Autoavalua la ciberseguretat del teu projecte:

Guia per a la gestió segura de l'ús de dispositius i programes pels col·laboradors

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per gestionar de manera segura l'ús de dispositius i programes pels col·laboradors.

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.

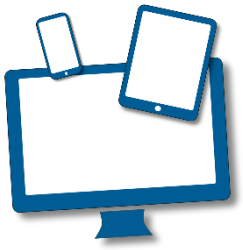
Es recomana comptar amb el suport d'un equip tècnic o servei informàtic especialitzat per garantir una implementació adequada de les mesures descrites. A més, assegura't de seguir sempre les instruccions oficials dels fabricants i desenvolupadors de software, aplicacions i dispositius que utilitzis, 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 l'ús de dispositius i programes pels col·laboradors



En l'entorn laboral actual, on les eines digitals són indispensables, gestionar correctament l'ús de dispositius i programes pels col·laboradors és clau per protegir la informació del negoci i garantir la seva operativitat. Aquesta gestió implica establir normes clares que assegurin que els dispositius i programes s'utilitzen de manera segura i responsable.

- **Què implica una bona gestió?**
  - Establir límits clars sobre l'ús de dispositius personals (**BYOD, "Bring Your Own Device"**).
  - Garantir que només es tingui accés a les dades necessàries segons el rol de cada col·laborador.
  - Controlar quins programes es poden instal·lar per evitar riscos associats al programari no verificat.
- **Per què és important?**
  - Els dispositius i programes gestionats correctament protegeixen les dades de clients i del negoci contra robatoris, pèrdues i filtracions.
  - Una política clara redueix la possibilitat d'incidents causats per errors humans, com la descàrrega de programari maliciós o la compartició accidental d'informació sensible.

1.2 Impacte d'una gestió deficient en petites empreses i autònoms

Les petites empreses i els autònoms sovint tenen menys recursos per gestionar incidents de ciberseguretat, per la qual cosa els efectes d'una gestió deficient poden ser greus.

- **Principals riscos d'una mala gestió:**
  - **Pèrdua d'informació sensible:**
    - Sense restriccions adequades, qualsevol persona pot accedir, modificar o eliminar dades importants del negoci.
  - **Infeccions per malware:**
    - L'ús de programari no autoritzat o descarregat de fonts insegures pot introduir malware als sistemes de l'empresa.
  - **Interrupcions en l'operativitat:**
    - Dispositius infectats o danyats poden paralitzar processos crítics del negoci.
  - **Incompliment legal:**
    - Si les dades personals de clients es veuen compromeses, el negoci podria infringir normatives com el RGPD, comportant sancions econòmiques.

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

- **Exemples de conseqüències comunes:**
  - Un col·laborador utilitza un dispositiu personal no protegit per accedir a dades sensibles, i aquest es perd o és robat.
  - La instal·lació d'un programa no autoritzat introdueix un ransomware que bloqueja l'accés als sistemes del negoci.
  - L'absència de restriccions en l'accés permet que un treballador accedeixi a informació que no necessita per al seu rol, comprometent la privacitat d'altres col·laboradors o clients.

1.3 Objectius d'aquesta guia

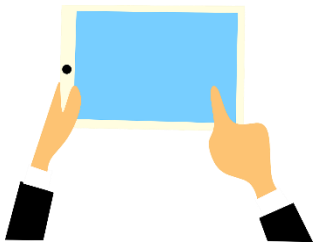
Aquesta guia té com a finalitat:

1. Proporcionar normes clares i pràctiques per gestionar l'ús de dispositius i programes de manera segura.
2. Ajudar-te a identificar i prevenir riscos associats a una gestió deficient.
3. Preparar-te per implementar polítiques efectives que protegeixin el teu negoci i les seves dades.

Amb aquestes bases, podràs establir un marc segur i eficient per al treball amb dispositius i programes dins del teu negoci.

2. Bones pràctiques per utilitzar dispositius personals (BYOD)

2.1. Què és el BYOD i quins són els seus riscos i beneficis



- **Què és el BYOD?** El BYOD ("Bring Your Own Device") és una pràctica en què els col·laboradors utilitzen els seus dispositius personals (ordinadors, mòbils o tauletes) per accedir a sistemes, dades i eines de treball de l'empresa. És una opció comuna en petites empreses i autònoms, ja que pot reduir costos en equipament i permet una major flexibilitat.

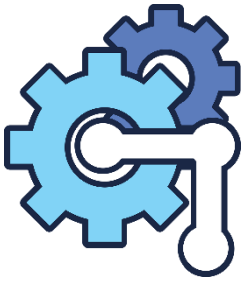
- **Beneficis del BYOD:**
  - **Estalvi de costos:** Els col·laboradors utilitzen els seus dispositius, evitant despeses en maquinari.
  - **Flexibilitat i comoditat:** Els treballadors poden utilitzar equips que ja coneixen.
  - **Mobilitat:** Facilita el treball remot o en mobilitat, ja que els dispositius personals sovint estan preparats per connectar-se a xarxes diverses.

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

- **Riscos del BYOD:**
  - **Pèrdua o robatori del dispositiu:** Si un dispositiu amb accés a dades sensibles es perd o és robat, la informació pot quedar exposada.
  - **Dispositius no protegits:** Els dispositius personals poden no complir els estàndards de seguretat del negoci, deixant les dades vulnerables.
  - **Barreja d'ús personal i professional:** Pot generar confusió sobre quines dades són privades i quines pertanyen al negoci.

2.2. Normes clares per a un ús segur de dispositius personals al treball

Per implementar el BYOD de manera segura, és imprescindible establir normes clares que protegeixin tant el negoci com els col·laboradors.



1. **Definir els dispositius permesos:**
   - Especifica quins tipus de dispositius són compatibles amb les necessitats de l'empresa (mòbils, portàtils, etc.).
   - Limita l'accés a dispositius que compleixin uns estàndards mínims de seguretat (sistema operatiu actualitzat, antivirus instal·lat, etc.).
2. **Configurar acords d'ús:**
   - Redacta un document que expliqui:
     - Quins sistemes i dades es poden accedir des de dispositius personals.
     - Les responsabilitats dels col·laboradors per mantenir els dispositius segurs.
     - Les conseqüències de no complir les normes (per exemple, restricció d'accés o altres mesures).
3. **Separar ús personal i professional:**
   - Promou l'ús d'aplicacions separades per treball i ús personal (per exemple, apps de correu electrònic o emmagatzematge al núvol específiques per al treball).
4. **Prohibir l'ús de dispositius compromesos:**
   - No permetis l'accés al sistema des de dispositius que hagin estat infectats amb malware o que hagin estat "rootejats" o modificats.

2.3. Configuracions bàsiques de seguretat per als dispositius BYOD

Garantir que els dispositius personals compleixin amb els estàndards de seguretat del negoci és essencial. Aquí tens algunes configuracions bàsiques:

- **Protecció amb contrasenyes robustes:**
  - Exigeix contrasenyes llargues i úniques, preferiblement amb autenticació multifactor (2FA).
- **Actualitzacions i parches:**

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

    - Els dispositius han de tenir el sistema operatiu i les aplicacions sempre actualitzades per tancar vulnerabilitats.
- **Antivirus i tallafocs:**
    - Assegura't que tots els dispositius personals utilitzin un programa antivirus actiu i configurin un tallafocs per protegir la connexió.
- **Xifrat de dades:**
    - Activa el xifrat al dispositiu per protegir les dades en cas de pèrdua o robatori.
- **Control de connexions:**
    - Configura els dispositius per connectar-se només a xarxes Wi-Fi segures o utilitza una VPN per protegir la comunicació.
- **Aplicacions segures:**
    - Utilitza només aplicacions verificades i de confiança per accedir a les dades i eines del negoci.

Beneficis d'aplicar bones pràctiques en BYOD

- **Seguretat reforçada:** Els dispositius personals són una extensió segura del sistema del negoci.
- **Tranquil·litat:** Tant el negoci com els col·laboradors saben que les dades estan protegides.
- **Productivitat millorada:** Els col·laboradors poden treballar des de qualsevol lloc amb la confiança que compleixen les normes de seguretat.

3. Gestió de permisos i accés a dades segons el rol

Una gestió adequada dels permisos i l'accés a dades és essencial per protegir la informació sensible d'una empresa, especialment en petites empreses i negocis autònoms, on les estructures poden ser menys complexes però igualment vulnerables.

3.1. Com assignar permisos per protegir informació sensible

Una estratègia clara per assignar permisos ajuda a garantir que només les persones adequades accedeixin a les dades necessàries.

- **Principi del mínim privilegi:**
    - Dona als col·laboradors accés només a la informació i eines necessàries per al seu rol específic.
    - Evita donar permisos generals que incloguin informació no relacionada amb les seves responsabilitats.

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

- **Segmentació de dades:**
  - Organitza la informació en nivells o categories segons la seva sensibilitat (p. ex., dades públiques, internes, confidencials).
  - Limita l'accés a nivells més alts només a persones autoritzades.
- **Assignació de rols clars:**
  - Defineix rols específics (per exemple, administradors, comercials, tècnics) i vincula els permisos a aquests rols.
  - Redueix la necessitat d'assignar permisos manualment a cada usuari.

3.2. Bones pràctiques per gestionar l'accés a dades i sistemes

Una bona gestió de l'accés redueix riscos de filtracions i errors humans. Segueix aquestes pràctiques per mantenir els sistemes segurs:

1. **Revisions periòdiques:**
   - Revisa regularment els permisos assignats per assegurar-te que són adequats per al rol actual del col·laborador.
   - Elimina l'accés de treballadors que han deixat el negoci o han canviat de funció.
2. **Autenticació multifactor (MFA):**
   - Implementa MFA per protegir els comptes d'accés a dades i sistemes, afegint una capa extra de seguretat.
3. **Control d'accés temporal:**
   - Per a tasques específiques, proporciona accés temporal que s'elimina automàticament després d'un període determinat.
4. **Registre d'activitats:**
   - Registra qui accedeix a què, quan i des d'on. Això ajuda a detectar accessos no autoritzats i a monitoritzar l'ús adequat dels permisos.
5. **Polítiques d'accés remotes:**
   - Si els col·laboradors treballen de manera remota, assegura't que accedeixen als sistemes a través de connexions segures, com una VPN.

3.3. Eines per supervisar i restringir l'accés segons el rol

Hi ha moltes eines que poden ajudar-te a gestionar l'accés als sistemes i dades de manera efectiva:

- **Gestió d'usuaris i permisos:**

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

  - **Microsoft Active Directory:** Ideal per gestionar permisos en entorns Windows.
  - **Google Workspace Admin:** Permet gestionar permisos i accés a fitxers i aplicacions per a col·laboradors que utilitzin Google Workspace.
- **Control de fitxers:**
  - **Box o Dropbox Business:** Permeten gestionar qui pot veure, editar o compartir documents dins de l'empresa.
  - **OneDrive for Business:** Ofereix eines similars amb integració directa amb l'entorn Microsoft.

Beneficis d'una bona gestió de permisos

- **Protecció de dades sensibles:** Evites accessos no autoritzats i minimitzes riscos de filtració.
- **Compliment normatiu:** Les polítiques d'accés ajuden a complir normatives com el RGPD.
- **Eficiència operativa:** L'accés ben organitzat facilita el treball dels col·laboradors sense comprometre la seguretat.

4. Restriccions per instal·lar programari no autoritzat

Permetre la instal·lació de programes no verificats o no autoritzats pot comprometre la seguretat del negoci. Aquest apartat detalla els riscos d'aquestes pràctiques, polítiques efectives per gestionar-les i eines útils per mantenir un control adequat.

4.1. Perills de programes no verificats i no autoritzats

Els programes no verificats poden semblar inofensius, però sovint introdueixen vulnerabilitats al sistema o poden ser directament maliciosos.

- **Principals riscos:**
  1. **Malware i ransomware:**
     - Els programes descarregats de fonts no fiables poden incloure malware que infecta el sistema.
  2. **Filtració de dades:**
     - Algunes aplicacions poden recopilar dades personals o sensibles sense el teu coneixement.
  3. **Compatibilitat i rendiment:**
     - Els programes no oficials poden ser incompatibles amb altres eines de l'empresa, causant errors i reduint el rendiment del dispositiu.
  4. **Incompliment normatiu:**

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

- L'ús de programari pirata o no autoritzat pot infringir normatives i exposar el negoci a sancions.

4.2. Polítiques per controlar la instal·lació de programes en dispositius corporatius

Establir normes clares per gestionar quins programes es poden instal·lar és crucial per mantenir la seguretat i el rendiment dels dispositius del negoci.

- **Normes bàsiques de control:**
  1. **Definir programes autoritzats:**
     - Elabora una llista de programes aprovats per al negoci (per exemple, suites ofimàtiques, programes de disseny o eines de gestió).
  2. **Prohibir instal·lacions sense autorització:**
     - Estableix una política que requereixi l'aprovació prèvia abans d'instal·lar qualsevol programari nou.
  3. **Ús exclusiu de fonts oficials:**
     - Només permet la descàrrega i instal·lació de programes des de botigues d'aplicacions oficials (Google Play, App Store) o pàgines verificades dels proveïdors.
  4. **Revisió periòdica:**
     - Programa revisions periòdiques per assegurar-te que els dispositius només tenen instal·lats programes autoritzats.
- **Com comunicar aquestes polítiques:**
  - Crea un document senzill que expliqui aquestes normes.
  - Proporciona exemples clars de programes autoritzats i no autoritzats.

4.3. Eines per monitoritzar i restringir l'ús de programari no autoritzat

Existeixen diverses eines que poden ajudar-te a controlar i supervisar quins programes s'instal·len als dispositius del negoci.

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.

- **Solucions per supervisar la instal·lació de programes:**
  - **Microsoft Intune:** Permet gestionar dispositius i aplicacions en entorns Windows i mòbils.
  - **Jamf:** Ideal per gestionar dispositius Apple en petites empreses.
  - **ManageEngine Desktop Central:** Ofereix funcions de supervisió i control d'instal·lacions.

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

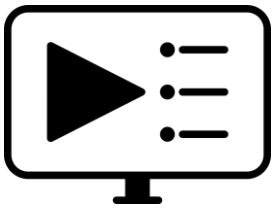
- **Eines per bloquejar instal·lacions no autoritzades:**
  - **AppLocker (Windows):** Permet crear regles per bloquejar programes específics o restringir les instal·lacions a programes verificats.
  - **Symantec Endpoint Protection:** Inclou opcions per monitoritzar i restringir l'execució de programes no autoritzats.
- **Monitorització d'activitat:**
  - **SolarWinds Patch Manager:** Ajuda a supervisar i mantenir programes actualitzats, assegurant-te que només hi ha programari legítim.

Beneficis d'una política estricta sobre programari

- **Reducció de riscos:** Evites infeccions per malware i problemes de seguretat associats a programes no verificats.
- **Compliment normatiu:** Garanteixes que tot el programari utilitzat compleix amb les lleis i llicències aplicables.
- **Millora del rendiment:** Els dispositius funcionen millor sense programes innecessaris o problemàtics.

5. Mesures preventives i formació per col·laboradors

La formació i la conscienciació dels col·laboradors són elements essencials per garantir l'aplicació correcta de les polítiques d'ús de dispositius i programes. Aquest apartat detalla com educar l'equip i sensibilitzar-lo sobre la importància de seguir bones pràctiques.



5.1. Educació en bones pràctiques d'ús de dispositius i programes

Els errors humans són una de les causes principals de problemes de seguretat en petites empreses. Educar els col·laboradors ajuda a prevenir incidents i fomenta un entorn més segur.

- **Temes clau de formació:**
  1. **Ús responsable de dispositius:**
     - Com mantenir dispositius segurs (per exemple, actualitzacions, contrasenyes robustes, ús d'antivirus).
  2. **Distinció entre ús personal i professional:**
     - Separar clarament les activitats personals de les laborals en dispositius utilitzats per treballar.
  3. **Gestió de programes:**

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

        - Només utilitzar programes verificats i autoritzats per l'empresa.
    4. **Prevenció d'errors comuns:**
        - Evitar fer clic en enllaços sospitosos o descarregar fitxers de fonts desconegudes.
- **Mètodes per impartir formació:**
    - **Tallers i sessions presencials o en línia:** Focalitzats en temes pràctics.
    - **Infografies i vídeos curts:** Materials visuals que expliquin bones pràctiques de forma senzilla.
    - **Simulacions:** Proves de phishing o altres incidents per educar sobre com actuar.

5.2. Creació d'un manual de polítiques clares i senzilles

Un document que resumeixi les polítiques del negoci facilita que els col·laboradors sàpiguen exactament què fer i què evitar.

- **Què incloure en el manual:**
    1. **Normes generals:**
        - Per exemple, "No descarreguis programes sense autorització" o "Utilitza una VPN quan treballis fora de l'oficina".
    2. **Rols i responsabilitats:**
        - Descriu què s'espera de cada col·laborador pel que fa a la seguretat digital.
    3. **Llista de programes autoritzats i no autoritzats.**
    4. **Procediments per reportar incidents:**
        - Instruccions senzilles sobre com informar d'un problema de seguretat (per exemple, correus sospitosos o pèrdua de dispositius).
- **Com distribuir-lo:**
    - Proporciona'l en format digital (per exemple, un PDF accessible per a tots els col·laboradors) i assegura't que tots l'han llegit i entès.

5.3. Casos pràctics per sensibilitzar sobre els riscos

Els exemples reals o simulacions són una eina efectiva per mostrar l'impacte que poden tenir les males pràctiques.

- **Exemples d'incidents habituals:**
    1. **Phishing:** Simula un correu sospitós i analitza com responen els col·laboradors.

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

2. **Instal·lació de programari maliciós:** Explica un cas on un programa no autoritzat va introduir malware al sistema d'una empresa.
3. **Accés indegut a dades sensibles:** Demostra com l'ús indegut de permisos pot posar en risc la informació del negoci.

- **Objectius dels casos pràctics:**
  - Mostrar com les accions individuals poden afectar la seguretat de tot el negoci.
  - Fomentar una cultura de seguretat i responsabilitat col·lectiva.
- **Com implementar-los:**
  - Organitza sessions periòdiques amb exemples reals o simulats.
  - Utilitza materials visuals (vídeos, captures de pantalla) per fer-ho més comprensible.

Beneficis de les mesures preventives i formació

- **Reducció de riscos:** Els col·laboradors formats són menys propensos a cometre errors que comprometin la seguretat.
- **Protecció col·lectiva:** Tota l'empresa es beneficia d'un equip conscient i preparat.
- **Compliment normatiu:** La formació adequada ajuda a complir normatives com el RGPD.

6. Preguntes d'autoavaluació

L'autoavaluació t'ajuda a mesurar si les polítiques d'ús de dispositius i programes estan implementades correctament i identificar àrees de millora. Aquesta secció inclou una llista de verificació i recomanacions per optimitzar la gestió dins del teu negoci.

6.1. 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.

Polítiques d'ús de dispositius (BYOD)

1. Tots els dispositius personals utilitzats per al treball compleixen els estàndards mínims de seguretat (antivirus, actualitzacions, xifrat de dades)?

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

2. Existeixen normes clares que separen l'ús personal i professional en dispositius BYOD?
3. Els col·laboradors han signat un acord d'ús de dispositius personals que inclou les seves responsabilitats?

Gestió de permisos i accés a dades

4. L'accés a dades sensibles està limitat segons el rol de cada col·laborador?
5. Utilitzeu autenticació multifactor (MFA) per accedir a sistemes i dades importants?
6. Es revisen periòdicament els permisos d'accés per assegurar que estan actualitzats i són necessaris?

Control del programari instal·lat

7. Només s'instal·len programes autoritzats i verificats en els dispositius del negoci?
8. Hi ha eines o polítiques que impedeixen la instal·lació de programari no autoritzat?
9. Es revisen regularment els programes instal·lats per eliminar aplicacions no necessàries?

Formació i sensibilització

10. Els col·laboradors han rebut formació en bones pràctiques d'ús de dispositius i programes?
11. Es disposa d'un manual o document que resumeixi les polítiques d'ús de l'empresa?
12. S'han realitzat casos pràctics o simulacions per sensibilitzar els col·laboradors sobre els riscos?

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

6.2. Resultats i Recomanacions

0-5 respostes afirmatives: Nivell de risc alt
• Estàs molt exposat a riscos relacionats amb l'ús inadequat de dispositius i programes. • Recomanació: Comença per establir polítiques bàsiques d'ús, implementar controls sobre els dispositius i programari, i formar els col·laboradors.
5-8 respostes afirmatives: Nivell de risc moderat
• Tens algunes mesures implementades, però encara hi ha vulnerabilitats importants. • Recomanació: Dona prioritat a reforçar les polítiques, gestionar millor els permisos i restringir la instal·lació de programari no autoritzat.
9-11 Respostes afirmatives: Nivell de risc baix
• Tens una bona estratègia en marxa, però pots ajustar certs aspectes per millorar encara més. • Recomanació: Realitza revisions periòdiques i assegura't que tot l'equip coneix i segueix les polítiques establertes.
12 Respostes afirmatives: Excel·lent
• Felicitats! Tens unes polítiques d'ús molt ben implementades i efectives. • Recomanació: Mantingues les bones pràctiques, i actualitza les polítiques segons les noves necessitats o tecnologies.

6.3. Recursos addicionals

Per reforçar la teva estratègia en la gestió segura de dispositius i programes pels col·laboradors, et recomanem consultar els recursos següents. Aquests t'ajudaran a millorar les polítiques d'ús i a mantenir-te actualitzat sobre les millors pràctiques en seguretat digital.

Guies i recursos en línia

- **INCIBE (Institut Nacional de Ciberseguretat):**
  - Ofereix guies i eines gratuïtes per implementar polítiques clares d'ús de dispositius i programes.
  - Accedeix al seu lloc web: www.incibe.es.
- **Agència de Ciberseguretat de Catalunya (Catalonia-CERT):**
  - Proporciona recursos específics per a petites empreses, incloent-hi consells sobre gestió de dispositius i permisos.
  - Web oficial: www.ciberseguretat.gencat.cat.
- **Google Workspace Admin Center:**
  - Inclou bones pràctiques per gestionar permisos, usuaris i dispositius en entorns de treball col·laboratiu.

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

- Accés: Workspace Admin Center.

Eines de formació en línia

- **Plataformes de formació gratuïtes:**
  - **Coursera i Udemy:** Cursos introductoris en ciberseguretat i gestió d'identitats digitals.
  - **INCIBE Formació:** Programes orientats a petites empreses i autònoms per millorar la seguretat digital.
  - **Google Actívate:** Cursos sobre seguretat digital i bones pràctiques d'ús de dispositius.
- **Tallers locals i webinars:**
  - Participa en formacions organitzades per cambres de comerç, associacions empresarials o organitzacions regionals com el Catalonia-CERT.

Suport i assistència

- **INCIBE (017):**
  - Telèfon d'ajuda gratuït per a empreses i particulars, disponible tots els dies de l'any. Pots consultar dubtes sobre gestió d'usuaris, permisos i altres polítiques.
- **Catalonia-CERT:**
  - Servei regional per assessorar en la implementació de polítiques i respondre a incidents de seguretat.
- **Suport dels proveïdors de les eines que utilitzes:**
  - Proveïdors com Google Workspace, Microsoft Intune o Dropbox Business ofereixen documentació i assistència tècnica per optimitzar la gestió de dispositius i permisos.

Aquests recursos t'ajudaran a establir polítiques efectives i a mantenir el teu negoci protegit contra els riscos associats a una mala gestió de dispositius i programes.

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