ACTIC NIVELL 1

AC4_Seguretat, benestar i civisme



Barcelona

Barcelona Activa



Sobre Barcelona Activa

Barcelona Activa és l'agència de desenvolupament econòmic local de Barcelona. Fundada el 1987, és una societat mercantil pública integrada a l'àrea d'Economia i Promoció Econòmica de l'Ajuntament de Barcelona.

55.000
persones ateses

7.000
empreses ateses

Missió

Promoure l'ocupació de qualitat, l'esperit emprenedor, la competitivitat empresarial i la diversificació del teixit productiu, per assolir un model econòmic sostenible, inclusiu i just.

Visió

Fer de Barcelona una ciutat de referència per treballar, emprendre i viure amb valors socials i ambientals.

Valors

Ens mou l'esperit de servei públic i l'ètica professional i personal, així com la igualtat d'oportunitats i el progrés social. Treballem en cooperació dins l'organització i amb altres per a una economia social i sostenible al servei de les persones.

Segueix-nos a:

Què fem?

Acompanyem la ciutadania durant tot el procés de recerca de feina.

barcelonactiva.cat/treball

Donem suport a les persones emprenedores per convertir la seva idea de negoci en una empresa viable.

barcelonactiva.cat/emprenedoria

Ajudem les empreses i organitzacions a créixer, connectar-se amb l'ecosistema i fer-se més competitives.

barcelonactiva.cat/empreses

Oferim formació a les persones que cerquen feina, emprenedores i professionals.

barcelonactiva.cat/formació



Xarxa d'equipaments de Barcelona Activa



Seu Central

Oficines de Barcelona Activa.



Centre d'Emprenedoria

L'equipament dels emprenedors i les emprenedores de la ciutat.



Cibernàrium Nou Barris

Centre de formació digital d'iniciació ubicat al Parc Tecnològic.



Porta22

2.000 m^2 per a l'ocupació i la carrera professional.



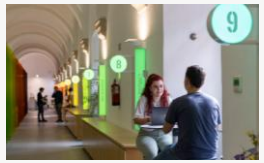
Startup Lab

L'equipament de les empreses innovadores de nova creació.



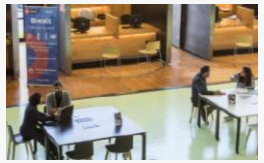
Parc Tecnològic

Clúster d'innovació al nord de la ciutat.



El Convent

L'equipament referent en ocupació per a joves, a Ciutat Vella.



Oficina d'Atenció a les Empreses

L'espai de referència per a les empreses i pimes de Barcelona.



LIDERA

Espai per a dones professionals, directives i emprenedores.



InnoBA

Centre per a la innovació socioeconòmica, a Ca n'Andalet.



Cibernàrium 22@

Centre de capacitació tecnològica per a professionals i empreses.

Espais Activa a la ciutat

- Nou Barris Activa
- Sant Andreu Activa
- Sants-Montjuïc Activa

Barcelona Activa està present a més de 50 punts de la ciutat

Equipaments de Barcelona Activa

1. Seu Central
2. Porta22
3. El Convent
4. Centre d'Emprenedoria
5. Startup Lab
6. LIDERA
7. Cibernàrium 22@
8. Cibernàrium Nou Barris
9. Oficina d'Atenció a les Empreses
10. Parc Tecnològic
11. InnoBA

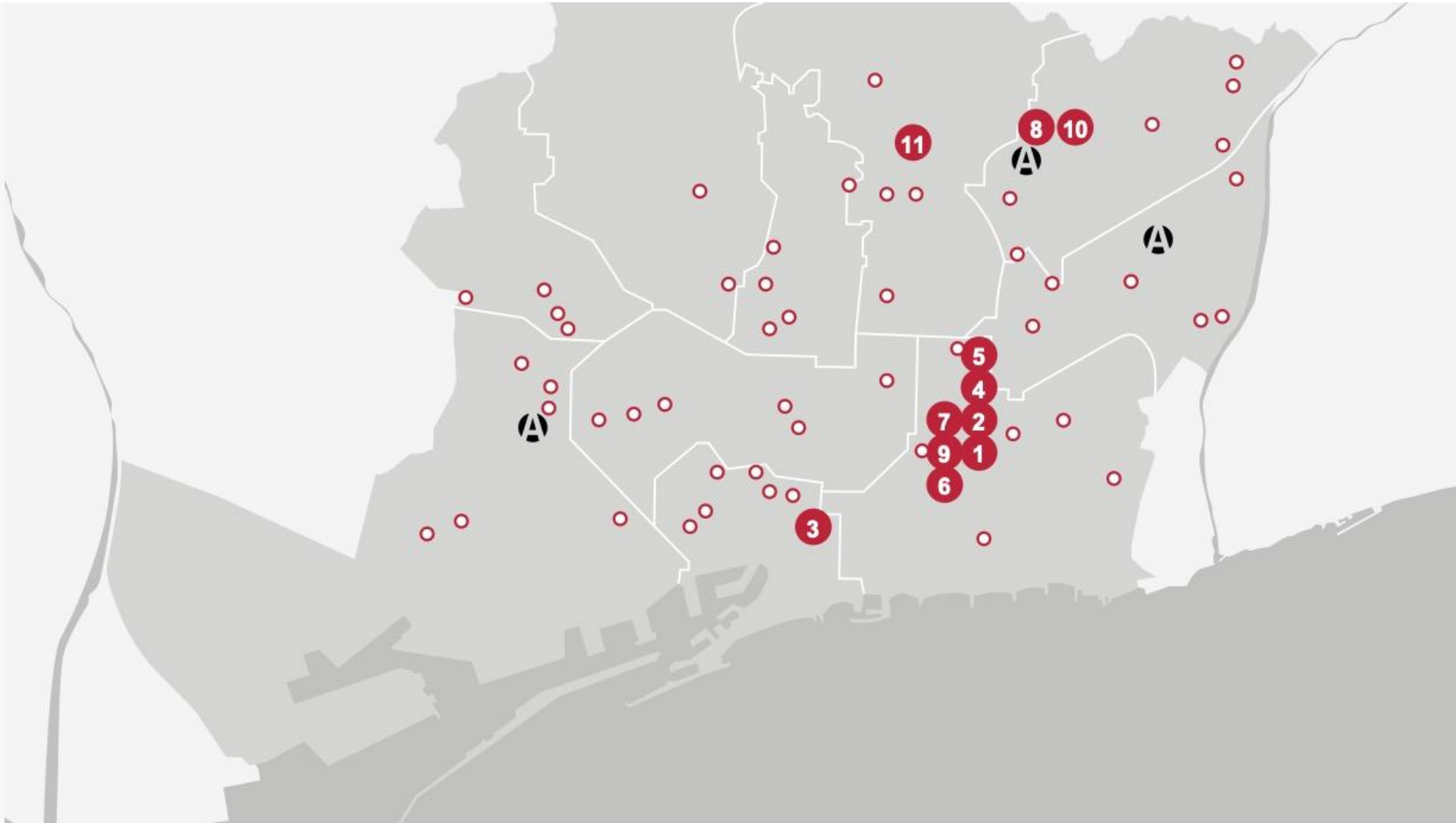
Espais Activa a la ciutat

Nou Barris Activa

Sant Andreu Activa

Sants-Montjuïc Activa

Altres punts d'atenció a la ciutat



Xarxa Cibernàrium

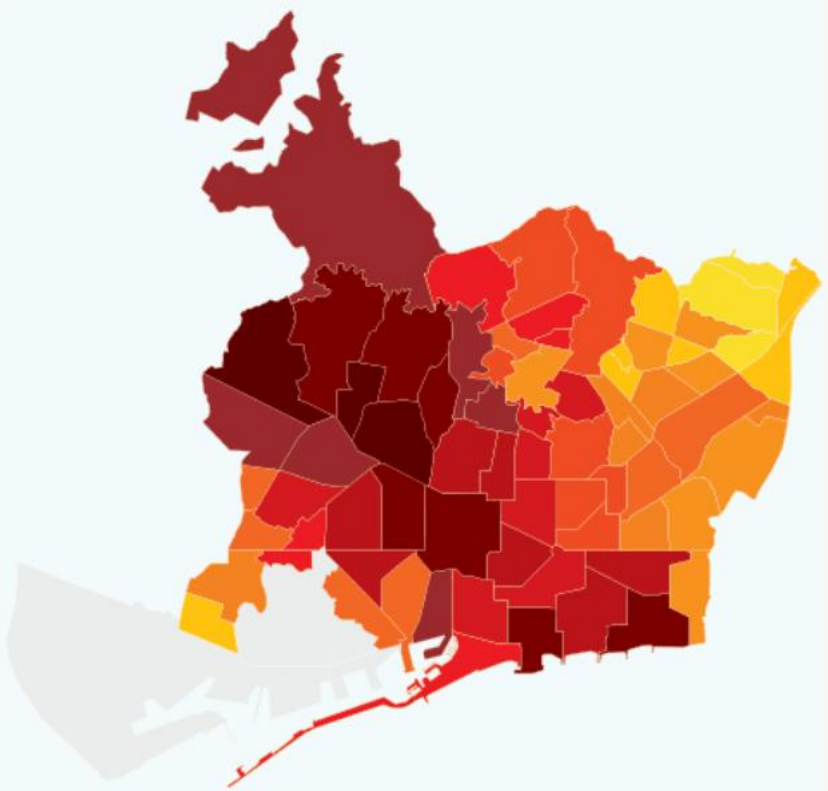
La Xarxa Cibernàrium està distribuïda per tota la ciutat de Barcelona, oferint formació en diversos equipaments.

Recorda que també et pots formar en línia des de casa, amb Aules Virtuals.

Consulta les activitats que pots realitzar als diferents equipaments:

- Activitats a BIBLIOTEQUES
- Activitats a CIBERNÀRIUM NOU BARRIS
- Activitats a CANÒDROM
- Activitats a PLAÇA CATALUNYA (Movistar Centre)
- Activitats a SANTS-MONTJUÏC ACTIVA

On estem?



Formació tecnològica per a tothom

Test de Competències digitals

1

FORMACIÓ TIC BÁSICA
2-4 hores

Test de Competències digitals

2

FORMACIÓ TIC ESPECIALITZADA
2-24 hores

3

FORMACIÓ TIC AVANÇADA
Reskilling (350h)
Upskilling (50-150h)

Presencial

Tallers dirigits
Cibernàrium Nou Barris
Biblioteques BCN
Canòdrom
Plaça Catalunya
(Movistar centre)
Sants Montjuic Activa

Coaching Digital

Cibernàrium 22@

Virtual

Aules Virtuals

VideoCàpsules

Suport Tic

Campus Virtual, Masterclass, online...



Índex

AC4. Seguretat, benestar i civisme

1. Protegeix sistemes, dispositius i continguts digitals.
2. Protegeix dades personals i la seva privacitat.
3. Protegeix la salut, el benestar i l'entorn.
4. Gestiona la identitat i perfils digitals.
5. Actua cívicament en l'entorn digital.

ACTIC NIVELL 1
Competència

Protegeix sistemes, dispositius i continguts digitals

Sessió 1



Índex

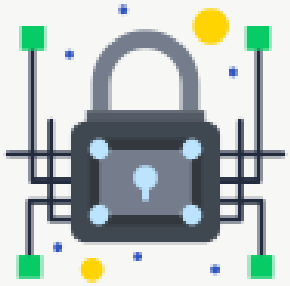
Protegeix sistemes, dispositius i continguts digitals

1. Riscos associats a l'ús de dispositius digitals
2. Mesures de protecció i seguretat digital
3. Prevenció del programari maliciós
4. Còpies de seguretat i recuperació de dades
5. Actualització de sistemes i aplicacions

1. Riscos associats a l'ús de dispositius digitals

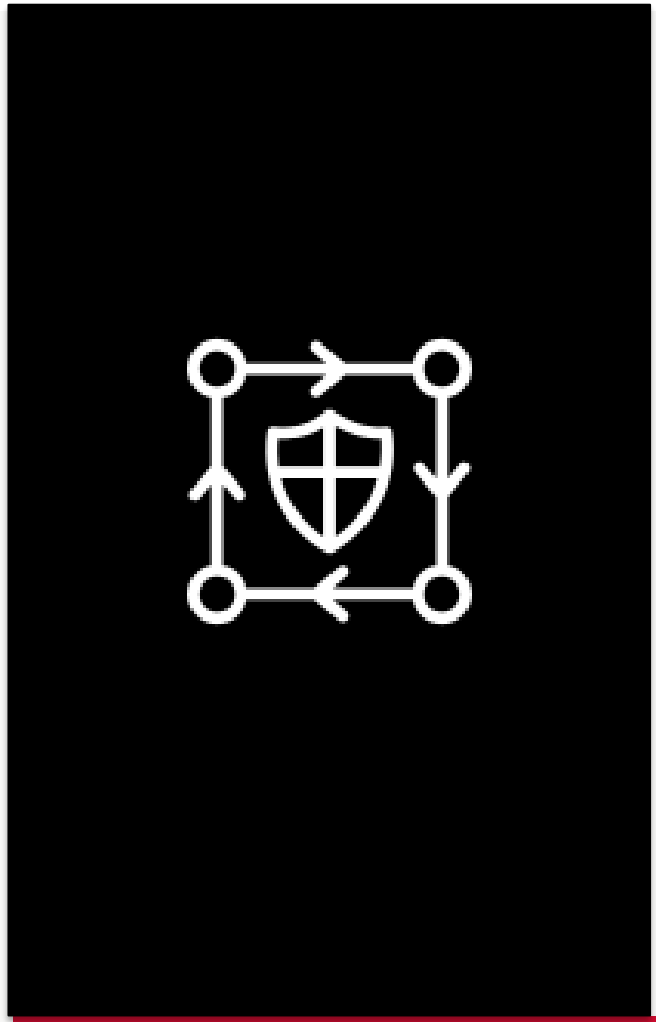
Prendre consciència dels riscos digitals

La seguretat absoluta a Internet no existeix, però **el risc es redueix dràsticament quan l'usuari deixa de ser passiu i pren les regnes de la seva protecció**. La seguretat digital és una combinació equilibrada entre les eines de programari utilitzades i el comportament de l'usuari.



Què és la ciberseguretat?

La ciberseguretat és el conjunt de pràctiques, tecnologies i mesures dissenyades per protegir els nostres sistemes, xarxes, dispositius i dades privades davant d'atacs digitals, accessos no autoritzats o pèrdues accidentals.



1. Riscos associats a l'ús de dispositius digitals



Les tres ciberamenaces principals

- **Phishing**: engany mitjançant el qual els cibercriminals es fan passar per una entitat de confiança (el teu banc, Correus, la Seguretat Social o la Generalitat) a través d'un correu electrònic, SMS o trucada. El que busquen generalment és que cliquis en un enllaç fals i introdueixis les teves contrasenyes o dades de la targeta de crèdit.

- **Programari maliciós** (*Malware*): qualsevol codi o aplicació informàtica dissenyada intencionadament per danyar un dispositiu, robar informació, espiar l'usuari o prendre el control del sistema (inclou virus, troians, espions, etc.).

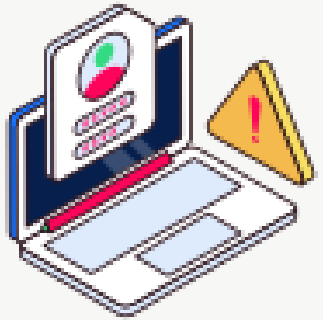
- **Suplantació d'identitat**: acció de fer-se passar per una altra persona a les xarxes socials, xats o correus electrònics per cometre estafes, danyar la seva reputació o obtenir informació confidencial dels seus contactes.

1. Riscos associats a l'ús de dispositius digitals



El factor humà: la clau de la seguretat

Un antivirus instal·lat no serveix de res si l'usuari clica voluntàriament un enllaç fraudulent o deixa la seva contrasenya apuntada en un post-it. Has d'assumir que **la seguretat depèn de les teves accions diàries**. Els hàbits més eficaços són:



- Bloquejar sempre la pantalla en separar-se de l'equip.
- Fer servir contrasenyes robustes que ningú pugui endevinar.
- Desconfiar de missatges alarmants o ofertes massa bones per ser veritat.

2. Mesures de protecció i seguretat digital

Per impedir que qualsevol persona física o digital accedeixi a la teva informació, cal configurar correctament les barreres d'accés del propi dispositiu.

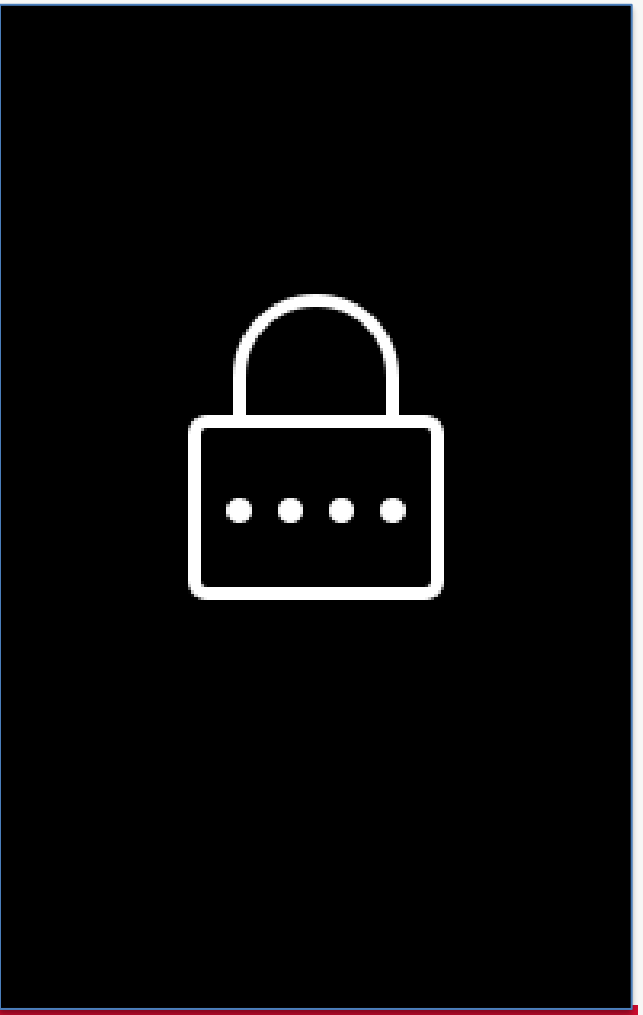
El bloqueig de pantalla

És la primera línia de defensa física. Impedeix que si perds el mòbil o si et separes de l'ordinador, algú pugui xafardejar. Els mètodes principals són:

- Mètodes biomètrics: empremta dactilar i reconeixement facial (Face ID). Són els més segurs i còmodes.
- Mètodes de codi: PIN numèric (mínim 4 dígits) o patró de dibuix (menys segur, ja que la marca que deixa el rastre del dit a la pantalla es pot veure a contrallum).



2. Mesures de protecció i seguretat digital



Creació de contrasenyes fortes i robustes

És crucial **distingir una contrasenya feble d'una de segura**.

Regla d'or d'una contrasenya robusta: ha de tenir com a mínim **8 caràcters** (millor 12 o més) i ha de **combinar quatre elements**:

I. lletres majúscules
II. lletres minúscules
III. números
IV. símbols especials (com `@`, `#`, `$`, `*`).

Exemples de contrasenya FEBLE (Incorrecta): `123456`, `barcelona`, `pere1985` (són fàcilment atacables per programes endevinadors).

Exemple de contrasenya ROBUSTA (Correcta):`Blau2026#Gat` (combina tots els elements requerits i és llarga).

2. Mesures de protecció i seguretat digital

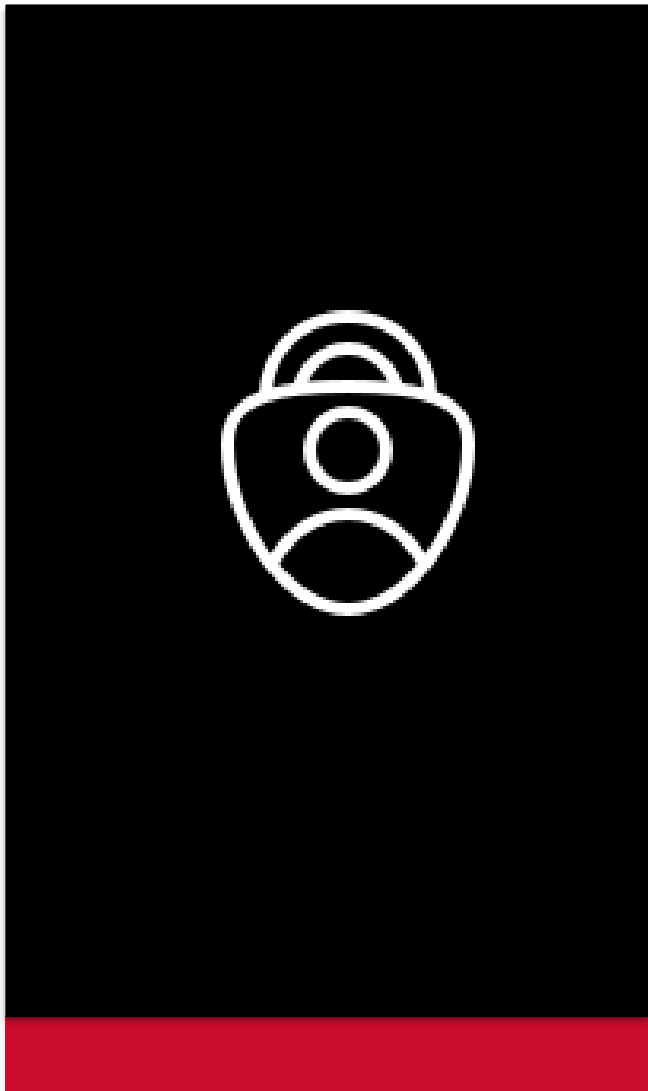
L'Autenticació Multifactor (MFA / 2FA)

Aquest és un dels conceptes tècnics més importants de la seguretat moderna. L'autenticació de doble factor afegeix una capa extra de protecció.

Quan entres al teu correu o compte bancari, no és suficient amb introduir el teu usuari i contrasenya. El sistema et demana una segona comprovació abans de deixar-te entrar, com ara:

- Un codi numèric temporal rebut per SMS al teu mòbil.
- Una notificació instantània dins d'una aplicació d'autenticació (com Google Authenticator o Microsoft Authenticator).
- La confirmació de la teva empremta digital al telèfon mòbil.

D'aquesta manera, encara que un cibercriminal et robi la contrasenya a través d'Internet, no podrà entrar al teu compte perquè no tindrà el teu mòbil físic per fer el segon pas.



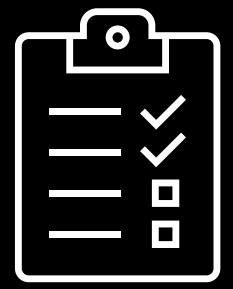
2. Mesures de protecció i seguretat digital

Exercici: **Cas pràctic**

L'Àlex fa servir el seu telèfon mòbil per a tot, però sempre va amb presa. Avui s'ha assegut a una cafeteria pública i ha fet el següent:

1. S'ha connectat directament al Wi-Fi obert i sense contrasenya de la cafeteria per estalviar les seves dades mòbils, i ha aprofitat per entrar al web del seu banc a fer una transferència.
2. No té posat cap codi PIN, patró ni empremta d'accés a la pantalla d'inici del mòbil perquè diu que "és una pèrdua de temps haver de desbloquejar-lo cada vegada".
3. Fa més d'un any que li surt un avís al mòbil dient que hi ha una actualització del sistema operatiu (Android/iOS) pendent, però sempre prem "Recorda-m'ho més tard" perquè no vol que el mòbil s'hagi de reiniciar.
4. Utilitza la mateixa contrasenya (Alex2022!) per al seu correu electrònic, per al compte d'Instagram i per a la botiga en línia on compra roba.

Quines accions correctives li recomanaries?



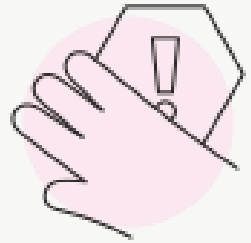
3. Prevenció del programari maliciós

Prevenció i eliminació de programari maliciós (Malware)

El **programari maliciós** pot entrar al teu dispositiu de moltes maneres silencioses, especialment a través de descàrregues o enllaços de correus brossa.

Com podem evitar-ho?

- **Antivirus o programari de seguretat**
- **Hàbits preventius digitals**



3. Prevenció del programari maliciós

Ús de l'antivirus o programari de seguretat

Un **antivirus** és un programa que monitoritza constantment el sistema per detectar, blocar i eliminar fitxers perillosos. Com a mínim cal saber fer anar les seves opcions bàsiques:

- Anàlisi del sistema (Scan): acció d'escanejar el disc dur per buscar amenaces amagades. Es recomana fer anàlisis completes de forma periòdica.
- Quarantena: quan l'antivirus detecta un fitxer sospitós però no el pot eliminar immediatament sense danyar el sistema, l'aïlla en una zona segura ("la quarantena") on el fitxer queda totalment bloquejat i no pot infectar la resta de l'ordinador.
- Eliminació: esborrat definitiu de l'amenaça un cop detectada i neutralitzada.



3. Prevenció del programari maliciós



Hàbits preventius digitals

L'antivirus és una xarxa de seguretat, però la millor prevenció és el teu comportament. Per evitar infeccions per **malware**:

Evita enllaços sospitosos: no cliquis mai en enllaços que vinguin de remitents desconeguts o que usin missatges alarmistes (com: "Compte bloquejat, clica aquí de forma urgent").

Para atenció als adjunts: no descarreguis ni obris mai arxius adjunts de correus estranys, especialment si tenen extensions executives o perilloses com .exe, .bat, .vbs, o documents de Word que demanen "activar macros".

4. Còpies de seguretat i recuperació de dades

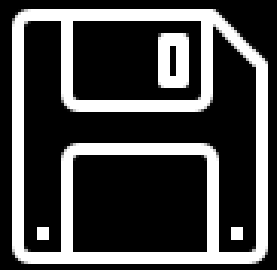


Davant d'un atac informàtic greu, d'un robatori del dispositiu o d'una avaria de maquinari, l'única manera de no perdre per sempre les teves fotografies, documents o feines és tenir una **còpia de seguretat** ben feta.

Diferència entre Còpia de Seguretat i Restauració

Còpia de seguretat (*Backup*): és el procés proactiu de duplicar els nostres fitxers importants i guardar aquesta còpia en un lloc diferent i independent del dispositiu original (per exemple, en un disc dur extern o al núvol com Google Drive, iCloud, OneDrive).

Restauració: és el procés d'agafar els fitxers d'aquella còpia de seguretat que hem realitzat prèviament i tornar-los a col·locar al mateix dispositiu (o a un de nou) després que l'equip original hagi patit un problema, un esborrat o una avaria.



4. Còpies de seguretat i recuperació de dades



Bones pràctiques per a la gestió de còpies

Periodicitat: la còpia s'ha de fer regularment segons les teves necessitats. Si treballes diàriament amb fitxers importants, la còpia s'hauria de fer cada dia. Si l'ús és esporàdic, pot ser setmanal o mensual.



Verificació obligatòria: un dels errors més comuns és confiar que la còpia s'ha fet sola. Després d'executar-se el procés, has de comprovar visualment que el fitxer de la còpia s'ha creat correctament, que ocupa espai i que té la data del dia.



La paperera de reciclatge: per a pèrdues menors accidentals, recorda que els sistemes disposen d'un pas intermedi: recuperar els elements eliminats directament des de la paperera abans que es buidi definitivament.



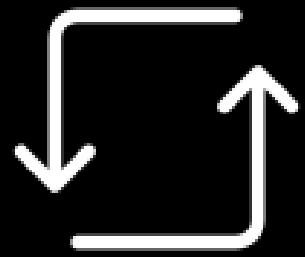
5. Actualització de sistemes i aplicacions

Per què són vitals les actualitzacions?

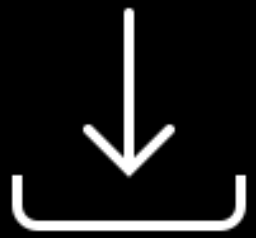
Els i sistemes operatius (Windows, Android, iOS) són complexos i sovint es descobreixen errors en el seu codi. Aquests errors s'anomenen **vulnerabilitats**.

Quan els fabricants (Microsoft, Apple, Google) s'adonen d'aquest error, publiquen immediatament una **actualització** de seguretat.

Els **cibercriminals** utilitzen aquestes vulnerabilitats o forats de seguretat per colar-se als ordinadors de la gent sense permís.



5. Actualització de sistemes i aplicacions



Com gestionar les actualitzacions?

Activar les actualitzacions automàtiques: sempre que el dispositiu ho permeti, s'ha d'activar aquesta funció. D'aquesta manera, l'ordinador o el mòbil descarregarà i instal·larà el complement de seguretat durant la nit o en moments d'inactivitat sense que tu te n'hagis de preocupar.

Comprovació manual: en cas de no tenir-les en automàtic, cal accedir periòdicament als paràmetres de configuració de l'equip (Windows Update, Actualització de programari en mòbils, o la Play Store / App Store per a les aplicacions) i prémer el botó "Buscar actualitzacions".

Exercicis

Cas Pràctic 1 (Identificació d'amenaces)

Plantejament

Reps un correu electrònic suposadament de la teva entitat bancària que et diu que el teu compte corrent s'ha bloquejat per motius de seguretat. El missatge conté un enllaç que et porta a una pàgina web on es demana que introdueixis el teu codi d'usuari i la teva contrasenya de banca digital. De quin tipus d'atac es tracta?

Resposta

Es tracta d'un cas clar de Phishing. L'entitat bancària mai utilitzarà enllaços externs d'urgència per demanar dades d'accés confidencials.



Exercicis



Cas Pràctic 2 (Procediment inclusiu i segur)

Plantejament

Vols protegir el teu nou compte de correu electrònic de la feina per evitar que si algú esbrina la teva contrasenya pugui llegir els teus missatges des d'un altre ordinador de la xarxa. Quina mesura de seguretat has d'activar?

Resposta

Has d'activar l'Autenticació Multifactor (MFA/2FA). D'aquesta manera, el sistema bloquejarà qualsevol intent d'entrada des d'un dispositiu nou fins que s'introdueixi el segon codi enviat al teu mòbil.

Exercicis

Cas Pràctic 3 (Hàbit correcte de còpia de seguretat)

Plantejament

Un usuari ha configurat el seu ordinador perquè cada divendres a les 20:00 es realitzi de manera automàtica una còpia de seguretat de tots els seus fitxers de feina en un disc dur extern. Quina acció posterior ha de realitzar per considerar el procés complet i segur?

Resposta

Dilluns al matí ha d'accedir al disc dur extern i verificar manualment que el fitxer de la còpia s'ha generat correctament, revisant-ne la mida i la data del fitxer de destí.



ACTIC NIVELL 1
Competència

Protegeix dades personals i la seva privacitat

Sessió 2



Índex

Protegeix dades personals i la seva privacitat

1. Dades personals en entorns digitals
2. Condicions d'ús i privacitat
3. Protecció de dades personals
4. Configuració de la privacitat digital
5. Seguretat en les transaccions electròniques
6. Detecció de la suplantació d'identitat

1. Dades personals en entorns digitals

Com es recullen i es generen les nostres dades?

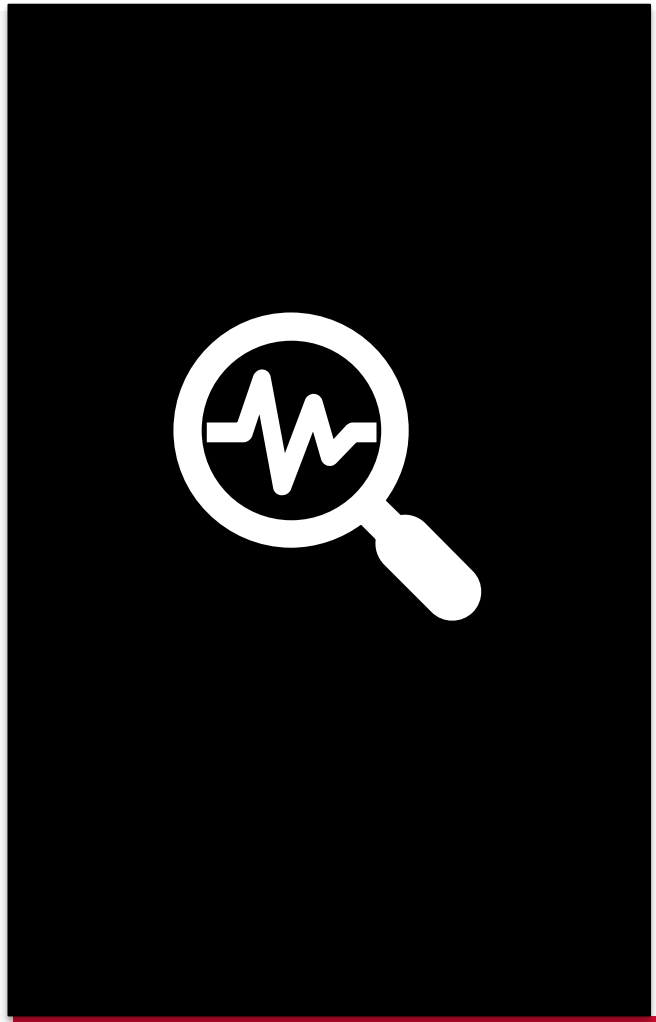
Les nostres dades s'alimenten contínuament a Internet a través de tres fonts principals:

- **Formularis de registre**: quan obrim un compte a una xarxa social o quan ens descarreguem una aplicació de cuina o comprem un bitllet de tren i introduïm l'adreça de correu, el telèfon o l'edat.
- **Ús d'aplicacions**: el programari recull metadades (dades ocultes), com ara les hores de connexió, el tipus de dispositiu que fem servir o els nostres hàbits de consum.
- **Navegació web**: a través de les *cookies* (petits arxius de text que els llocs web guarden al nostre navegador) es registra quines pàgines visitem, què mirem i quant de temps passem a cada lloc.

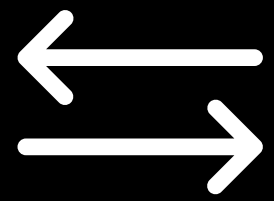


Què es consideren dades personal?

Les dades personals no són només el nostre nom i cognoms o el DNI. Dins d'Internet, qualsevol engruna d'informació que permeti identificar-nos directament o indirectament és una dada personal.



1. Dades personals en entorns digitals



Precaucions bàsiques abans de compartir les dades

Abans de prémer el botó "Enviar", és recomanable que apliquis el criteri de reflexió següent:

- **Principi de minimització:** has de valorar si les dades que et demanen són realment necessàries per al servei. Si una aplicació de llanterna et demana el número de telèfon o el correu electrònic, és un senyal d'alerta.

- **Evitar dades sensibles:** no proporcionis mai, si no és estrictament obligatori i en un entorn oficial (com Hisenda o Salut), dades considerades de nivell alt o sensibles (ideologia, religió, salut, orientació sexual o dades biomètriques).

- **Revisar amb qui es comparteixen:** comprova sempre qui és l'empresa o entitat que hi ha al darrere del web.

2. Condicions d'ús i privacitat



Elements bàsics d'una política de privacitat

Gairebé ningú llegeix els llargs contractes de "**Termes i condicions**", però és important que sàpigues extreure'n la informació essencial per decidir si acceptes o rebutges de manera informada. Quan obris un avís de privacitat, has d'aprendre a localitzar ràpidament **dos elements clau**:

Ús de les dades

Per a què faran servir la teva informació? S'utilitzarà només per enviar-te el producte a casa o es vendrà a empreses de publicitat externa?

Opcions de privacitat

Quines caselles pots desmarcar? Recorda que, per llei, l'acceptació de rebre publicitat o que es cedeixin les teves dades a tercers **ha de ser opcional** i no pot venir marcada per defecte.

2. Condicions d'ús i privacitat

El dret a la privacitat i les opcions de gestió

La normativa europea de protecció de dades (RGPD) reconeix que ets el propietari de les teves dades. Per tant, les plataformes digitals estan obligades a oferir-te eines de configuració per:

- **Modificar** les teves preferències de privacitat en qualsevol moment.
- **Sol·licitar canvis o l'eliminació** definitiva de les teves dades (el conegut com a Dret de Supressió o Dret a l'Oblit).



3. Protecció de dades personals



Riscos específics i el paper de la Intel·ligència Artificial (IA)

L'exposició de dades a Internet comporta riscos greus, especialment quan es tracta d'eines que analitzen el nostre comportament de manera automàtica.

Riscos directes
Compartir informació personal pot facilitar que ens creïn perfils falsos a les xarxes, que ens suplantin la identitat o que s'utilitzin les nostres fotos per a usos no previstos.

Sistemes automatitzats i IA
Molts serveis actuals utilitzen algorismes avançats i Intel·ligència Artificial per analitzar de manera automatitzada milers de dades teves (m'agrada, comentaris, cerques). L'objectiu és crear un perfil psicològic per personalitzar continguts, retenir-te més temps a la pantalla o mostrar-te publicitat altament dirigida per influir en les teves decisions de compra o vot.

3. Protecció de dades personals

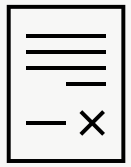
Protecció de menors i col·lectius vulnerables

El tractament de les dades d'aquests grups requereix un nivell de protecció excepcional, ja que tenen menys capacitat per detectar enganys.



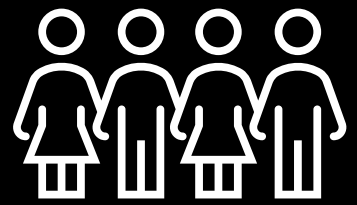
Mesures pràctiques

S'ha d'evitar taxativament difondre a Internet fotos de menors on se'ls pugui identificar, dades de la seva escola, horaris o ubicacions.

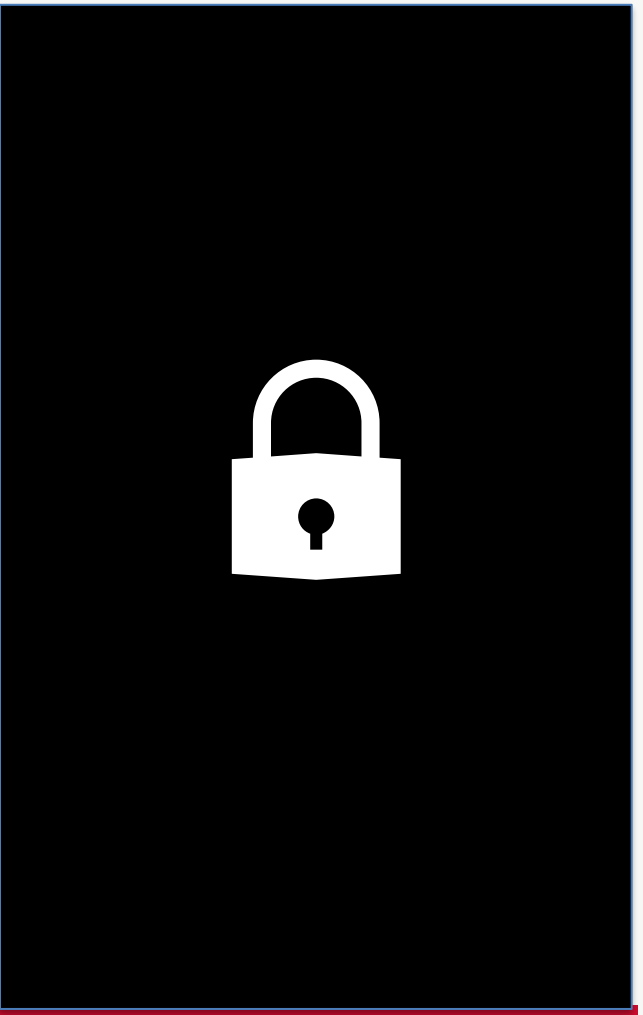


Consentiment i suport

Els menors d'edat (a Espanya, en general, els menors de 14 anys) no poden donar el seu consentiment digital de forma autònoma; necessiten obligatòriament el suport, supervisió i consentiment explícit dels seus pares o tutors legals.



4. Configuració de la privacitat digital



Configuració de permisos en aplicacions

Quan instal·les una aplicació al mòbil o un programa a l'ordinador, has de revisar els seus permisos des del menú de configuració del sistema:

Permisos d'accés

Controla si l'app té permís per usar la teva:

- Ubicació (GPS)
- Càmera
- Micròfon
- Llista de contactes.

Exemple: Si una aplicació de jocs et demana accés a la llista de contactes o a la càmera, denega el permís, ja que no afecta el seu funcionament bàsic i protegeix la teva privacitat.

Visibilitat del perfil

Configura les teves xarxes socials perquè el teu perfil o publicacions només siguin visibles per a "Amics" o "Contactes acceptats", evitant el mode "Públic“.

4. Configuració de la privacitat digital

Mesures per limitar el rastre digital

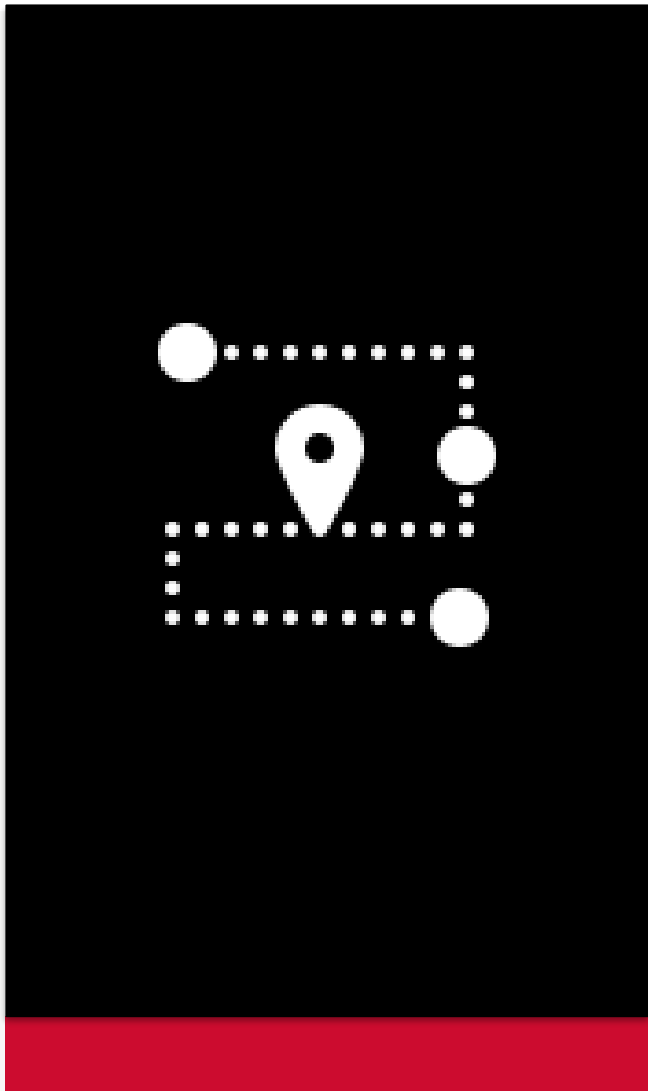
Per evitar que les empreses facin un seguiment complet de la teva navegació, pots aplicar accions molt senzilles:



- Eliminar l'historial de navegació: neteja regularment l'historial, la memòria cau (cache) i les cookies des de la configuració del teu navegador web (Chrome, Firefox, Edge, Safari).



- Limitar el seguiment: activa l'opció "No fer el seguiment" al navegador o utilitza el mode de navegació d'incògnit o privada quan no vulguis que es guardi historial al dispositiu local.



5. Seguretat en les transaccions electròniques



Indicadors bàsics de llocs web segurs

Comprar per Internet, fer transferències o pagar serveis en línia és molt segur si saps identificar els elements de protecció d'una passarel·la de pagament. Abans de posar el número de la teva targeta a un web, has de fer una **verificació visual** obligatòria:

El protocol HTTPS: revisa la barra de l'adreça del navegador. El web ha de començar per **https://** (la "s" final significa 'Segur'). Evita comprar en webs que només comencin per http://.



La icona del cadenat: Al costat esquerre de l'adreça web ha d'aparèixer una icona en forma de **cadenat tancat**. Si hi cliques, podràs veure el certificat digital que garanteix que la connexió està xifrada (les teves dades viatgen ocultes per la xarxa).



5. Seguretat en les transaccions electròniques

Mesures pràctiques durant la transacció

Verificació del lloc
Comprova que l'adreça del web estigui ben escrita (per exemple, https://www.amazon.com i no *https://www.amozon-ofertes.com*).

Revisió de l'import i destinatari
En el moment de confirmar el pagament (normalment quan el teu banc t'envia una notificació al mòbil), llegeix detingudament el missatge. Verifica que l'import i el nom de l'empresa coincideixen exactament amb el que estàs comprant.

Mai compartir codis
No facilitis mai a ningú per telèfon, xat o correu els codis de verificació de un sol ús (SMS o targeta de coordenades) que t'envia el banc.



6. Detecció de la suplantació d'identitat



Mètodes de manipulació més habituals

Els estafadors utilitzen la manipulació psicològica (coneguda com a enginyeria social) per enganyar-nos i fer que obrim les portes a dades confidencials. Juguen amb les nostres emocions a través dels missatges. Els ganxos més utilitzats són:

La urgència o la por

Per exemple, et diuen que tens el compte suspès i tens 24 hores per actuar.



L'autoritat

Es fan passar per un organisme oficial, inspectors d'hisenda o la policia.

El benefici o cobdícia

Un premi que no esperaves o un reemborsament de diners a favor teu.

6. Detecció de la suplantació d'identitat



Senyals típics d'alerta

Si reps un correu o SMS dubtós, busca aquests indicadors:

1. **Remitent sospitós**: l'adreça de correu que es mostra no correspon a l'oficial (per exemple: el correu diu ser de Correus, però l'adreça real de remitent és “correos-info32@gmail.com”).

2. **Enllaços o adjunts inesperats**: el missatge t'obliga a clicar un enllaç extern o a descarregar un fitxer adjunt no sol·licitat.

3. **Faltes d'ortografia o traduccions automàtiques estranyes:** molts d'aquests atacs es generen a l'estranger i usen traductors que cometen errors gramaticals evidents.

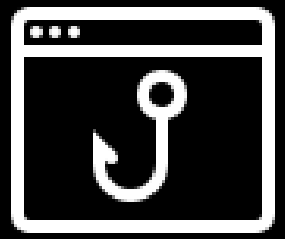


6. Detecció de la suplantació d'identitat

Protocol d'actuació segura

Davant de qualsevol sospita, has d'actuar seguint exactament aquests tres passos:

Què NO s'ha de fer	Què SÍ s'ha de fer
❌ No clicar en cap enllaç del missatge.	Verificar per un canal alternatiu: busca el telèfon oficial de l'entitat o entra a la seva aplicació oficial i comprova si l'avís és real.
❌ No descarregar cap fitxer adjunt.	Reportar o marcar com a spam: informa el teu proveïdor de correu que és un correu brossa.
❌ No respondre al missatge demanant explicacions.	🗑️ Eliminar el missatge definitivament de la paperera.



Exercicis pràctics

El Desxifrador de Clàusules i Drets RGPD

Llegiu aquest avís que us trobeu en instal·lar una aplicació de jocs gratuïta al mòbil:

"Accepto les condicions d'ús i la política de privacitat. Autoritzo a l'empresa i als seus socis comercials a utilitzar les meves dades de navegació, contactes i ubicació en segon pla per personalitzar anuncis publicitaris."

Responeu ràpidament amb la vostra parella:

1. Si només voleu jugar al joc sense que rastregin la vostra ubicació ni els vostres contactes, heu de marcar aquesta casella de forma obligatòria? Quin dret del RGPD us permet negar-vos-hi conservant el dret a fer servir el servei bàsic?

2. Imagina que ja t'has registrat, però ara vols que l'empresa esborri totes les teves dades del seu sistema per sempre. Quin dret de la normativa de protecció de dades (RGPD) has d'exercir de forma oficial? (Tria un d'aquests: Dret d'accés, Dret de rectificació o Dret a l'oblit/supressió).



Exercicis pràctics

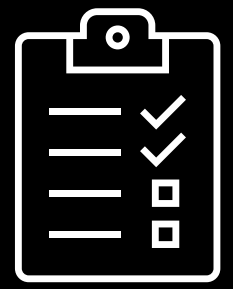
L'Auditor de Compres Express

Estàs a punt de comprar unes vambes en una botiga en línia nova que has descobert a Instagram. Analitza si és una compra segura o un risc (classifica-ho com a SEGURA 🟢 o PERILLOSA 🔴):

Cas A: A la barra d'adreces de la pàgina de pagament posa “http://vambesbarates.net” i no hi ha cap icona de cadenat al navegador. El mètode de pagament exclusiu és fer una transferència bancària directa a un número de compte privat d'un particular.

Cas B: L'adreça és “https://www.botigaoficial.cat” (té el cadenat tancat). En prémer "Pagar", s'obre una passarel·la de pagament segura (TPV virtual) que et demana el número de targeta, i acte seguit el teu banc t'envia un codi per SMS o una notificació a l'App del mòbil per autoritzar la transacció abans de cobrar-te-la (autenticació de doble factor/3D Secure).

Cas C: Una web té protocol https i un cadenat, però l'únic mètode de pagament admès és introduir el teu número de targeta directament en un formulari obert al mig de la pàgina web, sense redirigir-te a cap banc ni demanar-te cap codi de confirmació.



Exercicis pràctics

Que no et 'pesquin’

Reps aquest SMS al teu telèfon mòbil directament d'un remitent anomenat CORREOS-INFO:

"CORREOS: El seu paquet no s'ha pogut lliurar avui perquè falten pagar les taxes de duana (1,75€). Si us plau, pagui-les de forma urgent a aquest enllaç avui mateix per evitar que el paquet sigui retornat: https://correos-pagaments-verificats-cat.net/tarifes"

1. Troba ràpidament els 3 indicadors crítics (alarmes) que delaten que aquest missatge és un cas clar de suplantació d'identitat (phishing) i escriu què hauries de fer amb el missatge.

2. La teva acció immediata: Hauries de clicar per veure què passa o has d'esborrar el missatge directament sense fer res més?



ACTIC NIVELL 1
Competència

Protegeix la salut, el benestar i l'entorn

Sessió 3



Índex

Protegeix la salut, el benestar i l'entorn

1. Ergonomia digital
2. Impacte de la tecnologia en la salut
3. Riscos dels continguts digitals
4. Sostenibilitat i consum responsable de la tecnologia
5. Protecció digital de menors i col·lectius vulnerables

1. Ergonomia digital

Riscos per a la salut musculoesquelètica i la vista

Síndrome de la Fatiga Visual Digital (FVD)

Es produeix perquè, en mirar fixament una pantalla, la freqüència de parpelleig disminueix dràsticament (de les 15-20 vegades per minut habituals a només 5 o 6). Això provoca que la pel·lícula lacrimal s'evapori, causant ulls vermells, sensació de sorra, visió borrosa transitòria i mals de cap a la zona frontal.

La síndrome del "Coll de Text“

El cap humà pesa uns 5 kg en posició neutra. Però quan inclinem el coll uns 60° per mirar el telèfon mòbil, les cervicals suporten una força equivalent a uns 27 kg de pressió. Això provoca contractures greus, desgast prematur dels discs vertebrals i dolors irradiats cap a les espatlles.

Trastorns per Moviments Repetitius (TMR)

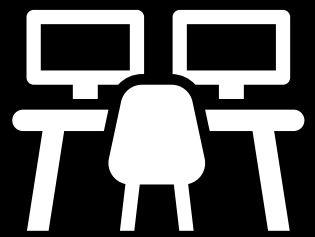
L'ús intensiu del ratolí tradicional i el teclat obliga a fer flexions forçades del canell. Això inflama els tendons i comprimeix el nervi medià que passa pel canell, derivant en la ‘Síndrome del Túnel Carpià’, caracteritzada per formigueig i pèrdua de força als dits.

Ergonomia i salut física en l'ús de dispositius

L'ergonomia digital és la ciència que dissenya i adapta els llocs de treball, eines i tasques a les característiques anatòmiques i fisiològiques de l'usuari. L'objectiu principal és evitar que l'ús diari de la tecnologia es tradueixi en lesions cròniques.



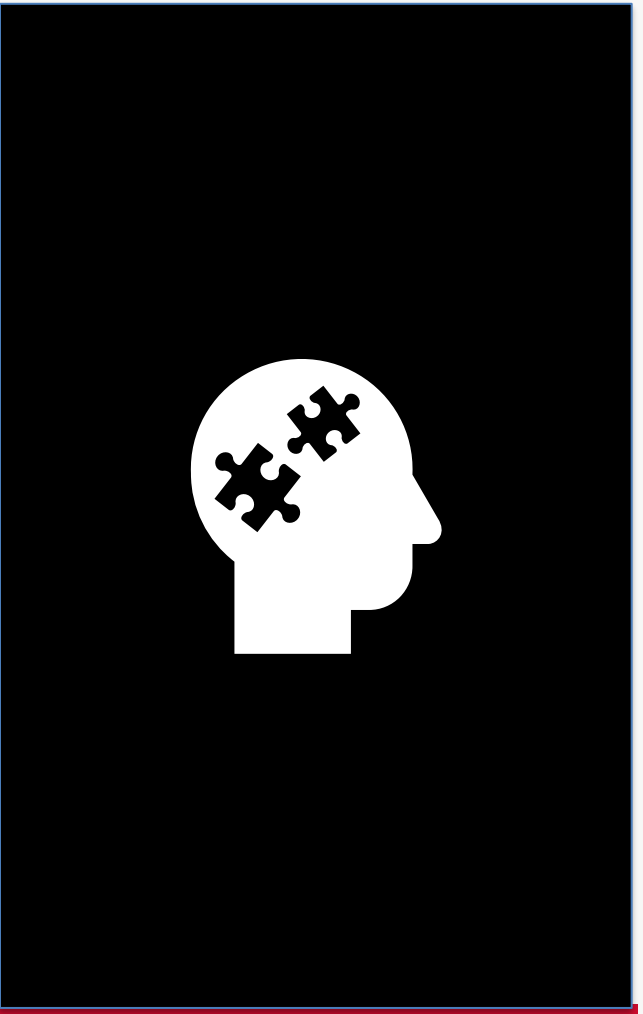
1. Ergonomia digital



Mesures personals i configuració de l'espai de treball

- Alçada de la pantalla: la vora superior del monitor ha d'estar a l'alçada dels teus ulls o com a màxim un 10-20% per sota. Mai per sobre, ja que t'obligaria a estendre el coll cap enrere. Si fas servir un ordinador portàtil, és indispensable utilitzar un elevador i connectar un teclat i ratolí externs.
- La distància òptica: s'ha de mantenir una distància d'entre 50 cm i 70 cm respecte a la pantalla (aproximadament la llargada del teu braç estirat). Una pantalla massa a prop fatiga els músculs ciliars de l'ull de tant enfocar; massa lluny fa que t'inclinis cap endavant.
- Esquena: sempre en contacte amb el respatller, especialment la zona lumbar (amb un coixí si cal).
- Braços i canells: els braços han de formar un angle de 90° a l'alçada del colze. Els canells han d'estar rectes i alineats amb el teclat, preferiblement recolzats sobre un reposacanells tou.
- Cames: dels genolls també a 90° i els peus completament plans a terra. Si les cames pengen, es talla la circulació sanguínia; cal utilitzar un reposapeus.
- Hàbits d'il·luminació i contrast: la llum ambiental ha d'igualar la lluminositat de la pantalla. Evita col·locar el monitor directament davant d'una finestra (provoca enlluernament) o darrere d'ella (provoca reflexos molestos). El text ha de tenir un contrast alt (negre sobre blanc de tota la vida) i una mida de lletra fàcil de llegir sense aclucar els ulls.

2. Impacte de la tecnologia en la salut



Benestar digital vs ús problemàtic

El **benestar digital** consisteix a desenvolupar una relació saludable i intencionada amb la tecnologia, evitant que els mecanismes de recompensa de les aplicacions (com els *likes* o el desplaçament infinit) controlin la nostra vida.

Les línies entre l'ús habitual, l'abús i la conducta addictiva poden ser difuses. Per tant es important aprendre a detectar els símptomes clars de pèrdua de control tenint en compte els següents factors:

1. **Símptomes d'alerta psicològica**

2. **Interferència i "phubbing"** (ignorar les persones que tens al davant perquè estàs pendent del telèfon mòbil)

3. **Impacte en el son i la salut mental**

2. Impacte de la tecnologia en la salut

Ventall de l'ús problemàtic de la tecnologia

Símptomes d'alerta psicològica

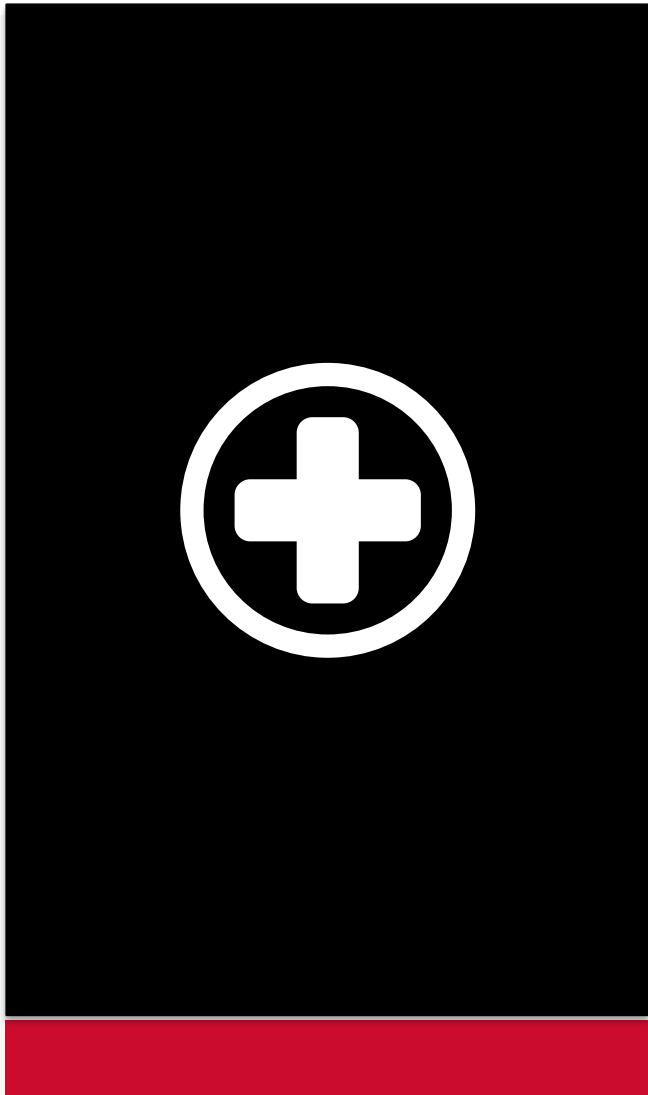
L'aparició de l'ansietat tecnològica o la síndrome de l'abstinència digital (irritabilitat, nerviosisme o mal humor quan no es té cobertura o s'acaba la bateria). També destaca el fenomen conegut com a FOMO (*Fear Of Missing Out*), la por irracional a quedar-se fora o perdre's alguna cosa important que està passant a les xarxes socials.

Interferència i Phubbing

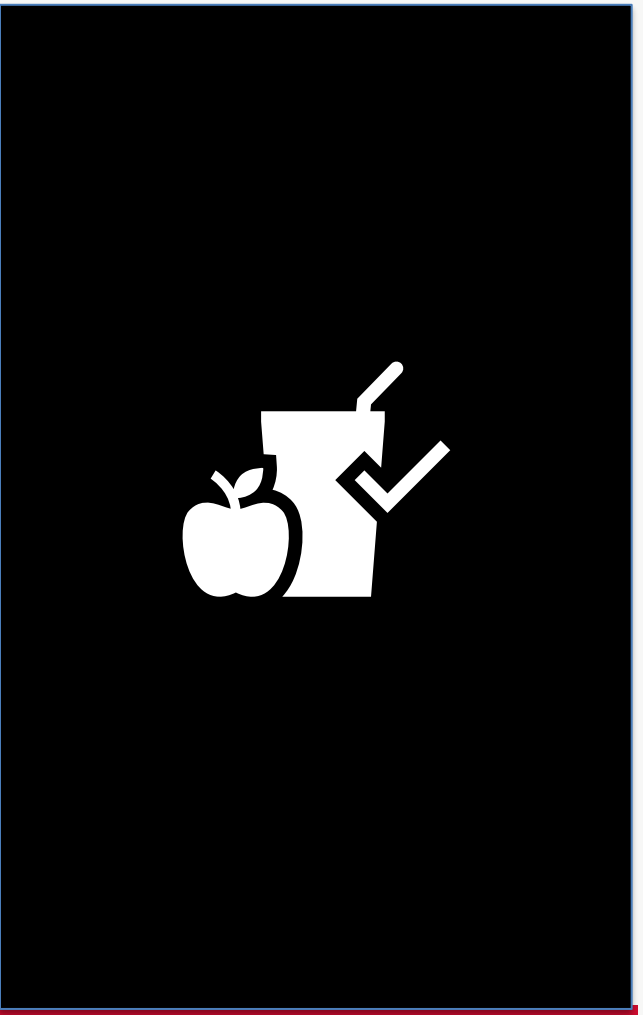
Un senyal clar d'abús és el *phubbing* (ignorar les persones que tens al davant físicament per mirar la pantalla del mòbil). Això degrada el benestar social i les relacions familiars.

L'impacte en el son i la salut mental

L'ús de pantalles abans d'anar a dormir activa de forma artificial el cervell a causa de la llum blava. Aquesta franja de llum frena la producció de melatonina, l'hormona que indica al cos que ha de dormir, provocant insomni tecnològic i un descans fragmentat que l'endemà es tradueix en falta de concentració i estrès.



2. Impacte de la tecnologia en la salut



Estratègies i eines per a la desconnexió digital

La desconnexió digital requereix programar barreres tècniques i canvis d'hàbits:

Eines de monitoratge intern: activar i revisar periòdicament el panell de gestió de temps de l'ordinador o mòbil. Configurar temporitzadors d'aplicacions que bloquegen l'accés a una xarxa social un cop has consumit, per exemple, els teus 30 minuts diaris permesos.

Higiene de notificacions: canviar la configuració per defecte de les aplicacions. Desactivar els globus vermells de notificació i els avisos sonors de tot allò que no requereixi una resposta humana immediata.

Configuració de modes de descans: programar el mode "No molestar" o "Mode descans" perquè s'activi automàticament a partir d'una hora determinada de la nit, passant la pantalla a escala de grisos (cosa que la fa molt menys atractiva per al cervell).

2. Impacte de la tecnologia en la salut

IA i assistents virtuals: Limitacions en la salut mental

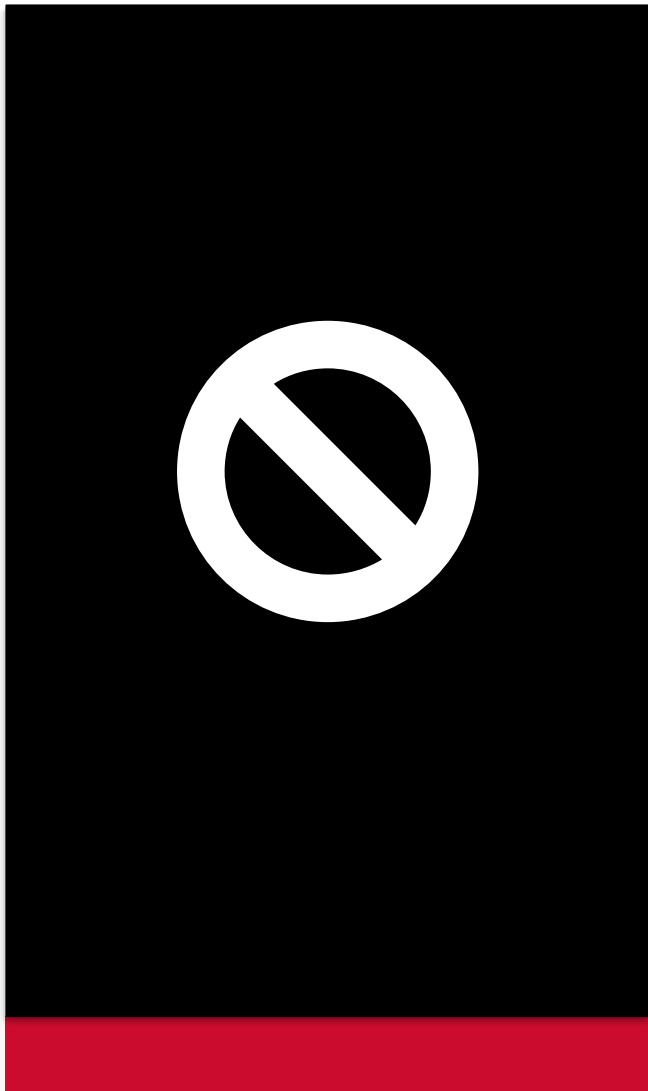
Davant de l'auge de xatbots d'intel·ligència artificial i aplicacions d'autocura basades en la IA, l'usuari ha de ser crític amb els seus límits:

Incapacitat de judici clínic

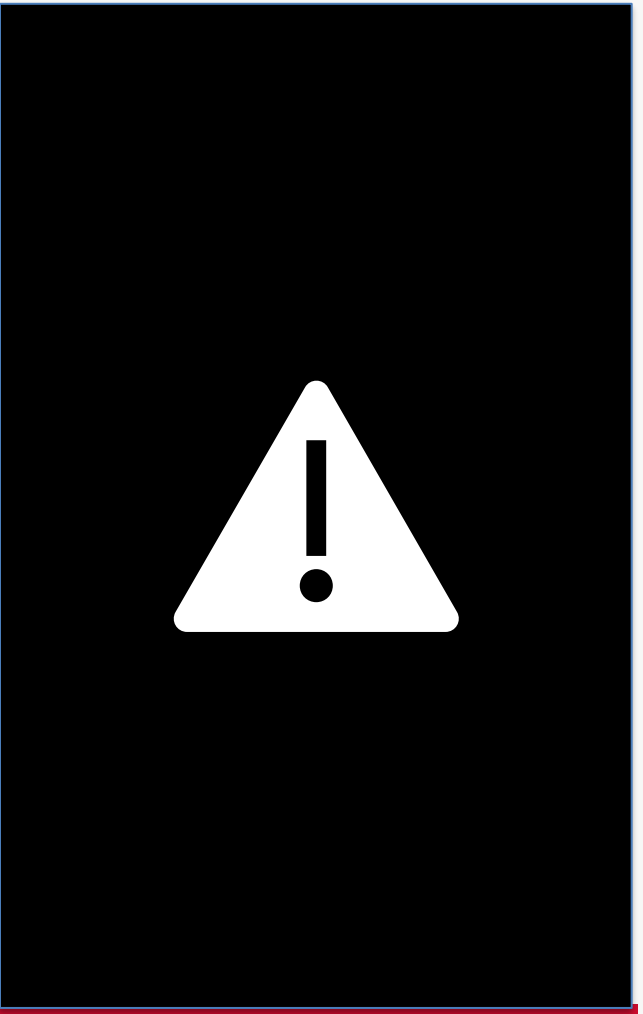
Un model de llenguatge d'IA genera respostes combinant paraules de base estadística. No té capacitat de diagnòstic real. Seguir un tractament de salut física o mental dictat per una IA sense supervisió mèdica posa en risc la vida.

L'efecte mirall i biaixos

Si una persona expressa tristesa o idees nocives, un sistema d'IA mal configurat pot arribar a validar o alimentar aquests pensaments de manera automatitzada en lloc de tallar-los i redirigir l'usuari cap a canals d'ajuda d'emergència humans.



3. Riscos dels continguts digitals



Tipologies de perills a la xarxa

L'espai digital amplifica la velocitat a la qual es transmeten els continguts, fent que qualsevol atac o contingut inapropiat esdevingui massiu en qüestió de minuts. Per això, cal conèixer els possibles perills i els mecanismes legals i tècnics de resposta.

Ciberassetjament (Cyberbullying)

Es diferencia de l'assetjament tradicional perquè no acaba quan el menor surt de l'escola; el persegueix a casa seva les 24 hores del dia a través del mòbil. Té l'agreujant que l'audiència que veu l'agressió pot ser de milers de persones.

Discurs d'odi i continguts radicalitzadors

Textos, vídeos o memes dissenyats específicament per atacar col·lectius vulnerables (per motius de raça, gènere, orientació sexual o religió).

Sextorsió i Grooming

El xantatge amb imatges íntimes o l'engany de menors per part d'adults que es fan passar per joves.

3. Riscos dels continguts digitals

Protocol de resposta davant de continguts nocius

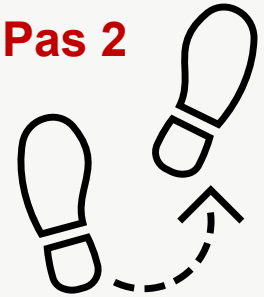
Pas 1

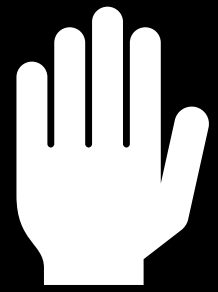


No difondre i tallar la cadena. Compartir un vídeo on s'insulta algú, encara que sigui per dir "mira quina vergonya", et converteix en còmplice de la difusió de la violència. El primer pas sempre és aturar la propagació de forma radical.

Recollir proves (Evidència digital). Abans de bloquejar o esborrar res, si ets la víctima o en tens constància directa, fes captures de pantalla on es vegi clarament l'usuari de l'agressor, la data, l'hora i el missatge. Aquestes captures seran claus en cas d'haver de fer una denúncia formal a la policia.

Pas 2





3. Riscos dels continguts digitals

Protocol de resposta davant de continguts nocius

Pas 3

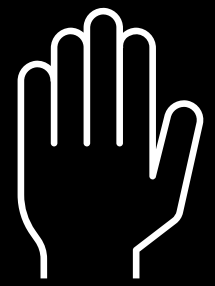


Bloquejar i Reportar/Denunciar a la plataforma. Totes les xarxes socials i aplicacions de missatgeria (WhatsApp, Instagram, TikTok) tenen un botó de "Reportar" o "Denunciar contingut". Això envia una alerta directament als moderadors de la plataforma perquè eliminin el contingut i cancel·lin el compte de l'infractor.

Demanar suport institucional. Si hi ha menors implicats, s'ha d'informar immediatament els tutors, la direcció del centre educatiu o utilitzar els canals oficials com el telèfon d'atenció a la infància o els cossos policials especialitzats en ciberdelictes.

Pas 4





4. Sostenibilitat i consum responsable de la

La petjada ecològica invisible d'Internet i la IA

Qualsevol activitat digital deixa una taca en el món real. L'ecologia digital busca optimitzar l'ús de la tecnologia perquè el seu impacte ecològic sigui el menor possible durant tot el seu cicle de vida.

Els centres de dades com a grans consumidors: Són immensos edificis plens de servidors funcionant sense interrupció. Requereixen un volum d'electricitat brutal i milions de litres d'aigua dolça per als seus sistemes de refrigeració líquida i aire condicionat per tal d'evitar que els processadors es cremin.



El cost ambiental de la Intel·ligència Artificial: Entrenar un sol model d'IA gran pot consumir tanta energia com diversos automòbils durant tota la seva vida útil. Una simple consulta a un xatbot de text o la generació d'una imatge consumeix fins a 10 vegades més energia que una cerca tradicional a Google, ja que requereix una potència de càlcul molt més elevada.



4. Sostenibilitat i consum responsable de la tecnologia

Mesures pràctiques per reduir el consum en el dia a dia

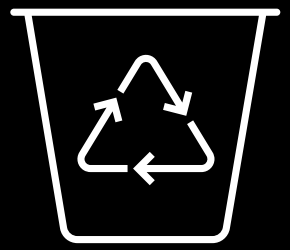
Gestió elèctrica
Configurar la suspensió automàtica de l'ordinador si està 5 minuts inactiu. Evitar el "consum fantasma" desconnectant els reglets d'endolls a la nit.

Neteja digital de dades
Guardar milers de fotos borroses o correus brossa antics a serveis al núvol (com iCloud o Google Drive) obliga a mantenir servidors encesos per a tu de manera innecessària. Practica el buidatge regular de la brossa i els fitxers temporals.

Optimització del streaming
Si escoltes música, utilitza plataformes d'àudio en lloc de reproduir un vídeo de YouTube en alta definició en segon pla només per escoltar la cançó, ja que el consum de dades d'un vídeo és infinitament superior.

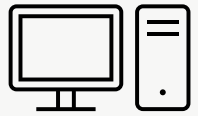


4. Sostenibilitat i consum responsable de la



Gestió dels residus tecnològics: **les 3R digitals**

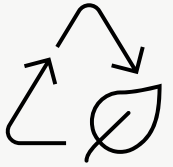
Reduir: no canviar de mòbil cada any per un simple caprici estètic.



Reutilitzar: si un ordinador va lent per treballar, es pot reinstal·lar amb un sistema operatiu lleuger (com Linux) i utilitzar-lo com a servidor domèstic, emmagatzematge de còpies de seguretat o per a tasques d'ofimàtica bàsica dels nens.



Reciclar: quan l'aparell ja no funciona ni es pot reparar, s'ha de portar a una deixalleria o punt verd. Per llei, quan compres un aparell electrònic nou en una botiga (física o online), els venedors estan obligats a recollir el teu aparell vell de forma totalment gratuïta per garantir-ne el reciclatge correcte.



5. Protecció digital de menors i col·lectius vulnerables

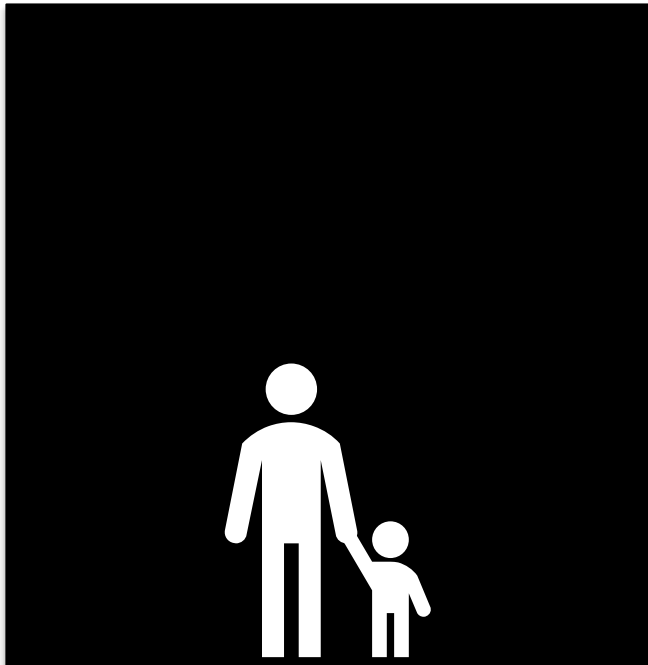
Implementació i configuració de mesures tècniques

El control parental és una eina d'acompanyament digital progressiu que protegeix el menor mentre aquest aprèn a desenvolupar el seu propi criteri. Aquestes són les principals opcions de configuració que ofereixen aquests sistemes:

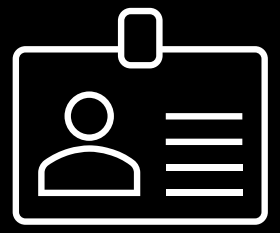
Filtres de contingut web (llistes negres i blanques): bloquegen l'accés a llocs web catalogats com a no aptes (pàgines d'apostes, contingut adult, violència). Les eines de control parental permeten activar motors de cerca segurs (com Google SafeSearch), que oculten automàticament els resultats explícits a les cerques de l'usuari menor.

Gàbies de temps i gestió horària: permeten establir un límit de temps (per exemple: un màxim de 45 minuts al dia a TikTok) i fixar hores de silenci. El sistema bloquejarà completament l'accés al dispositiu a partir de l'hora de dormir.

Supervisió de botigues d'aplicacions: configurar el compte del menor com a "compte infantil" vinculat al compte familiar de l'adult (com Google Family Link o Apple Family Sharing). Qualsevol intent de descàrrega d'una aplicació nova o qualsevol intenció de fer una compra dins d'un joc enviarà una notificació de sol·licitud al mòbil de l'adult, que haurà d'aprovar-la o denegar-la.



5. Protecció digital de menors i col·lectius



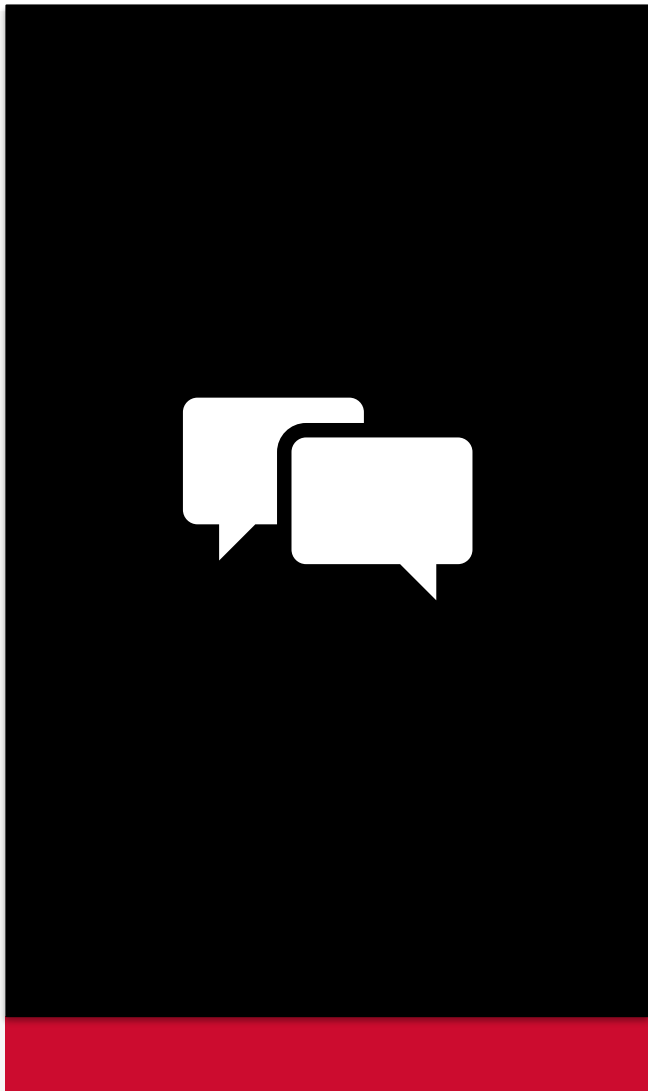
Tipus de control parental segons el nivell d'instal·lació

Nivell	On s'aplica?	Avantatge principal
Dispositiu	Configurat directament al sistema operatiu del mòbil, tauleta o PC del menor.	Protegeix el dispositiu utilitzi la xarxa que utilitzi (també amb les dades mòbils del carrer o Wi-Fi públiques).
Xarxa o router	Configurat directament al *router* de casa teva.	Aplica el filtre a tots els aparells que es connectin al Wi-Fi de la llar de forma simultània (televisions intel·ligents, consoles de jocs, mòbils d'amics).
Aplicació	Dins de la mateixa plataforma específica (per exemple, el perfil infantil de Netflix o YouTube).	Adapta específicament el catàleg audiovisual i els algorismes de recomanació a l'edat seleccionada.

5. Protecció digital de menors i col·lectius vulnerables

Cap programari de control parental és infal·lible al 100%. Els joves poden trobar maneres de **saltar-se els filtres** (per exemple, utilitzant connexions VPN).

La **millor eina de protecció** sempre és el diàleg permanent, l'educació digital en valors i establir un clima de confiança on el menor no tingui por de demanar ajuda si es troba amb un problema a la xarxa.



Exercicis pràctics

L'Auditoria Postural i de Salut Digital

"La Sara estudia a la seva habitació a les fosques per concentrar-se millor. Fa servir un ordinador portàtil recolzat directament sobre les seves cames mentre s'asseu al llit. Sovint passa de llarg 3 o 4 hores sense aixecar-se perquè perd la noció del temps, i últimament té molèsties als canells, mal de coll i fatiga visual."

Identifica els 3 errors ergonòmics i de salut que està cometent la Sara i proposa la mesura correctora/norma de prevenció adequada en cada cas:

- Error 1 (Postura i suport). Mesura correctora:
- Error 2 (Il·luminació). Mesura correctora:
- Error 3 (Fatiga visual i pauses). Mesura correctora (Pista: Regla 20-20-20):



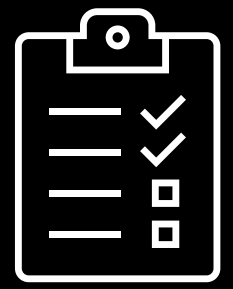
Exercicis pràctics

El Cas de la Foto de l'Èric i el Control Parental

"Els pares de l'Èric (un menor d'11 anys) estan molt orgullosos del seu primer dia d'institut. Han publicat una foto d'ell de cos sencer a Facebook (perfil públic), on se'l veu amb l'uniforme de l'escola i un escut ben visible. A més, a la descripció de la foto hi han posat la ubicació del centre. Per la seva banda, l'Èric utilitza un mòbil sense cap mena de filtre ni restricció d'edat activa."

1. Quin perill de privadesa o seguretat té el fet que es vegi l'uniforme escolar de l'Èric amb la ubicació?

2. Per protegir l'Èric en el seu propi dispositiu mentre sigui menor d'edat d'accedir a continguts no aptes per a ell, quina tecnologia haurien de configurar els seus pares al seu telèfon mòbil? Esmenta 2 funcions que permet aquesta tecnologia.



Exercicis pràctics

Test de Sostenibilitat Digital

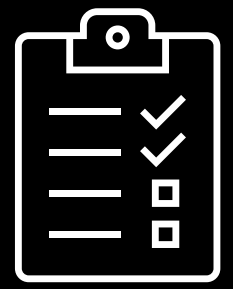
Classifica les següents afirmacions com a **VERDADER o FALS** segons el que dicta la sostenibilitat i el consum responsable dels mitjans digitals:

A. L'emmagatzematge de correus electrònics brossa, fotos repetides al núvol o missatges antics no contamina gens perquè és un format totalment digital i intangible.

B. Quan un mòbil o dispositiu s'espatlla de forma definitiva, s'ha de portar exclusivament a un punt net o deixalleria oficial perquè conté metalls pesants (com el liti o el cobalt) altament contaminants.

C. L'obsolescència programada és una mesura ecològica de les marques que ajuda a fer que els dispositius durin molt més temps i consumeixin menys energia.

D. Per reduir la petjada de carboni digital és més sostenible reparar o actualitzar un ordinador que comprar-ne un de nou cada vegada que vagi lent.



ACTIC NIVELL 1
Competència

Gestiona la identitat i perfils digitals

Sessió 4



Barcelona

Barcelona Activa

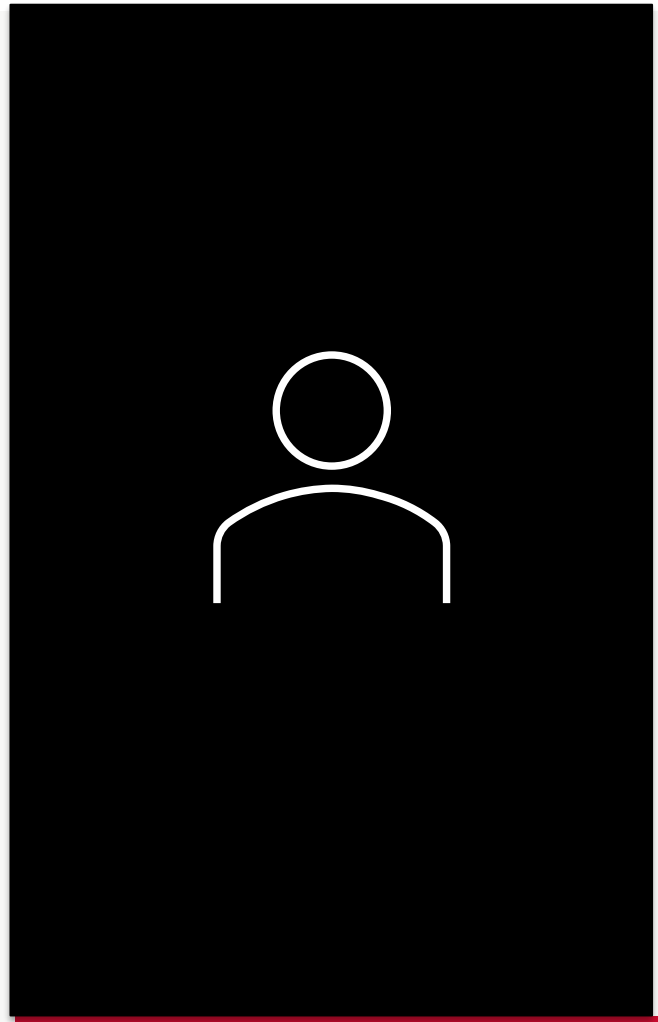
Índex

Gestiona la identitat i perfils digitals

1. Beneficis i riscos de la identitat digital
2. Perfils i presència en entorns digitals
3. Gestió de la identitat digital personal i professional

1. Beneficis i riscos de la identitat digital

Identitat digital és la suma de tot el que un usuari fa a Internet, combinat amb el que les plataformes i altres usuaris diuen o recullen sobre ell.



La identitat digital com a mètode d'autenticació

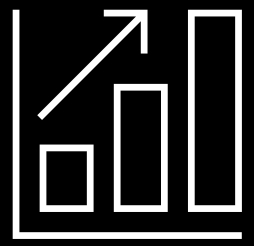
En el funcionament d'Internet, la identitat ha passat de ser purament social a ser un requisit tècnic de seguretat basat en l'autenticació.

L'**autenticació** és el procés pel qual un sistema verifica que tu ets realment qui dius ser.

El fenomen de l'Autenticació Federada (Social Login)

És el sistema basat en protocols (com OAuth) que utilitzen empreses com Google, Apple, Facebook o Microsoft. Permet que actuïn com a "proveïdors d'identitat". En lloc de crear un compte des de zero a cada botiga en línia o aplicació, delegues la teva identitat en un d'aquests gegants (per exemple, registrar-se a Wallapop utilitzant el compte de Gmail).

1. Beneficis i riscos de la identitat digital



Anàlisi de **beneficis** de l'Autenticació Federada

- Reducció de la fatiga de contrasenyes: l'usuari no ha d'inventar, recordar ni gestionar dotzenes de claus diferents (evitant la pràctica de risc de repetir la mateixa contrasenya a tot arreu).
- Seguretat centralitzada: si el teu compte de Google o Apple té activat el doble factor d'autenticació (2FA), tots els serveis on entris amb aquest botó estaran indirectament protegits per aquesta alta seguretat.
- Rapidesa en l'accés: simplifica els formularis de registre eliminant la necessitat de confirmar el correu electrònic a cada nova plataforma.

1. Beneficis i riscos de la identitat digital

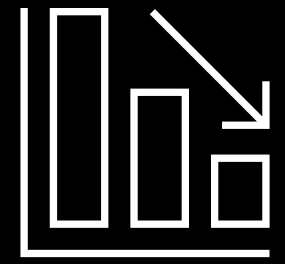
Anàlisi de **riscos** de l'Autenticació Federada

Efecte dominó en cas de robatori de credencials

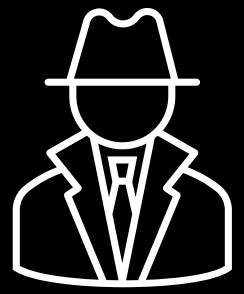
Si un atacant descobreix la clau del teu compte centralitzat, no només et roba el correu; té la clau per entrar automàticament a totes les aplicacions vinculades (bancs, plataformes de salut, xarxes socials, etc.).

Pèrdua de privadesa per encreuament de dades

En utilitzar la identitat federada, el proveïdor (per exemple, Google) rep informació de quines altres aplicacions fas servir, a quina hora hi entres i des d'on, enriquint el seu perfil publicitari sobre tu.



1. Beneficis i riscos de la identitat digital



El rastre digital passiu

Cada vegada que naveguem, generem informació sense adonar-nos-en. La identitat digital es nodreix d'aquestes dades de comportament generades per la nostra activitat en línia:

Registres d'ús (logs): són fitxers de text guardats automàticament als ordinadors centrals de les webs on entres. Recullen la teva adreça IP (que revela la teva ubicació geogràfica aproximada i el teu operador d'Internet), el sistema operatiu del teu dispositiu, el navegador (Chrome, Safari, Firefox), l'idioma i el registre d'errors.

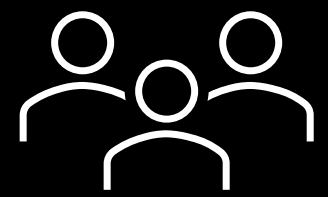
Galetes (Cookies) i rastrejadors: petits fragments de codi que les webs guarden al teu navegador per recordar qui ets. N'hi ha de tècniques (necessàries per mantenir obert el carret de la compra) i de rastreig o de tercers, que segueixen els teus passos per diferents llocs web per saber quins productes has estat mirant.

Empremta digital del dispositiu: una tècnica avançada on les webs recullen la configuració exacta del teu ordinador (mida de pantalla, lletra tipogràfica instal·lada, connectors). Permet identificar-te i rastrejar-te encara que esborris les galetes o facis servir el mode d'incògnit.

2. Perfils i presència en entorns digitals

Creació de perfils socials i gestió de la privadesa

Un **perfil digital** és la interfície pública d'una persona en una plataforma. Crear un perfil implica prendre decisions crítiques sobre quin nivell de privadesa requereix cada entorn segons els objectius perseguits. Un aspecte important és distingir el disseny del perfil segons si els objectius són **personals** o **professionals**.



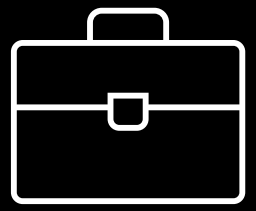
ÀMBIT PERSONAL (Instagram, TikTok, Facebook)

- **Objectiu**: Interacció íntima i oci.
- **Regla d'or**: Visibilitat PRIVADA o RESTRINGIDA.
- **Acció tècnica**: Activar la sol·licitud de seguiment. Ocultar el compte dels motors de cerca.

ÀMBIT PROFESSIONAL (LinkedIn, Portfolis, Twitter/X sectorial)

- **Objectiu**: Oportunitats laborals i reputació de marca personal.
- **Regla d'or**: Visibilitat PÚBLICA i indexable.
- **Acció tècnica**: Permetre que qualsevol usuari de la xarxa et trobi per nom i cognom a Google.

2. Perfils i presència en entorns digitals



Perfil personal vs perfil professional

Alguns aspectes més a tenir en compte a l'hora de configurar el nostre perfil són:

Configuració de la informació bàsica personal

En perfils d'oci, s'han d'evitar dades reals sensibles. És aconsellable utilitzar un pseudònim o àlies, ometre la data de naixement completa (per evitar robatoris d'identitat o felicitacions automatitzades que revelin l'edat), i mai exposar dades de contacte directes com el telèfon personal o l'adreça de casa.

Configuració professional

En aquest àmbit, el perfil s'ha de tractar com un currículum o aparador obert. La imatge de perfil ha de ser professional (fons neutre, enquadrament de cara, aspecte cuidat), el nom ha de ser el real i complet, i s'ha de facilitar un mètode de contacte formal, com un correu electrònic exclusiu per a assumptes laborals.

2. Perfils i presència en entorns digitals

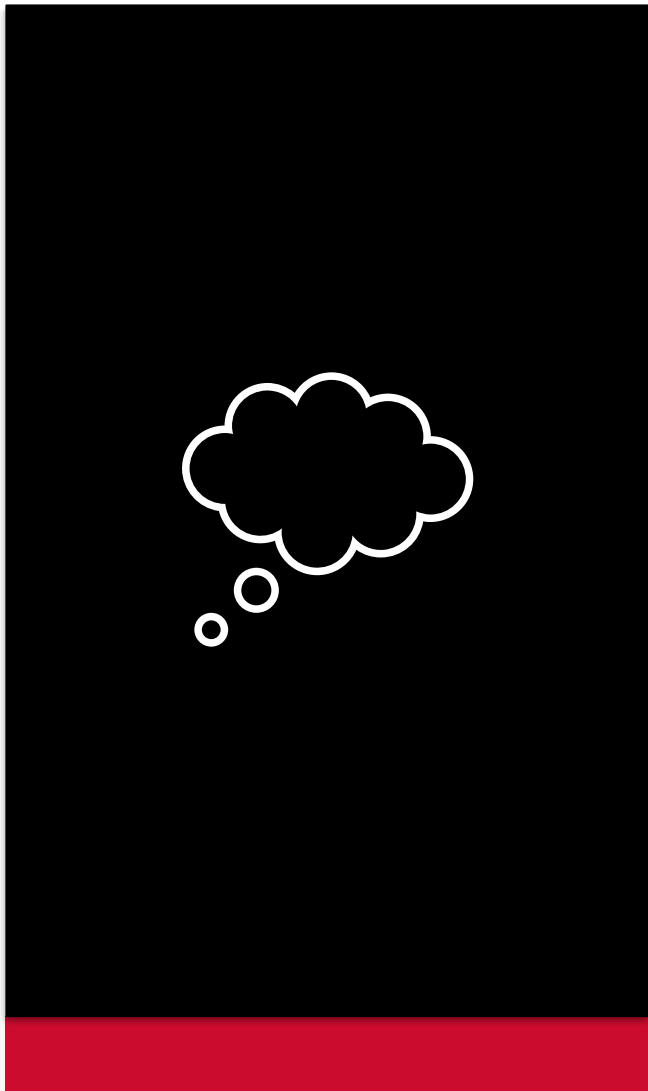
La persistència de la informació i el Principi de Precaució

Un error comú en els usuaris digitals és creure que l'acció d'"Eliminar" fa desaparèixer les dades del mapa digital.

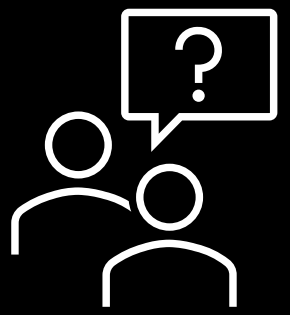
- La realitat de la persistència en línia: Quan puges una imatge, aquesta passa per servidors intermedis i xarxes de distribució de continguts (CDN). En qüestió de segons, pot ser emmagatzemada en la memòria cau (*caché*) dels cercadors com Google, replicada per bots automatitzats o desada mitjançant una simple captura de pantalla per un altre usuari.

- El dret a l'oblit: tot i que la legislació europea (RGPD) empara el dret a demanar que s'eliminin les teves dades personals dels motors de cerca sota certes condicions, el procés és complex i no pot esborrar les còpies privades que la gent hagi fet de la teva informació.

- L'aplicació del Principi de Precaució: s'ha d'actuar de forma preventiva. La millor mesura de seguretat és la que s'aplica abans de publicar. Si un contingut (text, foto o vídeo) et pot generar un problema d'aquí a cinc anys, la decisió correcta és mantenir-lo fora de la xarxa.



2. Perfils i presència en entorns digitals

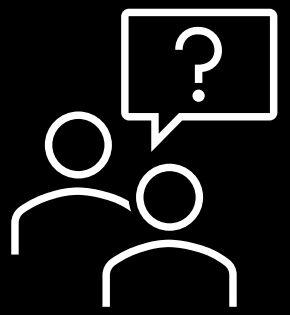


Situació pràctica per a la reflexió

Imagina que has configurat el teu perfil personal com a **Públic**, hi has penjat un vídeo de broma d'una festa i, al cap de deu minuts, te'n penedeixes i l'esborres.

Creus que estàs 100% lliure de riscos gràcies a haver-lo eliminat?

2. Perfils i presència en entorns digitals



Resposta

La **prevenció** és l'única mesura de seguretat 100% efectiva.

L'eliminació digital no garanteix la desaparició real de la informació. Aplica sempre el Principi de Precaució abans de prémer "Publicar".

3. Gestió de la identitat digital personal i professional

Coherència transversal a través de diferents plataformes

Per construir una identitat digital sòlida i fiable (especialment en el món professional), cal mantenir un fil conductor homogeni en tots els teus perfils públics:

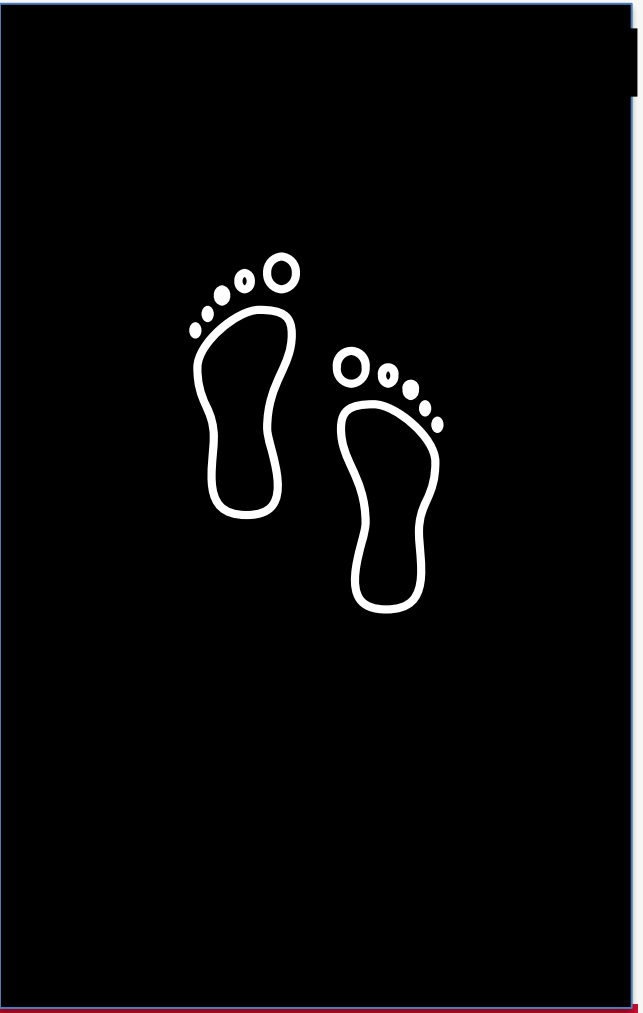
- ✓ El nom com a marca (*Username*): s'ha d'intentar reservar el mateix identificador a tot arreu (per exemple, @joan_garcia_enginyer). Això simplifica la cerca i evita que altres persones utilitzin el teu nom creant confusions.

- ✓ L'avatar o imatge corporativa personal: utilitzar la mateixa fotografia de perfil a LinkedIn, Twitter i el teu bloc professional ajuda a crear un reconeixement visual immediat.

- ✓ La proposta de valor (Descripció breu): la descripció o *bio* ha de mantenir la mateixa narrativa. Si a LinkedIn et defineixes com a "Especialista en ciberseguretat", el teu perfil professional a altres xarxes ha de reflectir el mateix sector d'expertesa.



3. Gestió de la identitat digital personal i



Anatomia completa de la Petjada Digital i la seva gestió

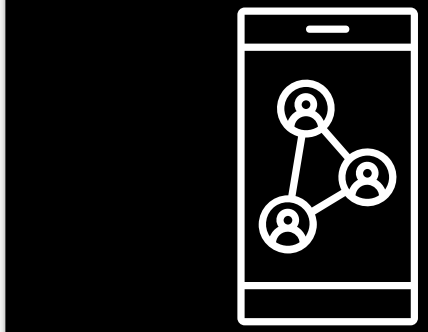
Component	Exemples concrets	Com afecta la teva reputació?
Publicacions	Fotos d'Instagram, posts a blocs, fils de discussió, articles d'opinió.	Mostra el teu nivell de coneixement, el teu estil de comunicació i maduresa.
Comentaris	Ressenyes a Google Maps d'un restaurant, crítiques a vídeos.	Revela el teu caràcter i el teu nivell de respecte cap als altres.
Interaccions	Fer un “m'agrada”, retuitar o retornar una piulada, compartir posts d'altres, subscriure's a canals.	Recolzar públicament un contingut inadequat et vincula directament.
Dades d'Ús	Grups públics de Facebook, llistes públiques de música o vídeo.	Detalla els teus interessos secundaris, aficions i el tipus de comunitats.

3. Gestió de la identitat digital personal i professional

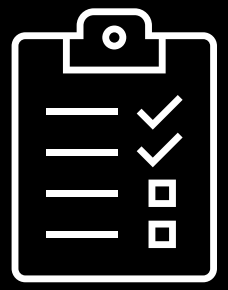
El perill dels algoritmes i el procés d'*Egosurfing*

La selecció algorítmica: les plataformes utilitzen la teva petjada digital d'interaccions mostrar-te només continguts que s'ajusten al que prèviament has mirat. Això pot radicalitzar la identitat digital d'un usuari sense que se n'adoni.

Auditoria d'*Egosurfing*: es recomana fer *egosurfing* (autocerca) periòdicament. Consisteix a introduir el teu nom i cognoms (entre cometes, `"Nom Cognom"`) als cercadors des d'una finestra d'incògnit (perquè els resultats no estiguin alterats pels teus propis gustos). D'aquesta manera, veuràs exactament el mateix currículum invisible que veuria un reclutador laboral o qualsevol desconegut, i podràs detectar així informació antiga, enllaços trencats o imatges que calgui demanar que s'eliminin per protegir la teva reputació.



Exercici 1: El meu "Jo" digital (Auditoria d'*Egosurfing*)



1. **Preparació**: Obre una finestra de navegació d'incògnit al teu navegador preferit (això evita que els resultats de Google estiguin alterats pel teu historial o la teva sessió iniciada).

2. **Cerca simple**: Introdueix el teu nom i cognoms complets entre cometes: "Nom Cognom1 Cognom2". Què hi apareix?

3. **Cerca combinada**: Afegeix la teva localitat o el teu centre d'estudis/feina actual: "Nom Cognom" + "Ciutat".

4. **Cerca d'imatges i vídeos**: Passa a la pestanya d'imatges de Google. Hi ha alguna fotografia teva o on se't pugui identificar? De quin compte o web prové?

5. **Anàlisi de xarxes**: Cerca els teus perfils a Instagram, TikTok o Facebook des de fora (sense iniciar sessió). Es pot veure la teva biografia, la teva llista de seguidors o alguna publicació?

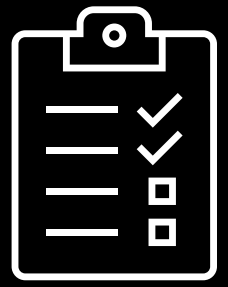
Exercici 1: El meu "Jo" digital (Auditoria d'*Egosurfing*)

Fitxa de treball

Pregunta d'Auditoria	Resposta i Reflexió de l'Alumne
1. Quins canals dominen?	Per exemple: Apareixen enllaços al meu compte de LinkedIn, butlletins del meu club esportiu o el meu nom al BOE.
2. Privadesa detectada:	S'ha pogut veure alguna foto o dada personal des d'una finestra d'incògnit? Estan realment capats els meus perfils personals?
3. Coherència de marca:	Si algú compara el meu perfil de LinkedIn amb el d'Instagram, hi ha elements comuns (nom, foto) o són completament oposats?
4. Pla d'Acció:	Quina foto o informació que ha sortit a Google m'agradaria esborrar o protegir millor a partir d'avui?



Exercici 2: El Semàfor de la Publicació (Principi de Precaució)



Debatiu amb la vostra parella com classificaríeu les següents situacions de publicació utilitzant els colors del semàfor. Escriviu el color triat i una breu frase de justificació:



VERD = És segur publicar-ho en un perfil públic.



TARONJA = Compte! Només es pot publicar si es restringeix molt la privadesa (perfil tancat) o si es canvien dades.



VERMELL = Perill! No s'ha de publicar per cap motiu (risc de reputació o privadesa).

Exercici 2: El Semàfor de la Publicació (Principi de Precaució)

Cas 1: Un vídeo de TikTok on surts ballant a la cuina de casa teva, on de fons es veu un calendari familiar penjat a la paret on hi ha apuntats els aniversaris i les adreces de la família.

El nostre color és: _____ perquè...

Cas 2: Una fotografia a LinkedIn on celebres que has acabat un curs de programació web, acompanyada d'un text formal on agraeixes el suport dels teus professors.

El nostre color és: _____ perquè...

Cas 3: Una piulada a Twitter/X queixant-te amb paraules molt dures i insults d'un servei d'atenció al client d'una marca de roba coneguda, utilitzant el teu compte personal on tens posats els teus cognoms reals.

El nostre color és: _____ perquè...



ACTIC NIVELL 1
Competència

Actua cívicament en l'entorn digital

Sessió 5



Barcelona

Barcelona Activa

Índex

Actua cívicament en l'entorn digital

1. Normes de comportament i etiqueta digital
2. Propietat intel·lectual i llicències digitals
3. Privacitat i respecte a la intimitat digital
4. Llibertat d'informació i expressió digital
5. Protecció i defensa dels drets digitals
6. Detecció de notícies falses i perfils fraudulents

1. Normes de comportament i etiqueta digital

Normes de comportament i etiqueta digital (Netiquette)

La comunicació **digital** difereix radicalment de la presencial. Els principals factors de distorsió són:

- L'absència d'elements de comunicació no verbal (els gestos, el to de veu, la mirada o l'expressió facial).
- L'asincronia de l'escriptura.

Sense aquests elements reguladors, qualsevol missatge pot ser **malinterpretat** amb facilitat si no s'apliquen de manera conscient unes normes bàsiques de cortesia conegudes universalment com a **Netiquette** (etiqueta digital).



1. Normes de comportament i etiqueta digital



Conceptes clau de l'etiqueta digital

- L'asincronia i l'absència de canal no verbal: En persona, un comentari irònic s'acompanya d'un somriure que indica complicitat. En format textual, la mateixa frase es pot percebre com una agressió directa o fredor. La netiquette ens obliga a redactar avaluant constantment com llegirà el missatge un receptor que no ens pot veure.

- La regla d'or de les majúscules: En la cultura històrica d'Internet, escriure paraules o textos completament en MAJÚSCULES equival a cridar, expressar ràbia o exigir de manera agressiva. S'ha de limitar el seu ús exclusivament a sigles oficials.

- L'ús estratègic d'emoticones i el to: Les emoticones o emojis no són elements infantils o superflus; en la comunicació escrita informal actuen com a "reconstructors" del canal no verbal. Ajuden a matisar l'estat d'ànim del remitent. Per exemple, afegir un punt final sec a un "D'acord“ pot denotar enuig, mentre que un "D'acord! 😊" transmet col·laboració i cordialitat.

1. Normes de comportament i etiqueta digital

Adaptació i canvi de registre segons el canal

Un bon ciutadà digital domina la versatilitat comunicativa. No es tracta d'escriure sempre amb "ultracorrecció", sinó de saber on i quan aplicar cada registre:

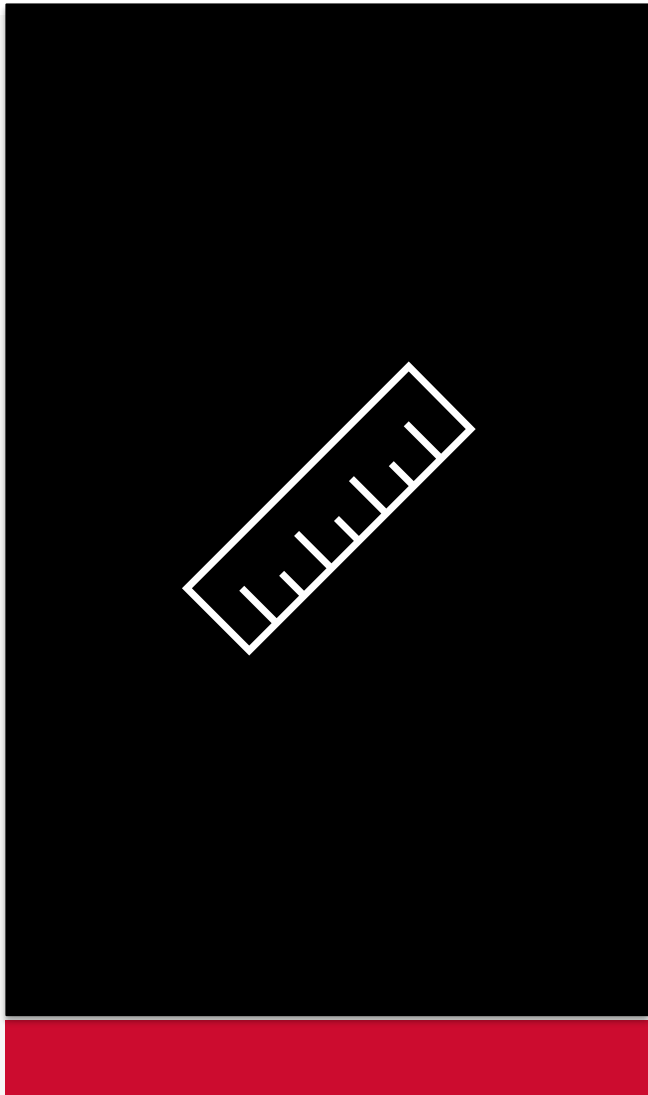
Registre Informal (Xats de missatgeria com WhatsApp, Telegram)

Permet abreviatures espontànies, ús lliure d'emojis, immediatesa i frases fragmentades. Tot i això, s'ha de respectar la privadesa del temps de l'altre (evitar enviar missatges fragmentats un rere l'altre en lloc d'un únic bloc coherent).

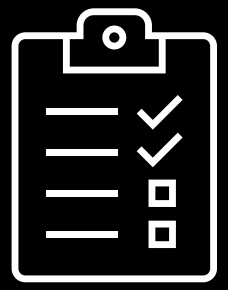
Registre Formal (Correu electrònic professional, acadèmic o tràmits administratius)

Exigeix una estructura clàssica i pulcra. Tot missatge formal ha de constar de:

- Capçalera/Assumpte clar i descriptor (mai deixar-ho en blanc o posar "Hola").
- Salutació inicial formal (p. ex., "Benvolgut/da [Nom]" o "Estimat/da [Nom]").
- Cos del text amb bona ortografia, paràgrafs definits i absència d'abreviatures col·loquials.
- Comiat cordial i signatura clara amb el nom complet de qui envia el missatge i el seu rol.



1. Normes de comportament i etiqueta digital



Exercici: **El Traductor de To i Registre**

Cas A (to inapropiat i majúscules): L'Àlex envia un correu electrònic a un professor perquè té un dubte sobre un treball del curs. El missatge diu:

"NO ENTENC EL QUE HEM DE FER AL PUNT 3!!! M'HO POTS EXPLICAR ALTRA VEGADA???"

1. Quins errors de netiquette comet l'Àlex?
2. Reescriu el correu de l'Àlex de forma correcta i formal.

Cas B (excés de confiança i interpretació): En un correu enviat a una adreça de suport de l'institut, un alumne escriu:

"hola, la meva contrasenya no va... soluciona-ho ràpid k tinc pressa, thx"

1. Com es podria interpretar aquest missatge?
2. Reescriu el missatge mantenint la cordialitat i el respecte.

2. Propietat intel·lectual i llicències digitals

Propietat intel·lectual i llicències d'ús

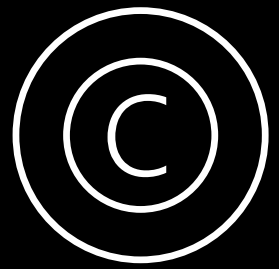
Qualsevol creació original (imatge, cançó, codi de programació, text de bloc, vídeo, dissenys 3D) té un autor o creador immediat. Per defecte, la legislació internacional i estatal sobre “Propietat Intel·lectual” protegeix aquestes obres des del moment mateix de la seva creació sense necessitat de cap registre previ. Per tant, és un error de seguretat jurídica greu assumir que "si està a Google, es pot utilitzar gratuïtament i lliure".

Drets d'Autor (Copyright)

És la protecció de caràcter restrictiu i privatiu representat per la icona ©. Sota aquesta llicència, l'autor es reserva absolutament tots els drets d'explotació, còpia, distribució i modificació. Per reutilitzar qualsevol d'aquestes obres cal demanar permís escrit exprés a l'autor i, normalment, realitzar una contraprestació econòmica.

Domini Públic

Obres amb drets d'explotació de les quals han expirat legalment. A l'estat espanyol, de manera generalitzada, això passa transcorreguts 70 o 80 anys de la mort de l'autor (depenent de la data de decés). Les obres en domini públic es poden copiar, modificar i utilitzar lliurement, tot i que sempre cal respectar l'atribució moral de l'autor original.



2. Propietat intel·lectual i llicències digitals



Llicències Lliures o Obertes (Creative Commons - CC)

Són un model innovador on l'autor utilitza els seus propis drets d'autor per declarar, d'entrada, quins usos gratuïts permet fer al públic general de la seva obra. Aquestes llicències es configuren combinant de manera modular quatre condicions bàsiques representades per sigles o icones:

BY (Atribució/Reconeixement): Condició obligatòria en gairebé totes les llicències CC. S'ha de citar obligatòriament l'autor original, enllaçar a l'obra i especificar quina llicència té.

NC (No Comercial): Es pot utilitzar, copiar i distribuir l'obra, però mai amb finalitats lucratives o comercials directes o indirectes.

ND (Sense Obra Derivada - No Derivatives): Es permet l'ús de l'obra sempre que es mantingui exactament en la seva forma original. Està prohibit retallar-la, traduir-la, acoblar-la amb altres materials o utilitzar-la com a base per a un contingut nou.

SA (Compartir Igual - Share Alike): Si es modifica o es crea una obra a partir de l'original, el producte resultant s'ha de registrar i distribuir exactament sota la mateixa llicència que tenia l'original.

2. Propietat intel·lectual i llicències digitals

Exercici: **L'Auditoria de Llicències de Treball**

La Clara i el Lluc estan creant un web per al projecte de l'escola i necessiten incloure unes imatges i una cançó de fons. Determineu si les seves accions són legals o si estan infringint la propietat intel·lectual:

Situació 1: La Clara troba una foto de Google d'un fotògraf professional que té la indicació © Tots els drets reservats. Com que és per a un treball escolar sense ànim de lucre, la descarrega, la retalla una mica i la penja al seu web d'escola en obert.

És legal? Justifica la resposta.

Situació 2: La Clara troba una foto preciosa d'un bosc a Wikimedia Commons amb la llicència CC BY. Ella la posa al web del treball escolar i, a sota de la imatge, hi col·loca el text: "Foto de Joan Puig, disponible a Wikimedia Commons, sota llicència CC BY".

Està actuant correctament? Quina regla compleix?



3. Privacitat i respecte a la intimitat digital

El dret a l'honor i a la intimitat dels altres

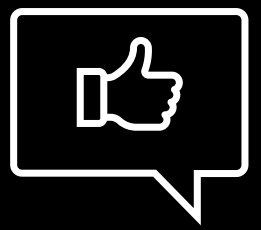
La protecció de la privadesa és **bidireccional**.

Sovint ens centrem exclusivament a protegir les nostres dades i configuracions (visió egoista), oblidant que tenim el deure ètic i l'obligació legal de **respectar rigorosament els drets civils** dels nostres companys i persones de l'entorn digital.

Qualsevol vulneració pot comportar no només problemes disciplinaris al centre educatiu, sinó també **responsabilitat civil i penal**.



3. Privacitat i respecte a la intimitat digital



Consentiment i confidencialitat

El Consentiment Explícit de la Imatge

No es pot publicar, difondre ni etiquetar cap persona en una fotografia o vídeo en una xarxa social o web de manera oberta sense disposar de la seva autorització lliure i explícita. El fet que una foto s'hagi pres en un espai públic no atorga un dret automàtic de publicació a Internet si s'identifica clarament el rostre d'una persona.

La confidencialitat de la missatgeria privada

Capturar una conversa de xat de caràcter privat (com WhatsApp o Telegram) i reenviar-la a tercers, penjar-la a un grup escolar o difondre-la públicament sense el consentiment de tots els participants en la conversa és una infracció de la privadesa regulada legalment. Es considera una vulneració greu del dret fonamental a la intimitat i al secret de les comunicacions.

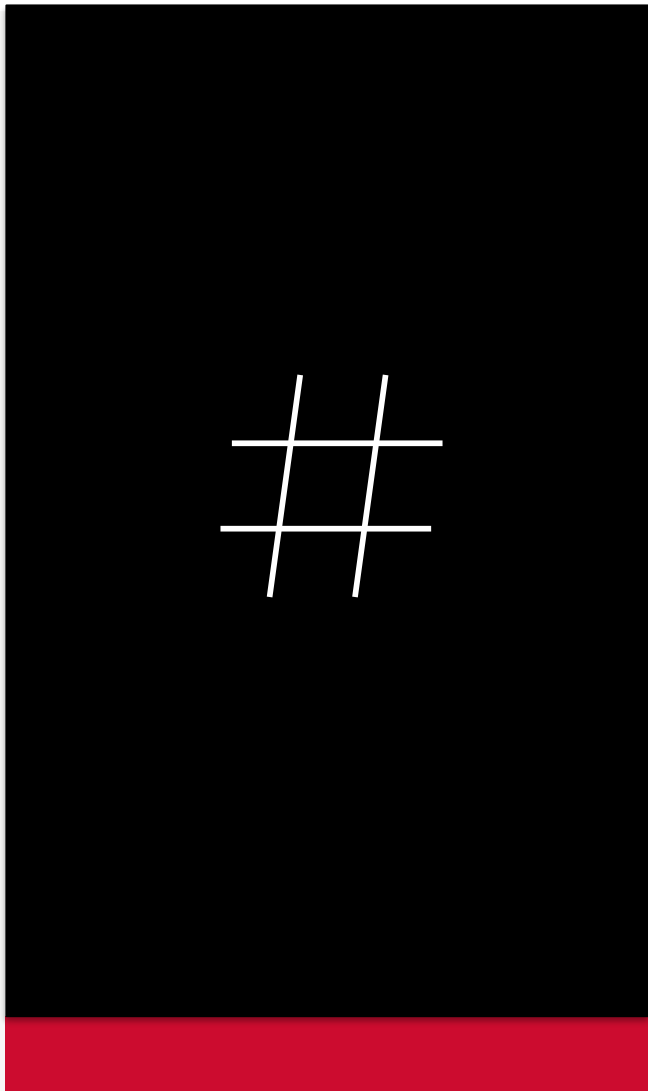
3. Privacitat i respecte a la intimitat digital

El Dret a l'Honor i a la Pròpia Imatge

A escala normativa (per exemple: la Llei Orgànica 1/1982 de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge), l'honor és el reconeixement de la dignitat d'una persona. Per tant, difondre imatges distorsionades, mems humiliants d'un company o fets falsos o íntims que el desprestigien és directament il·legal, i pot encasellar-se dins de conductes greus com el ciberassetjament (cyberassetjament) o la difamació.

L'etiquetatge responsable

S'ha de consultar sempre de manera prèvia abans d'etiquetar un company en una publicació. L'etiquetatge associa de manera permanent aquella imatge a la seva identitat digital, la qual cosa pot afectar la seva reputació de cara al futur laboral o acadèmic sense que aquesta persona ho hagi decidit.



3. Privacitat i respecte a la intimitat digital

Exercici: **El Judici de la Captura de Pantalla**

"El Pau s'està fent un tip de riure perquè una companya d'aula s'ha equivocat enviant-li un àudio on confessa que s'ha adormit estudiant i que no farà el treball d'avui. El Joan fa una captura de la conversa on es veu la foto de perfil i el número de telèfon de la noia, i la reenvia directament al grup de WhatsApp de l'estudiantat i del seu equip de futbol perquè tothom s'ho passi bé."

1. Quins dos drets o aspectes de la privadesa de la seva companya està vulnerant el Joan en aquesta acció?

2. Quin perill té de cara a l'honor i reputació de la noia a nivell d'aula o d'escola?

3. Quina hauria d'haver estat l'actuació cívica i responsable del Joan en rebre aquest àudio privat enviat per error?



4. Llibertat d'informació i expressió digital



Llibertat d'expressió i d'informació responsable

Tots els ciutadans digitals gaudeixen del dret a expressar lliurement les seves opinions, pensaments i idees mitjançant qualsevol plataforma o eina tecnològica. No obstant això, s'ha de comprendre de manera molt clara que la llibertat d'expressió no és un dret absolut ni il·limitat. El dret propi s'acaba immediatament allà on comencen els drets de l'altre o la comissió d'un delicte penal.

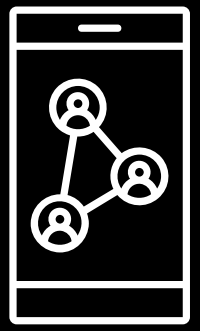
Els límits de la llibertat d'Expressió

No està emparat sota aquest dret l'ús d'insults personals, la difamació sistemàtica, les injúries, les calúmnies (acusar algú de cometre un delicte sabent que és fals) o l'emissió de discurs d'odi dirigit a col·lectius vulnerables (per motius de raça, gènere, orientació sexual, religió o discapacitat).

4. Llibertat d'informació i expressió digital

El Marc de Moderació de les Plataformes (normes de la comunitat)

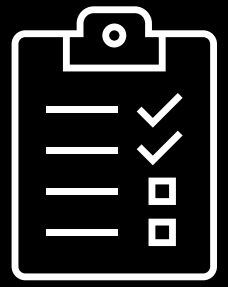
Les xarxes socials (TikTok, Instagram, YouTube, Twitter/X) no són espais neutrals desregulats. Com a empreses privades, disposen d'unes Condicions del Servei i unes "Normes de la Comunitat" que defineixen de forma estricta quin contingut és admès. Les plataformes apliquen mecanismes de moderació actius, recolzats en Intel·ligència Artificial i equips humans, que poden eliminar continguts d'ofici o bloquejar comptes d'usuaris que incompleixen repetidament aquestes directrius sobre assetjament, nuesa, violència o odi.



Dret a la Informació vs. Difusió Responsable

Garantir el dret de la societat a rebre informació veraç implica actuar amb extrema diligència abans de propagar qualsevol afirmació. La llibertat d'expressió no empara la difusió conscient de difamacions que destrueixen la reputació professional o personal d'altri. El civisme digital exigeix que, si no tenim la certesa o proves d'un fet, evitem fer-nos eco d'afirmacions que facin mal a un tercer.

4. Llibertat d'informació i expressió digital



Exercici: **Opinió Constructiva vs. Atac Digital**

Classifica els següents dos comentaris publicats a la secció de ressenyes de Google d'un establiment local. Indica si entren dins de la Llibertat d'Expressió Responsable (LLE) o si són un Atac/Vulneració de Drets (AV) i justifica la tria:

Comentari 1: "El tracte en aquest restaurant ha estat molt dolent. El cambrer que es diu Miquel i que viu al carrer Major és un dropo inepte que no serveix per a res, s'hauria de tancar el lloc i fer-los fora a tots d'aquest poble!"

- ✓ Classificació: LLE o AV?

Comentari 2: "Vam esperar més de 45 minuts que ens portessin el menjar i la carn ens va arribar freda. No recomano el lloc si teniu pressa perquè el servei és lent, tot i que el local és net i bonic."

- ✓ Classificació: LLE o AV?

5. Protecció i defensa dels drets digitals

Actua i defensa els drets digitals (Bloqueja i reporta)

Davant de situacions d'assetjament, suplantació d'identitat, discurs d'odi o contingut inadequat, el ciutadà digital no ha d'adoptar un paper d'espectador passiu ni tampoc de defensors agressius que alimenten el conflicte.

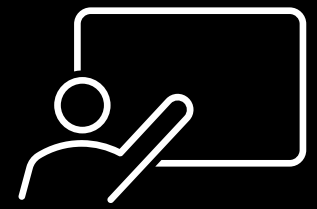
Les xarxes i les administracions ofereixen eines legals i tècniques eficaces que cal conèixer per restablir el control de la situació d'una manera civilitzada i autònoma.



BLOQUEJAR



DENUNCIAR



5. Protecció i defensa dels drets digitals



Mecanismes Tècnics de Plataforma



Bloquejar: És una acció restrictiva de caràcter immediat que impedeix que l'usuari conflictiu pugui enviar-nos missatges, veure el nostre perfil, localitzar les nostres publicacions o comentar qualsevol dels nostres continguts. És l'eina principal per tallar l'accés directe d'un agressor al nostre entorn personal.



Reportar/Denunciar a la plataforma: És un avís oficial que s'envia als equips de moderació del servei (Instagram, TikTok, etc.) per advertir que un determinat perfil, foto o comentari incompleix de manera flagrant les normes de comportament. Si el report és estimat, la plataforma elimina el contingut o inhabilita el compte de l'infractor.

5. Protecció i defensa dels drets digitals

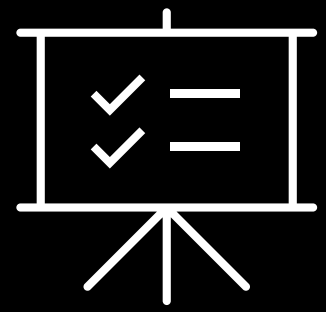
El Protocol Seqüencial d'Actuació davant l'Abús

Quan som víctimes directes d'un abús o d'un cas de ciberassetjament, s'ha de seguir una seqüència clara de passes:

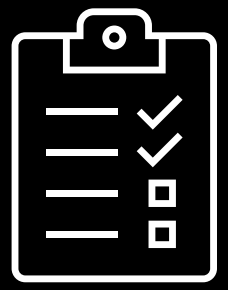
1. Aturar completament la interacció: Per cap motiu s'ha de respondre a insults o provocacions. Els agressors digitals cerquen la confrontació pública per augmentar la seva audiència o visibilitat; respondre només escala el nivell del conflicte.

2. Preservar proves irrefutables: Abans de procedir al bloqueig o a l'esborrament, hem d'assegurar-nos de fer captures de pantalla on es visualitzi de manera nítida el nom d'usuari de l'infractor, el contingut dels missatges, la data, l'hora i, si és possible, les adreces URL afectades. Aquestes proves seran indispensables si cal interposar una denúncia legal.

3. Demana ajuda i comunica l'abús: Cal comunicar la situació immediatament a una persona adulta de referència (pares, tutors, professorat de l'institut) per no fer front a la pressió emocional en solitud i rebre el guiatge necessari de cara a accions judicials o administratives de protecció.



5. Protecció i defensa dels drets digitals



Exercici: **Protocol de reacció davant d'un assetjament**

La Marina està rebent diàriament comentaris insultants i humiliants d'un compte anònim a les seves fotos d'Instagram. Està molt angoixada i us demana consell de com actuar. Ordeneu correctament de l'1 al 5 els següents passos del protocol recomanat d'actuació cívica i de seguretat digital:

A. Utilitzar l'opció oficial de la plataforma per bloquejar l'usuari anònim i fer un report/denúncia del seu compte per assetjament.

B. Demanar ajuda a un adult de confiança (els seus pares, un docent o el tutor de l'institut) i ensenyar-li les captures realitzades.

C. Fer captures de pantalla de tota la conversa i dels comentaris ofensius, incloent-hi l'adreça de perfil de l'assetjador, per conservar les proves del que ha passat.

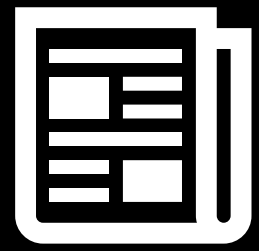
D. Evitar respondre o insultar de tornada el compte assetjador per no augmentar la gravetat de l'agressió verbal.

E. Si la situació no s'atura o constitueix una amenaça seriosa, posar-se en contacte amb la policia o entitats oficials d'ajuda al menor.

6. Detecció de notícies falses i perfils fraudulents

El fenomen de la desinformació

L'accés universal a la creació de continguts és un dels grans avantatges d'Internet, però també representa un dels seus perills més importants: la desinformació sistemàtica i la degradació dels espais comuns de diàleg provocada per usuaris que es dediquen exclusivament a sabotejar la comunicació saludable.



Fake News

- Moltes notícies o publicacions a xarxes es creen de manera deliberada i falsa per **motius econòmics** (rebre clics fàcils que generen publicitat: clickbait) o polítics (manipular les creences col·lectives o fomentar l'odi).
- Avui dia, tecnologies avançades com la Intel·ligència Artificial permeten crear fotografies, àudios i vídeos completament realistes de persones conegudes dient o fent coses que mai han succeït, un fenomen conegut com a **Deepfakes**.

6. Detecció de notícies falses i perfils fraudulents



El principi de verificació i el civisme de difusió

Com a usuaris digitals som corresponsables de la salut de la informació d'Internet. Reenviar un rumor alarmista, un consell mèdic miraculós o una notícia falsa "per si de cas és veritat" danya greument la societat. Abans de compartir qualsevol informació sorprenent o cridanera hem de fer una pausa de verificació (*fact-checking*):

- ✓ Comprovar si mitjans de comunicació oficials i contrastats en parlen.
- ✓ Verificar si la font que ho publica és una entitat oficial o un domini d'Internet estrany que suplanta una capçalera famosa.
- ✓ Utilitzar cercadors d'imatges inversos per comprovar si una fotografia correspon a un esdeveniment diferent de fa anys.

6. Detecció de notícies falses i perfils fraudulents

Els trols i la seva psicologia

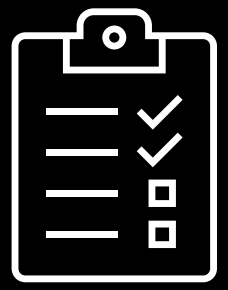
Un trol és un perfil d'usuari (sovint anònim) el propòsit del qual no és debatre de manera legítima, sinó generar enuig, polèmica, insults i reaccions negatives de ràbia o de frustració per divertiment personal o per boicotejar un grup.

La Regla d'Or: "No alimentis el trol"

La millor resposta civil davant d'un trol és ignorar-lo del tot. Respondre'ls amb enfadat, intentar argumentar lògicament amb ells o contestar els seus insults és donar-los exactament el que volen: atenció i polèmica. **Si el trol és ignorat de manera col·lectiva, acaba marxant del fòrum o del xat.** En casos on la conducta sigui d'odi, assetjament o atacs de difamació, s'ha de procedir directament a bloquejar-los, silenciar-los i reportar-los al canal d'ajuda de la plataforma.



6. Detecció de notícies falses i perfils fraudulents



Exercici: **Detectors de la Desinformació**

Llegeix amb atenció els següents dos casos i respon a les preguntes per posar a prova el teu ull crític de ciutadà digital:

Cas A (La Notícia)

El teu millor amic et reenvia pel xat de la classe un enllaç a una web desconeguda de notícies de poc prestigi. El titular diu:

"ALERTA! Un estudi científic secret de la NASA demostra que els exàmens de matemàtiques provoquen al·lèrgies físiques als menors de 16 anys. Comparteix-ho amb tota la teva classe ràpidament!"

1. Indica 2 alarmes de Fake News que té aquest missatge

2. Quina acció cívica hauries de prendre abans de reenviar el missatge a ningú?

6. Detecció de notícies falses i perfils fraudulents

Exercici: **Detectors de la Desinformació**

Cas B (El Comentari)

Un usuari amb un perfil sense foto ni seguidors escriu aquest comentari en una publicació de l'institut sobre les festes del barri:

"Aquesta festa és un fàstic total, tots els que hi aneu sou uns banyuts sense cervell. No teniu gust de res! Segur que la meitat dels nens s'hi posaran a plorar de vergonya. Vinga, contesteu-me i digueu-me si m'equivoco!"

1. A quin tipus de perfil problemàtic correspon aquest comportament digital?

2. Com s'anomena la regla d'or que cal aplicar en aquesta situació? Què s'hauria de fer en lloc de contestar-li?




barcelonactiva.cat