els utilitzen, els usuaris. No n'hi ha prou amb aplicar totes les mesures existents en tots els nivells de seguretat si els usuaris no coneixen les amenaces que els poden afectar o no saben com actuar quan n'estan davant una.

És fonamental que tant els usuaris domèstics com els empleats de les empreses disposin de certs coneixements sobre ciberseguretat. Se sap que la gran majoria dels atacs que resulten reeixits no es deu a la manca de mesures o controls de seguretat, sinó al desconeixement per part dels usuaris. Un dels exemples més comuns en aquest sentit, i que té més taxa d'èxit, és la pesca. Aquests atacs es basen en l'engany a l'usuari, li envien un missatge fent-se passar per una tercera persona o entitat perquè faci una acció específica. L'usuari confia en el missatge i segueix els passos, cosa que acaba en molts casos en robatoris de dades, accés a comptes, etc.

A escala personal, és interessant conèixer les diferents fonts d'informació que hi ha en matèria de seguretat per poder-les consultar i adquirir coneixement en aquesta matèria. Aquests recursos disposen d'informació rellevant, tant per a usuaris com per a empreses, sobre les diferents amenaces que hi ha avui dia i com ens podem protegir.

**FUENTES DE INFORMACIÓN SOBRE SEGURIDAD**

*Documento referenciado:* ***A4C41A1D02***

## Auditories de seguretat informàtica

A més de conèixer les diferents amenaces que ens poden afectar, tant a personalment com a la feina, i aplicar mesures per protegir-nos, també és important conèixer el nivell de seguretat de què disposen els nostres sistemes. Per fer-ho, es fan auditories de seguretat, que permeten conèixer l'estat de seguretat d'un conjunt de sistemes d'informació.

Les auditories de seguretat permeten comprovar que, efectivament, les mesures de seguretat s'apliquen correctament i en compleixen la funció. Aquestes auditories serveixen, a més a més, per descobrir l'existència de vulnerabilitats que no havien estat identificades prèviament i que poden suposar una via potencial d'entrada a atacs. Les auditories són un punt clau per conèixer l'estat de seguretat d'un sistema o organització.

Hi ha diferents tipus d'auditories, però en general les podem classificar en auditories internes o externes. Les auditories internes les fan personal de l'organització sobre els seus sistemes. Per altra banda, les auditories externes són contractades a una empresa externa. És important establir les condicions i l'abast d'aquestes auditories abans de fer-les per evitar malentesos o problemes imprevistos. Hi ha també auditories que són certificables i que serveixen per garantir un cert nivell de seguretat de cara a possibles clients o proveïdors.

## Conseqüències de la no aplicació dels principis de la seguretat de la informació

A la societat actual, tant els ciutadans a les seves vides privades com les empreses i organitzacions públiques fan les seves tasques diàries utilitzant sistemes d'informació. Avui dia, la gran majoria dels negocis tenen una gran dependència dels sistemes informàtics per dur a terme les seves operacions. De fet, hi ha un alt valor per al negoci en totes les dades que són registrades, processades i emmagatzemades per les empreses.

És fonamental, doncs, adoptar els principis de la seguretat de la informació que hem vist per garantir que no patim cap atac que pugui interrompre les nostres tasques diàries. En cas contrari, hi ha multitud de conseqüències negatives, tant a personalment com per a les empreses. Diàriament, hi podem veure multitud de notícies relacionades amb atacs i riscos relacionats amb la seguretat de la informació. Alguns exemples d'aquestes conseqüències a l'entorn corporatiu són:

- **Pèrdua de la credibilitat** i, per tant, danys a la imatge i la reputació de l'organització.
- **Robatori de dades** confidencials de clients, empleats, proveïdors i socis comercials.
- **Incompliment de les lleis** vigents a la Unió Europea en matèria de protecció de dades personals.
- **Pèrdua econòmica,** en cas que no sigui possible recuperar la informació extreta o eliminada dels nostres sistemes. A més, els atacants poden exigir el pagament d'una suma de diners, utilitzant un tipus de programari maliciós anomenat programari de segrest (ransomware). Aquest tipus de programes suposen una de les principals amenaces existents avui dia.
- **Paralització dels processos de producció,** pèrdues en vendes i impacte en la qualitat del servei.

Seguretat

Nivell A1 4.1 Protecció de dispositius

# Fonts d’informació sobre seguretat

# Fonts d'informació sobre seguretat

Per mantenir més nivell de seguretat i ser conscients dels perills que podem tenir, cal estar informats. Moltes vegades ens assabentem de notícies sobre la ciberseguretat a la premsa o per xarxes socials. Aquesta documentació mostra diverses fonts fiables d'informació sobre ciberseguretat.

## Organismes rellevants en ciberseguretat

Durant les darreres dècades s'han creat organismes especialitzats en ciberseguretat. Encara que hi ha empreses dedicades a aquest àmbit, també cal comptar amb institucions públiques que puguin dedicar-se a la **vigilància del ciberespai**, a proporcionar **informació al ciutadà**, **assessorar empreses** i, fins i tot, **protegir infraestructures crítiques**.

Conèixer aquests organismes ens permet acudir-hi en necessitat d'informació o assessorament, alhora que ens permet **aprendre sobre nous conceptes en ciberseguretat** que ens poden ser útils com a ciutadans.

### Àmbit estatal: organismes a Espanya

A Espanya es disposa de diversos organismes, dedicats a diferents funcions. Un dels principals organismes és el **Centre Criptològic Nacional (CCN)** (*ccn-cert.cni.es*), dependent del Centre Nacional d'Intel·ligència (CNI) espanyol. La cara pública del CCN és el seu equip de resposta a incidents i emergències de ciberseguretat: el CCN-CERT. Al lloc web podem trobar molta informació relacionada amb la seva tasca: aconseguir un ciberespai més segur i fiable, així com la protecció d'informació classificada i sensible.

Al costat del CCN-CERT podem trobar altres organismes importants com el **Centre Nacional de Protecció d'Infraestructures i Ciberseguretat (CNPIC)** i el **Comandament Conjunt del Ciberespai (MCCE)** del Ministeri de Defensa. D'altra banda, el **Grup de Delictes Telemàtics (GDT)** de la **Guàrdia Civil o la Brigada Central de Recerca Tecnològica (BCIT)** de la Policia Nacional són les unitats especials dels cossos de seguretat estatal per investigar i perseguir la delinqüència relacionada amb la informàtica.

Hi ha altres organismes com l'OSI o l'INCIBE, que veurem a continuació en profunditat.

### Àmbit comunitari: organismes a Europa

En els darrers anys la Unió Europea ha impulsat una sèrie de reglaments i iniciatives per millorar l'estat de la ciberseguretat comunitària. En aquest sentit, la institució més rellevant a escala europea és l'***European Union Agency for Cybersecurity (ENISA)***. Aquesta organització vetlla per mantenir un alt nivell de ciberseguretat comú a tots els estats membres de la Unió.

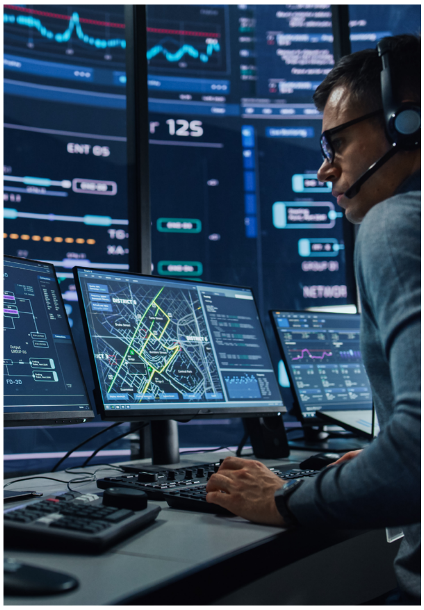
A més de l'ENISA, hi ha un grup de lluita contra el cibercrim organitzat, anomenat l'***European Cybercrime Centre (EC3)***. Aquest organisme, creat per l'Europol, té com a principal objectiu protegir els ciutadans, les empreses i els governs de la Unió Europea del crim en línia, enfortint la resposta davant aquest tipus d'amenaces.

### Àmbit internacional: organismes d'altres països

A escala internacional, cada estat disposa de diferents institucions i legislació en matèria de ciberseguretat. En aquest context, una de les agències més conegudes per la seva rellevància i capacitats operatives és la ***National Security Agency (NSA)*** dels Estats Units. Aquesta agència d'intel·ligència està especialitzada en la captació i el processament d'informació i en la intel·ligència de senyals. Una altra de les agències relacionades és la ***Cybersecurity & Infrastructure Security Agency (CISA)***, que compta amb nombrosos recursos en anglès en matèria de ciberseguretat.

***Saber-ne més***

**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 de l'ENISA:** *enisa.europa.eu*
**Web de l'EC3:** *e.digitall.org.es/EC3*
**Web del NSA:** *nsa.gov*
**Web del CISA:** *cisa.gov*



## OSI: Oficina de Seguretat de l'Internauta

L'**Oficina de Seguretat de l'Internauta (OSI)** forma part de l'INCIBE i proporciona la informació i el suport necessaris per evitar i resoldre els problemes de seguretat que hi pot haver en navegar per Internet. El seu objectiu principal se centra en la conscienciació i visualització dels problemes de ciberseguretat que poden afectar l'internauta. La informació que ens ofereix està enfocada principalment cap al ciutadà amb coneixements digitals bàsics.

La pàgina web disposa d'una àmplia gamma de recursos d'informació de tota mena, eines, guies, etc. Alguns exemples d'informació útil per al ciutadà són:

- **Actualitzacions diàries:** l'OSI proporciona informació actualitzada sobre notícies, avisos de ciberseguretat, articles de bloc, etc. Els exemples més il·lustratius d'aquesta secció són les "Històries reals". En aquests articles podem trobar exemples reals de situacions on es descriu un atac o amenaça i les directrius que cal seguir en cas que ens passi a nosaltres. Per exemple, l'OSI ens explica les amenaces dels hipertrucatges o **com actuar si han segrestat els nostres comptes** (*incibe.es/ciudadania*).
- **Campanyes:** aquest tipus de publicacions es divideixen en diferents temàtiques, com ara les contrasenyes, els dispositius mòbils o l'IoT. Dins de cadascun d'aquests temes podem trobar una llista de recursos de l'OSI relacionats amb aquest tema com ara infografies, vídeos, històries reals, etc. Un exemple d'això és la campanya **"Enginyeria social: que no t'enganyin"** (*incibe.es/ciudadania/tematicas*).
- **Manuals per aprendre a protegir-nos:** l'OSI publica diferents manuals amb recomanacions de protecció i amb diferents temàtiques. Se centra a abordar problemàtiques concretes, entendre-les i mostrar les mesures que hem de prendre per protegir-nos-hi. Algunes de les temàtiques que s'inclouen aquí són: com protegir la teva xarxa Wi-Fi o **com tenir cura de la teva privadesa** (*incibe.es/ciudadania*).

**Saber-ne més**

**IoT** són les sigles d'***Internet of Things***, que en català significa Internet de les coses. Es tracta d'un concepte que descriu la xarxa d'objectes físics que porten sensors, programari i altres tecnologies incorporats per tal de connectar-se i intercanviar dades amb altres dispositius i sistemes a través d'Internet o d'altres xarxes de comunicació.

*e.digitall.org.es/iot*

- **Recursos:** aquesta secció agrupa diferents recursos, com ara tallers, guies, eines, serveis, etc.
- **Jocs educatius:** al lloc web també podem trobar una sèrie de jocs que ens ajuden a comprendre millor els conceptes relacionats amb la ciberseguretat com, per exemple, els jocs de taula (*incibe.es/ciudadania*) que es poden descarregar directament.

Cal esmentar que, dins dels recursos que ens ofereix l'OSI, hi ha una iniciativa particular que se centra en la conscienciació i la protecció dels més petits: **Internet Segura 4 Kids**. Aquesta iniciativa pretén formar tant menors d'edat, com els seus professors i famílies, en matèria de ciberseguretat.

*Saber-ne més*

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

## INCIBE: Institut Nacional de Ciberseguretat

INSTITUTO NACIONAL DE CIBERSEGURIDAD

L'**Institut Nacional de Ciberseguretat (INCIBE)** és un organisme governamental dedicat completament a la ciberseguretat, centrada en els ciutadans, les empreses, les xarxes acadèmiques o de recerca i altres sectors estratègics.

Ja hem esmentat l'OSI, que està orientada a la ciutadania en general. Per dotar també les empreses de materials útils, l'INCIBE compta amb la iniciativa "Protegeix la teva empresa". Amb ella pretenen formar les empreses, especialment les PIMES, i oferir recursos útils com el **kit de conscienciació per entrenar els empleats** (*e.digitall.org.es/kit-incibe*). A més, l'institut té recursos orientats a fomentar l'emprenedoria al sector de la ciberseguretat, amb iniciatives com INCIBE Emprende.

*Saber-ne més*

**Web del INCIBE:** *incibe.es*
**Iniciativa "Protegeix la teva empresa":** *incibe.es/protege-tu-empresa*
**Iniciativa "INCIBE Emprèn":** *incibe.es/emprendimiento*

L'INCIBE també compta amb un lloc web interactiu perquè els emprenedors i les PIMES s'introdueixin en conceptes relacionats amb la ciberseguretat. Per això, presenten dos personatges animats que acompanyen l'espectador en la seva formació. Aquesta formació està adaptada a diferents sectors empresarials o itineraris.

**ITINERARIS DE CIBERSEGURETAT INCIBE:**

*itinerarios.incibe.es*

**UN PASSA MÉS ENLLÀ: GESTIÓ DE LA CIBERSEGURETAT**

*La ciberseguretat es gestiona, tant a les PIMES com a les grans empreses. En aquest vídeo, s'hi introdueixen conceptes com l'impacte i el risc, que ajuden a gestionar les amenaces a una empresa.*

*e.digitall.org.es/A4C41A2V02*

## CCN-CERT

El **Centre Criptològic Nacional (CCN-CERT)** és una de les fonts d'informació principals per mantenir-se actualitzats en matèria de ciberseguretat i la seva legislació associada a Espanya. Aquest organisme és l'encarregat de desenvolupar diferents eines de ciberseguretat usades per moltes empreses. Una de les més interessants per a la formació específica i tècnica en ciberseguretat és ***Ángeles*** (***e.digitall.org.es/angeles***), una eina amb multitud de recursos de diferents nivells orientats a les empreses, com ara "ciberconsells" o informes de bones pràctiques.

El CCN compta amb nombroses guies tècniques i informes de seguretat periòdics, com l'informe anual "Ciberamenazas y Tendencias", publicat a finals de cada any amb una anàlisi del panorama de ciberseguretat nacional.

***Saber-ne més***

**Web sobre l'Esquema Nacional de Ciberseguretat (ENS):** *ens.ccn.cni.es/es*
**Web Informes CCN-CERT públics:** *e.digitall.org.es/informes-cert*
**Web de Guies del CCN-CERT:** *e.digitall.org.es/guias-cert*

## ENISA

La **European Union Agency for Cybersecurity (ENISA)** és un organisme europeu que proporciona multitud de recursos en anglès sobre ciberseguretat. Igual que el CCN-CERT, aquesta agència europea té informes periòdics com el Cyber Europe, que es publiquen a finals d'any amb un resum de les tendències de ciberseguretat europees.

El lloc web (*enisa.europa.eu*) és molt útil per trobar informació organitzada per temàtiques.

DigitAll

Seguretat

# 4.2

# PROTECCIÓ DE LES DADES PERSONALS I LA PRIVACITAT

Seguretat

*Nivell A1* 4.2 Protecció de les dades personals i la privacitat

# Drets dels ciutadans en matèria de protecció de dades

# Drets de la ciutadania en matèria de protecció de dades personals

## El dret a la informació

Els drets que recull la Constitució espanyola es classifiquen en diferents categories segons la rellevància. Els més importants són els anomenats Drets Fonamentals. El dret a la protecció de les dades personals és un dret fonamental. A partir d'aquí, el legislador dona contingut a aquest dret per vies diferents: imposa deures als subjectes que tracten o manipulen dades personals, reconeix drets més concrets a la ciutadania o estableix mandats d'actuació als poders públics. Aquest document desenvolupa aquests drets de la ciutadania en què s'esqueixa el dret a la protecció de les dades personals.

**ELS DRETS DE LA CIUTADANIA EN MATÈRIA DE PROTECCIÓ DE DADES PERSONALS (I)**

*e.digitall.org.es/A4C42A2V08*

El primer és el dret a la informació. Les manifestacions són molt àmplies i variades (per exemple, el dret d'accés que es tracta una mica més endavant es pot considerar una concreció del dret a la informació).


Una de les manifestacions per garantir aquest dret és la imposició al responsable del tractament del deure de facilitar determinada informació a la persona interessada. La normativa preveu que aquesta informació es pugui facilitar per capes o nivells:

- Primera capa, una informació bàsica.
- Segona capa, una informació detallada.

El contingut de la informació varia segons les dades personals s'obtinguin directament de l'interessat (per exemple, s'introdueixen dades en obrir un compte a Facebook o YouTube) o d'un tercer (per exemple, una cadena hotelera cedeix certes dades personals a una agència de viatges per a la realització d'una campanya de publicitat).

## Informació que cal facilitar quan les dades personals s'obtinguin de l'interessat

A la primera capa (informació bàsica), l'Agència Espanyola de Protecció de Dades recomana facilitar la informació següent:

- La identitat del responsable del tractament.
- Una descripció senzilla de les finalitats del tractament, incloent-hi l'elaboració de perfils si existís.
- La base jurídica del tractament.
- Si es preveu que les dades puguin ser cedides a tercers. Previsió o no de transferències a països tercers.
- La possibilitat d'exercir els drets que s'exposen en aquest document.
- Una adreça electrònica o un altre mitjà (per exemple, la descàrrega d'un document pdf) que permeti accedir de manera senzilla i immediata a la informació restant.

A la segona capa (informació detallada), es recomana incloure la informació següent:

- Dades de contacte del responsable. Identitat i dades del representant (si existís). Dades de contacte del delegat de protecció de dades (si existís).
- Descripció ampliada de les finalitats del tractament. Terminis o criteris de conservació de les dades. Decisions automatitzades, perfils i lògica aplicada.
- Detall de la base jurídica del tractament, en els casos d'obligació legal, interès públic o interès legítim. Obligació o no de facilitar dades i conseqüències de no fer-ho.
- Destinataris o categories de destinataris. Decisions d'adequació, garanties, normes corporatives vinculants o situacions específiques aplicables.
- Com exercir els drets d'accés, rectificació, supressió i portabilitat de les dades, i la limitació o l'oposició al tractament. Dret a retirar el consentiment prestat. Dret a reclamar davant de l'Autoritat de Control.

**ATENCIÓ**

Quan les dades personals es recullen directament dels interessats, la informació s'ha de facilitar amb caràcter previ a aquesta recollida.

### Informació que cal facilitar quan les dades personals no s'obtinguin de la persona interessada

Quan les dades personals no han estat obtingudes de l'interessat, **a més de la informació que s'indica a l'apartat anterior**, cal facilitar la següent:

A la primera capa (bàsica):

- La font de les dades, és a dir, la seva procedència.

A la segona capa (detallada):

- La informació detallada de l'origen de les dades, encara que provenen de fonts d'accés públic. Són fonts d'accés públic, per exemple, els diaris i els butlletins oficials, els mitjans de comunicació social, les pàgines web, etc.
- La categoria de dades que es tractin (per exemple, dades identificatives generals com el nom o el telèfon; o dades confidencials com l'origen racial o les opinions religioses).

**ATENCIÓ**

Quan les dades personals no es demanen de l'interessat, el responsable del tractament ha d'informar-lo d'aquesta recollida en el termini d'un mes i, a tot tardar, en la primera comunicació a l'interessat.

***Saber-ne més***

**Grup de treball sobre protecció de dades de l'article 29.** Directrius sobre la transparència en virtut del Reglament (UE) 2016/679 (WP 260)
*e.digitall.org.es/articulo29*

## El dret d'accés

Consisteix en el dret de la persona interessada a obtenir del responsable del tractament confirmació de si s'està tractant o no dades personals que el concerneixen.

En aquest cas, el responsable ha de facilitar dues coses:

- Una còpia d'aquestes dades o un sistema d'accés remot, directe i segur.
- Una sèrie d'informació que coincideix amb l'exposada a la secció anterior (fins del tractament, categories de dades personals, destinataris, termini de conservació, etc.).

**ATENCIÓ**

L'exercici del dret d'accés permet a l'interessat esbrinar què en saben les empreses, és a dir, quines dades personals tracten i controlar-ne la licitud i l'exactitud.

Aquest dret té una sèrie de limitacions materials i formals. Pel que fa als materials, en són dos:

- No ha d'afectar negativament els drets i les llibertats de tercers, inclosos els secrets comercials o la propietat intel·lectual.
- Certs interessos públics (seguretat de l'Estat; defensa; seguretat pública; etc.).

Quant a la limitació formal, quan el responsable tracti una gran quantitat de dades relatives a l'afectat i aquest exerceixi el seu dret d'accés sense especificar si es refereix a tothom o a una part, el responsable podrà sol·licitar-li que especifiqui les dades o activitats de tractament als que es refereix.

***Saber-ne més***

**Comitè Europea de Protecció de Dades.** Directrius 1/2022 sobre dret d'accés. *e.digitall.org.es/directrices*

## El dret de rectificació

El dret de rectificació té dues manifestacions:

- D'una banda, obtenir sense dilació indeguda del responsable del tractament la rectificació de les dades personals inexactes que el concerneixin. L'interessat ha d'indicar a quines dades es refereix i la correcció que cal fer.
- De l'altra, tenint en compte els fins del tractament, el dret que es completin les dades personals que siguin incompletes. Suposa que en aquells casos en què la informació que aporti l'interessat s'adeqüi a les finalitats del tractament i completi les dades que tracta el responsable, aquest vindrà obligat a admetre-la i a incloure-la en el seu tractament (per ex., imaginau-vos el tractament de dades sobre solvència creditícia).

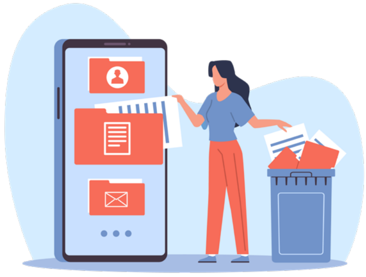
En cas que sigui necessari, l'interessat haurà d'acompanyar a la sol·licitud la documentació justificativa de la inexactitud o caràcter incomplet de les dades objecte de tractament.

En qualsevol cas, el responsable té el deure de garantir l'exactitud en les dades que tracta, és a dir, que és una cosa que ha de fer fins i tot d'ofici sense cap sol·licitud.

**ATENCIÓ**

El dret de rectificació es pot exercir quan es tractin dades inexactes o incompletes.

## El dret de supressió i el dret a l'oblit



El dret de supressió suposa el dret a obtenir sense dilació indeguda del responsable del tractament l'eliminació de les dades personals que el concerneixin. Es pot exercir respecte de la totalitat de les dades que es tracten o només sobre alguna.

Aquesta supressió és obligatòria quan concorrin algunes de les circumstàncies següents:

**1 |** Les dades personals ja no siguin necessàries en relació amb les finalitats per a les quals van ser recollides o tractades.
**2 |** L'interessat retiri el consentiment en què es basa el tractament i aquest no es basa en un altre fonament jurídic.
**3 |** L'interessat s'oposi al tractament i no prevalguin altres motius legítims per a aquest tractament.
**4 |** Les dades personals hagin estat tractades il·lícitament.
**5 |** Les dades personals s'han de suprimir per complir una obligació legal.
**6 |** Les dades personals s'hagin obtingut amb relació a l'oferta de serveis de la societat de la informació relatius als infants.

**ATENCIÓ**

Quan el responsable hagi fet públiques les dades personals i estigui obligat a suprimir-les, adoptarà les mesures raonables per informar altres responsables que tractin aquestes dades personals perquè també procedeixin a suprimir-les. **Això és el dret a l'oblit**.

Quan el dret de supressió s'exerceix sobre dades fetes públiques, es parla del dret a l'oblit. Per tant, el dret a l'oblit només s'exigeix davant del responsable que hagi publicat les dades personals i no arriba als supòsits de mera comunicació de dades, és a dir, quan aquestes dades s'hagin facilitat a persones o entitats singulars.

**NOTA**

El Tribunal Suprem ha declarat que no es pot exercir el dret de supressió davant les dades del llibre de baptisme.

**NOTA**

Des del 2014 fins al 2020, Google ha rebut peticions per retirar més de 4 milions d'enllaços. A Espanya, el percentatge de peticions acceptades s'aproxima el 40%.

En qualsevol cas, el dret de supressió no és absolut i la normativa preveu una sèrie de supòsits en què no és procedent, encara que amb determinades condicions. Els més rellevants:

**1 |** Per exercir el dret a la llibertat d'expressió i informació (penseu, per ex., en les notícies publicades a la premsa digital).
**2 |** Per complir una obligació legal que requereixi el tractament de dades i que s'apliqui al responsable del tractament, o per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable (per ex., certes dades investigacions policials o penals).
**3 |** Per raons d'interès públic en l'àmbit de la salut pública.
**4 |** Amb finalitats d'arxiu en interès públic, finalitats de recerca científica i històrica i finalitats estadístiques.
**5 |** Per a la formulació, exercici o defensa de reclamacions.

***Saber-ne més***

**Comitè Europeu de Protecció de Dades.** Directrius 5/2019 sobre els criteris del dret a l'oblit en els casos de motors de cerca en virtut del RGPD.
*e.digitall.org.es/directrices*

## El dret a la limitació del tractament

**ELS DRETS DE LA CIUTADANIA EN MATÈRIA DE PROTECCIÓ DE DADES PERSONALS (II)**

*e.digitall.org.es/A4C42B1V08*

És el dret a obtenir del responsable el marcatge de les dades personals conservades per tal de limitar-ne el tractament de manera provisional quan sigui procedent alguna de les circumstàncies següents:

- L'interessat impugni l'exactitud de les dades mentre el responsable la verifica.
- El tractament sigui il·lícit i l'interessat s'oposi a la supressió de les dades personals i sol·liciti al seu lloc la limitació de

l'ús. En aquest cas, allò que es pretén fonamentalment és evitar que es destrueixin les proves acreditatives de la infracció comesa pel responsable.

- El responsable ja no necessiti les dades personals per a fins del tractament, però l'interessat les necessiti per a l'exercici o la defensa de reclamacions.
- L'interessat s'hagi oposat al tractament mentre es verifica si els motius legítims invocats pel responsable per continuar el tractament prevalen sobre els de l'interessat.

Mentre duri aquesta limitació, les dades només poden ser objecte de tractament, a excepció de la seva conservació, per una sèrie de motius taxats: consentiment de la persona interessada, formulació de reclamacions, protecció dels drets d'una altra persona i raons d'interès públic.

Com s'exposa, aquesta limitació es regula com un dret de l'interessat i no com un deure del responsable del tractament. Això és, el responsable del tractament no té el deure de procedir d'ofici a la limitació del tractament quan concorrin algunes de les circumstàncies exposades, sinó que perquè això passi l'interessat haurà d'exercir expressament aquest dret.

**ATENCIÓ**

La limitació del tractament és de caràcter provisional mentre concorren o es verifiquen determinades circumstàncies.

## El dret a la portabilitat de les dades

Consisteix en el dret de l'interessat a rebre les dades personals que li incumbeixin, que hagi facilitat a un responsable del tractament, en un format estructurat, d'ús comú i lectura mecànica, i a transmetre'ls a un altre responsable del tractament sense que ho impedeixi el responsable al tractament que se'ls hagués facilitat.

Les dades sobre les quals es pot exercir aquest dret són les que l'interessat hagi facilitat. Aquests no són només aquells que de manera conscient i activa va lliurar la persona interessada (per exemple, mitjançant un formulari), sinó que també estan inclosos en aquesta noció aquells obtinguts a partir de l'activitat de l'usuari en l'ús d'un servei o d'un dispositiu, per als quals no es produeix realment un lliurament actiu (per exemple, l'historial d'activitat física d'un usuari registrat en una app d'entrenament). S'exclouen les dades creades pel responsable del tractament (per exemple, les puntuacions o estadístiques que aquesta app generi a partir d'aquestes dades). Aquest dret està sotmès a dues condicions:

1 | Que el tractament estigui basat en el consentiment o un contracte. Si les causes de licitud del tractament són altres (per exemple, una obligació legal), les dades no poden ser objecte d'aquest dret.

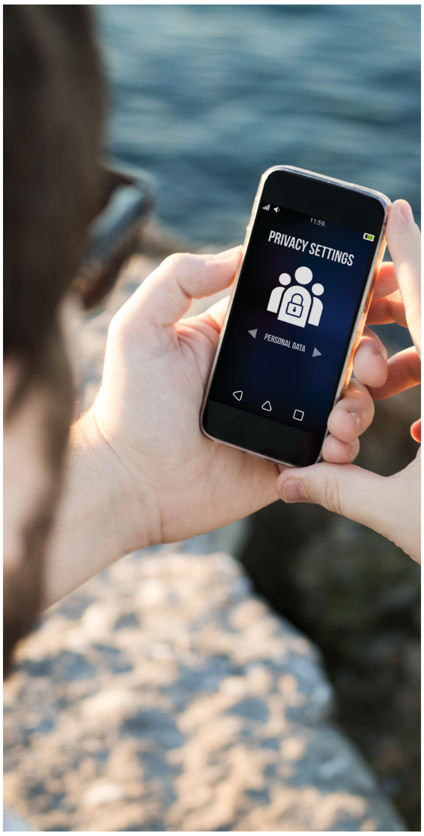
2 | Que el tractament s'efectuï per mitjans automatitzats.

En exercir aquest dret, la persona interessada tindrà dret que les dades personals es transmetin directament de responsable a responsable quan sigui tècnicament possible. Per exemple, la portabilitat de les dades dels rebuts domiciliats que una persona té en una entitat bancària a una altra entitat bancària.

Són evidents les implicacions i les dificultats d'ordre pràctic i tècnic que pot comportar l'exercici d'aquest dret. Cal que tingueu en compte que en l'extensió de les dades de caràcter personals, de tot tipus i en diferent format, que es mouen per les diferents xarxes socials, blocs, serveis d'informàtica en el núvol, de correu electrònic, etc. A tots aquests serveis se'ls confia l'emmagatzematge i el tractament massiu de dades de caràcter personal. Del que es tracta és establir mecanismes jurídics que impedeixin, sota l'argument de dificultats tècniques, que els interessats queden captius digitals de per vida d'un proveïdor concret. A més, això origina un efecte beneficiós per a la promoció de la competència.

Per aquests motius, cal elaborar un conjunt de normes i formats comuns que siguin interoperables per tal de respondre als requisits del dret a la portabilitat de dades. Tot i això, és immens el camí que queda per recórrer.

Quant a la diferència entre aquest dret i el dret d'accés, la portabilitat garanteix a l'interessat obtenir una còpia de la informació susceptible de ser processada fàcilment per un altre subjecte, mentre que l'accés es limita a garantir la informació en si mateixa. Aquesta diferència també té conseqüències quant a la manera de complir amb la sol·licitud d'exercici del dret. En el dret d'accés, les dades s'han de facilitar a l'interessat en un format de lectura accessible, que us permeti conèixer i entendre la informació.



En el dret a la portabilitat, les dades es poden facilitar en un format incomprensible per a l'ésser humà, però sí per al tractament informatitzat. També es pot establir alguna diferència entre tots dos drets pel que fa al seu abast. Per exemple, un subjecte té dret a accedir a la seva història clínica en un hospital privat. Això inclou les proves mèdiques i el diagnòstic. Però si l'interessat sol·licita la portabilitat a un altre hospital privat, es pot limitar als resultats de les proves en brut –les dades–, sense incloure-hi els diagnòstics mèdics –que és informació generada pel responsable–.

**ATENCIÓ**

El dret a la portabilitat implica que les dades personals de l'usuari es puguin transmetre directament d'una entitat o empresa a una altra, sense necessitat de ser lliurades al mateix usuari, sempre que sigui tècnicament possible.

***Saber-ne més***

**Grup d'autoritats europees de protecció de dades.** Directrius sobre el dret a la portabilitat de dades (WP 242). *e.digitall.org.es/wp-242*

**NOTA**

La normativa bancària permet la portabilitat dels comptes, migrant d'un banc a un altre tots els serveis i dades personals, així com les transferències periòdiques o les domiciliacions.

## El dret d'oposició

El dret d'oposició atribueix a la persona interessada la facultat per impedir el tractament de les vostres dades personals. Hi ha dos supòsits:

- Quan el tractament tingui per objecte el màrqueting directe (publicitat) o l'elaboració de perfils relacionats amb aquest màrqueting, l'interessat podrà oposar-se sense necessitat de cap justificació i ha d'acceptar necessàriament el responsable.
- Quan el tractament tingui com a fonament l'interès públic, l'exercici de poders públics o l'interès legítim del responsable o d'un tercer, ha de motivar aquesta oposició en funció de la situació particular.

Per exemple, una universitat pública, sobre la base de la seva missió realitzada en interès públic, imposa als alumnes que encenguin les càmeres en la docència en línia. Això no obstant, un alumne, per les seves especials circumstàncies personals i familiars (només pogués connectar-se a llocs on hi ha altres membres de la família), pot exercir el seu dret d'oposició a aquest tractament.

En aquest segon supòsit, el responsable pot continuar tractant les dades si acredita motius legítims que prevalguin sobre els de la persona interessada. Per exemple, possiblement la universitat podria imposar la mesura anterior si fos per verificar la identitat de l'alumne a l'hora de fer un examen.

En qualsevol cas, cal que el responsable respongui a la persona interessada expressant els motius pels quals rebutja la seva sol·licitud d'oposició.

**ATENCIÓ**

El dret d'oposició no es pot exercir davant de molts tractaments de dades que realitzen les administracions públiques (Hisenda, policia, Seguretat Social, etc.)

***Saber-ne més***

**Agència Espanyola de Protecció de Dades. Coneix els teus drets.**
[e.digitall.org.es/conoce-tus-derechos](e.digitall.org.es/conoce-tus-derechos)

DigitAll

Seguretat

# 4.3

# PROTECCIÓ DE LA SALUT I EL BENESTAR

Seguretat

*Nivell A1* 4.3 Protecció de la salut i el benestar

# Principis de la salut digital

# Principis de la salut digital

En aquest document s'aborda el concepte de salut digital, l'e-salut i les diferències i similituds. Tot i que són coneguts els beneficis que pugui aportar la tecnologia a la salut i el benestar, s'identifiquen les principals diferències bàsiques, entre els riscos i les amenaces relacionades amb la salut digital a escala psicològica, física i social.

## Introducció al concepte de salut digital

En els temes relacionats amb la salut i el món digital, hi ha poca evidència sobre els beneficis i els danys que tenen les solucions digitals sobre la salut i el benestar de les persones. Tot i això, en aquest document intentarem facilitar la identificació de les repercussions que la tecnologia pugui tenir sobre la nostra salut.

La **salut digital** és un concepte creat per relacionar l'impacte positiu o negatiu que tenen les tecnologies de la informació i les comunicacions (TIC) (des d'ordinadors portàtils, intel·ligència artificial fins a dispositius portables) sobre la salut i el benestar de les persones. Segons l'Organització Mundial de la Salut (OMS), l'any 2012 s'ha conceptualitzat del terme de salut digital, que inclou l'ús de tecnologia per millorar la salut i altres camps relacionats amb aquesta. Segons l'OMS, la salut digital comprèn des dels consumidors digitals fins a la robòtica, considera dispositius intel·ligents i connectats i abasta diferents usos de les tecnologies per a la salut, com l'internet de les coses, l'aprenentatge automàtic, la intel·ligència artificial, la informàtica avançada i l'anàlisi de grans volums de dades.

NOTA

**Salut digital**: concepte que abasta l'impacte que té l'ús i l'ús de les TIC sobre la salut i el benestar.

La salut digital no només es caracteritza per aplicar diferents eines tecnològiques a la salut, sinó que també implica un canvi en la pràctica sanitària i assistencial. Per això, el seu objectiu és promoure i potenciar una assistència sanitària millor mitjançant l'ús de la tecnologia. Així, podem dir que aquest concepte ha suposat la transformació digital dels sistemes de salut i ha provocat reformes a escala legal, administratiu i financera.

La digitalització de la salut ens permetrà prevenir malalties, i fins i tot detectar-les en fases primerenques, mantenir una atenció més efectiva i de qualitat, reduir els costos de l'atenció sanitària i fer un seguiment personalitzat de la salut de les persones, sigui pel metge de capçalera o per la pròpia autogestió de la salut.

Des de la Comissió Europea s'espera que la salut digital promogui la participació de les persones en la gestió de la salut, fent èmfasi en l'estil de vida i en la prevenció i connectant els diferents agents i sectors del sistema de salut i l'assistència social per millorar les situacions d'emergència, les epidèmies, els procediments i, sobretot, per reduir les deficiències de l'atenció sanitària actual.

En aquesta línia, aproximadament des de l'any 1999, hi ha hagut un terme relacionat amb la salut digital que ha generat confusió, usant-se de manera errònia com a sinònim; parlem del concepte de l'e-salut o l'*e-health*.

L'**e-salut** es defineix com una branca dins de la salut digital. Comprèn les TIC com a eines emprades a l'entorn sanitari en matèria de prevenció, diagnòstic, tractament i seguiment, així com en la gestió de la salut, estalviant costos al sistema sanitari i millorant-ne l'eficàcia. La principal diferència entre totes dues és que les iniciatives de l'e-salut no s'originen des del pacient, com passa a la salut digital. A més, les categories dins de l'e-salut estan més relacionades amb el tractament informàtic de dades sanitàries, incloent-hi eines com:

- El registre mèdic electrònic o historial de la clínica electrònica.
- La telesalut (inclosa la telemedicina).
- L'aprenentatge o la formació digital a distància, també conegut com a *e-Learning*.
- L'educació continua en tecnologies de la informació i la comunicació.

Tot i això, malgrat tots els beneficis que ens pugui aportar la tecnologia, també pot tenir un impacte negatiu sobre la salut i el benestar, sigui de manera directa o indirecta sobre el seu ús diari.

**ATENCIÓ**

E-salut i salut digital no són sinònims, sinó que la primera és una branca dins de la segona.

Dins dels diferents riscos i amenaces que pot provocar l'ús de la tecnologia, trobem els conceptes d'addicció digital i ciberassetjament. Tot i això, també es tractaran altres amenaces digitals relacionades amb l'e-salut i el tractament de dades.

## Amenaces digitals relacionades amb l'e-salut

La ràpida evolució de les TIC ha provocat una sèrie de canvis a què cal adaptar el sistema sanitari. Un és la privadesa dels usuaris, ja que el tractament d'aquesta informació és un aspecte altament sensible. Per això, cada cop més, els governs i entitats públiques relacionades amb la salut i la seguretat treballen en un emmagatzematge més segur per a les dades de la població. En aquesta línia, l'ús de les noves tecnologies i l'emmagatzematge de les dades al núvol és una millora de la salut digital, ja que permet i promou la salut participativa a la ciutadania mitjançant la visualització i la compartició de les dades de la seva salut , facilitant l'atenció i la gestió sanitària.

***Saber-ne més***

Les principals amenaces considerades s'enfoquen en l'addicció digital i el ciberassetjament.

**ATENCIÓ**

La privadesa pel que fa a les dades de salut dels usuaris és un tema altament sensible i necessari de tractar.

La incorporació de tecnologies que interactuen amb el medi físic i que poden ser monitorades i controlades remotament (pegats “intel·ligents” d’insulina, marcapassos programables a través de xarxes sense fil, pròtesis per compensar discapacitats físiques, etc.) han posicionat la salut i l’afectació directament a la vida de les persones com un risc molt més preocupant. Alguns exemples recents, com el hackeig de marcapassos i bombes d’insulina, així ho demostren.

**NOTA**

Aquests avenços també suposen un repte per a la seguretat, ja que aquests sistemes han de fer front a la lluita de hackejos o fuites que puguin provocar que la informació personal relacionada amb l’estat de salut d’una persona sigui pública. Per això, en l’àmbit nacional i europeu, es treballa en lleis que protegeixin la informació personal. Així, la salut digital s’ha de sotmetre al Reglament Europeu de Protecció de Dades i a la Llei de Protecció de Dades i Garantia de Drets Digitals, que afecten els professionals sanitaris, hospitals, clíniques i centres mèdics que manegen tota aquesta informació. Aquesta normativa es relaciona amb la confidencialitat de les dades mèdiques, millorar la qualitat de les dades, fer ús del consentiment del pacient en tot moment, mantenir informat el pacient sobre el seu diagnòstic i tractament.

La complexitat del nou context tecnològic fa que el nombre d’actors involucrats en el cicle de vida dels nous processos digitals sigui tan extens que alguns ni tan sols són conscients de la seva influència i interacció amb aquests processos i, conseqüentment, no hi estan incorporant els prou controls de seguretat en les seves funcions ni en les tecnologies que proporcionen.

A les mancances existents a les tecnologies d’Internet cal afegir-hi que alguns dels nous serveis de teleassistència o de monitoratge remota de les persones preveuen l’ús dels telèfons mòbils particulars dels consumidors/clients com a font d’informació (biometries, geoposicionament, generació d’alertes, etc.), sense calibrar adequadament el que no siguin dispositius de precisió especialitzats ni fiables.

***Saber-ne més***

Les tecnologies englobades a Internet de les coses inclouen la teleassistència o el monitoratge remot de la salut de les persones.

A més, a la complexitat i mancances anteriors, cal sumar-hi les mancances existents als edificis des dels quals es presten aquests serveis, ja siguin fàbriques on es construeix tecnologia mèdica, farmacèutiques on es produeixen medicaments, centres d'atenció sanitària o qualsevol altre tipus d'instal·lació relacionada amb serveis de medicina i salut en general. Bona part d'aquestes instal·lacions han incorporat tecnologies intel·ligents connectades a internet per optimitzar els seus recursos (calefacció, il·luminació, control d'accessos, ascensors, vídeovigilància, manteniment preventiu, etc.) i aquestes tecnologies poden tenir, alhora, vulnerabilitats que poden ser explotades remotament. Vulnerabilitats que, a més d'afectar el funcionament de l'edifici, poden facilitar l'accés a persones no autoritzades que, fins i tot, alterin els processos que s'hi desenvolupen, arribant a impactar en la salut dels consumidors finals.

## Riscos i amenaces de la tecnologia a la salut digital

### Riscos i amenaces a escala física

Un ús inadequat de la tecnologia pot afectar en gran manera la nostra salut física. Aquesta afectació es deu, principalment, a temps d'ús excessius o a mantenir una postura inadequada. Aquesta situació es pot produir tant en entorns laborals com a casa nostra o en espais d'oci. Alguns dels problemes que podem patir són:

- **Mal a la vista:** la utilització de pantalles durant períodes molt llargs de temps pot causar problemes als nostres ulls com ardor, llagrimeig o envermelliment. Això és degut, en gran part, a la llum blava dels LEDS que formen la pantalla, l'exposició dels quals afecta la retina. També cal destacar un altre gran problema com és la fatiga ocular, que és ocasionada per una disminució en la freqüència amb què parpellejam. Així mateix, aquests problemes relacionats amb la vista poden, alhora, ocasionar mal de cap.
- **Esquena i cervicals**: l'ús prolongat de dispositius tecnològics fa que les espatlles estiguin habitualment inclinades cap endavant i que les cervicals es mantinguin en tensió durant llargs períodes de temps, cosa que provoca l'aparició de contractures.

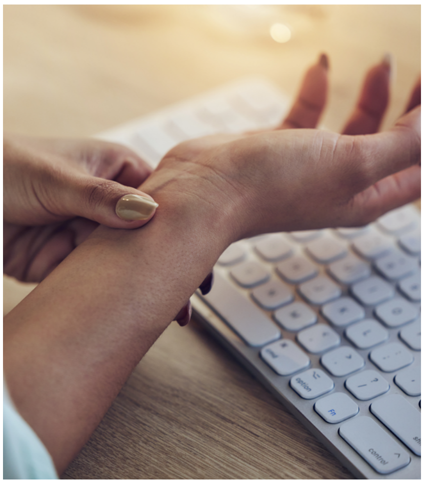
**NOTA**

A més, les infraestructures com els edificis no estan preparats per als avenços tecnològics, ja sigui per la connectivitat sigui per Wi-Fi, Bluetooth o altres alternatives.

**ATENCIÓ**

Un ús inadequat dels dispositius tecnològics pot donar lloc a diferents riscos i amenaces a escala física, social i psicològica.

- **Síndrome del túnel carpià:** un ús prolongat del teclat i el ratolí pot provocar aquesta síndrome. Passa quan el nervi que va des de l'avantbraç a la mà es comprimeix al pas pel túnel carpià, una zona de lligaments que es troba sota el palmell de la mà. Aquesta afecció sol provocar adormiment, entumiment o pèrdua de força i mobilitat al canell afectat, entre d'altres.



Els problemes anteriors afecten directament diferents parts del nostre cos, però també hem de tenir en compte que un abús en l'ús de la tecnologia també pot derivar en un **estil de vida sedentari**. Això pot suposar un risc per a la nostra salut generalment i ser la causa de múltiples malalties com l'**obesitat**, els **problemes de cor o el colesterol elevat**.

### Riscos i amenaces a l'àmbit social

L'ús de les noves tecnologies a nivell social pot ser positiu sempre que no es deixin de banda les activitats de la vida quotidiana com ara estudiar, fer esport, sortir amb amics i estar en família, entre d'altres. Quan el seu ús és desmesurat i descontrolat, pot donar lloc a una sèrie de riscos:

- **Aïllament social:** l'addicció a xarxes socials, videojocs o diverses aplicacions pot generar que l'usuari s'acabi aïllant del món; cosa que l'afectarà en les relacions interpersonals amb amics, familiars, companys... En casos d'adolescents pot arribar a influir negativament en el desenvolupament de les seves habilitats socials. Per exemple, amb la pèrdua del contacte físic o la dificultat per apreciar emocions i gestos.
- **Manca de relació amb el món real:** l'ús desmesurat de les TIC pot portar l'individu a abstreure's totalment del món on viu, creant una desconnexió total amb el seu entorn. En molts casos, la major part de la realitat que perceben es correspondria amb la realitat digital.

**ATENCIÓ**

Un ús desmesurat de les noves tecnologies pot donar lloc a una sèrie de riscos socials com ara l'aïllament social o la manca de relació amb el món real.

## Riscos i amenaces en el marc psicològic

La tecnologia també presenta un gran impacte a la població psicològicament. Els riscos i trastorns psicològics derivats de la tecnologia són més comuns a la població adolescent. Entre els diferents riscos i amenaces destaquen:

- **Nomofòbia:** és un problema cada vegada més habitual a la societat. Es defineix com la por irracional a estar sense el dispositiu mòbil, ja que moltes persones presenten una dependència total cap al dispositiu. Aquesta situació pot provocar mal de cap o estómac, ansietat, estrès i, en casos més greus, pot provocar el desenvolupament de trastorns mentals com a trastorns obsessius.
- **Síndrome de la trucada imaginària:** aquest problema fa referència a la sensació que el telèfon està vibrant i sonant, encara que no sigui així, provocant l'impuls d'haver de mirar el dispositiu. Aquest problema és perquè el cervell relaciona qualsevol impuls que rep amb el mòbil.
- **Dependència d'Internet:** aquest tipus de dependència ve provocada per l'ús continu que es dona a aquesta xarxa informàtica pel contingut que ens aporta i que ens permet utilitzar el nostre telèfon intel·ligent, les xarxes socials, els xats, les pàgines de contactes, etc. Aquesta dependència pot provocar el desenvolupament de problemes d'ansietat, estrès, alteracions de conducta o aïllament.
- **Problemes d'inseguretat:** l'ús freqüent de dispositius mòbils per fer ús de xarxes socials pot provocar que les persones comencin a comparar-se amb altres persones, o vulguin aparentar una vida ideal mitjançant aquestes plataformes, i poder exposar-se a crítiques, així com la necessitat d'obtenir una retroacció de les xarxes socials com els "M'agrada". Tots aquests factors poden provocar en les persones danys psicològics com a malestar que promoguin el desenvolupament d'ansietat, depressió o trastorns alimentaris.

- **Tecnoestrès:** un altre risc que pot provocar l'ús de la tecnologia a la població és el tecnoestrès. Aquest problema és la manca d'habilitats per tractar amb la tecnologia de manera saludable. Això pot provocar alts nivells d'ansietat i frustració a la persona i també el desenvolupament d'actituds negatives cap a la tecnologia. Algunes persones també poden presentar certa por a aquests dispositius, resistència a parlar i fins i tot pensar-hi, i tenir pensaments hostils i agressius cap al món de les TIC.

**ATENCIÓ**

La dependència, la nomofòbia o la síndrome de la trucada, són alguns dels riscos psicològics per l'ús excessiu de la tecnologia.

Els professionals de la salut també fan referència a altres riscos de la tecnologia que poden influir en la vida diària d'una persona, com són: problemes de son, necessitat de les TIC per sentir-se conforme amb un mateix, manca de concentració, problemes de comunicació o augment descontrolat del temps d'ús.

***Saber-ne més***

**Principi Activa. Què és la salut digital i l'e-salut.**
*principioactiva.com*

**Salut Digital. Fundació Carlos Slim.**
*saluddigital.com*

DigitAll

Seguretat

# 4.4
# PROTECCIÓ DEL MEDI AMBIENT

Seguretat

Nivell A1 4.4 Protecció del medi ambient

# Consum sostenible de tecnologia

# Consum sostenible de tecnologia

## Introducció: consum d'energia de la tecnologia digital

El consum de materials i energia associat a la fabricació i ús de dispositius tecnològics es troba en continu creixement a escala mundial, incrementat fins i tot després de la pandèmia de la COVID-19.

Com vam veure al vídeo 2 de la sèrie ("***Necessitam els recursos tecnològics que fabricam?***"), algunes dades són contundents a l'hora d'il·lustrar el fenomen. Segons els informes de GSMA Intelligence, plataforma que representa els interessos del sector de la telefonia mòbil, des de l'any 2017 ja hi ha més dispositius mòbils en ús que persones al planeta. En aquell moment, segons GSMA, s'estava a punt d'arribar als 8.092 milions de connexions mòbils, mentre que el total de població a tot el món era de 7.373 milions (GSMA, 2017). Al nou informe afegeixen, a més, les dades de persones que tenen almenys un dispositiu mòbil i mostren que, a finals del 2021, 5.300 milions de persones estaran abonades a serveis mòbils, cosa que representa el 67% de la població mundial (GSMA), 2022).

**NECESSITAM ELS RECURSOS TECNOLÒGICS QUE FABRICAM?**
e.digitall.org.es/A4C44A1V02

**ATENCIÓ**

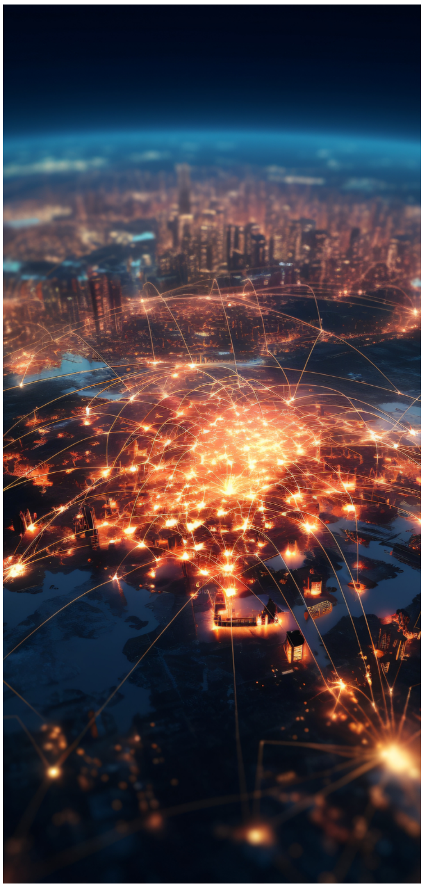
Segons els informes de *GSMA Intelligence*, plataforma que representa els interessos del sector de la telefonia mòbil, des de l'any 2017 ja hi ha més dispositius mòbils en ús que persones al planeta.

El mateix informe detalla com, amb el 95% de la població mundial coberta per una xarxa de banda ampla mòbil, el repte principal és abordar la bretxa d'ús, és a dir, el 40% de la població mundial coberta per una xarxa de banda ampla mòbil, però que encara no utilitza Internet. Per tant, és més que probable que aquestes dades d'ús de connexions i dispositius mòbils es vagin incrementant a curt termini.

Precisament, aquest increment d'ús d'Internet també es pot representar amb dades realment cridaneres. Segons l'*Informe Clicking Clean* de Greenpeace (2017), es calcula que la petjada energètica del sector de les tecnologies de la informació ja equival a un consum d'aproximadament el 7% de l'electricitat mundial i continua en augment. Més enllà d'aquesta dada, el mateix informe ens detalla com Internet genera quatre àrees principals de demanda d'energia: centres de dades, xarxes de comunicació, dispositius dels usuaris i energia per fabricar els equips necessaris per als tres anteriors.

El consum creixent de tecnologia digital està impulsant la creació de la infraestructura necessària, en concret una gran quantitat de nous centres de dades que consumeixen molta energia per servir com a elements indispensables de la nova economia digital. En aquests centres de dades se situen els servidors que serveixen per emmagatzemar els nostres missatges, fotos i altres fitxers que s'intercanvien entre dispositius mòbils i ordinadors. La tendència és que aquests centres vagin creixent cada cop més en grandària i recursos necessaris, però avui dia les instal·lacions més grans ja necessiten consumir tanta energia com una ciutat de mida mitjana, principalment per refrigerar-se (Greenpeace, 2017:2).

La manera com es construeixi i s'alimenti d'energia la infraestructura digital global determinarà com es poden encarar alguns dels desafiaments socioambientals més rellevants a què s'enfronten les societats actuals, incloent-hi la crisi climàtica. De fet, si els centres de dades i infraestructures digitals s'alimenten amb energies renovables, la creixent dependència i la necessitat de tecnologia digital pot liderar i accelerar la transició cap a un model econòmic més sostenible i amb menys empremta de carboni.



Diferents informes d'avaluació de la sostenibilitat de les infraestructures digitals posen el focus en la necessitat que les grans corporacions al sector de la tecnologia digital apostin decididament per la generació de l'energia necessària per als seus desenvolupaments a partir de fonts renovables i que no emetin o minimitzin les emissions de diòxid de carboni. De fet, hi ha un augment significatiu en la priorització de l'ús d'energies renovables entre algunes de les empreses d'internet més grans. No només per les necessitats vinculades a la reducció d'emissions per combatre la crisi climàtica, sinó també per l'horitzó d'esgotament de combustibles fòssils en el futur.

En aquest mateix sentit, la descarbonització s'ha instaurat com a meta clau en la lluita contra el canvi climàtic, motiu pel qua lla Comissió Europea ha inclòs el gas i l'energia nuclear a la taxonomia verda, és a dir, inclourà en la llista d'activitats econòmiques mediambientalment sostenibles.

Corporacions líders al sector com Apple, Facebook i Google es van comprometre ja fa 10 anys a una transició total a la generació 100% d'origen renovable, i al llarg de l'última dècada s'han sumat a aquest compromís més de 20 companyies del sector. Aquestes empreses estan motivades per diferents raons de pes, ja que els seus clients comencen a estar preocupats per la sostenibilitat de la tecnologia digital. Però, a més a més, les energies renovables comencen a ser més rendibles que certs combustibles fòssils per a produccions a gran escala, especialment en contractes a llarg termini, a més de proporcionar més seguretat de subministrament relacionada amb aspectes geopolítics.

Però si bé és cert que cada cop més empreses s'estan sumant a l'aposta per un consum d'energia 100% d'origen renovable, cal vigilar que les apostes per un model transformador siguin fermes, i no una simple façana o mètode d'ecoblanqueig per les corporacions. Per tant, l'actitud crítica dels consumidors i associacions és imprescindible per vigilar el compliment d'aquestes apostes.

**Saber-ne més**

El terme ecoblanqueig fa referència al procés de transmetre una falsa impressió o informació enganyosa sobre el grau de sostenibilitat i ecologia dels productes o serveis d'una empresa. És una manera de fer màrqueting que cerca aprofitar la creixent demanda dels consumidors per opcions més respectuoses amb el medi ambient.

*es.wikipedia.org/wiki/Ecoblanqueo*

## Demanda de materials per a la tecnologia digital

A més de la demanda d'energia que hem vist al punt anterior, la indústria de la tecnologia digital també requereix una alta demanda de materials per a la producció de dispositius i la construcció d'infraestructures. Per posar-ne un exemple, es calcula que cada telèfon intel·ligent necessita més de 60 components per al seu procés de fabricació i entre els quals hi ha materials com alumini, or, coure o cobalt que s'extreuen de la natura en quantitats considerables des de fa dècades, però també altres com liti o silici l'extracció dels quals s'està multiplicant per cobrir les necessitats de la tecnologia digital, com ja vam veure al vídeo 3 del nivell "***Processos de fabricació de recursos tecnològics***".

PROCESSOS DE FABRICACIÓ DE RECURSOS TECNOLÒGICS

e.digitall.org.es/A4C44A1V03

Precisament el liti és un material cada cop més sol·licitat per ser el component fonamental de la majoria de les bateries. Bàsicament, una bateria està formada per dues o més cel·les electroquímiques i dos elèctrodes per convertir energia química en energia elèctrica. En una bateria de liti, l'elèctrode positiu de la bateria funciona principalment amb un compost de liti, mentre que l'elèctrode negatiu de la bateria empra carboni en forma de grafit. A més, ha d'estar coberta per una carcassa d'alumini on també es pot trobar cobalt.

D'altra banda, components microelectrònics i el cablejat del telèfon estan fabricats fonamentalment amb metalls com el coure, la plata i l'or que són molt bons conductors de l'electricitat, encara que també es poden trobar platí, estany, plom i pal·ladi. L'electrònica dels dispositius es fonamenta en xips de silici pur, que es bombardegen amb elements semiconductors com fòsfor, antimoni, arsènic, bor, gal·li i indi per millorar les seves propietats elèctriques.

Tant per als condensadors dels dispositius com per a les lents de les càmeres es necessita el tàntal, element present al coltan, que és una abreviatura comercial utilitzada en parts d'Àfrica per anomenar la Columbita-Tantalita. El coltan és conegut responsable indirecte dels conflictes bèl·lics que pateix la República Democràtica del Congo, on es troben les majors reserves mundials, però també es troba a la Xina, Rússia o altres països africans com Etiòpia, Moçambic, Nigèria i Rwanda.

El nivell de producció en aquests països varia segons els dipòsits, ja que molts són d'explotació artesanal. Un concentrat de tàntal pot contenir de 10% a 40% Ta2O5, el seu valor comercial es calcula sobre el concentrat d'òxid de tàntal.

Tant el micròfon com l'altaveu d'un dispositiu digital estan formats per imants, que contenen aliatges de neodimi, ferro i bor, a més de disprosi i praseodimi. Aquests dos últims elements pertanyen a les anomenades "terres rares", 17 elements de la taula periòdica, 15 dels quals pertanyen als lantànids. Les seves propietats més destacables són d'índole química, òptica i magnètica, i són crítics per a la transició energètica i la tecnologia digital. A més del disprosi i el praseodimi, l'itri, lantà, terbi, europi i el gadolini s'utilitzen per a les pantalles de dispositius digitals; i el neodimi per a l'electrònica d'aquests.

I, finalment, les carcasses metàl·liques dels nostres dispositius estan compostes per aliatges de magnesi, a més de poder trobar níquel, que evitarà les interferències electromagnètiques, i compostos de brom que, a causa de les seves propietats ignífugues, fan que el dispositiu sigui més resistent a la calor.

Després d'aquest repàs, podem fer un **llistat no exhaustiu de 30 elements necessaris per a la fabricació de dispositius mòbils** (a la dreta).

Al cost econòmic i energètic necessari per a l'extracció d'aquests elements químics, cal sumar-hi l'impacte ambiental de les activitats mineres. A més, tots aquests recursos naturals són limitats, és a dir, que es van esgotant i els jaciments que queden disponibles cada cop són més difícils d'explotar. Es calcula que abans del 2050, ja es podrien haver esgotat els principals materials imprescindibles per a la fabricació de tecnologia digital, i això serà degut a l'augment exponencial del consum a escala mundial.

Així mateix, cada any es generen més de 46 milions de tones de residus electrònics pels telèfons intel·ligents, ordinadors, entre altres aparells que es rebutgen i amb ells es perd una enorme quantitat de minerals i materials preciosos.

**1** | Coure
**2** | Plata
**3** | Or
**4** | Platí
**5** | Pal·ladi
**6** | Silici
**7** | Fòsfor
**8** | Antimoni
**9** | Arsènic
**10** | Estany
**11** | Plom
**12** | Alumini
**13** | Cobalt
**14** | Boro
**15** | Gal·li
**16** | Indi
**17** | Tàntal
**18** | Neodimi
**19** | Ferro
**20** | Boro
**21** | Disprosi
**22** | Praseodimi
**23** | Itri
**24** | Lantani
**25** | Terbi
**26** | Europi
**27** | Gadolini
**28** | Magnesi
**29** | Níquel
**30** | Brom

30 elements necessaris per a la fabricació de dispositius mòbils.

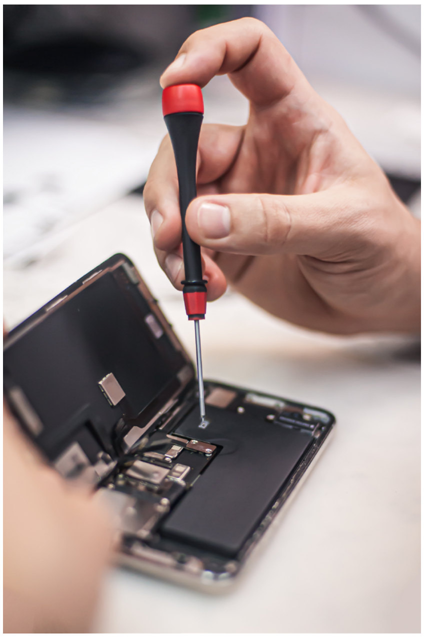
## Hàbits de consum sostenible de tecnologia

Davant d'aquest panorama, es fa imprescindible plantejar nous enfocaments per optimitzar la sostenibilitat de la producció i el consum de tecnologia digital. Com hem vist al vídeo 4 de la sèrie, titulat "***Consum sostenible de tecnologia***", en primer lloc, ens hem de centrar en les 3 R clàssiques de la sostenibilitat, és a dir, Reduir el nostre consum, tant de dispositius com d'energia; Reutilitzar dispositius i components en la mesura que sigui possible; i, finalment, Reciclar els materials que es fan servir en la fabricació.

**CONSUM SOSTENIBLE DE TECNOLOGIA**
e.digitall.org.es/A4C44A1V04

Quant a la reutilització i el reciclatge, cal tenir en compte que tots els dispositius utilitzats i rebutjats fins ara, l'anomenada "escombraries electròniques" o residus d'aparells elèctrics i electrònics (RAEE), poden ser una font indispensable de materials cadascú més escassos, en la mesura que s'aconsegueixin reutilitzar o reciclar. El reciclatge i la reutilització de les escombraries electròniques no només permet donar-li més "vides" a un mateix recurs natural, sinó que també suposa un important estalvi des del punt de vista energètic, ja que és molt més rendible adreçar un material que extreure'l des de la font natural i transformar-ho.

Pel que fa a la reducció del nostre consum de dispositius, no només és una qüestió de voluntat personal. A més de tenir en compte les opcions de reutilitzar o tornar a condicionar dispositius disponibles abans d'adquirir-ne un de nou, també cal fer incidència política i reclamar a les administracions competents una major regulació a l'hora de limitar les obsolescències que operen sobre aquest tipus de dispositius des dels seus dissenys i processos de comercialització, tant l'obsolescència programada, com les obsolescències percebudes o d'especulació.



D'aquesta manera, s'hauria d'afavorir el "dret a reparar" els dispositius digitals i electrònics a partir de dissenys que en possibilitin la reparació i l'adquisició de recanvis durant diversos anys. Ja existeixen exemples en aquest sentit, com el "fairphone" o telèfon just, una iniciativa que prioritza l'extensió de la vida útil dels dispositius a partir d'un disseny modular que facilita les reparacions fàcils; a més d'afavorir la reducció de residus electrònics a través de la reutilització i la reparació, sinó també incrementant l'ús de materials reciclats en la fabricació. Per acabar, és una iniciativa que també garanteix que els materials utilitzats no provenen de zones de conflicte i que les persones que treballen en la seva fabricació ho fan amb unes condicions justes.

Pel que fa al consum energètic lligat a la tecnologia digital, el més senzill és començar per hàbits i gestos quotidians per reduir la nostra empremta digital. Un informe de l'Agence de la transició ecològica francesa afirma que 43% de les persones mai apaga la caixa de la seva televisió o el rúter. Són detalls que poden marcar la diferència a escala global, com ara apagar els interruptors, no deixar la televisió, la impressora o la consola en espera, no deixar l'ordinador suspès, així com col·locar regletes amb interruptor d'apagat, ja que, si l'equip està connectat directament a la xarxa, continuarà consumint.

La Comissió Europea, al seu programa "La Dècada Digital d'Europa: metes digitals per al 2030", exposa literalment que "els dispositius digitals han d'afavorir la sostenibilitat i la transició ecològica, sent imprescindible que els usuaris no només han de conèixer l'impacte mediambiental i el consum d'energia dels seus dispositius", sinó que també "han de poder participar en el procés democràtic a tots els nivells i tenir el control sobre les dades pròpies".

**Saber-ne més**

*Agence de la transition écologique, (2022). Evaluation environnementale des équipements et infrastructures numériques en France.* (Avaluació ambiental dels equipaments i infraestructures digitals a França). *e.digitall.org.es/evaluacion-ambiental*

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

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

Observatori Nacional de Tecnologia i Societat (ONTSI), (2021) "Tendències en l'ús de dispositius tecnològics" *e.dgitall.org.es/ontsi*

Parlament Europeu (2022). Dret a reparar: el PE vol productes més duradors i fàcils de reparar. *e.digitall.org.es/derecho-reparar*

Comissió Europea (2021). La Dècada Digital d'Europa: metes digitals per al 2030. *e.digitall.org.es/metas-2030*

DigitAll

Formació en
Competències
Digitals

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**

Gobierno de España · Ministerio de Ciencia e Innovación
Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia