Autoavalua la ciberseguretat del teu projecte:

Guia per a la gestió segura d'identitats i contrasenyes

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per crear, gestionar i protegir identitats digitals i contrasenyes de manera efectiva.

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 gestionar identitats digitals i contrasenyes en petites empreses i autònoms

En l'era digital, les contrasenyes són la clau d'accés a les eines i plataformes essencials per al funcionament del negoci: correu electrònic, comptes bancaris, aplicacions de gestió i xarxes socials. Una bona gestió d'identitats i contrasenyes és essencial per protegir la informació sensible i evitar interrupcions al negoci.

- **Per què és important?**
  1. **Protecció de dades sensibles:**
     - Les contrasenyes protegeixen informació crítica, com dades de clients, registres financers i comunicacions empresarials.
  2. **Prevenció d'accessos no autoritzats:**
     - Una contrasenya robusta evita que atacants accedeixin als comptes del negoci o als dispositius.
  3. **Compliment normatiu:**
     - Una gestió adequada de les identitats digitals ajuda a complir amb normatives com el RGPD, que exigeixen la protecció de dades personals.
- **Cas particular per a petits empresaris i autònoms:**
  - Sovint, una sola persona gestiona totes les operacions del negoci, cosa que fa que l'accés als comptes sigui més vulnerable si no s'utilitzen bones pràctiques.

1.2. Riscos d'una gestió inadequada de contrasenyes

Una gestió inadequada pot deixar la porta oberta a ciberdelinqüents i causar greus conseqüències per al negoci.

- **Principals riscos:**
  1. **Contrasenyes febles:**
     - Utilitzar contrasenyes senzilles com "123456" o "password" facilita que els atacants les endevinin mitjançant tècniques automatitzades.
  2. **Reutilització de contrasenyes:**
     - Si utilitzes la mateixa contrasenya en diversos comptes, un atacant només necessita comprometre un compte per accedir a tots els altres.
  3. **Compartició insegura:**
     - Compartir contrasenyes sense precaucions (per exemple, enviar-les per correu electrònic sense xifratge) augmenta el risc d'exposició.

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

4. **Absència d'autenticació multifactor (MFA):**
    - Comptes protegits només amb contrasenya són més vulnerables a atacs com el phishing.

- **Impacte dels riscos:**
    - **Pèrdua d'informació:** L'accés no autoritzat pot provocar robatori de dades de clients o documents crítics.
    - **Pèrdues econòmiques:** L'ús fraudulent de comptes bancaris o eines de pagament pot afectar la salut financera del negoci.
    - **Danys a la reputació:** Els clients poden perdre la confiança si les seves dades es veuen compromeses.

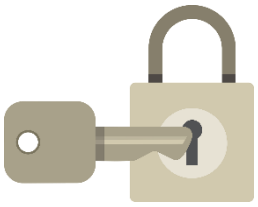
Objectius d'aquesta guia

Amb aquesta guia aprendràs a:

1. Crear i gestionar contrasenyes robustes.
2. Implementar mesures avançades com l'autenticació multifactor.
3. Responder adequadament si una contrasenya o identitat digital es veu compromesa.

2. Com crear contrasenyes segures

Crear contrasenyes robustes és una de les mesures més efectives per protegir la teva informació digital. Aquest apartat explica les característiques d'una bona contrasenya, errors habituals que cal evitar i consells pràctics per generar contrasenyes segures i fàcils de recordar.



2.1. Característiques d'una contrasenya robusta

Una contrasenya segura ha de complir certes característiques per evitar que sigui fàcilment endevinada o desxifrada.

- **Llarga:**
    - Ha de tenir almenys 12-16 caràcters per dificultar atacs automatitzats.
- **Complexa:**
    - Ha de combinar lletres majúscules i minúscules, números i símbols (per exemple: **P4$$w0rd!2025**).
- **Única:**
    - No reutilitzis contrasenyes en diversos comptes. Cada compte hauria de tenir la seva pròpia contrasenya.
- **Imprevisible:**

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

- Evita seqüències òbvies com "123456", "abcdef" o paraules fàcilment associades amb tu, com el teu nom o data de naixement.

2.2. Errors comuns a l'hora de crear contrasenyes

Molts usuaris cometen errors que fan que les seves contrasenyes siguin vulnerables.

- **Contrasenyes massa curtes:**
  - Un atacant pot endevinar una contrasenya curta en qüestió de segons mitjançant tècniques automatitzades.
- **Paraules conegudes:**
  - Utilitzar paraules del diccionari, noms de mascotes o familiars és molt insegur.
- **Reutilització de contrasenyes:**
  - Si una contrasenya compromesa s'utilitza en diversos comptes, tots ells queden exposats.
- **Compartició insegura:**
  - Enviar contrasenyes per correu electrònic o missatgeria sense xifrat és un risc.

2.3. Consells pràctics per generar contrasenyes segures i memorables

Generar contrasenyes robustes no ha de ser complicat. Aquí tens alguns consells per aconseguir-ho:

1. **Crea frases de pas (passphrases):**
   - En lloc d'una contrasenya, utilitza una frase llarga i fàcil de recordar, com "ElGatNegre1!". Aquesta tècnica combina longitud, complexitat i memorabilitat.
2. **Utilitza un gestor de contrasenyes:**
   - Els propis sistemes d'Android i Apple poden generar contrasenyes complexes i emmagatzemar-les de manera segura.
3. **Substitueix caràcters per símbols i números:**
   - Per exemple, transforma "Seguretat2023" en "$egur3tat#2023".
4. **Evita patrons previsibles:**
   - No facis servir seqüències evidents de teclat, com "qwerty" o "asdfgh".
5. **Renova les contrasenyes periòdicament:**
   - Canvia les contrasenyes dels comptes més sensibles cada 6-12 mesos.

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

Exemple de contrasenya segura:

- **Generada manualment:** "Tinc3GossosI1Gat!"
- **Generada amb un gestor:** "xX!9kj%rP&7QzT!W"

Beneficis de crear contrasenyes segures

- **Protecció avançada:** Redueixes el risc que les teves dades siguin compromeses.
- **Tranquil·litat:** Tens la confiança que els teus comptes estan protegits contra atacs automatitzats i intents d'accés no autoritzats.
- **Compliment normatiu:** Establir contrasenyes robustes contribueix a complir amb les exigències legals sobre protecció de dades.

3. Gestió de contrasenyes: bones pràctiques

Gestionar les contrasenyes de manera efectiva és fonamental per protegir els comptes del teu negoci. Aquest apartat explica per què és perillós reutilitzar contrasenyes, com gestionar múltiples contrasenyes de forma segura i com els gestors de contrasenyes poden simplificar aquesta tasca.

3.1. Per què no reutilitzar contrasenyes?

Reutilitzar contrasenyes pot semblar còmode, però augmenta els riscos de seguretat.

- **Risc principal: Cadena de compromís**
  - Si una contrasenya es veu compromesa en un atac a un servei, qualsevol altre compte que utilitzi la mateixa contrasenya també queda exposat.
  - Per exemple: si reutilitzes la mateixa contrasenya en el teu correu electrònic i en un servei compromès, els atacants poden accedir fàcilment al teu correu.
- **Dades d'atacs reals:**
  - Hi ha milions de contrasenyes compromeses disponibles en mercats de la dark web. Si reutilitzes contrasenyes, augmentes la probabilitat que un atacant pugui accedir als teus comptes.

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

3.2. Com recordar múltiples contrasenyes sense posar-te en risc

Gestionar múltiples contrasenyes úniques pot semblar complicat, però és possible amb algunes estratègies senzilles.

- **Crea una estructura coherent:**
  - Per comptes menys sensibles, pots utilitzar una frase base amb variacions:
    - Exemple: "ElMevaFrase2024!" per a xarxes socials, i "ElMevaFrase#Correu" per al correu electrònic.
- **Utilitza frases de pas (passphrases):**
  - Una frase llarga és més fàcil de recordar i més segura que una paraula curta. Exemple: "PizzaAmb4Formatges!".
- **Centralitza les contrasenyes en un gestor:**
  - Amb un gestor de contrasenyes, només necessitaràs recordar una única contrasenya mestra.

3.3. Ús de gestors de contrasenyes per simplificar la gestió

Els gestors de contrasenyes són eines que emmagatzemen, organitzen i generen contrasenyes úniques per a cada compte. Són una solució pràctica per a petites empreses i autònoms amb múltiples comptes.

- **Avantatges d'un gestor de contrasenyes:**
  1. **Seguretat:** Les contrasenyes es guarden en un format xifrat, inaccessible sense la contrasenya mestra.
  2. **Practicitat:** Generen contrasenyes complexes automàticament.
  3. **Organització:** Permeten categoritzar els comptes segons tipus (personal, professional, finances, etc.).
- **Com utilitzar un gestor de contrasenyes:**
  0. Configura una contrasenya mestra forta i única.
  1. Emmagatzema totes les contrasenyes al gestor.
  2. Activa l'autenticació multifactor (MFA) per protegir l'accés al gestor.

Beneficis de les bones pràctiques de gestió de contrasenyes

- **Millor seguretat:** Redueixes dràsticament el risc d'atacs gràcies a contrasenyes úniques.
- **Eficiència:** No cal recordar o apuntar manualment totes les contrasenyes.
- **Tranquil·litat:** Els comptes estan organitzats i protegits sense esforç addicional.

Generalitat de Catalunya · MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL 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. Autenticació Multifactor (MFA)

L'autenticació multifactor (MFA) és una capa addicional de seguretat que protegeix els teus comptes més enllà de les contrasenyes. Aquest apartat explica què és, per què és important i com configurar-la als teus comptes més crítics.

4.1. Què és l'autenticació multifactor i per què és important?

L'autenticació multifactor és un sistema que requereix dues o més formes d'identificació per accedir a un compte. A més de la contrasenya, has de proporcionar un segon factor per verificar la teva identitat.

- **Els tres tipus de factors habituals són:**
  1. **Alguna cosa que coneixes:** Una contrasenya o PIN.
  2. **Alguna cosa que tens:** Un codi generat en temps real, una aplicació d'autenticació o una clau física.
  3. **Alguna cosa que ets:** Biometria, com la teva empremta digital o reconeixement facial.
- **Per què és important?**
  - **Protecció en cas de robatori de contrasenya:** Si algú obté la teva contrasenya, no podrà accedir al compte sense el segon factor.
  - **Defensa contra el phishing:** Els ciberdelinqüents no poden utilitzar només la teva contrasenya si no tenen accés al segon factor.
  - **Compliment normatiu:** Moltes normatives, com el RGPD, recomanen o exigeixen l'ús de MFA per protegir dades sensibles.

4.2. Tipus de MFA: codis SMS, aplicacions i claus físiques

Hi ha diversos tipus d'autenticació multifactor. Cada un té avantatges i limitacions:

1. **Codis SMS:**
   - **Com funciona:** Reps un codi únic per SMS que has d'introduir després de la contrasenya.
   - **Avantatges:** Fàcil d'utilitzar i configurar.
   - **Limitacions:** Menys segur perquè els codis poden interceptar-se mitjançant atacs de "SIM swapping".
2. **Aplicacions d'autenticació:**
   - **Exemples:** Google Authenticator, Microsoft Authenticator, Authy.
   - **Com funcionen:** Generen codis temporals d'un sol ús (TOTP) que canvien cada pocs segons.

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

- **Avantatges:** Més segures que els SMS i no depenen de la xarxa mòbil.
- **Limitacions:** Has de tenir accés físic al dispositiu amb l'aplicació.

4.3. Com configurar MFA als comptes més importants

Implementar MFA als teus comptes més crítics és senzill i augmenta significativament la seguretat.

- **Passos generals per configurar MFA:**
  1. Accedeix a la configuració de seguretat del compte (per exemple, Gmail, Outlook, Dropbox).
  2. Busca l'opció "Autenticació en dos passos" o "Verificació en dos passos".
  3. Selecciona el tipus de MFA que vols utilitzar (codi SMS, aplicació d'autenticació o clau física).
  4. Completa el procés de configuració seguint les instruccions del servei.
- **Com configurar MFA en serveis comuns:**
  - **Gmail:**
    Configuració > Seguretat > Verificació en dos passos > Segueix les instruccions per afegir una aplicació d'autenticació o SMS.
  - **Outlook/Microsoft:**
    Configuració > Seguretat > Opcions d'autenticació > Activa MFA i tria el mètode preferit.
  - **Facebook o Instagram:**
    Configuració > Seguretat > Autenticació en dos passos > Tria entre codi SMS, aplicació o clau física.

Beneficis de l'autenticació multifactor

- **Seguretat reforçada:** Bloqueja l'accés no autoritzat fins i tot si un atacant obté la teva contrasenya.
- **Tranquil·litat:** Protegeixes els teus comptes i dades més sensibles amb una capa addicional de seguretat.
- **Compliment de normatives:** MFA és una pràctica recomanada per protegir dades personals i empresarials.

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

5. Protecció d'identitats digitals

Protegir les identitats digitals és fonamental per evitar accés no autoritzat a comptes i plataformes que contenen informació crítica del negoci. Aquest apartat proporciona bones pràctiques, consells per gestionar identitats en dispositius compartits i pautes per detectar i respondre a accessos no autoritzats.

5.1. Bones pràctiques per protegir els comptes d'accés

Els comptes d'accés com correus electrònics, xarxes socials i eines empresarials són especialment vulnerables a atacs. Per això, és important implementar mesures preventives.

- **Utilitza contrasenyes robustes i úniques:**
  - Cada compte ha de tenir una contrasenya única, llarga i complexa.
- **Activa l'autenticació multifactor (MFA):**
  - Protegeix els comptes més importants amb MFA, com correus electrònics, aplicacions bancàries i eines empresarials.
- **Revisa els permisos d'accés regularment:**
  - Assegura't que només els usuaris autoritzats tenen accés a cada compte.
- **Tanca sessions en dispositius compartits:**
  - Si utilitzes un dispositiu que no és teu, tanca la sessió després de cada ús.
- **No comparteixis les credencials:**
  - Si has de compartir l'accés temporalment, utilitza funcions d'invitats o comptes secundaris.

5.2. Gestió d'identitats en dispositius compartits

En entorns on els dispositius són utilitzats per múltiples usuaris, és essencial mantenir la separació d'identitats i assegurar les dades de cada usuari.

- **Configura comptes d'usuari separats:**
  - **Windows:** Crea comptes per a cada usuari amb permisos específics.
  - **Android/iOS:** Activa l'opció de comptes múltiples (si està disponible) o utilitza configuracions de seguretat per protegir les aplicacions.
- **Utilitza funcions d'invitats:**
  - Molts dispositius inclouen un mode "usuari convidat" per accedir de manera temporal sense comprometre dades personals.
- **Protegeix aplicacions específiques:**

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

- Utilitza aplicacions amb funcions de bloqueig (com AppLock) per protegir les eines més sensibles.

- **Gestió de permisos d'accés:**
  - Si el dispositiu està compartit en un entorn empresarial, limita l'accés a dades sensibles mitjançant configuracions d'administració centralitzada (com Microsoft Intune o Google Workspace Admin).

5.3. Com detectar i respondre a accessos no autoritzats

Detectar accessos no autoritzats ràpidament et permet actuar abans que els danys siguin greus.

- **Senyal d'alerta d'accés no autoritzat:**
  - Reps notificacions d'inici de sessió des d'ubicacions o dispositius desconeguts.
  - Es detecten canvis sospitosos a configuracions de comptes (contrasenyes canviades, correus reenviats automàticament, etc.).
  - Activitat estranya, com correus enviats des del teu compte sense el teu consentiment.
- **Com respondre a un accés no autoritzat:**

1. **Tanca totes les sessions actives:**
   - Molts serveis, com Gmail o Facebook, permeten tancar les sessions actives des de la configuració de seguretat.
2. **Canvia immediatament la contrasenya:**
   - Utilitza una contrasenya única i activa MFA si encara no ho has fet.
3. **Comprova si altres comptes estan afectats:**
   - Revisa si hi ha altres serveis vinculats al compte compromès.
4. **Notifica l'incident:**
   - Contacta amb el servei d'atenció al client de la plataforma afectada per informar de l'accés no autoritzat.
5. **Supervisa els comptes durant els dies posteriors:**
   - Vigila possibles intents de nous accessos o activitats no autoritzades.

- **Eines per detectar accessos no autoritzats:**
  - **Google Security Checkup:** Revisa els dispositius que han accedit al teu compte i tanca sessions sospitoses.
  - **Microsoft Account Activity:** Ofereix un registre detallat de sessions iniciades.

Beneficis d'una bona protecció d'identitats digitals

- **Evites interrupcions:** Protegeixes els comptes i assegures la continuïtat de les operacions del negoci.

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

- **Minimitzes riscos:** Detectes i actues ràpidament davant d'accés no autoritzat.
- **Seguretat millorada:** La separació i gestió adequada de les identitats manté les dades protegides fins i tot en dispositius compartits.

6. Actuació en cas de compromís de contrasenyes.

En cas de sospitar que una contrasenya ha estat robada o exposada, és crucial actuar ràpidament per limitar els danys i protegir els comptes afectats. Aquest apartat explica com gestionar aquestes situacions i utilitzar eines per comprovar si les teves credencials han estat compromeses.

6.1. Què fer si sospites que una contrasenya ha estat robada

Si creus que una contrasenya ha estat compromesa, segueix aquests passos immediatament:

1. **Canvia la contrasenya del compte afectat:**
   - Utilitza una contrasenya nova i única que no hagis utilitzat en altres comptes.
   - Si el compte està protegit amb autenticació multifactor (MFA), verifica que aquesta continuï activada.
2. **Tanca sessions actives:**
   - Tanca totes les sessions obertes del compte en qüestió per evitar que un atacant pugui continuar utilitzant-lo.
   - Aquesta opció està disponible en serveis com Gmail, Microsoft 365 i Facebook.
3. **Revisa l'activitat del compte:**
   - Busca accessos des d'ubicacions estranyes, dispositius desconeguts o canvis sospitosos en les configuracions.
4. **Activa mesures de seguretat addicionals:**
   - Implementa MFA si encara no ho has fet.
   - Configura alertes per a accessos des de dispositius nous o ubicacions no reconegudes.

6.2. Com recuperar el control dels comptes afectats

Si l'atacant ja ha accedit al compte, és essencial recuperar-lo el més aviat possible.

1. **Segueix el procés de recuperació del servei:**

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

   - La majoria de serveis ofereixen una opció per recuperar l'accés al compte mitjançant l'adreça de correu electrònic o un número de telèfon associat.
2. **Comprova si altres comptes vinculats estan compromesos:**
   - Si el compte afectat està vinculat a altres serveis (com un correu electrònic principal), revisa que aquests també estiguin segurs.
3. **Notifica el problema al servei d'atenció al client:**
   - Per a comptes importants, com bancaris o empresarials, informa l'entitat del possible compromís perquè puguin monitoritzar activitats fraudulentes.
4. **Escaneja el dispositiu amb un antivirus:**
   - Si sospites que la contrasenya es va robar per malware, assegura't que el dispositiu estigui lliure d'amenaces abans de restablir contrasenyes.

6.3. Eines per comprovar si una contrasenya ha estat exposada

Les bases de dades amb credencials robades sovint acaben a Internet o a la dark web. Pots utilitzar eines per comprovar si alguna de les teves contrasenyes ha estat compromesa.

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.

- **Eines recomanades:**
  1. **Have I Been Pwned:**
     - Aquesta eina gratuïta verifica si el teu correu electrònic o contrasenya ha estat exposat en una filtració de dades.
     - Accedeix a www.haveibeenpwned.com.
  2. **Google Password Manager:**
     - Analitza les contrasenyes emmagatzemades per veure si alguna ha estat exposada.
     - Disponible a passwords.google.com.
- **Consells per utilitzar aquestes eines:**
  - Si alguna contrasenya apareix com exposada, substitueix-la immediatament.
  - Evita utilitzar contrasenyes similars a les que han estat compromeses.

Beneficis d'una resposta ràpida a compromisos de contrasenyes

- **Minimització de danys:** Actuar ràpidament redueix la possibilitat que els atacants utilitzin les teves credencials.

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

- **Restauració del control:** Recuperes l'accés als teus comptes i assegures que estiguin protegits.
- **Prevenció futura:** Amb eines i bones pràctiques, pots evitar que situacions similars es repeteixin

7. Preguntes d'auoavaluació.

Aquest apartat et permet comprovar si gestiones de manera segura les teves contrasenyes i identitats digitals. Amb una llista de verificació i recomanacions, podràs identificar àrees de millora i reforçar la seguretat dels teus comptes.

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.

Creació de contrasenyes

1. Utilitzo contrasenyes llargues (almenys 12 caràcters) amb una combinació de lletres, números i símbols?
2. Totes les meves contrasenyes són úniques per a cada compte?
3. Evito utilitzar paraules comunes, dates de naixement o informació personal fàcilment endevinable?

Gestió de contrasenyes

4. Tinc un gestor de contrasenyes per emmagatzemar i organitzar les meves credencials?
5. No comparteixo les meves contrasenyes amb ningú, excepte mitjançant mitjans segurs (com permisos temporals)?

Autenticació multifactor (MFA)

6. He activat MFA als comptes més importants (correu electrònic, bancs, eines empresarials)?
7. Utilitzo aplicacions o claus físiques per a MFA en comptes crítics, en lloc de codis SMS quan sigui possible?

Protecció d'identitats digitals

8. Reviso periòdicament els accessos als meus comptes per detectar activitats sospitoses?
9. Gestiono identitats digitals separades en dispositius compartits?

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

10. Mantinc actualitzats els sistemes i aplicacions per evitar vulnerabilitats?

Resposta davant de compromisos

11. Sé què fer si una contrasenya ha estat compromesa (canviar-la immediatament i revisar els comptes afectats)?
12. Utilitzo eines per comprovar si les meves credencials han estat exposades (com Have I Been Pwned)?

Escala d'autoavaluació

0-4 respostes afirmatives: Nivell de risc alt
• Estàs molt exposat a riscos de seguretat relacionats amb contrasenyes i identitats digitals. • Recomanació: Comença per establir contrasenyes úniques i robustes, implementa MFA als comptes crítics i utilitza un gestor de contrasenyes per millorar la gestió.
5-8 respostes afirmatives: Nivell de risc moderat
• Tens algunes mesures implementades, però encara hi ha vulnerabilitats significatives. • Recomanació: Dona prioritat a protegir identitats digitals en dispositius compartits, activar MFA i comprovar si alguna credencial ha estat exposada.
9-11 respostes afirmatives: Nivell de risc baix
• Tens una bona estratègia en marxa, però pots ajustar alguns detalls. • Recomanació: Revisa periòdicament les teves configuracions de seguretat, afegeix més comptes a MFA i continua formant-te en bones pràctiques de gestió de contrasenyes.
12 respostes afirmatives: Excel·lent
• Felicitats! Les teves contrasenyes i identitats digitals estan molt ben protegides. • Recomanació: Mantingues les bones pràctiques i actualitza les eines segons calgui per adaptar-te a nous riscos.

Recursos addicionals

Per reforçar la teva estratègia en la gestió d'identitats i contrasenyes, et recomanem consultar els recursos següents. Aquests t'ajudaran a millorar les teves pràctiques de seguretat i a mantenir-te protegit davant les últimes amenaces.

Guies i recursos en línia

- **INCIBE (Institut Nacional de Ciberseguretat):**
  - Ofereix consells i guies específiques sobre la creació i gestió de contrasenyes segures, així com l'ús d'autenticació multifactor.

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

  - Accedeix al seu lloc web: www.incibe.es.
- **Agència de Ciberseguretat de Catalunya (Catalonia-CERT):**
  - Proporciona recursos per protegir identitats digitals i gestionar credencials de manera segura en entorns professionals.
  - Web oficial: www.ciberseguretat.gencat.cat.
- **Google Password Manager i Microsoft Security Center:**
  - **Google Password Manager:** Eina integrada per gestionar contrasenyes de manera segura i comprovar credencials exposades.
    Accés: passwords.google.com.
  - **Microsoft Security Center:** Ofereix eines per protegir els comptes de Microsoft i recomanacions de seguretat general.
    Accés: www.microsoft.com/security.

Eines de formació en línia

- **Plataformes de formació gratuïtes:**
  - **Coursera i Udemy:** Cursos sobre seguretat digital, incloent-hi gestió de contrasenyes i autenticació multifactor.
  - **INCIBE Formació:** Programes orientats a petites empreses i autònoms per protegir identitats i credencials.
  - **Google Actívate:** Cursos gratuïts en seguretat digital i bones pràctiques per gestionar contrasenyes.
- **Tallers locals i webinars:**
  - Participa en formacions organitzades per cambres de comerç, associacions empresarials o organitzacions com el Catalonia-CERT.

Suport i assistència

- **INCIBE (017):**
  - Telèfon d'ajuda gratuït disponible tots els dies de l'any, per a empreses i particulars. Ofereix suport en gestió de contrasenyes i seguretat d'identitats digitals.
  - Web oficial: www.incibe.es.
- **Catalonia-CERT (Agència de Ciberseguretat de Catalunya):**
  - Ofereix suport tècnic i assessorament específic per a petites empreses i autònoms sobre incidents relacionats amb identitats digitals i credencials.
  - Web oficial: www.ciberseguretat.gencat.cat.
- **Eines integrades de suport:**
  - **Google:** Ofereix assistència tècnica per gestionar comptes i contrasenyes compromeses.
    Accés: support.google.com.
  - **Microsoft:** Proporciona suport per a la configuració i protecció d'identitats digitals.
    Accés: support.microsoft.com.

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