DigitAll

Formació en Competències Digitals

4

Seguretat

DigitAll

Formació en competències digitals

Seguretat

Nivell C2

ÍNDEX

DigitAll

Seguretat

4.1 PROTECCIÓ DE DISPOSITIUS

Seguretat

Nivell C2 4.1 Protecció de dispositus

Pla de resposta a incidents

Pla de resposta a incidents

Un pla de resposta a incidents és un conjunt de procediments i mesures dissenyades per manejar de manera eficient i efectiva els incidents de seguretat de la informació o de ciberseguretat que puguin ocórrer en una organització.

Els objectius d'un pla de resposta a incidents són minimitzar l'impacte, restaurar la normalitat, protegir els actius d'informació, identificar la causa arrel, complir amb els requisits legals i normatius, i millorar contínuament les capacitats de resposta de l'organització.

Les etapes d'un pla de resposta a incidents poden variar segons la metodologia o guia que se segueixi en la seva implementació, però en totes solen existir les següents o una variant d'aquestes:

1 | **Preparació:** aquesta etapa s'enfoca en la preparació prèvia a l'incident. Inclou la creació i documentació del pla de resposta a incidents, la designació i capacitació de l'equip de resposta, la identificació i classificació dels actius crítics de l'organització, i l'establiment de polítiques i procediments clars.

2 | **Detecció i notificació**: en aquesta etapa, es monitoren els sistemes i s'utilitzen eines de detecció per identificar possibles incidents que hauran de ser notificats a l'equip de resposta.

3 | **Avaluació i classificació**: en aquesta etapa, es du a terme una avaluació inicial de l'incident per determinar la seva naturalesa, abast i gravetat.

4 | **Contenció i mitigació**: en aquesta etapa, es prenen mesures per contenir i limitar l'impacte de l'incident. L'objectiu és evitar que l'incident es propagui i causi més mal.

5 | **Recerca i anàlisi:** després de contenir l'incident, es du a terme una recerca exhaustiva per comprendre la causa arrel i el mètode d'atac. L'anàlisi ajuda a comprendre com va ocórrer l'incident i quines mesures s'han de prendre per a evitar futurs incidents similars.

6 | **Recuperació i restauració:** una vegada que s'ha contingut i s'ha fet la recerca, es procedeix a la recuperació i restauració dels sistemes afectats.

GESTIÓ

Gestió d'incidents i disseny de polítiques d'aquest tipus en les organitzacions. Tipus d'incidents de seguretat i passos més comuns. Pla de contingència i de continuïtat de negoci.

e.digitall.org.es/A4C44C1V02

7 | Lliçons apreses: després de completar la resposta a l'incident, es fa una revisió i anàlisi exhaustiva de les accions preses per millorar el pla de resposta a incidents i enfortir les mesures de seguretat de l'organització.

Per ajudar-nos en la implementació d'aquesta mena de plans disposem principalment de dues eines, la norma ***ISO 27035*** (*e.digitall.org.es/iso-27035*) i la guia ***NIST SP 800-61*** (*e.digitall.org.es/nist-sp800-61*).

ISO 27035

La norma ISO 27035 és un estàndard internacional d'ISO que proporciona directrius i millors pràctiques per al maneig d'incidents, esdeveniments i vulnerabilitats de seguretat de la informació.

Se centra profundament en la gestió d'incidents de seguretat de la informació i abasta tot el cicle de vida d'un incident, des de la preparació i detecció fins a la resposta, recuperació i aprenentatge.

Està dissenyada per a ajudar les organitzacions a establir i millorar les seves capacitats de resposta a incidents i a mitigar els impactes negatius dels incidents de seguretat. Aquesta norma es pot considerar com una expansió de la secció d'administració d'incidents de seguretat prevista a l'ISO 27002.

NIST SP 800-61

La NIST SP 800-61 és una guia publicada pel National Institute of Standards and Technology (NIST) dels Estats Units que pretén ajudar les organitzacions en l'establiment de la seguretat informàtica necessària per tenir la capacitat de resposta davant incidents i el seu tractament de manera eficient. Aquesta publicació ofereix pautes per a la gestió d'incidents, sobretot per a l'anàlisi de dades i determinar la resposta apropiada per a cada tipus.

Aquestes directrius es poden seguir de manera independent segons la plataforma de maquinari, sistema operatiu, protocols o aplicacions utilitzades.

Igual que l'ISO 27035 aborda tots els aspectes del cicle de vida de la gestió d'incidents i és àmpliament reconeguda com una guia de referència per al maneig d'incidents de seguretat de la informació.

Seguretat

Nivell C2 4.1 Protecció de dispositius

Vulnerabilitats més esteses: OWASP Top 10

Vulnerabilitats més esteses: OWASP Top 10

Les tecnologies web són una part fonamental de la nostra vida digital. La majoria dels serveis que utilitzam diàriament, des de la banca electrònica o la gestió de la salut digital, estan implementats sobre les tecnologies web: pàgines, aplicacions i servidors web que utilitzen principalment HTML, CSS i JavaScript per funcionar.

En aquesta secció s'introdueix la importància de la seguretat de les aplicacions web i les vulnerabilitats característiques d'aquestes tecnologies. Per això s'aprofundeix en una de les referències més esteses i consensuades de categorització de vulnerabilitats web, l'OWASP Top 10.

L'**OWASP Top ten (Open Web Application Security Project Top ten)** és una llista de les deu vulnerabilitats de seguretat més crítiques en aplicacions web. Va ser creada pel Projecte OWASP, una comunitat d'experts en seguretat d'aplicacions web que es dedica a millorar la seguretat del programari.

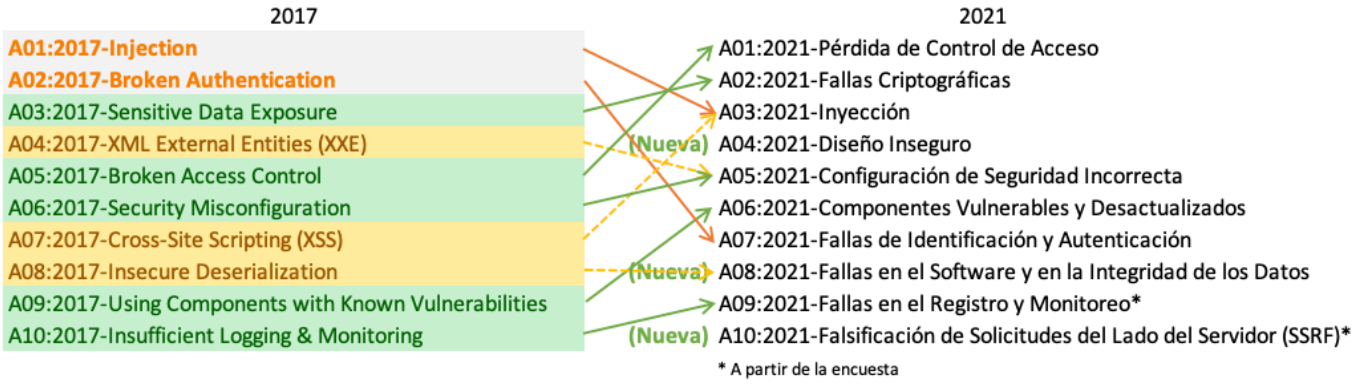
Web oficial de l'OWASP Top 10
owasp.org/www-project-top-ten

El propòsit principal de l'OWASP Top ten és proporcionar una guia perquè els desenvolupadors, professionals de seguretat i organitzacions comprenguin les **principals amenaces a les quals s'enfronten les aplicacions web** i prenguin mesures per mitigar aquests riscos.

La llista s'actualitza periòdicament per a reflectir les noves amenaces i tendències en seguretat d'aplicacions web. La darrera versió publicada, en data d'elaboració d'aquest document, és l'**OWASP Top 10 2021**. No obstant això, un coneixement molt interessant és el que ens brinda la possibilitat de comparar la versió anterior, l'OWASP Top 10 2017, amb la versió actual, per a conèixer quines són les tendències en els darrers anys pel que fa a amenaces web. En els següents subapartats s'explica en què consisteixen les vulnerabilitats de cada categoria, les quals estan identificades per un codi, de la forma "A<ranking>:2021".

NOTA

La informació utilitzada per elaborar aquesta catalogació de les vulnerabilitats web prové de diverses fonts, com a informes, anàlisis d'incidents, enquestes, etc. Aquestes dades són subministrades per experts de seguretat i empreses especialitzades en el sector, el treball diari del qual es basa a desenvolupar i garantir la seguretat d'aquesta mena d'aplicacions.



Pèrdua del control d'accés

La primera de les categories del OWASP Top 10 2021 és "A01:2021-Broken Access Control", o pèrdua del control d'accés. Aquest tipus de vulnerabilitats es refereixen a situacions en les quals un sistema permet l'accés no autoritzat, de manera equivocada, a unes certes funcionalitats o dades.

Un exemple d'això és quan un usuari sense privilegis pot accedir a informació confidencial o dur a terme accions que haurien d'estar restringides, com modificar registres d'altres usuaris o accedir a seccions administratives sense autorització adequada.

Cal destacar la tendència que estam vivint en els darrers anys amb aquesta mena de vulnerabilitats, que han pujat de la posició número cinc a la primera des de la versió del 2017 del rànquing.

Fallades criptogràfiques

La segona categoria de l'OWASP Top 10 2021 és "A02:2021-Cryptographic Failures", en català, "fallades criptogràfiques". Aquesta categoria s'enfoca en les febleses relacionades amb l'ús inadequat d'algorismes criptogràfics, gestió de claus i emmagatzematge segur de dades. Aquestes utilitats s'utilitzen per a garantir la confidencialitat i integritat de les dades, tant dels usuaris com de les aplicacions.

Un exemple comú de fallades criptogràfiques és l'ús d'algorismes de xifratge febles o vulnerables, com l'ús de xifratge obsolet o l'emmagatzematge insegur de claus, la qual cosa podria permetre a un atacant desxifrar dades confidencials.

En la versió anterior d'aquesta guia, aquesta categoria era coneguda com a "Sensitive Data Exposure", o exposició de dades delicades, situada en la tercera posició d'aquest. En la versió actual, ha pujat un lloc fins a col·locar-se en la segona de les vulnerabilitats més crítiques.

Injecció

El tercer tipus de vulnerabilitats s'agrupen en la categoria "A03:2021-Injection", les vulnerabilitats d'injecció. Aquesta categoria agrupa aquelles vulnerabilitats que consisteixen en la inserció no desitjada de codi maliciós en aplicacions web, generalment a través de camps d'entrada no filtrats o mal validats.

XSS I SQL INJECTION

Conceptes de Cross-Site Scripting (XSS) i SQL Injection (SQLi), destacant la seva rellevància dins del context de la seguretat de les aplicacions web. S'expliquen les conseqüències d'aquesta mena d'atacs i com protegir-se'n.

e.digitall.org.es/A4C41C2V05

En OWASP Top ten 2017 aquesta vulnerabilitat ocupava la primera posició, i encara que en els darrers anys hagi caigut en el rànquing respecte d'altres categories, continua sent una de les vulnerabilitats més crítiques de la seguretat web.

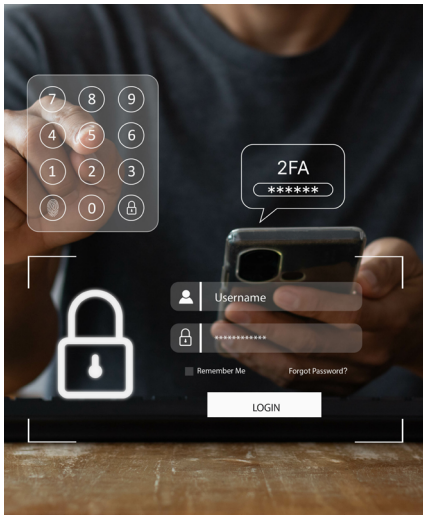
Disseny insegur

La categoria "A04:2021-Insecure Design" o disseny insegur agrupa les fallades de disseny que poden comprometre la seguretat d'una aplicació. Això implica la falta de consideració dels principis de seguretat des de l'inici del procés de desenvolupament.

Un exemple seria la falta d'autenticació adequada en un sistema, on no s'implementen mesures sòlides per verificar i autoritzar els usuaris, la qual cosa permet l'accés no autoritzat a recursos o dades confidencials.

Aquesta és una de les categories noves, que no existien a la versió de 2017, del rànquing OWASP Top 10.

Configuració de seguretat incorrecta



En cinquè lloc, es troben les vulnerabilitats "A05:2021- Security Misconfiguration" o de configuració de seguretat incorrecta. Aquestes es refereixen a la configuració incorrecta de components de l'aplicació i dels servidors que poden permetre l'accés no autoritzat o exposar informació delicada.

Un exemple seria deixar accessibles directoris o arxius confidencials a través de la configuració incorrecta de permisos d'arxius o configuracions de seguretat en un servidor web.

Components vulnerables i desactualitzats

Aquesta categoria, "A06:2021-Vulnerable and Outdated Components" o components vulnerables i desactualitzades, destaca els riscos associats amb l'ús de components de programari que contenen vulnerabilitats conegudes o desactualitzades.

Un exemple seria utilitzar una biblioteca o connector obsolets en una aplicació web, que té vulnerabilitats conegudes i que podrien ser explotades per un atacant per comprometre la seguretat de l'aplicació.

Fallades d'identificació i autenticació

La setena categoria del rànquing és "A07:2021-Identification and Authentication Failures", que en català significa fallades d'identificació i autenticació. Es refereix a febleses en els mecanismes d'identificació i autenticació d'usuaris en una aplicació web. Això pot incloure contrasenyes febles, manca de protecció contra atacs de força bruta o vulnerabilitats en el procés de recuperació de contrasenyes.

Un exemple és la falta de bloqueig de comptes després d'un nombre determinat d'intents fallits d'inici de sessió, la qual cosa facilita els atacs de força bruta.

Fallades en el programari i en la integritat de les dades

La vuitena categoria del OWASP Top 10 2021 és nova respecte de la versió de 2017, i és "A08:2021-Programari and Data Integrity Failures" o fallades en el programari i en la integritat de les dades. Aquesta categoria se centra en els riscs relacionats amb la integritat i el comportament correcte del programari, així com en la manipulació no autoritzada de dades crítiques.

Un exemple seria una aplicació que no fa una validació adequada de les dades d'entrada, la qual cosa podria permetre la introducció de dades malicioses que podrien causar fallis en l'aplicació o comprometre la seva integritat.

Fallades en els registraments i monitoratge de la seguretat

En la novena posició es troba "A09:2021-Security Logging and Monitoring Failures" o fallades en el registre i monitoratge de la seguretat. Aquesta vulnerabilitat es refereix a la falta d'un registre i monitoratge adequat d'esdeveniments i activitats d'una aplicació web. Això pot dificultar la detecció i resposta davant incidents de seguretat.

Un exemple seria l'absència d'un sistema de logs d'esdeveniments de seguretat, la qual cosa dificulta la identificació d'activitats sospitoses o atacs en curs.

Falsificació de sol·licituds del costat del servidor

Finalment, ens trobem amb una categoria molt específica, "A10:2021-Server-Side Request Forgery" o la falsificació de sol·licituds del costat del servidor. Aquesta categoria es refereix a atacs en els quals un atacant pot enganyar el servidor perquè facu accions no desitjades en nom de l'usuari legítim.

Un exemple comú és l'atac CSRF (Cross-Site Request Forgery), on un atacant enganya l'usuari perquè dugui a terme accions sense el seu consentiment, com canviar la seva contrasenya o gestionar transaccions no autoritzades.

Seguretat

Nivell C2 4.1 Protecció de dispositius

Xarxa TOR

Xarxa TOR

La xarxa TOR és la xarxa anònima a Internet més coneguda. Permet navegar per serveis ocults de la *dark web*, però també accedir a qualsevol servei d'Internet. Tot això, de manera anònima. A continuació, es defineix què és l'anonimat, les xarxes anònimes i TOR.

Anonimat i privacitat

La privacitat i l'anonimat són dos termes relacionats, però el seu significat és diferent.

La privacitat es refereix al dret d'una persona a controlar la informació que revela sobre si mateixa i a decidir qui hi té accés. En l'àmbit digital, la privacitat implica protegir les dades personals i assegurar que només siguin accessibles per les persones autoritzades. Això implica tenir control sobre quina informació es recopila, com s'utilitza, qui l'utilitza i com es comparteix.

L'anonimat, d'altra banda, es refereix a la capacitat d'ocultar la identitat d'una persona o mantenir-la desconeguda. Implica la possibilitat d'executar activitats en línia sense revelar informació personal identificable, com a nom, adreça o qualsevol altra dada que permeti identificar la persona darrere d'una acció.

Existeixen diferents motius pels quals una persona necessita l'anonimat a la xarxa:

- **Llibertad d'expressió:** expressar les opinions lliurement sense por de represàlies, sobretot de governs o organitzacions repressives.
- **Connexió de persones:** connectar-se en comunitats i grups que comparteixin interessos similars sense por de la repressió.
- **Llibertat de recerca:** cercar informació sense por de ser jutjats o discriminats.
- **Periodisme i activisme:** filtracions d'informació o publicació de notícies sobre governs.

Tant la privacitat com l'anonimat són importants com a drets digitals per a protegir la informació personal o identitat en l'entorn digital. No obstant això, és important tenir en compte que l'anonimat absolut pot plantejar desafiaments per a l'aplicació de la llei i la responsabilitat en línia, ja que pot permetre activitats il·legals sense deixar rastre.

Xarxes anònimes a Internet: *deep web* i *dark web*

Existeixen diferents alternatives per aconseguir anonimat a Internet. Ja hem vist algunes opcions com l'ús de xarxes virtuals (VPN) o *proxies*, la qual cosa permeten ocultar l'adreça IP d'origen o ubicació geogràfica. Tanmateix, això requereix confiança en el proveïdor de VPN o proxy.

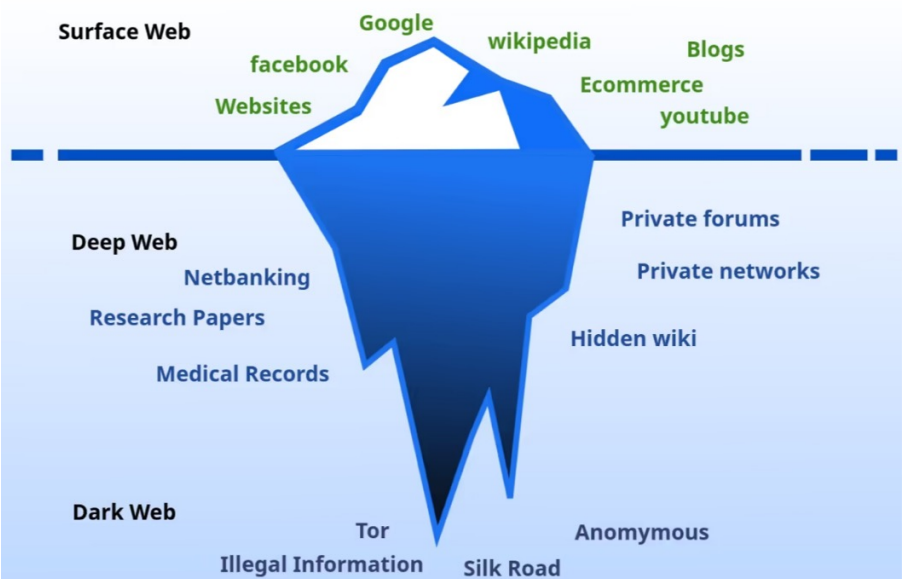
VPN, PROXIES I ANONIMAT EN LA XARXA

Les xarxes privades virtuals o VPN juntament amb els proxies permeten connectar-se a diferents xarxes o llocs web sense utilitzar l'adreça IP pròpia. D'aquesta manera, permeten accedir a serveis i recursos en Internet amb un cert nivell d'anonimat.

e.digitall.org.es/A4C41C2V09

Per aquest motiu, diverses iniciatives han creat el que es coneixen com a xarxes anònimes. Les xarxes anònimes utilitzen Internet per a crear protocols de comunicació que garanteixin l'anonimat dels usuaris. Per exemple, les xarxes Freenet i Invisible Internet Project (I2P) permeten als usuaris connectats compartir continguts i comunicar-se de manera anònima. TOR, que veurem a continuació, és una xarxa anònima que, a més de permetre accedir a contingut dins de la mateixa xarxa, permet la connexió a serveis exposats a Internet. És a dir, fora de la xarxa anònima.

Internet permet compartir informació a través del web, però també crear xarxes anònimes que comparteixin contingut de manera anònima. La diferència entre el web convencional i les xarxes anònimes se sol representar amb la següent imatge.



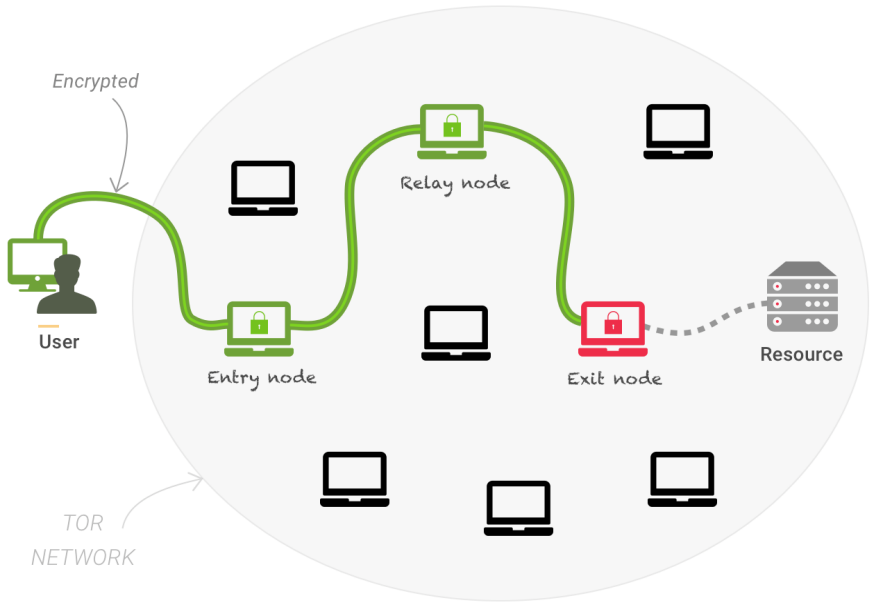
El web superficial o **Surface web** fa referència a totes les pàgines web a les quals es pot accedir de manera convencional a través d'Internet. A més, aquests continguts són indexats pels cercadors, com Google o Bing. Per tant, es poden trobar i accedir fàcilment. Realment, aquest tipus de contingut representa una petita part de tot el contingut que pot accedir-se a través d'Internet. D'aquesta manera, els continguts com a fòrums privats, xarxes privades o qualsevol contingut que no es pugui accedir sense passar un control d'accés, es coneix com la *deep web*. Això és informació que no està accessible de manera directa, ni que pot trobar-se emprant cercadors com Google.

Finalment, les xarxes anònimes formen part de la ***dark web***. Aquests continguts només són accessibles a través d'aquestes xarxes, utilitzant aquesta tecnologia.

The Onion Router (TOR)

El projecte The Onion Encaminador (TOR) ofereix un programari que permet a l'usuari connectar-se a la xarxa TOR i accedir a continguts de manera anònima. Aquest programari utilitza el protocol de comunicacions "*onion routing*" o "encaminador ceba". Per assegurar l'anonimat de l'usuari, l'*onion routing* utilitza, almenys, dos nodes repetidors o "relays".

Per connectar-se a un lloc web, un usuari es connectarà a un node repetidor qui, al seu torn, es connectarà a un altre repetidor. El darrer node repetidor és qui, al final, es connectarà al lloc web.



D'aquesta manera, el primer node repetidor és l'únic que coneix a l'usuari, però no sap on es connectarà. Així mateix, només el darrer repetidor sabrà on es connecta, però desconeix la identitat de l'usuari que ha iniciat la connexió. Per accedir a la xarxa TOR només és necessari descarregar el ***navegador TOR*** (*torproject.org*). Aquest navegador basat a Firefox permet connectar-se i navegar per la xarxa TOR, composta de serveis ocults recognoscibles pels dominis ".ONION".

⚠ ATENCIÓ

La Hidden Wiki és un servei ocult accessible en la xarxa TOR. Per accedir-hi, és necessari utilitzar el navegador TOR i emprar el domini ".ONION" d'aquest lloc web:

http://paavlaytlfsqyvkg3yqj7hflfg5jw2jdg2fgkza5ruf6lplwseeqtvyd.onion/

Finalment, és important tenir en compte algunes recomanacions. Per navegar per TOR és recomanable fer-ho connectat a una VPN. A més, és molt important tenir en compte que a la xarxa TOR preval l'anonimat, per la qual cosa cal tenir molt de compte amb la ciberdelinqüència i navegar amb cautela.

Seguretat

Nivell **C2** 4.1 Protecció de dispositius

Solucions d'anonimat a la xarxa

Solucions d'anonimat a la xarxa

Una vegada hem vist què és l'anonimat a la xarxa, en aquest apartat se citaran diferents utilitats que has de conèixer per mantenir la teva identitat protegida.

XARXA TOR

Document referenciat: ***A4C41C2D03***

Serveis VPN

Les xarxes privades virtuals permeten connectar-se de manera remota a una xarxa. En l'ús domèstic, els serveis VPN s'utilitzen per accedir a llocs web de manera anònima o per poder consultar contingut disponible només per a uns certs països.

És important assegurar-se d'utilitzar una VPN de pagament que siguin de confiança. Els serveis VPN han de tenir una política de privacitat estricta, igual que els proveïdors de connexió a Internet.

NordVPN

NordVPN és un dels serveis més coneguts de VPN, amb més de 5700 servidors al voltant de 60 països. A més, és compatible amb multitud de dispositius, com per exemple, Linux, MacOS i Windows, però també uns altres com a dispositius mòbils i, fins i tot, Android TV.

NordVPN

NordVPN
nordvpn.com/es

ProtonVPN

ProtonVPN és un servei oferit per una empresa suïssa que aposta per la privacitat dels usuaris. Permet emprar fins a 10 dispositius i ofereix altes velocitats. A més, permet configurar serveis com a blocador d'anuncis i privacitat avançada. Igual que NordVPN, suporta un gran ventall de dispositius.

Proton VPN

ProtonVPN
protonvpn.com/es

Mullvad VPN

Mullvad VPN és un servei que promociona un alt nivell de privacitat i anonimat per als seus usuaris, ja que permet registrar-se i pagar el servei de manera anònima. Té aplicacions fàcils d'emprar i senzilles.

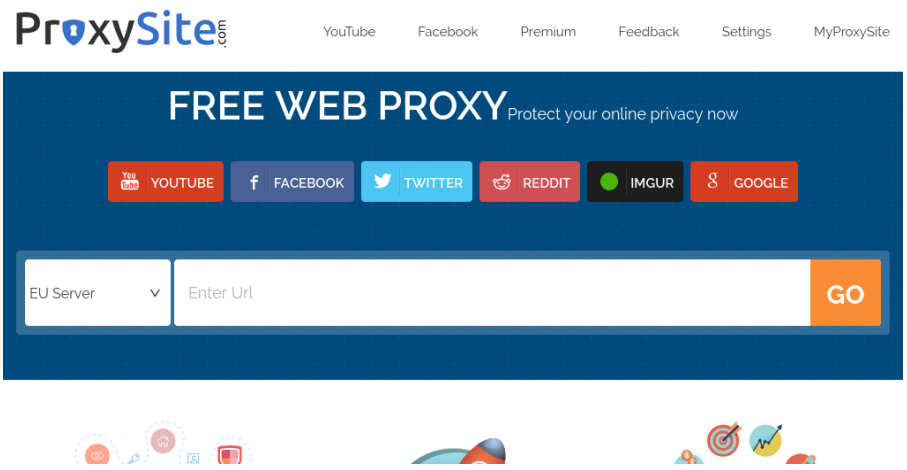
MULLVAD VPN

ProtonVPN
mullvad.net/es

Serveis Proxy

D'altra banda, existeixen serveis que permeten fer consultes web en el nostre nom. És a dir, permeten utilitzar un intermediari per a navegar per webs sense exposar l'adreça IP. És destacable comentar que la majoria d'aquests serveis ja s'han mudat a serveis VPN.

ProxySite



Proxysite és un servei que permet consultar qualsevol web a través del seu lloc web. Només amb una adreça URL, es poden visualitzar continguts bloquejats o disponibles exclusivament a altres països.

ProxySite
proxysite.com

IP Vanish

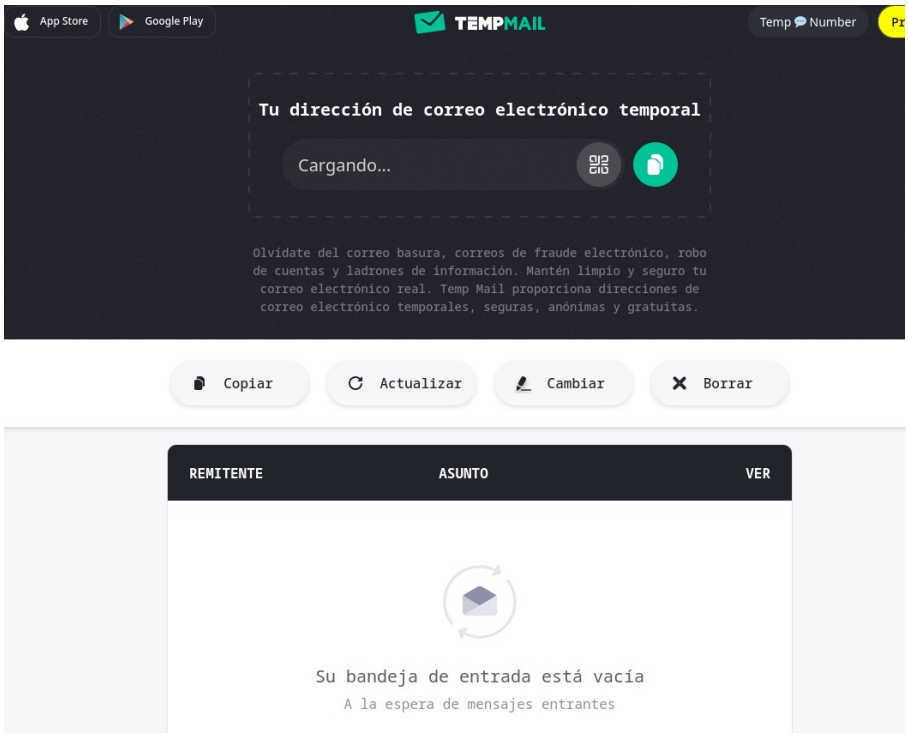
A més d'una VPN, IP Vanish ofereix un servei de proxy amb la tecnologia SOCKS5. Aquesta tecnologia es pot configurar com proxy en diferents aplicacions, com a missatgeria instantània o el navegador web.

IP VANISH
ipvanish.com/socks5-proxy

Mantenir la identitat anònima

L'anonimat a la xarxa requereix un esforç considerable. Encara que s'utilitzi TOR, per mantenir l'anonimat és molt important mantenir oculta qualsevol dada personal identificable.

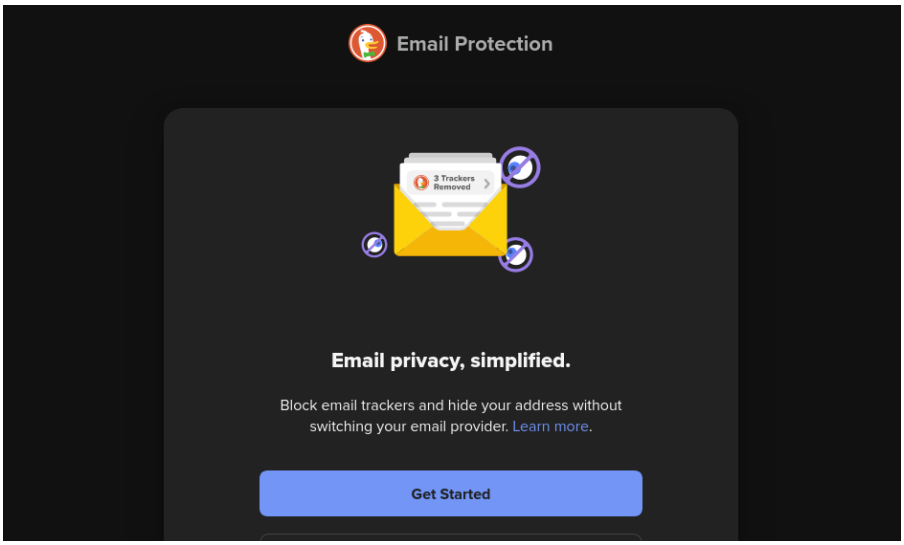
Safata de correu temporal



TEMPMAIL
temp-mail.org/es

En primer lloc, existeixen serveis en línia que requereixen una adreça de correu electrònic per registrar-se. Per evitar emprar el correu personal, es poden utilitzar els serveis de correu temporal. Un dels més coneguts és "Temp Mail", encara que existeixen uns altres. És important tenir en compte que aquest servei és temporal, per la qual cosa perdrem accés a aquesta adreça de correu passat el període d'ús.

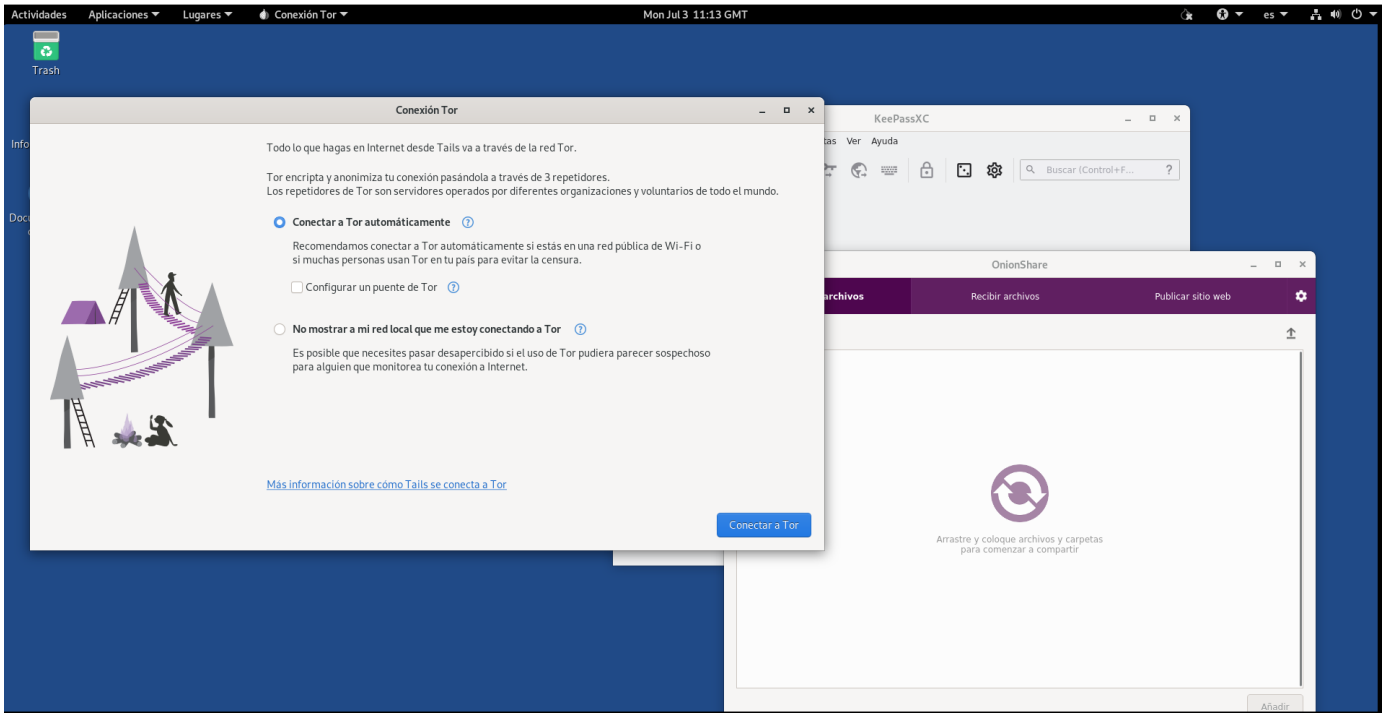
DuckDuckGo Email Protection



DuckDuckGO
duckduckgo.com/email

Si volem mantenir l'accés al correu temporal o utilitzar el nostre compte sense revelar l'adreça de correu real, podem emprar un proxy de correu electrònic. Això ens permet ocultar l'adreça de correu electrònic real després d'una adreça de correu aleatòria. Un dels serveis més coneguts és DuckDuckGo Email Protection, del famós cercador. Una vegada creat un compte, permet crear "àlies" o pseudònims de l'adreça de correu real.

TailsOS: sistema operatiu anònim



TailsOS és un sistema operatiu que unifica diverses tecnologies per oferir un nivell alt de privacitat i anonimat per a l'ús diari. Per defecte, empra TOR per a la connexió a Internet.

TailsOS
tails.net

Aquest sistema operatiu pretén executar-se en qualsevol ordinador des d'un USB, el qual intenta evitar qualsevol sistema operatiu no fiable i proporciona "amnèsia". És a dir, minimitza el registre de qualsevol activitat.

DigitAll

Seguretat

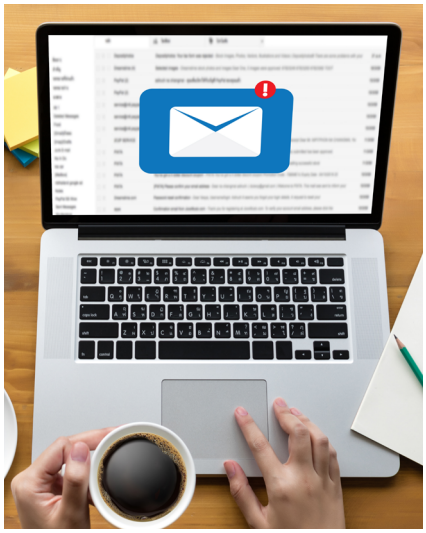
4.2
PROTECCIÓ DE LES DADES PERSONALS I LA PRIVACITAT

Seguretat

Nivell C2 4.2 Protecció de los dades personals i la privacitat

Privacitat al correu electrònic

Privacitat al correu electrònic



L'ús del correu electrònic està àmpliament estès en l'actualitat. S'estima que l'any 2022 es van enviar més de 330.000 milions de correu electrònic entre uns 4.000 milions d'usuaris. Amb tal volum, el correu electrònic és un negoci tan ampli que hi ha múltiples empreses involucrades. Fins i tot algunes que ofereixen de manera gratuïta el servei de correu electrònic. Independentment del nombre d'emails i de la plataforma o aplicació de correu electrònic utilitzat, és necessari garantir que la privacitat dels usuaris no es vegi compromesa.

Webmail

El correu electrònic o e-mail es pot utilitzar tant a través d'aplicacions com de plataformes web. Aquest darrer mecanisme és un servei al núvol que es denomina webmail. Utilitzant aquest sistema, els usuaris poden enviar i rebre correus sense necessitat d'instal·lar cap aplicació.

Existeixen moltes empreses que ofereixen webmail, algunes de pagament i altres de manera gratuïta. Aquestes ofereixen adreça d'email per a rebre i enviar correus electrònics des de la web, encara que alguns proveïdors proporcionen alguns serveis addicionals: connexió amb clients de correu electrònic, encriptació de correus, etc.

El webmail oferit per moltes empreses no ens costa diners, perquè el cost li ho cobren amb la nostra privacitat.

Aquestes empreses volen que les nostres dades i els nostres perfils d'ús de l'email per poder vendre-l'hi a tercers. Analitzarem algunes de les pràctiques que poden posar en risc la nostra privacitat.

Riscos de privacitat en l'ús de webmail

En emprar serveis webmail, si no prenem algunes precaucions, podem estar deixant desprotegida molta informació. El principal motiu és perquè, tret que es contracti i s'activi, els missatges s'envien sense encriptar.

⚠ ATENCIÓ

El contingut és accessible a qualsevol sistema intermedi.

El segon motiu és que els mateixos servidors webmail emmagatzemen els missatges desencriptats, per la qual cosa, el mateix servidor pot accedir al contingut amb una potencial pèrdua de privacitat. Els servidors argumenten la necessitat d'aquest accés per poder classificar els missatges rebuts i integrar-los en diferents serveis al núvol, com el calendari personal, les notes, etc.

⚠ ATENCIÓ

Els servidors poden accedir al contingut dels nostres missatges i dades.

Finalment, en funció del país en el qual es trobi el servidor, els serveis de seguretat d'aquest país podrien accedir al contingut dels teus emails, simplement amb una sol·licitud al proveïdor. Per exemple, si el servidor està als EUA, la CIA o la NSA podrien obtenir els teus correus amb una simple petició al proveïdor.

⚠ ATENCIÓ

Entitats estrangeres poden accedir a les nostres dades i missatges, sense la nostra autorització.

Gmail

El servei d'email de Google es diu Gmail i, probablement, és el servei webmail més utilitzat del món, precisament per la seva integració amb tot l'ecosistema de serveis i aplicacions de Google.

Des de 2017, Google no accedeix als teus emails per defecte, has d'autoritzar-lo per poder tenir una integració efectiva. En aquests casos, Gmail utilitza el seu servei d'anàlisi del contingut dels teus emails per poder oferir-te anuncis més adaptats als teus interessos, detectar possibles cites i incloure-les en el teu calendari, creuar perfils d'ús del navegador en el qual accedeixes a webmail amb les cerques, etc.

En el cas d'utilitzar dispositius amb la ubicació activada, Gmail és capaç d'establir la localització des d'on s'accedeix al webmail, amb la pèrdua de privacitat que això comporta.

PRIVACITAT EN EL NÚVOL

Com establir mesures per evitar la pèrdua de privacitat en emprar serveis en el núvol? Entre altres, com evitar que situïn la localització des d'on accedim?

e.digitall.org.es/A4C42C2V04

Gmail no proporciona un sistema d'encriptació dels missatges ni de signatura digital. Pel que no és possible enviar missatges xifrats ni signats digitalment sense l'ús d'extensions.

Hotmail, Outlook.com

Microsoft va llançar diferents plataformes webmail, encara que a poc a poc totes han anat migrant cap a un mateix servei. Tant és així que si en el navegador cerques ***Hotmail*** (***hotmail.com***) te redirecciona cap a ***Outlook*** (***outlook.com***).

Outlook sí que té un sistema reforçat de seguretat amb l'encriptació dels correus electrònics.

Igual que Gmail, el contingut del correu electrònic a Outlook es pot vincular a l'ecosistema d'aplicacions de Microsoft Office en el núvol, encara que no és automàtic sinó que l'usuari ha d'activar en cada cas la transferència del contingut cap a cada aplicació.

Outlook és un sistema webmail una mica menys intrusiu que Gmail, encara que presenta característiques que afecten la privacitat dels usuaris en certa manera.

Altres sistemes webmail de major privacitat

Altres proveïdors han tingut en compte les exigències d'alguns usuaris que sol·licitaven un major grau de privacitat que les plataformes webmail descrites en els punts anteriors i van llançar altres plataformes webmail amb més privacitat.

Sistemes com ***ProtonMail*** (***proton.me***), amb seu a Suïssa, o ***tutanota*** (***tutanota.com/es***), amb seu també a Suïssa, o tutanota (tutanota.com/es), amb seu a Alemanya, incorporen diferents mesures de privacitat. El fet d'estar fora del territori dels EUA reforça la privacitat, en tant que no és possible l'accés al contingut dels correus electrònics, excepte per mandat judicial.

ProtonMail utilitza una doble contrasenya: la primera per a accedir al servei i la segona, per desencriptar la bústia. Així, es fa un xifratge en el mateix navegador del client usant aquesta segona contrasenya, desconeguda totalment per ProtonMail. Per tant, tots els missatges s'envien xifrats des del client i ProtonMail no pot accedir al contingut dels correus en cap cas.

Tutanota és un servei de webmail xifrat d'extrem a extrem d'alta seguretat, basat en l'ús de programari lliure. En el cas d'enviar missatges a un usuari que no estigui en Tutanota, es crea un enllaç a un compte temporal de Tutanota en la qual, introduint una clau, prèviament intercanviada amb l'usuari destinatari, podrà llegir el missatge desencriptat.

Aplicacions de correu electrònic

Una altra opció és la utilització d'aplicacions en el teu ordinador, tauleta o telèfon intel·ligent que s'encarreguin de l'enviament dels correus electrònics directament sense accedir a les plataformes webmail.

Si bé l'anterior és cert amb caràcter general, d'igual manera, cal mantenir algunes mesures per garantir la privacitat. Aquestes mesures són encara més necessàries en el cas de dispositius mòbils.

⚠ ATENCIÓ

Les aplicacions de correu electrònicsón més segures i privades que les versions webmail.

PRIVACITAT EN DISPOSITIUS MÒBILS

Diverses consideracions per garantir la nostra privacitat en l'ús de dispositius mòbils.

e.digitall.org.es/A4C42C2V03

Riscos de privacitat a l'hora d'usar aplicacions de correu electrònic

Com s'ha indicat, la utilització d'aplicacions de correu electrònic és molt més segura i té una major garantia de privacitat que l'ús de webmail. No obstant això, com qualsevol servei interconnectat pot presentar alguns riscos enfront de la privacitat.

La inclusió d'imatges, vídeos i altres elements HTML allotjats en servidors remots implica un risc. En descarregar-se els diferents elements, el servidor on està allotjat és capaç d'obtenir informació de l'aplicació de correu electrònic: quan s'usa, adreça IP, sistema utilitzat, etc.

⚠ ATENCIÓ

L'ideal és tenir configurat per defecte el bloqueig automàtic de descàrregues de remitents desconeguts.

Un altre risc és la resposta automàtica de confirmació de recepció de missatge. D'aquesta manera, l'emissor de correu electrònirc té constància que has rebut el correu i que l'has obert. Analitzant la reposada automàtica, l'emissor original pot obtenir informació del receptor: que és una adreça d'*email* activa, l'adreça IP des de la qual s'ha manat la resposta automàtica, etc.

⚠ ATENCIÓ

Com a recomanació, és preferible no activar per defecte la resposta de confirmació de recepció de missatges.

Microsoft Outlook 365

Microsoft Outlook 365
outlook.com

Una de les aplicacions de correu electrònic més utilitzada en el món és la versió en dispositiu del webmail Outlook, denominada en la seva darrera versió, Microsoft Outlook 365. Aquesta aplicació està desenvolupada per Microsoft i permet una integració d'aquest gestor de correu electrònic amb altres aplicacions de la suite Office d'aquesta empresa.

Aquesta aplicació està desenvolupada per Microsoft i permet una integració d'aquest gestor d'email amb altres aplicacions de la *suite* Office d'aquesta empresa. Aquesta aplicació incorpora en una sola aplicació el gestor de correu electrònic, juntament amb el calendari, un sistema de llistes de tasques i l'agenda de contactes.

L'aplicació Outlook permet encriptar tots els missatges utilitzant el certificat digital, per fer un xifratge asimètric de clau pública i privada. Això proporciona un nivell de privacitat molt alta extrem a extrem, és a dir, que només el receptor podrà llegir el contingut del missatge xifrat i no es guardarà desencriptadament en cap servidor intermedi.

Hi ha versions tant per a ordinador, versió Windows i per a Mac, com per a telèfon intel·ligent, a Android i iPhone.

Thunderbird
thunderbird.net/es-ES

Thunderbird

Thunderbird, desenvolupat per Mozilla, que és l'empresa darrere del famós navegador Firefox, aquesta aplicació de correu electrònic és una opció molt interessant tant en ordinadors personals, aLinux, Windows i Mac, com a dispositius mòbils, Android i iOS. Està construïda emprant programari lliure, totalment lliure i gratuït.

Incorpora múltiples característiques de privacitat, com a protecció contra el rastreig d'emails, bloqueig de contingut remot, encriptació mitjançant certificat digital, etc.

The Bat!
e.digitall.org.es/thebat

The Bat!

Aquesta aplicació de correu electrònic és menys coneguda que les anteriors, però està dissenyada per garantir la màxima privacitat i seguretat. Utilitza l'encriptació en tots els nivells: realitza totes les comunicacions a través de canals segurs encriptats, xifra tota la informació en l'ordinador local, incorpora una encriptació extrem a extrem per a l'enviament dels correu electrònic, etc.

És capaç de funcionar sense suport de proveïdors globals en el núvol, per evitar deixar cap missatge fora del teu ordinador.

The Bat! és de pagament i només té versions per a Windows.

Canary Mail
canarymail.io/es

Canary Mail

L'aplicació Canary Mail integra tant privacitat com productivitat. La privacitat es garanteix amb la combinació del xifratge asimètric juntament amb l'encriptació extrem a extrem. La productivitat es fomenta amb la incorporació de la intel·ligència artificial per automatitzar de manera intel·ligent moltes accions com la detecció de frau per suplantació, eliminació d'anuncis i descobriment de possibles emails de correu brossa.

Aquesta aplicació té versions tant per a ordinador, Windows i Mac, com per a telèfons intel·ligents, Android i iOS.

Saber-ne més

Privacitat al correu electrònic: algunes recomanacions. e.digitall.org.es/privacidad-email

Descobreix 5 serveis de correu electrònic que respecten la teva privacitat. e.digitall.org.es/privacidad-email-2

ProtonMail. proton.me

tutanota. tutanota.com/es

Microsoft Outlook. outlook.com

Características de Thunderbird. e.digitall.org.es/thunderbird

The Bat! e.digitall.org.es/thebat

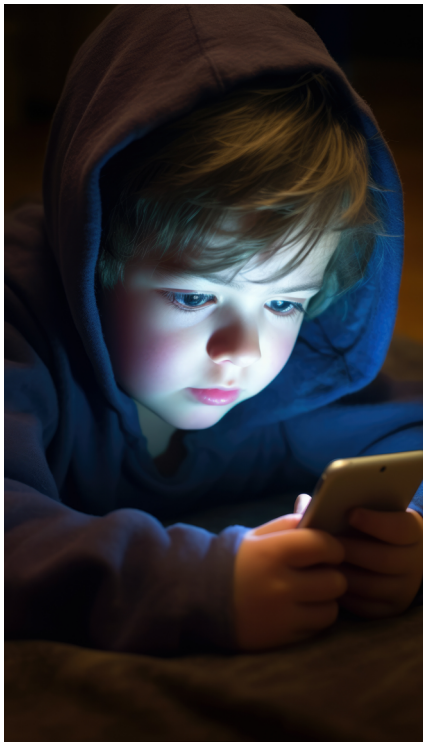
Canary Mail. canarymail.io/es

Seguretat

Nivell C2 4.2 Protecció de los dades personals i la privacitat

Privacitat i intel·ligència artificial

Privacitat i intel·ligència artificial



Introducció

En l'actualitat, els avanços tecnològics han permès que pugui utilitzar-se una gran quantitat d'informació per part dels sistemes informàtics, incrementant tant la capacitat de computació com la d'emmagatzematge o comunicacions. Aquesta informació és captada de nombroses fonts, entre elles figuren, des de la informació que directament introduïm en els nostres ordinadors fins a la informació que és adquirida o captada per innombrables dispositius sensors (càmeres de vídeo, sensors ambientals, comptadors de pas, sensors de pes, etc.), passant per la mateixa informació que nosaltres mateixos generem en la nostra navegació quotidiana per xarxes socials i Internet en general (pàgines que visitem, vídeos visualitzats, comentaris, preferències d'ús, etc.).

Tota aquesta informació és recollida en servidors de dades que emmagatzemen aquesta informació de manera més o menys estructurada, però que permet establir algorismes o processos dels quals es poden extreure informació útil en la majoria dels casos. Es tracta del procés de minat de dades que ajuda institucions i empreses a prendre decisions sobre estratègies o desenvolupaments a implementar, o promocions i ofertes que oferir a determinats usuaris.

Aquests avanços tecnològics, a més, han permès l'establiment de sistemes automàtics per a la presentació d'informació o presa de decisions per part de màquines de manera autònoma en el que es coneix com a intel·ligència artificial (IA).

Aquestes tecnologies, juntament amb els dispositius mòbils personals, les utilitzem quotidianament i són elements inseparables de les nostres vides, interactuant entre elles i afectant directament la informació o continguts amb els quals treballem o arriben directament als nostres dispositius personals. Les xarxes socials i l'ús de dispositius mòbils que utilitzem diàriament i assíduament són una font important de dades per a tecnologies com la mineria de dades o la intel·ligència artificial, complementant-se mútuament i transformant la manera en la qual consumim contingut digital. En aquest sentit, hem de tenir present, també, com de

protegida es troba la nostra informació particular i les nostres dades personals, en definitiva, la nostra privacitat i si aquesta és utilitzada d'algun mode per aquestes tecnologies i en quin mode és utilitzada. Per garantir l'ús responsable d'aquestes tecnologies i contemplar els aspectes ètics que poguessin afectar-los es treballa actualment a Europa, desenvolupant i difonent una guia per adaptar al RGPD (reglament general de protecció de dades) els productes i serveis que utilitzen intel·ligència artificial.

La privacitat de la informació i la protecció de dades són conceptes que s'han desenvolupat en alguns vídeos, com els següents

POLÍTICA DE PRIVACITAT EN INTERNET I EN LES APLICACIONS

Es comenta el concepte de política de privacitat. On trobar el document de polítiques de privacitat tant a Internet com en qualsevol aplicació. Importància de la política de privacitat. Contingut d'un document de política de privacitat.

e.digitall.org.es/A4C42A1V07

POLÍTICA DE PRIVACITAT. INFORMACIÓ PRIVADA

El vídeo mostra generalitats en l'ús d'aplicacions de missatgeria instantània, fent especial èmfasi en les polítiques de privacitat i compartició de dades.

e.digitall.org.es/A4C42A2V05

QUÈ INTRODUÏM AL NOSTRE ORDINADOR QUAN NAVEGAM?

El concepte tècnic de galeta, com s'emmagatzema al nostre navegador la informació que ens envien des d'un web. Funció inicial de les galetes i usos maliciosos (programari maliciós i cucs). Compte amb acceptar galetes de sistemes no de confiança.

e.digitall.org.es/A4C42B2V06

A més, en el vídeo que s'indica a continuació es desenvolupen conceptes d'intel·ligència artificial (IA), mineria de dades i com hem de procedir per protegir la privacitat dels individus.

INTEL·LIGÈNCIA ARTIFICIAL, MINERIA DE DADES I PRIVACITAT

L'ús cada vegada més generalitzat de les nostres dades personals per part de la intel·ligència artificial, la mineria de dades i els algorismes en general, planteja nous reptes enfront dels quals hem d'estar atents per a preservar la nostra privacitat.

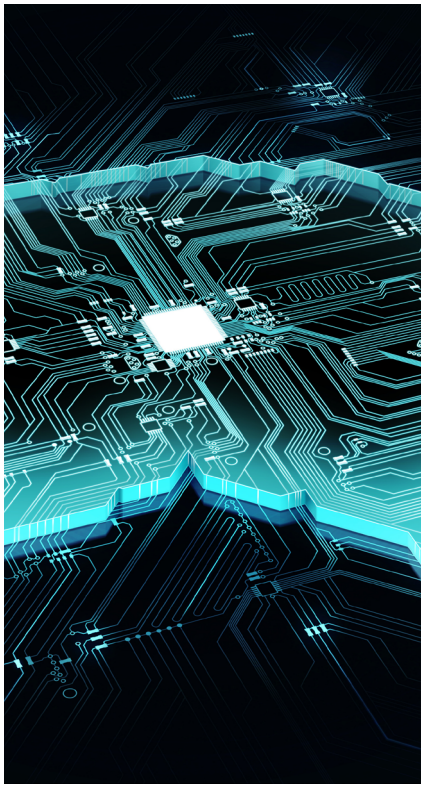
e.digitall.org.es/A4C42C2V06

En aquest document es desenvolupen, de manera resumida, els conceptes d'intel·ligència artificial, mineria de dades i la relació que aquestes tecnologies pogués tenir amb la privacitat i protecció de les nostres dades personals.

Intel·ligència artificial. Concepte i aplicacions

La intel·ligència artificial pot definir-se, segons diversos autors, com l'habilitat d'una màquina o sistema automàtic de presentar de manera autònoma les mateixes capacitats de raonament, aprenentatge, planificació i creativitat que l'ésser humà. La intel·ligència artificial permet a aquests sistemes automàtics percebre el seu entorn a través de sensors, relacionar-s'hi, resoldre problemes i actuar amb una finalitat específica.

Els sistemes d'intel·ligència artificial són capaços de processar la informació del seu entorn o una altra informació externa a aquest, adaptar una resposta al comportament esperat i analitzar els efectes que la seva decisió tindrà, sempre tenint en compte les accions prèvies que s'han dut a terme.



L'ús de la intel·ligència artificial està en plena expansió a causa del desenvolupament d'algunes aplicacions, entre les més destacades es troben aplicacions, fonamentals avui dia, per a diversos temes com: màrqueting, amb aplicacions IA específiques per a comerç electrònic, enviament de correus, o publicitat en línia; assistents virtuals, que responen a preguntes, executen determinades tasques i recomanacions com Siri o Alexa; automatització de la llar; sistemes de recomanació de visionament de contingut multimèdia, com a canals de televisió o preferències web; sistemes de traducció automàtica; sistemes de conducció autònoma; assessorament i prediccions, des de prediccions meteorològiques a assessorament financer; reconeixement facial; i diagnòstics mèdics.

Es pot resumir que els tipus d'intel·ligència artificial són dues, segons la comissió de la Unió Europea: IA programari, on s'inclouen anàlisi d'imatges, assistents virtuals, motors de cerca i sistemes de reconeixement de veu i rostre; i IA integrada, on estarien els robots, drons, vehicles autònoms o Internet de les coses.

Mineria de dades. Definició, mètodes i tècniques

La mineria de dades pot definir-se com l'anàlisi computacional automatitzada d'informació en format digital, segons la Comissió Europea, i inclou en aquesta informació textos, sons, imatges i dades. La mineria de dades fa possible el tractament de grans quantitats d'informació amb la finalitat d'adquirir nous coneixements i descobrir noves tendències, pautes o correlacions. Realment, es tracta de descobrir patrons de comportament i una altra informació valuosa en grans conjunts de dades.

L'evolució tecnològica en emmagatzematge d'informació i capacitats computacionals ha fet possible que el processament de grans quantitats de dades (big data) evolucioni i es desenvolupi com a matèria pròpia, i la tecnologia de processament de grans volums de dades s'ha convertit en una ciència en si mateixa. Previ a l'aplicació de tècniques i models de cerca de resultats en les dades cal dur a terme una anàlisi dels mateixos i preprocessament de dades per definir quins són realment significatius i quins cal obviar o eliminar de l'anàlisi final.

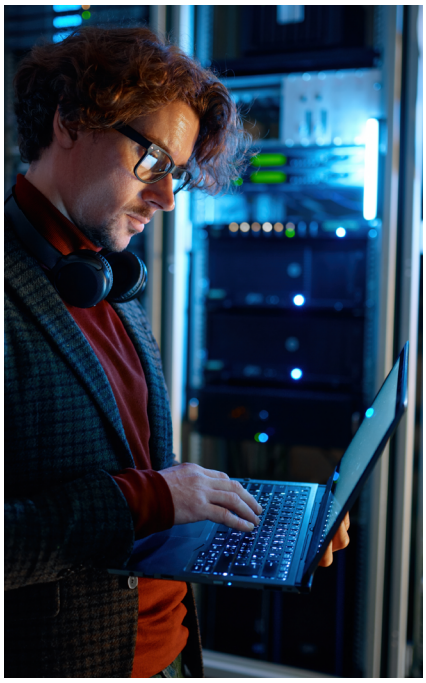
En l'actualitat, empreses i institucions utilitzen tècniques i tecnologia de mineria de dades assíduament en la presa de decisions, a través de multitud d'eines que analitzen dades (des del mateix Excel, passant que Qlik, Knime, R, o Tableau, fins a Oracle mineria de dades).

Actualment, s'està desenvolupant el concepte d'"espai de dades", i desenvolupament dels bessons digitals, com un mètode de conèixer previsions precises sobre diferents àmbits o entorns de treball. Així, podem trobar-nos el concepte d'espai de dades en temes d'agricultura, ramaderia, indústria o socioculturals. Un espai de dades és el conjunt de diverses

fonts distintes de grans quantitats de dades que ajuden a saber, per situacions anteriors similars, què succeirà en el futur i, d'aquesta manera, prendre la decisió més precisa per a això succeeixi o no. És possible, per exemple, saber amb antelació quina serà la collita d'oli d'oliva quan tenim totes les dades possibles sobre què va succeir en campanyes anteriors. Disposant de grans quantitats de dades sobre meteorologia, condicions ambientals, característiques del terreny, humitat, fertilitzants, plagues, etc., podem, sobre la base de la informació actual, predir la quantitat i qualitat d'oliva que serà recollida. Encara que aquest pot semblar un exemple senzill, que és possible conèixer amb l'anàlisi disponible en eines que utilitzem habitualment com Excel (en el seu apartat d'anàlisi de dades podem trobar diverses eines bàsiques d'anàlisis com a correlació, mitjanes, histogrames, regressió, estadístiques descriptives, covariància, etc.), és bastant habitual utilitzar eines més complexes i desenvolupades a mesura depenent del tipus de sistema.

Interrelació entre IA i mineria de dades

Després de les diferents etapes en les quals es divideix el procés de mineria de dades (com definir l'objectiu del seu procés de mineria i netejar, analitzar o preprocessar les dades) i arribar a determinar el conjunt de dades. A aquest es farà el treball real de mineria de dades des d'on es necessita o utilitza la intel·ligència artificial. Aquí s'introdueix l'aprenentatge automàtic, el qual pot ser aquest supervisat o no supervisat.



La tècnica més comuna utilitzada en **aprenentatge supervisat** són les xarxes neuronals, on es divideixen les dades en dos conjunts i es deixa que la xarxa aprengui a classificar les seves dades, s'entrena la xarxa per classificar les dades. D'altra banda, la tècnica més comuna en **aprenentatge no supervisat** és l'**algorisme genètic**, no se supervisa perquè no ensenya res, s'executa l'algorisme en el conjunt de dades i s'espera a descobrir relacions ocultes entre les dades.

Els grans volums de dades i el big data formen part de la intel·ligència artificial en tant que suposa de disposar d'informació que pot ser processada. La intel·ligència artificial analitza les dades de maneres que els humans són incapaços de fer, per a nosaltres hi hauria massa persones amb les quals comparar i massa punts d'informació per mirar. No obstant

això, les solucions d'intel·ligència artificial troben patrons on les persones fins i tot mai pensen a mirar. Poden trobar noves tendències en coses com a dades de xarxes socials, dades financeres i fins i tot dades geogràfiques. Per exemple, la intel·ligència artificial pot saber si és probable que algú compri un producte en funció de les seves inclinacions polítiques, per això, només necessita mirar a través dels perfils de les xarxes socials i comparar-los amb tota la informació de la qual disposa a través del big data, les dades són el combustible que manté la intel·ligència artificial en funcionament. A més, la intel·ligència artificial recopila informació mentre cerca patrons, i aquesta informació s'agrega a bases de dades plenes d'informació: infraestructura de big data. D'aquesta manera, el big data i la intel·ligència artificial es donen suport mútuament per crear una poderosa màquina d'anàlisi. Per exemple, si alguna vegada t'han recomanat una sèrie a Netflix que t'ha agradat, és perquè la intel·ligència artificial de la plataforma ha utilitzat les teves dades de consum.

La privacitat de dades associada a l'ús d'intel·ligència artificial, mineria de dades

La nostra identitat digital i hàbits de navegació a Internet queden registrats a través de galetes, que nosaltres autoritzem, on permetem accés a tercers a aquesta informació. Aquests tercers són, habitualment, empreses que treballen i desenvolupen tècniques de mineria de dades i intel·ligència artificial per oferir-nos ofertes, productes, promocions o serveis que puguin resultar del nostre interès. A més, depenent de la informació que compartim en les xarxes socials o en l'autorització de les nostres dades podrem trobar-nos més o menys ofertes, productes o informació dedicada específicament a nosaltres mateixos a Internet. En aquest sentit, ens oferiran productes que probablement resulten del nostre interès i no sapiguem com o per què es produeix això. Encara que tots coneixem com s'utilitzen les nostres preferències en les xarxes socials.

En contraposició a l'esmentat, existeix el Reglament General de Protecció de Dades, que protegeix o hauria de protegir la nostra informació particular de la utilització per part dels altres. En aquest sentit, i davant els canvis tecnològics i avenços tant

en mineria de dades com intel·ligència artificial, es proposen solucions o respostes a la desprotecció que puguem tenir en relació amb aquestes tecnologies.

En concret, l'Agència Espanyola de Protecció de Dades ha publicat una ***guia per a adaptar al Reglament General de Protecció de Dades els productes i serveis que utilitzin intel·ligència artificial*** (*e.digitall.org.es/adecuacion-rgdp*). Aquest document se centra en l'adequació al reglament de protecció de dades d'aquells tractaments de dades que incorporin parts d'intel·ligència artificial que desenvolupen solucions a un problema concret i delimitat, no intervé o refereix al desenvolupament de la intel·ligència artificial de manera genèrica com a tecnologia ni als processos de recerca implicats en aquesta.

La guia és dirigida a responsables de sistemes i desenvolupadors que incorporin o donin suport, respectivament, a elements d'intel·ligència artificial en els seus programes o tractaments de dades, ja que aquests elements podrien estar tractant dades personals en diferents fases o etapes del cicle de vida del sistema i, per consegüent, haurien de complir amb les obligacions del RGPD. A més, es repassen les relacions que podrien establir-se entre el responsable del tractament de dades personals i terceres persones que podrien estar interessats a desenvolupar IA amb aquestes dades.

En la guia es recullen les condicions que han de complir aquestes tecnologies per garantir i demostrar que el tractament efectuat s'adequa al RGPD. Entre aquestes condicions es plantegen aspectes com la legitimació per al tractament de dades, la informació processada i generada, l'exercici de drets i la presa de decisions automatitzades. El document se centra, també, en aspectes com l'exactitud de la informació, la minimització de les dades utilitzades, l'avaluació que l'impacte dels resultats de l'aplicació de la IA pogués implicar i una anàlisi de la proporcionalitat del tractament de dades. Fins i tot, analitza la possibilitat que l'ús de tecnologies basades en IA impliqui transferències internacionals de dades.

En definitiva, l'Agència posa de manifest que la posada en el mercat de tecnologies que fan tractaments de dades en els quals s'utilitza intel·ligència artificial exigeix que s'apliquin garanties de qualitat i privacitat, i exigeix cert nivell de maduresa als models d'intel·ligència artificial, de manera que es pugui determinar objectivament l'adequació dels tractaments i l'existència de mesures per gestionar els riscos que poguessin generar-se.

Saber-ne més

Què és la intel·ligència artificial i com s'empra? Parlament Europeu. e.digitall.org.es/inteligencia-artificial-uso

Protecció de dades de caràcter personal. Institut Nacional d'Administració Pública. e.digitall.org.es/proteccion-datos-sede

Big data, privacitat i protecció de dades. Agència Espanyola de Protección de Dades. e-digitall.org.es/big-data

Guia d'adaptació al RGPD de productes i serveis d'intel·ligència artificial. Agència Espanyola de Protecció de Dades. e.digitall.org.es/adecuacion-rgdp

Seguretat

Nivell **C2** 4.2 Protecció de les dades personals i la privacitat

Aprofundiment sobre els delictes informàtics

Aprofundiment sobre els delictes informàtics

Els delictes contra els sistemes informàtics o les TIC

Les expressions "delictes informàtics" o "ciberdelictes" no apareixen com a tals en el Codi Penal espanyol. No obstant això, habitualment se solen incloure en les mateixes les següents dues categories de delictes:

1 | Aquells en els quals l'objecte de l'activitat delictiva són els mateixos sistemes informàtics o les TIC.
2 | Aquells en els quals l'activitat delictiva se serveix de manera determinant de la informàtica o les TIC com a mitjà.

ELS DELICTES INFORMÀTICS

En aquest vídeo s'han analitzat de manera genèrica i sintèticament els delictes més rellevants que es poden incloure en totes dues categories i s'han exposat exemples de tot això.

e.digitall.org.es/A4C42C2V07

Com a complement, en aquest document es recolliran amb més detall les conductes que poden incloure's en cadascun d'aquests delictes mitjançant la reproducció dels preceptes del Codi Penal que les defineixen o tipifiquen. Aquestes definicions o tipus són essencials, perquè una conducta pugui ser castigada hi ha d'encaixar exactament. Si falta algun requisit no es podrà sancionar.

ATENCIÓ

Perquè una conducta pugui sancionar-se ha d'encaixar exactament en la definició o tipus que reculli el Codi Penal.

En la primera categoria exposada es poden incloure els delictes que s'enumeren en els següents subepígrafs:

NOTA

Si program un virus i simplement el guard en el meu ordinador no hi ha delicte, perquè la definició del Codi Penal exigeix que es faci amb la intenció de facilitar altres delictes.

Delictes de danys, sabotatge informàtic i atacs de denegació de serveis

"Allò que, per qualsevol mitjà, sense autorització i de manera greu esborrés, danyés, deteriorés, alterés, suprimís o fes inaccessibles dades informàtiques, programes informàtics o documents electrònics aliens, quan el resultat produït fos greu" (article 264 Codi Penal).

Delictes d'accés sense autorització a dades, programes o sistemes informàtics

"...al qual, sense estar autoritzat, s'apoderi, utilitzi o modifiqui, en perjudici de tercer, dades reservades de caràcter personal o familiar d'un altre que es trobin registrats en fitxers o suports informàtics, electrònics o telemàtics, o en qualsevol altra mena d'arxiu o registre públic o privat" (article 197.3 del Codi Penal).

Delictes de descobriment i revelació de secrets d'empresa arxivats en suports informàtics o electrònics

"El que, per descobrir un secret d'empresa s'apoderés per qualsevol mitjà de dades, documents escrits o electrònics, suports informàtics o altres objectes que es refereixin a aquest, o emprés algun dels mitjans o instruments assenyalats en l'apartat 1 de l'article 197..." (article 278 del Codi Penal).

Delictes contra serveis de radiodifusió o interactius

"...allò que, sense consentiment del prestador de serveis i amb finalitats comercials, faciliti l'accés intel·ligible a un servei de radiodifusió sonora o televisiva, a serveis interactius prestats a distància per via electrònica, o subministri l'accés condicional a aquests, considerat com a servei independent, mitjançant:

1r. La fabricació, importació, distribució, posada a disposició per via electrònica, venda, lloguer, o possessió de qualsevol equip o programa informàtic, no autoritzat en un altre estat membre de la Unió Europea, dissenyat o adaptat per fer possible aquest accés.

2n. La instal·lació, manteniment o substitució dels equips o programes informàtics esmentats en el paràgraf 1r" (article 286 del Codi Penal).

Els delictes en els quals l'activitat delictiva se serveix de la informàtica o TIC

Delictes d'estafa

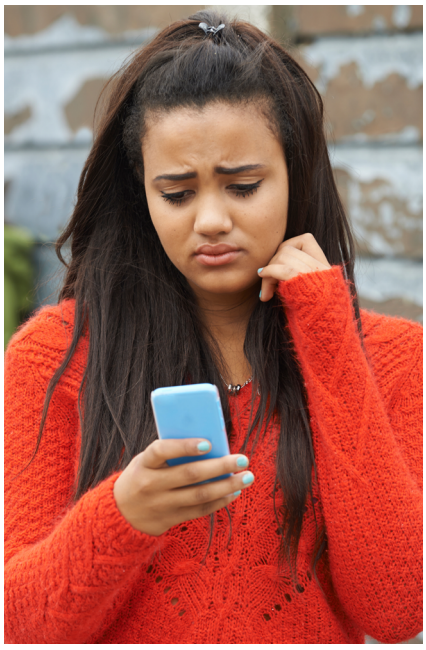
"1.[...] a) Els que, amb ànim de lucre, obstaculitzant o interferint indegudament en el funcionament d'un sistema d'informació o introduint, alterant, esborrant, transmetent o suprimint indegudament dades informàtiques o valent-se de qualsevol altra manipulació informàtica o artifici semblant, aconsegueixin una transferència no consentida de qualsevol actiu patrimonial en perjudici d'un altre.

b) Els que, utilitzant de manera fraudulenta targetes de crèdit o dèbit, xecs de viatge o qualsevol altre instrument de pagament material o immaterial distint de l'efectiu o les dades que consten en qualsevol d'ells, efectuïn operacions de qualsevol classe en perjudici del seu titular o d'un tercer."

"2. [...] a) Els que fabriquessin, importessin, obtinguessin, posseïssin, transportessin, comerciessin o d'una altra manera facilitessin a tercers dispositius, instruments o dades o programes informàtics, o qualsevol altre mitjà dissenyat o adaptat específicament per a la comissió de les estafes previstes en aquest article". (article 249 del Codi Penal).

Delictes d'assetjament i corrupció de menors/ persones discapacitades; o relatius a pornografia infantil/ persones discapacitades

"El que a través d'Internet, del telèfon o de qualsevol altra tecnologia de la informació i la comunicació contacti amb un menor de setze anys i proposi concertar una trobada amb el mateix a fi de cometre qualsevol dels delictes descrits en els articles 181 (realització actes de caràcter sexual) i 189 (pornografia)..." (article 183 del Codi Penal).



Delictes de fustigació

"1. ... el que assetgi una persona duent a terme de manera insistent i reiterada, i sense estar legítimament autoritzat, alguna de les conductes següents i, d'aquesta manera, alteri el normal desenvolupament de la seva vida quotidiana: [...]

2. Estableixi o intenti establir contacte amb ella a través de qualsevol mitjà de comunicació...

3. Mitjançant l'ús indegut de les seves dades personals, adquireixi productes o mercaderies, o contracti serveis, o faci que terceres persones es posin en contacte amb ella. [...]

4. El que, sense consentiment del seu titular, utilitzi la imatge d'una persona per fer anuncis o obrir perfils falsos a xarxes socials, pàgines de contacte o qualsevol mitjà de difusió pública, i que li ocasioni la mateixa situació d'assetjament, fustigació o humiliació..." (article 172 del Codi Penal).

Delictes contra la propietat intel·lectual

"...qui, en la prestació de serveis de la societat de la informació, amb ànim d'obtenir un benefici econòmic directe o indirecte, i en perjudici de tercer, faciliti de mode actiu i no neutral i sense limitar-se a un tractament merament tècnic, l'accés o la localització a Internet d'obres o prestacions objecte de propietat intel·lectual sense l'autorització dels titulars dels corresponents drets o dels seus cessionaris, en particular oferint llistats ordenats i classificats d'enllaços a les obres i continguts referits anteriorment, encara que aquests enllaços haguessin estat facilitats inicialment pels destinataris dels seus serveis" (article 270 del Codi Penal).

Saber-ne més

Llei orgànica 10/1995, de 23 de novembre, del Codi Penal.
e.digitall.org.es/boe-25444

Ministeri de l'Interior. Informe sobre la cibercriminalitat a Espanya 2021.
e.digitall.org.es/estadisticas

DigitAll

Seguretat

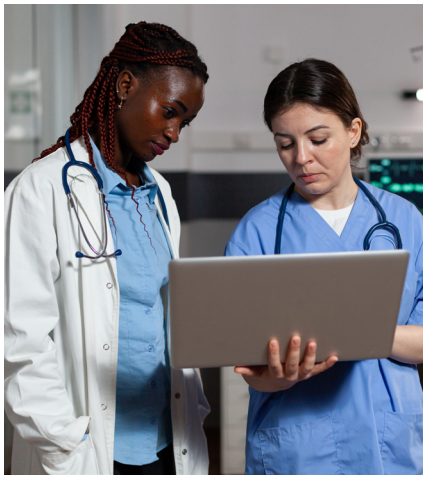
4.3 PROTECCIÓ DE LA SALUT I EL BENESTAR

Seguretat

Nivell **C2** 4.3 Protección de la salut i el benestar

Recopilació de fonts fiables de salut a Internet

Recopilació de fonts fiables de salut a Internet



Recopilació de fonts fiables a Internet

En aquest document presentarem una sèrie de recursos en els quals consultar fonts fiables a Internet per a temes relacionats amb la salut. Per això, hem seleccionat una sèrie de recursos, que poden ser d'utilitat, i, sobretot, perquè el puguis prendre com a referència per a seleccionar altres possibles fonts.

Medline

MedlinePlus és un servei informatiu en línia de salut per a pacients, familiars i amics. Té per objectiu brindar informació de qualitat sobre la salut i el benestar, oferint dades fiables i fàcils d'entendre.

La informació d'aquesta font de salut procedeix de la Biblioteca Nacional de Medicina dels EUA (NLM), la biblioteca mèdica més gran del món, que forma part dels Instituts Nacionals de la Salut dels EUA (NIH).

A la pàgina es pot accedir de manera gratuïta des de qualsevol dispositiu i en els idiomes d'anglès i espanyol, però no en català.

Salupedia

Salupedia és una enciclopèdia mèdica en línia que recupera, classifica i ordena la informació sanitària continguda en Internet que tingui el suport de professionals del sector.

Es basa en les publicacions que fan els professionals del sector recomanant als pacients, familiars i ciutadans, continguts de salut ja existents en la xarxa.

D'aquesta manera, el ciutadà troba un lloc on accedir a informació de confiança recomanada per professionals; i el professional, al seu torn, disposa d'un lloc de confiança on dirigir-se als seus pacients quan vol prescriure informació.

Agència Espanyola de Medicaments i Productes Sanitaris

L'Agència Espanyola de Medicaments i Productes Sanitaris (AEMPS) és una agència estatal adscrita al Ministeri de Sanitat.

Té per objectiu garantir a la societat la qualitat, seguretat, eficàcia i correcta informació dels medicaments i productes sanitaris, des de la seva recerca fins a la seva utilització.

En el seu web ofereix informació sobre medicaments, productes sanitaris, cosmètics, productes de cuidat personal i biocides, promovent el coneixement cientificotècnic.

Societat Espanyola de Medicina de Família i Comunitària

És una societat científica mèdica, sense ànim de lucre, que vetlla per l'adequat desenvolupament de la Medicina familiar i comunitària (MFiC) a Espanya. Actualment, és la societat científica més gran del país.

La semFYC està integrada per les 17 Societats de Medicina de Família i Comunitària que existeixen a Espanya i reuneix més de 20.000 socis especialistes en la medicina de família.

A través de la seva pàgina web es pot fer una cerca de filtratge per diverses competències clíniques (ecografia, cardiovascular, dermatologia, infeccions, etc.), es poden trobar diverses publicacions científiques i de salut, esdeveniments del sector i altres temes d'actualitat sobre medicina.

Societat Espanyola de Metges d'Atenció Primària

La Societat Espanyola de Metges d'Atenció Primària (SEMERGEN) ha creat una web l'objectiu de la qual és informar i formar al pacient, amb criteris mèdics adequats, consensuats i documentats, sobre diversos temes de l'àmbit de la medicina i salut.

El web, anomenada Pacients Semergen, sorgeix per fer front a l'excés d'informació mèdica a l'abast de qualsevol internauta, la qual pot suposar un import risc per a la salut de la població.

S'hi pot trobar una secció de preguntes i respostes, en la qual es rep resposta directa dels professionals, un apartat de malalties freqüents, a més de diverses notícies d'actualitat relacionades amb la salut.

PiCuida

PiCuida és la Xarxa de Cures d'Andalusia, creada per l'Estratègia de Cures d'Andalusia (Servei Andalús de Salut). Al web oficial es pot trobar informació científica i metgessa sobre diversos temes de la salut.

La plataforma compta amb una biblioteca de cerca on es pot cercar la paraula clau que es vulgui, o bé triar una categoria ja predeterminada del sector (atenció a la infància, cures i salut mental, ètica i cures, preguntes clíniques, etc.).

Saber-ne més

La pàgina web oficial de l'Organització Mundial de la Salut (OMS) compta amb un cercador alfabètic on es poden cercar diverses malalties o patologies per la seva lletra inicial. A més, disposa d'un apartat de publicacions, comunicats o articles relacionats amb el tema de la salut.

who.int/es

Recomanacions per reconèixer una pàgina fiable

Internet ens dona accés a multitud de fonts d'informació relacionades amb diverses temàtiques com la salut. No obstant això, tal com es va abordar al vídeo 03 d'aquest nivell no totes les pàgines web sobre salut a les quals podem accedir són fiables. La selecció i recopilació de la informació fiable sobre salut a Internet és important per evitar uns certs problemes en la nostra salut mental. Però quines pautes podem seguir per a reconèixer una pàgina fiable? A continuació, es mostren alguns dels principis bàsics a seguir per distingir aquestes pàgines.

NOTA

La fiabilitat de la informació a Internet fa referència a la probabilitat que la informació que s'adjunta en aquesta pàgina web sigui vàlida i de qualitat, basant-se en fonts científiques principalment. Per a més informació pots revisar el vídeo: ***Fiabilitat de la informació de salut en Internet***.

FIABILITAT DE LA INFORMACIÓ DE SALUT EN INTERNET

e.digitall.org.es/A4C43C2V03

Patrocinador del lloc web

A més de conèixer la informació rellevant sobre l'autor, també és necessari conèixer qui patrocina aquesta pàgina web. Pel que, l'URL d'aquesta pàgina ens pot oferir informació útil en aquest sentit. Així, per exemple: .gov (indica les agències del govern), .edu (identifica les entitats educatives), .org (defineix les organitzacions sense ànim de lucre) i .com (indica les pàgines web amb finalitats comercials).

Política de privacitat

Totes les pàgines web haurien de presentar una política de privacitat. En aquest sentit, moltes de les pàgines web que podem visitar, fan ús de galetes, les quals poden alterar la privacitat dels visitants en aquestes pàgines. Per evitar-ho, es pot optar per desactivar l'ús de les galetes a través del navegador d'Internet.

Protecció de la nostra informació sobre salut a Internet

És important saber com es recopilarà aquesta informació. La majoria dels llocs web segurs solen presentar un "http" amb una "s" al final. De fet, en moltes pàgines solen demanar un usuari i contrasenya.

Recorda que algunes pautes relacionades amb aquest tema són: fer ús d'una contrasenya segura, utilitzar factors d'autenticació, no compartir informació privada sobre salut en una xarxa wifi d'ús públic.

Saber-ne més

Existeixen diverses llistes de verificacions que ens poden ajudar a conèixer si una pàgina web és fiable o no. A continuació, es mostren algunes de les preguntes que un/a hauria de fer-se a si mateix per a l'ús de pàgines web sobre salut:

- Pertany aquesta pàgina web a alguna organització, entitat o govern? Qui és l'autor que redacta aquesta informació sobre la salut?
- Es reflecteix l'objectiu d'aquesta pàgina web? Per què va ser creada aquesta pàgina web?
- Per què va ser creat el lloc web? És clara la missió o l'objectiu del patrocinador del lloc web?
- La pàgina web presenta algun contacte o persona o grup de referència?
- Quan va ser la darrera actualització d'aquesta pàgina web?
- La informació sobre la seva privacitat està protegida?
- Aquesta pàgina recull informació sobre cures miraculoses?

Exemples de pàgines de salut no fiables

Després d'observar diferents punts rellevants per conèixer la fiabilitat d'una pàgina web sobre salut, es mostren alguns exemples de pàgines web lligades a la salut no fiables.

- Blogs i pàgines relacionades amb temes de nutrició, oferint dietes i fàrmacs per a combatre contra l'obesitat, que finalment no són miraculoses i poden provocar un efecte negatiu en l'estat de salut. A més, aquest tipus de pàgines no solen presentar l'autor del seu contingut.

- Pàgines web relacionades amb la salut de la dona. Aquestes pàgines contenen remeis i algunes consideracions a tenir en compte en uns certs moments vitals de la dona. A més, també, es realitzen venda de productes. En general, aquestes pàgines solen ser administrades per persones sense formació mèdica.

Saber-ne més

- medlineplus.gov/spanish
- who.int/es
- salupedia.org
- aemps.gob.es
- semfyc.es/medicos
- pacientessemergen.es
- picuida.es
- e.digitall.org.es/informacion-salud
- e.digitall.org.es/bulos-salud

DigitAll

Seguretat

4.4
PROTECCIÓ DEL MEDI AMBIENT

Seguretat

Nivell **C2** 4.4 Protecció del medi ambient

ODS i tecnologies digitals

ODS i Tecnologies Digitals

Introducció

En aquest document es tractaran de manera més detallada els conceptes que s'han inclòs en els vídeos del nivell C1 i C2 ODS i Tecnologies digitals (I i II).

ODSS I TECNOLOGIES DIGITALS (I)

Situació actual de les problemàtiques i desafiaments relacionats amb la tecnologia digital per al compliment dels ODS.

e.digitall.org.es/A4C44C1V05

ODSS I TECNOLOGIES DIGITALS (II)

Potencials aplicacions de la tecnologia digital per al compliment dels ODS.

e.digitall.org.es/A4C44C2V05

La seva finalitat és la d'ampliar informació sobre els Objectius de Desenvolupament Sostenible (ODS), aprovats el 2015 pels estats membres de les Nacions Unides.

Aquest document se centrarà, especialment, a donar a conèixer la importància dels ODS, quina és la seva comesa i per què persegueixen reptes que tenen, i tindran, repercussió mundial per al planeta, les persones, la prosperitat, la pau i les aliances internacionals.

Veurem que l'*Agenda 2030* per al Desenvolupament Sostenible, adoptada per l'Assemblea General de l'ONU (2015), és el pla d'acció que guia els programes d'implementació de les metes que persegueixen els 17 ODS: es tracta de 169 metes interrelacionades que s'encaminen cap a l'optimització (sostenibilitat) de les esferes econòmica, social i ambiental, posant-se com a data de consecució l'any 2030.

El compromís dels països amb els ODS marca un abans i un després en l'aposta internacional i la mobilització de recursos per aconseguir els majors reptes del món actual: des de l'erradicació de la fam, la pobresa o la desigualtat social, fins a l'accés universal a la sanitat, l'educació, el treball decent i l'accés generacional als recursos naturals.

A més, s'aporta informació per comprendre com aquests reptes únicament podran ser assolits si el progrés es fonamenta en l'economia circular, és a dir, que es du a terme en paral·lel a la protecció ambiental i social, el consum sostenible de recursos naturals i l'adequada gestió i reciclatge dels residus generats.

En definitiva, comprendrem com els ODS mostren que l'*economia i la societat* han de llegir-se com a parts necessàriament dependents de la sostenibilitat de la biosfera del nostre planeta.

També entendrem la importància d'aplicar els principis de sostenibilitat en la fabricació de la tecnologia digital com a única via perquè veritablement suposin una eina essencial al procés de digitalització sostenible.

Acabarem per mostrar la contribució de la digitalització sostenible en la implementació dels ODS: tinguem en compte que tecnologia digital és present en totes i cadascuna de les activitats industrials, empresarials, administratives i personals de la societat del segle XXI.

El *pastís de noces* dels ODS

Al llarg de la sèrie de vídeos hem pogut conèixer que la tecnologia digital ens ha obert pas cap a un nou estil de vida fonamentat en la transformació digital en constant evolució. Sens dubte, que la innovació digital al servei de la societat facilita el nostre sistema de vida. Però, també és ben cert que el seu ús en la transformació digital suposa una enorme demanda de dispositius digitals la fabricació dels quals, ús i consum està tenint un impacte ambiental que està posant en risc les reserves naturals del món.

Hem de ser conscients de tots dos panorames:

- D'una banda, el benefici de la transformació digital per contribuir en la sostenibilitat del nostre progrés.
- D'altra banda, de l'impacte ambiental associat a la transformació digital.

I, efectivament, conseqüent amb aquesta suposada incompatibilitat entre la sostenibilitat i la insostenibilitat del progrés humà i els seus recursos actuals, entre altres, la transformació digital, l'Agenda 2030 per al Desenvolupament

Sostenible (2015) estableix una sèrie d'objectius encaminats a millorar el nostre sistema de vida actual i el de les generacions futures.

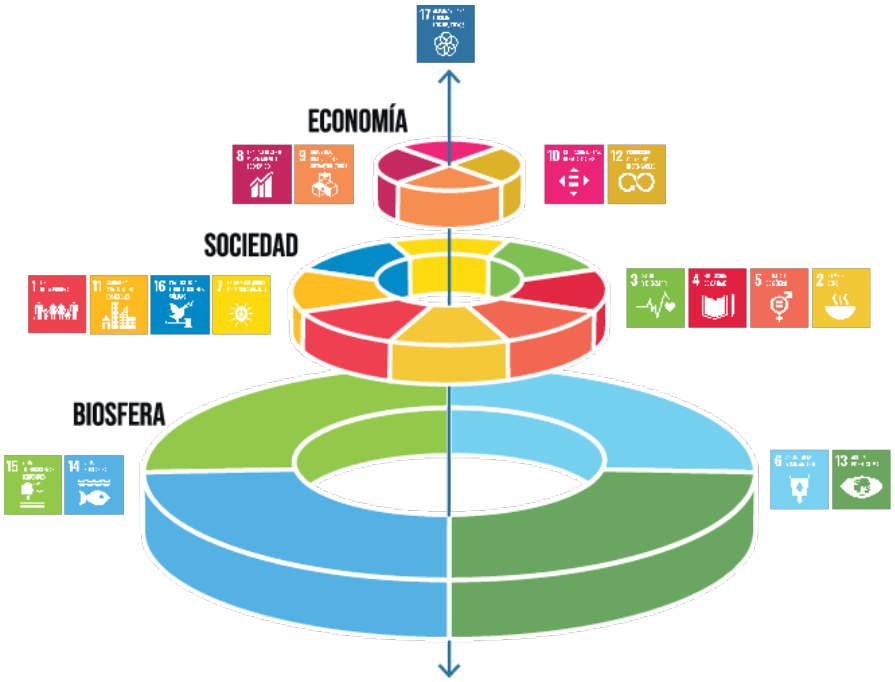
Els Objectius de Desenvolupament Sostenible (ODS) s'estableixen per guiar el progrés de la humanitat considerant que ha de ser integrador, inclusiu i universalment just i equitatiu. Per això, els països de l'ONU es van comprometre al fet que, abans de 2030, la nostra societat haurà prosperat en benestar i qualitat de vida, però sense descurar la seva obligació de fer-ho ambiental i econòmicament sostenible.

Els ODS aposten per desafiaments a escala mundial que cal entendre en context. La implicació per contribuir a la consecució dels ODS recau tant en les institucions públiques, l'àmbit polític i el teixit productiu industrial i empresarial com en tots i cadascun de nosaltres i nosaltres.

Calia donar a conèixer els ODS en termes que ens permetin entendre la seva essencialitat i la importància de la implicació a tots els nivells socials, econòmics i ambientals. Havíem de comptar amb una manera de "mirar" els ODS en els quals s'evidenciés on encaixa la nostra societat, és a dir, on encaixem com a individus i consumidors, i la nostra forma de vida.

Per això, el Centre de Resiliència de la Universitat d'Estocolm va presentar en 2016 una nova manera d'observar els ODS, a la qual va denominar "el pastís de noces dels ODS" (2016).

Va ser presentada en Stockholm EAT Food Fòrum de 2016 per a fer veure la importància de l'alimentació com un dels reptes més transcendentals dels desafiaments mundials de salut i sostenibilitat als quals s'enfronta el món.



Aquesta il·lustració mostra com **l'Economia** i la **Societat** han de contemplar-se com a parts necessàriament dependents de la sostenibilitat de la **Biosfera** del nostre planeta. Representa una visió nova, allunyant-se de l'actual enfocament sectorial on el desenvolupament social, econòmic i ecològic es veuen com a parts separades.

La base d'aquest pastís mostra els ODS més mediambientals, és a dir, els que sostenen a la resta dels ODS perquè el pastís no s'enfonsi. No tendríem res sense Aigua neta i sanejament (ODS 6), Vida submarina (ODS 14), Acció pel clima (ODS 13) i Vida dels Ecosistemes terrestres (ODS 15).

El primer pis del pastís inclou els ODS que donen sentit a la nostra vida: les persones i la societat. La humanitat serà justa quan es posi fi a la Pobresa (ODS 1), arribem a aconseguir la Fam Zero (ODS 2), tinguem accés universal a Salut i benestar (ODS 3), a Educació de qualitat (ODS 4), a Energia assequible i no contaminant (ODS 7) i visquem a Ciutats i comunitats sostenibles (ODS 11), tot això en un entorn en el qual s'hagi obtingut la total Igualtat de gènere (ODS 5).

I on es troba l'economia? Per a això es reserva el tercer pis del pastís, ja que amb l'economia estan vinculats el Treball decent i el creixement econòmic (ODS 8), la Indústria, Innovació i Infraestructura (ODS 9), la Producció i consum responsables (ODS 12) i en el qual la Reducció de les desigualtats (ODS 10) sigui una realitat.

Aconseguir la consecució de tots aquests ODS només serà possible amb la implicació i acció efectiva internacional, pels quals les Aliances per aconseguir els ODS (ODS 17) s'instauren com l'objectiu coordinador que subjecta i assegura tots aquests desafiaments.

Les 5P dels ODS per a l'Acció Digital

Com ja hem vist, els ODS aposten per reptes summament importants per als nostres valors vitals, ja que se centren en la protecció del nostre *Planeta*, les *Persones* i la *Prosperitat*, al mateix temps que vetllen per la *universalització de la Pau* per a tots a través *d'Aliances internacionals*.
Encara que no correspon exactament amb els seus termes en català, aquests reptes s'han donat a conèixer com les 5P de l'Agenda 2030 per la seva terminologia en anglès: *Planet* (Planeta), *People* (Persones), *Prosperity* (Prosperitat), *Peace* (Pau) i *Partnership* (Aliances).

Vegem per què i la seva relació amb l'Acció Digital. Comencem per distingir els ODS que s'engloben en cadascuna d'aquestes P:

- **Personas (*People*):** fàcilment identificam quins són els ODS enfocats directament en les persones. Són ODS 1 Fi de la pobresa, ODS 2 Fam zero, ODS 3 Salut i benestar, ODS 4 Educació de qualitat i ODS 5 Igualtat de gènere.
- **Planeta (*Planet*):** la protecció ambiental es converteix en la base de la nostra pròpia existència i res serà possible sense la consecució dels ODS relacionats amb això: ODS 6 Aigua neta i sanejament, ODS 12 Producció i consum responsables, ODS 13 Acció pel clima, ODS 14 Vida submarina i ODS 15 Vida d'ecosistemes terrestres.
- **Prosperitat (Prosperity):** hem d'aspirar a viure amb harmonia amb el que la naturalesa ens ofereix amb la finalitat de ser coherents amb els ODS 7 Energia assequible

i no contaminant, ODS 8 Treball decent i creixement econòmic, ODS 9 Indústria, innovació i infraestructures, ODS 10 Reducció de desigualtats i ODS 11 Ciutats i comunitats sostenibles.

- **Pau (Peace):** no hi ha dubte que els conflictes, les guerres, la inseguretat, les institucions febles i les desigualtats i la injustícia social constitueixen una de les pitjors amenaces per a l'avanç cap a un desenvolupament sostenible i per millorar aquesta situació es persegueixen els objectius de l'ODS 16 Pau, justícia i institucions sòlides.

- **Aliances (Partnership):** l'ODS 17 Aliances per assolir els ODS fomenta les relacions de cooperació entre líders mundials amb la finalitat de proveir finançament i acció coordinada a escala internacional.

És important recordem que per digitalització sostenible entenem el procés pel qual les societats es digitalitzen protegint el medi ambient, l'economia circular i el benestar de les persones. Únicament, llegint aquesta definició podem veure fàcilment alguna interrelació amb les 5P, però vegem-ne alguns exemples.

Comencem per l'impacte ambiental de la tecnologia digital. Com ja hem vist en els vídeos, qualsevol activitat que facem a l'entorn digital genera impactes, ja sigui per emissions de gasos d'efecte d'hivernacle, ja sigui per l'ús de recursos naturals imprescindibles en la fabricació de dispositius digitals i la infraestructura per al seu funcionament. A això cal sumar tant el consum energètic que necessita tot el procés, així com la ingent quantitat de residus que generem i que han de ser degudament gestionats per a reduir i prevenir conseqüències negatives per a la nostra seguretat i la del nostre planeta.

La *contaminació digital* incideix directament en els ODS tant dificultant la seva consecució com afavorint-la. Quant al tema que ens ocupa, els ODS estableixen metes que criden l'atenció sobre qualsevol mena d'impacte negatiu, entre els quals està la contaminació digital, i insten a aturar-los i atenció constant per a la seva prevenció, minimització i, en ser possible, evitació.

Ja el 2010, l'investigador Jonathan Koomey, va indicar que s'hauria de fer front perquè la tendència a l'alça de despesa energètica dels dispositius digitals anés cada vegada més eficient (Llei de Koomey, 2010), la qual cosa ha millorat els processos per a una producció i infraestructures digitals sostenibles, incloent-hi l'optimització de programari, maquinari, xarxes d'accés i centres de dades.

En la transició ecològica fonamentada en la coherència amb els ODS, la tecnologia digital no és només una necessitat operativa, sinó que, a més, avui dia és l'eina per excel·lència que permet dur a terme una transformació digital sostenible. L'*Estratègia Digital de la UE* (2021), amb el document "*Brúixola Digital 2030: l'enfocament d'Europa per al Decenni Digital*", marca la visió i objectius concrets per això: ciutadans amb capacitats digitals (*Pla Nacional de Competències Digitals. DigitAll*), Digitalització dels serveis públics, Infraestructures digitals segures i sostenibles i Transformació digital de les empreses.

A la *Brúixola Digital 2030* es destaca que els dispositius digitals han d'afavorir la sostenibilitat i transició ecològica, posant l'accent en els drets i principis digitals, com a via per contribuir als ODS amb la implicació i suport social, institucional i empresarial. És una ambició declarada per "*aplicar polítiques digitals que capacitin a les persones i les empreses per aprofitar un futur digital centrat en l'ésser humà, sostenible i més pròsper*" (UE, 2021).

Per part seva, el Pacte Mundial de l'ONU (2019) exposa que la tecnologia digital ofereix un gran potencial per accelerar el compliment dels ODS i reduir els seus processos d'implementació. Per exemple, promoure l'accés a la informació de qualitat, l'anàlisi i la recol·lecció de dades a gran escala (Big data) té impacte positiu en tots els ODS, entre altres àmbits per a ajudar a acostar els serveis socials d'educació, salut, alimentació, ocupació, igualtat d'oportunitats, etc., així com la presa de decisions en temes ambientals o econòmics.

La *digitalització empresarial i industrial* fa possible tant l'optimització sostenible dels seus processos com noves maneres de negoci que aprofiten el seu potencial per millorar el seu impacte positiu. Així redueixen la seva petjada ambiental, com el comerç electrònic, l'optimització de labors agrícoles o sistemes de salut, entre altres.

Per tant, els dispositius electrònics cada vegada més eficients i sostenibles es conceben com a impulsors de l'Acció Digital per a la consecució dels ODS de l'*Agenda 2030* i la transformació digital per a "*aconseguir una societat més sana i ecològica*" (UE, 2021).

Saber-ne més

Parlament Europeu (2021). Brussel·les, 9.3.2021 COM(2021) 118. *Estratègia Digital de la UE (2021), Brúixola Digital 2030: l'enfocament d'Europa per al Decenni Digital*. e.digitall.org.es/brujula-digital

Pacte Mundial Xarxa Espanyola (2019). *Set maneres en les quals la tecnologia pot contribuir als ODS*. e.digitall.org.es/pacto-mundial

The SDGs wedding cake. Stockholm Resilience Centre. Stockholm University (2016). e.digitall.org.es/tarta-boda

Assemblea General de l'ONU (2015). *Transformar el nostre món: l'Agenda 2030 per al Desenvolupament Sostenible*. e.digitall.org.es/onu-agenda2030

Materials de comunicació dels ODS de l'ONU (2015).e.digitall.org.es/materiales-ods

Koomey, J. et all. (2010) *Implications of Historical Trends in the Electrical Efficiency of Computing*. DOI:10.1109/MAHC.2010.28. Corpus ID: 8305701. e.digitall.org.es/koomey

Altres recursos:

- Stockholm EAT Food Forum (2016). e.digitall.org.es/2016-eat
- e.digitall.org.es/tarta-bbva
- e.digitall.org.es/5p

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