Autoavalua la ciberseguretat del teu projecte:

Guia per a la prevenció de ciberseguretat en telèfons mòbils i tauletes

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per mantenir segurs els teus dispositius mòbils i tauletes.

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:

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

1.1. Importància de la ciberseguretat en dispositius mòbils i tauletes

Els telèfons mòbils i tauletes són eines essencials per a petites empreses i autònoms. S'utilitzen per gestionar correus electrònics, accedir a comptes bancaris, emmagatzemar dades de clients i fins i tot per dur a terme vendes i facturacions. Tot i això, aquests dispositius són sovint menys protegits que els ordinadors, fet que els converteix en un objectiu fàcil per als ciberdelinqüents.

- **Per què és crucial protegir-los?**
  - **Volum d'informació:** Contenen dades personals, empresarials i financeres que poden ser sensibles.
  - **Connectivitat constant:** Es connecten a xarxes públiques, privades i a Internet, augmentant el risc d'exposició.
  - **Menys atenció a la seguretat:** Sovint no es prenen les mateixes mesures de seguretat en dispositius mòbils que en ordinadors.
- **Quins beneficis aporta la ciberseguretat mòbil?**
  - Evita robatoris d'informació confidencial de clients o de l'empresa.
  - Protegeix dades financeres, com comptes bancaris o aplicacions de pagament.
  - Garanteix la continuïtat del negoci, evitant interrupcions per problemes de seguretat.

1.2. Principals riscos per a petites empreses i autònoms

Els petits empresaris i autònoms són objectius atractius per als atacants perquè sovint tenen menys recursos per dedicar a la ciberseguretat.

- **Riscos més comuns:**
  1. **Aplicacions malicioses:**
     - Aplicacions descarregades de fonts no oficials poden contenir programari espia o malware.
  2. **Connexions a xarxes no segures:**
     - Utilitzar Wi-Fi públiques sense protecció pot exposar dades sensibles a tercers.
  3. **Robatori o pèrdua del dispositiu:**
     - Si un dispositiu amb accés a dades empresarials es perd o és robat, tota la informació pot quedar compromesa.

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

4. **Phishing mòbil:**
    - Atacs dissenyats per enganyar l'usuari perquè reveli informació confidencial, sovint a través de correus electrònics, missatges de text o aplicacions de missatgeria.
5. **Accés no autoritzat:**
    - La manca de protecció amb contrasenyes robustes o autenticació multifactor facilita que qualsevol pugui accedir a les dades.

- **Impactes d'aquests riscos:**
    - **Pèrdua de dades:** Informació crítica de clients o finances pot ser eliminada o robada.
    - **Interrupcions del negoci:** Un atac pot paralitzar l'activitat fins que es resolgui el problema.
    - **Reputació danyada:** Els clients poden perdre confiança si les seves dades es veuen compromeses.

Objectius d'aquesta guia

Amb aquesta guia, aprendràs:

1. A implementar mesures pràctiques per protegir els teus dispositius mòbils i tauletes.
2. A evitar riscos comuns, com el phishing o el malware.
3. A mantenir les dades empresarials i personals segures en tot moment.

2. Configuracions bàsiques de ciberseguretat

Adoptar configuracions bàsiques de seguretat és el primer pas per protegir els telèfons mòbils i tauletes. Aquestes accions són senzilles, però molt efectives per evitar riscos.

2.1. Com configurar un bloqueig de pantalla segur

Un bloqueig de pantalla adequat és una de les defenses més importants per impedir l'accés no autoritzat al dispositiu.

- **Opcions de bloqueig disponibles:**
    1. **Contrasenya o PIN robust:**
        - Utilitza un PIN d'almenys 6 dígits o una contrasenya alfanumèrica que no sigui fàcil de deduir (evita dates de naixement o seqüències simples com "1234").

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

2. **Autenticació biomètrica:**
    - Si el dispositiu ho permet, activa el reconeixement facial o d'empremta dactilar per augmentar la seguretat.
3. **Patró de desbloqueig:**
    - Només recomanat si és complex i no deixa rastre visible al vidre del dispositiu.

- **Com activar-lo:**
    - **Android:** Configuració > Seguretat > Bloqueig de pantalla > Tria PIN, contrasenya o biometria.
    - **iOS:** Configuració > Face ID i codi > Configura el codi o Face ID.
- **Consell addicional:**
    - Configura un bloqueig automàtic del dispositiu després d'un període d'inactivitat (p. ex., 30 segons o 1 minut).

2.2. Activació de xifrat de dades i còpies de seguretat automàtiques

El xifrat i les còpies de seguretat protegeixen les dades del dispositiu en cas de pèrdua, robatori o atac.

- **Xifrat de dades:**
    - El xifrat converteix la informació en un format il·legible per a tercers sense autorització.
    - **Android:** La majoria de dispositius moderns ja tenen el xifrat activat per defecte. Pots comprovar-ho a Configuració > Seguretat > Xifrat de dades.
    - **iOS:** Els dispositius tenen el xifrat activat automàticament si utilitzes Face ID, Touch ID o un codi d'accés.
- **Còpies de seguretat automàtiques:**
    - Configura el dispositiu perquè faci còpies de seguretat periòdiques al núvol o a un dispositiu extern.
    - **Android:**
        - Configuració > Comptes i còpia de seguretat > Google Drive > Activa "Còpia de seguretat automàtica".
    - **iOS:**
        - Configuració > [El teu nom] > iCloud > Còpia de seguretat d'iCloud > Activa "Còpia de seguretat".
- **Consell addicional:**
    - Verifica regularment que les còpies de seguretat s'estan realitzant correctament.

2.3. Actualització del sistema operatiu i aplicacions

Els sistemes operatius i les aplicacions sovint inclouen actualitzacions amb pegats de seguretat per protegir contra noves amenaces.

- **Per què és important?**

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

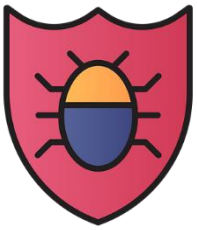
  - Les actualitzacions solucionen vulnerabilitats que els atacants poden utilitzar.
  - Garanteixen que el dispositiu i les aplicacions funcionen correctament.
- **Com configurar actualitzacions automàtiques:**
  - **Android:**
    - Configuració > Sistema > Actualitzacions del sistema > Activa les actualitzacions automàtiques.
    - Per aplicacions: Google Play Store > Configuració > Actualitza aplicacions automàticament.
  - **iOS:**
    - Configuració > General > Actualització de programari > Activa "Actualitza automàticament".
    - Per aplicacions: Configuració > App Store > Activa "Actualitzacions automàtiques".

- **Consell addicional:**
  - Comprova regularment si hi ha actualitzacions pendents, especialment per aplicacions clau com navegadors, eines financeres o gestors de contrasenyes.

Beneficis d'aquestes configuracions

- **Protecció bàsica:** Bloqueja l'accés no autoritzat i protegeix les dades en cas de pèrdua o robatori.
- **Continuïtat del negoci:** Les còpies de seguretat garanteixen que les dades es poden recuperar fàcilment.
- **Prevenció d'atacs:** Les actualitzacions tanquen les portes als atacants que aprofiten vulnerabilitats.

3. Protecció contra aplicacions malicioses



Les aplicacions malicioses són una de les principals fonts d'infecció per malware en telèfons mòbils i tauletes. Aquest apartat t'ajudarà a identificar i evitar aquestes amenaces, així com a gestionar de manera segura les aplicacions que utilitzes.

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

3.1. Com identificar i evitar aplicacions sospitoses

Les aplicacions sospitoses poden semblar legítimes, però sovint estan dissenyades per robar dades, introduir malware o comprometre la seguretat del dispositiu.

- **Senyals d'advertència:**
  1. **Poca reputació:**
     - Les aplicacions amb poques descàrregues o sense ressenyes podrien ser sospitoses.
  2. **Permissions excessives:**
     - Si una app demana accés a funcions no relacionades amb el seu ús (per exemple, una app de llanterna que sol·licita accés a la càmera o contactes).
  3. **Errors gramaticals o traduccions pobres:**
     - Les aplicacions malicioses solen tenir descripcions i interfícies poc professionals.
  4. **Llocs web o fonts no oficials:**
     - Descarregar aplicacions fora de botigues oficials augmenta el risc d'infecció.
- **Com evitar-les:**
  - Llegeix les ressenyes i puntuacions abans de descarregar una aplicació.
  - Comprova el nom del desenvolupador i assegura't que sigui legítim.
  - Evita instal·lar aplicacions suggerides per anuncis emergents o correus electrònics.

3.2. Normes per descarregar apps de manera segura

Descarregar apps de manera segura és un pas crucial per mantenir protegits els dispositius.

- **Descarrega només de botigues oficials:**
  - **Android:** Google Play Store.
  - **iOS:** App Store.
  - Aquestes botigues tenen mecanismes per revisar aplicacions i eliminar les sospitoses.
- **Evita les apps de tercers o APKs:**
  - Instal·lar aplicacions mitjançant arxius APK (fora de la botiga oficial) és una pràctica que pot introduir malware.
- **Revisa els permisos abans d'instal·lar:**
  - Llegeix amb atenció els permisos que sol·licita l'app. Si semblen excessius o innecessaris, busca una alternativa.
- **Configura controls de seguretat:**
  - **Android:** Configuració > Seguretat > Desactiva "Permet instal·lació de fonts desconegudes".
  - **iOS:** Per defecte, només permet instal·lacions de l'App Store.
- **Actualitza les aplicacions:**

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

- Mantingues totes les apps actualitzades per tancar possibles vulnerabilitats.

3.3. Eines per analitzar i gestionar permisos d'aplicacions

Gestionar els permisos de les aplicacions és clau per protegir la privacitat i evitar que accedeixin a informació innecessària.

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 negoci.

- **Com revisar i ajustar permisos:**
  - **Android:**
    - Configuració > Apps > Selecciona una aplicació > Permisos > Activa o desactiva els permisos segons les necessitats.
  - **iOS:**
    - Configuració > Privacitat i seguretat > Permisos (com càmera, micròfon) > Selecciona les aplicacions que poden accedir-hi.
- **Eines útils per gestionar permisos:**
  - **Bitdefender Mobile Security (Android/iOS):**
    - Escaneja aplicacions i permisos per identificar riscos.
  - **Norton App Advisor (Android):**
    - Analitza aplicacions abans d'instal·lar-les per detectar comportaments sospitosos.
  - **GlassWire (Android):**
    - Monitoritza el consum de dades per detectar apps que envien informació sense autorització.
- **Configuració recomanada:**
  - Reviseu periòdicament els permisos de totes les aplicacions i elimineu les que no utilitzeu.

Beneficis d'una bona gestió d'aplicacions

- **Protecció de dades:** Evites que aplicacions malicioses accedeixin a informació personal o empresarial.
- **Rendiment millorat:** Les aplicacions segures optimitzen l'ús de recursos del dispositiu.
- **Tranquil·litat:** Saps que només tens instal·lades aplicacions confiables i necessàries.

Amb aquestes pràctiques, podràs protegir els teus dispositius mòbils i tauletes contra aplicacions sospitoses i gestionar-les de manera eficient.

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

4. Seguretat en xarxes wi-fi i connexions

Les connexions Wi-Fi són una de les formes més habituals d'accedir a Internet amb dispositius mòbils i tauletes. Tot i això, utilitzar xarxes no segures pot posar en risc la informació del negoci i exposar dades sensibles. Aquest apartat detalla com protegir-te mentre et connectes a Internet.

4.1. Riscos d'utilitzar xarxes públiques o no segures

Les xarxes Wi-Fi públiques, com les d'aeroports, cafeteries o hotels, són molt convenients, però també són una porta d'entrada per als ciberdelinqüents.

- **Riscos principals:**
  1. **Intercepció de dades:**
     - Els atacants poden capturar la informació que envies i reps a través de la xarxa, incloent-hi contrasenyes, dades bancàries o correus electrònics.
  2. **Punts d'accés falsos:**
     - Els atacants poden crear xarxes falses amb noms semblants a les legítimes (per exemple, "Wi-FiGratuitHotel") per enganyar-te i accedir a les teves dades.
  3. **Distribució de malware:**
     - Alguns atacs utilitzen xarxes no segures per instal·lar malware als dispositius connectats.
- **Com evitar aquests riscos:**
  - Evita connectar-te a xarxes públiques sense contrasenya o amb seguretat WEP (obsoleta).
  - Si és imprescindible connectar-te, assegura't de no accedir a dades sensibles (com comptes bancaris) mentre estiguis connectat.

4.2. Ús de VPNs per protegir les connexions mòbils

Una VPN (Xarxa Privada Virtual) és una eina imprescindible per protegir les teves connexions a Internet, especialment en xarxes públiques. La VPN xifra la comunicació entre el teu dispositiu i Internet, protegint la informació de tercers.

- **Avantatges d'utilitzar una VPN:**
  1. **Xifrat de dades:** La informació que envies i reps és il·legible per als atacants.
  2. **Anonimat:** Oculta la teva adreça IP, millorant la teva privacitat en línia.
  3. **Protecció en xarxes no segures:** Permet utilitzar Wi-Fi públiques amb més seguretat.

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

- **Opcions recomanades de VPN:**
  - **NordVPN:** Fàcil d'utilitzar i amb alta velocitat.
  - **ProtonVPN:** Ofereix una opció gratuïta per a ús ocasional.
  - **ExpressVPN:** Ideal per a negocis que necessiten connexions segures i ràpides.

- **Com configurar una VPN:**
  - **Android:**
    - Configuració > Xarxes i Internet > VPN > Afegeix un perfil de VPN (si utilitzes una app de VPN, segueix les instruccions del proveïdor).
  - **iOS:**
    - Configuració > General > VPN > Afegeix configuració de VPN (o descarrega una app oficial del servei que triïs, com NordVPN o ProtonVPN).

4.3. Altres consells per protegir les connexions

- **Utilitza el teu pla de dades mòbil:**
  - Quan siguis en una xarxa pública i hagis de gestionar dades sensibles, fes servir la teva connexió mòbil en lloc del Wi-Fi.
- **Desactiva la connexió automàtica:**
  - Configura el teu dispositiu perquè no es connecti automàticament a xarxes Wi-Fi desconegudes.
  - **Android:** Configuració > Xarxes i Internet > Wi-Fi > Desactiva "Connecta automàticament".
  - **iOS:** Configuració > Wi-Fi > Selecciona la xarxa > Desactiva "Connecta automàticament".
- **Revisa les xarxes disponibles:**
  - Evita connectar-te a xarxes amb noms genèrics o sospitosos.

Beneficis de protegir les connexions

- **Seguretat millorada:** Evites que les dades siguin interceptades mentre utilitzes Wi-Fi públiques.
- **Privacitat:** Protegeixes la teva informació personal i la del negoci contra accessos no autoritzats.
- **Tranquil·litat:** Pots connectar-te a Internet amb confiança, sabent que estàs prenent les mesures adequades.

Aquestes pràctiques són fonamentals per garantir connexions segures en dispositius mòbils i tauletes

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

5. Gestió de dades i privacitat

Una gestió adequada de dades i privacitat és fonamental per protegir la informació personal i professional en dispositius mòbils i tauletes. Aquest apartat ofereix consells pràctics per assegurar-te que les dades estan segures i accessibles només per a les persones autoritzades.

5.1. Consells per protegir la informació personal i professional

La informació que emmagatzemes al dispositiu pot incloure dades personals, financeres i confidencials del negoci. Protegir-la és essencial per evitar robatoris o filtracions.

- **Separa dades personals i professionals:**
  - Si és possible, utilitza aplicacions o perfils diferents per a cada tipus de dades (molts dispositius Android i iOS permeten crear perfils o espais separats per al treball).
- **Activa l'autenticació multifactor (MFA):**
  - Assegura't que les aplicacions importants, com les de banca o gestió d'arxius, requereixin un segon pas de verificació (codi SMS, aplicació de verificació, etc.).
- **Evita emmagatzemar dades sensibles al dispositiu:**
  - Utilitza serveis al núvol confiables (com Google Drive, Dropbox Business o iCloud) per emmagatzemar dades importants, en lloc de deixar-les al dispositiu.
- **Elimina dades antigues o innecessàries:**
  - Esborra periòdicament arxius, fotos o aplicacions que ja no necessitis. Això redueix la quantitat d'informació exposada en cas d'incident.

5.2. Normes per compartir arxius i dades de forma segura

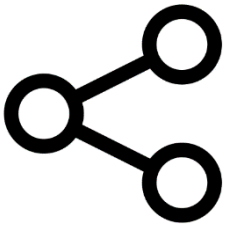
Compartir arxius de manera segura és essencial per protegir la informació de clients i del negoci.

- **Utilitza eines segures per compartir arxius:**
  - Evita compartir arxius mitjançant aplicacions de missatgeria no segures. En lloc d'això, utilitza plataformes com:
    - **Google Drive:** Permet configurar permisos per visualitzar o editar.
    - **Dropbox Business:** Ofereix control avançat sobre qui pot accedir als arxius.
    - **OneDrive:** Permet compartir arxius amb dates de caducitat i contrasenyes.
- **Configura permisos abans de compartir:**

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

  - Dona accés només a les persones necessàries i revoca'l quan ja no sigui necessari.
- **Evita utilitzar xarxes públiques per compartir dades:**
  - Si has de transferir arxius importants, fes-ho des d'una xarxa segura o utilitzant una VPN.
- **Crea còpies de seguretat dels arxius compartits:**
  - Guarda una còpia local o al núvol per assegurar-te que no es perdin durant la transferència.

5.3. Eines per controlar l'accés a la informació en dispositius compartits



Si utilitzes dispositius compartits entre diversos usuaris (com en entorns familiars o negocis amb pocs recursos), és important limitar i protegir l'accés a les dades.

- **Configura comptes d'usuari separats:**
  - **Android:** Configuració > Usuaris i comptes > Afegir usuari.
  - **iOS:** Tot i que no permet diversos perfils, assegura't que les dades sensibles estan protegides amb contrasenyes i aplicacions tancades.
- **Utilitza gestors de contrasenyes:**
  - Poden protegir contrasenyes importants i garantir que només les persones autoritzades hi tenen accés.
- **Bloqueja aplicacions sensibles:**
  - Utilitza aplicacions que permeten configurar contrasenyes específiques per protegir dades (per exemple, AppLock a Android).
- **Monitoritza l'accés a fitxers compartits:**
  - Plataformes com **Google Drive for Business** o **Dropbox Business** permeten veure qui ha accedit a un fitxer i quan.

Beneficis d'una bona gestió de dades i privacitat

- **Protecció de la informació del negoci:** Redueixes el risc de pèrdua o filtració de dades crítiques.
- **Privacitat millorada:** Assegures que la informació personal i professional està protegida contra accessos no autoritzats.
- **Eficiència operativa:** Les eines i pràctiques adequades faciliten la col·laboració segura i l'accés a les dades quan sigui necessari.

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

6. Prevenció de robatoris i pèrdua de dispositius

Els telèfons mòbils i tauletes són dispositius molt valuosos i vulnerables a robatoris o pèrdues. Aquest apartat ofereix consells i eines per protegir-los i minimitzar l'impacte si es produeix un incident.

6.1. Eines per localitzar, bloquejar o esborrar dispositius en cas de pèrdua

La majoria de dispositius mòbils i tauletes tenen funcions integrades que permeten localitzar-los, bloquejar-los o esborrar-ne les dades remotament.

- **Funcions integrades de localització:**
  - **Android: Troba el meu dispositiu**
    - Configuració > Seguretat > Troba el meu dispositiu > Activa l'opció.
    - Accedeix a findmymobile.google.com per localitzar, bloquejar o esborrar el dispositiu.
  - **iOS: Troba el meu iPhone**
    - Configuració > [El teu nom] > Troba > Activa "Troba el meu iPhone".
    - Pots utilitzar l'aplicació "Troba" o accedir a www.icloud.com per localitzar i gestionar el dispositiu.
- **Consells per configurar aquestes eines:**
  - Assegura't que la localització està activada al dispositiu.
  - Mantingues la sessió iniciada al compte de Google o Apple associat per utilitzar aquestes funcions.

6.2. Bones pràctiques per prevenir robatoris físics

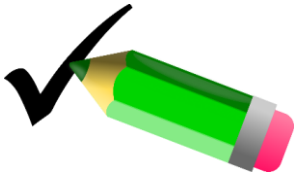
Prevenir el robatori d'un dispositiu és sempre millor que gestionar-ne les conseqüències.

- **Consells per prevenir robatoris:**
  1. **Mantingues el dispositiu fora de la vista:**
     - Evita deixar-lo sobre taules o superfícies accessibles, especialment en llocs públics.
  2. **Utilitza accessoris de seguretat:**
     - Fes servir fundes amb bloqueig o corretges per assegurar el dispositiu.
  3. **No deixis el dispositiu sense vigilància:**
     - Encara que sigui un moment, porta'l sempre amb tu.
  4. **Configura alertes de moviment:**
     - Algunes aplicacions poden notificar-te si el dispositiu es mou sense permís.
- **Evita riscos durant el transport:**

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

- Utilitza motxilles o bosses amb compartiments discrets per protegir el dispositiu quan el portis amb tu.

6.3. Com protegir dades si el dispositiu és robat o es perd



Si el dispositiu cau en mans equivocades, protegir les dades és essencial per evitar problemes majors.

- **Accions immediates en cas de pèrdua o robatori:**
  1. **Bloqueja el dispositiu remotament:**
     - Utilitza les eines "Troba el meu dispositiu" o "Troba el meu iPhone" per bloquejar l'accés.
  2. **Esborra les dades si és necessari:**
     - Si creus que no recuperaràs el dispositiu, esborra'n tot el contingut de manera remota per protegir la informació sensible.
  3. **Canvia contrasenyes:**
     - Actualitza immediatament les contrasenyes de comptes vinculats al dispositiu (com correu electrònic, aplicacions financeres o serveis al núvol).
- **Mesures preventives per protegir les dades:**
  - **Activa el xifrat de dades:**
    - Aquesta opció assegura que les dades no es puguin llegir sense les credencials d'accés.
  - **Configura còpies de seguretat periòdiques:**
    - Si has de restaurar les dades en un dispositiu nou, tenir còpies de seguretat actualitzades t'estalviarà molts problemes.
- **Informa les autoritats:**
  - Denuncia el robatori amb el número de sèrie del dispositiu. Això pot ajudar a identificar-lo si apareix en alguna investigació.

Beneficis d'aquestes pràctiques

- **Protecció de dades sensibles:** Les eines i pràctiques descrites redueixen el risc que les teves dades caiguin en mans equivocades.
- **Recuperació més fàcil:** Si utilitzes funcions com "Troba el meu dispositiu", tens més probabilitats de localitzar-lo.
- **Tranquil·litat:** Estar preparat per gestionar pèrdues o robatoris redueix l'estrès i els impactes negatius en el negoci.

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

7. Preguntes d'auoavaluació.

Aquest apartat et permet valorar si els teus dispositius mòbils i tauletes estan protegits adequadament. Amb una llista de verificació i recomanacions, podràs identificar punts de millora i reforçar la seguretat.

7.1. 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.

Configuracions bàsiques de seguretat

1. Els teus dispositius tenen un bloqueig de pantalla segur configurat (PIN, contrasenya o autenticació biomètrica)?
2. Les dades dels teus dispositius estan xifrades?
3. Tens activades còpies de seguretat automàtiques per protegir les dades?
4. Els sistemes operatius i aplicacions estan sempre actualitzats?

Protecció contra aplicacions malicioses

5. Només descarregues aplicacions de botigues oficials (Google Play, App Store)?
6. Revisa i gestiones els permisos de les aplicacions periòdicament?
7. Tens eines instal·lades per analitzar aplicacions sospitoses o malicioses?

Seguretat en connexions

8. Evites connectar-te a xarxes Wi-Fi públiques sense protecció?
9. Utilitzes una VPN per protegir les connexions mòbils quan accedeixes a dades sensibles?

Gestió de dades i privacitat

10. Separes les dades personals de les professionals als teus dispositius?
11. Utilitzes eines segures per compartir arxius (Google Drive, Dropbox, etc.)?

Prevenció de robatoris i pèrdues

12. Tens activades eines per localitzar, bloquejar o esborrar dispositius en cas de pèrdua?
13. Els dispositius estan configurats per bloquejar-se automàticament després d'un període d'inactivitat?

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

14. Has configurat còpies de seguretat per restaurar dades en cas de pèrdua o robatori?

Escala d'autoavaluació

4 respostes afirmatives: Nivell de risc alt
• Estàs molt exposat a riscos de seguretat. • Recomanació: Comença per implementar les configuracions bàsiques de seguretat, com el bloqueig de pantalla, el xifrat de dades i les còpies de seguretat. Dona prioritat a protegir connexions i gestionar aplicacions amb cura.
5-9 respostes afirmatives: Nivell de risc moderat
• Tens algunes mesures implementades, però encara hi ha vulnerabilitats importants. • Recomanació: Reforça la seguretat en connexions, la gestió de dades i la protecció contra robatoris i aplicacions sospitoses.
10-13 respostes afirmatives: Nivell de risc baix
• Tens una bona estratègia de seguretat, però encara hi ha petits ajustos per fer. • Recomanació: Assegura't que totes les funcions de seguretat estan activades i revisa periòdicament les configuracions per mantenir-les actualitzades.
14 respostes afirmatives: Excel·lent
• Felicitats! Els teus dispositius mòbils i tauletes estan molt ben protegits. • Recomanació: Mantingues les bones pràctiques i adapta les mesures segons les noves necessitats o riscos que puguin sorgir.

Recursos addicionals

Per reforçar la teva estratègia en la prevenció de ciberseguretat en dispositius mòbils i tauletes, et recomanem consultar els recursos següents. Aquests t'ajudaran a protegir els teus dispositius, millorar-ne la gestió i mantenir-te actualitzat sobre les millors pràctiques en seguretat mòbil.

Guies i recursos en línia

- **INCIBE (Institut Nacional de Ciberseguretat):**
  - Ofereix consells pràctics i guies específiques per protegir dispositius mòbils en entorns empresarials.
  - Accedeix al seu lloc web: www.incibe.es.
- **Agència de Ciberseguretat de Catalunya (Catalonia-CERT):**
  - Proporciona recomanacions per a la seguretat en dispositius mòbils, incloent-hi bones pràctiques per a petites empreses i autònoms.
  - Web oficial: www.ciberseguretat.gencat.cat.

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

- **Google i Apple Security Centers:**
  - **Google:** Ofereix eines i consells per protegir dispositius Android.
    Accedeix a: Google Safety Center.
  - **Apple:** Inclou guies per millorar la seguretat i privacitat en dispositius iOS.
    Web oficial: Apple Privacy and Security.

Eines de formació en línia

- **Plataformes de formació gratuïtes:**
  - **INCIBE Formació:** Programes dissenyats per a petites empreses que inclouen la protecció de dispositius mòbils.
  - **Google Actívate:** Cursos gratuïts en seguretat digital, incloent-hi bones pràctiques per a dispositius mòbils.
- **Tallers locals i webinars:**
  - Participa en formacions organitzades per cambres de comerç, associacions empresarials o organitzacions com el Catalonia-CERT.

Suport i assistència

- **INCIBE (Institut Nacional de Ciberseguretat):**
  - Telèfon d'ajuda gratuït: **017**, disponible tots els dies de l'any, per a empreses i particulars.
  - Ofereix assistència en casos de seguretat mòbil, gestió de dispositius i protecció de dades.
  - Web oficial: www.incibe.es.
- **Catalonia-CERT (Agència de Ciberseguretat de Catalunya):**
  - Proporciona suport específic per a petites empreses i autònoms a Catalunya en matèria de ciberseguretat mòbil i gestió d'incidents.
  - Contacta amb el seu servei d'assistència a través de: www.ciberseguretat.gencat.cat.
- **Suport dels fabricants i desenvolupadors:**
  - **Google (Android):** Ofereix documentació i assistència tècnica per millorar la seguretat dels dispositius Android.
    Accés: support.google.com/android
  - **Apple (iOS):** Proporciona suport per configurar i protegir dispositius Apple.
    Accés: support.apple.com.

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