

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

ÉS IMPORTANT QUE FEM SERVIR GESTORS DE
CONTRASENYES A LA NOSTRA ORGANITZACIÓ?

Febrer 2026
Document d'ús públic

1 EL PROBLEMA DE LES CONTRASENYES

2 QUÈ ÉS UN GESTOR DE CONTRASENYES?

3 COM FUNCIONA UN GESTOR DE CONTRASENYES?

4 AVANTATGES CLAU D'UN GESTOR DE CONTRASENYES

5 BENEFICIS PER A L'ORGANITZACIÓ



6 BONES PRÀCTIQUES D'ÚS

7 GESTORS DE CONTRASENYES RECOMANATS

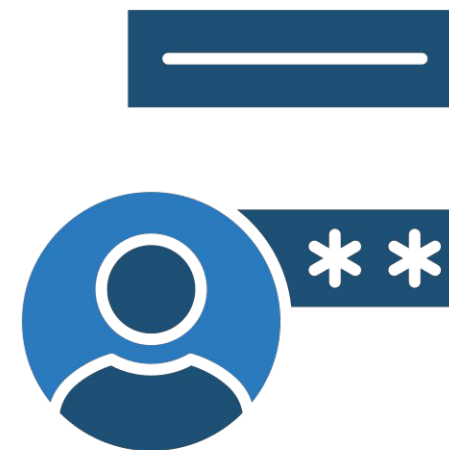


1. EL PROBLEMA DE LES CONTRASENYES



- **El 51 % de les contrasenyes que es fan servir avui en dia es poden piratejar en menys d'un minut, segons anàlisis de ciberseguretat recents.**
- **La majoria de les bretxes de dades afecten credencials en risc, i el 86 % dels atacs a aplicacions web es deuen a problemes amb contrasenyes o credencials compromeses.**

**L'ÚS DE CONTRASENYES DÈBILS O
REUTILITZADES SEGUEIX SENT UNA
VULNERABILITAT CRÍTICA**



2. QUÈ ÉS UN GESTOR DE CONTRASENYES?



És un programa o servei dissenyat per **emmagatzemar, organitzar i protegir de manera segura** totes les combinacions d'usuari i contrasenya que fem servir en diferents serveis digitals. Les dades s'encripten mitjançant una única **clau mestra**.

BENEFICIS D'UTILITZAR UN GESTOR DE CONTRASENYES

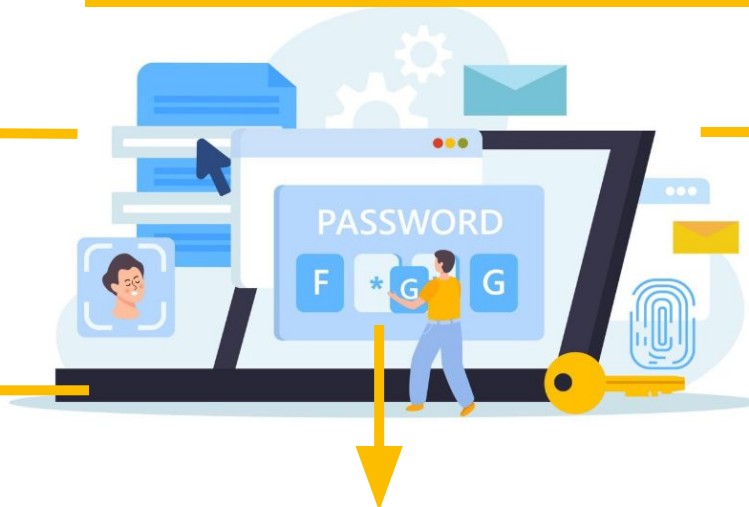
Redueix riscos de seguretat

Millora la seguretat en les organitzacions

Facilita la productivitat

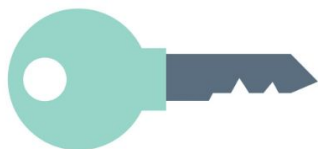
Centralitza i protegeix credencials

Permet l'ús de contrasenyes fortes i úniques



3. COM FUNCIONA UN GESTOR DE CONTRASENYES?

Un gestor de contrasenyes desa totes les teves credencials (usuari, contrasenya, URL, notes, etc.) en una **base de dades encriptada**. Aquesta caixa forta està protegida per una **clau mestra**.



- Crees una **CLAU MESTRA** forta.
- Aquesta clau **NO S'EMMAGATZEMA** en el gestor: s'utilitza per generar la clau que xifra i desxifra la teva caixa forta.

XIFRATGE FORT PER PROTEGIR LES TEVES DADES:

Els gestors utilitzen algorismes de xifratge avançats, si algú aconsegueix la base de dades, **no la pot llegir** sense la clau mestra.



AUTOCOMPLETAMENT SEGUR

- El gestor reconeix la pàgina.
- Omple automàticament usuari i contrasenya.

4. AVANTATGES CLAU D'UN GESTOR DE CONTRASENYES



SEGURETAT

- Xifratge fort i caixa forta segura.
- Contrasenyes úniques i robustes.
- Model coneixement zero.
- Protecció contra pesca.



PRODUCTIVITAT

- Compleció automàtica ràpida i precisa.
- Menys temps perdut en recuperacions.
- Sincronització entre dispositius.



CONTROL

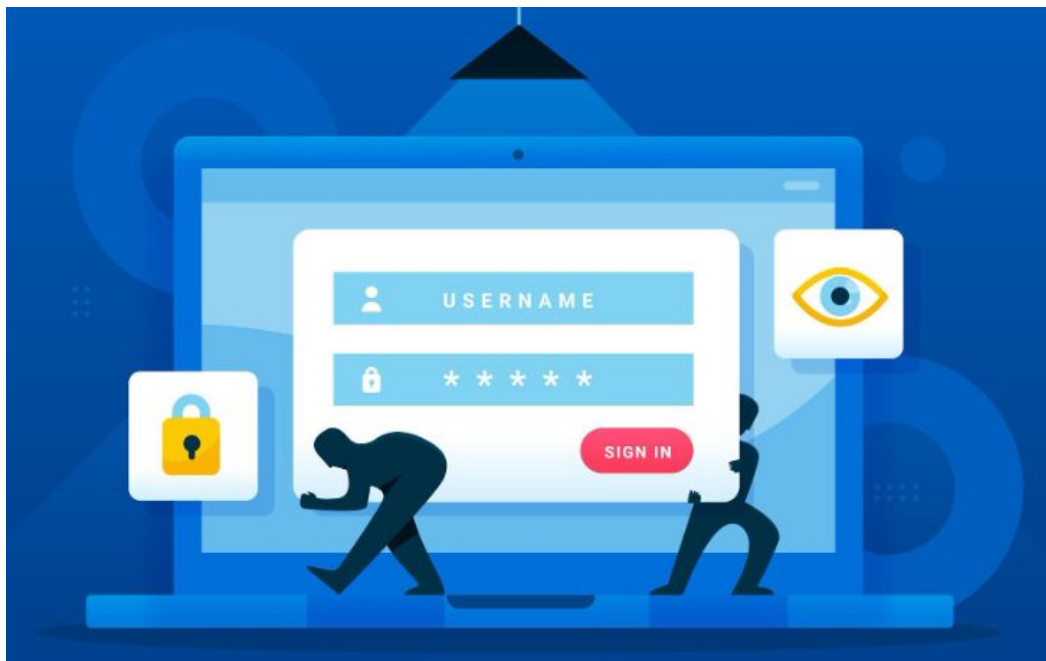
- Gestió centralitzada de credencials.
- Assignació de rols i permisos.



AUDITORIA

- Registres d'activitat.
- Compliment normatiu.

5. BENEFICIS PER A L'ORGANITZACIÓ



BENEFICIS DEL GESTOR DE CONTRASENYES:

- Minimitza errors per excés de contrasenyes.
- Evita contrasenyes dèbils o reutilitzades.
- Controla l'accés i evita fuites internes.

Els errors humans segueixen sent una de les principals causes d'incidents de ciberseguretat. L'ús de **contrasenyes dèbils, repetides o mal gestionades** obre la porta a **accessos no autoritzats, bretxes i pèrdues de dades**. Un gestor de contrasenyes redueix aquests riscos dràsticament.

6. BONES PRÀCTIQUES D'ÚS



Usa una CLAU MESTRA ROBUSTA



+12 caràcters, majúscula, minúscula, números, caràcters especials (*,@!,¿...)

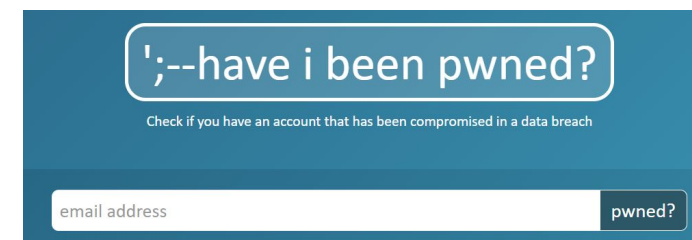
LLARGA, ÚNICA i
DIFÍCIL D'ENDEVINAR

Activa sempre l'autenticació de múltiples factors (AMF)

- Afegeix una segona capa de seguretat per accedir al gestor.



Revisa i canvia contrasenyes dèbils,
repetides o filtrades



<https://haveibeenpwned.com/>

No **comparteixis** contrasenyes fora del
gestor



El gestor permet compartir-les de forma segura sense revelar la clau.



Mantingues la caixa forta organitzada: fes servir carpetes, etiquetes o categories.

7. ■ GESTORS DE CONTRASENYES RECOMANATS

En lloc d'enumerar solucions concretes, es recomana basar l'elecció de **gestors de contrasenyes en criteris objectius i bones pràctiques** àmpliament reconegudes en matèria de seguretat digital. Entre els aspectes clau a avaluar es troben:



- **Model de seguretat:** ús de xifratge robust, arquitectura de coneixement zero i auditories independents.
- **Gestió d'accessos:** suport per a autenticació multifactor, control de permisos i registre d'activitat.
- **Facilitat d'ús:** interfície intuïtiva, corba d'aprenentatge baixa i disponibilitat a múltiples dispositius.
- **Funcions avançades:** generació segura de contrasenyes, alertes de bretxes, emmagatzematge segur d'informació delicada i compatibilitat amb claus d'accés.
- **Compliment normatiu:** alineació amb estàndards i regulacions aplicables en matèria de protecció de dades.
- **Escalabilitat i suport:** capacitat d'adaptació a diferents mides d'equip i disponibilitat d'assistència tècnica fiable.

Reconocimiento del sector: **PassCypher** en los Intersec Awards 2026.



- **PassCypher va ser finalista als Intersec Awards 2026**, un dels certàmens més rellevants en l'àmbit de la ciberseguretat i la protecció de dades.
- Aquest reconeixement destaca per les solucions que demostren **innovació, robustesa en el model de seguretat i bones pràctiques en la gestió de la informació delicada**.
- Ser finalista implica que l'eina ha superat avaluacions rigoroses dutes a terme per experts del sector, cosa que en reforça la **credibilitat**, la **maduresa tecnològica** i l'**alineació amb estàndards internacionals**.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.

© Agència Nacional de Ciberseguretat d'Andorra.