DigitAll

Formació en
Competències
Digitals

4

Seguretat

DigitAll

Formació en
Competències
Digitals

Seguretat

Nivell A2

ÍNDEX

DigitAll

Seguretat

4.1 PROTECCIÓ DE DISPOSITIUS

Seguretat

Nivell A2 4.1 Protecció de dispositius

OSINT: la informació de fonts obertes

OSINT: la informació de fonts obertes

Al llarg de la nostra vida digital generem gran quantitat de dades, moltes personals, de tota mena, com fotos, vídeos, text, àudios, ubicacions, etc. Molta d'aquesta informació roman pública a l'abast de qualsevol persona amb una connexió a Internet. Per protegir la nostra privadesa, és important ser conscient en tot moment de la informació que publiquem a les xarxes, així com d'aquella que estigui disponible sobre nosaltres a través d'altres fonts.

En aquesta secció s'explica com es pot fer ús de la informació pública de les persones per dur a terme investigacions. A les tècniques i procediments de recuperar dades públiques i aconseguir transformar-les en informació rellevant se'l coneix com a OSINT.

Què és OSINT?

La **intel·ligència de codi obert** o ***Open Source Intelligence*** (**OSINT**) és un mètode de recopilació d'informació en què s'utilitza informació disponible públicament per extreure dades útils i rellevants que es puguin utilitzar en la presa de decisions informades.

Les **fonts d'informació** per a OSINT poden ser diverses, com ara **mitjans de comunicació**, xarxes socials, fòrums, blocs, llocs web governamentals, bases de dades públiques, entre d'altres. La informació recopilada mitjançant OSINT s'utilitza en diferents àmbits, com ara la seguretat nacional, la investigació criminal, la gestió de riscos, la intel·ligència empresarial i moltes altres àrees.

La popularitat d'OSINT ha augmentat significativament els darrers anys a causa de l'**accessibilitat i l'abundància d'informació pública disponible**. A més, el desenvolupament de tecnologies i eines específiques per a la recopilació, l'anàlisi i la visualització de dades ha facilitat l'ús d'aquesta tècnica en diverses àrees.

L'objectiu principal d'OSINT és proporcionar una visió clara i objectiva de la informació disponible al públic per ajudar a prendre decisions informades. En utilitzar la informació disponible públicament, OSINT pot proporcionar una visió única i més completa d'un tema en particular que altrament seria difícil d'obtenir.

En resum, OSINT és una tècnica efectiva i àmpliament utilitzada per recopilar informació rellevant, útil i disponible públicament per prendre decisions informades. Aquesta tècnica s'ha tornat cada cop més important i popular a causa de l'accessibilitat de la informació i el desenvolupament de tecnologies i eines específiques.

Procés OSINT

El procés d'OSINT és el conjunt de passos que cal seguir per fer una investigació efectiva utilitzant fonts d'informació públiques. El procés pot variar segons el tipus de recerca que s'estigui realitzant i les eines que s'utilitzen, però generalment es compon dels passos següents:

1 | Planificació
Aquest és el primer pas del procés i s'enfoca a establir els objectius de la investigació, definir-ne l'abast i determinar les fonts d'informació que s'utilitzaran. És important establir un pla per a la recerca per mantenir-se enfocat a l'objectiu final i per assegurar-se de no perdre temps o recursos en informació irrellevant.

2 | Compilació
En aquest pas, es recopila la informació de les fonts identificades a la fase de planificació. És important tenir en compte que no tota la informació disponible és rellevant o precisa, per la qual cosa cal fer una avaluació crítica de la informació recopilada.

3 | Anàlisi
Un cop es recopila la informació, s'ha d'analitzar i avaluar per determinar-ne la rellevància i la utilitat en el context de la recerca. És important utilitzar eines i tècniques d'anàlisi per processar grans quantitats d'informació de manera eficient i efectiva.

4 | Interpretació
En aquest pas, s'interpreten els resultats de l'anàlisi per obtenir una clara comprensió de la informació i com es relaciona amb els objectius de la recerca. La interpretació pot requerir la validació de la informació i la identificació de patrons i de relacions rellevants.

5 | Presentació
La presentació és el darrer pas del procés i s'enfoca a la comunicació dels resultats de la recerca a les parts interessades. És important presentar la informació de manera clara i concisa, utilitzant visualitzacions de dades i altres mitjans per facilitar-ne la comprensió.

Cal destacar que les fases del procés OSINT no han de ser dutes a terme de manera lineal. De fet, a la majoria d'investigacions se sol tornar a fases anteriors una vegada es descobreix alguna informació interessant que canvia el rumb dels fets.

En resum, el procés d'OSINT implica planificar, recopilar, analitzar, interpretar i presentar informació pública per obtenir coneixements i prendre decisions informades. Cada pas del procés és important i s'ha de fer amb compte per garantir que la informació recopilada i analitzada sigui rellevant i precisa en el context de la investigació.

Fonts d'informació

Les fonts d'informació de l'OSINT poden variar àmpliament, des de xarxes socials i bases de dades públiques fins a llocs web governamentals i mitjans de comunicació. A més, és fonamental assegurar-se que la informació obtinguda sigui legal i ètica. Algunes de les fonts d'informació més comunes utilitzades a OSINT són:

1 | Xarxes socials
Les xarxes socials són una de les fonts més utilitzades i accessibles de l'OSINT. Plataformes com Facebook, X, Instagram i LinkedIn permeten als usuaris compartir informació personal, opinions i llocs que visiten. A més, aquestes plataformes també ofereixen informació valuosa sobre la xarxa de contactes d'un individu, com ara amics, familiars, col·legues i contactes professionals. Alguns exemples d'informació que es poden trobar a les xarxes

socials són: fotografies, ubicacions, gustos i preferències personals, publicacions sobre opinions, entre d'altres.

2 | Bases de dades públiques
Les bases de dades públiques són una font important d'informació per a OSINT. Algunes de les bases de dades més utilitzades inclouen registres de propietat, registres d'empreses, registres judicials i registres de vehicles. Per exemple, una persona que cerca comprar una casa pot utilitzar una base de dades de registres de propietat per obtenir informació sobre l'historial de la propietat, el valor actual i la ubicació.

3 | Llocs web governamentals
Els llocs web governamentals són una font fiable d'informació sobre polítiques públiques, informes governamentals i estadístiques. Per exemple, un estudiant que cerca informació sobre la població i l'economia del seu país pot visitar un lloc web governamental per obtenir dades actualitzades i fiables.

4 | Mitjans de comunicació
Els mitjans de comunicació, tant tradicionals com en línia, poden proporcionar informació actualitzada sobre esdeveniments i notícies rellevants. Els diaris, les revistes, els canals de televisió i els llocs web de notícies són algunes de les fonts més utilitzades per obtenir informació sobre esdeveniments actuals. Per exemple, una persona que cerca informació sobre el clima i les condicions del trànsit pot consultar el lloc web de notícies local.

Tota la informació que es troba pública a Internet pot suposar un problema de privadesa important per a les persones. Pel simple ús dels serveis de la xarxa, com ara la navegació web o les xarxes socials, estem deixant una empremta digital que és molt difícil d'amagar o modificar. En aquest sentit, les dades personals tenen una gran rellevància, i hi ha legislació que protegeix la seva utilització i intercanvi de manera segura, com el Reglament General de Protecció de Dades (RGPD). Si vols saber més sobre aquest tema, pots veure el vídeo:

PRIVACITAT, PETJADA DIGITAL I REPUTACIÓ EN LÍNIA

En aquest vídeo es ressalta la importància de la informació que existeix a Internet en relació amb un usuari, a través la petjada digital, i es destaca l'ús de les xarxes socials i la reputació en línia.

e.digitall.org.es/A4C41A2D02

NOTA

Qualsevol persona amb accés a Internet podria accedir a la informació que es troba publicada a la part oberta de la xarxa. És important, per tant, **ser conscients de tota la informació que pugem a les xarxes**, com fotografies, vídeos, missatges, etc., perquè gran part d'ella pot arribar a contenir dades rellevants. Aquesta informació podria ser utilitzada per un atacant per crear enganys més creïbles o fer suplantació d'identitat.

Eines

Hi ha nombroses eines OSINT disponibles, i aquestes es poden categoritzar en diferents àrees segons la seva funcionalitat. Aquí es presenten algunes de les eines més populars:

- **Motors de cerca**
  Els motors de cerca són una de les eines més utilitzades a OSINT. Google és un dels motors de cerca més populars i s'utilitza per trobar informació en línia. Altres motors de cerca populars són Bing, Yahoo!, i DuckDuckGo. A més, hi ha motors de cerca especialitzats en la cerca d'informació a xarxes socials, com Social Catfish i PeekYou.
- **Eines de monitoratge de xarxes socials**
  Aquestes eines es fan servir per monitorar i recopilar informació de diferents plataformes de xarxes socials. Algunes eines populars són Hootsuite, TweetDeck, i Meltwater.
- **Eines d'anàlisi d'imatges**
  Aquestes eines s'utilitzen per analitzar i extreure informació d'imatges. Algunes eines populars són Google Images, TinEye, i Yandex Images.

- **Eines d'anàlisi de metadades**
  Les metadades són informació oculta en fitxers digitals, com ara imatges i documents. Les eines d'anàlisi de metadades s'utilitzen per extreure aquesta informació. Algunes eines populars són ExifTool i Metagoofil.
- **Eines d'anàlisi de dades al web**
  Aquestes eines s'utilitzen per extreure i analitzar dades del web, dels llocs web i xarxes socials. Algunes eines populars són Import.io, Scrapy, i BeautifulSoup.
- **Eines d'anàlisi de correu electrònic**
  Aquestes eines s'utilitzen per analitzar correus electrònics, la informació de la capçalera i el contingut. Algunes eines populars són MxToolbox i Email Header Analyzer.
- **Eines d'anàlisi de noms de domini**
  Aquestes eines s'utilitzen per analitzar noms de domini, informació de registre, adreça IP i ubicació geogràfica. Algunes eines populars són DomainTools i Whois.

És important tenir en compte que aquestes eines només són útils si es fan servir adequadament. Per obtenir els millors resultats, és important tenir una comprensió sòlida de la font d'informació que s'està analitzant i de les tècniques i metodologies de l'OSINT.

Cas d'ús: Google Dorks

Google Dorks són ordres de cerca avançades que permeten als usuaris realitzar cerques més precises i detallades a Google. En lloc de simplement cercar paraules clau, els usuaris poden utilitzar Google Dorks per filtrar resultats de cerca utilitzant paràmetres específics.

Per què són útils els Google Dorks? Els Google Dorks són útils perquè permeten als usuaris trobar informació específica i detallada en línia. Els Google Dorks s'utilitzen comunament a OSINT per cercar informació sobre una persona, organització o tema específic en línia.

A continuació, es presenten alguns exemples d'ordres de Google Dorks útils per a usuaris no avançats:

- **site:** aquesta ordre permet als usuaris buscar en un lloc web específic. Per exemple, "site:nytimes.com coronavirus" cercarà resultats al lloc web del New York Times que incloguin la paraula "coronavirus".
- **filetype:** aquesta ordre permet als usuaris cercar un tipus de fitxer específic, com PDF o DOCX. Per exemple, "filetype:pdf hackeig informàtic" cercarà resultats que continguin la frase "hackeig informàtic" en arxius PDF.
- **intext:** aquesta ordre permet als usuaris cercar paraules o frases específiques dins del contingut d'una pàgina web. Per exemple, "intext:password seguretat" cercarà resultats que continguin la paraula "seguretat" i la paraula "contrasenya".
- **inurl:** aquesta ordre permet als usuaris cercar un URL específica o una part de l'URL. Per exemple, "inurl:seguretat informàtica" cercarà resultats que continguin la frase "seguretat informàtica" a l'URL.
- **intitle:** aquesta ordre permet als usuaris cercar una pàgina web per títol. Per exemple, "intitle:seguretat informàtica" cercarà resultats que continguin la frase "seguretat informàtica" al títol de la pàgina.

Si volem trobar exemples reals d'aquest tipus d'ordres per trobar informació concreta, podem utilitzar la base de dades de l'Exploit Database anomenada Google Hacking Database. Aquesta pàgina permet trobar multitud de Google Dorks concrets que ens permeten visualitzar la seva aplicació real al camp de la seguretat informàtica, així com recuperar certa informació que de primeres podria passar inadvertida. Aquest tipus de recursos ens permeten entendre la rellevància i el potencial de les tècniques d'OSINT a l'hora de fer una investigació amb fonts obertes.

> **NOTA**
>
> És important tenir en compte que, encara que els Google Dorks poden ser útils, també poden presentar riscos de seguretat i privadesa si s'utilitzen incorrectament. Per tant, és important utilitzar-los amb precaució i tenir sempre en compte la legalitat i ètica de l'ús de la informació trobada.

Comunitat OSINT

Trace Labs és una comunitat de l'OSINT dedicada a cercar persones desaparegudes utilitzant tècniques de recerca i tecnologia avançada. Han tingut molts casos d'èxit a la recerca de persones desaparegudes, però un dels més destacats és el cas de "Mary".

En el cas de Mary, una dona va desaparèixer sense deixar rastre el 2019 a l'estat de Nova York, Estats Units. La policia local havia intentat localitzar-la sense èxit durant mesos, per la qual cosa la família de Mary va recórrer a Trace Labs per obtenir-ne ajuda. La comunitat Trace Labs va començar a treballar en el cas i va utilitzar diverses tècniques de l'OSINT per buscar informació sobre Mary en línia. Alguns dels mètodes que van utilitzar van incloure la cerca d'informació a les xarxes socials, la investigació de registres públics i la revisió de càmeres de seguretat.

Finalment, l'equip de Trace Labs va trobar informació important que va portar a la ubicació de Mary. La informació incloïa un registre de càmera de seguretat que mostrava Mary en una àrea propera a un llac, cosa que va portar la policia a buscar en aquesta zona. Mary va ser trobada amb vida i va ser tornada a la seva família.

Aquest cas demostra el poder de l'OSINT i la capacitat de la comunitat Trace Labs per treballar en conjunt per ajudar les famílies a trobar els seus éssers estimats desapareguts. Trace Labs ha dut a terme molts altres casos d'èxit similars i continua treballant per ajudar a trobar persones desaparegudes a tot el món.

En l'àmbit de la investigació existeixen també diferents esdeveniments en què diversos professionals del sector de la seguretat, en aquest cas especialitzats a OSINT, exposen les seves investigacions i eines pròpies. Alguns exemples poden ser l'**Osintomàtic Conference** o **IntelCon**.

Seguretat

Nivell A2 4.1 Protecció de dispositius

Privacitat, petjada digital i reputació en línia

Privadesa, empremta digital i reputació en línia

L'ús d'Internet i la publicació d'informació sobre nosaltres fa que creem una identitat digital. Aquesta identitat pot reflectir la que associem al món real, però a diferència d'aquesta, la identitat digital està formada per informació de fàcil accés per qualsevol.

En aquesta secció, aprendrem com funcionen els motors de cerca com Google o Bing, i quina informació forma la nostra empremta digital. És important conèixer-la i fer una anàlisi conscient de quines implicacions pot tenir per a nosaltres.

Identitat i empremta digital

La identitat digital és la que es conforma a partir de l'empremta digital d'un usuari a Internet. És a dir, tota aquella informació que està disponible públicament i que es pot associar a una identitat conforma la identitat digital.

Xarxes socials

Utilitzam xarxes socials diàriament, però molta gent no és conscient del que hi està compartint. Quan fem ús dels nostres perfils a les xarxes socials, hem de ser molt curosos a l'hora de compartir la nostra informació i pensar en els riscos que ens pot ocasionar.

Moltes vegades compartim massa detalls dia a dia a les xarxes socials, fins i tot hi ha certa informació que hem de proporcionar de forma obligatòria si volem fer-ne ús, normalment informació personal. Això no ens hauria de preocupar, sempre que les dades no siguin accessibles per terceres persones.

⚠ ATENCIÓ

La informació personal, dades personals i informació personalment identificable és la que permet identificar un individu. Per exemple, el DNI, el lloc de residència, l'estat civil o la nacionalitat.

Hi ha certa informació que no hauríem de fer pública a la xarxa. És a dir, és recomanable que pensem dues vegades abans de publicar:

- **Dades personals:** com a nom i cognoms complet, telèfon, DNI, e-mail... A través d'ells podem ser identificats!
- **Plans i vacances:** poden saber quan no som a casa per intentar entrar a robar.
- **Ubicació actual:** permeten saber les nostres rutines diàries, el nostre domicili i la nostra feina.
- **Informació bancària:** ens poden robar o fer càrrecs fraudulents als nostres comptes.
- **Informació sobre menors:** poden ferir-ne la sensibilitat en el futur, o acabar en males mans.

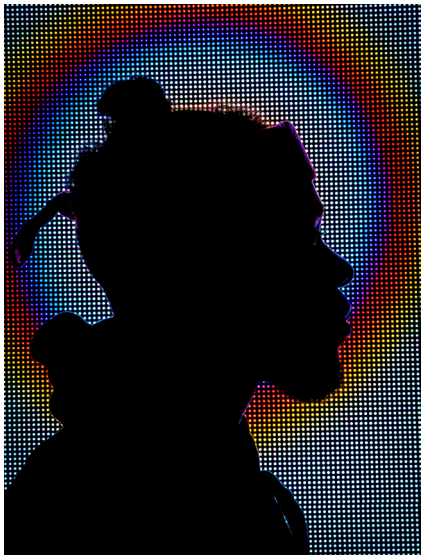
NOTA

Has de revisar les opcions de seguretat i privadesa de les teves xarxes socials. Les opcions de configuració més comunes solen estar sota un apartat en ajustaments anomenat "privadesa i seguretat". Aquí, pots amagar informació perquè no es mostri de forma pública, i gestionar el que comparteixes i la teva exposició a la xarxa.

Reputació en línia

A més de la informació anterior, cal pensar dues vegades també quan publiquem comportaments inadequats o alguna opinió personal. Tot això forma part de la nostra reputació en línia. Concretament, la petjada digital que formem crearà la nostra identitat digital, que pot correspondre més o menys amb la nostra identitat real.

Hi ha cert tipus de publicacions que ens poden afectar negativament. Quan publiquem alguna cosa, deixem de tenir control sobre aquesta informació.



Les publicacions que poden afectar la nostra **reputació en línia** són moltes, com, per exemple:

- **Publicacions ofensives o comentaris negatius:** insultar o amenaçar a través de xarxes pot ser delicte i fer publicacions ofensives es pot girar en contra nostra.
- **Ciberassetjament:** burles, insults i humiliacions a una persona. Si ets víctima o un testimoni, ho has de denunciar.

- **Queixes laborals:** moltes empreses revisen les xarxes socials dels seus treballadors per evitar que comparteixin contingut inapropiat, o fins i tot durant processos de selecció.
- **Fotos i vídeos inapropiats:** si puges una fotografia a una xarxa social, perds el control sobre ella. A més, fotografies que ens puguin comprometre, poden arribar a mans de terceres persones per fer xantatge o perjudicar-nos.
- **Propagació de notícies falses o *fake news*:** no hem de creure tot allò que veiem per xarxes socials o Internet.

Abans de publicar una notícia, és recomanable comprovar-ne les fonts. Compartir una bèstia o estafa, pot afectar molt negativament la teva reputació en línia.

Els motors de cerca

Google, Bing, DuckDuckGo i Ecosia són motors de cerca a Internet. Ens permeten cercar informació accessible de forma pública cercant a través de paraules clau o consultes. Encara que sona complex, estem molt acostumats a utilitzar-los al nostre dia a dia, responent-nos a dubtes amb una gran quantitat d'enllaços o referències a contingut al web.

No obstant això, **els motors de cerca també poden incloure contingut com a perfils de xarxes socials, imatges, notícies o informació general sobre nosaltres**. Per això, és important entendre el seu funcionament i com gestionar la informació sobre nosaltres a la xarxa, accessible a través d'aquests motors de cerca.

Com funcionen?

L'objectiu principal dels motors de cerca és **ajudar els usuaris a trobar informació rellevant i útil a Internet**. Per aconseguir això, els motors de cerca recopilen, organitzen i presenten la informació disponible al web de manera eficient i efectiva, per tal de proporcionar als usuaris els resultats més rellevants per a la seva consulta.

Alguns cercadors també tenen com a objectiu millorar l'experiència de l'usuari, proporcionant resultats de cerca precisos i actualitzats en format fàcil d'usar i accessible.

> **NOTA**
>
> En aquest context, han sorgit intel·ligències artificials conversacionals com ChatGPT, d'OpenAI. Aquests sistemes han estat entrenats amb una gran quantitat d'informació al web i són capaços de respondre preguntes complexes, a diferència dels cercadors que només ens proporcionen referències a la informació.

Perquè els cercadors puguin oferir a l'usuari la informació rellevant després d'una consulta, cal que hagin rastrejat el web prèviament. Durant el procés de **rastreig del web** o *web crawling*, els cercadors ordenen la informació en una llista. Això és conegut com a "**indexació de continguts**". És a dir, els cercadors exploren al i processen el contingut d'aquesta per incloure-la a la llista de pàgines web conegudes.

Aquesta llista o índex és el que el motor de cerca consulta quan l'usuari escriu a la barra de cerca o consulta. D'aquesta manera, si hi ha algun contingut que s'acaba de publicar a Internet en els darrers minuts, el més probable és que el cercador no ho mostri, perquè encara no estarà "indexat".

Per detectar quina informació ha indexat sobre nosaltres un determinat motor de cerca, és recomanable practicar l'***ego surfing***. Això consisteix a cercar el nostre propi nom o informació personal en motors de cerca com Google, Bing o Yahoo. És a dir, cercar informació sobre un mateix al web, i així analitzar la nostra reputació en línia o la nostra empremta digital.

El posicionament SEO

El *Search Engine Optimisation* (SEO) és un conjunt de tècniques que utilitzen els creadors de continguts, organitzacions i empreses per **aconseguir que algun contingut aparegui entre els primers resultats dels motors de cerca quan l'usuari realitza determinades consultes**. Per exemple, un concessionari de cotxes a Barcelona estarà interessat a tenir la seva pàgina web al primer lloc quan l'usuari busqui "venda de cotxes a Barcelona".

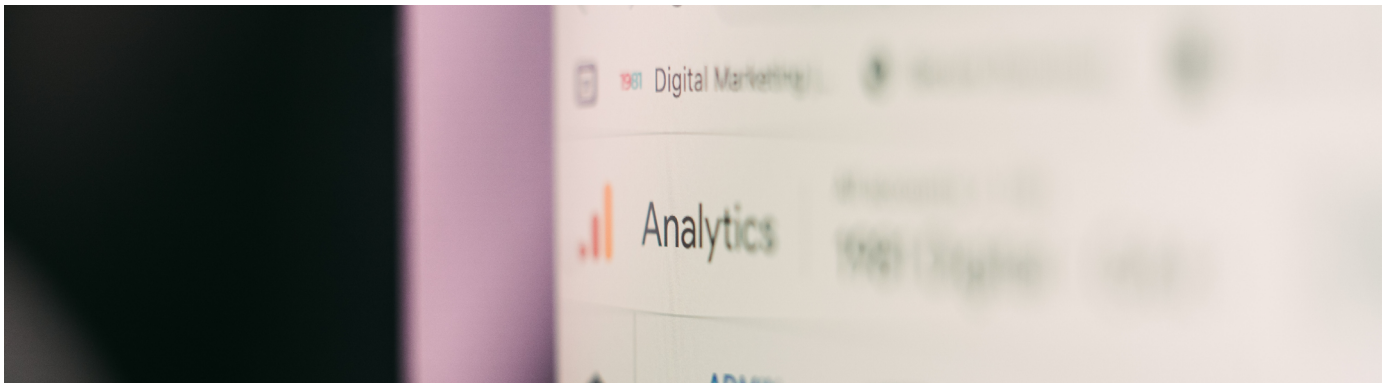
No obstant això, les tècniques SEO es poden utilitzar per fer atacs com l'**enverinament SEO**, que busquen introduir informació falsa amb algun propòsit maliciós. Alguns exemples són cometre estafes o minar la reputació d'una persona o organització.

És important conèixer el funcionament dels cercadors i del posicionament SEO perquè jugui a favor nostre. La nostra reputació en línia i la petjada digital formen la nostra identitat a Internet.

Per això, és important afavorir que es posicioni bé la informació que ens interessi promocionar, i vigilar si hi apareix alguna informació personal certa o falsa que ens pugui perjudicar. En aquest sentit, recorda que les tècniques OSINT permeten a atacants aprofitar-se dels motors de cerca i obtenir informació sobre nosaltres. Per evitar-ho, podem eliminar el contingut i sol·licitar als motors de cerca que no l'incloguin en la llista o índex.

OSINT: LA INFORMACIÓ DE FONTS OBERTES

Document referenciat: ***A4C41A2D01***



DigitAll

Seguretat

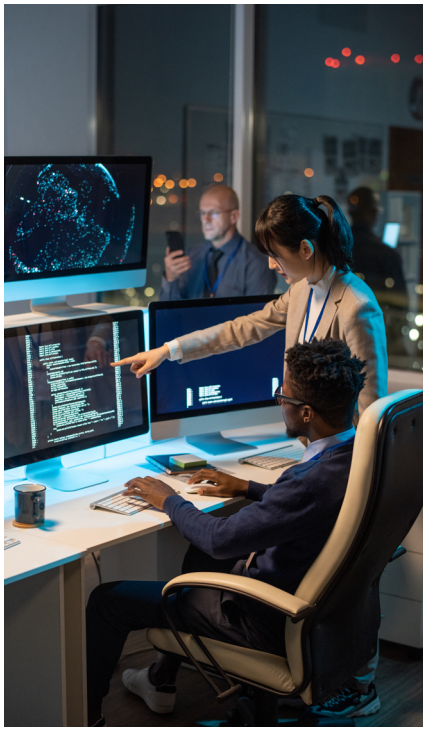
4.2
PROTECCIÓ DE LES DADES PERSONALS I LA PRIVACITAT

Seguretat

Nivell A2 4.2 Protecció de les dades personals i la privacitat

Polítiques de seguretat. Informació privada

Polítiques de seguretat. Informació privada



Introducció

Les polítiques de seguretat en l'àmbit de la informàtica contemplen els procediments i les normes que permeten garantir la confidencialitat, integritat i disponibilitat de la informació. Aquests procediments i normativa afecten qualsevol mecanisme d'accés als sistemes i dispositius tant on s'emmagatzema la informació com des d'on es pugui tenir accés. Les polítiques de seguretat afecten tant la seguretat física, mitjançant sistemes mecànics, com la seguretat lògica, mitjançant sistemes electrònics amb accés directe oa través de xarxes de comunicacions. Els procediments bàsics de seguretat s'estableixen a la Norma internacional ISO 27000 (establertes per l'Organització Internacional d'Estàndards), i les que se'n deriven, que aborda tots els aspectes relacionats amb la Seguretat de la Informació, i es desenvoluparan de forma resumida en aquest document. Aquesta norma està desenvolupada en cooperació amb la Comissió Electrotècnica Internacional (IEC-International Electrotechnical Commission) per la qual cosa s'anomena també ISO/IEC 27000.

Les polítiques de seguretat s'estableixen, entre d'altres, per mantenir la protecció de la informació privada dels usuaris en l'accés i la utilització dels sistemes, de qualsevol tipus i a qualsevol nivell. Entenent, per tant, la informació privada com aquella que correspon a la privadesa de l'individu i que cal protegir, tant la corresponent a les dades privades (nom i cognoms, domicili, DNI, telèfon, email, activitats que realitza, amics, comentaris, etc.) com la relativa a la identitat de l'individu en els sistemes computadors on treballa o que visita.

Polítiques de seguretat

Les polítiques de seguretat en els sistemes d'informació han de contemplar tant la seguretat física, identificant els procediments a establir respecte a restriccions en l'accés als sistemes, portes de seguretat amb accés restringit, protecció contra incendis, refrigeració, disseny i estructura eficients de les infraestructures, etc.; com la seguretat lògica, tots els requisits per a la seguretat dels sistemes d'informació, quant a l'accés, processament i atacs a través de qualsevol mecanisme o dispositiu electrònic o informàtic. A més, entre les directrius que estableix la normativa, figuren normes sobre aspectes administratius que abasten des de l'assignació de responsabilitats fins a la seguretat dels contractes amb tercers i l'accés a la informació per part d'aquests.

Les normes i estàndards són disposicions que es fan servir en organitzacions per garantir que els productes i serveis oferts per aquestes organitzacions compleixen els requisits de qualitat del client i els objectius previstos. En aquest sentit, i en relació amb l'aspecte particular que ens pertoca, la norma ISO 27000 i les seves derivades, normes sorgides a partir de la norma matriu, tracten la seguretat dels sistemes d'informació en tots els aspectes.

POLÍTIQUES DE SEGURETAT. ACCÉS A SISTEMES I DISPOSITIUS

Generalitats en polítiques de seguretat dels sistemes d'informació (seguretat mecànica, accés directe, accés a través de xarxes).

e.digitall.org.es/A4C42A2V06

Norma ISO 27000. Seguretat de la informació

La sèrie ISO 27000 és la que aglomera totes les normatives en matèria de seguretat de la informació. Les normes més importants d'aquesta família, per establir una implementació efectiva de la seguretat de la informació mitjançant un Sistema de Gestió de Seguretat de la Informació (SGSI) centrat en la prevenció de riscos, són les normes ISO 27001 i ISO 27002. Mitjançant aquesta normativa, s'indiquen les

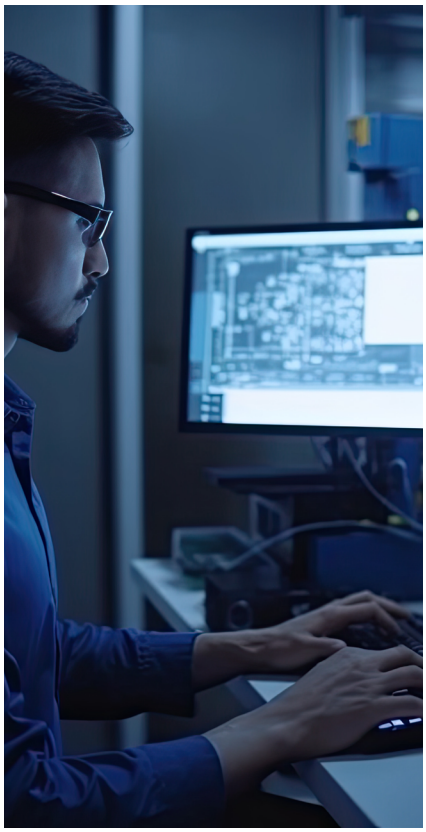
mesures orientades a protegir la informació, indistintament del format de la mateixa (emmagatzemada electrònicament, transmesa per correu o per mitjans electrònics, impresa en paper, mostrada en vídeo o parlada en conversa), contra qualsevol amenaça, de manera que garantim a tot moment la Confidencialitat, Integritat i Disponibilitat de la Informació.

Aquesta normativa disposa d'un reconeixement internacional i que proporciona un marc de gestió de la seguretat de la informació utilitzable per qualsevol tipus d´organització, pública o privada, gran o petita. La norma ISO/IEC 27001 ajuda a protegir l'empresa, la institució o el negoci, la seva reputació i afegeix valor extra a qualsevol transacció; protegeix els registres personals i la informació sensible; redueix els riscos de ser piratejat o atacat per agents maliciosos; e inspira confiança en l'organització que l'estableix.

La norma ISO/IEC 27002:2022, tractada com un codi de bones pràctiques, ha estat renovada a un conjunt de controls de seguretat que permeten verificar la implantació de la norma 27001.

Indicacions de les normes 27001 i 27002

A grans trets, aquesta normativa estableix els protocols a implementar per a la seguretat i la fiabilitat dels sistemes. En concret, aquesta norma identifica els protocols o procediments que cal establir tant pel que fa a la seguretat física dels sistemes, com pel que fa a la seguretat lògica, d'accés a través de mecanismes electrònics o informàtics, processament de la informació o atacs als sistemes d'informació . S'inclouen aquí els procediments a seguir per a la protecció contra codi maliciós, les còpies de seguretat, la seguretat a les xarxes o l'intercanvi d'informació i la gestió de serveis amb tercers. Recomanacions sobre la notificació d'esdeveniments i punts febles de seguretat, i els procediments i responsabilitats per a la gestió d'incidents i millores de seguretat de la informació. També s'hi inclouen protocols relatius a recursos humans i aspectes administratius o d'organització que abasten des de l'assignació de responsabilitats per a l'accés a la informació fins a la seguretat dels contractes amb tercers i l'accés a la informació per part d'aquests.



En concret, algunes d'aquestes normes fan referència a:

- **Restriccions mecàniques a l'accés als sistemes**
  Cal protegir els servidors que mantenen la informació per evitar l'accés físic no autoritzat a les instal·lacions. Els equips on es processa i s'emmagatzema la informació han d'estar en àrees segures i protegides dins d'un perímetre definit amb controls per saber qui hi accedeix.

Sistema de identificación para acceso a los sistemas informáticos.

- **Protecció contra incendis i altres catàstrofes**
  A més de la normativa existent sobre la protecció contra incendis d'edificis, instal·lacions industrials i entorns naturals, hi ha una normativa específica per a la protecció contra incendis molt estricta per evitar que la informació pateixi danys o es pugui perdre, especialment en centres de processament de dades on s'emmagatzema la nostra informació. El maquinari existent en aquests centres emet gairebé el 100% de l'energia utilitzada en forma de calor i un augment excessiu de la temperatura podria danyar els sistemes, per la qual cosa la refrigeració és fonamental (s'estableix una densa xarxa de detectors i un sistema de detecció primerenca d'incendis). En molts casos, es fa obligatori disposar de rèpliques sincronitzades del sistema d'informació, en llocs llunyans entre si, de manera que, si un sistema falla o cau, per incendi o fins i tot per catàstrofe natural, el servei continuï per a l'usuari final.

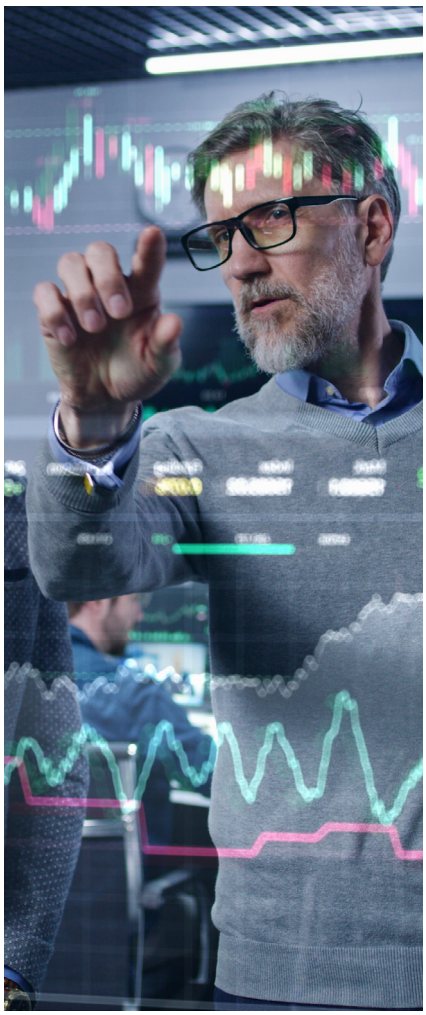
- **Disseny i estructura eficients de les infraestructures i refrigeració**
  Habitualment, a les diferents organitzacions, institucions o empreses, els sistemes d'informació s'ubiquen en centres de processament de dades que mantenen els serveis i sistemes d'informació actius. Aquests centres de procés de dades han de disposar d'unes infraestructures que els permetin, de manera organitzada i estructurada, donar servei tant intern com a usuaris externs a aquesta.

  La normativa estableix els requisits quant al disseny de suports i canals per a les vies de comunicació i connexió, disposant d'un sistema de cablatge estructurat i a prova d'errors que permeti l'ampliació senzilla a elevades necessitats de transmissió; sistemes d'alimentació elèctrica segura i SAI (sistema d'alimentació ininterrompuda), en cas que falli el subministrament elèctric principal, les bateries del sistema SAI prenen


Diseño de un centro de procesamiento de datos, conexionado y racks.

temporalment el relleu; desplegament de racks de servidors a la zona interior del centre de procés de dades, d'aquesta manera es facilita la configuració, enllaçat i possible substitució d'elements al sistema d'informació.

- **Recursos humans**
  La norma, i les actualitzacions, tracten aspectes sobre la contractació de personal, els processos disciplinaris, el cessament de relació laboral o el canvi de lloc de treball, com la suspensió de les credencials d'accés. Indica de manera concisa les actuacions sobre política de control d'accés, gestió d'accessos d'usuaris i accessos a la xarxa, sistema operatiu i aplicacions i el maneig d'ordinadors portàtils i teletreball.
- **Seguretat i controls criptogràfics**
  Els atacs contra la seguretat de la informació fan que la normativa sobre la seguretat de la informació sigui cada dia més actual i permeten assignar la importància necessària als controls sobre la seguretat dels sistemes. Així, s'ha de garantir que la informació i les instal·lacions de processament d'informació estan protegides contra el codi maliciós. Per això, en primer lloc, cal disposar de sistemes de detecció de codi maliciós als servidors i als llocs de treball. A més, els controls criptogràfics pretenen la protecció de la informació en cas que un intrús pugui tenir accés físic a la informació, s'estableix un sistema de xifratge per mantenir la confidencialitat i la integritat de la informació.



Norma ISO 27002. Controls de verificació seguretat de la informació

La normativa presentada a l'ISO 27002 es planteja com un inventari de bones pràctiques sobre controls de seguretat de la informació. La norma ofereix una sèrie de controls que s'utilitzen com a guia d'implementació per assolir els objectius de la seguretat de la informació que s'estableixen a les normes anteriors.

Els paràmetres de control que incorpora aquesta norma afecten, per tant, les polítiques de seguretat de la informació, l'organització d'aquesta seguretat i els recursos emprats, controls d'accés i seguretat física de l'entorn, criptografia i seguretat de les comunicacions i les operacions, i gestió d'actius, entre d'altres.

Normes ISO 27017 i 27018. Sistemes d'informació al núvol (cloud). Protecció de dades personals

La norma ISO 27017 estableix els controls de seguretat de la informació per a serveis al núvol, entenent per tals els que es realitzen a través d'internet, és a dir, aquells que ofereixen aplicacions que no estan instal·lades al mateix ordinador. Per fer-ho, el servidor d'aquestes aplicacions o programes ha de ser accessible des de qualsevol dispositiu connectat a internet i ha de disposar de garanties de seguretat i capacitat d'emmagatzematge suficients per a qualsevol usuari. Aquesta norma disposa d'una guia de controls addicionals als establerts a l'ISO 27002, específics per al núvol.

És una norma internacional que indica la millor manera de protegir les dades personals de salut. Entre d'altres, establiu controls d'accés a dades amb indicació d'accés privilegiat; gestió criptogràfica de dades confidencials, amb protecció de les claus de xifratge; i, registre de la utilització de les dades d'usuaris, protegint-les d'alteracions i accessos no autoritzats.

Norma ISO 27799. Gestió de la seguretat de la informació en sanitat

És una norma internacional que indica la millor manera de protegir les dades personals de salut. Entre d'altres, establiu controls d'accés a dades amb indicació d'accés privilegiat; gestió criptogràfica de dades confidencials, amb protecció de les claus de xifratge; i, registre de la utilització de les dades d'usuaris, protegint-les d'alteracions i accessos no autoritzats.

Informació privada

En els sistemes d'informació, especialment en la navegació per internet i accessos al núvol, cal mantenir la protecció de la informació privada dels usuaris, en l'accés i la utilització d'aquests. La informació privada és la que correspon a la privadesa de l'individu, tant les dades privades com la relativa a la identitat digital de l'individu.

POLÍTICA DE PRIVACITAT A INTERNET I A LES APLICACIONS

Importancia de la política de privacidad. Contenido de un documento de política de privacidad).

e.digitall.org.es/A4C42A1V07

Contemplant la importància de la privadesa de la informació i de la identitat de l'individu, s'estableixen unes polítiques de privadesa que tots els sistemes que visitem o en què treballem han de satisfer. Cal demanar una acceptació expressa a l'usuari que accepta les condicions establertes en aquestes polítiques, especialment en aquells llocs on les nostres dades són sol·licitades. El document amb la política de privadesa s'ha de mostrar al primer nivell d'informació previ a la recopilació de dades dels usuaris. A més, per a cada formulari ha de figurar qui és el responsable de les dades, la finalitat de la recollida de les dades, la legitimació, on s'emmagatzemaran i els drets que tenen els usuaris. A la política de privadesa han de figurar:

- La normativa i la legislació aplicable.
- Com s'introdueixen les dades per part dels usuaris.
- Per què s'utilitzaran les dades.
- Perquè han d'introduir les dades i què passarà si no ho fan.
- Quines dades són necessàries per comunicar-se amb la pàgina web o aplicació.
- Compromís de confidencialitat.
- Compromís de no compartir les dades amb tercers.
- Compromís de no enviar publicitat sense el vostre consentiment.
- Informació relativa al dret a cancel·lació, rectificació, portabilitat o limitació de tractament de les dades.

La política de privadesa evita que tercers utilitzin les nostres dades personals si així ho indiquem expressament.

Norma ISO 29100. Protecció de dades i privadesa al núvol

Aquest estàndard internacional proporciona un marc de referència d'alt nivell per a la protecció d'informació d'identificació personal (PII), amb l'objectiu d'ajudar les organitzacions a definir els mecanismes de protecció relacionats amb la privadesa de dades. En concret, la norma especifica una terminologia comuna quant a privadesa; defineix els actors i els seus rols quant al processament d'informació d'identificació personal; indica les recomanacions i consideracions a contemplar per salvaguardar la privadesa; i, estableix els principis de privadesa relatius a les tecnologies de la informació i les comunicacions.

DigitAll

Seguretat

4.3
PROTECCIÓ DE LA SALUT I EL BENESTAR

Seguretat

Nivell A2 4.3 Protección de la salud y el bienestar

Signes i símptomes associats a la salut digital. Casos típics

Signes i símptomes associats a la salut digital. Casos típics

Aquest document us aproximarà al concepte de salut digital i casos típics, juntament amb els principals signes i símptomes més típics associats a la salut digital des d'una perspectiva biopsicosocial, és a dir, la implicació en l'àmbit físic, psicològic i social, corresponent amb el concepte de salut definit per l'Organització Mundial de la Salut.

Casos típics de salut digital

El concepte salut digital abasta l'impacte que té l'ús i l'ús de les Tecnologies de la Informació i les Comunicacions (TIC) sobre la salut i el benestar de les persones. A continuació, es mostraran diferents situacions típiques en què es podria considerar que gaudeixis d'una bona salut digital:

- Respectes els temps de dedicació a la tecnologia, buscant un equilibri en l'ús de la tecnologia i intentant en la mesura que sigui possible dedicar el mínim temps indispensable al seu ús. En cas de fer ús prolongat, respectes i incloguis pauses intercalades en el temps.
- Ets conscient del temps que li dediques a l'ús de la tecnologia i de vegades fins i tot arribes a cronometrar quant de temps exacte estàs dedicant. Periòdicament, revises les estadístiques del telèfon mòbil per veure en quines aplicacions passes més temps.
- Ets conscient que un ús abusiu i descontrolat dels dispositius electrònics et pot portar a una addicció digital. Saps que mantenir-te informat/ada sobre aquest tipus d'addicció t'ajudarà a portar un millor control sobre l'ús de la tecnologia i a preveure'n els efectes.
- Mantens una postura corporal correcta i adequada quan fas ús del telèfon mòbil, de l'ordinador, de la tauleta o de qualsevol altre dispositiu. A més, no fas moviments repetitius i excessius de les mans quan utilitzes els dispositius.
- Mantens una vida social activa a banda de fer ús de la tecnologia, sense estar aïllat o aïllada del món real.

Signes i símptomes associats a la salut digital a escala física

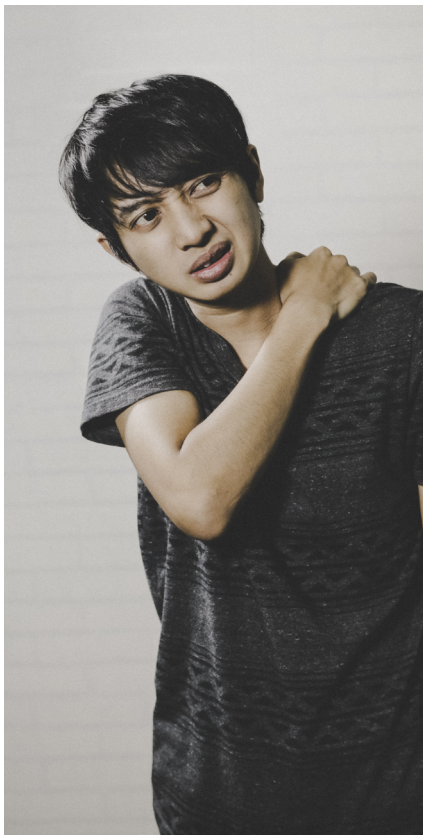
L'ús desmesurat dels aparells o dispositius tecnològics, com romandre molt de temps davant d'una pantalla, pot afectar la nostra salut física. Hauries de tenir cura si identifiques alguns dels casos següents relacionats amb l'ús indegut de la tecnologia dels que podries no ser-ne conscient:

- Sents que veus borrós o que tens la vista cansada després d'haver estat moltes hores observant la pantalla d'un dispositiu tecnològic. Fins i tot, de vegades, pots arribar a veure doble o veure les línies tortes. Poden ser signes o símptomes que cal consultar amb el teu metge de capçalera.

- La teva esquena, espatlles, coll, o mateix les teves extremitats es noten engarrotades (podent arribar a experimentar dolor) després de romandre molt de temps assegut fent ús de les noves tecnologies. És possible que a alçada de la pantalla o del dispositiu de què fas ús, t'estigui provocant que forcis una postura inadequada. Tots aquests signes perllongats en el temps poden donar lloc a lesions cronificades.

- El coll i les mans es presenten entumits o amb un lleuger malestar després de l'ús constant de dispositius mòbils, com el telèfon, o per l'ús repetitiu de les tecles de l'ordinador, que mantingut en el temps pot derivar en situacions més greus.

- Si tens mal de cap més del que és habitual, pot estar relacionat amb haver estat molt de temps observant fixament una pantalla.



Signes i símptomes associats a la salut digital en l'àmbit psicològic

La tecnologia i especialment diverses xarxes socials com Instagram o Facebook poden provocar problemes a escala psicològica a causa de diversos factors. Per això, en aquest punt es tractaran aspectes que ens poden ajudar a identificar alguns problemes que ens provoca la tecnologia a escala psicològica.

- El desenvolupament d'ansietat provocat per la por de perdre o no saber on és el nostre dispositiu electrònic.
- Deixar de fer les activitats de la vida diària que no comporten l'ús de la tecnologia a causa de l'existència de dependència digital.
- Sentir que les teves emocions varien segons l'ús de la tecnologia. D'una banda, el fet de no tenir accés als dispositius tecnològics provoca un sentiment de tristesa i irritabilitat. De l'altra, sents felicitat a causa de la compra o ús d'un nou dispositiu tecnològic.
- Tens una sensació de solitud quan no tens el teu dispositiu a prop. Sents la necessitat d'interactuar amb les persones mitjançant la tecnologia, incrementant en aquest sentit la dependència d'aquests dispositius.
- No ets capaç de fer un ús controlat del dispositiu, xarxes socials o diverses aplicacions durant un període de temps. Això altera els teus hàbits i rutines i provoca una reducció de les teves hores de son.
- Dissocies la teva imatge corporal a causa de l'ús excessiu de filtres de xarxes socials com Instagram o Snapchat per manipular la teva imatge, o bé no t'identifiques amb alguna part del teu cos real, fet que provoca alteracions d'autopercepció estètiques.

Signes i símptomes associats a la salut digital a escala social

La utilització excessiva o descontrolada de dispositius tecnològics pot afectar la manera com ens relacionem amb altres persones. Així, l'ús inadequat de dispositius tan habituals al nostre dia a dia com el mòbil, l'ordinador o una consola poden modificar la manera i la freqüència amb què ens relacionem amb la nostra família, amics, companys de feina i, en general, amb la resta de la societat.

Hi ha alguns signes i símptomes que ens poden indicar que l'ús d'un determinat dispositiu ens està afectant a escala social. La seva identificació pot ajudar-nos a modificar el nostre comportament en una etapa inicial, evitant conseqüències més grans a la nostra vida. A continuació, s'anomenen alguns dels signes i símptomes més comuns:

- Disminuir la freqüència habitual amb què ens reunim amb la família o els amics i preferir invertir aquest temps en l'ús dels dispositius tecnològics.
- Abandonar o reduir activitats esportives o de lleure que solies fer al teu dia a dia.
- Primar les comunicacions en línia sobre la presencialitat, és a dir, optes per parlar per trucada, videotrucada, WhatsApp, entre altres opcions, abans de quedar presencialment amb les persones del teu entorn. Per comoditat pot ser una opció òptima, però perllongat en el temps ens pot aïllar del món real.

ATENCIÓ

El canvi en la manera de relacionar-nos no és un succés immediat, sinó que és un procés progressiu, condicionat per la persona en particular i com gestioni l'ús dels diferents dispositius tecnològics.

NOTA

Després de la pandèmia, de vegades tendim a utilitzar els avantatges de les TIC, en el sentit que mantenim reunions virtuals, videotrucades, entre d'altres, mentre que, el que és recomanable, en la mesura del possible, és mantenir la presencialitat i el contacte físic amb els altres. Els índexs de solitud han augmentat a la població, sent els més afectats els joves i la gent gran, augmentant al seu torn, els suïcidis a la població, i per tant, realçant els problemes de salut mental.

Saber-ne més

Organització Mundial de la Salut. Recomanacions sobre intervencions digitals per enfortir els sistemes de salut.

e.digitall.org.es/directriz-oms

DigitAll

Seguretat

4.4
PROTECCIÓ DEL MEDI AMBIENT

Seguretat

Nivell A2 4.4 Protecció del medi ambient

Impactes ambientals de la tecnologia

Impactes ambientals de la tecnologia

Introducció

Tal com hem vist als diferents vídeos d'aquest nivell, especialment al vídeo 3 "***El consum energètic dels dispositius tecnològics (l'empremta del teu email)" i el vídeo 5 "Utilitzem de manera eficient i sostenible la tecnologia?***" , cada vegada està més clar que l'augment constant de l'ús de la tecnologia digital fa efecte en la salut del planeta. Segons s'assenyala als vídeos i es detalla en un informe de Greenpeace el 2017, la petjada energètica del sector de les tecnologies digitals es corresponia aproximadament amb un 7% del consum total de l'electricitat mundial (Greenpeace, 2017). És una qüestió cada cop més preocupant, tenint en compte el context postpandèmia i l'escenari actual de transició energètica global.

Aquest informe posa el focus en el consum creixent de productes digitals, tant el maquinari com el programari, i en els materials i l'energia que es necessiten per a la seva producció i ús.

Una altra de les qüestions més preocupants és la dels residus tecnològics, que estan en creixement continu i que es relacionen amb el fenomen de les obsolescències, ja siguin la programada, la percebuda o la d'especulació.

⚠ ATENCIÓ

Per exemple, si ens centrem en els telèfons mòbils, els experts adverteixen que el cicle de vida és massa curt, ja que hi ha càlculs que mostren que cada dos anys el 40% dels usuaris canvia de telèfon, mentre que gairebé el 60% han canviat de telèfon més de vuit vegades al llarg de la vida (ONTSI, 2021).

Per tant, encara que els impactes ambientals associats a les tecnologies digitals són múltiples, els podem dividir en tres grans blocs: impactes associats a l'extracció de materials i el procés de producció de dispositius; consum d'energia del sector de les tecnologies digitals; i generació de residus electrònics. Ja que el consum d'energia de la tecnologia digital es va analitzar al nivell anterior, en aquest document ens centrarem en els altres dos blocs esmentats.

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

e.digitall.org.esA4C44A2V03

FEM SERVIR DE MANERA EFICIENT I SOSTENIBLE LA TECNOLOGIA)?

e.digitall.org.es/A4C44A2V05

Impactes de l'extracció de materials per a la tecnologia digital

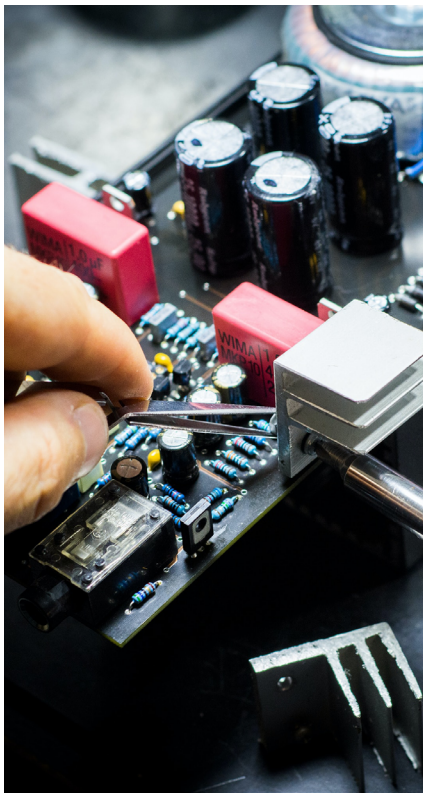
Com ja vam veure al nivell anterior, especialment al vídeo 3 "***Processos de fabricació de recursos tecnològics***", la majoria dels elements necessaris per a la fabricació de dispositius digitals com els telèfons mòbils, però també els ordinadors personals o les tauletes, s'han d'extreure mitjançant activitats mineres.

PROCESSOS DE FABRICACIÓ DE RECURSOS TECNOLÒGICS

e.digitall.org.es/A4C44A1V03

Podem classificar les activitats mineres dins de diferents tipus segons diferents criteris. Si atenem el volum d'extracció, podem parlar de mineria a gran escala, mitjana i petita mineria, i fins i tot de mineria artesanal. També podem classificar-les segons el tipus d'extracció, distingint-se així entre la mineria d'interior o subterrània, i la mineria a cel obert.

Tradicionalment, s'ha utilitzat majoritàriament la mineria en galeria o en petites rases per extreure carbó i altres materials, i fins i tot avui dia se continua utilitzant la mineria artesanal per extreure or i altres minerals en petites quantitats. Però la mineria a cel obert s'està convertint en la fórmula preferida actualment per a l'extracció de materials de tota mena, i especialment els necessaris per al desenvolupament de la tecnologia digital.



Els projectes extractius de mineria a gran escala a cel obert són molt comuns per explotar jaciments de coure o liti. Aquests són essencials per a la indústria digital, però també per als jaciments polimetàl·lics, que contenen diversos minerals en diferents concentracions.

NOTA

La mineria a cel obert és comparativament menys costosa, tant en infraestructura com en mà d'obra, a causa de la gran quantitat de superfície que es pot explotar en un mateix projecte. Però, precisament per això, presenta molts més impactes ambientals i socials per a l'entorn explotat i les comunitats que hi habiten.

Entre els **impactes ambientals de la mineria a cel obert**, podem destacar els següents:

1. **Contaminació atmosfèrica.** Es produeixen impactes a l'atmosfera deguts a les voladures emprades per a l'obertura del tall, i l'arrencada de material, generant soroll intens i emetent grans quantitats de pols a l'aire.
2. **Impactes sobre el terreny.** Principalment la desforestació, l'erosió, la modificació del relleu i la morfologia local pels moviments de terra, a més d'acumulacions de material de rebuig.
3. **Contaminació del sòl.** Als sòls s'alteren diverses propietats físiques i químiques, i fins i tot pot suposar la inutilització absoluta d'aquests per a altres usos com l'agricultura.
4. **Contaminació de les aigües superficials i danys a aqüífers.** Hi pot haver afectacions als cursos dels rius i aqüífers, a més de la contaminació per metalls pesants i variacions de pH de les aigües subterrànies.
5. **Impactes sobre la flora i fauna.** A més de les alternacions directes sobre el terreny que eliminen la flora superficial i desplacen a la fauna, es produeixen canvis a l'hàbitat i contaminació de fonts d'aigua que poden afectar les poblacions.
6. **Contaminació visual.** L'impacte visual generat per l'alteració de la morfologia del terreny, així com dels buits o cràters enormes que es generen durant l'explotació minera.
7. **Conflictes entre comunitats i empreses de mineria,** a causa de l'ús indegut de les terres i amenaça els modes tradicionals de subsistència.

A una altra escala, les disputes pel control dels recursos naturals per al desenvolupament de la tecnologia digital generen conflictes de més importància i intensitat, definits per factors geopolítics i estratègics que seran analitzats en nivells següents.

Residus electrònics i tecnològics

Els aparells elèctrics i electrònics necessaris per al desenvolupament de la tecnologia digital solen ser productes molt complexos que normalment contenen peces i components de diversos tipus, que van des del plàstic, fusta o metall; fins als components de les targetes de circuits impresos o les pantalles de cristall líquid, sense oblidar els cables, piles, bateries o cartutxos d'impressió (Miteco, 2022).

⚠ ATENCIÓ

Segons estimacions del Fòrum Econòmic Mundial i l'OIT, cada any des del 2018 es generen més de 50 milions de tones de residus d'aparells electrònics i elèctrics (RAEE) i és una xifra que va en augment (World Economic Forum, 2019).

D'aquesta quantitat, només se'n recicla formalment menys d'un 20%, mentre que la resta és dipositat en abocadors on aquests residus són abandonats generant diferents tipus d'impactes a l'entorn; o en què milions de persones treballen informalment per recol·lectar, reciclar i rebutjar els residus electrònics, i gran part d'aquest treball és realitzat en condicions nocives tant per a la salut com per a l'ambient (OIT, 2019).

Gran part d'aquests residus que acaben a abocadors no controlats provenen de països del Nord on haurien de ser sotmesos a processos de reciclatge formals. No obstant això, acaben en països on la regulació ambiental és menys estricta, tot i que hi ha un acord internacional, la Convenció de Basilea de Nacions Unides, que regula el trànsit de deixalles perilloses entre països i prohibeix l'anomenat "*dumping* ecològic".

Però aquesta Convenció no és efectiva i els residus tecnològics continuen inundant països com Ghana, Nigèria o Índia. L'informe Forats a l'economia circular: Fuites als residus electrònics d'Europa, redactat per la BAN (Basel Action Network), denuncia que almenys 10 països europeus, entre els quals hi ha Espanya, van exportar de forma il·legal més de 350.000 tones de residus de RAEE el 2017.

NOTA

El mateix informe, a més, detalla com cada persona a Europa genera 17,7 kg de RAEE a l'any, pels 20 kg. de cada nord-americà, mentre a Àfrica la mitjana és d'1,7 kg. per persona.

Com veurem en propers nivells, el reciclatge correcte d'aquests residus, així com el foment de la reducció del consum i la reutilització dels dispositius ja en ús, ens pot portar a pal·liar la problemàtica actual. Els materials valoritzables que contenen suposen un recurs que no s'ha de perdre ni es pot perdre. Per exemple, reciclar de manera correcta i responsable els telèfons mòbils que es rebutgen cada any permetria recuperar grans quantitats de coure, d'or o de liti, per posar exemples de materials que requereixen processos extractius que generen grans impactes ambientals i poden desencadenar conflictes de divers tipus.

No obstant això, aquests aparells o equips també contenen substàncies perilloses que, si bé són necessàries per garantir-ne la funcionalitat, poden generar contaminació ambiental i danys per a la salut humana si, una vegada convertits en residus, els aparells no es gestionen i tracten adequadament.

Per exemple, molts aparells o dispositius poden contenir cadmi, mercuri, plom, arsènic, fòsfor, que són elements amb alta capacitat contaminant. És per això que totes les etapes de la gestió dels RAEE, de la recollida, de l'emmagatzematge, del transport i del tractament s'han de fer en unes condicions segures i que evitin manipulacions o trencaments que puguin alliberar aquest tipus de substàncies perilloses a l'ambient o exposar als treballadors que estan en contacte amb aquests residus, durant el tractament (Miteco, 2019).

El problema principal és que els productes electrònics no estan dissenyats actualment perquè es puguin actualitzar o tenir una vida llarga, de manera que s'agreuja la problemàtica de generació de residus. Davant d'aquesta situació, com ja vam veure al nivell anterior, l'informe "La Dècada Digital d'Europa: metes digitals per al 2030" de la Comissió Europea proposa que els usuaris tinguin accés al coneixement sobre l'impacte mediambiental dels seus dispositius i de les opcions de minimitzar-los.

Davant d'aquesta situació, sembla clar que la gestió responsable de RAEE és de vital importància per assolir els objectius de desenvolupament sostenible. Tractar-los correctament ajudaria a millorar la salut i el benestar de les persones i de l'entorn, a més de contribuir a una transformació del model de producció i consum cap a alternatives més sostenibles.

Però, per descomptat, aquesta qüestió no és només responsabilitat de les consumidors de tecnologia digital. Cal posar el focus en processos col·lectius, i promoure la col·laboració entre les multinacionals, les petites i mitjanes empreses (PIME), els emprenedors, les universitats, els sindicats, la societat civil i les associacions empresarials per tal de crear les vies necessàries per assolir progressivament una economia circular de l'electrònica on es limiti el malbaratament de recursos i materials, es redueixi l'impacte ambiental i es creïn feines decents per a milions de persones (OIT, 2019).

Saber-ne més

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

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

Lillo (2010). *Impactes de la mineria al medi natural.*
e.digitall.org.es/impactos-minería

Miteco (2019). *Aparells elèctrics i electrònics.*
e.digitall.org.es/miteco

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.digitall.org.es/tendencias-uso-dispositivos

Organització Internacional del Treball (2019). *50 milions de tones de residus electrònics es rebutgen cada any.*
e.digitall.org.es/residuos-tecnologicos

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

World Economic Forum (2019). *A New Circular Vision for Electronics.*
e.digitall.org.es/vision-electronics

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