DigitAll

Formació en
Competències
Digitals

4

Seguretat

DigitAll

Formació en
Competències
Digitals

Seguretat

Nivell B1

ÍNDEX

DigitAll

Seguretat

4.1 PROTECCIÓ DE DISPOSITIUS

Seguretat

Nivell B1 4.1 Protecció de dispositius

Sessions i autenticació web

Sessions i autenticació web

Entendre com funciona la navegació web és essencial per al nostre dia a dia en línia. Utilitzam el web per fer compres, gestions, cercar informació o per veure una pel·lícula. Per ajudar-nos a protegir els nostres comptes als serveis del web, veurem a continuació com funciona l'**autenticació web i les sessions**.

Servidors i navegadors

Com hem après en nivells anteriors, la navegació web fa servir els servidors i els navegadors per funcionar. La majoria dels serveis a què accedim, en lloc de ser pàgines web estàtiques, ofereixen certes funcionalitats. Aquests serveis es coneixen com a aplicacions web.

Tant les pàgines web estàtiques com les aplicacions web usen **adreces web** o URL, que es tradueixen en adreces IP a través del DNS. Així, el nostre navegador pot accedir als recursos allotjats al servidor. Cada imatge, pàgina o document allotjat al servidor, té un URL diferent. El nostre navegador **fa una sol·licitud per cadascun dels continguts, a través del protocol HTTP**.

NAVEGACIÓ WEB SEGURA

La navegació web forma part del nostre dia a dia. Aquest vídeo ens explica què és un URL i com funciona la comunicació entre servidor i navegador.

e.digitall.org.es/A4C41A1V06

Introducció a les sessions web

Hi ha certs casos en què el servidor **ha de conèixer la nostra identitat per oferir contingut personalitzat o al qual només tenim accés nosaltres**. Per exemple, els missatges privats d'una xarxa social. En aquest cas, l'aplicació web de la xarxa social, ens ha d'autenticar quan accedim al nostre compte.

Les sessions web es fan servir per identificar amb nosaltres cadascuna de les peticions HTTP del navegador. Un cop hem accedit al nostre compte a l'aplicació, el servidor **ens atorga un identificador de sessió.** A cada petició que el navegador faci al servidor, inclourà aquest identificador, per fer saber que som nosaltres i que ja hem verificat la nostra identitat en entrar al compte.

L'**identificador de sessió** es desa a les **galetes de sessió**, un petit fitxer que guarda el navegador durant la navegació. Quan el servidor rep una petició HTTP, el navegador consulta la galeta

GALETES, SESSIONS I PRIVACITAT AL WEB

Les sessions es fan servir per autoritzar les peticions web. Les galetes de sessió mantenen aquesta informació. No obstant això, hi ha altres galetes que poden afectar la nostra privadesa.

e.digitall.org.es/A4C41C1V09

i envia l'identificador a la petició. D'aquesta manera, com que hem accedit al nostre compte i el servidor ens ha assignat un identificador, només es mostren els nostres missatges privats, i no els d'una altra persona. L'autorització es produeix quan el navegador tria quin contingut mostrar-nos d'acord amb aquest identificador de sessió. L'**autorització es produeix quan el navegador tria quin contingut mostrar-nos d'acord amb aquest identificador de sessió**.

Les galetes solen tenir diferents períodes de caducitat, igual que les sessions web. Això es defineix quan ens autenticam i el servidor ens assigna l'identificador. Si un atacant ens roba el nostre identificador de sessió, es podria fer passar per nosaltres. Tot i això, si el període de caducitat és curt, això evita que l'atacant pugui mantenir accés per un període llarg.

Registre, autenticació i sessions

Per utilitzar els serveis web amb un compte, el primer que fem és registrar-nos al servei. A més del nom d'usuari i dades necessàries del mateix registre, és en aquest moment en què configuram el mètode d'autenticació. A la majoria de les aplicacions web, el mètode per defecte és una contrasenya.

En aquest punt, cal recordar que l'**autenticació no és el mateix que l'autorització**. L'autenticació verifica la identitat de l'usuari, utilitzant algun mètode com a contrasenya. D'altra banda, l'autorització permet o denega l'accés a algun recurs d'acord amb algun criteri, com ara la identitat d'un usuari a través de l'identificador de sessió. La primera vegada que facem servir un servei, farem el següent:

1 | Registre

- Per crear un compte, introduïm les dades necessàries.
- Establim el mètode d'autenticació, normalment una contrasenya.

2 | Autenticació

- Per accedir al compte, ens identificam.
- L'aplicació web verifica la nostra identitat **autenticant-nos** amb el mètode escollit durant el registre.
- El servidor instal·la una galeta de sessió al nostre navegador.

ETS QUI DIUS QUE ETS? INTRODUCCIÓ A L'AUTENTICACIÓ

L'autenticació és el procés de verificar la identitat. Per fer això al món digital, hi ha diversos mètodes, tots basat en algun dels tres tipus principals: alguna cosa que soc, alguna cosa que sé o alguna cosa que tenc.

e.digitall.org.es/A4C41A2V06

3 | Accés als recursos web

- Un cop hem entrat al nostre compte, consultem la informació privada. Per exemple, els nostres missatges de xarxa social.
- Per accedir als missatges, el navegador **envia la petició amb la galeta de sessió**.
- El servidor ens identifica i autoritza la petició d'accés al recurs privat: els nostres missatges de la xarxa social.

4 | Tancar sessió

- El servidor oblida l'identificador i el navegador l'elimina.
- En fer les peticions, el servidor denega l'accés i ens obliga a tornar-nos a autenticar.

Aquest procés és comú a la majoria de les aplicacions web. Tot i això, hi ha casos concrets en cadascuna. La diferència principal és el mètode d'autenticació emprat.

Com recordaràs, el més segur és fer servir més d'un mètode d'autenticació. Molts serveis permeten fer servir **autenticació multifactor** (MFA) o un **segon factor d'autenticació** (2FA). Per exemple, al costat de la contrasenya, podem fer servir codis TOTP amb un generador de codis en una aplicació, o una clau de seguretat. D'aquesta manera, si un atacant aconsegueix la contrasenya, també hauria d'aconseguir accés al segon factor d'autenticació.

Per acabar, si perdem accés al compte, el més habitual és que el servei ens permeti **recuperar el compte** enviant un correu electrònic a l'adreça que hàgim registrat. Una altra opció comuna és descarregar uns codis d'un sol ús, coneguts com a **codis de recuperació**.

⚠ ATENCIÓ

Procura mantenir el teu compte de correu electrònic protegit! Si un atacant es fa amb la contrasenya, podria utilitzar la funcionalitat de recuperació del compte per obtenir accés a altres serveis.

AUTENTICACIÓ BASADA EN TOKENS: ALGUNA COSA QUE TENC

L'autenticació multifactor es pot basar en una cosa que posseïm físicament, un token. En són exemple les claus de seguretat, els codis TOTP o els codis SMS. Tots permeten millorar la seguretat dels nostres comptes quan es fan servir conjuntament amb un altre mètode.

e.digitall.org.es/A4C41C1V07

Seguretat

Nivell B1 4.1 Protecció de dispositius

Cyber Kill Chain

Cyber Kill Chain

Actualment, els ciberatacs són cada cop més comuns i sofisticats. Per poder-nos-hi defensar eficaçment en contra, és fonamental comprendre el procés que els atacants utilitzen per comprometre els sistemes. En aquest document, s'explicarà detalladament el concepte Cyber Kill Chain, i analitzarem un atac d'exemple per mostrar com s'apliquen les diferents fases.

El 2020, l'empresa SolarWinds va patir un ciberatac altament sofisticat que va permetre als atacants accedir als sistemes de milers d'organitzacions, d'agències governamentals i de grans empreses a tot el món. L'atac es va dur a terme seguint les set fases de la Cyber Kill Chain.

Fases del Cyber Kill Chain

El Cyber Kill Chain té set fases diferents. Les primeres fases corresponen amb la preparació de l'atacant i les últimes amb l'explotació i l'objectiu final de l'atac.

> ***Saber-ne més***
>
> Podeu trobar informació del Cyber Kill chain i les seves aplicacions en diferents organismes especialitzats en ciberseguretat. Per exemple, a l'INCIBE: *e.digitall.org.es/fases-ciberataque*

1 | Reconeixement
La primera fase vol estudiar l'objectiu de l'atac. A l'exemple, els atacants van començar investigant SolarWinds i els seus clients. Van utilitzar tècniques de cerca en línia per identificar possibles vulnerabilitats i objectius, i van recopilar informació sobre els sistemes i la xarxa de SolarWinds.

2 | Preparació
A continuació, es creen les armes o programari maliciós necessari per a l'atac. En l'exemple, els atacants van crear un codi maliciós personalitzat anomenat SUNBURST que va ser integrat en una actualització de programari de SolarWinds. L'objectiu d'aquesta actualització era distribuir-la als clients de SolarWinds i permetre als atacants obtenir accés no autoritzat als seus clients sistemes.

3 | Lliurament

Un cop creada l'arma, és el moment de cercar el vector d'atac i fer el lliurament del programari maliciós (malware). A l'exemple, els atacants van utilitzar una tècnica anomenada "supply chain attack" per distribuir el codi maliciós creat per ells mateixos. En lloc d'atacar directament les víctimes, els atacants van comprometre un proveïdor de programari de confiança (en aquest cas, SolarWinds) i van distribuir el codi maliciós a través de les seves actualitzacions de programari.

4 | Explotació

Les vulnerabilitats trobades a la primera fase pels atacants són explotades en aquesta fase. A l'exemple, una vegada que el codi maliciós es va instal·lar en els sistemes dels clients de SolarWinds, els atacants van començar a explotar les vulnerabilitats en els sistemes per obtenir control total. Van utilitzar tècniques d'engany per obtenir informació d'inici de sessió i credencials dels empleats i van fer servir eines de penetració per accedir a la xarxa interna.

ELS SISTEMES INFORMÀTICS NO SÓN PERFECTES: VULNERABILITATS

Les vulnerabilitats són fallades dels sistemes informàtics que poden ser explotades pels atacants. Quan una vulnerabilitat es descobreix, s'anomena 0-day. Per arreglar-les, els fabricants dissenyen i els apliquen com a actualitzacions.

e.digitall.org.es/A4C41B1V04

5 | Ordre i control

Quan ja s'ha obtingut accés al sistema víctima, els atacants no perden el control de l'arma. En aquesta fase, es comuniquen amb la víctima infectada usant servidors coneguts com a "Command & Control" (C2). En aquest exemple, els atacants van instal·lar eines addicionals per mantenir l'accés a llarg termini i el control sobre els sistemes compromesos. També van fer servir tècniques d'evasió per ocultar la seva activitat i evitar ser detectats pels sistemes de seguretat.

6 | Acció sobre els objectius

Finalment, s'executa l'atac d'acord amb l'objectiu principal dels atacants. A l'exemple, l'objectiu final dels atacants era l'extracció d'informació confidencial. Quan van tenir accés als sistemes compromesos, els atacants van descarregar i van extreure dades delicades, informació governamental i empresarial altament confidencial.

Per què es fa servir Cyber Kill Chain

El ciberatac a SolarWinds va ser un exemple molt sofisticat d'un atac cibernètic que segueix les fases de la Cyber Kill Chain. L'atac subratlla la importància de mantenir una postura de seguretat sòlida i estar alerta davant de possibles amenaces en línia. A més, també ressalta la importància d'enfortir la cadena de subministrament i la necessitat de realitzar controls rigorosos a tots els proveïdors de programari i serveis per mitigar els riscos dels ciberatacs.

El concepte de Cyber Kill Chain és un marc útil per entendre com els atacants poden comprometre sistemes i quines mesures podem prendre per defensar-nos. És important tenir en compte que cada atac és únic i que les diferents fases poden ser més o menys rellevants depenent de la situació. En comprendre com funciona el Cyber Kill Chain, podem millorar la nostra postura de seguretat en línia i estar millor preparats per detectar i respondre a possibles ciberatacs.

Seguretat

Nivell B1 4.1 Protecció de dispositius

Els algorismes a les xarxes socials

Els algorismes a les xarxes socials

A l'era digital, les xarxes socials han transformat la manera com ens relacionam, comunicam i consumim informació. Darrere d'aquesta revolució tecnològica hi ha els algoritmes: sistemes intel·ligents que processen i analitzen enormes quantitats de dades per oferir-nos contingut personalitzat.

Tot i això, l'impacte d'aquests algoritmes en els usuaris i en la gestió de la informació **planteja desafiaments i preocupacions en termes de privadesa, biaixos i manipulació**.

Ja hem vist alguns dels problemes amb la privadesa i la gestió de la informació en xarxes socials, com són la petjada digital, la reputació, i l'accés a la informació de les fonts obertes (OSINT). A continuació, s'explicaran els algoritmes a les xarxes socials, la seva influència en els usuaris i com aquests algorismes gestionen la informació.

La influència dels algorismes en els usuaris

En el context de les xarxes socials, els algorismes són un aspecte clau per gestionar la gran quantitat d'informació que l'usuari pot veure. Aquests algoritmes tenen la capacitat de personalitzar el contingut que es mostra a cada usuari, i l'adapten als seus interessos i preferències.

No obstant això, aquesta personalització pot portar a la formació de **bombolles d'informació** on els usuaris són exposats únicament a informació i opinions similars a les seves. Les bombolles d'informació poden fomentar la polarització i limitar la diversitat de perspectives.

Saber-ne més

La influència dels algorismes i els biaixos d'informació a les xarxes socials són un tema que es troba en debat públic. El documental ***El dilema de les xarxes socials*** (thesocialdilemma.com) mostra l'impacte d'aquests biaixos d'informació a la societat.

OSINT: LA INFORMACIÓ DE FONTS OBERTES

Document referenciat: ***A4C41A2D01***

PRIVACITAT, EMPREMTA DIGITAL I REPUTACIÓ EN LÍNIA

Document referenciat: ***A4C41A2D02***

Una de les representacions més grans del poder dels algorismes i de la segmentació de la informació és la manipulació de masses o les campanyes polítiques altament personalitzades. **El cas de *Cambridge Analytica* és possiblement el més conegut, en el context de les eleccions presidencials dels Estats Units el 2016**. Aquesta empresa, dedicada a les campanyes polítiques, va tenir accés a dades recopilades per Facebook sense el consentiment adequat. Gràcies a aquesta informació, va utilitzar perfils psicològics detallats per dirigir informació esbiaixada i de campanya política de manera molt personalitzada.

Aquest incident va generar gran controvèrsia en relació amb la privadesa de les dades a les xarxes socials i va plantejar preocupacions sobre la manipulació de la informació i els biaixos algorítmics.

Saber-ne més

El documental *El Gran Hackeig*, de Jehane Noujaim i Karim Amer (estrenat el 2019) tracta el cas de Facebook amb Cambridge Analytica.

Com les xarxes socials gestionen la informació

La influència dels algorismes és possible a causa de la gran quantitat de dades que els algorismes recopilen sobre els usuaris. Això és a causa del **model de negoci de les xarxes socials**, els clients de les quals són les empreses publicitàries, i el producte és la mateixa plataforma de publicitat dirigida: la xarxa social.

Entre una altra, la informació recopilada sobre els usuaris pot ser:

- **Dades demogràfiques:** els algorismes poden tenir accés a informació com l'edat, el gènere, la ubicació geogràfica, l'idioma i l'ocupació de l'usuari.

- **Comportament a la xarxa social:** els algorismes registren l'activitat de l'usuari a la plataforma, com els perfils que es visiten, les publicacions que es fan clic, els "m'agrada" que es donen i els comentaris que es fan.

- **Interaccions socials:** els algoritmes analitzen les connexions socials de l'usuari, com els seus amics, seguidors i persones amb qui interactua amb més freqüència.

- **Historial de navegació:** en alguns casos, els algorismes poden rastrejar l'historial de navegació de l'usuari dins i fora de la plataforma de xarxes socials, usant galetes de tercers, per exemple.

- **Dades de dispositius:** els algorismes també poden recopilar informació sobre el dispositiu que s'utilitza per accedir a la plataforma, com ara el tipus de dispositiu, el sistema operatiu i la resolució de pantalla.

És molt important tenir en compte tota la informació que les xarxes socials són capaces de recopilar sobre els usuaris, i ser-ne conscients. Hem de limitar què compartim a les xarxes socials, com les fem servir i revisar periòdicament les configuracions de privadesa, ja que són la clau per fer-ne un bon ús i minimitzar la capacitat d'influència dels algorismes.

Seguretat

Nivell B1 4.1 Protecció de dispositius

Metodologies de gestió de riscos

Metodologies de gestió de riscos

Metodologies de gestió de riscos

Característiques principals

Per ajudar-nos a guiar el procés de gestió de riscos amb més garanties d'assolir els objectius desitjats apareixen diferents metodologies.

NOTA

Metodologia de gestió de riscos: conjunt de processos i tècniques utilitzades per identificar, avaluar i mitigar els riscos que puguin afectar una organització o projecte.

Saber-ne més

La metodologia de gestió de riscos és essencial per garantir la continuïtat de l'operació de l'organització i maximitzar la probabilitat d'èxit i d'assoliment dels seus objectius.

GESTIÓ DE RISCOS: ACTIU, PROBABILITAT I IMPACTE

La gestió de riscos és el procés d'identificar, analitzar i avaluar els riscos potencials que poden afectar una organització i implementar les mesures preventives i de mitigació oportunes.

e.digitall.org.es/A4C41B1V02

Totes les metodologies de gestió de riscos haurien d'incloure a més de les fases ja comentades (identificació, valoració i priorització dels riscos) les de: planificació i implementació de la resposta, monitoratge contínua de l'evolució dels riscos i reportar-los a totes les persones interessades.

Cal tenir en compte que hi ha diferents metodologies de gestió de riscos i cadascuna pot ser més adequada per a certes indústries o per a diferents tipologies de riscos com poden ser riscos financers, operacionals, estratègics, legals, etc.

Atès que la temàtica relacionada amb aquesta formació és la seguretat de la informació es revisaran les següents metodologies que s'utilitzen en aquest marc:

- ***ISO 27005*** (*e.digitall.org.es/iso27005*)
- ***Magerit*** (*e.digitall.org.es/magerit*)
- ***OCTAVE*** (*e.digitall.org.es/octave*)
- ***NIST SP 800-30*** (*e.digitall.org.es/nistsp800-30*)
- ***FAIR*** (*fairinstitute.org/learn-fair*)

ISO 27005

L'ISO 27005 és una norma internacional desenvolupada per l'Organització Internacional de Normalització (ISO) revisada per darrera vegada l'any 2018.

Les principals característiques de l'ISO 27005 són el seu enfocament basat en el risc, la seva adaptabilitat a diferents tipus d'organitzacions, la seva estructura clara i fàcil de seguir, i la capacitat per integrar-se amb altres normes de seguretat de la informació com l'ISO 27001.

Inclou diferents eines com les matrius de risc, les llistes de control, les entrevistes amb experts i les anàlisis estadístiques.

Magerit

MAGERITv3 és una metodologia que es fa servir a Espanya desenvolupada per l'antic Consell Superior d'Administració Electrònica d'Espanya.

Com a punts forts de la metodologia MAGERIT podem destacar el catàleg d'elements que marca pautes pel que fa a tipus d'actius, dimensions de valoració, criteris de valoració, amenaces típiques i salvaguardes. Cal destacar també la guia de tècniques que proporcionen una orientació de com dur a terme projectes d'anàlisi i gestió de riscos.

Octave

Octave (*Operationally Critical Threat, Asset i Vulnerability Evaluation*) és una metodologia del Programari Engineering Institute (SEI) de la Universitat Carnegie Mellon. L'última versió disponible és Octave Allegro, que es va llançar el 2012.

Els punts forts de la metodologia Octave inclouen un enfocament centrat en els processos de negoci de l'organització i com la informació s'hi utilitza, un procés estructurat, un enfocament col·laboratiu d'equip i un alt grau de personalització.

Hi ha eines especialitzades per facilitar el procés de gestió de riscos, com el programari OCTAVE Allegro desenvolupat pel SEI.

NIST SP 800-30

El NIST SP 800-30 és una guia desenvolupada pel National Institute of Standards and Technology (NIST) dels Estats Units, sent la darrera revisió de setembre de 2021.

Les característiques fonamentals o punts forts del NIST SP 800-30 són la seva estructura, de 4 fases (preparació, avaluació, mitigació i comunicació), la seva adaptabilitat a les necessitats específiques de qualsevol organització i el seu origen basant-se en estàndards i millors pràctiques de la indústria.

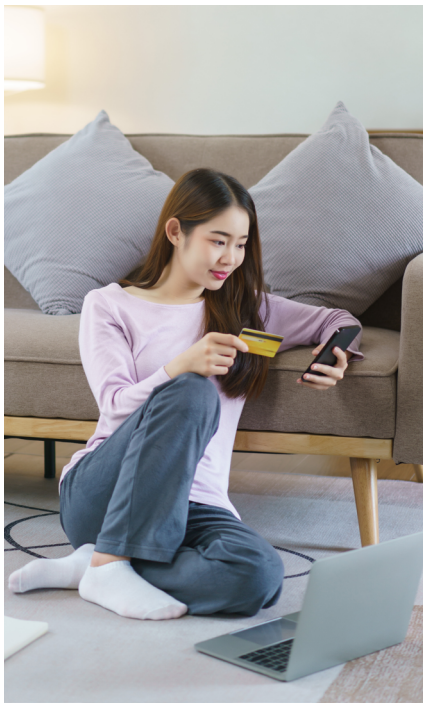
És important destacar que el NIST SP 800-30 és una guia de gestió de riscos i no prescriu eines específiques per implementar-les.

FAIR

FAIR (*Factor Analysis of Information Risk*) és un model desenvolupat per l'Open Group el 2006. La revisió actual és la 3.0 publicada l'abril de 2019.

És un model quantitatiu que utilitza tècniques d'anàlisi de dades i estadística per mesurar la probabilitat i l'impacte financer d'un risc de seguretat de la informació. FAIR es basa en un enfocament *bottom-up* que permet una avaluació precisa i objectiva del risc en el marc d'actius d'informació específics. És important destacar que s'integra fàcilment amb altres metodologies i marcs de ciberseguretat, com ara NIST o ISO.

Per implementar FAIR, hi ha diverses eines que permeten fer l'avaluació quantitativa dels riscos de seguretat de la informació, com ara RiskLens, FAIR-U i Open Fair.



PILAR

Es dedica un apartat especial a l'eina **Plataforma Integrada d'Anàlisi i Gestió de Riscos (PILAR)** (*e.digitall.org.es/pilar*) desenvolupada pel Centre Criptològic Nacional (CCN).

És una eina gratuïta i d'accés restringit, la utilització de la qual està subjecta a la sol·licitud prèvia i autorització prèvia per part del CCN-CERT.

PILAR està dissenyat per ajudar les organitzacions a identificar, avaluar i gestionar els riscos de seguretat de la informació de manera efectiva, seguint tant la metodologia MAGERIT com la metodologia ISO. Entre les principals característiques d'aquesta eina hi ha la capacitat per fer avaluacions de riscos tant qualitatives com quantitatives, la flexibilitat per adaptar-se a diferents tipus d'organitzacions i la capacitat per generar informes detallats dels resultats de les avaluacions.

Aquesta eina és una de les més utilitzades a Espanya per a la gestió de riscos de seguretat de la informació i és àmpliament reconeguda per la fiabilitat i la precisió en l'avaluació de riscos.

DigitAll

Seguretat

4.2
PROTECCIÓ DE LES DADES PERSONALS I LA PRIVACITAT

Seguretat

Nivell B1 4.2 Protecció de les dades personals i la privacitat

Atacs a la privacitat: Pesca

Atacs a la privadesa: pesca i pesca digital

Potser, una de les principals amenaces a la identitat digital és una de les modalitats de ciberatac conegut com a pesca (*phishing*). L'objectiu dels ciberdelinqüents és aconseguir les nostres dades personals i bancàries per suplantar la nostra identitat digital. D'aquesta manera poden robar els nostres diners, o influir com els altres ens veuen publicant comentaris en el nostre nom. Aquest tipus d'atac no és nou, es produeix des de fa molt de temps. Tot i això, amb les noves tecnologies digitals, ha incrementat enormement el seu nombre de víctimes i les formes de realitzar-se.

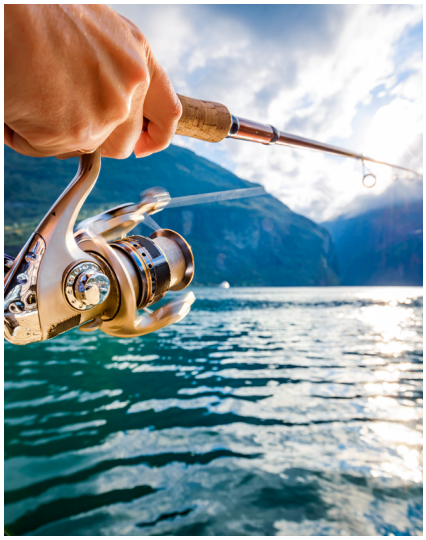
En aquest document s'explicarà en què consisteix l'atac de pesca, quines modalitats pot presentar, com podem identificar que som atacats i com ens podem protegir.

Què significa pesca?

Al diccionari de l'Institut d'Estudis Catalans no es troba una definició del terme pesca en aquest sentit. Tot i això, al diccionari terminològic TERMCAT sí que és acceptat quan es refereix al conjunt de tècniques o mètodes emprats pels delinqüents utilitzant el frau, l'engany i l'estafa per manipular les seves víctimes i fer que revelin informació personal confidencial. L'objectiu final és fer servir aquesta informació privada per suplantar la identitat digital de la víctima amb fins maliciosos.

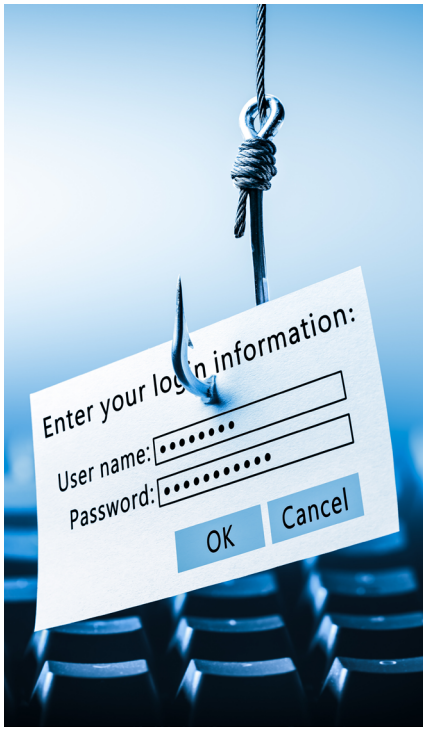
La informació que aquests delinqüents intenten aconseguir pot ser molt variada, per exemple, el nom dels nostres fills, el nostre número de seguretat social o dades bancàries com el número de la nostra targeta de crèdit. El problema és que moltes vegades és difícil saber l'efecte maliciós que pot produir que una determinada dada personal sigui coneguda. El terme en anglès *Phishing* s'origina a partir de la paraula *fishing*, que significa pescar.

El terme es fa servir com una metàfora de l'acte d'utilitzar un esquer per aconseguir que un peix (la víctima) piqui l'ham i sigui peix. De manera similar, als delinqüents que utilitzen aquest tipus d'atac se'ls anomenen "*phishers*".



El terme en anglès *Phishing* fa referència a l'activitat de pescar ("*fishing*" en anglès).

Funcionament de la pesca



Potser la millor manera de prevenir aquest tipus d'atac és conèixer com funciona. Independentment de la tècnica concreta utilitzada, els atacs de pesca segueixen un mateix patró:

1 | L'atacant inicia una comunicació amb la víctima, suplantant la identitat d'alguna organització o persona de confiança per a aquesta víctima. Per exemple, el banc, l'agència tributària, un amic, etc.

2 | En aquesta comunicació, l'atacant proporciona un esquer. Per exemple, "has d'actualitzar la informació de la targeta xxxxx", "tens una multa pendent de pagar del cotxe amb matrícula yyyyy" o "t'ha tocat un premi".

3 | La víctima pica l'esquer i proporciona alguna informació confidencial confiada que està fent el que és correcte. Per exemple, dona una contrasenya, un número de compte, etc.

A l'època anterior a Internet, les maneres d'iniciar la comunicació eren principalment una trucada telefònica, una carta o una visita al nostre domicili. No obstant això, avui dia, a l'era digital, les maneres en què els atacants poden començar aquesta comunicació poden ser molt variades. Potser les més conegudes són un correu electrònic o un missatge de text al mòbil.

Els atacants utilitzen tècniques conegudes com a enginyeria social, que són el conjunt de tècniques que fan servir els ciberdelinqüents per guanyar-se la confiança de l'usuari i així per confeccionar un esquer atractiu per a la seva víctima (*e.digitall.org.es/ingenierial-social*). En més vegades de les desitjables, serà la mateixa víctima la que faciliti tot el que és necessari per confeccionar aquest atractiu esquer, ja que ella mateixa ha publicat massa informació privada, per exemple, als estats d'una xarxa social.

Saber-ne més

Es recomana visionar el vídeo (*e.digitall.org.es/experimento-social*) per fer-se una idea de la quantitat d'informació privada que es publicita a Internet i que els "phishers" poden utilitzar per confeccionar esquers atractius.

Efectes de la pesca

Ser víctima de pesca pot tenir efectes desastrosos. Un atacant que es pogués fer amb la contrasenya per accedir al banc de la víctima podria ordenar transferències. Si la contrasenya és del perfil de la víctima en una xarxa social, podria afectar la seva identitat digital fent comentaris per desacreditar-la o, fins i tot, servir com a base per atacar una segona víctima.

AUTENTICACIÓ MULTIFACTOR

Hi ha tècniques com la identificació multifactor que permeten protegir-se fins i tot si és víctima d'un robatori de contrasenya.

e.digitall.org.es/A4C41A2V07

Si la víctima és una empresa o entitat pública, els efectes de pesca poden ser encara més desastrosos, ja que pot provocar una fugida massiva de dades privades tant dels empleats com dels clients o usuaris. Moltes vegades, la situació encara és pitjor perquè no es fa públic l'atac sofert i això impossibilita a les possibles víctimes col·laterals poder adoptar mesures per protegir-se com, per exemple, canviar la contrasenya.

AUTENTICACIÓ: GESTIÓ DE CONTRASENYES

Per evitar el problema de ser víctima col·lateral d'un atac a una empresa o entitat, es recomana utilitzar una contrasenya segura diferent per a cada empresa o entitat on estigui registrat.
e.digitall.org.es/A4C41B1V08

Tipus de pesca digital

Com ja hem comentat, la pesca en aquest sentit és una tècnica utilitzada abans que existís Internet. Amb l'arribada d'Internet i les tecnologies digitals, han aparegut noves modalitats de pesca que utilitzen aquestes tecnologies.

Aquest document se centra en les modalitats de pesca que utilitza alguna tecnologia digital i que s'anomenen genèricament com a pesca digital.

Pesca usant el correu electrònic

Potser és la modalitat de pesca digital més comuna. Els missatges de correu electrònic s'utilitzen per lliurar l'esquer a les víctimes. Aquests missatges solen contenir enllaços que porten fins a llocs web maliciosos o arxius adjunts infectats amb programes malignes (coneguts com a programari maliciós o "*malware*").

Com que el cost d'enviar un correu electrònic és sovint zero, el més comú és que s'utilitzi un mateix missatge que s'envia de manera massiva a milers d'usuaris. Aquí l'esquer sol ser groller, però l'esperança de l'atacant és que piquin un petit percentatge de víctimes.

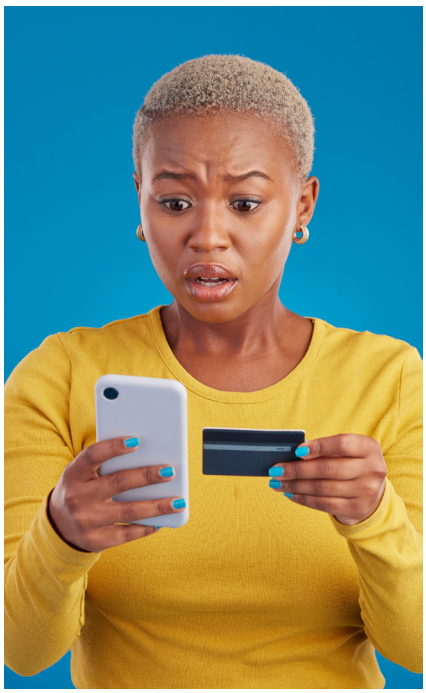
Altres vegades l'atac és més especialitzat aprofitant alguna campanya publicitada d'una empresa, o algun missatge acabat enviat a tots els clients. En aquest cas es remet una còpia modificada del missatge anterior amb enllaços maliciosos. En aquesta modalitat és més difícil detectar que és un atac.

Pesca usant el web

En aquesta modalitat, l'atacant crea una còpia exacta d'un lloc web. D'aquesta manera, la víctima quan accedeix a la còpia maliciosa es confia i proporciona la informació privada que l'atacant desitja, normalment, la contrasenya per autenticar-se.

Una altra tècnica que poden fer servir els delinqüents és injectar codi maliciós en un lloc web. D'aquesta manera, la víctima en accedir al lloc web legítim, en estar modificat pels atacants, de nou pot proporcionar la informació privada sense saber-ho. Un exemple recent han estat les finestres emergents per introduir les credencials d'inici de sessió.

També és coneguda una altra tècnica on els atacants creen pàgines web on publiciten productes a molt baix cost. Això pot provocar que els cercadors web dirigeixin a les potencials víctimes cap a aquestes pàgines on, com és lògic, hauran de proporcionar molta informació confidencial per fer la suposada compra. Exemples han estat pàgines de falsos bancs publicitant préstecs amb baix interès o targetes de crèdit sense comissions.



Pesca per veu

En aquest mode, l'atacant utilitza una trucada telefònica. El terme pesca per veu o *vishing* prové de contraure els termes "*voice phishing*". En aquest tipus d'atac, el delinqüent se sol camuflar com a treballador d'alguna empresa o entitat de prestigi. No és estrany que, fins i tot, hagi estudiat els perfils de les xarxes socials de les seves víctimes per proporcionar informació suposadament privada durant la trucada. Això fa que la víctima baixi el seu estat d'alerta i se'n confiï. A continuació, el delinqüent sol·licitarà la informació privada que realment voleu.

Pesca per SMS

En aquesta modalitat, l'atacant utilitza un missatge SMS. El terme "*smishing*" prové de la contracció dels termes "sms phishing". Aquesta modalitat d'atac és similar a la que utilitza correu electrònic. Normalment, la víctima rep un missatge de text on se li demana que premi sobre un enllaç o descarregueu una aplicació. No obstant això, en fer-ho se us enganya perquè descarregueu al telèfon una app maliciosa que pot captar la vostra informació personal i enviar-la a l'atacant. De nou és molt comú que aquests tipus d'atacs coincideixin amb campanyes generals com ara les campanyes per fer la declaració de la renda de les persones físiques a l'Agència Tributària.

Pesca usant les xarxes socials

En aquesta modalitat, els delinqüents utilitzen tota la informació privada que es publica a les xarxes socials per intentar segrestar el perfil de la víctima i forçar-la a enviar enllaços maliciosos als seus amics. D'aquesta manera, els amics es converteixen en víctimes alhora. Altres delinqüents creen perfils falsos simulant ser altres persones i els utilitzen per enganyar les víctimes intentant influir-hi.

Principals recomanacions per prevenir ser víctima de pesca digital

Ara que s'han mostrat les principals modalitats de pesca digital, és hora de donar algunes pautes per prevenir-ho.

Pautes per prevenir ser víctima de pesca.

1 | **Cal que cerqueu formació.** És el que esteu fent en llegir aquest document. L'**Oficina de Seguretat de l'Internauta** (*incibe.es/ciudadania*) és una bona font per ampliar la seva formació i estar al dia de les darreres estafes conegudes.

2 | **Heu de tenir el vostre programari actualitzat.** Un element clau és utilitzar eines actualitzades a la seva darrera versió, en especial, el navegador web. Els navegadors web moderns tenen tecnologies capaces de detectar i prevenir moltes de les tècniques que utilitzen els delinqüents per robar informació privada.

3 | **Cal que sigueu descregut.** És millor pecar per prudent davant de qualsevol correu electrònic. Amb els enllaços, confirmeu que us connecten amb els llocs web que diu el text. Una tècnica és llegir sempre els correus en mode text pla. D'aquesta manera veureu les adreces reals dels enllaços o si hi ha enllaços "camuflats" en imatges o logos. Si hi ha aplicacions penseu primer si veritablement és necessari descarregar-les. A més, com a regla general mai instal·leu aplicacions que no siguin oficials en el sistema operatiu que utilitzeu: Google Play, Microsoft Store, Apple Store, etc.

4 | **Heu de confirmar abans d'actuar.** Avui dia la majoria de les empreses mai sol·liciten als seus clients informació privada mitjançant correu electrònic o trucades telefòniques. Si fos el cas, cal que esborreu el missatge o que pengeu i confirmeu vosaltres mateixos amb l'empresa si aquesta sol·licitud és real. Per exemple, en comptes de prémer sobre l'enllaç d'un correu electrònic per connectar-vos al vostre banc, heu d'iniciar la connexió directament usant el navegador introduint l'adreça web. Si és una trucada, posau-vos en contacte amb el vostre banc preguntant si és real la campanya per la qual ha estat cridat.

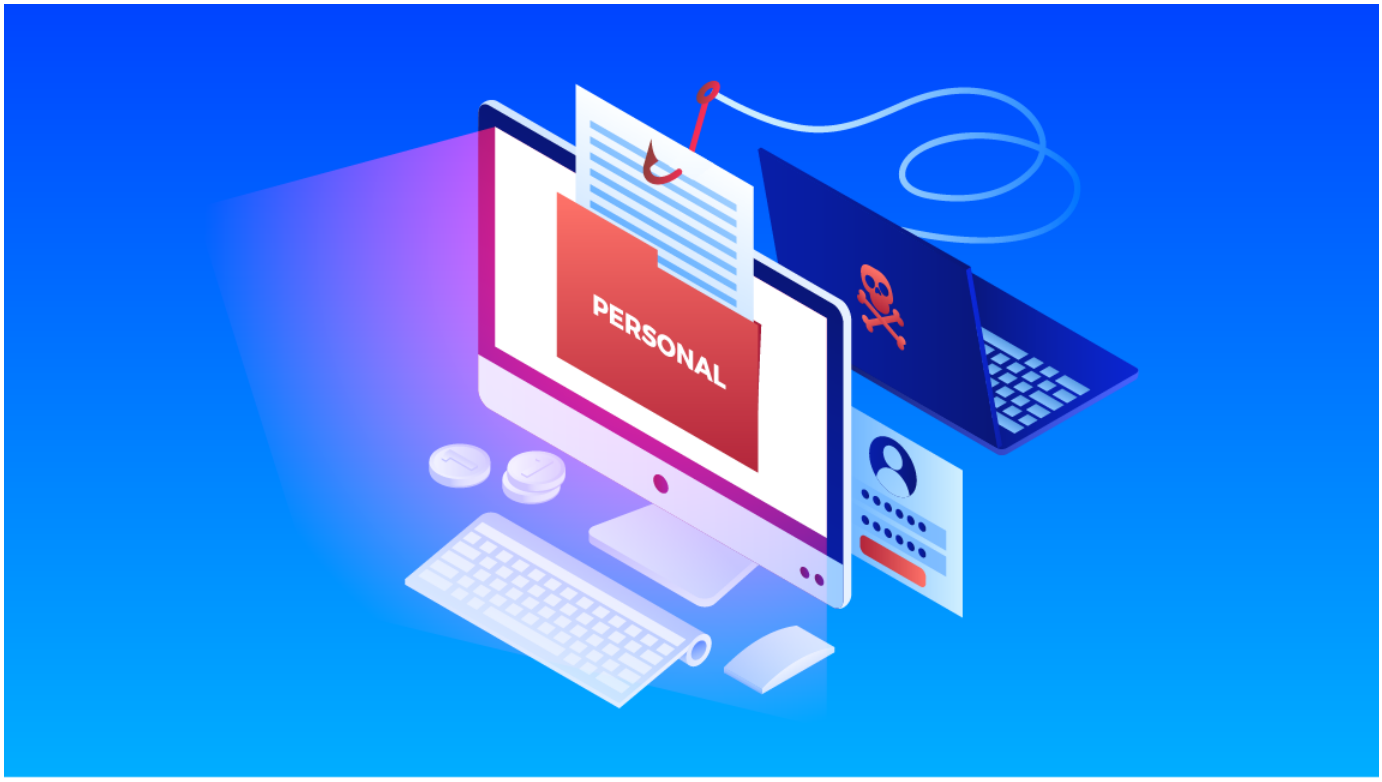
5 | Utilitzau un gestor de contrasenyes. Si una empresa pateix una bretxa de seguretat, és possible que els vostres clients quedin indefensos si utilitzen per exemple una mateixa contrasenya basada en alguna de les dades personals que han quedat compromeses, per exemple, la data de naixement. El recomanable és utilitzar una contrasenya forta diferent a cada lloc web on estiguem registrats. Per gestionar totes les contrasenyes farem servir un gestor de contrasenyes. La majoria dels navegadors web moderns incorporen un gestor de contrasenyes, encara que també hi ha programari especialitzat.

Saber-ne més

Oficina de Seguretat de l'Internauta. *incibe.es/ciudadania*

Experiment social - els riscos de les nostres dades personals a Internet. *youtu.be/3S7qFGVfsqM*

Enginyeria social. *incibe.es/aprendeciberseguridad/ingenieria-social*



Seguridad

Nivell B1 4.2 Protecció de les dades personals i la privacitat

FAQs sobre l'ús adequat de les dades personals en àmbits concrets

FAQs sobre un ús adequat de les dades personals en àmbits concrets

És possible un consentiment tàcit per al tractament de dades personals?

No. El Reglament General de Protecció de Dades exigeix que el consentiment sempre sigui exprés. No constitueix consentiment el silenci, les caselles ja marcades o la inacció. Aquest Reglament exigeix que el consentiment es formuli "mitjançant un acte afirmatiu clar que reflecteixi una manifestació de voluntat lliure".

Un menor d'edat pot donar el vostre consentiment perquè les vostres dades siguin tractades per Facebook, TikTok, X, etc.?

Aquest tractament únicament es pot fundar en el consentiment del menor quan sigui més gran de 14 anys. El tractament de les dades dels menors de catorze anys, fundat al consentiment, només és lícit si consta el del titular de la pàtria potestat o tutela, amb l'abast que determinin els titulars de la pàtria potestat o tutela.

Es poden enviar els resultats acadèmics als pares o tutors sense el consentiment dels menors?

Sí. En aquest cas, el tractament que realitza la institució educativa és necessari per a la satisfacció d'un interès legítim d'un tercer, els pares o els tutors. Aquest interès legítim deriva de la pàtria potestat. Cal tenir en compte que l'article 154 del Codi Civil imposa als pares/tutors el deure d'educar i procurar una formació integral als fills i filles no emancipats.

Respondre les preguntes en una entrevista de feina equival a un consentiment per al tractament?

No. És habitual que durant una entrevista de treball, el candidat respongui nombroses preguntes que contenen dades de caràcter personal (la seva opinió d'un assumpte, les seves aficions, les seves perspectives de futur, la seva situació familiar, etc.). La resposta a aquestes preguntes no equival a un consentiment per al tractament de dades personals.

A més, el fet de sotmetre el candidat a preguntes familiars i personals totalment alienes a la feina que s'exercirà suposa una conducta contrària als deures de minimització de dades i limitació de la finalitat.

NOTA

Constitueix infracció administrativa molt greu «Sol·licitar dades de caràcter personal en els processos de selecció..., que constitueixin discriminacions per a l'accés a l'ocupació per motius de sexe, origen, inclòs el racial o ètnic, edat, estat civil, discapacitat, religió o conviccions, opinió política, orientació i identitat sexual, expressió de gènere, característiques sexuals, afiliació sindical, condició social i llengua dins de l'Estat» [art. 16.1.c) Text refós de la Llei d'Infraccions i Sancions a l'Ordre Social].

L'ocupador pot accedir a la informació mèdica del treballador obtinguda pels serveis de prevenció?

No. La Llei de prevenció de riscos laborals obliga l'empresari a garantir als seus treballadors una vigilància periòdica del seu estat de salut en funció dels riscos inherents a la feina. La regla general és que aquesta vigilància només es pot dur a terme quan el treballador presta el seu consentiment. L'accés a aquesta informació mèdica de caràcter personal i especialment protegida es limitarà al personal mèdic i a les autoritats sanitàries que duguin a terme la vigilància de la salut. No es pot facilitar a l'empresari o a altres persones sense consentiment exprés del treballador.

L'empresari només serà informat de les conclusions que es derivin dels reconeixements efectuats en relació amb l'aptitud del treballador per a l'exercici del lloc de treball.

És legal rebre trucades publicitàries?

Depèn. D'acord amb la Llei General de Telecomunicacions, es poden distingir dos supòsits:

- Les **trucades automàtiques**, és a dir, en què no hi ha una intervenció humana, requereixen consentiment previ i informat per part de l'abonat perquè es realitzin.

- Les **trucades en què intervé una persona** són legals, llevat que l'abonat hagi manifestat la seva oposició a la recepció.

PROTECCIÓ DE DADES I ÀMBITS PARTICULARS

Es va exposar com protegir-te de la publicitat no desitjada.

e.digitall.org.es/A4C42C1V08

Es poden fer imatges o gravar vídeos en esdeveniments escolars?

Seguint les directrius de l'Agència Espanyola de Protecció de Dades, quan es tracti d'esdeveniments organitzats pel centre escolar, cal distingir:

a) Si l'esdeveniment respon a l'exercici de la funció educativa del centre (per ex., una funció de teatre programada a l'assignatura de literatura), la utilització de les dades s'entendria emparada a la Llei orgànica d'educació. Per tant, no cal el consentiment.

b) Si es tracta d'un esdeveniment al marge de la funció educativa que compleix el centre escolar (per ex., una festa de Nadal o de disfresses):

- Si és el centre escolar el que procedeix a l'enregistrament de les imatges haurà d'informar els interessats, els mateixos menors si tenen més de 14 anys i, si fossin més petits, els seus pares o tutors, de la finalitat de l'enregistrament de les imatges i de la difusió que se'n pretén fer (si seran publicades en pàgines web, en xarxes socials, ...) i sol·licitar-ne el consentiment.

- Si la presa d'imatges la fan els familiars dels alumnes i el seu ús és exclusivament personal o domèstic, estaria fora de l'àmbit d'aplicació del Reglament General de Protecció de dades. Tot i això, la divulgació fora d'aquest àmbit d'imatges de persones sense el seu consentiment a tercers, per exemple, la publicació de les imatges en xarxes socials "en obert", constitueix un tractament de dades que sí que necessitaria del consentiment dels afectats, ja que en aquest cas, li seria aplicable la legislació de protecció de dades.

Un centre d'educació infantil pot instal·lar un sistema de videovigilància a les aules?

No. Segons l'informe 475/2014 de l'Agència Espanyola de Protecció de Dades, la instal·lació d'un sistema de videovigilància per controlar el personal laboral és desproporcionada, ja que això es pot aconseguir mitjançant mecanismes menys agressius i intrusius. En definitiva, s'estaria vulnerant el principi de minimització de dades. A aquests efectes seria indiferent que existís el consentiment dels pares (per les imatges dels seus fills) i fins i tot del personal laboral.

Sí que es podria instal·lar aquest sistema davant d'una situació concreta d'incompliments laborals molt greus o una altra finalitat que en fes proporcional l'ús.

Un òrgan administratiu pot publicar un acte administratiu (per ex., llistat d'admesos a un concurs oposició) on aparegui el DNI complet?

No. La Llei Orgànica de Protecció de Dades personals i garantia dels drets digitals, estableix que quan sigui necessària la publicació d'un acte administratiu que contingués dades personals de l'afectat, s'hi identificarà mitjançant el seu nom i cognoms, afegint-hi quatre xifres numèriques aleatòries del document nacional d'identitat, número d'identitat d'estranger, passaport o document equivalent.

Com s'eliminen fotografies i vídeos d'Internet amb la nostra imatge?

La imatge és una dada personal, ja s'inclogui en una fotografia o en un vídeo. És habitual la presència de fotos i vídeos a internet sense que hi hagi una causa de legitimació per a aquest tractament. En aquests supòsits, per aconseguir aquesta eliminació cal exercir el dret de supressió davant del responsable del tractament.

Els prestadors de serveis a internet més populars disposen de mecanismes propis per exercir aquest dret:

Facebook:

- A través del servei d'ajuda: *e.digitall.org.es/ayuda-facebook*
- També a través de l'enllaç Denunciar, que apareix situat a la majoria dels continguts publicats.

Google:

- Formulari de sol·licitud de retirada de contingut: *e.digitall.org.es/contenido-google*

Youtube:

- A través de l'enllaç Denunciar, que apareix a sota del vídeo.
- Hi ha altres opcions de denúncia per reflectir de manera més precisa el problema: *e.digitall.org.es/denuncia-youtube*

X:

- En aquesta pàgina es recull la informació i els vincles: *e.digitall.org.es/denuncia-x*
- També es pot denunciar directament des d'un Tweet, Llista o perfil.

Instagram:

- En aquest enllaç es troba la informació corresponent *e.digitall.org.es/ayuda-instagram*

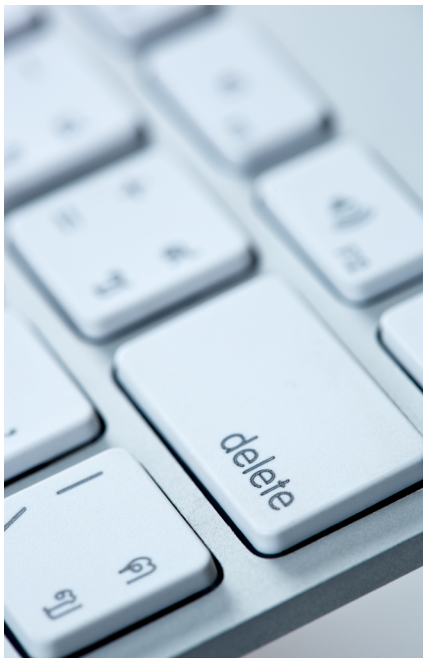
TikTok:

- En aquesta pàgina es facilita informació i enllaços segons el problema: *e.digitall.org.es/ayuda-tiktok*

Totes aquestes empreses i qualsevol altra han de resoldre sobre la sol·licitud de supressió en el termini màxim d'un mes a comptar des de la recepció. Transcorregut aquest termini sense que de manera expressa responguin a la petició o si l'interessat considera que aquesta resposta és insatisfactòria, es pot interposar la reclamació corresponent davant l'Agència Espanyola de Protecció de Dades, a través de la seva seu electrònica:
e.digitall.org.es/sede-electronica

Aquesta reclamació s'ha d'adjuntar a la documentació acreditativa d'haver sol·licitat la supressió davant de l'entitat de què es tracti.

Com s'eliminen continguts confidencials d'Internet?



L'Agència Espanyola de Protecció de Dades té un Canal Prioritari per a l'atenció de situacions excepcionalment delicades, quan els continguts (fotografies o vídeos) tinguin caràcter sexual o mostrin actes d'agressió i s'estiguin posant en alt risc els drets i les llibertats dels afectats. A aquest canal s'hi accedeix a través de la seu electrònica de l'Agència: e.digitall.org.es/seu-electronica: *e.digitall.org.es/sede-electronica*

La informació que es faciliti s'analitzarà de forma prioritària i, si escau, l'Agència Espanyola de Protecció de Dades ordenarà la retirada del contingut al prestador del servei o la plataforma on s'estigui difonent. A més, si hi ha indicis de delicte, ho posarà en coneixement de la Fiscalia.

DigitAll

Seguretat

4.3
PROTECCIÓ DE LA SALUT I EL BENESTAR

Seguretat

Nivell B1 4.3 Protecció de la salut i el benestar

Guia visual per utilitzar el control de temps dels dispositius

Guia visual per utilitzar el control de temps dels dispositius

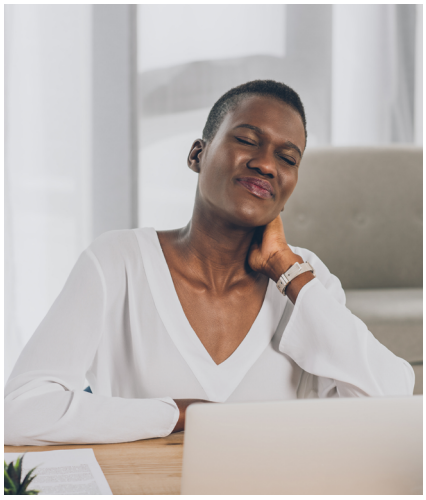
En aquest document es mostrarà una guia visual per utilitzar el control del temps dels dispositius començant amb una introducció sobre l'ús abusiu dels dispositius, seguit de la necessitat de controlar el temps i la repercussió sobre la salut i es mostraran diferents mètodes pel control del temps.

L'ús abusiu dels dispositius

Els dispositius electrònics com els mòbils, tauletes i ordinadors ocupen cada vegada més un lloc molt important a la vida diària de la gent. Avui dia, gairebé tothom en disposa i els fa servir amb regularitat, tant en un àmbit laboral com lúdic, familiar, entre d'altres.

Tot i que aquestes noves tecnologies han suposat un gran avenç en diversos àmbits i ens han facilitat la vida per bé, cal tenir en compte que també poden tenir un impacte negatiu sobre la nostra salut física i mental. Fer-ne un ús desmesurat pot ocasionar als usuaris alts graus d'addicció i dependència.

A més de l'addicció, aquest ús abusiu de les tecnologies pot causar conseqüències físiques, emocionals o socials a la persona que en fa ús. Les conseqüències més comunes solen ser insomni, ansietat, estrès, depressió, irritabilitat i dolors articulars i musculars, entre d'altres.

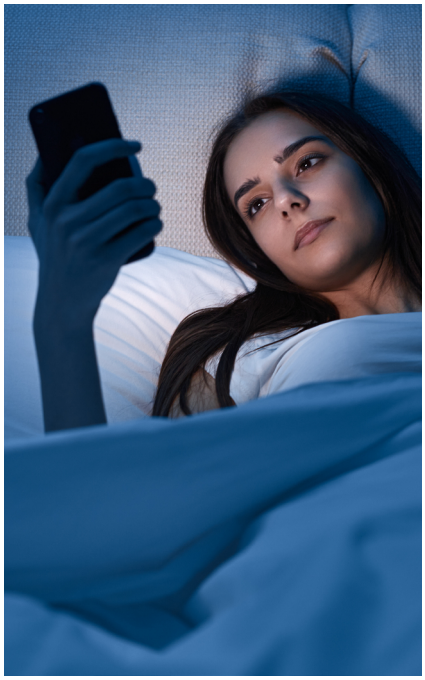


NOTA

A la pàgina web de Kapersky han publicat un article molt interessant sobre com l'ús de dispositius electrònics influeix en la salut dels usuaris. Se centra en diferents problemes com els musculoesquelètics, psicològics, la fatiga visual, influència negativa a l'hora de dormir...

Efectes de la tecnologia a la salut (e.digitall.org.es/kapersky)

La necessitat de controlar el temps



Per evitar la dependència de què parlem anteriorment, cal aprendre a desconnectar-se i a tenir un control conscient del temps que es passa fent ús dels dispositius.

És per això que és altament recomanable limitar l'ús dels dispositius electrònics al mínim temps possible i sempre que sigui estrictament necessari. Per dur a terme aquest control hi ha una sèrie d'aplicacions i de funcionalitats que permeten cronometrar el temps dedicat a l'ús de la tecnologia al llarg del dia.

A més d'això, hi ha una sèrie de recomanacions més senzilles que també poden ajudar a controlar i limitar millor l'ús desmesurat:

No mirar el telèfon mòbil o altres dispositius abans d'anar a dormir ni tampoc només aixecar-se, ja que repetir sovint aquestes accions fa que es converteixi en una rutina, cosa que porta a estar més hores amb els dispositius. A més, pot repercutir negativament en el descans i en l'estat d'ànim de l'usuari.

Saber-ne més

Usar durant molt de temps els dispositius electrònics abans d'anar a dormir afectarà la glàndula pineal, la qual és part del cervell que s'encarrega de produir melatonina, l'hormona que regula el cicle del nostre somni. Revisar constantment el mòbil abans d'anar a descansar ens farà perdre hores de son. Per això, l'ideal serà deixar el mòbil mitja hora abans, i allunyar-lo del nostre llit, perquè ens costi una mica més el fet de tornar-lo a agafar.

Deixar els dispositius en una cambra diferent de l'usuari, cosa que limitarà l'accés directe i propiciarà que se centri en altres tasques que tingui al davant. De la mateixa manera que l'exemple anterior, l'usuari no podrà veure notificacions, cosa que farà que no estigui subjecte a tants estímuls auditius ni visuals.

Mètodes per al control del temps

Pel que fa a les aplicacions i funcionalitats de control temps dedicat a l'ús de la tecnologia que anomenem a l'apartat anterior, destaquen:

Alarmes i cronòmetre

Fer ús de les alarmes o del cronòmetre dels mòbils, tauletes o wearables servirà per ser conscients del temps que es dedica a l'ús de la tecnologia. Aquestes avisen del temps que s'està usant o no el dispositiu, a més, el cronòmetre permet calcular el temps amb més exactitud.

En general, la majoria dels dispositius mòbils compten amb una app pròpia de Rellotge. Per accedir-hi i activar una alarma cal:

1 | Obrir l'app de Rellotge del telèfon.
2 | A la part inferior, premeu Alarma.
3 | Triar una alarma.
- Per afegir una alarma, premeu Afegeix.

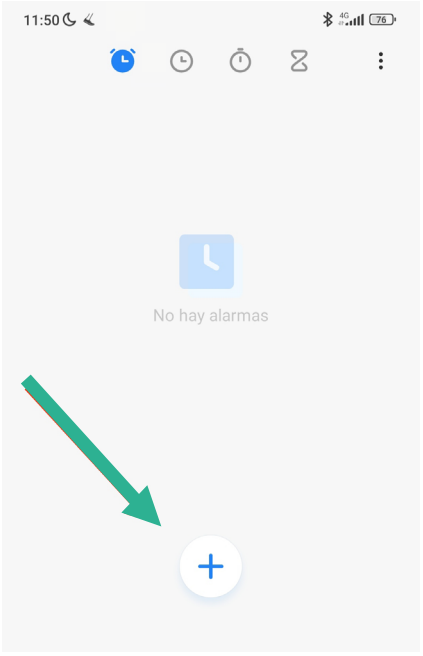
4 | Establiu l'hora de l'alarma.
- **Al rellotge analògic:** lliscar l'agulla fins a l'hora que vulgueu. Després, fer el mateix per trobar els minuts que es vulgui.
- **Al rellotge digital:** introduïu l'hora i els minuts que vulgueu.
- **Amb el format de 12 hores:** pressionar A.M. o P.M.

5 | Pressionar Aceptar.

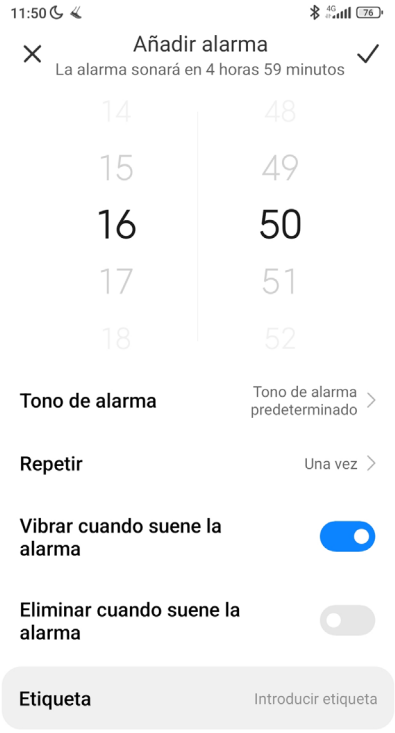
En cas de voler anul·lar aquesta alarma:

1 | Obrir l'app de Rellotge del telèfon.
2 | A la part inferior, premeu Alarma.
3 | A l'alarma corresponent, premeu la fletxa cap avall.
- **Cancel·lar:** si voleu cancel·lar una alarma programada per sonar en les dues pròximes hores, premeu Descartar.
- **Esborrar:** per treure l'alarma de forma permanent, premeu Esborrar.

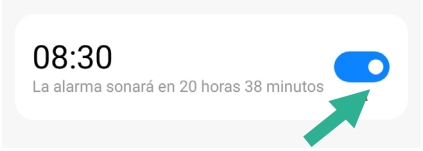
En altres casos l'alarma apareix amb un botó al costat, cosa que us permet activar-la i desactivar-la directament sense necessitat de seguir tot el pas 3.



Font: autoria pròpia.



Font: autoria pròpia.



Font: autoria pròpia.

Mode avió

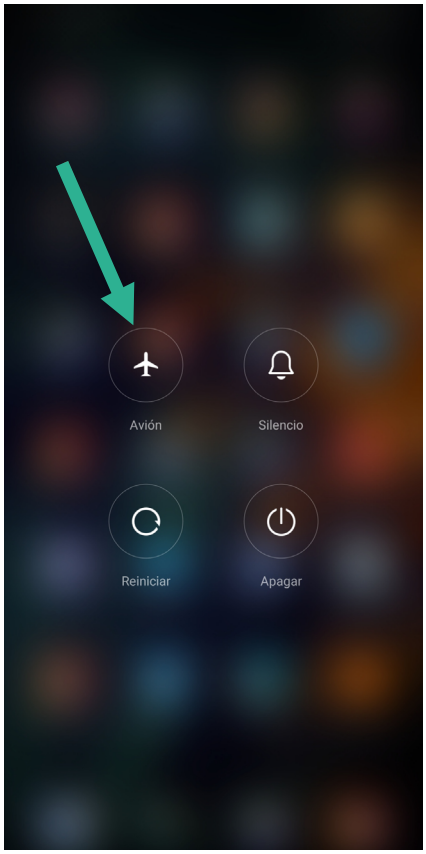
Usar el mode avió del telèfon o tablet per intentar limitar el temps d'ús, o mateix apagar durant un temps. El mode avió impedeix que el dispositiu rebi notificacions o trucades, de manera que l'usuari no estarà tan pendent d'aquests estímuls i us ajudarà a desconnectar.

Per accedir al mode d'avió d'un dispositiu mòbil es pot fer de tres maneres:

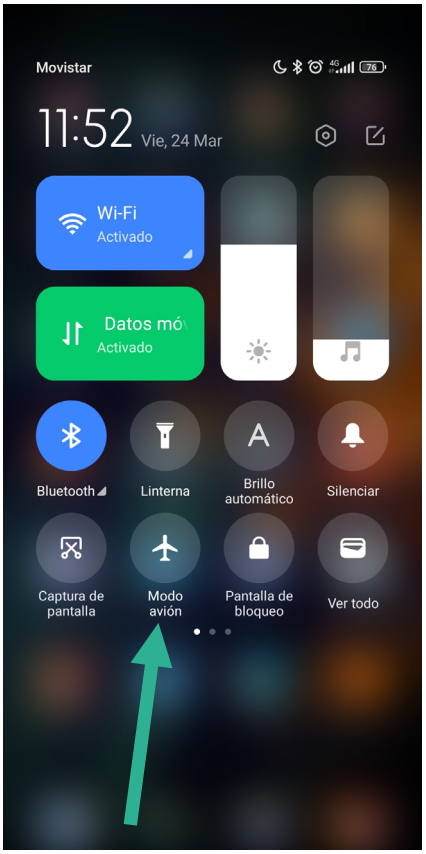
1 | Mantenint premut el botó d'apagat del dispositiu, el que farà que aparegui l'opció de manera avió. Aquí es pot activar i desactivar.

2 | Accediu a l'apartat de configuració del dispositiu. En general sol estar entre les primeres opcions de la llista, amb un botó d'apagat i encès al costat.

3 | A través de la barra de notificacions del dispositiu. Només cal baixar aquesta barra des de la part superior del dispositiu. També sol aparèixer entre les primeres opcions, i es pot activar i desactivar.



Font: autoria pròpia.



Font: autoria pròpia.

Benestar digital d'Android

És una aplicació nativa implementada en Android 9 que permet monitoritzar el temps que s'està usant cada app i també permet posar límits alhora que es passa a un web oa una app concreta.

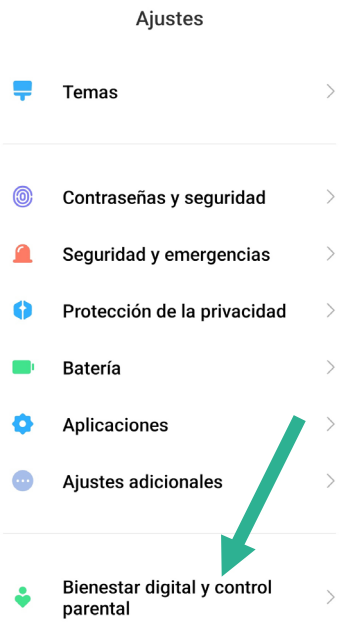
Altres fabricants com Huawei tenen també les seves pròpies aplicacions de Benestar Digital implementades als dispositius. En aquests casos, poden utilitzar el mateix nom o altres de diferents, com l'Equilibri digital de Huawei. Cadascuna d'aquestes opcions té la seva interfície i controls diferents.

En el cas de dispositius Android, per accedir a l'apartat de Benestar Digital cal:

1 | Entrar a l'opció de configuració del dispositiu mòbil.

2 | Seleccioneu l'opció de Benestar Digital i Control Parental. En altres casos, tal com es va esmentar amb anterioritat, podria aparèixer un altre nom com a Equilibri Digital.

3 | Un cop dins es podrà veure una gràfica amb el temps que s'ha utilitzat el dispositiu en general (temps d'ús); també es mostrarà l'aplicació que s'ha fet servir més durant aquest temps. A sota, es podrà veure un comptador amb el nombre de desbloquejos del dispositiu i la quantitat de notificacions que s'han rebut durant tot el dia.



Font: autoria pròpia.

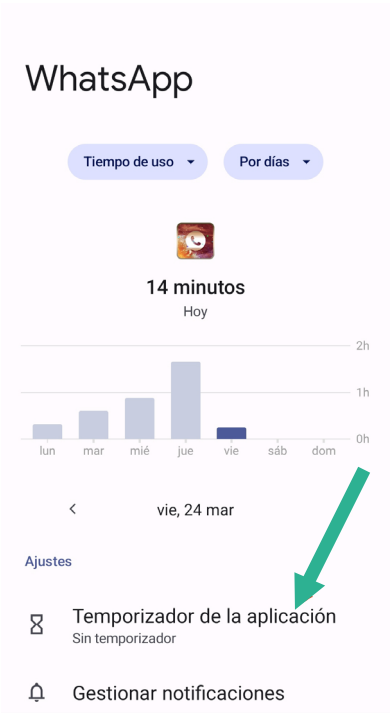
Font: autoria pròpia.

4 | Si feu clic sobre la quantitat de minuts que s'ha estat mirant el mòbil, a la pantalla apareixerà una llista del temps d'ús del dispositiu al costat de les apps que s'han fet servir, es podran veure totes les aplicacions que es van obrir i durant quant de temps . També es pot observar un gràfic comparatiu amb les dades de tota la setmana, i així es podrà consultar altres dies passats.

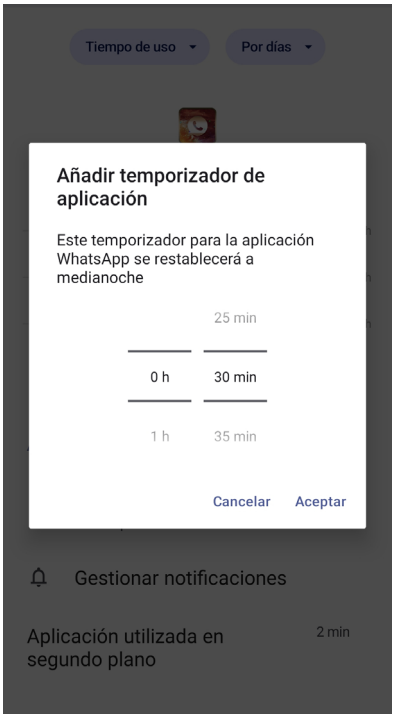
5 | Si feu clic sobre una de les aplicacions de la llista anterior, apareixerà una pantalla gairebé idèntica, però amb les dades úniques d'aquesta aplicació concreta. Així es pot saber quant s'utilitza cada app dia a dia. A sota hi ha les opcions per anar a la configuració de notificacions i el temporitzador de l'aplicació.

6 | Si feu clic a l'opció Temporitzador de l'aplicació, es podrà establir el temps màxim que Android permetrà utilitzar una app en concret. Així, si voleu limitar l'ús de les apps, quan s'arribi al temps establert, Android bloquejarà l'app.

Font: autoria pròpia.



Font: autoria pròpia.



Font: autoria pròpia.

NOTA

Un cop superat algun dels límits establerts l'aplicació en qüestió apareix ombrejada a la pantalla principal. I si decideixes accedir-hi apareix un cartell que et recorda el bloqueig establert, encara que sempre tens l'opció d'ignorar-lo

Saber-ne més

DEPENDÈNCIA, ÚS I ABÚS DELS DISPOSITIUS TECNOLÒGICS - Psicòloga Gloria Martínez Ayala. *https://psicologagloriamartinezayala.es/dependencia-uso-y-abuso-de-los-dispositivos-tecnologicos/*

Què és el mode avió i com activar-lo/desactivar-lo a Android? *https://androidspain.es/modo-avion/*

Com establir, cancel·lar o posposar alarmes - Ajuda d'Android. *https://support.google.com/android/answer/2840926?hl=es-419#zippy=%2Cc%C3%B3mo-establecer-la-hora-de-la-alarma*

Temps d'ús en Android: com saber quant de temps passes al mòbil i quines apps fas servir més. *https://www.xataka.com/basics/tiempo-uso-android-como-saber-cuanto-tiempo-pasas-movil-que-apps-usas*

Efectes de la tecnologia a la salut. *https://www.kaspersky.es/resource-center/preemptive-safety/impacts-of-technology-on-health*

Benestar digital a mòbils: com funciona el Temps d'ús a iPhone i iPad? | Blog Educació i Benestar digital. *https://gaptain.com/blog/bienestar-digital-en-moviles-como-funciona-el-tiempo-de-uso-en-iphone-y-ipad/*

Per què no hauries d'estar amb el mòbil abans de dormir. *https://www.movilzona.es/noticias/problemas/utilizar-movil-antes-dormir/*

DigitAll

Seguridad

4.4
PROTECCIÓ DEL MEDI AMBIENT

Seguretat

Nivell B1 4.4 Protecció del medi ambient

Hàbits de consum “e-corresponsable” de la tecnologia

Hàbits de consum "e-corresponsable" de la tecnologia

Introducció. El concepte "e-corresponsable"

En aquest document es presenta un breu marc conceptual al voltant del terme "e-corresponsable", que fa referència a la necessitat d'assumir responsabilitats sobre les accions que el consum de tecnologia digital pugui tenir a escala social i ambiental. Des d'aquesta perspectiva, el concepte integra tres vessants.

En primer lloc, l'ambiental ("ecoresponsable"), amb relació als impactes sobre l'entorn natural dels processos lligats a la producció, comercialització, manteniment i rebuig dels dispositius tecnològics i les infraestructures que hi donen suport. Aquests impactes han estat descrits en vídeos i documents anteriors, per exemple, els vídeos del nivell A1 "**Processos de fabricació de recursos tecnològics**" i "**Matèries primeres per al desenvolupament de la tecnologia**"; el vídeo del nivell A2 "**El consum energètic dels dispositius tecnològics (l'empremta del teu correu electrònic)**"; o el document del nivell A2 "**Impactes ambientals de la tecnologia**".

Per tant, en aquest text ens centrarem en les accions propositives de disseny, producció, comercialització i consum que puguin obrir camí cap a vies d'actuació menys impactants amb l'entorn.

D'altra banda, el vessant social també s'ha de considerar com a eix central del concepte. Ser "corresponsable" implica entendre el nostre paper com a elements interrelacionats dins d'una societat, en què les accions individuals poden tenir repercussions tant per a l'entorn com per a altres persones. Per tant, aquesta perspectiva s'ha de tenir en compte per reflexionar sobre els nostres comportaments individuals, però també per plantejar intervencions col·lectives d'incidència política.

El tercer eix del concepte fa referència a la rellevància del sector tecnològic a escala econòmica i social a les nostres societats contemporànies, per això és important tenir en compte la "e" d'electrònic en el concepte "e-corresponsable".

PROCESSOS DE FABRICACIÓ DE RECURSOS TECNOLÒGICS

e.digitall.org.es/A4C44A1V03

PRIMERES MATÈRIES PER AL DESENVOLUPAMENT DE LA TECNOLOGIA

e.digitall.org.esA4C44A1V05

EL CONSUM ENERGÈTIC DELS DISPOSITIUS TECNOLÒGICS (LA PETJADA DEL TEU CORREU ELECTRÒNIC)

e.digitall.org.es/A4C44A2V03

IMPACTES AMBIENTALS DE LA TECNOLOGIA

Document referenciat:
A4C44A2D01

⚠ ATENCIÓ

En suma, hem de ser responsables i corresponsables tant ambientalment com socialment a l'hora d'exercir el nostre paper com a consumidors i usuàries de tecnologia, tant individualment com col·lectivament

L'ecoresponsabilitat al sector empresarial

La presa de decisions per adquirir hàbits socialment i ambientalment responsables en el consum i ús de tecnologia digital no ha de recaure només en les persones usuàries o consumidores de béns i serveis tecnològics. Al contrari, bona part d'aquesta responsabilitat s'ha d'enfocar tant a les institucions encarregades de la legislació específica com a les empreses del sector de la tecnologia digital.

Com ja vam veure en documents anteriors, ja està en marxa diverses iniciatives institucionals que posen el focus en la necessitat de dissenyar els productes i dispositius tecnològics tenint en compte els possibles impactes ambientals i socials del seu cicle de vida complet, per exemple, la proposta del Parlament Europeu que promou el dret a reparar (Parlament Europeu, 2022).

Aquestes disposicions impliquen que cada cop més empreses de diferents àmbits i sectors busquin implicar-se en les propostes d'ecoresponsabilitat en les seves activitats. Segons un informe de la Cambra Oficial de Comerç d'Espanya a Bèlgica i Luxemburg (2022), cada cop més empreses europees s'estan implicant en la transformació de processos productius i comercials en una aposta per l'ecoresponsabilitat. Aquesta aposta obeeix, principalment, **a quatre raons:**

1 | **Imatge.** Els consumidors avui dia presten cada vegada més atenció als detalls sobre l'origen i els processos productius del que compren i és més probable que comprin els seus productes o serveis si saben que la seva empresa es preocupa pel seu impacte en el medi ambient i la societat.

2 | **Estalvi.** L'aplicació d'accions concretes cerca que la sostenibilitat ambiental dels processos, com ara reducció, reciclatge, reutilització o gestió del consum energètic, per exemple, pot permetre estalviar diners a mitjà, i fins i tot a curt termini.

NOTA

Altres iniciatives a destacar serien les diferents metes relacionades amb la contribució a la transició ecològica dels dispositius digitals incloses en les metes de la Comissió Europea (2021).

3 | Criteris d'avaluació. Els enfocaments que busquen optimitzar l'ús de l'energia i reduir l'impacte ambiental i la sostenibilitat en general són ara criteris importants en l'avaluació i la qualificació de les empreses. Molts inversors, com ara el banc HSBC, ara només financen projectes amb un rigor en l'avaluació de l'impacte social i ambiental demostrat.

4 | Captació de talent. A causa de la creixent conscienciació ambiental en certs sectors socials i formatius, molts futurs empleats són més propensos a treballar a empreses amb una sòlida reputació social i ambiental. En altres paraules: per ser un imant de nous talents, cal ser verd.

Però, com pot transformar una empresa el seu funcionament en ecoresponsable? Més enllà de plans concrets de sostenibilitat i gestió ambiental com els basats en les normes ISO 14.000, que asseguren certs estàndards ambientals que poden ser constatats en processos de certificació, hi ha alguns passos concrets senzills que qualsevol companyia pot posar en marxa de forma autònoma per promoure processos ecoresponsables de producció i comercialització.

Més enllà dels processos de **reducció coneguts en l'ús de materials; separació i reciclatge de residus; reutilització de recursos i gestió de la despesa d'aigua i energia**, hi ha altres consells interessants per fomentar l'ecoresponsabilitat dels processos productius empresarials.

En primer lloc, cal fomentar el **consum d'energia procedent de fonts renovables**, com ara panells solars, vent, biogàs o energia geotèrmica. Actualment, en el marc de la promoció de l'Agenda 2030, en el context europeu es poden trobar multitud de subvencions i ajuts institucionals per promoure la transició energètica, i el sector empresarial hi ha de ser clau.

Per altra banda, la **mobilitat** és un altre eix clau a treballar. Precisament, la tecnologia digital permet introduir jornades de teletreball que no només estalviaran temps en termes de desplaçaments, sinó que també reduiran l'impacte ambiental.

A una escala més concreta i gairebé anecdòtica, hi ha microiniciatives que poden ajudar a fomentar la sostenibilitat a les instal·lacions i a més promoure la seguretat i salut laboral, com l'ús de plantes verdes per netejar l'aire dels centres de treball. En efecte, hi ha plantes que poden absorbir certes substàncies nocives per a la salut (per exemple, el benzè i el tricloroetilè).

Finalment, cal destacar els **incentius fiscals** com a eina clau per promoure l'ecoresponsabilitat empresarial. Per exemple, podem destacar aquí la iniciativa de l'**ecoxec** que s'ha posat en marxa a Bèlgica. L'ecoxec es defineix com un xec per a la compra de productes i serveis respectuosos amb el medi ambient que una empresa lliura als seus empleats.

A més d'un avantatge econòmic i fiscal concret, és una oportunitat per adaptar lleugerament el patró de consum cap a formes més sostenibles. L'ecoxec permet adonar-se que la forma de consumir pot tenir un impacte sobre les opcions de: mobilitat, les activitats de lleure sostenibles, la reutilització, el reciclatge, la prevenció de residus o la compra de productes locals i circuits curts de comercialització.

Per tant, les opcions de consum ecoresponsable no només han de partir d'iniciatives individuals, sinó que poden i han d'estar afavorides i fomentades per apostes institucionals i corporatives, com hem vist amb els exemples anteriors.

L'ecodisseny com a element central del consum eco-responsable

L'**ecodisseny** és un dels conceptes clau per concretar el canvi del nostre model de producció i consum cap a altres de menys impactants a escala ambiental i social, en la línia de les propostes afins a l'economia circular. A un nivell bàsic, l'ecodisseny consisteix a incloure la sostenibilitat ambiental com un criteri fonamental en la fase de disseny de productes i sistemes, com ara la funcionalitat, la seguretat o l'ergonomia. L'objectiu últim de l'ecodisseny és reduir l'impacte ambiental del producte o servei.

NOTA

El concepte va guanyar popularitat a finals de la dècada de 1970, principalment a partir de la publicació de Victor Papanek "Dissenyar per a un món real" (Papanek, 1977). Actualment, el concepte ha guanyat rellevància fins al punt de generar la directiva europea d'ecodisseny (2005/32/EC).

Aquesta directiva va ser actualitzada l'any 2009 (2009/125/EC) i el seu objectiu principal és definir un marc que estableix els requisits fonamentals de disseny ecològic per als productes que utilitzen energia i poden generar impacte ambiental. Si bé aquesta directiva va ser considerada com un element consultiu i gairebé accessòria durant la dècada anterior, en el marc de l'Agenda 2030 i el **Pla d'Acció per a l'Economia Circular 2020** presentat per la UE dins del Pacte Verd Europeu, el concepte d'ecodisseny ha esdevingut un element central.

Prenent com a referència la normativa anterior i el treball de diversos grups de recerca, com ara l'Institut de Ciència i Tecnologia Ambientals (ICTA) de la Universitat Autònoma de Barcelona, es poden destacar diverses iniciatives de desenvolupament de productes basats en l'ecodisseny en diferents sectors com poden ser el mobiliari o el dels envasos (González-García et al., 2011; Sanyé-Mengual et al., 2014).

En aquesta línia, hi ha múltiples eines qualitatives i quantitatives per analitzar el perfil ambiental del producte i establir les consideracions ambientals. Cadascuna d'aquestes eines serà apropiada per a unes aplicacions i circumstàncies concretes, ja que difereixen en complexitat i cost. Entre les metodologies que es poden aplicar per a l'ecodisseny de productes/serveis es poden esmentar les següents: Anàlisi de Cicle de Vida (ACV), Petjada Ecològica, Petjada de Carboni, Intensitat Material per Unitat de Servei, Avaluació del Canvi de Disseny, Demanda Acumulada d´Energia, Llistes de Comprovació, Matrius d´Anàlisi d'Aspectes Ambientals o Valorització de l´Estratègia Ambiental de Producte (Cambra de Comerç, 2023).

Com ja hem vist en vídeos i documents anteriors, el sector de la tecnologia digital ha de transformar-se cap a modes de producció i consum més sostenibles ambientalment i socialment, i les propostes i estratègies centrades en el foment de la reparabilitat, el reciclatge, la reutilització o l'allargament de la vida útil, totes vinculades a l'ecodisseny, poden resultar fonamentals en aquesta transformació.

⚠ ATENCIÓ

Tenint en compte tot això, queda clar que l'ecodisseny pot i ha de ser una estratègia central en el procés de transformació cap a models d'economia circular que minimitzin els impactes socials i ambientals dels nostres hàbits de producció i consum i per descomptat, el sector de la tecnologia digital s'ha d'erigir en punta de llança del procés esmentat.

Com a conclusió, en aquest document assenyalem la importància que la transformació d'hàbits de consum de tecnologia cap a un model ecorresponsable no recaigui únicament en les persones consumidores, sinó que tant les institucions com les empreses i companyies implicades al sector promoguin els canvis necessaris a través d'estratègies com l'ecodisseny.

Saber-ne més

Cambra de Comerç (2023) Ecodisseny: Disseny de Productes-Serveis Sostenibles. https://www.camara.es/innovacion-y-competitividad/como-innovar/diseno-sostenible

DIRECTIVA 2009/125/CE DEL PARLAMENT EUROPEU I DEL CONSELL (2009) de 21 d'octubre del 2009 per la qual s'instaura un marc per a l'establiment de requisits de disseny ecològic aplicables als productes relacionats amb l'energia. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0125&from=LV

Comissió Europea (2021). La Dècada Digital d'Europa: metes digitals per al 2030. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

González-García, Sara, Carles M. Gasol, Raúl García Lozano, M Teresa Moreira, Xavier Gabarrell, Joan Rieradevall i Pons, Gumersindo Feijoo (2014) of The Total Environment, Volums 410–411. https://www.sciencedirect.com/science/article/abs/pii/S004896971101093X

Papanek, Victor (1977) Dissenyar per al món real. https://www.academia.edu/28853738/Dise%C3%B1ar_para_el_mundo_real_Victor_Papanek_pdf

Parlament Europeu (2022). Dret a reparar: el PE vol productes més duradors i fàcils de reparar. https://www.europarl.europa.eu/news/es/press-room/20220401IPR26537/derecho-a-reparar-el-pe-quiere-productos-mas-duraderos-y-faciles-de-reparar

Sanyé-Mengual, E., Lozano, R.G., Oliver-Solà, J., Gasol, C.M., Rieradevall, J. (2014) Eco-design andproduct carbon footprint use in the packagingsector, In: Subramanian, S.M.: Assessment ofcarbon footprint different industrial sectors,Vol. 1, EcoProduction 2014, Springer, Singapore, pàg. 221-245. https://www.researchgate.net/publication/276266546_Eco-Design_and_Product_Carbon_Footprint_Use_in_the_Packaging_Sector

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

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