Autoavalua la ciberseguretat del teu projecte:

# Còpies de seguretat i recuperació de dades.

---

*Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per a protegir els teus actius digitals en cas de ciberincidents.*

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: còpies de seguretat i recuperació de dades


1. **Introducció**
   - Importància de les còpies de seguretat per a autònoms i petites empreses.
   - Principals riscos de no tenir una estratègia de còpia de seguretat.
2. **Tipus de còpies de seguretat**
   - Completes: Definició, avantatges i inconvenients.
   - Incrementals: Com funcionen i quan utilitzar-les.
   - Diferencials: Comparació amb les incrementals i aplicacions pràctiques.
3. **Estratègies de còpies de seguretat**
   - La regla 3-2-1: Explicació i aplicació pràctica.
   - Còpies en local vs. còpies al núvol: Pros i contres de cada opció.
   - Frequència recomanada de còpies de seguretat.
4. **Eines per realitzar còpies de seguretat**
   - Solucions gratuïtes i de pagament.
   - Eines per a petites empreses i autònoms.
   - Consideracions per triar l'eina adequada.
5. **Recuperació de dades**
   - Passos per restaurar còpies de seguretat.
   - Proves periòdiques per garantir que la recuperació funciona.
   - Errors comuns en la recuperació i com evitar-los.
6. **Mesures preventives per reduir el risc de pèrdua de dades**
   - Protecció contra malware i ransomware.
   - Bones pràctiques per minimitzar errors humans.
7. **Autoavaluació**
   - **Llista de verificació**: Comprova si estàs preparat davant una possible pèrdua de dades.
   - **Resultats i recomanacions**: Suggeriments específics per millorar la teva estratègia de còpia de seguretat.


**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 les còpies de seguretat per a autònoms i petites empreses*

En un món cada vegada més digital, la informació és un dels actius més valuosos per a qualsevol empresa i de qualsevol mida i aquestes **dades es conserven en dispositius físics o espais virtuals**. Sovint són ocuments de clients, factures, projectes en curs i registres financers són només alguns exemples de dades que poden ser crítiques per al funcionament diari.

Tot i això, moltes petites empreses i autònoms no implementen una estratègia adequada de còpies de seguretat, deixant-se exposats a situacions que poden tenir greus conseqüències, com ara:

- **Pèrdua accidental de dades**: Per errors humans, fallades tècniques o esborrat involuntari.
- **Atacs de ransomware**: Programes maliciosos que bloquegen l'accés a les dades fins que es paga un rescat.
- **Robatoris o danys físics**: Com el robatori d'un ordinador o la destrucció del mateix per foc o inundació.

Les còpies de seguretat són, per tant, una mesura imprescindible per garantir la continuïtat del negoci. Quan estan ben implementades, permeten recuperar ràpidament les dades en cas de pèrdua, minimitzant l'impacte sobre les operacions.

## *Principals riscos de no tenir una estratègia de còpia de seguretat*

No comptar amb còpies de seguretat o tenir una estratègia ineficient pot provocar situacions com aquestes:

1. **Interrupció de l'activitat**:
   - Sense accés a dades essencials, les operacions es poden paralitzar completament.
   - Recuperar-se d'una pèrdua de dades pot trigar dies o setmanes, afectant la productivitat.
2. **Costos econòmics**:
   - La recreació de dades perdudes pot suposar despeses significatives.
   - El cost mitjà d'un atac de ransomware per a petites empreses pot ser devastador.

3. **Danys a la reputació**:
   - La pèrdua d'informació dels clients pot danyar la confiança i provocar que busquin alternatives.
4. **Incompliment legal**:



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

- Algunes normatives, com el RGPD, exigeixen mesures per protegir i restaurar dades. No complir-les pot implicar sancions.

### *Objectius d'aquesta guia*

Aquesta guia té com a finalitat ajudar-te a:

- Comprendre per què les còpies de seguretat són fonamentals per a la seguretat i continuïtat del teu negoci.
- Aprendre a seleccionar i implementar una estratègia de còpia de seguretat adaptada a les teves necessitats.
- Tenir els coneixement essencials per recuperar dades de manera ràpida i eficient en cas d'incident.

## 2. Tipus de Còpies de Seguretat

Seleccionar el tipus de còpia de seguretat adequat és crucial per a petites empreses i autònoms en la protecció dels seus documents i altres actius digitals, ja que una estratègia ben planificada pot estalviar temps, diners i complicacions en cas de pèrdua de dades. Aquest apartat descriu els tipus principals de còpies de seguretat, els seus avantatges i inconvenients, i com triar-ne el més adequat.

| Còpia completa | Còpia incremental | Còpia diferencial |
|---|---|---|

### *2.1. Còpia de seguretat completa*

La còpia completa és la forma més bàsica i completa de fer una còpia de seguretat: es creen duplicats de totes les dades seleccionades en un moment concret.

- **Com funciona**: es copia tot el contingut seleccionat, independentment de si ha canviat des de l'última còpia de seguretat.
- **Avantatges**:
  - **Fàcil de restaurar**: Com que inclou totes les dades, la recuperació és ràpida i senzilla.
  - **Completa i independent**: No depèn d'altres còpies de seguretat.
- **Inconvenients**:


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

  - **Espai d'emmagatzematge**: Requereix molt espai, especialment si les dades són voluminoses.
  - **Temps de còpia**: Pot trigar molt a completar-se.
- **Quan utilitzar-la**:
  - Com a primera còpia de seguretat inicial.
  - Per a dades crítiques que necessiten una restauració ràpida i integral.

### *2.2. Còpia de seguretat incremental*

La còpia incremental només guarda les dades que han canviat o s'han afegit des de l'última còpia de seguretat (independentment del tipus que fos).

- **Com funciona**:
  - Després d'una còpia inicial completa, les següents còpies només inclouen els canvis més recents.
- **Avantatges**:
  - **Eficiència en l'espai**: Només es copien fitxers nous o modificats, requerint menys espai d'emmagatzematge.
  - **Velocitat**: La còpia de seguretat és molt ràpida.
- **Inconvenients**:
  - **Restauració més complexa**: Per recuperar totes les dades, cal combinar la còpia completa inicial i totes les incrementals.
- **Quan utilitzar-la**:
  - Per a còpies freqüents (diàries o fins i tot horàries) en negocis amb molts canvis constants.

### *2.3. Còpia de seguretat diferencial*

La còpia diferencial guarda totes les dades que han canviat des de l'última còpia completa, acumulant els canvis en cada còpia successiva.

- **Com funciona**:
  - A diferència de la còpia incremental, la còpia diferencial no es basa en còpies anteriors, sinó només en la còpia completa inicial.
- **Avantatges**:
  - **Restauració més senzilla**: Només cal la còpia completa inicial i l'última còpia diferencial per restaurar totes les dades.
  - **Espai relativament eficient**: Tot i que creix en mida amb el temps, és més manejable que fer còpies completes constants.
- **Inconvenients**:
  - **Espai i temps intermedis**: A mesura que passa el temps, les còpies diferencials creixen en mida i triguen més.
- **Quan utilitzar-la**:
  - Per a negocis amb canvis regulars però no constants, on la restauració ràpida és una prioritat.


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

### *2.4. Comparativa entre tipus de còpies*

Aquí tens una taula ràpida per ajudar a decidir quin tipus és el més adequat:

| Tipus | Espai necessari | Temps de còpia | Velocitat de restauració | Complexitat |
|---|---|---|---|---|
| **Completa** | Alt | Lent | Ràpida | Baixa |
| **Incremental** | Baix | Ràpid | Lent (requereix múltiples còpies) | Mitjana |
| **Diferencial** | Mitjà | Intermedi | Intermedi | Mitjana |

### *2.5. Consells per a petites empreses i autònoms*

- **Combina tipus de còpies**: Realitza una còpia completa inicial i després utilitza còpies incrementals o diferencials per optimitzar espai i temps.
- **Prioritza la restauració**: Si la rapidesa de recuperació és crítica per al teu negoci, considera còpies completes o diferencials.
- **Prova l'estratègia**: Realitza simulacions de recuperació per assegurar-te que les còpies funcionen com esperes.

## 3. Estratègies de còpies de seguretat

Disposar d'una estratègia clara de còpies de seguretat és fonamental per garantir la protecció de les dades en petits negocis i per als autònoms. A continuació, es presenten diverses estratègies pràctiques que equilibren eficiència, cost i seguretat, adaptades a diferents necessitats.

### *3.1. La regla 3-2-1*


La regla 3-2-1 és un estàndard àmpliament reconegut per garantir còpies de seguretat robustes i segures.

- **Què significa la regla 3-2-1?**:
  1. **3 còpies de les dades**:
     - Una còpia original i dues còpies de seguretat.
  2. **2 formats diferents**:
     - Per exemple, una còpia en un disc dur extern i una altra al núvol.
  3. **1 còpia fora de l'empresa**:
     - Aquesta còpia es guarda en una ubicació física diferent per protegir-se de desastres locals com incendis o inundacions.


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

- **Beneficis de la regla 3-2-1**:
  - Protecció davant múltiples escenaris, com errors humans, fallades tècniques o desastres naturals.
  - Assegura que sempre hi hagi almenys una còpia accessible.
  - **Exemples pràctics**: dades originals a l'ordinador, una còpia de seguretat en un disc extern, una segona còpia al núvol amb un servei com Google Drive, Dropbox o un proveïdor especialitzat.

### *3.2. Còpies en local vs. còpies al núvol*



Decidir on emmagatzemar les còpies de seguretat depèn de les necessitats del negoci i els recursos disponibles.

| Aspecte | Còpies en local | Còpies al núvol |
|---|---|---|
| **Accessibilitat** | Ràpida i no depèn d'Internet. | Accessible des de qualsevol lloc amb connexió a Internet. |
| **Espai d'emmagatzematge** | Limitat pel dispositiu físic, NAS*, etc.. | Espai ampliable segons el pla contractat. |
| **Seguretat física** | Vulnerable a desastres locals (incendis, robatoris). | Protecció contra desastres físics. |
| **Seguretat digital** | Depèn de les configuracions pròpies (xifrat, contrasenyes). | Inclou mesures de seguretat avançades del proveïdor (xifrat, autenticació). |
| **Cost inicial** | Inversió en maquinari (discs, servidors). | Cost baix inicial, però amb subscripcions recurrents. |
| **Temps de restauració** | Molt ràpid si el dispositiu està disponible. | Pot ser més lent depenent de la velocitat d'Internet. |
| **Dependència de tercers** | Control total sobre les dades. | Depens del proveïdor per a l'accés i manteniment. |
| **Exemples d'ús** | Còpies en discos durs externs, NAS o pendrives. | Solucions com Google Drive, OneDrive, Dropbox. |

**Un NAS (Network Attached Storage) és un dispositiu d'emmagatzematge connectat a una xarxa local que permet guardar, gestionar i accedir a fitxers des de diversos dispositius (ordinadors, mòbils, etc.). És com un disc dur extern, però amb funcionalitats avançades i compartit a través de la xarxa.*


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

- **Estratègia recomanada tenint en compte les diferències entre local i al núvol i els beneficis de cada mètode**:
  - Combina ambdues opcions: mantenir una còpia en local per a recuperacions ràpides i una al núvol per a desastres greus.

### *3.3. Frequència recomanada de còpies de seguretat*

La freqüència de les còpies de seguretat depèn de la quantitat i la importància de les dades que es generen o actualitzen diàriament.

- **Freqüències suggerides**:

**Diària:**
- Ideal per a negocis amb dades crítiques que canvien sovint, com factures o arxius de projectes.

**Setmanal:**
- Per a negocis amb menys activitat o autònoms que no generen grans volums de dades.

**Mensual:**
- Per a còpies completes en negocis amb dades estàtiques o amb canvis mínims.

- **Un consell pràctic sobre la freqüència**: planifica còpies automàtiques per evitar errors humans o descuits.

### *3.4. Automatització de les còpies de seguretat*

Automatitzar el procés de còpies de seguretat garanteix que sempre es realitzin a temps sense requerir accions manuals.

- **Eines d'automatització**:
  - **Còpies en local**: eines integrades com **Historial de fitxers** de Windows o **Time Machine** de macOS.
  - **Còpies al núvol**: programes o serveis de sincronització com OneDrive, iCloud o Google Drive automatizen còpies.
- **Beneficis de l'automatització**:
  - Redueix la càrrega de treball.
  - Evita errors humans com l'oblit o configuracions inadequades.

### *3.5. Consells per a petites empreses i autònoms*

- **Defineix prioritats**:
  - No totes les dades necessiten el mateix nivell de protecció. Identifica quines són crítiques (clients, finances) i quines són prescindibles.
- **Etiqueta les còpies**:


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

    - Organitza les còpies de manera clara, amb dates o identificadors per saber ràpidament quina és la més recent.
- **Prova la restauració periòdicament**:
    - Comprova regularment que les còpies de seguretat són funcionals i que pots restaurar-les sense problemes.

### *Beneficis d'una bona estratègia de còpies de seguretat*

- **Protecció completa**: Redueix riscos davant qualsevol tipus de pèrdua de dades.
- **Continuïtat del negoci**: Permet recuperar dades ràpidament i reprendre l'activitat sense interrupcions greus.
- **Tranquil·litat**: Saber que les dades estan segures et permet centrar-te en el teu negoci.

## 4. Eines per realitzar còpies de seguretat

Per als autònoms i petites empreses, triar les eines adequades per fer còpies de seguretat és crucial. Existeixen opcions gratuïtes i de pagament adaptades a diferents necessitats. A continuació, es presenten les millors eines per gestionar còpies de seguretat, des de solucions locals fins a serveis al núvol.

**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.

### *4.1. Solucions gratuïtes*

Les eines gratuïtes són una bona opció per a negocis amb pressupost limitat. Tot i això, poden tenir funcionalitats més bàsiques.

- **Historial de fitxers (Windows)**: Eina integrada a Windows que permet fer còpies automàtiques de fitxers en dispositius externs o ubicacions de xarxa.
    - **Avantatges**: gratuïta i fàcil d'utilitzar ic onfiguració ràpida.
    - **Inconvenients**: no ofereix còpies completes del sistema.
- **Time Machine (macOS)**: Solució integrada als dispositius Apple que permet fer còpies automàtiques de tot el sistema.
    - **Avantatges**: senzilla i fiable i inclou còpies incrementals.
    - **Inconvenients**: només disponible per a dispositius Apple.


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

- **Google Drive / OneDrive / iCloud (versions gratuïtes)**: Ofereixen emmagatzematge al núvol gratuït (15 GB a Google Drive, 5 GB a iCloud, 5 GB a OneDrive).
  - **Avantatges**: solucions al núvol gratuïtes per a fitxers petits.
  - **Inconvenients**: espai limitat, menys opcions de personalització i interfície pot ser complexa per a usuaris novells.

### *4.2. Algunes solucions de pagament*

Les eines de pagament ofereixen funcionalitats més avançades i són ideals per a negocis que necessiten seguretat i eficiència màximes.

Aqui tens alguns proveïdors de pagament perquè els puguis cercar a Internet i revisar les seves propostes d'emmagatzament segur al núvol: Acronis Cyber Protect Home Office, Backblaze**,** Carbonite o Synology NAS, entre d'altres.

### *4.3. Com triar l'eina adequada*

Per decidir quina eina s'adapta millor al teu negoci, tingues en compte els següents factors:

- **Volum de dades**: si tens grans volums, podries per solucions amb emmagatzematge il·limitat.
- **Pressupost**: comença amb opcions gratuïtes com Google Drive o Time Machine si tens un pressupost reduït.
- **Freqüència de còpies**: si necessites còpies constants, assegura't que l'eina tingui automatització i còpies incrementals.
- **Ubicació de les dades**: per a dades sensibles, prioritza solucions amb xifrat i emmagatzematge al núvol segur.
- **Simplicitat vs. configuració avançada**: si prefereixes una eina fàcil d'usar, opta per solucions com Time Machine o Acronis. Per configuracions avançades, tria SyncBack o Synology.

### *4.4. Consells per utilitzar eines de còpia de seguretat*

- **Configura alertes**: Activa notificacions per assegurar-te que les còpies s'estan fent correctament.
- **Prova periòdicament la restauració**: Verifica que pots recuperar dades sense problemes.
- **Actualitza el programari**: Mantén les eines actualitzades per evitar vulnerabilitats.


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

*Beneficis d'una eina adequada*

- **Protecció completa**: Garantitza que les teves dades estan segures i accessibles en qualsevol moment.
- **Eficiència**: Automatitza processos i estalvia temps.
- **Tranquil·litat**: Saber que tens una estratègia robusta redueix l'estrès davant possibles incidents

## 5. Recuperació de dades

La recuperació de dades és tan important com fer còpies de seguretat. Una còpia és inútil si no pots accedir-hi o restaurar-la en cas de necessitat. Aquest apartat t'ajudarà a comprendre els passos clau per restaurar còpies de seguretat i garantir que el procés funcioni sense problemes.

### *5.1. Passos per restaurar còpies de seguretat*

- **1) Identifica què necessites recuperar**:
  - Assegura't de saber quines dades específiques has perdut o necessites restaurar.
  - Determina si necessites restaurar tot el sistema, una carpeta concreta o fitxers específics.
- **2) Selecciona la còpia adequada**:
  - Si tens múltiples còpies, escull la més recent o la que contingui les dades necessàries.
  - Assegura't que no estigui corrupta o incompleta.
- **3) Segueix les instruccions de l'eina utilitzada**:
    - **Windows (Historial de fitxers)**: vés a la configuració de l'historial i selecciona la versió que vols restaurar.
    - **Time Machine (macOS)**: obre Time Machine, selecciona la data de la còpia i fes clic a "Restaura".
    - **Eines al núvol**: accedeix al teu compte (Google Drive, OneDrive, etc.), selecciona els fitxers i descarrega'ls.
- **4) Prova les dades recuperades**:
  - Verifica que els fitxers recuperats funcionin correctament.
  - Comprova que no hi hagi dades corruptes o incompletes.

### *5.2. Proves periòdiques de recuperació*

Un error comú és donar per fet que les còpies funcionaran sempre. Realitzar proves regulars ajuda a evitar sorpreses desagradables en situacions d'emergència.

- **Per què provar la recuperació?**
  - Garantir que les còpies no estan danyades.

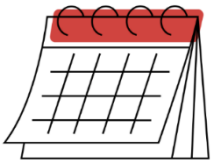

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

  - Identificar problemes en els procediments de còpia.
  - Assegurar-se que saps com recuperar les dades ràpidament.
- **Com fer-ho?**
  - Escull un fitxer o carpeta a l'atzar i prova de restaurar-lo.
  - Simula un escenari realista, com la pèrdua d'un dispositiu.
  - Revisa que les dades recuperades siguin exactament les que necessites.
- **Freqüència recomanada**:
  - Per a petites empreses, almenys una prova cada trimestre.
  - Per a dades crítiques, una prova mensual.

### *5.3. Errors comuns en la recuperació i com evitar-los*

1. **No tenir accés a les eines de còpia**:
   - **Problema**: Si la clau de xifrat o l'accés al núvol es perd, no podràs recuperar les dades.
   - **Solució**: Guarda les claus de xifrat i credencials en un lloc segur i accessible.
2. **Còpies incompletes o corruptes**:
   - **Problema**: Una còpia que no es va completar correctament no servirà per a la recuperació.
   - **Solució**: Configura alertes per assegurar-te que totes les còpies es realitzen amb èxit.
3. **Restauració parcial o errònia**:
   - **Problema**: Recuperar fitxers incorrectes o oblidar algunes dades.
   - **Solució**: Fes un inventari clar de les dades a recuperar i comprova que totes les necessàries es restauren.
4. **Desconeixement del procés**:
   - **Problema**: No saber com utilitzar l'eina de recuperació en un moment d'urgència.
   - **Solució**: Forma't en l'ús de les eines i mantingues una guia escrita per a consultes ràpides.

### *5.4. Consells per una recuperació efectiva*



- **Planifica amb antelació**: tenir un pla clar per saber què fer en cas de pèrdua de dades ajuda a actuar amb rapidesa i confiança.
- **Crea còpies redundants**: si una còpia falla, una altra ha de ser accessible. Aquesta és la base de la regla 3-2-1.
- **Comunica el procés**: en petites empreses, assegura't que tothom que pugui necessitar accés a les dades sap com utilitzar el sistema de còpies de seguretat.


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

*Beneficis d'una bona estratègia de recuperació*

- **Temps mínim d'interrupció**: Les dades es recuperen ràpidament, reduint l'impacte en el negoci.
- **Evita pèrdues de dades**: Un bon sistema de còpies i proves garanteix que no es perdin arxius importants.
- **Confiança en el sistema**: Saber que pots restaurar dades de manera efectiva et dona tranquil·litat i seguretat.

## 6. Mesures preventives per reduir el risc de pèrdua de dades

Tot i tenir una bona estratègia de còpies de seguretat, implementar mesures preventives és essencial per reduir al mínim la possibilitat de perdre dades. Aquesta combinació de prevenció i còpies de seguretat assegura que els teus dispositius i informació estiguin protegits davant qualsevol incident.

### *6.1. Protecció contra malware i ransomware*

Els atacs de malware i ransomware són una de les principals causes de pèrdua de dades. Aquests programes maliciosos poden danyar fitxers o segrestar informació a canvi d'un rescat.

- **Com prevenir-los**:
  - **Utilitza un antivirus actualitzat**:
    - Eines com Bitdefender, Avast o Norton poden detectar i eliminar amenaces.
  - **Evita enllaços i arxius sospitosos**:
    - No obris correus electrònics o fitxers d'origen desconegut.
  - **Activa un tallafocs**:
    - Protegeix el dispositiu bloquejant connexions no autoritzades.
  - **Desconfia de correus amb urgències falses**:
    - Els atacs de phishing sovint utilitzen enganys per fer-te clicar en enllaços maliciosos.
- **Còpies de seguretat com a defensa addicional**:
  - En cas d'atac, una còpia recent et permet recuperar les dades sense pagar rescats.

### *6.2. Bones pràctiques per minimitzar errors humans*

Els errors humans són una altra causa comuna de pèrdua de dades, especialment en petites empreses.

- **Formació de l'equip**:


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

    - Educa els treballadors sobre bones pràctiques de seguretat, com reconèixer correus electrònics sospitosos o gestionar contrasenyes amb seguretat.
- **Eines per reduir riscos**:
    - **Gestors de contrasenyes**:
        - Eines com LastPass o Dashlane eviten l'ús de contrasenyes febles o repetides.
    - **Restricció d'accés**:
        - Dona accés només a les dades necessàries segons el rol de cada treballador.
    - **Confirmació abans d'esborrar fitxers**:
        - Configura sistemes per demanar confirmació abans d'eliminar fitxers crítics.
- **Automatització**:
    - Redueix la dependència de tasques manuals (com còpies de seguretat) per minimitzar errors.

### *6.3. Protecció física dels dispositius*

Una bona protecció física ajuda a prevenir robatoris, pèrdues o danys accidentals que podrien afectar les dades.

- **Consells per protegir dispositius físicament**:
    - Guarda ordinadors i dispositius en llocs segurs, especialment fora de l'horari laboral.
    - Utilitza fundes i protectors per evitar danys per caigudes.
    - Configura opcions de bloqueig automàtic per protegir dades en cas de robatori.
- **Emmagatzematge fora del lloc de treball**:
    - Per a còpies físiques, utilitza un disc dur extern guardat en una ubicació diferent.

### *6.4. Actualitzacions regulars del sistema i aplicacions*

Un programari obsolet pot tenir vulnerabilitats que els atacants poden explotar.

- **Avantatges de mantenir el sistema actualitzat**:
    - Resol errors de seguretat coneguts.
    - Millora la compatibilitat amb eines de seguretat modernes.
- **Com assegurar-te que el sistema està actualitzat**:
    - Activa les actualitzacions automàtiques tant per al sistema operatiu com per a aplicacions crítiques.
    - Revisa periòdicament si hi ha actualitzacions pendents.


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

### *6.5. Monitoratge i alertes*

Detectar problemes de seguretat o anomalies a temps pot evitar pèrdues de dades.

- **Eines de monitoratge**:
  - Utilitza eines com SolarWinds o Nagios per controlar l'estat dels teus dispositius i xarxes.
  - Configura alertes per detectar activitat sospitosa o fallades en el sistema.
- **Què monitoritzar?**
  - Estat dels discos durs per evitar fallades imminents.
  - Activitat inusual de fitxers o aplicacions.

### *Beneficis de les mesures preventives*

- **Reducció de riscos**: Prevenir és sempre millor que solucionar un problema.
- **Millora de la seguretat global**: Amb mesures combinades, protegeixes tant les dades com els dispositius.
- **Estalvi de temps i costos**: Menys incidents significa menys temps invertit en solucionar problemes i menys pèrdues econòmiques.



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

## 7. 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.

#### Configuració de les còpies de seguretat

1. Tinc una estratègia de còpies de seguretat basada en la regla 3-2-1?
2. Realitzo còpies de seguretat amb la freqüència adequada segons les meves necessitats (diàries, setmanals, etc.)?
3. Les meves còpies de seguretat inclouen totes les dades crítiques (clients, finances, projectes, etc.)?

#### Emmagatzematge i eines

4. Les meves còpies estan distribuïdes entre dispositius locals i al núvol?
5. Les eines que utilitzo per fer còpies de seguretat estan configurades i actualitzades correctament?
6. Tinc còpies de seguretat protegides amb xifrat o contrasenyes fortes?

#### Recuperació de dades

7. He realitzat proves de recuperació de dades recentment per garantir que funcionen?
8. Sé com accedir i restaurar les meves dades en cas de necessitat?
9. Tinc documentat un procediment per recuperar dades de manera ràpida i eficient?

#### Mesures preventives

10. Tinc instal·lat un antivirus i un tallafocs actualitzats?
11. Realitzo actualitzacions periòdiques dels sistemes operatius i aplicacions?
12. Els treballadors o col·laboradors del meu negoci han rebut formació en bones pràctiques de seguretat?



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

## 7.2. Escala d'autoavaluació

**0-5 respostes afirmatives: Nivell de risc alt**

- Estàs exposat a múltiples riscos que poden afectar greument el teu negoci.
- Recomanació: Comença per establir una estratègia bàsica de còpies de seguretat i implementa mesures de protecció mínimes, com antivirus i actualitzacions.

**6-9 respostes afirmatives: Nivell de risc moderat**

- Has implementat algunes mesures, però encara tens àrees crítiques per millorar.
- Recomanació: Dona prioritat a la recuperació de dades i assegura't que totes les còpies estan protegides i accessibles.

**10-11 respostes afirmatives: Nivell de risc baix**

- Tens una estratègia de còpies de seguretat i mesures preventives sòlides.
- Recomanació: Mantingues les bones pràctiques i revisa periòdicament les teves còpies i el pla de recuperació.

**12 respostes afirmatives: Excel·lent**

- Felicitats! Tens una estratègia robusta que garanteix la seguretat i la continuïtat del teu negoci.
- Recomanació: Continua monitoritzant i actualitzant el teu sistema per mantenir aquest nivell de seguretat.

## 7.3. 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