DigitAll

Formació en Competències Digitals

4

Seguretat

DigitAll

Formació en competències digitals

Seguretat

Nivell C1

Seguretat

ÍNDEX

DigitAll

Seguretat

4.1 PROTECCIÓ DE DISPOSITIUS

Seguretat

Nivell C1 4.1 Protecció de dispositius

Estàndards de seguretat a l'empresa

Estàndards de seguretat a l'empresa

Estàndard de seguretat

Un estàndard de seguretat és un conjunt de normes i pràctiques establertes per garantir la seguretat i protecció dels sistemes, dades, infraestructures o processos. Aquests estàndards es desenvolupen amb l'objectiu de mitigar els riscos i amenaces que podrien comprometre la integritat, confidencialitat i disponibilitat de la informació.

Els estàndards de seguretat poden abastar diferents àrees, com la seguretat informàtica, la seguretat de la informació, la seguretat de xarxes, la seguretat física i la seguretat en el desenvolupament de programari. Aquests estàndards defineixen els requisits tècnics, controls, polítiques i procediments que han d'implementar-se per assegurar que els sistemes i dades estiguin protegits de manera efectiva.

> ***Saber-ne més***
>
> Complir amb els estàndards de seguretat adequats ajuda a garantir la confiança dels usuaris, clients i socis comercials, i redueix els riscos associats amb incidents de seguretat, com l'accés no autoritzat, el robatori de dades o les interrupcions del sistema.

Existeixen nombrosos estàndards de seguretat en el món, per tant, parlar de quins o quants són resulta molt complicat, però sí que podem afirmar que els més coneguts o estesos són els següents:

- **ISO/IEC Familia 27K** (*e.digitall.org.es/iso*): estàndard internacional per a la gestió de la seguretat de la informació.
- **NIST SP 800** (*e.digitall.org.es/sp-800*): marc de seguretat desenvolupat per l'Institut Nacional d'Estàndards i Tecnologia dels Estats Units (NIST).
- **PCI DSS** (*e.digitall.org.es/pci*): estàndard de seguretat de dades per a la indústria de targetes de pagament.
- **HIPAA** (*e.digitall.org.es/hipaa*): Llei de Portabilitat i Responsabilitat d'Assegurança Mèdica als Estats Units, que estableix requisits de seguretat i privacitat de la informació mèdica.

- **GDPR** (*e.digitall.org.es/gdpr*): Reglament General de Protecció de Dades de la Unió Europea, que estableix normes de protecció de dades i privacitat per als ciutadans de la UE.
- **CIS Controls** (*e.digitall.org.es/cis*): conjunt de controls de seguretat desenvolupats pel Centre de Seguretat d'Internet (CIS) per ajudar a protegir els sistemes d'informació.

La manera de demostrar el compliment d'estàndards de seguretat radica en l'obtenció d'una certificació on s'avalua i certifica que es compleix aquest estàndard. És important ressaltar que no tots els estàndards són susceptibles de ser certificats.

El procés de certificació de seguretat generalment implica les següents etapes:

1 | **Avaluació inicial:** s'avalua exhaustiva de l'organització, sistema o procés de seguretat per determinar si ja es compleix amb els estàndards i requisits establerts.
2 | **Implementació de controls:** si s'identifiquen deficiències o àrees de millora durant l'avaluació inicial, l'organització ha d'implementar controls i mesures de seguretat addicionals per complir amb els requisits.
3 | **Auditoria:** un auditor extern o un organisme de certificació independent realitza una revisió detallada i exhaustiva del sistema de seguretat per verificar el compliment dels estàndards i criteris establerts.
4 | **Emissió de certificació:** si l'organització o sistema compleix amb èxit els requisits de seguretat, s'emet una certificació oficial que valida que s'ha complert amb els estàndards de seguretat establerts.

A continuació, es revisen alguns d'aquests estàndards per ser els més estesos.

ISO/IEC Familia ISO27k

La família ISO 27k, també coneguda com la sèrie ISO/IEC 27000, es refereix a un conjunt d'estàndards internacionals que aborden la gestió de la seguretat de la informació. Aquests estàndards són desenvolupats per l'Organització Internacional de Normalització (ISO) i la Comissió Electrotècnica Internacional (IEC) amb l'objectiu d'establir un marc de bones pràctiques per a la seguretat de la informació en organitzacions de qualsevol grandària i sector.

La sèrie ISO/IEC 27000 proporciona directrius i recomanacions per a la gestió de la seguretat de la informació, i està composta per diversos estàndards interrelacionats, sent els més coneguts:

- **ISO/IEC 27001:** És l'estàndard principal de la família i especifica els requisits per a establir, implementar, mantenir i millorar un Sistema de Gestió de Seguretat de la Informació (SGSI) dins d'una organització.
- **ISO/IEC 27002:** Proporciona un conjunt de controls i bones pràctiques de seguretat de la informació que poden ser utilitzats per implementar els requisits del SGSI descrits a l'ISO/IEC 27001.
- **ISO/IEC 27005:** Se centra en la gestió de riscos de seguretat de la informació, i proporciona pautes per identificar i avaluar els riscos, així com per seleccionar i implementar controls de seguretat adequats.

A més d'aquests, existeixen altres estàndards dins de la família ISO 27k que cobreixen temes específics, com la gestió d'incidents de seguretat, la continuïtat del negoci, l'auditoria de seguretat de la informació, entre altres.

NIST SP 800

L'estàndard NIST SP 800 es refereix a la sèrie de publicacions de l'Institut Nacional d'Estàndards i Tecnologia (NIST) dels Estats Units relacionades amb la seguretat de la informació i la ciberseguretat. El NIST SP 800 (*Special Publication 800*) proporciona directrius, recomanacions i millors pràctiques per a diversos aspectes de la seguretat de la informació i la gestió de riscos.

El NIST SP 800 es compon de múltiples publicacions, cadascuna de les quals se centra en una àrea específica de la seguretat i la ciberseguretat.

El NIST és àmpliament reconegut com una autoritat en matèria d'estàndards de seguretat i ciberseguretat, i les seves publicacions són àmpliament utilitzades per organitzacions i indústries per enfortir la seva postura de seguretat i gestionar els riscos relacionats amb la informació i els sistemes.

PCI DSS

PCI DSS (*Payment Card Industry Data Security Standard*) és un estàndard de seguretat de dades per a la indústria de targetes de pagament. Va ser desenvolupat pel Consell de Normes de Seguretat del PCI (PCI SSC), que és un organisme format per les principals companyies de targetes de crèdit i dèbit, com Visa, Mastercard, American Express, Discover i JCB.

L'objectiu de l'estàndard PCI DSS és protegir la informació confidencial dels titulars de targetes de pagament, com els números de targeta, mitjançant la promoció de pràctiques de seguretat en les organitzacions que manegen, processen o emmagatzemen aquesta informació. PCI DSS estableix un conjunt de requisits tècnics i operatius que han de complir els comerciants, processadors de pagaments, emissors de targetes i altres actors involucrats en les transaccions amb targetes de pagament.

El compliment del PCI DSS és requerit pels proveïdors de serveis de pagament i les xarxes de targetes de crèdit per garantir la seguretat de les transaccions amb targetes de pagament. Les organitzacions que manegen targetes de pagament han de sotmetre's a auditories periòdiques per demostrar el compliment de l'estàndard.

Seguretat

Nivell C1 4.1 Protecció dedispositius

Protecció enfront d'atacs a xarxes

Protecció enfront d'atacs a xarxes

La **protecció de les xarxes de comunicacions és una part fonamental de la seguretat informàtica**. Això té especial rellevància en les xarxes empresarials, on s'alberguen serveis crítics per a un negoci, es duen a terme multitud d'operacions diàries i es comparteix informació confidencial. Els atacs que hem vist en vídeos d'aquest nivell representen una amenaça constant, per a interrompre o comprometre la comunicació i el flux de dades.

ATACS MÉS COMUNS A LES XARXES

Tant en xarxes domèstiques com en xarxes empresarials, existeixen atacs comuns, però efectius que amenacen la seguretat d'aquestes. DHCP i IP Spoofing, Man in the Middle o les denegacions de servei en són alguns.

e.digitall.org.es/A4C41C1V03

A continuació, s'abordaran les mesures de protecció necessàries per a mitigar els atacs específics, com el DHCP spoofing, IP spoofing, Man in the Middle (MitM) i la denegació de servei (Dos). Això és una guia de bones pràctiques, encara que per a més detall de configuració s'hauran de consultar els manuals específics de cada dispositiu de xarxa.

DHCP Spoofing

Els atacs **DHCP Spoofing** s'utilitzen per a fer-se passar per un **servidor DHCP** legítim en una xarxa i p**rendre el control de la configuració dels dispositius de la xarxa compromesa**. D'aquesta manera, es podria modificar la porta d'enllaç predeterminada i redirigir el trànsit dels dispositius compromesos a través de l'ordinador de l'atacant, cosa que permet la intercepció o inspecció de les comunicacions.

Quan un dispositiu es connecta a una xarxa, sol·licita la configuració a qualsevol servidor DHCP que pugui respondre. Per això, si el servidor DHCP fals de l'atacant respon més de pressa que el legítim, el dispositiu obtindrà la configuració errònia. Per prevenir aquest tipus d'atacs existeixen algunes recomanacions clau:

1 | Connectar correctament els encaminadors a la xarxa

- Si es connecta un encaminador a la xarxa utilitzant el port erroni i la configuració per defecte, pot ser que respongui a peticions DHCP i desconfigure els dispositius de la xarxa.
- En general, no s'ha de permetre l'ús d'encaminadors no configurats per l'administrador de la xarxa, ja que poden ser una amenaça per a aquesta.

2 | Supervisar el trànsitc DHCP amb DHCP Snooping

- Per evitar un possible atac de DHCP Spoofing, els dispositius empresarials de xarxa com *switches* disposen del mecanisme de DHCP Snooping.
- Aquest mecanisme permet escanejar per paquets DHCP no autoritzats. D'aquesta manera, només s'autoritzaran respostes DHCP des del servidor legítim de l'empresa, mitigant els atacs que provenen d'usuaris connectats a la xarxa.

IP Spoofing

De manera similar, els atacs d'IP Spoofing cerquen **suplantar la identitat d'un dispositiu legítim de la xarxa**. És a dir, s'intenta suplantar l'adreça de xarxa de servidors importants, d'un usuari, o fins i tot la de l'encaminador. Aquest atac fa possible molts altres que es basen en aquesta suplantació d'identitat. Per mitigar l'atac, existeixen algunes mesures fonamentals:

3 | Configurar Dynamic ARP Inspection (DAI)

- Per a evitar la suplantació d'adreça IP associant una adreça física falsa, es pot activar la inspecció del protocol ARP amb DAI.
- Això mitiga atacs ARP Spoofing que permetrien a un atacant fer-se passar per una IP que no li correspon.

4 | Configurar regles d'accés mitjaçant un tallafoc

- Com s'ha vist en aquest nivell, la configuració de xarxa amb tallafocs i la segmentació de xarxa són mecanismes útils per evitar molts atacs.

CONTROLANT LES CONNEXIONS: INTRODUCCIÓ ALS TALLAFOCS

Els tallafocs o tallafocs en una xarxa permeten el filtratge i bloqueig de trànsit de xarxa mitjançant llistes de control d'accés o regles. Depenent del tipus de tallafoc, es poden bloquejar paquets de xarxa atenent diferents característiques de la comunicació, com l'adreça IP o el port.

e.digitall.org.es/A4C41C1V05

- El filtratge amb tallafoc i el bloqueig de peticions d'IP que no pertanyen a una xarxa, mitiga atacs de suplantació d'IP de manera remota.

Man in the Middle (MitM)

D'altra banda, els taques **Man in the Middle (MitM)** són un concepte genèric que agrupa amenaces en les quals l'atacant se situa enmig de la comunicació, amb l'objectiu d'**interceptar, inspeccionar o manipular la comunicació**. Per evitar aquest tipus d'atacs, és important evitar la suplantació IP, ARP i DHCP, com s'ha comentat abans. A més, hi ha mesures que ajuden a mitigar els atacs MitM:

5 | Dissenyar una topologia de xarxa segura i segmentada

- Mantenir una xarxa segmentada permet establir regles que separen les diferents parts d'una xarxa corporativa. Per exemple, establint zones privades, públiques i desmilitaritzades (DMZ).
- D'aquesta manera, s'evita que un atacant connectat a una xarxa més fàcilment accessible tingui accés a la xarxa de servidors o d'administració.

6 | Xifrar i autenticar les comunicacions

- El xifratge de la informació en trànsit mitiga les inspeccions de trànsit i manté la informació confidencial.
- Emprar sistemes de xifratge com TLS permet autenticar a les parts i transmetre la informació xifrada entre ambdues, evitant manipulacions.

TOPOLOGIA SEGURA DE XARXA

La segmentació d'una xarxa i la seva organització permeten establir controls d'accés més eficients. A més, la separació en zones de dispositius crítics, dispositius públics i els dels usuaris utilitzant xarxes virtuals o VLAN són algunes de les pràctiques per a establir un disseny de xarxa més segur.

e.digitall.org.es/A4C41C1V04

Denegació de Servei (DoS)

Finalment, les **denegacions de servei** són atacs menys sofisticats però molt destructius, que **afecten la disponibilitat de la xarxa de comunicacions i, per tant, de la informació**. Aquest tipus d'atacs pretenen neutralitzar i paralitzar les comunicacions per impedir l'accés als sistemes d'informació amb l'objectiu d'afectar el procés de negoci d'una empresa.

Existeixen diferents tipus d'atacs de Denial of Service (Dos), per la qual cosa han de tenir-se en compte mesures de seguretat de diferent índole, com:

7 | Mantenir els dispositius de xarxa i d'usuaris actualitzats

- Existeix programari maliciós com el programari de segrest (ransomware) o un altre tipus de cucs que poden distribuir-se per la xarxa i afectar la disponibilitat de la informació.
- El programari maliciós s'aprofita de les vulnerabilitats existents en el programari, per la qual cosa mantenir als equips actualitzats mitiga aquest tipus d'amenaces.

8 | Instal·lar sistemes de detecció i prevenció d'intrusions

- Els IDS i IPS són sistemes que permeten monitorar la xarxa, detectar i fins i tot bloquejar atacs coneguts com les denegacions de servei.
- Instal·lar i mantenir actualitzats aquests mecanismes ajuda a prevenir Dos bloquejant la comunicació i la saturació dels sistemes.

9 | Dissenyar sistemes redundants i manteir còpies de seguretat

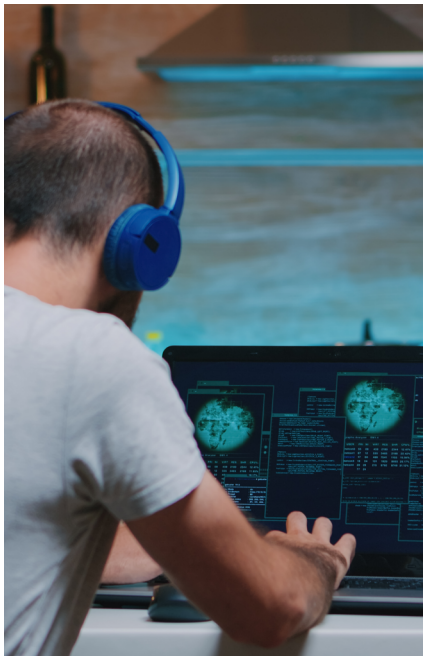
- Les denegacions de servei impedeixen l'accés a sistemes, saturant-los o fent inaccessible la informació que alberguen.
- Per evitar la pèrdua de servei o la pèrdua d'informació, s'han de mantenir còpies de seguretat de la informació i sistemes redundants. En cas de fallada o saturació, es redirigirà a usuaris al sistema redundant, o es restablirà la còpia de seguretat de la informació.

Com hem vist, existeixen multitud de mesures que poden aplicar-se per mitigar els atacs més comuns a les xarxes. La seguretat és un procés, per la qual cosa aquestes contramesures s'han d'anar aplicant gradualment, mantenint actualitzades les solucions i revisant el seu correcte funcionament de manera periòdica.

SISTEMES DE DETECCIÓ I PREVENCIÓ D'INTRUSIONS (IDS/IPS)

Els sistemes de detecció i prevenció d'intrusions permeten monitorar el trànsit de xarxa per detectar atacs coneguts o fins i tot desconeguts. Els IPS permeten, a més, bloquejar la comunicació si es detecta algun tipus d'atac, com una denegació de servei.

e.digitall.org.es/A4C41C2V08

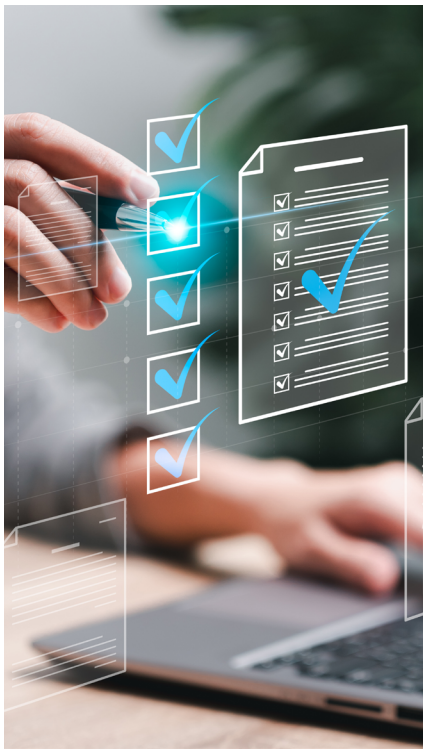


Seguretat

Nivell C1 4.1 Protecció de dispositius

Certificats digitals

Signatures digitals



En l'era digital, on la seguretat de la informació és primordial, els certificats digitals exerceixen un paper fonamental en l'autenticació i en la protecció de la integritat de les dades. Els certificats digitals són documents electrònics que contenen informació criptogràfica, cosa que permet la verificació de la identitat d'una entitat en entorns digitals. En aquest article, explorarem els formats de certificats digitals més comuns, la informació que emmagatzemen i les diverses aplicacions en les quals s'utilitzen.

Concepte i funcionament dels certificats digitals

Què és un certificat digital i com funciona?

Com hem vist, un certificat digital és un arxiu electrònic que s'utilitza per a associar una identitat digital a una entitat o persona física. És emès per una Autoritat de Certificació (CA, per les seves sigles en anglès) de confiança i és utilitzat per establir la identitat i confiança en entorns digitals.

Els certificats digitals utilitzen criptografia de clau pública per garantir l'autenticitat de l'entitat a la qual s'associen. El certificat conté la clau pública de l'entitat i està signat digitalment per la CA emissora. Quan un usuari o sistema necessita verificar la identitat d'una entitat, verifica la signatura digital del certificat utilitzant la clau pública de la CA.

Tipus de certificats digitals i les seves aplicacions

- **Certificats emesos per autoritats-format X.509**: el format X.509 és un dels més utilitzats per a certificats digitals. És àmpliament reconegut i és compatible amb una àmplia varietat d'aplicacions i protocols de seguretat. Els certificats en format X.509 contenen informació com el nom del titular, el període de validesa, la clau pública, el nom de la CA emissora i la seva signatura digital.
  - Un exemple d'aquesta mena de certificats són els certificats de persona física emesos per la Fàbrica Nacional de Moneda i Timbre (FNMT). Per sol·licitar-

los, només és necessari utilitzar un navegador web compatible i seguir el procediment de la seva pàgina web.
  - Una vegada obtingut aquest certificat, s'instal·larà en el navegador que hàgim usat. Podem fer una còpia d'aquest certificat des de la configuració del navegador, exportant-lo a un arxiu protegit per contrasenya, perquè pugui importar-se en altres navegadors o dispositius.

- **Certificats personals generats per un mateix per al xifratge de correu - protocol PGP/GPG**: Pretty Good Privacy (PGP) i GNU Privacy Guard (GPG) són protocols de criptografia que utilitzen formats de certificats propis. Aquests certificats són populars en l'àmbit de la seguretat de correu electrònic i permeten l'autenticació i el xifratge de missatges.
  - Per poder generar-los i utilitzar-los, és necessari tenir instal·lat programari com Kleopatra i OpenPGP. Existeixen diversos clients de correu electrònic, com Thunderbird, que permeten xifrar i signar correus electrònics usant PGP/GPG.
- **Certificats de correu electrònic - protocol S/MIME**: l'estàndard S/ACARONI (Secure/Multipurpose Internet Mail Extensions) utilitza certificats digitals per a proporcionar seguretat i autenticació en el correu electrònic. Els certificats S/ACARONI es basen en el format X.509 i s'utilitzen per signar i xifrar missatges de correu electrònic.
  - Existeixen alguns certificats X.509 que permeten el seu ús per a xifrar correus electrònics. Usant clients de correu com Outlook o Thunderbird, és possible xifrar i signar correus electrònics amb certificats compatibles.

Informació emmagatzemada en els certificats digitals

- **Identitat del titular**
  Un dels components clau d'un certificat digital és la informació d'identitat del titular. Això pot incloure el nom, l'adreça de correu electrònic, l'organització o empresa associada i altres dades rellevants per verificar la identitat de l'entitat.
- **Clau pública**
  Els certificats digitals també emmagatzemen la clau pública corresponent a l'entitat a la qual s'associen. La clau pública s'utilitza per verificar l'autenticitat i establir una comunicació segura amb l'entitat en qüestió.
- **Firma Digital de la CA**
  Per garantir la integritat del certificat, la CA emissora signa digitalment el certificat utilitzant la seva clau privada. Aquesta signatura permet als usuaris i sistemes verificar que el certificat no ha estat alterat i que prové d'una font de confiança.

Aplicacions dels certificats digitals

Autenticació en llocs web

Els certificats digitals exerceixen un paper fonamental en l'autenticació de llocs web a través del protocol HTTPS. Els certificats SSL/TLS (Secure Sockets Layer/Transport Layer Security) permeten establir connexions segures i autenticar la identitat d'un lloc web, proporcionant confiança als usuaris i protegint la informació transmesa. Quan un usuari intenta accedir a un lloc web segur, el seu navegador sol·licita al servidor que presenti un certificat vàlid. El navegador verifica l'autenticitat del certificat i si coincideix amb el domini al qual s'accedeix. Si el certificat és vàlid i de confiança, s'estableix una connexió segura i es mostra un indicador visual, com un cadenat, per indicar a l'usuari que la connexió és segura.

Signatures digitals

Els certificats digitals també s'utilitzen per a la signatura digital de documents electrònics. En signar un document digitalment amb un certificat vàlid, es pot verificar la integritat del document i la identitat del signant, la qual cosa és essencial en entorns legals i empresarials. La signatura digital utilitza criptografia de clau pública per crear una empremta digital única del document. Aquesta empremta digital s'adjunta al document i es pot verificar utilitzant la clau pública del certificat associat. Si el document ha estat alterat d'alguna manera, la verificació de la signatura digital fallarà, la qual cosa garanteix la integritat del contingut. A més, la signatura digital està vinculada a la identitat del signant, la qual cosa proporciona més confiança i autenticitat.

Xifratge de correu electrònic

Mitjançant l'ús de certificats S/MIME, és possible xifrar i signar missatges de correu electrònic per garantir la seva confidencialitat i autenticitat. Això protegeix la privacitat de les comunicacions i evita que els missatges siguin interceptats o alterats. Quan un usuari envia un correu electrònic xifratge amb S/MIME, el missatge s'encripta utilitzant la clau pública del destinatari, la qual cosa assegura que només el destinatari pugui desxifrar i llegir el contingut. A més, en signar digitalment el missatge amb el certificat del remitent, es verifica l'autenticitat del remitent i s'assegura que el contingut del missatge no hagi estat alterat en trànsit.

Conclusió

En resum, els certificats digitals són una peça fonamental en la seguretat i autenticació d'entorns digitals. Quan s'empra criptografia de clau pública i formats com a X.509, PGP/GPG i S/MIME, els certificats digitals permeten verificar la identitat de les entitats, protegir la integritat de la informació i establir comunicacions segures. Des de l'autenticació en llocs web fins a la signatura digital i el xifratge de correu electrònic, els certificats digitals són eines versàtils i essencials per garantir la confiança i seguretat en l'era digital.

Seguretat

Nivell C1 4.1 Protecció de dispositius

Infraestructura de clau pública (PKI)

Infraestructura de clau pública (PKI)

La **Infraestructura de Clau Pública** (PKI, per les seves sigles en anglès) és un sistema vital per a la seguretat de la informació. A través de la PKI, s'estableix una infraestructura de confiança que permet l'autenticació, integritat i confidencialitat de les comunicacions digitals.

La PKI es basa en l'ús de certificats digitals emesos per una Autoritat de Certificació (CA). Aquests certificats contenen claus públiques utilitzades per verificar la identitat dels participants i xifrar la informació. Com hem vist abans, els certificats digitals exerceixen un paper fonamental en aplicacions com el xifratge de correu electrònic, la signatura digital i la protecció de les connexions segures en línia.

CERTIFICATS DIGITALS

Document referenciat: ***A4C41C1D03***

És necessari comprendre bé com funciona la PKI i aplicar els seus principis en la pràctica, per aprofitar els seus avantatges i portar a la pràctica l'ús dels certificats digitals.

Autoritats de Certificació

Les **Autoritats de Certificació** (CA, per les seves sigles en anglès) són components essencials dins de la PKI. Són entitats de confiança encarregades d'emetre i gestionar els certificats digitals.

En l'àmbit tècnic, les CA utilitzen les seves claus privades per signar els certificats digitals que emeten. D'aquesta manera, quan es validen les signatures dels certificats digitals, es fa amb la clau pública de l'Autoritat de Certificació.

Prenguem com a exemple un usuari que signa un document PDF amb un certificat digital, expedit per la Fàbrica Nacional de Moneda i Timbre (FNMT) com a Autoritat Certificadora. Quan es validi la signatura usant les claus públiques, es pot utilitzar el servei Validi de la FNMT, que verificarà usant les seves claus d'Autoritat Certificadora per autenticar el certificat.

Saber-ne més

El servei VALIDe (*valide.redsara.es/valide*) permet validar la signatura de documents signats amb certificats expedits per tots els prestadors que es troben inscrits en el registre de la Secretaria d'Estat de Telecomunicacions i per a la Societat d'Informació del Ministeri d'Indústria, Turisme i Comerç d'autoritats.

Estructura d'una PKI

Els certificats digitals són normalment signats per una autoritat certificadora de darrer nivell. Una PKI és una estructura jeràrquica amb diversos nivells.

En el cim d'aquesta estructura, estan les CA arrel, en les quals es diposita màxima confiança. Aquestes CA arrel són encarregades de signar els certificats d'altres CA, sota en aquesta jerarquia de confiança. Així, aquestes darreres CA signen al seu torn els certificats dels usuaris.

D'aquesta manera, es permet una millor gestió de claus asimètriques i de la confiança en aquestes. Les claus privades de les CA han d'estar molt ben protegides, ja que són les que signen els certificats. Com més a dalt en la cadena del PKI, més confiança dipositem en la CA i, per tant, en la seva gestió de claus. Si una CA intermèdia és compromesa, llavors només aquells certificats que hagi signat aquesta han de ser revocats, és a dir, invalidats.

Les estructures PKI ens permeten crear una cadena de confiança i gestionar de manera més eficient els certificats, garantint la seva validesa i fiabilitat. D'aquesta manera, es poden emprar amb validesa legal i amb el suport de governs i estats.

FONAMENTS TÈCNICS DE LA FIRMA DIGITAL

e.digitall.org.es/A4C41C1V08

DigitAll

Seguretat

4.2
PROTECCIÓ DE LES DADES PERSONALS I LA PRIVACITAT

Seguretat

Nivell C1 4.2 Protecció de les dades personals i la privacitat

Millora de la privacitat en les compres i pagaments en línia

Millora de la privacitat en les compres i pagaments en línia

Web de compres

Gràcies a Internet i al seu ús generalitzat, la societat actual ha anat evolucionant cap a un entorn digital amb una alta interacció entre persones i serveis. Un dels serveis que s'ha digitalitzat i que ha tingut un gran acolliment és el mercat de compravenda de productes i serveis. Ja no és necessari ajustar-se a compres en els establiments pròxims, sinó que pots adquirir el producte o el servei que vols gairebé a qualsevol lloc del món.

Milers d'empreses s'han llançat a oferir productes i serveis a través dels seus webs. La manera de compra és senzilla i consta d'uns passos que es descriuen a continuació.

Procediment habitual de compra en línia d'un producte:

1 | **L'usuari accedeix al web de l'empresa.**
2 | **L'usuari cerca el producte que vol.**
3 | **L'usuari l'afegeix al seu carret de la compra.**
4 | **L'usuari proporciona les dades de lliurament.**
5 | **L'usuari proporciona les dades de facturació.**
6 | **L'usuari efectua el pagament.**
7 | **L'empresa rep el pagament.**
8 | **L'empresa empaqueta el producte.**
9 | **L'empresa lliura el paquet amb el producte a un operador logístic.**
10 | **L'operador logístic s'encarrega de fer arribar el producte a l'usuari.**

Aquest mecanisme requereix un cert grau de confiança entre l'usuari, l'empresa i l'operador logístic: l'usuari s'arrisca donant els seus diners a una empresa que ha d'enviar-li el producte, l'empresa s'arrisca al fet que la transferència de diners de l'usuari no es faci realment i l'empresa logística al fet que el producte no sigui recollit per l'usuari final i que hagi de córrer amb les despeses de devolució a l'empresa venedora.

L'empresa logística és un actor important en aquesta transacció, però el seu risc és menor, ja que solen contractar assegurances que cobreixen aquestes despeses i com solen fer

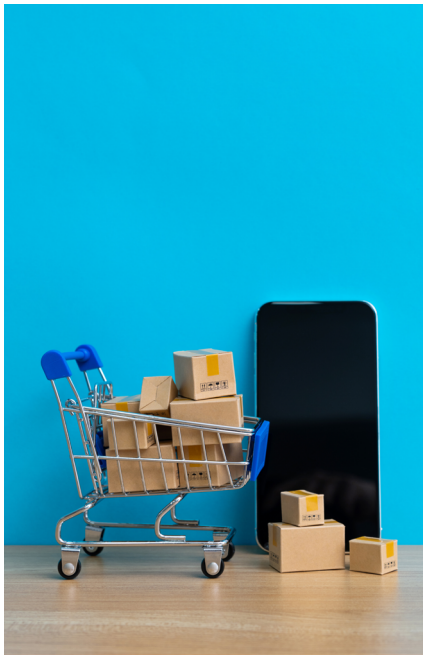
un nombre elevat de lliuraments des dels mateixos proveïdors, poden esperar a haver de realitzar un nou trajecte a l'empresa per a fer la devolució i minimitzar els costos de trajectes.

Per tant, són els usuaris i les empreses venedores qui ha de tenir una seguretat de no ser enganyats. Ens centrarem en els usuaris i veurem algunes idees bàsiques que han de seguir-se per a incrementar la seguretat i la seva privacitat en les compres en línia.

Confiança en el web de compres

Per poder mantenir una alta privacitat, el primer que ha de comprovar un usuari és que el web en la qual pretén fer la compra és de confiança: no donarem les nostres dades personals a ningú en qui no confiam. En la vida real, les persones solen preferir comprar els productes en botigues d'empreses conegudes abans que a un desconegut pel carrer. Això s'aplica igual quan comprem per Internet. Hem de conèixer el web en què compram i hem de confiar que l'empresa que la gestiona té una bona reputació.

Hi ha milers, milions de webs a Internet. La gran majoria són d'empreses que volen fer vendes reals, guanyant-se un benefici en aquest intercanvi. No obstant això, aquesta minoria de webs fraudulentes que només volen enganyar-nos per obtenir els nostres diners i les nostres dades personals són les que hem de detectar i rebutjar.



Si compram a webs d'empreses conegudes i amb bona reputació com Amazon, El Corte Inglés, Carrefour, MediaMarkt, etc. tenim el suport de grans companyies amb molts anys d'experiència i que tenen un gran prestigi. Tots aquests indicadors mostren que podem tenir un nivell alt de confiança en aquests webs i és fiable donar-li les nostres dades personals, ja que donaran un ús legítim a aquestes dades.

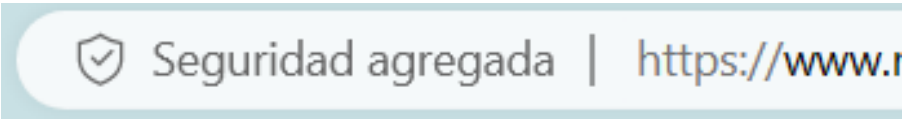
Si el web de compra no és d'una empresa coneguda, podem fer una cerca de ressenyes d'altres usuaris. És preferible que les opinions no siguin del mateix web, ja que podrien haver-se posat únicament aquells que siguin favorables a l'empresa, o fins i tot que siguin inventats.

Hi ha alguns consells que es poden seguir per tenir indicis de si un web és fraudulent:

- Està mal traduïda.
- Té un excés de publicitat o de finestres emergents de productes "estranys" o poc rellevants en relació amb la compra que es pretén fer.
- L'aspecte general és poc professional.
- Els títols de les seccions no coincideixen amb el contingut mostrat.
- Els preus són excessivament barats sense oferir motius que ho justifiquin clarament (per exemple, són barats perquè són productes de segona mà, devolucions, descatalogats, etc.).

Xifratge de la web de compres

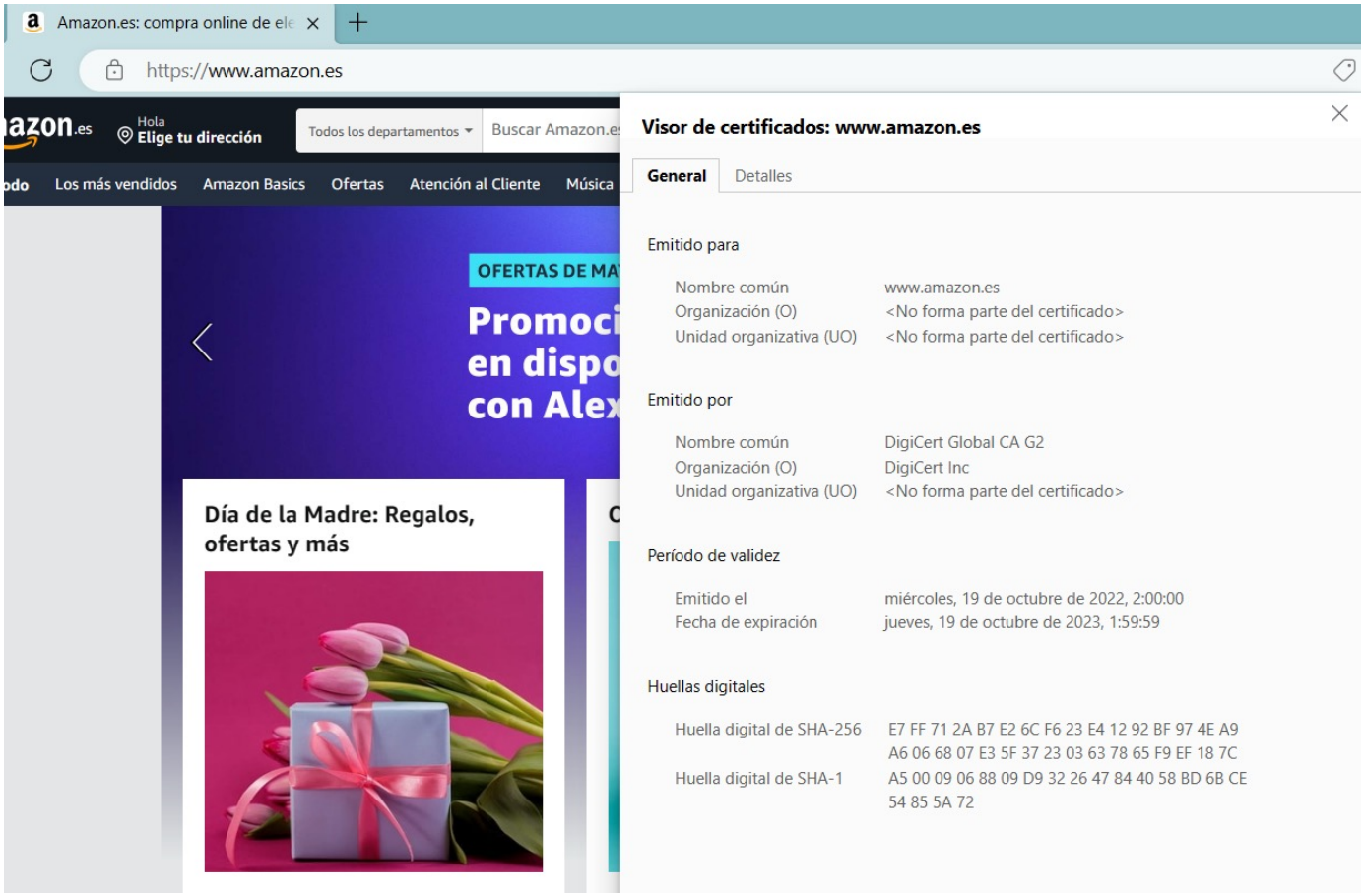
Abans de proporcionar cap dada personal a un web en què vols fer una compra has de fixar-te si la connexió és segura. Per això has de comprovar si la connexió que fas amb el navegador està xifrada. Les connexions segures es fan utilitzant el protocol segur **https.**



Detall del navegador amb connexió amb protocol **https** i símbol de seguretat.

Les pàgines web que no tenen protocols segurs https podrien ser pàgines legítimes, però la seva inseguretat podria fer que les nostres dades poguessin ser capturats per qualsevol atacant.

A més, el protocol https permet saber qui ha generat el certificat d'identitat. Aquest certificat SSL és el que s'empra per establir la connexió segura entre el nostre navegador i el web de compra de l'empresa. Així, revisant el certificat podem assegurar-nos que el web coincideix amb el nom certificat i que l'**organització certificadora és fiable**.



Detall del certificat digital de www.amazon.es.

Altres estàndards de seguretat

Encara que l'ús del protocol **https** és el principal estàndard de seguretat, existeixen altres estàndards en els quals hem de fixar-nos per tenir més confiança en el web de compres.

Les empreses que gestionen de manera segura les teves dades privades seguint uns requisits molt estrictes obtenen la certificació **ISO 27001**. Per tant, aquelles empreses que tenguin aquesta certificació han demostrat que tenen un procediment molt segur que garanteix la privacitat de les nostres dades personals.

Exemple de web d'empresa certificada amb ISO/IEC 27001 i altres certificats.

Existeixen empreses a Internet dedicades a analitzar la privacitat de les pàgines web de les empreses i atorgar-los segells de fiabilitat. Un dels segells de privacitat més coneguts és TRUSTe®. Tenir-ho incrementa la seguretat dels usuaris en com aquest web maneja la privacitat de les dades, la qual cosa la fa molt més de confiança.

Logo del segell TRUSTe® de garantia de seguretat i privacitat d'empreses i webs.

Polítiques de privacitat, lliurament i mètodes de compra

Una vegada l'usuari ha pogut establir un nivell de confiança en el web, es pot passar a un segon nivell, en el qual l'usuari ha d'avaluar si l'empresa utilitzarà les seves dades personals de la manera que ell vol i si existeixen mètodes de compra que li interessin i li garanteixin el nivell de privacitat que vol.

Polítiques de privacitat

Abans de proporcionar les nostres dades personals a una web, hem d'informar-nos per què volen les dades. Per exemple, realment és necessari que un web sàpiga la nostra adreça del treball si el que volem fer és una compra personal?

O bé, guardaran les nostres dades en els servidors de l'empresa o els cediran a terceres empreses perquè ens enviïn missatges? Si l'empresa és de la Unió Europea haurà de complir determinades normatives, com el Reglament General de Protecció de Dades (RGPD, o en anglès, GPRD). Si el web està localitzat fora de la Unió Europea, caldrà revisar la normativa del país en la qual se situa per saber quin dret tenim sobre les dades personals que cedim.

Altres polítiques de compres

A més de la privacitat, els usuaris hem de revisar altres polítiques que tengui la botiga i que poden influir molt la compra del nostre producte. Per exemple, quina garantia té el producte? On s'aplica la garantia? Qui s'encarrega de les despeses de transport? S'inclouen els costos de duanes si és una venda internacional? Quant temps es pot retardar l'enviament abans de poder reclamar? En cas de reclamació legal, a quina legislació i tribunal s'acull l'usuari?

En general, els usuaris han de tenir en compte els següents aspectes per fer la seva compra:

- **Formes d'enviament:** tipus de transport, embalatge, lloc de lliurament, etc.
- **Garantia:** tipus de garantia (reposició completa, arranjament sense franquícia, arranjament amb franquícia, bo de recompra, etc.) i temps per aplicar-la.
- **Desistiment de compra:** durant quant temps podem rebutjar la compra, cost del desistiment, etc.
- **Reclamacions:** temps de reclamació, lloc i mode de reclamació.
- **Transport:** costos, terminis, taxes addicionals.
- **Serveis addicionals:** assegurances de reparació, de transport, actualitzacions, postvenda, etc.

L'anàlisi d'aquests apartats pot fer aparèixer preus ocults que no es mostrin en el preu inicial del producte.

Mètodes d'entrega

Existeixen múltiples formats per efectuar els lliuraments. Cadascun té un procediment diferent, amb costos distints i també amb implicacions de privacitat de les dades diferents, en cada cas.

Quant al lliurament sol haver-hi tres tipus:

- **Lliurament en domicili:** l'empresa logística lliurament el producte en el domicili (o on li indiqui el client). Per això, necessita moltes dades personals, des de nom, cognoms, DNI i adreça del domicili. És el mecanisme amb un menor nivell de privacitat.
- **Lliurament a Correus o en una botiga associada:** el producte es diposita en l'oficina de Correus o en una botiga associada, i l'usuari va a aquests llocs i recull el seu producte. L'empresa ha de conèixer dades personals del client, per poder autoritzar la recollida, però no ha de saber el domicili o una altra dada personal.
- **Lliurament en un punt de recollida:** el producte es lliura en un caseller segur i l'usuari pot obrir-lo amb una combinació única i recollir el seu producte. En aquest cas, l'empresa no té cap dada personal d'ubicació ni de domicili. És el tipus de lliurament amb més nivell de privacitat.

Mètodes de pagament

Les nostres dades bancàries és una de les dades personals més crítiques quant a privacitat. Per tant, hem de parar esment particular als mètodes de pagament.

Respecte d'aquests, existeixen diverses opcions:

- **Transferència bancària:** és el mecanisme que té un nivell de privacitat més baix, ja que és necessari proporcionar un codi de compte bancari complet, amb la inseguretat que això pot implicar de càrrecs indeguts.
- **Pagament amb targeta de crèdit:** el client proporciona les dades de la seva targeta de crèdit i a través d'una passarel·la segura es fa el càrrec en la targeta. En determinades entitats bancàries pots activar un segon nivell de seguretat havent de fer una autorització d'aquest càrrec a través d'aplicacions bancàries. Això proporciona un nivell addicional de seguretat, ja que no poden fer càrrecs addicionals sense l'autorització del client.

- **Pagament amb moneder electrònic/targeta de prepagament:** el procediment de pagament és igual al de pagament amb targeta, però la que s'usa és una targeta en la qual es carrega el cost que es vol pagar. D'aquesta manera, en el pitjor dels casos, l'atacant només hauria disposat de l'efectiu que hi ha en aquesta targeta sense possibilitat de fer càrrecs addicionals. És un nivell de privacitat superior perquè no es dona una targeta associada al compte bancari de l'usuari.
- **Pagament a través de PayPal, Google Pay, o similar:** l'empresa PayPal (Apple, Google o altres similars) fa un pagament en el teu nom, carregant-li el cost a l'usuari en el seu compte corrent o en una targeta bancària que prèviament haurà registrat. És un dels sistemes més segurs, perquè l'usuari no ha de proporcionar dades bancàries a la botiga, la qual cosa implica una major privacitat.
- **Pagament contra reemborsament:** l'usuari paga al transportista en recollir el producte. Sol tenir un cert sobrecost per a cobrir l'assegurança del transport. És un dels mètodes amb més privacitat, ja que només es proporciona el lloc de lliurament i el nom de l'usuari.

Privacitat en la compra

En fer compres per Internet podem estar deixant rastres a possibles atacants que puguin aprofitar per envair la nostra privacitat. És convenient conèixer diferents opcions per evitar, o almenys limitar, l'atac a la nostra privacitat.

Registre d'usuari al web

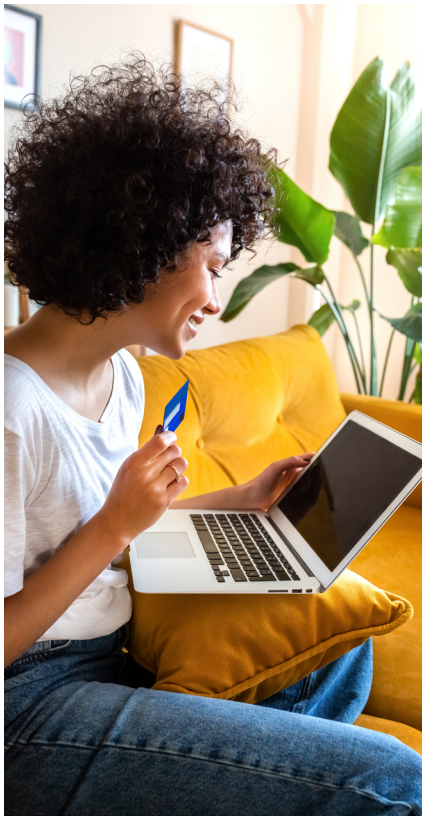
És habitual que totes les botigues electròniques ens sol·licitin un registre en el seu sistema. Gràcies a aquest registre podem recuperar comandes, continuar amb el procés de compra, incorporar targetes bancàries per accelerar el mecanisme de pagament, etc.

Aquests avantatges, no obstant això, pot ser que no siguin interessants si es farà una compra única i puntual en una determinada web. Li proporcionam moltes dades personals, amb la pèrdua de privacitat que això comporta. Hi haurà

determinades dades que haurem de proporcionar per fer la compra segons el procediment de lliurament i el mètode de pagament que triam.

Existeixen algunes botigues que permeten comprar com a **convidats**, sense necessitat de fer un registre, demanant les dades personals exclusivament necessàries per fer la compra. Però la gran majoria dels webs exigeixen el registre per comprar i en molts casos, sol·liciten un correu electrònic.

En aquests casos, per evitar haver de donar el nostre correu personal personal, podem crear altres correus electrònics secundaris que emprem únicament per fer compres. De tal manera, que separem el nostre correu electrònic personal de l'email de compres. Si per algun motiu hi hagués una fallada de seguretat al web de compres o es produís un hackeig, no estaríem donant accés al nostre correu electrònic personal.



COMPARTINT DADES EN LA XARXA I XARXES SOCIALS (INFORMACIÓ, FORMULARIS, ARXIUS, FOTOS, ETC.)

Veure diferents maneres de compartir informació a la xarxa.

e.digitall.org.es/A4C42C1V07

Una altra opció és l'ús d'àlies de correu electrònic. Es creen diferents àlies de la mateixa adreça d'*email* original, de tal manera que un correu electrònic enviat a l'àlies es rep en la carpeta de correu de l'adreça d'email original. Se solen agregar filtres de recepció, que a mesura que es rebi un email d'un àlies s'enviï a una subcarpeta. En aquest cas, igual que en l'anterior, un atacant no tindria accés al correu principal i les contramesures es podrien implementar fàcilment, simplement anul·lant aquest àlies.

Finalment, hi ha servidors de correu electrònic que permeten agregar al nostre correu principal etiquetes, ja que alteren l'identificador de l'email, però lliurant el correu en la mateixa carpeta del correu original. Això és possible fer-ho amb Gmail.

Saber-ne més

Gmail és capaç de crear adreces email afegint el símbol + darrere del nom d'usuari i abans de @gmail.com. Tots els correus arribaran a la mateixa safata d'entrada de l'usuari, però mitjançant un filtre d'etiqueta, es podrà gestionar millor els correus electrònics que es proporcionin als webs.

Per exemple, per a l'usuari maria@gmail.com pots crear adreces electròniques addicionals:

maria+webcompra@gmail.com
maria+amazon@gmail.com
maria+spam@gmail.com

Tots els correus arribaran a la carpeta d'entrada de maria@gmail.com però cadascun amb una etiqueta diferent.

Dispositius segurs

El procés de compra per Internet comença per la navegació fins a trobar el producte que desitges en un web. A partir d'aquí, com hem vist, es produeix tot el procediment de compra digital. Per tant, l'ús d'un dispositiu informàtic per navegar és imprescindible.

Hi ha múltiples dispositius que poden utilitzar-se per navegar per Internet: telèfons intel·ligents, tauletes, ordinadors portàtils, ordinadors de sobretaula, etc. Tots ells requereixen un navegador per explorar les pàgines web de les botigues on comprar: Chrome, Firefox, Edge, etc.

La principal recomanació és que utilitzis un dispositiu personal i no compartit amb cap altra persona. Si el dispositiu està compartit, és possible que es deixin arxius després de la navegació i la compra, que podrien explorar-se per altres usuaris amb la consegüent bretxa de privacitat.

Si s'utilitza un dispositiu compartit, es recomana que cada usuari tengui el seu perfil propi protegit amb contrasenya, sense que la resta d'usuaris tingui possibilitat d'accedir a aquest perfil.

Si no és possible tenir un perfil propi protegit per contrasenya, es recomana utilitzar el mode incògnit o de navegació privada dels navegadors, perquè en finalitzar la sessió tots els fitxers creats pel mateix navegador s'eliminin.

Navegació en xarxes segures

Els webs poden ser molt segurs i garantir una alta privacitat, però si estàs usant una xarxa sense fil que no és segura, deixes que qualsevol atacant pugui veure el quefas.

El primer consell és no utilitzar xarxes públiques. Tampoc no són segures les xarxes wifi que ofereixen gratis els establiments, cafeteries o altres comerços. Aquestes utilitzen xarxes amb seguretat, però que s'exposa públicament la clau, de tal manera que qualsevol pot conèixer-la i accedir a aquesta xarxa.

Millor emprar la nostra xarxa pròpia amb seguretat i control d'accés, per garantir que no hi ha atacants en aquesta xarxa que puguin espiar-nos.

No obstant això, si no podem utilitzar la nostra xarxa, tenim algunes opcions per evitar el problema d'utilitzar una xarxa wifi que podria no ser segura.

1 | **Crear una wifi a partir de les dades del teu telèfon mòbil:** utilitzant el teu telèfon intel·ligent pots crear una xarxa wifi amb una clau que només tu sàpigues i utilitzar el mateix telèfon intel·ligent per accedir a Internet, cosa que et garanteix que cap altre dispositiu utilitzarà aquesta wifi.

2 | **Utilizar una VPN:** les Xarxes Privades Virtuals (VPN, per les seves sigles en anglès) permeten crear una connexió segura dins d'una xarxa pública mitjançant una connexió encriptada amb un servidor remot que s'encarregarà de tramitar les peticions que fem.

Saber-ne més

Mètodes de pagament i la seva seguretat. *e.digitall.org.es/pago-seguridad*

Mètodes de pagament segur. *e.digitall.org.es/metodos-pago*

Detecta si una pàgina és fiable per comprar o és una estafa. *e.digitall.org.es/detectar-estafas*

TRUSTe® Privacy Certification. *e.digitall.org.es/truste*

DigitAll

Seguretat

4.3 PROTECCIÓ DE LA SALUT I EL BENESTAR

Seguretat

Nivell C1 4.3 Protecció de la salut i el benestar

Guia visual sobre el bloqueig d'usuari i missatges. Enfocament des de la salut

Guia visual sobre el bloqueig d'usuari i missatges. Enfocament des de la salut

En el present document es mostrarà una guia visual per bloquejar usuaris i missatges que no volem rebre. D'aquesta manera, es presenten els bloquejos en els dispositius mòbils i també en les xarxes socials.

Bloqueig d'usuaris i missatges a la xarxa

Els ordinadors i dispositius mòbils proporcionen un accés ràpid i senzill a múltiples formes de comunicació com anomenades, missatges o xarxes socials. Això ha suposat innombrables avantatges a l'hora de relacionar-se, però també ha provocat alguns perills com el ciberassetjament o el *flaming*. En un dels vídeos d'aquest nivell s'han explicat aquests conceptes i s'han proporcionat una sèrie de pautes per detectar-los i protegir-se.

CIBERASSETJAMENT I *FLAMING*: COM DETECTAR-LOS I PROTEGIR-SE'N?

En aquest vídeo s'aprofundeix en els conceptes de ciberassetjament i flaming. Així mateix, es proporcionen diversos mètodes per evitar aquestes situacions i detectar-les aviat.

e.digitall.org.es/A4C43C1V02

Aquest document se centra en la mateixa configuració dels dispositius tecnològics i de les xarxes socials. En concret, presenta diferents possibilitats de bloqueig d'usuaris i missatges en la xarxa.

NOTA

L'arribada dels ordinadors a les llars, l'accés a dispositius mòbils assequibles i la propagació d'Internet han provocat un canvi profund en el mode en què les persones es relacionen.

Avui dia, pràcticament tothom disposa d'un mòbil amb accés a Internet. Això possibilita múltiples maneres de comunicar-nos: crides, videotrucades, missatges de text o interacció a les xarxes socials.

Els avantatges són clars. Actualment, és possible trucar des de pràcticament qualsevol lloc, fer una foto de l'activitat que es

fa i enviar-la a l'instant o debatre sobre un esdeveniment en temps real. No obstant això, aquest tipus de comunicacions poden comportar uns certs perills com el ciberassetjament o el *flaming*.

Alguns d'aquests perills també poden passar al món real, no obstant això, el que passi a través d'un mitjà digital podria tenir més repercussió sobre uns certs tipus d'assetjament, a causa de la facilitat amb la qual es pot difondre un missatge.

Aquest tipus de situacions poden provocar un enorme sofriment a la víctima, la qual cosa podria derivar en una afecció sobre la seva salut mental.

En una situació així, a més de posar el succeït en coneixement de les autoritats i de valorar el fet d'acudir a un especialista en salut mental, és possible prendre mesures en els dispositius tecnològics i xarxes socials. En les següents subseccions s'explicaran diferents maneres de bloquejar a un determinat usuari a la xarxa, així com a limitar la recepció de trucades i missatges en els dispositius mòbils.

Bloqueig de trucades i missatges a dispositius mòbils

Una de les maneres més habituals d'assetjament mitjançant l'ús de dispositius tecnològics és l'assetjament telefònic. Aquest tipus d'assetjament implica la realització de crides o l'enviament de missatges de text de manera insistent i reiterada. A més, en moltes ocasions aquestes crides inclouen amenaces o insults. Tot això pot comportar una situació de temor, ansietat o estrès a la víctima, i li pot causar implicacions importants a la salut mental.

Saber-ne més

L'assetjament telefònic és un tipus d'assetjament, i conseqüentment, és un delicte recollit en el Codi Penal Espanyol. L'article 172 ter. estableix el següent:

Serà castigat amb la pena de presó de tres mesos a dos anys o multa de sis a vint-i-quatre mesos qui assetgi a 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.

e.digitall.org.es/acoso-telefonico

Davant una situació d'assetjament telefònic, a més de posar-ho en coneixement de les autoritats, és possible prendre mesures a través del menú de configuració del dispositiu mòbil.

Avui dia pràcticament tots els equips, independentment de la marca o model, compten opcions per bloquejar números de telèfon. Això permet impedir les trucades o missatges provinents d'un número determinat.

NOTA

A vegades, la situació d'assetjament no prové d'una persona en particular, sinó d'una companyia que intenta captar clients. A més de les recomanacions ja indicades, existeix una opció molt interessant denominada Llista Robinson. Es tracta d'un servei per evitar rebre publicitat d'entitats o empreses a les quals no se li hagi donat un consentiment exprés per això.

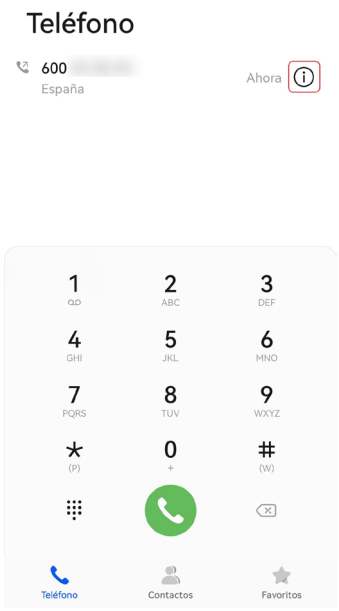
listarobinson.es

A continuació, s'indicarà com bloquejar un número de telèfon en un dispositiu Android. No obstant això, el procediment és molt similar en terminals iOS.

- La manera més senzilla de bloquejar un número és obrint l'aplicació **Telèfon**. Habitualment, quan es du a terme aquesta acció ja es visualitza l'historial de trucades, en cas contrari, caldrà seleccionar l'opció **Recents** o **Historial de trucades**, en funció del dispositiu.

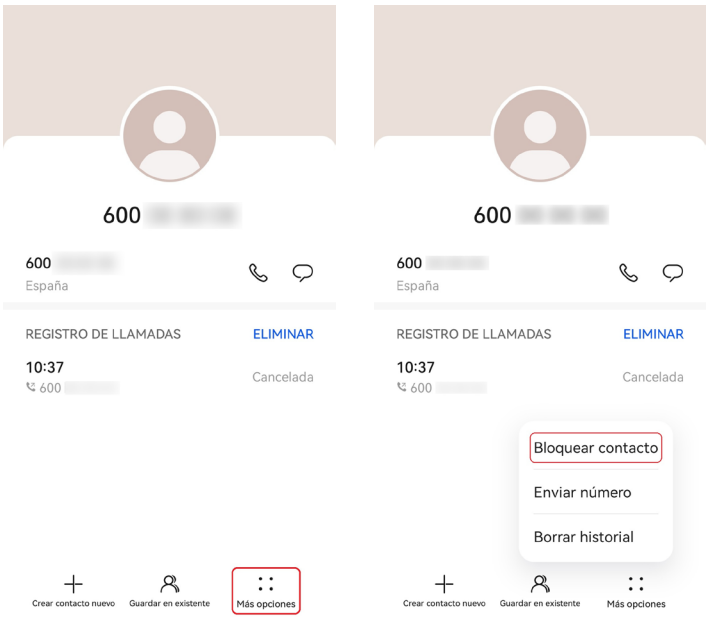
Font: Autoria pròpia.

- Una vegada es visualitzen les darreres trucades rebudes, simplement cal localitzar el número que es vol bloquejar i pressionar la icona. ⓘ



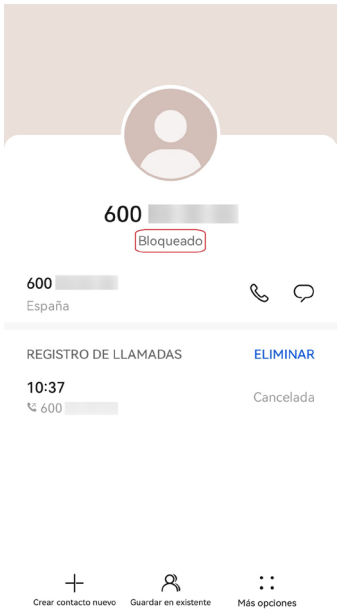
Font: Autoria pròpia

- A continuació, cal seleccionar la icona corresponent a **Opcions** i fer clic a **Bloquejar contacte**.



Font: Autoria pròpia.

- D'aquesta manera, el número quedarà bloquejat i no es rebran trucades ni missatges que en provinguin.



Font: Autoria pròpia

Si el número que es vol bloquejar es troba guardat com a contacte en l'agenda del dispositiu, el procediment és pràcticament igual. Simplement cal obrir l'aplicació Contactes, seleccionar el contacte que es vol bloquejar, i fer el procés explicat anteriorment.

Saber-ne més

A més de permetre bloquejar un número concret, els dispositius permeten configurar filtres per bloquejar números desconeguts, és a dir, tot aquell que no es trobi guardat com a contacte en el terminal. Així mateix, també és possible bloquejar qualsevol trucada que no estigui identificada, això és, que oculti el número de telèfon.

Enllaç web Android: *e.digitall.org.es/bloquear-telefono-android*
Enllaç web iOS: *e.digitall.org.es/bloquear-telefono-ios*

Bloqueig d'usuaris i missatges a les xarxes socials

L'ús de xarxes socials ha augmentat en gran manera en els darrers anys i s'ha convertit en una de les principals maneres de comunicar-se entre les persones. Això també ha suposat que siguin utilitzades com un mitjà de ciberassetjament. Algunes de les possibles maneres d'assetjament estan relacionades amb l'enviament reiterat de missatges, imatges o vídeos feridors, o que suposin una amenaça, amb la difusió de mentides o amb l'enviament de missatges suplantant la identitat de la víctima.

Saber-ne més

UNICEF disposa en el seu web d'un complet document en el qual donen resposta a algunes de les preguntes més freqüents sobre el ciberassetjament i en el qual també s'ofereixen diversos consells sobre la manera de fer-li front.

e.digitall.org.es/ciberacoso

Entre les xarxes socials més utilitzades en el món destaquen Facebook, YouTube, WhatsApp o Instagram. A través de totes elles poden produir-se situacions de ciberassetjament, per això és important conèixer que opcions ofereixen respecte del bloqueig d'usuaris i missatges.

Generalment, bloquejar un usuari implica no rebre missatges, ni cap mena de contingut procedent d'aquest. D'altra banda, l'usuari bloquejat no podrà visualitzar el contingut de l'altra persona, ni interactuar amb aquesta, entre altres accions.

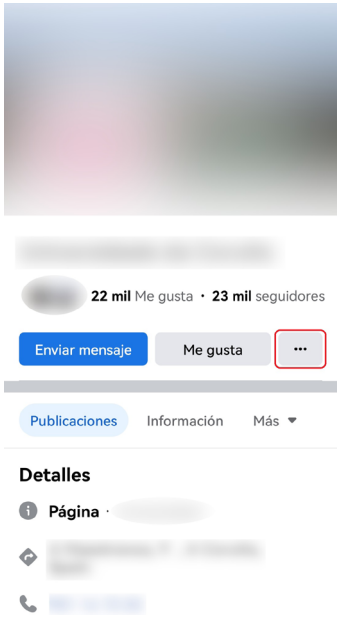
A continuació, s'explicarà com bloquejar un usuari a les xarxes socials esmentades. En qualsevol cas, habitualment tota xarxa social compta amb opcions de bloqueig.

Facebook

Si es bloqueja el perfil d'algú a Facebook, aquest no podrà etiquetar la persona que l'ha bloquejat ni consultar les seves publicacions, entre altres accions.

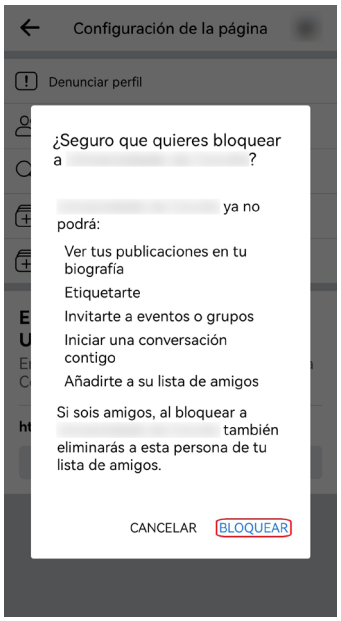
Per bloquejar un perfil en Facebook cal seguir els següents passos:

1 | Cercar el perfil de la persona que es vol bloquejar i fer clic en la icona.



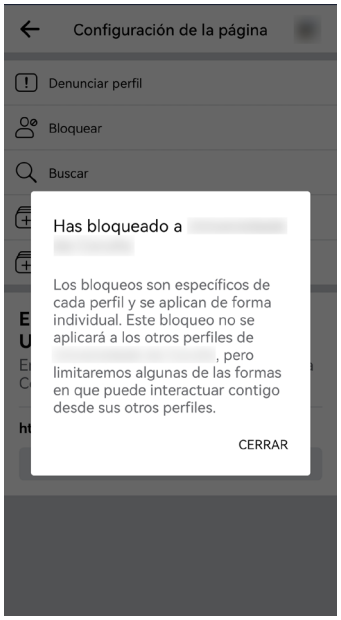
Font: Autoria pròpia.

2 | A continuació, un missatge emergent mostrarà les accions que no podrà fer el perfil una vegada aquest bloquejat. Per continuar amb el procés, simplement cal fer clic a **Bloquejar**.



Font: Autoria pròpia.

3 | Finalment, un missatge informarà que el perfil ha estat bloquejat correctament.

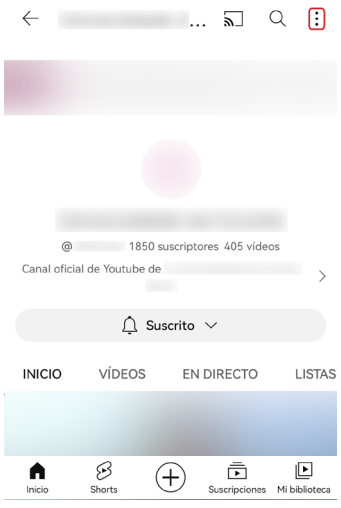


Font: Autoria pròpia.

YouTube

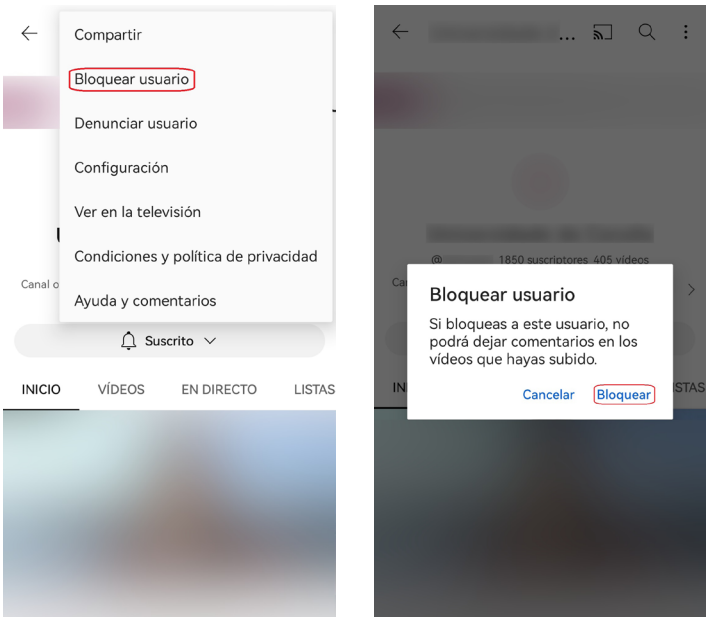
YouTube és una plataforma en la qual els usuaris poden compartir els seus vídeos. Per tant, el seu objectiu principal no és l'enviament de missatges. No obstant això, sí que és possible deixar comentaris en els vídeos, la qual cosa podria suposar un mitjà per publicar missatges que cerquen molestar o assetjar l'autor de la publicació o a la resta d'usuaris.

1 | Localitzar el canal de l'usuari que es desitja bloquejar i seleccionar la icona.



Font: Autoria pròpia

2 | Fer clic a l'opció **Bloquejar usuari** i confirmar l'acció. A partir d'aquest moment, l'usuari bloquejat no podrà deixar comentaris en els vídeos de la persona que ha sol·licitat el bloqueig.



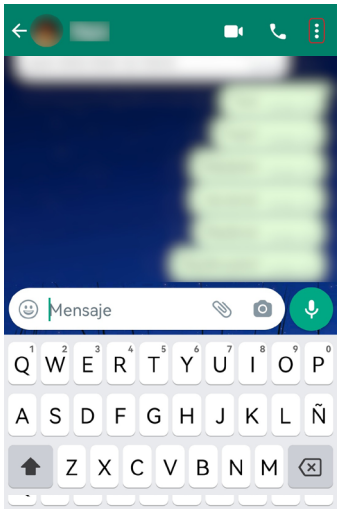
Font: Autoria pròpia.

WhatsApp

WhatsApp és sens dubte una de les principals plataformes per comunicar-se a la xarxa i, per tant, fa que sigui un dels principals mitjos presents en situacions de ciberassetjament.

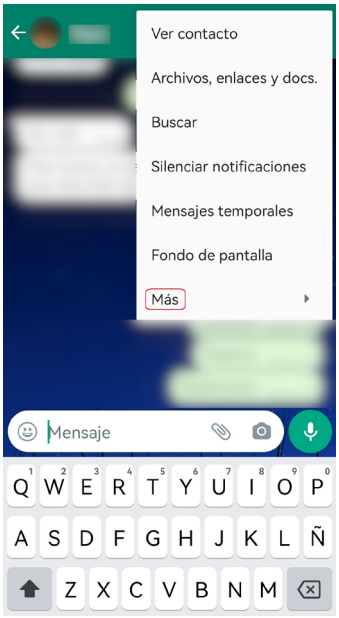
El procediment per bloquejar a un contacte en WhatsApp és el següent:

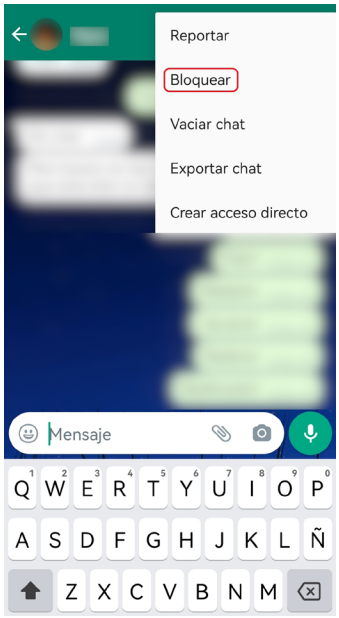
1 | Obrir el xat amb el contacte i seleccionar els tres punts:



Font: Autoria pròpia.

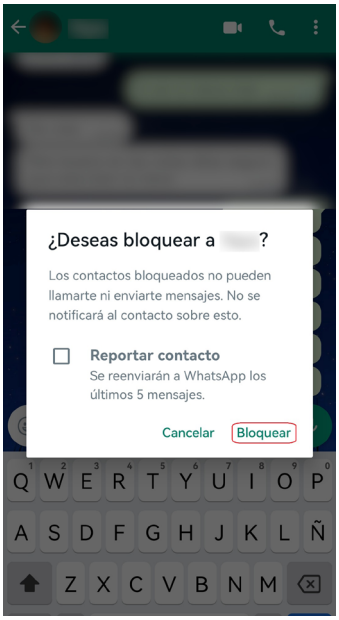
2 | Al menú emergent fer clic en **Més** i, posteriorment, a **Bloquejar**.

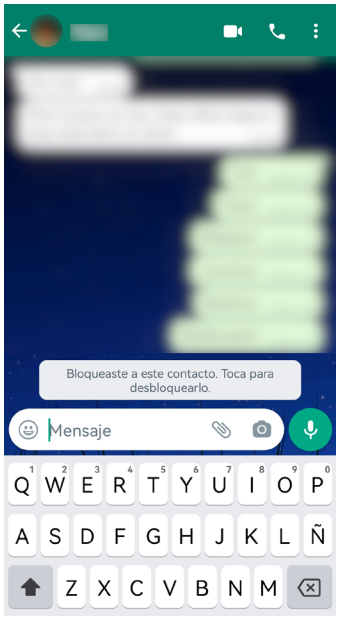




Font: Autoria pròpia.

3 | Confirmar l'acció.



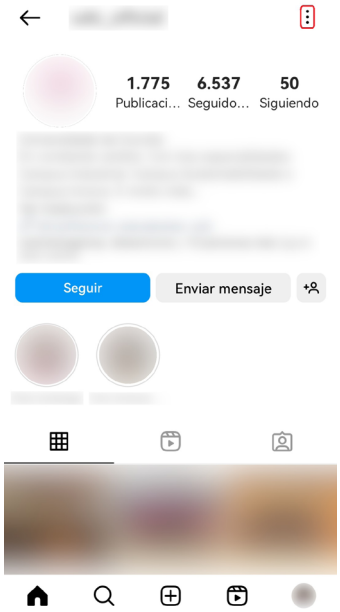


Font: Autoria pròpia.

Instagram

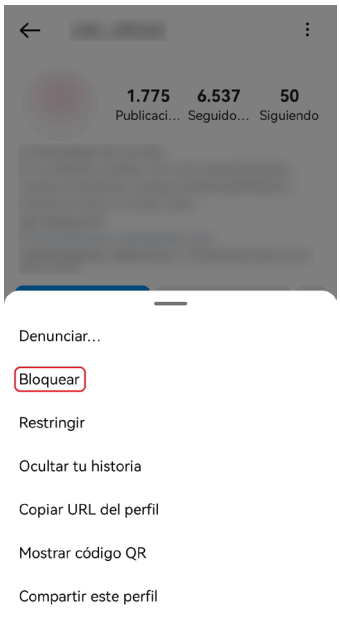
Instagram és una altra de les xarxes socials més utilitzades en el món. Els passos a seguir per bloquejar a un perfil d'aquesta xarxa són molt similars a la resta de plataformes vistes. A continuació, es detalla el procés que s'ha de dur a terme:

1 | Localitzar el perfil de l'usuari i seleccionar els tres punts:



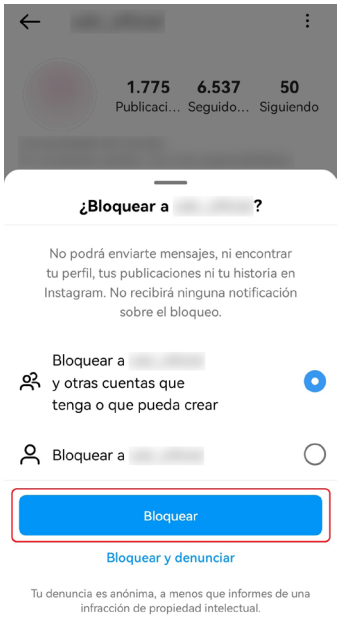
Font: Autoria pròpia

2 | Fer clic a l'opció Bloquejar.



Font: Autoria pròpia.

3 | Seleccionar si es vol bloquejar tots els perfils pertanyents a l'usuari o que pugui crear en el futur, o bloquejar únicament el perfil seleccionat. Finalment, fer clic a Bloquejar.



Font: Autoria pròpia.

NOTA

La majoria de les xarxes socials, a més de permetre bloquejar usuaris, també solen comptar amb l'opció de denunciar al mateix en la plataforma. D'aquesta manera, els administradors de la xarxa social investigaran el succeït i podrien prendre mesures com la suspensió del compte denunciat, entre altres accions.

DigitAll

Seguretat

4.4
PROTECCIÓ DEL MEDI AMBIENT

Seguretat

Nivell C1 4.4 Protecció del medi ambient

Big Data i tecnologies digitals per a la sostenibilitat ambiental

Big Data i tecnologies digitals per a la sostenibilitat ambiental

En aquest document desenvoluparem el glossari de termes i ampliar conceptes relacionats amb les aplicacions de les tecnologies digitals i el *big data* en referència a l'eficiència energètica i sostenibilitat que s'han inclòs en els vídeos del nivell.

Com hem vist en el vídeo **A4C44C1V02 "Tecnologies digitals, *big data* i sostenibilitat ambiental"** relacionat amb el *big data* en aquest nivell, titulat també "Tecnologies digitals, Big Data i sostenibilitat ambiental" actualment ens enfrontam a reptes molt importants relacionats amb la situació ambiental del planeta. Reptes que ens afecten en tots els aspectes de la nostra vida diària i que hem de modificar per poder adaptar-nos als canvis esdevenidors.

TECNOLOGIES DIGITALS, BIG DATA I SOSTENIBILITAT AMBIENTAL

Aplicacions ambientals de l'anàlisi del flux de dades provinents de l'ocupació massiva de les tecnologies digitals que contribueixen a millorar l'eficiència energètica i apostar per la sostenibilitat.

e.digitall.org.es/A4C44C1V02

Per això, els governs i empreses privades, conscients del moment decisiu en què ens trobam, han començat a desenvolupar polítiques per fer front a aquests reptes i protegir i conservar els recursos naturals mantenint el respecte pel medi ambient. Per al desenvolupament d'aquestes polítiques, utilitzen els resultats de l'ús d'eines tan eficaces com l'anàlisi del *big data*, que s'ha convertit en una eina fonamental per a la presa de decisions, la qual analitza l'èxit o fracàs de mesures o coneixent l'opinió de la població.

Cada dia es generen a tot el món milions de dades digitals que, o bé l'administració, o bé les empreses emmagatzemen per al seu posterior ús.

ATENCIÓ

La varietat d'aquestes dades és tan àmplia que abasten des de tots els aspectes de l'activitat humana fins als registres naturals que es donen en totes les àrees del planeta. Aquesta acumulació, processament, estudi i ús de dades a gran escala es denomina *big data*. Quan s'utilitzen aquestes dades per a la gestió ambiental i el desenvolupament sostenible, es parla llavors de Sustainable Data o Dades sostenibles.

Origen del Big Data

TECNOLOGIES DIGITALS, BIG DATA I SOSTENIBILITAT AMBIENTAL

e.digitall.org.es/A4C44C1V02

Com es comenta en el vídeo **"Tecnologies digitals, Big data i Sostenibilitat Ambiental"** d'aquest nivell, en parlar del big data sorgeixen diverses preguntes com què és?, com s'origina?, i per a què serveix?

Big Data, què és?

El Big Data són moltíssimes dades recollides en "brut" que es processen amb programes informàtics específics per obtenir informació que pugui ajudar sectors concrets. Big data com s'origina?

Big Data, s'origina?

Aquesta quantitat d'informació pot ser recopilada de diverses formes. Poden ser imatges de satèl·lits, estacions meteorològiques, dispositius mòbils, sensors de temperatura, sensors d'humitat, sensors de lluminositat o fins i tot es poden obtenir de xarxes socials (Facebook, Instagram, TikTok, etc.) o bases de dades públiques. Podríem resumir que les principals fonts de big data són:

1 | **Produïts per persones.** Una gran font d'informació de primera mà i que es considera de molt bona qualitat, són les xarxes socials. Aquestes xarxes recopilen dades, opinions, reaccions a continguts i, fins i tot, imatges dels mateixos usuaris sobre aspectes que puguin interessar a governs i empreses. Per exemple, enviar un correu, escriure un comentari en Facebook, contestar a una enquesta telefònica, ficar informació en un full de càlcul, respondre a un WhatsApp, agafar les dades de contacte d'un client, fer clic en un enllaç d'Internet, etc. Infinitat d'accions que fem en el dia a dia suposen una font de dades immensa.

NOTA

Un exemple de l'envergadura del big data són les dades que es generen de les xarxes socials per part dels usuaris: Google processa més de 3,5 mil milions de consultes de cerca tots els dies, cada dia es carreguen 350 milions de fotos en Facebook, tots els dies s'envien 306,4 mil milions de correus electrònics i es fan 5 milions de piulades.

2 | Generats per l'intercanvi d'informació entre màquines. A més de la interconnexió entre persones, les màquines també estan interconnectades i comparteixen dades directament, en el que es coneix com a M2M, que ve de l'anglès «*machine to machine*». Així, sistemes de control de temperatura, parquímetres, sistemes de reg automàtic de jardins, GPS de vehicles i telèfons mòbils, màquines expenedores de tota mena situades en centres públics i privats, o comptadors d'electricitat dels habitatges, entre molts altres sistemes controlats per màquines, es comuniquen a través de dispositius amb altres sistemes, als quals transmeten les dades que van recollint. Tots utilitzen mètodes de comunicació per dur a terme la interconnexió com a wifi, ADSL, fibra òptica o Bluetooth.

3 | Biomètriques. Són dades que provenen de sensors d'ús en la vida diària per a accés a recintes o que duim posats (de l'anglès *weareables*), alguns exemples són sensors d'empremtes dactilars de telèfon mòbils, escàners de retina, lectors d'ADN, sensors de reconeixement facial o reconeixement de veu, polseres d'activitat, pulsòmetres, etc. El seu ús està molt estès en matèria de seguretat en totes les seves variants (privada, corporativa, militar, policíaca, de serveis d'intel·ligència, etc.) i també en la tecnologia esportiva i mèdica.

4 | Màrqueting web. L'augment del comerç electrònic i els portals de venda en línia fa que els nostres moviments en la xarxa estiguin subjectes a tota mena de mesuraments que tenen com a objecte estudis de màrqueting i anàlisi de comportament. Per exemple, quan es fan mapes de calor basats en el rastreig del moviment del cursor per part dels usuaris d'un web, en la detecció de la posició de la pàgina, o en el seguiment de desplaçament vertical al llarg d'aquesta. Amb aquestes dades s'arriba a conclusions com ara quines parts d'una pàgina atreuen més l'usuari, o quins productes són els que més li interessen (seran aquells on se situïn els productes sobre els quals fa clic o a quina zona passa més temps).

5 | **Transaccions de dades.** De la mateixa manera que ha augmentat el comerç electrònic, els traspassos de doblers d'un compte bancari a una altra, la reserva d'un bitllet d'avió o afegir un article a un carret de compra virtual d'un portal de comerç electrònic, serien alguns exemples.

Big Data, per a què serveix?

Una de les preguntes que més es fa avui dia, sobretot tenint en compte que per al públic en general aquest concepte és bastant nou, és la utilitat o els beneficis que aporta el big data. Existeixen moltes utilitats i beneficis, entre les quals destaquen:

1 | **Reduir els costos de producció i optimitzar recursos.** Les grans tecnologies de dades i l'anàlisi basada al núvol aporten importants avantatges en termes de costos quan es tracta d'emmagatzemar grans quantitats de dades i identificar maneres més eficients de gestionar recursos per dedicar-los a les activitats que donaran millor rendiment o benefici, sigui econòmic, social o tecnològic.

2 | **Detectar el comportament fraudulent o opinions sobre accions que s'han dut a terme.** Quan els governs o empreses prenen mesures o llancen productes, utilitzen el big data per a sondejar el resultat d'aquestes accions. Aquestes dades analitzades i estructurades donen molta informació per a modificar, millorar o cancel·lar la continuació d'aquestes accions.

3 | **Prendre decisions intel·ligents i disminuir-ne el temps.** La velocitat de l'anàlisi, barrejada amb la capacitat d'examinar noves fonts de dades, fa que les organitzacions puguin prendre decisions basades en el que han après.

4 | **Determinar les causes d'origen de fallades**, problemes i defectes gairebé en temps real.

5 | **Desenvolupar nous productes.** Amb la capacitat d'avaluar les necessitats dels clients i la seva satisfacció, ve el poder de donar-los el que volen. Això significa que és possible crear nous ítems per donar resposta a aquests requeriments.

6 | **Optimitzar les ofertes.** El big data permet predir com es comportaran els compradors en el futur en funció dels seus comportaments anteriors, per la qual cosa es poden establir ofertes d'un mode fonamentat i estalviar diners.

7 | Generar cupons per als clients en el punt de venda basats en els seus hàbits de compra.

8 | Tenir més coneixement del mercat.

9 | Seguiment de la competència. Les macrodades proporcionen una major comprensió de la competència i poder anticipar-s'hi.

10 | Informació en temps real. La informació antiquada no té valor aplicable en el present i menys en el futur, per això la recopilació de dades de manera diària que proporciona aquesta tecnologia permet disposar d'una retroacció gairebé en el moment.

Tipus de big data

Estructurats

Qualsevol data que es pugui emmagatzemar, accedir i processar en format fix rep el nom de data «estructurada». Són els que tradicionalment s'han usat en el tractament de dades. Les seves característiques principals són que es puguin emmagatzemar en taules i tenen una clara definició de longitud i format.

S'hi troben els números, cadenes de caràcters i les dades. Encara que hi hagi altres tipus de dades que contenguin més informació, no significa que aquests no tenguin importància. No obstant això, avui dia, existeixen problemes quant a la grandària d'aquestes dades, ja que creixen en gran manera, arribant a dimensions típiques del rang de múltiples zettabytes.

No estructurats

Són qualsevol dada desconeguda o l'estructura de la qual es classifica com una data no estructurada. A més de ser enormes en grandària, les dades no estructurades plantegen múltiples desafiaments respecte del seu processament per derivar-ne valor.

Es tracten de dades en la seva forma original, tal com van ser recollides. No posseeixen un format específic que permeti emmagatzemar-les de manera tradicional, perquè no es

pot desglossar la informació que faciliten a tipus de dades definides en longitud i format. Entre aquests formats són comuns, per exemple, els correus electrònics, les presentacions multimèdia com els PowerPoint, documents de processadors de textos o els arxius en format PDF.

Un exemple típic de dades no estructurades són les fonts de dades heterogènies que contenen una combinació d'arxius de text simples, imatges, vídeos, entre altres.

En l'actualitat, les organitzacions compten amb una gran quantitat de dades disponibles. Però, desafortunadament, no saben com derivar-ne valor perquè aquestes dades es troben en la seva forma crua o format no estructurat.

Semiestructurats

Les dades semiestructurades poden contenir tots dos tipus de dades. Solen tenir un format que es pot definir, però l'usuari no el pot comprendre fàcilment i requereix l'ús de regles complexes que ajudin a determinar com llegir cada peça de la informació. Un exemple d'una dada semiestructurat és una dada representada en un arxiu XML.

Segueixen una espècie d'estructura, però aquesta no és prou regular per gestionar-la com a dades estructurades. Té uns certs patrons comuns que els descriuen i donen informació sobre les relacions entre aquests. Com a exemple, l'HTML, llenguatge per a l'elaboració de pàgines web, on el seu sistema d'etiquetes permet detectar aquestes pautes comunes.

Exemples d'ús

A més dels exemples mostrats en el vídeo **A4C44C1V02 "Tecnologies digitals, big data i sostenibilitat ambiental"** sobre aquest tema, existeixen molts més exemples d'ús del big data per a la sostenibilitat, com per exemple el projecte de la companyia leonardo (*leonardo.com*). Aquesta companyia està desenvolupant diferents projectes basats en el big data utilitzant informació de satèl·lits.

Entre diversos projectes, destaquen l'ús d'imatges satel·litàries que processen amb potents algorismes per ajudar a aconseguir els Objectius de Desenvolupament Sostenible (ODS) de l'Agenda 2030 de l'ONU, com la gestió sostenible del

TECNOLOGIES DIGITALS, BIG DATA I SOSTENIBILITAT AMBIENTAL

e.digitall.org.es/A4C44C1V02

sòl, els recursos hídrics, els boscos i les ciutats. Els satèl·lits fan una contribució molt important, ja que, a través d'un únic punt d'observació, ofereixen una mesura de les variables i fenòmens que volem observar, és a dir, globals, objectives i traslladables d'un punt a un altre del planeta, per correlacionar-los amb indicadors de sostenibilitat.

Saber-ne més

- e.digitall.org.es/sustainable-data
- e.digitall.org.es/un-bigdata
- e.digitall.org.es/master-bigdata
- e.digitall.org.es/data-catalog
- e.digitall.org.es/fao
- e.digitall.org.es/bigdata-analysis
- lifeunderyourfeet.org
- e.digitall.org.es/bangladesh
- e.digitall.org.es/postgrado-bigdata
- e.digitall.org.es/youtube-bigdata

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