Autoavalua la ciberseguretat del teu projecte:

Navegació segura a Internet

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per a una navegació segura, la protecció de dades i la prevenció de riscos digitals.

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: navegació segura a Internet

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 la navegació segura per a petits negocis i autònoms

La navegació a Internet és una eina indispensable per a la majoria d'autònoms i petites empreses. Permet accedir a clients, gestionar comandes, comunicar-se amb proveïdors i fins i tot realitzar tràmits administratius. Però aquesta connexió constant també comporta riscos.

Els negocis petits solen ser un objectiu fàcil per als ciberdelinqüents perquè, sovint, no tenen els mateixos recursos de seguretat que les grans empreses. Una navegació insegura pot portar a problemes com:

- **Pèrdua de dades**: Els atacs poden robar informació confidencial del negoci o dels clients.
- **Infeccions per malware**: L'accés a llocs web maliciosos pot introduir programes que danyen el sistema.
- **Fraus financers**: Transaccions insegures poden resultar en robatoris o pèrdues econòmiques.

Adoptar bones pràctiques de navegació segura és una inversió senzilla i molt efectiva per protegir el teu projecte o negoci.

Principals riscos d'una navegació insegura

Quan navegues per Internet, et pots trobar amb diverses amenaces que podrien comprometre la seguretat de les teves dades o dels teus dispositius. Aquests són els riscos més comuns:

1. **Phishing**:
   - Correus electrònics o llocs web falsos que intenten enganyar-te per obtenir dades personals, com contrasenyes o informació bancària.
2. **Llocs web maliciosos**:
   - Pàgines dissenyades per instal·lar programari maliciós al teu dispositiu o robar dades sensibles.
3. **Connexions insegures**:
   - Navegar en llocs sense HTTPS o connectar-te a xarxes Wi-Fi públiques pot exposar la teva informació a interceptacions.
4. **Descàrregues perilloses**:
   - Arxius que aparenten ser inofensius però contenen malware o virus.

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

Objectius d'aquesta guia

Aquesta guia té com a finalitat ajudar-te a:

- **Reconèixer riscos**: Identificar llocs web, correus o pràctiques insegures.
- **Aplicar mesures senzilles**: Implementar hàbits que garanteixin la teva seguretat a Internet.
- **Millorar la teva tranquil·litat**: Saber que la teva navegació i les teves dades estan protegides.

2. Identificació de Llocs Web Segurs

Saber reconèixer si un lloc web és segur és una habilitat essencial per protegir les teves dades i el teu negoci. Petites empreses i autònoms sovint accedeixen a portals per fer compres, gestions o treballar amb clients, i garantir que aquests llocs són fiables és clau per evitar problemes.

2.1. Com reconèixer llocs amb HTTPS i certificats vàlids

Els llocs web segurs utilitzen el protocol HTTPS (HyperText Transfer Protocol Secure), que xifra la comunicació entre el teu navegador i el servidor. Això evita que tercers puguin interceptar les dades que envies o reps.

- **Com detectar HTTPS**:
  - Assegura't que l'adreça del lloc comença amb **https://**.
  - Cerca un **candau** a la barra d'adreces del navegador. Un candau tancat indica que el lloc web utilitza xifratge.
- **Certificats vàlids**:
  - Fes clic al candau per verificar que el certificat és vàlid i no ha expirat.
  - Els navegadors solen mostrar alertes si el certificat no és de confiança o està caducat. Evita interactuar amb aquests llocs.
- **Exemple pràctic**:
  - Una botiga en línia amb HTTPS i un certificat vàlid és molt més fiable que una que utilitza HTTP, ja que aquesta última no protegeix la informació.

Generalitat de Catalunya · 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

2.2. Com detectar llocs web sospitosos

No tots els llocs web són el que semblen. Aprendre a identificar senyals de sospita t'ajuda a evitar problemes.

- **Adreces estranyes**:
  - Desconfia de llocs amb noms d'adreça inusuals, errors tipogràfics (com **goooogle.com** en lloc de **google.com**) o extensions poc conegudes (com .xyz, .top, etc.).
- **Contingut de baixa qualitat**:
  - Llocs amb moltes faltes d'ortografia, dissenys poc professionals o contingut desordenat solen ser menys fiables.
- **Pàgines amb massa anuncis**:
  - Si un lloc té un excés de publicitat intrusiva o finestres emergents, pot ser sospitós.
- **Sospites al processar pagaments**:
  - Si un lloc web et demana informació bancària o personal en una pàgina sense HTTPS, és un senyal clar de perill.

2.3. Eines per verificar la seguretat d'un lloc web

Existeixen eines gratuïtes que t'ajuden a confirmar si un lloc web és segur abans d'interactuar-hi.

- **Google Transparency Report**:
  - Comprova l'estat de seguretat d'un lloc web introduint l'URL a transparencyreport.google.com.
- **VirusTotal**:
  - Escaneja un lloc web per detectar si està associat amb programari maliciós o amenaces. Disponible a virustotal.com.
- **Extensions del navegador**:
  - Eines com **Web of Trust (WOT)** o **Netcraft** poden alertar-te de llocs web perillosos en temps real.

2.4. Consells pràctics per petites empreses i autònoms

- **No confiïs cegament en enllaços**:
  - Evita fer clic en enllaços enviats per correu electrònic o missatgeria si no estàs segur del seu origen.
- **Verifica abans d'introduir dades**:
  - Abans d'introduir contrasenyes, dades de clients o informació bancària, assegura't que el lloc és segur.

Generalitat de Catalunya · 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

- **Educa't i educa el teu equip**:
  - Comparteix aquestes bones pràctiques amb qualsevol persona que treballi amb tu per garantir que tots estigueu protegits.

Beneficis d'identificar llocs segurs

- **Protecció de dades**: Redueixes el risc que informació sensible sigui robada o interceptada.
- **Confiança en els negocis en línia**: Pots operar amb seguretat en compres o col·laboracions digitals.
- **Tranquil·litat**: Saps que estàs prenent les mesures adequades per protegir el teu negoci.

3. Evitar Llocs Maliciosos i Descàrregues Sospitoses

Els llocs web maliciosos i les descàrregues sospitoses són fonts comunes d'infeccions per malware i robatori d'informació. Aquest punt ofereix consells pràctics per detectar i evitar aquestes amenaces mentre navegues per Internet.

3.1. Bones pràctiques per evitar enllaços enganyosos i anuncis perillosos

- **Desconfia d'enllaços no verificats**:
  - Evita fer clic en enllaços de correus electrònics, missatges o xarxes socials si no estàs segur del seu origen.
  - Passa el ratolí per sobre de l'enllaç per veure l'adreça real abans de clicar-hi. Si sembla estranya o sospitosa, no la segueixis.
- **Compte amb els anuncis intrusius**:
  - Molts llocs maliciosos utilitzen anuncis falsos que prometen premis o ofertes irresistibles per atraure't.
  - Evita fer clic en anuncis que semblen massa bons per ser veritat.
- **Utilitza navegadors amb bloquejadors d'anuncis**:
  - Extensions com **uBlock Origin** o **AdBlock Plus** poden reduir dràsticament els anuncis intrusius.
- **Fes servir el sentit comú**:
  - Si un lloc web et demana informació personal o financera sense motiu aparent, probablement no és de confiança.

3.2. Què fer si accedeixes accidentalment a un lloc web maliciós

Si entres per error en un lloc web sospitós, segueix aquests passos per minimitzar els riscos:

Generalitat de Catalunya · SEPE · emforsi · 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

- **No facis clic en res**:
  - No interactuïs amb finestres emergents, botons o missatges dins del lloc.
- **Tanca el navegador immediatament**:
  - Utilitza la combinació de tecles per tancar-lo ràpidament (per exemple, **Alt + F4** a Windows o **Cmd + Q** a macOS).
- **Escaneja el dispositiu**:
  - Passa un antivirus actualitzat per comprovar que no s'ha descarregat res sospitós.
- **Canvia les contrasenyes si cal**:
  - Si has introduït informació en el lloc sospitós, canvia immediatament les contrasenyes de tots els comptes afectats.

3.3. Consells per evitar descàrregues sospitoses

- **Baixa només d'orígens oficials**:
  - Descarrega programari, documents o fitxers únicament des de llocs web oficials o botigues d'aplicacions reconegudes (com Google Play o Apple App Store).
- **Evita formats de fitxers dubtosos**:
  - Desconfia de fitxers amb extensions inesperades com **.exe**, **.scr** o **.bat** si no estàs segur de la seva font.
- **Analitza fitxers abans d'obrir-los**:
  - Utilitza antivirus o serveis com **VirusTotal** per escanejar els fitxers abans de descarregar-los o executar-los.
- **Desconfia dels missatges urgents**:
  - Correus o finestres emergents que et pressionen per descarregar alguna cosa amb urgència sovint són una tàctica d'engany.

3.4. Eines útils per evitar llocs i descàrregues perilloses

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

- **Antivirus actualitzats**:
  - Programes com Norton, Kaspersky o Avast poden detectar i bloquejar llocs i fitxers maliciosos en temps real.
- **Extensions de seguretat per navegadors**:
  - Utilitza complements com **Malwarebytes Browser Guard** o **Web of Trust (WOT)** per rebre avisos en accedir a llocs sospitosos.
- **Navegadors amb filtres integrats**:
  - Navegadors com Google Chrome i Mozilla Firefox tenen filtres de seguretat que bloquegen llocs coneguts per ser maliciosos.

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

3.5. Beneficis d'evitar llocs i descàrregues sospitoses

- **Evites infeccions per malware**: Protegeixes els teus dispositius de programari maliciós que pot afectar la teva feina.
- **Redueixes el risc de robatori de dades**: Mantens segura la informació personal i professional.
- **Tranquil·litat durant la navegació**: Pots centrar-te en el teu negoci sense preocupar-te per amenaces digitals.

4. Extensions i Eines de Protecció per a Navegadors

Utilitzar extensions i eines de protecció és una manera efectiva d'enfortir la seguretat mentre navegues per Internet. Aquest apartat descriu les millors opcions disponibles per a petites empreses i autònoms, així com consells per configurar el navegador de manera segura.

4.1. Configuració del navegador per a una navegació més segura

Configurar correctament el navegador és una altra manera senzilla de protegir-te mentre navegues. Aquí tens alguns consells per fer-ho:

- **Actualitza el navegador regularment**:
  - Els navegadors com Google Chrome, Mozilla Firefox o Microsoft Edge reben actualitzacions constants amb millores de seguretat. Assegura't que tens activades les actualitzacions automàtiques.
- **Activa l'opció de navegació segura**:
  - **Google Chrome**: Activa "Navegació segura" a la configuració per rebre alertes de llocs web perillosos.
  - **Mozilla Firefox**: Activa "Protecció reforçada contra el rastreig" per bloquejar contingut sospitós.
- **Evita l'autocompletat de contrasenyes sensibles**:
  - Desactiva l'autocompletat de dades financeres o informació personal en llocs web.
- **Configura alertes de descàrregues perilloses**:
  - Assegura't que el navegador et notifiqui abans de descarregar fitxers sospitosos.

Generalitat de Catalunya
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

4.2. Altres eines per millorar la seguretat

A més de les extensions i configuracions del navegador, pots utilitzar eines complementàries per protegir-te:

- **Antivirus amb protecció per a navegadors**:
  - Programes com **Norton 360** o **McAfee Total Protection** inclouen complements per a navegadors que bloquegen amenaces en temps real.
- **VPN (Xarxa Privada Virtual)**:
  - Eines com **NordVPN**, **ExpressVPN** o **ProtonVPN** xifren la teva connexió i protegeixen la teva privacitat, especialment quan utilitzes xarxes públiques.
- **Programes antimalware**:
  - **Malwarebytes**:
    - Detecta i elimina programari maliciós que podria infectar el navegador.

4.3. Consells pràctics per a petites empreses i autònoms

- **Utilitza una combinació d'eines**:
  - Instal·la un bloquejador de publicitat, un gestor de contrasenyes i un antivirus per obtenir una protecció integral.
- **Forma't en l'ús de les eines**:
  - Dedica temps a conèixer les funcionalitats de les eines que utilitzes per aprofitar-ne tot el potencial.
- **Revisa periòdicament les extensions instal·lades**:
  - Elimina les que no utilitzis per evitar riscos innecessaris.

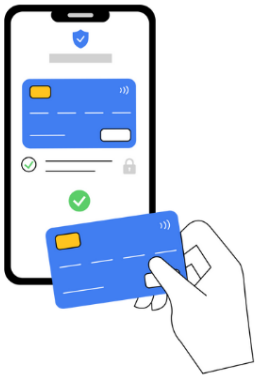
Beneficis d'utilitzar extensions i eines de protecció

- **Reducció de riscos**: Bloqueges llocs sospitosos abans d'interactuar amb ells.
- **Millora de l'eficiència**: Navegues més ràpid i sense distraccions gràcies als bloquejadors d'anuncis.
- **Tranquil·litat**: Saps que tens capes addicionals de protecció contra amenaces digitals.

Generalitat de Catalunya
SEPE
emfosl
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

5. Protecció de Dades durant Compres en Línia i Banca Digital



Les compres en línia i les operacions bancàries són activitats habituals per a petites empreses i autònoms. Tanmateix, també són punts vulnerables per a atacs com el phishing o el robatori de dades. Aquest apartat proporciona consells pràctics per garantir que aquestes transaccions siguin segures.

5.1. Com garantir transaccions segures

- **Assegura't que el lloc web és de confiança**:
  - Verifica que l'adreça del lloc comenci amb **https://** i que hi hagi un candau a la barra d'adreces.
  - Si tens dubtes sobre la reputació del lloc, consulta'l a eines com **Google Transparency Report** o **Web of Trust (WOT)**.
- **Fes servir mètodes de pagament segurs**:
  - Utilitza targetes de crèdit o sistemes com **PayPal**, que ofereixen proteccions addicionals en cas de frau.
  - Evita transferències directes a comptes bancaris desconeguts.
- **Activa l'autenticació de dos factors (2FA)**:
  - Per a portals bancaris o de compres importants, configura l'autenticació multifactor per afegir una capa extra de seguretat.
- **Compra des de dispositius segurs**:
  - Evita fer compres des de dispositius públics o compartits, com ordinadors d'espais de coworking o cibercafès.

5.2. Protecció contra el phishing en portals bancaris i botigues en línia

- **Reconèixer correus electrònics fraudulents**:
  - Els correus de phishing solen tenir errors gramaticals, adreces d'enviament sospitoses o demanar acció immediata ("verifica el teu compte ara").
  - No facis clic en enllaços de correus electrònics que semblin sospitosos. Accedeix directament al portal digitant l'adreça manualment.
- **Verifica l'adreça del lloc web**:
  - Assegura't que l'URL del portal bancari o de la botiga és correcte. Els atacs de **typosquatting** (petits canvis en l'URL, com "paypa1.com") són comuns.
- **Desconfia de les ofertes exagerades**:

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosl · 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

    - Les botigues en línia falses solen oferir preus molt baixos per atraure clients. Si una oferta sembla massa bona per ser veritat, probablement ho és.
- **Utilitza navegadors amb protecció contra phishing**:
    - Navegadors com Google Chrome i Firefox tenen filtres que bloquegen llocs coneguts per ser fraudulents.

5.3. Bones pràctiques per gestionar dades en línia

- **No emmagatzemis informació financera en portals desconeguts**:
    - Si no és estrictament necessari, evita guardar dades de targetes de crèdit en llocs web.
- **Activa notificacions de transaccions**:
    - Configura alertes al teu banc o al sistema de pagament per rebre notificacions de totes les operacions realitzades.
- **Fes còpies de seguretat de les factures i registres**:
    - Guarda còpies digitals de les teves transaccions en un emmagatzematge segur per tenir proves en cas de discrepàncies.

5.4. Consells pràctics per petites empreses i autònoms

- **Centralitza les operacions en portals de confiança**:
    - Utilitza botigues en línia reconegudes per comprar subministraments i serveis.
- **Estableix límits a les targetes de crèdit**:
    - Si pots, configura límits de despesa per evitar càrrecs fraudulents alts.
- **Forma l'equip sobre compres segures**:
    - Si tens treballadors que gestionen compres, assegura't que coneguin aquestes bones pràctiques.

Beneficis de protegir les teves dades durant transaccions

- **Evites fraus i càrrecs no autoritzats**: Mantens el control sobre els diners i la informació financera.
- **Garanteixes la continuïtat del negoci**: Protegeixes dades essencials per operar amb normalitat.
- **Confiança i professionalitat**: Les transaccions segures reforcen la imatge del teu negoci davant clients i proveïdors.

Generalitat de Catalunya
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL SEPE
emforsl
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

6. Navegació en Xarxes Públiques o Desconegudes

Les xarxes públiques, com les d'aeroports, cafeteries o hotels, són convenients però comporten riscos importants. Navegar sense protecció en aquestes xarxes pot exposar-te a atacs que comprometen les teves dades i el teu dispositiu.

6.1. Riscos de connectar-se a xarxes Wi-Fi públiques

- **Intercepció de dades**:
  - Els atacants poden utilitzar eines per capturar la informació que envies i reps, incloent-hi contrasenyes, dades bancàries i correus electrònics.
- **Punts d'accés falsos**:
  - Els atacants poden crear xarxes Wi-Fi amb noms semblants als legítims per enganyar-te (per exemple, "CafeteriaGratis" en lloc de "CafeteriaOficial").
- **Atacs mitjançant programari maliciós**:
  - Les xarxes públiques poden permetre la distribució de malware als dispositius connectats.

6.2. Com utilitzar una VPN per protegir la connexió

Una VPN (Xarxa Privada Virtual) és una eina que xifra la connexió entre el teu dispositiu i Internet, fent-la inaccessible per a tercers.

- **Avantatges de la VPN**:
  - Xifra totes les dades que envies i reps, protegint-les d'intercepcions.
  - Oculta la teva adreça IP, millorant la privacitat.
  - Permet accedir de manera segura a xarxes corporatives o serveis restringits geogràficament.
- **Eines recomanades**:
  - **NordVPN**, **ExpressVPN**, **ProtonVPN** (per a una protecció robusta i fàcil d'utilitzar).
  - Algunes VPN gratuïtes són útils per ús ocasional, però assegura't que siguin de confiança.

Generalitat de Catalunya
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

6.3. Consells pràctics per utilitzar xarxes públiques amb seguretat

- **No realitzis transaccions sensibles**:
  - Evita accedir a bancs en línia, portals de compres o dades sensibles mentre estiguis connectat a una xarxa pública.
- **Desactiva la connexió automàtica a xarxes**:
  - Configura el teu dispositiu perquè només es connecti manualment a xarxes de confiança.
- **Utilitza el teu pla de dades mòbil**:
  - Si pots, utilitza el teu hotspot personal en lloc de xarxes Wi-Fi públiques.
- **Tanca les sessions després d'usar-les**:
  - Desconnecta't de serveis com correu electrònic o portals de treball després d'utilitzar-los.

Beneficis de protegir la teva connexió en xarxes públiques

- **Reducció del risc d'intercepció**: Les dades no poden ser capturades fàcilment.
- **Privacitat millorada**: Protegeixes la teva identitat i activitat en línia.
- **Continuïtat segura del negoci**: Pots treballar en moviment sense preocupar-te per vulnerabilitats.

7. Mesures Preventives per una Navegació Segura

A més de les eines i pràctiques específiques descrites anteriorment, adoptar mesures preventives generals millora la seguretat durant la navegació.

7.1. Actualitzacions del navegador i sistemes operatius

- **Mantenir el navegador actualitzat**:
  - Els navegadors actualitzen regularment els seus sistemes per tancar vulnerabilitats de seguretat.
  - Configura actualitzacions automàtiques per evitar riscos.
- **Actualitza les extensions i plugins**:
  - Extensions obsoletes poden ser punts febles que els atacants poden explotar.
- **Revisa el sistema operatiu**:
  - Mantenir Windows, macOS, Android o iOS actualitzats és clau per protegir els dispositius.

7.2. Educació per reconèixer i evitar amenaces en línia

- **Forma't sobre ciberseguretat**:

Generalitat de Catalunya · 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

    - Participa en formacions bàsiques o tallers en línia per aprendre a identificar riscos i reaccionar-hi.
- **Comparteix bones pràctiques amb el teu equip**:
    - Assegura't que tothom que treballa al teu negoci entén la importància de la navegació segura.
- **Desenvolupa habilitats pràctiques**:
    - Aprèn a reconèixer enllaços sospitosos, llocs fraudulents i missatges de phishing.

7.3. Consells generals per prevenir riscos

- **Utilitza contrasenyes úniques i robustes**:
    - Evita reutilitzar contrasenyes entre llocs. Un gestor de contrasenyes com **Bitwarden** pot ajudar.
- **Evita compartir informació sensible**:
    - No introdueixis dades personals o financeres en llocs que no siguin absolutament de confiança.
- **Realitza còpies de seguretat regularment**:
    - Si alguna cosa va malament, una còpia recent de les dades et permetrà recuperar la informació ràpidament.

Beneficis d'unes bones mesures preventives

- **Reducció de riscos**: Prevenir incidents és sempre més fàcil que corregir-ne els efectes.
- **Protecció integral**: Les mesures preventives cobreixen múltiples fronts de seguretat.
- **Tranquil·litat**: Pots navegar amb confiança sabent que estàs protegit.

8. Preguntes d'autoavaluació

Aquest apartat t'ajuda a **comprovar si estàs aplicant correctament les mesures de navegació segura** descrites a la guia. Amb una llista de verificació i recomanacions personalitzades, podràs identificar àrees per millorar i reforçar la teva seguretat en línia.

8.1. 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.

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

Identificació de llocs web segurs

1. Sempre comprovo que els llocs web tinguin HTTPS i un certificat vàlid abans d'introduir dades?
2. Reconec els senyals d'un lloc web sospitós (adreces estranyes, contingut de baixa qualitat, etc.)?

Evitar llocs maliciosos i descàrregues sospitoses

3. Evito fer clic en enllaços de correus electrònics o missatges sospitosos?
4. Només descarrego fitxers des de fonts oficials o de confiança?
5. Utilitzo eines com bloquejadors d'anuncis i antivirus per protegir la meva navegació?

Extensions i configuració de navegadors

6. Tinc instal·lades extensions recomanades per millorar la seguretat (bloquejadors de publicitat, gestors de contrasenyes)?
7. El meu navegador està configurat per bloquejar llocs i descàrregues sospitoses?
8. Actualitzo el navegador i les extensions periòdicament?

Compres en línia i banca digital

9. Només realitzo compres i operacions bancàries en llocs web verificats i de confiança?
10. Utilitzo sistemes de pagament segurs i autenticació multifactor quan és possible?

Ús de xarxes públiques o desconegudes

11. Sempre utilitzo una VPN quan em connecto a xarxes Wi-Fi públiques?
12. Desactivo la connexió automàtica a xarxes no segures?

Mesures preventives generals

13. He rebut formació bàsica en ciberseguretat o he educat el meu equip?
14. Tinc hàbits de navegació segurs (evitant compartir informació sensible en llocs no verificats)?

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

8.2. Escala d'autoavaluació

0-5 respostes afirmatives: Nivell de risc alt

- T'estàs exposant a greus riscos durant la navegació, que podrien comprometre les teves dades i el teu negoci.
- Recomanació: Comença aplicant mesures bàsiques, com reconèixer llocs segurs i utilitzar una VPN en xarxes públiques.

6-10 respostes afirmatives: Nivell de risc moderat

- Tens algunes mesures de seguretat aplicades, però encara hi ha punts vulnerables.
- Recomanació: Dona prioritat a configurar el navegador i utilitzar extensions i eines que reforcin la teva protecció.

11-13 Respostes afirmatives: Nivell de risc baix

- Tens un bon nivell de seguretat, però encara pots millorar en alguns detalls.
- Recomanació: Mantingues les bones pràctiques i revisa regularment la teva configuració per garantir-ne l'eficàcia.

14 Respostes afirmatives: Excel·lent

- Felicitats! Estàs navegant de manera segura i protegint el teu negoci de manera eficient.
- Recomanació: Continua formant-te i actualitzant les teves eines per mantenir aquest nivell de protecció.

8.3. Recursos addicionals

Per millorar en les àrees on has detectat mancances, pots consultar recursos addicionals com:

- **Guies en línia sobre navegació segura**: Google, Mozilla i altres navegadors tenen recursos gratuïts per millorar la seguretat.
- **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.

Generalitat de Catalunya
SEPE
emfosl
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