Autoavalua la ciberseguretat del teu projecte:

Ús segur dels dispositius.

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per a un ús més segur dels dispositius.

Recomanacions en ciberseguretat

Abril de 2025

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

Índex de continguts: ús segur dels dispositius

Avís de responsabilitat en la prevenció i protecció:
Les recomanacions incloses en aquesta guia tenen com a objectiu proporcionar consells pràctics i senzills per millorar la ciberseguretat del teu negoci. Tot i això, la **responsabilitat** última de la prevenció i protecció dels dispositius, dades i sistemes recau en els usuaris.

Es recomana comptar amb el suport d'un equip tècnic o servei informàtic especialitzat per garantir una implementació adequada de les mesures descrites. A més, assegura't de seguir sempre les instruccions oficials dels fabricants i desenvolupadors de software, aplicacions i dispositius que utilitzis, ja que cada sistema pot tenir requisits específics o actualitzacions que afectin la seva seguretat.

Aquest document no substitueix una auditoria professional de seguretat ni consells específics adaptats a les teves necessitats particulars.

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

1. Introducció

Importància de la seguretat en els dispositius tecnològics

En l'era digital actual, els dispositius tecnològics (telèfons mòbils, ordinadors, tauletes i altres dispositius intel·ligents) són eines indispensables per a la vida quotidiana i professional. Tanmateix, la seva omnipresència els converteix en objectius principals per a ciberatacs, robatoris d'informació i altres activitats malicioses.

Mantenir els dispositius segurs no només protegeix la informació personal o empresarial que contenen, sinó que també evita:

- **Filtracions de dades sensibles**: Informació com contrasenyes, dades financeres o documents privats poden ser robades.
- **Pèrdues econòmiques**: El robatori de dades o els atacs com el ransomware poden tenir un impacte econòmic important.
- **Danys a la reputació**: Una filtració de dades empresarials pot perjudicar la confiança dels clients i socis.
- **Interrupcions en el treball**: Dispositius afectats per malware o altres atacs poden quedar inutilitzables.

A més, la seguretat dels dispositius no només afecta l'usuari directe, sinó que pot tenir repercussions en altres persones o empreses com clients i proveidors o en els sistemes connectats a la mateixa xarxa.

Principals amenaces associades als dispositius insegurs

És fonamental conèixer les amenaces més comunes per entendre millor els riscos als quals estem exposats. Les següents són algunes de les més freqüents:

1. **Malware i virus**
   - Programes maliciosos dissenyats per infectar dispositius amb l'objectiu de robar dades, danyar el sistema o espiar l'usuari.
   - Exemples: troians, ransomware i spyware.
2. **Phishing**
   - Atacs que utilitzen enganys (generalment a través de correu electrònic, missatges o llocs web falsos) per aconseguir que l'usuari reveli informació sensible.
3. **Accés no autoritzat**
   - El robatori de contrasenyes o la manca de mesures de protecció permeten que persones no autoritzades accedeixin al dispositiu.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

4. **Connexió a xarxes insegures**
   - Utilitzar xarxes Wi-Fi públiques sense protecció adequada pot exposar els dispositius a interceptació de dades.
5. **Pèrdua o robatori físic**
   - La manca de mesures de protecció física pot permetre que tercers accedeixin al dispositiu de manera directa.
6. **Aplicacions no segures**
   - Instal·lar aplicacions de fonts no fiables pot introduir vulnerabilitats al sistema o accés no autoritzat a les dades.

Objectius d'aquesta guia

- Proporcionar una comprensió clara de les amenaces més comunes.
- Ensenyar mesures pràctiques per protegir els dispositius contra aquestes amenaces.
- Empoderar els usuaris perquè adoptin hàbits de seguretat que redueixin significativament els riscos.

2. Configuració inicial del dispositiu

La configuració inicial és un pas fonamental per assegurar els dispositius tecnològics des del primer moment. Una configuració adequada redueix considerablement el risc de ciberatacs o d'altres amenaces de seguretat.

2.1. Actualització del sistema operatiu i aplicacions

Una de les primeres accions a fer quan es posa en funcionament un dispositiu és assegurar-se que el sistema operatiu i totes les aplicacions estiguin actualitzades. Això és essencial perquè:

- **Les actualitzacions solen incloure pegats de seguretat** que solucionen vulnerabilitats descobertes.
- Els atacs sovint aprofiten aquestes vulnerabilitats en sistemes o aplicacions no actualitzades.

Bones pràctiques:

- Activa les **actualitzacions automàtiques** si és possible.
- Comprova regularment si hi ha noves actualitzacions per a aplicacions clau.
- Prioritza l'ús d'aplicacions que encara rebin suport actiu del fabricant.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

2.2. Configuració de contrasenyes i autenticació biomètrica

Les contrasenyes són la primera línia de defensa contra accessos no autoritzats. Una configuració inicial adequada implica:

- **Crear contrasenyes robustes**: Úniques, amb almenys 12 caràcters que incloguin lletres majúscules, minúscules, números i símbols.
- **Evitar contrasenyes predeterminades**: Els fabricants sovint utilitzen contrasenyes genèriques que són fàcils de descobrir.
- **Utilitzar autenticació multifactor (MFA)**: Afegir una capa extra de seguretat, com ara un codi enviat al telèfon o l'ús d'un lector d'empremtes dactilars.

Autenticació biomètrica:

- Si el dispositiu ho permet, configura opcions com l'empremta dactilar o el reconeixement facial, que són més segures que les contrasenyes senzilles.

2.3. Ajustament de les configuracions de privacitat

Molts dispositius venen amb configuracions predeterminades que poden exposar més dades del necessari. Revisa i ajusta les configuracions de privacitat:

- **Revoca permisos innecessaris**: Per exemple, impedeix que aplicacions tinguin accés a la ubicació, càmera o micròfon si no és imprescindible.
- **Controla la compartició de dades**: Desactiva opcions que comparteixin informació amb tercers sense el teu consentiment.
- **Personalitza les opcions de visibilitat**: Configura qui pot veure la teva activitat o interactuar amb tu (sobretot en xarxes socials o aplicacions de missatgeria).

2.4. Configuració del tallafocs i antivirus

Encara que alguns dispositius ja inclouen proteccions bàsiques, configurar un tallafocs i un programari antivirus és imprescindible:

- **Tallafocs**: Ajuda a bloquejar connexions no autoritzades cap al dispositiu.
- **Antivirus i antimalware**: Protegeix contra programes maliciosos que puguin infectar el dispositiu.

Assegura't d'instal·lar eines de seguretat d'un proveïdor de confiança i mantén-les sempre actualitzades.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

2.5. Configuració d'una còpia de seguretat automàtica

Per prevenir la pèrdua de dades en cas de fallada del dispositiu o atac cibernètic, configura una còpia de seguretat:

- **Opcions locals**: Còpies en discs durs externs o memòries USB.
- **Opcions al núvol**: Ús de serveis segurs com Google Drive, iCloud o OneDrive.
- **Freqüència**: Programa còpies regulars per garantir que les dades més recents estiguin protegides.

Beneficis d'una configuració inicial robusta

- Redueix el risc de vulnerabilitats explotables.
- Ofereix un control més gran sobre la privacitat i seguretat de les dades.
- Millora l'experiència de l'usuari amb un dispositiu més protegit i fiable.

3. Protecció física

La seguretat dels dispositius no només depèn de les mesures digitals; la protecció física és **igualment essencial per evitar robatoris, pèrdues o accessos no autoritzats**. Aquest apartat se centra en les accions necessàries per garantir que els dispositius estiguin físicament protegits en tot moment.

3.1. Seguretat contra robatoris i accessos no autoritzats

Els dispositius tecnològics solen ser objectius atractius per als lladres, tant pel seu valor com per la informació que contenen. Algunes mesures per evitar robatoris o accessos no autoritzats inclouen:

- **Evita deixar els dispositius sense supervisió**: Sobretot en llocs públics com cafeteries, biblioteques o aeroports.
- **Configura bloquejos automàtics**: Activa el bloqueig de pantalla després d'un període d'inactivitat breu (per exemple, 30 segons o 1 minut).
- **Utilitza una funda discreta**: Evita que el dispositiu cridi l'atenció per la seva marca o model.
- **No comparteixis els codis d'accés**: Mantingues les contrasenyes o patrons de desbloqueig només per al teu ús.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

3.2. Ús de bloqueigs físics i fundes protectores

La protecció física no només prevé robatoris, sinó que també redueix el risc de danys per cops o caigudes.

- **Cadenats de seguretat per portàtils**: Si utilitzes un ordinador portàtil en entorns compartits, considera l'ús d'un cadenat de seguretat que impedeixi que sigui retirat fàcilment.
- **Fundes resistents i protectors de pantalla**: Protegeixen el dispositiu contra cops, ratllades o altres danys accidentals.
- **Bateries i carregadors certificats**: Evita l'ús de components de mala qualitat que puguin sobreescalfar el dispositiu o danyar-lo.

3.3. Registre de dispositius i serveis de localització

En cas de robatori o pèrdua, tenir un registre dels dispositius i habilitar eines de localització pot facilitar-ne la recuperació:

- **Registra els dispositius**: Anota els números de sèrie, models i altres detalls útils. Això pot ser fonamental per informar a les autoritats o a l'asseguradora.
- **Activa la localització remota**: Configura serveis com "Troba el meu iPhone" (Apple), "Troba el meu dispositiu" (Android) o equivalents per a ordinadors. Això et permetrà localitzar, bloquejar o fins i tot esborrar les dades del dispositiu a distància.
- **Configura notificacions d'activitat sospitosa**: Alguns serveis t'avisen si el dispositiu es connecta a una ubicació no reconeguda.

3.4. Emmagatzematge segur dels dispositius

Quan no utilitzes els dispositius, és important guardar-los en llocs segurs:

- **Utilitza calaixos o armaris amb clau**: Especialment en entorns laborals o espais compartits.
- **Evita deixar els dispositius visibles**: Al cotxe, en llocs públics o fins i tot a la teva llar, mantenir els dispositius fora de la vista pot prevenir temptacions.

3.5. Transport segur dels dispositius

Portar els dispositius d'un lloc a un altre pot exposar-los a riscos, per la qual cosa cal prendre precaucions:

- **Utilitza motxilles o maletins amb compartiments dedicats**: Això protegeix els dispositius de pressions o cops.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Evita transportar dispositius amb bateries molt baixes**: En cas d'emergència, podries necessitar energia per localitzar el dispositiu o fer una còpia de seguretat.
- **Revisa les polítiques de seguretat de l'aeroport**: Si viatges, assegura't de mantenir els dispositius a mà i protegits durant les inspeccions.

Beneficis de la protecció física

- **Evita costos innecessaris**: Reparacions o substitucions de dispositius poden ser costoses.
- **Protegeix dades sensibles**: Un dispositiu físicament segur és menys vulnerable a la pèrdua d'informació.
- **Redueix l'estrès**: Saber que els teus dispositius estan protegits et dona tranquil·litat.

4. Seguretat en Xarxes

Connectar-se a xarxes de forma segura és essencial per evitar que terceres persones interceptin la informació que enviem o rebem. Aquest apartat ofereix bones pràctiques per protegir la connexió a Internet dels teus dispositius, **tant en entorns domèstics com públics**.

4.1. Connexió segura a xarxes Wi-Fi

Una connexió Wi-Fi no protegida adequadament pot ser un punt d'entrada per als ciberatacs. Algunes mesures clau són:

- **Configura un Wi-Fi segur a casa**:
  - **Utilitza contrasenyes fortes** per al teu router. Evita contrasenyes predeterminades o senzilles.
  - Activa el xifrat **WPA3** (o WPA2 si WPA3 no està disponible), que és més segur que protocols com WEP.
  - Canvia el nom de la xarxa (SSID) per un que no identifiqui clarament el teu dispositiu o ubicació.
- **Desactiva la difusió pública del SSID** si no és necessari.
- **Revisa els dispositius connectats**: Comprova regularment quins dispositius estan connectats al teu router i elimina aquells desconeguts.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

4.2. Evitar xarxes públiques no segures

Les xarxes Wi-Fi públiques, com les de cafeteries, aeroports o hotels, són especialment vulnerables a atacs, ja que no solen estar protegides.

- **Evita connectar-te a xarxes obertes** sense contrasenya o xifrat.
- Si necessites utilitzar una xarxa pública:
  - Evita accedir a llocs amb dades sensibles, com ara comptes bancaris o botigues en línia.
  - Utilitza una **VPN (xarxa privada virtual)** per xifrar la connexió.
- **Desactiva la connexió automàtica a xarxes Wi-Fi** en el teu dispositiu:
  - Aquesta opció impedeix que el dispositiu es connecti a xarxes no segures sense que tu te n'adonis.

4.3. Ús de VPN en dispositius mòbils i portàtils

Una VPN (Virtual Private Network) és una eina que protegeix la teva connexió a Internet xifrant totes les dades enviades i rebudes. És especialment útil en xarxes públiques o en llocs on la seguretat de la xarxa és dubtosa.

- **Avantatges de la VPN**:
  - Protegeix les teves dades contra espies.
  - Amaga la teva adreça IP, millorant la privacitat.
  - Permet accedir a contingut restringit geogràficament de forma segura.
- **Com triar una bona VPN**:
  - Assegura't que utilitzi protocols segurs com OpenVPN.
  - Tria un proveïdor de confiança que no emmagatzemi registres de la teva activitat.

4.4. Configuració de tallafocs

El tallafocs actua com un filtre entre el teu dispositiu i Internet, bloquejant connexions sospitoses o no autoritzades.

- **Activa el tallafocs al teu router**: La majoria dels routers tenen un tallafocs integrat que pots configurar fàcilment.
- **Configura el tallafocs al dispositiu**: Els sistemes operatius com Windows o macOS inclouen tallafocs integrats que es poden activar i personalitzar.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

4.5. Navegació segura

La seguretat a les xarxes també implica protegir les dades mentre navegues per Internet.

- **Utilitza llocs web amb HTTPS**: Comprova que els llocs web que visites utilitzen el protocol segur HTTPS (mostrat amb un candau al navegador).
- **Activa bloquejadors de publicitat i extensions de seguretat**: Aquestes eines poden protegir-te contra llocs web maliciosos o programari espia.
- **Evita fer clic en enllaços sospitosos**: Fes servir el sentit comú per no accedir a enllaços o llocs web que no coneguis.

4.6. Monitorització de la xarxa

Controlar l'activitat de la xarxa pot ajudar-te a detectar possibles amenaces.

- Utilitza eines per monitoritzar la xarxa del router i identificar dispositius no autoritzats.
- Revisa l'activitat de la xarxa periòdicament per assegurar-te que no hi ha cap activitat inusual.

Beneficis de la seguretat en xarxes

- **Protecció de dades sensibles**: Garanteix que la informació privada no sigui interceptada.
- **Reducció del risc d'atacs**: Minimitza les oportunitats per als ciberdelinqüents.
- **Privacitat millorada**: Protegeix la teva identitat i activitat en línia.

5. Instal·lació i Ús d'Aplicacions

Les aplicacions són eines essencials per treballar, comunicar-nos i gestionar les nostres activitats diàries. No obstant això, cada aplicació instal·lada en un dispositiu pot suposar un risc si no es selecciona, configura i utilitza amb precaució. Aquest apartat detalla com assegurar que les aplicacions no es converteixin en punts vulnerables.

5.1. Descàrrega d'aplicacions des de fonts fiables

Instal·lar aplicacions de fonts no verificades és una de les formes més comunes d'introduir malware o altres amenaces en un dispositiu.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Utilitza botigues oficials**: Com Google Play Store, Apple App Store o el lloc web oficial del proveïdor.
- **Evita arxius APK descarregats** d'Internet o aplicacions que no provinguin de fonts reconegudes (les botigues d'aplicacions), ja que poden contenir codi maliciós.
- **Revisa les ressenyes i valoracions**: Això pot ajudar a detectar aplicacions problemàtiques o fraudulentes.
- **Comprova la identitat del desenvolupador**: Assegura't que sigui un proveïdor de confiança.

5.2. Configuració de permisos adequats

Les aplicacions solen demanar permisos per accedir a funcions o dades del dispositiu, però alguns d'aquests permisos poden no ser necessaris per al seu funcionament.

- **Revisa els permisos durant la instal·lació**:
  - Denega els permisos que semblin innecessaris (per exemple, una aplicació de jocs no necessita accés a la teva agenda).
  - Configura manualment els permisos a la configuració del dispositiu.
- **Actualitza periòdicament els permisos**:
  - A mesura que una aplicació es modernitza, pot sol·licitar nous permisos. Revisa i ajusta aquestes sol·licituds.
  - Desactiva els permisos d'aplicacions que ja no utilitzes sovint.

5.3. Actualització constant del programari

Les aplicacions obsoletes poden contenir vulnerabilitats de seguretat que els atacants poden explotar.

***Activa les actualitzacions automàtiques**: Això garanteix que les aplicacions es mantinguin actualitzades amb els últims pegats de seguretat.

*Si no vols actualitzar automàticament, **comprova periòdicament** si hi ha actualitzacions disponibles.

*Elimina les aplicacions que ja no rebin suport o actualitzacions del desenvolupador.

5.4. Evita les aplicacions excessivament intrusives

Algunes aplicacions poden recopilar grans quantitats de dades sense necessitat.

- **Llegeix les polítiques de privacitat** abans d'instal·lar una aplicació.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Evita les aplicacions amb excessives sol·licituds de dades** personals o sensibles.
- Si una aplicació ofereix funcions innecessàriament gratuïtes, considera si això pot estar compensat per una recopilació agressiva de dades.

5.5. Utilització d'aplicacions de seguretat

Hi ha aplicacions específiques dissenyades per millorar la seguretat dels teus dispositius.

- **Antivirus i antimalware**: Protegeix contra aplicacions malicioses instal·lades accidentalment.
- **Gestors de contrasenyes**: Emmagatzema i genera contrasenyes segures.
- **Aplicacions de monitoratge**: Detecta comportaments sospitosos d'altres aplicacions.

5.6. Auditories periòdiques de les aplicacions

Per garantir que només tens instal·lades aplicacions útils i segures:

- **Fes una revisió periòdica** de les aplicacions instal·lades:
  - Elimina les que ja no utilitzes.
  - Comprova les que ocupen més recursos del dispositiu o consum de bateria sense raó aparent.
- **Desinstal·la les aplicacions duplicades** o de funcionalitat similar per reduir riscos i optimitzar recursos.

5.7. Protecció contra aplicacions falses o fraudulentes

Les aplicacions fraudulentes intenten semblar legítimes però poden estar dissenyades per robar dades.

- **Comprova el nombre de descàrregues**: Les aplicacions fiables solen tenir un alt nombre de descàrregues.
- **Fixa't en detalls sospitosos**: Errors d'ortografia al nom, logotips poc professionals o descripcions incompletes poden ser indicadors d'un frau.
- **Denuncia aplicacions sospitoses** a la botiga oficial del teu dispositiu.

Beneficis d'un ús segur de les aplicacions

- **Protecció de dades**: Redueixes la probabilitat que les teves dades personals o sensibles es filtrin.
- **Evites malware**: Minimitzes el risc d'infeccions o danys al dispositiu.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Optimització del rendiment**: Les aplicacions segures i actualitzades funcionen millor i consumeixen menys recursos.

6. Xifrat de dades

El xifrat de dades és una de les mesures de seguretat més eficients per protegir la informació sensible dels teus dispositius. Aquesta tècnica converteix les dades en un format il·legible per a qualsevol persona que no tingui la clau d'accés, impedint que siguin utilitzades en cas de robatori o accés no autoritzat.

Nota important: Les eines llistades en aquesta guia són exemples representatius i no les úniques opcions. T'invitem a explorar alternatives que s'ajustin millor al teu negoci, pressupost i necessitats de projecte de

6.1. Activació del xifrat en discos i dispositius mòbils

La majoria dels dispositius moderns ofereixen opcions per xifrar les dades d'emmagatzematge intern.

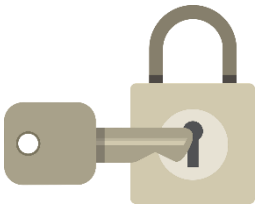
- **En dispositius mòbils**:
  - En dispositius Android:
    - Vés a **Configuració > Seguretat > Xifrat** i activa el xifrat complet del dispositiu si no està habilitat per defecte.
    - Alguns dispositius ja venen amb el xifrat activat de manera automàtica.
  - En dispositius iOS:
    - El xifrat està activat per defecte si tens una contrasenya o autenticació biomètrica configurada.
- **En ordinadors**:
  - Windows:
    - Utilitza **BitLocker** (només disponible en edicions Pro i Enterprise).
    - Habilita el xifrat accedint a **Configuració > Sistema > Xifrat de dispositius**.
  - macOS:
    - Activa **FileVault** a **Preferències del sistema > Seguretat i privacitat > FileVault**.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

6.2. Pràctiques recomanades per a la gestió de les claus de xifrat

Les claus de xifrat són imprescindibles per accedir a les dades protegides. Una mala gestió d'aquestes claus pot deixar les dades vulnerables.



- **Emmagatzema les claus de forma segura**:
  - Utilitza gestors de contrasenyes per guardar les claus d'accés.
  - No deixis les claus emmagatzemades al mateix dispositiu que xifres.
- **Crea còpies de seguretat de les claus**:
  - Guarda-les en ubicacions separades (per exemple, en un dispositiu extern o en un paper guardat en un lloc segur).
- **Evita compartir les claus**: Només tu o persones de confiança heu de tenir accés a les claus.

6.3. Avantatges del xifrat de dades

El xifrat ofereix una capa de protecció extra que minimitza els riscos de seguretat:

- **Protecció en cas de robatori o pèrdua del dispositiu**:
  - Si un dispositiu xifrat és robat, el lladre no podrà accedir a les dades sense la clau.
- **Confidencialitat**:
  - Garanteix que només els usuaris autoritzats puguin accedir a la informació.
- **Compliment normatiu**:
  - Moltes normatives de protecció de dades, com el RGPD, recomanen o exigeixen el xifrat per protegir dades sensibles.

6.4. Limitacions i precaucions

Tot i els beneficis del xifrat, cal tenir en compte algunes precaucions:

- **Pèrdua de claus**:
  - Si perds la clau d'accés, no podràs recuperar les dades. Per això és essencial gestionar-les correctament.
- **Impacte en el rendiment**:
  - En dispositius més antics, el xifrat pot reduir lleugerament el rendiment del sistema.
- **Compatibilitat**:
  - Comprova que el dispositiu o aplicacions siguin compatibles amb les eines de xifrat.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

6.5. Casos pràctics d'ús

- **Empresa**:
  - Xifrar ordinadors portàtils amb informació confidencial d'empleats o clients.
  - Protegir discos externs utilitzats per fer còpies de seguretat.
- **Ús personal**:
  - Xifrar fotos, documents o arxius sensibles per evitar que caiguin en mans equivocades en cas de pèrdua del dispositiu.

Beneficis generals del xifrat

- **Seguretat reforçada**: Les dades són pràcticament inaccessibles per a tercers sense autorització.
- **Tranquil·litat**: Saber que les teves dades estan protegides, fins i tot en situacions inesperades.
- **Compliment legal i ètic**: Especialment important per a negocis que treballen amb dades personals.

7. Gestió de dispositius

La gestió adequada dels dispositius tecnològics és essencial per garantir la seva seguretat i eficiència. Mantenir un **registre actualitzat de tots el dispositius a l'empresa** (telèfons, ordinadors, impressores, etc.), utilitzar eines de control i aplicar polítiques clares permet reduir riscos i millorar el rendiment.

Per tenir un millor control dels dispositius, és fonamental mantenir un registre detallat que inclogui:

- **Informació bàsica**:
  - Model, número de sèrie i tipus de dispositiu.
  - Sistema operatiu i versió instal·lada.
- **Propietari i ús**:
  - Qui utilitza el dispositiu i amb quina finalitat.
  - Data d'adquisició i últim manteniment.
- **Historial d'incidències**:
  - Problemes tècnics, reparacions o altres incidències relacionades amb el dispositiu.

Aquest registre ajuda a identificar ràpidament qualsevol pèrdua, robatori o dispositiu que necessiti actualitzacions o manteniment.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

7.2. Polítiques d'ús acceptables

Establir polítiques clares d'ús dels dispositius és essencial per evitar males pràctiques o usos inadequats que puguin comprometre la seguretat.

- **Per a entorns professionals**:
  - Prohibeix la instal·lació d'aplicacions no autoritzades.
  - Limita l'accés a dades sensibles segons el rol de cada usuari.
  - Defineix normes sobre l'ús de dispositius personals per accedir a xarxes empresarials.
- **Per a ús personal o familiar**:
  - Estableix regles sobre la descàrrega d'aplicacions.
  - Evita l'ús compartit de dispositius amb persones desconegudes.
  - Configura perfils separats per a nens o altres membres de la família.

7.3. Gestió de dispositius obsolets

Els dispositius antics poden representar un risc de seguretat si no es gestionen correctament.

- **Revisa periòdicament els dispositius**:
  - Identifica equips que ja no reben actualitzacions del sistema operatiu.
  - Substitueix els dispositius que ja no poden suportar les últimes mesures de seguretat.
- **Elimina dades abans de desfer-te d'un dispositiu**:
  - Fes un esborrat segur de totes les dades.

7.4. Estratègies per a l'organització de dispositius

En entorns amb molts dispositius, és útil aplicar mesures per simplificar-ne la gestió:

- **Etiqueta els dispositius físicament**:
  - Utilitza adhesius o gravats amb identificadors únics.
- **Classificació digital**:
  - Assigna noms clars i consistents als dispositius en les xarxes per facilitar-ne la identificació.
- **Estableix un responsable de la seguretat**:
  - Designa una persona o equip per supervisar la gestió de dispositius en entorns professionals.

Beneficis de la gestió de dispositius

- **Millor seguretat**:
  - Permet identificar ràpidament dispositius vulnerables o perduts.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Optimització de recursos**:
  - Ajuda a mantenir el rendiment i l'actualització dels equips.
- **Compliment normatiu**:
  - Redueix riscos legals associats a la protecció de dades.

8. Seguretat en cas de pèrdua o robatori de dispositius

En cas de pèrdua o robatori d'un dispositiu, és fonamental disposar de mesures preventives i eines per reduir l'impacte d'aquest incident. Aquest apartat detalla les accions necessàries per protegir les dades i, si és possible, recuperar el dispositiu.

Nota important: Les eines llistades són exemples representatius i no les úniques opcions. T'invitem a explorar alternatives que s'ajustin millor al teu negoci, pressupost i necessitats de projecte de negoci.

8.1. Configuració d'eines per localitzar i bloquejar dispositius

Activar eines de localització i control remot és la primera línia de defensa en cas de pèrdua o robatori. La majoria dels dispositius inclouen funcionalitats integrades per localitzar-los.

- **Dispositius mòbils**:
  - **iOS**:
    - Activa "Troba el meu iPhone" des de **Configuració > [el teu nom] > Troba**.
    - Permet localitzar el dispositiu, fer que emeti un so, bloquejar-lo o esborrar-lo a distància.
  - **Android**:
    - Activa "Troba el meu dispositiu" a **Configuració > Seguretat > Troba el meu dispositiu**.
    - Ofereix funcionalitats similars, com localitzar, bloquejar o esborrar les dades remotament.
- **Ordinadors**:
  - **Windows**:
    - Activa "Troba el meu dispositiu" des de **Configuració > Actualització i seguretat > Troba el meu dispositiu**.
  - **macOS**:
    - Activa "Troba el meu Mac" des de **Preferències del sistema > ID d'Apple > iCloud**.
- **Dispositius de tercers**:
  - Utilitza etiquetes intel·ligents com **AirTag** o **Tile** per localitzar objectes físics, incloent portàtils o accessoris.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

8.2. Eliminació remota de dades

En cas que el dispositiu no es pugui recuperar, és essencial garantir que les dades no puguin ser accedides.

- Activa opcions d'eliminació remota:
  - **iOS** i **Android**: L'eina de localització inclou una opció per esborrar totes les dades del dispositiu.
  - **Ordinadors**:
    - Utilitza serveis de gestió remota com **Microsoft Intune**, **Prey** o eines similars per esborrar dades de forma remota.
- **Consells addicionals**:
  - Les dades emmagatzemades al núvol no es veuran afectades si elimines el contingut local. Assegura't de protegir el compte del núvol amb contrasenyes fortes i autenticació multifactor.

8.3. Procediments en cas de pèrdua o robatori

Enfrontar-se a la pèrdua d'un dispositiu pot ser estressant, però seguir un procediment clar ajuda a mitigar els riscos.

1. **Localitza el dispositiu**:
   - Utilitza les eines de localització activades prèviament.
   - Si el dispositiu està en una ubicació propera, fes-lo sonar per trobar-lo més fàcilment.
2. **Bloqueja el dispositiu**:
   - Activa el bloqueig remot per evitar que ningú pugui accedir a les teves dades.
3. **Informa a les autoritats**:
   - Denuncia el robatori a la policia, facilitant el número de sèrie del dispositiu.
   - Proporciona informació de localització si en tens disponible.
4. **Notifica al teu proveïdor de serveis**:
   - Si el dispositiu robat conté una SIM, contacta amb la teva operadora per bloquejar la línia i evitar abusos.
5. **Actualitza contrasenyes**:
   - Canvia immediatament les contrasenyes dels comptes vinculats al dispositiu, especialment aquells amb accés a dades sensibles o financeres.

8.4. Mesures preventives per reduir l'impacte

És millor prevenir que curar, per això és important tenir en compte aquestes mesures abans que es produeixi un incident:

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Còpies de seguretat regulars**:
  - Configura còpies automàtiques per assegurar-te que no perdràs dades importants encara que perdis el dispositiu.
- **Protecció amb contrasenya i xifrat**:
  - Configura bloqueigs de pantalla i activa el xifrat complet del dispositiu per impedir que s'accedeixi a les dades.
- **Autenticació multifactor**:
  - Activa l'autenticació multifactor als comptes per dificultar l'accés en cas que la contrasenya sigui compromesa.
- **Etiquetatge físic**:
  - Afegeix una etiqueta amb el teu número de contacte al dispositiu (sense informació sensible) per facilitar-ne la devolució si algú el troba.

Beneficis d'una bona gestió en cas de pèrdua

- **Reducció de riscos**: Assegures que les teves dades no puguin ser utilitzades per tercers.
- **Recuperació més ràpida**: Les eines de localització augmenten les possibilitats de trobar el dispositiu.
- **Tranquil·litat**: Saber que tens un pla preparat et permet reaccionar de manera més efectiva davant de situacions inesperades.

9. Educació i sensibilització dels usuaris

La tecnologia pot ser robusta i segura, però els errors humans continuen sent una de les principals causes d'incidents de seguretat. Per aquest motiu, educar i sensibilitzar els usuaris és essencial per reduir riscos i fomentar bones pràctiques en l'ús dels dispositius.

9.1. Formació sobre pràctiques segures

Una formació bàsica en seguretat digital ajuda els usuaris a identificar riscos i a actuar correctament.

- **Temes clau a incloure en la formació**:
  - Com crear contrasenyes segures i utilitzar gestors de contrasenyes.
  - Identificació d'enllaços sospitosos, correus electrònics de phishing o llocs web fraudulents.
  - Importància de mantenir el dispositiu actualitzat.
  - Com protegir dades sensibles amb xifrat i còpies de seguretat.
- **Metodologies efectives**:
  - Sessions formatives presencials o en línia.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- Tallers pràctics amb exemples reals.
- Manuals o guies visuals amb passos senzills.

9.2. Identificació d'amenaces comunes

Capacitar els usuaris per reconèixer amenaces habituals és fonamental per prevenir incidents. Alguns dels riscos més comuns inclouen:

- **Phishing**:
  - Correus electrònics o missatges que intenten enganyar l'usuari per obtenir dades personals o financeres.
  - Recomanació: Comprovar sempre l'adreça de l'emissor i evitar clicar en enllaços sospitosos.
- **Malware i ransomware**:
  - Aplicacions malicioses que poden danyar el dispositiu o xifrar les dades per exigir un rescat.
  - Recomanació: Evitar instal·lar aplicacions de fonts no fiables i mantenir l'antivirus actualitzat.
- **Enganys en xarxes socials**:
  - Suplantacions d'identitat o missatges que sol·liciten informació personal.
  - Recomanació: Verificar la identitat dels contactes i evitar compartir informació confidencial.

9.3. Importància de reportar incidents ràpidament

Un error comú és intentar amagar o ignorar un incident per vergonya o por. Sensibilitzar els usuaris sobre la importància de reportar incidents a temps és clau per mitigar els danys.

- **Comunicació immediata**:
  - Els usuaris haurien de notificar qualsevol sospita d'incident, com un correu electrònic estrany o un comportament inusual del dispositiu.
  - Recorda que tens a la teva disposició **el telèfon nacional, gratuït, confidencial** i de suport 017 de l'INCIBE i que funciona de manera gratuïta per a empreses i persones físiques tots els dies de l'any.
- **Protocols clars**:
  - Proporciona un procés senzill per informar incidents (telèfon, correu electrònic o aplicació específica).
- **Exemples d'incidents a reportar**:
  - Pèrdua o robatori del dispositiu.
  - Descàrrega accidental d'una aplicació sospitosa.
  - Rebre missatges o correus amb contingut dubtós.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

9.4. Creació d'una cultura de seguretat en la teva empresa

La formació puntual és útil, però el més efectiu és fomentar una cultura de seguretat contínua en la teva pròpia organització.

- **Incorporar bones pràctiques al dia a dia**:
  - Recordatoris periòdics sobre actualitzacions o canvis de contrasenya.
  - Promoció de l'ús d'eines com VPN o xifrat en entorns no segurs.
- **Reconeixement d'iniciatives individuals**:
  - Valora i recompensa els usuaris de la teva empresa que adoptin bones pràctiques de seguretat.
- **Compartició de casos reals**:
  - Explica exemples d'incidents cibernètics que hagin afectat altres organitzacions o persones per reforçar la importància de la prevenció.

Beneficis d'educar i sensibilitzar els usuaris

- **Reducció d'errors humans**:
  - Els usuaris formats són menys propensos a caure en trampes com el phishing o l'execució de malware.
- **Millora de la seguretat general**:
  - Amb més coneixement, els usuaris prenen millors decisions, protegint no només els seus dispositius sinó també les xarxes a les quals estan connectats.
- **Reaccions més ràpides i efectives**:
  - Els usuaris conscienciats reporten incidents amb més rapidesa, minimitzant l'impacte de qualsevol amenaça.

Generalitat de Catalunya
SEPE
emfosi
Ajuntament de Mollet del Vallès
Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

10.Preguntes d'autoavaluació

L'autoavaluació és una eina clau per **comprovar si estàs aplicant correctament les mesures de seguretat descrites en aquesta guia**. A través d'aquesta secció, podràs identificar punts febles i obtenir recomanacions específiques per millorar.

10.1. Llista de verificació (Checklist dels conceptes principals)

Respon les següents preguntes amb **Sí** o **No**. Si la resposta és "No" a alguna d'elles, revisa l'apartat corresponent de la guia per implementar les millores necessàries.

Dispositius i configuració inicial

1. Tens el sistema operatiu i totes les aplicacions actualitzades?
2. Els teus dispositius estan protegits amb contrasenyes segures o autenticació biomètrica?
3. Has revisat i ajustat les configuracions de privacitat dels teus dispositius?

Protecció física

4. Mantens els dispositius en llocs segurs quan no els utilitzes?
5. Utilitzes fundes protectores o mecanismes de bloqueig físic en portàtils o altres dispositius?

Connexions a xarxes

6. Només et connectes a xarxes Wi-Fi segures i confiables?
7. Utilitzes una VPN en connexions públiques o no segures?

Ús d'aplicacions

8. Només instal·les aplicacions de botigues oficials o fonts verificades?
9. Revisa regularment els permisos de les aplicacions instal·lades?
10. Totes les teves aplicacions estan actualitzades?

Xifrat i protecció de dades

11. Els teus dispositius tenen el xifrat activat?
12. Fas còpies de seguretat periòdiques de les dades més importants?

Gestió de dispositius

13. Tens un registre dels teus dispositius amb informació bàsica (model, número de sèrie, etc.)?
14. Estàs preparat per localitzar o esborrar dades remotament en cas de pèrdua o robatori?

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

15. Saps identificar correus electrònics o missatges sospitosos?
16. Coneixes el procediment per reportar incidents de seguretat?

10.2. Escala d'autoavaluació

0-5 respostes amb un SI: Nivell de risc alt

- Estàs exposat a múltiples amenaces de seguretat.
- Recomanació: Comença per implementar mesures bàsiques, com configurar contrasenyes segures, actualitzar dispositius i utilitzar una VPN.

6-10 respostes afirmatives: Nivell de risc moderat

- Ja tens algunes mesures aplicades, però encara hi ha riscos importants.
- Recomanació: Prioritza millorar els punts febles detectats, especialment en protecció física i configuracions de privacitat.

11-15 respostes afirmatives: Nivell de risc baix

- Tens una bona gestió de la seguretat, però encara pots perfeccionar aspectes clau.
- Recomanació: Assegura't d'estar preparat per gestionar situacions d'emergència com la pèrdua d'un dispositiu.

16 respostes afirmatives: Excel·lent

- Felicitats! Tens un alt nivell de seguretat en els teus dispositius i pràctiques digitals.
- Recomanació: Mantingues els bons hàbits i segueix actualitzat sobre noves amenaces i eines de protecció.

10.3. Recursos addicionals

Per millorar en les àrees on has detectat mancances, pots consultar recursos addicionals com:

- **Guies oficials de fabricants**: Per configurar opcions de seguretat als teus dispositius.
- **Eines de formació en línia**: Curs gratuïts sobre ciberseguretat en plataformes d'aprenentatge de centres com l'Agència de Ciberseguretat de Catalunya o l'Institut Nacional de Ciberseguretat.
- **Suport i assistència**: contacta amb el telèfon d'atenció a Catalunya, el CATALONIA-CERT o bé amb el servei nacional de l'INCIBE.

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local