

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

DECÀLEG DE CIBERSEGURETAT

Agost 2025
Document d'ús públic

- 1 DECÀLEG DE CIBERSEGURETAT PER A TOTES LES ORGANITZACIONS**
.....
- 2 RECOMANACIONS PER IMPLEMENTAR LA CIBERSEGURETAT**
.....
- 3 DECÀLEG DE CIBERSEGURETAT: 10 PASSOS**
.....
- 4 CONCLUSIONS**
.....



1 ■ DECÀLEG DE CIBERSEGURETAT PER A TOTES LES ORGANITZACIONS

Decàleg de ciberseguretat: millora el nivell de ciberseguretat de la teva organització

Què és la ciberseguretat?

La **ciberseguretat** és un element essencial per a qualsevol organització en l'era digital en què vivim. **Protegir els actius d'informació, garantir la continuïtat del negoci i mantenir la confiança dels nostres clients, socis, col·laboradors i/o proveïdors** són objectius clau en totes les organitzacions.



Contingut d'aquest decàleg

- ✓ Aquest decàleg conté **DEU PASSOS** imprescindibles per incrementar el nivell de ciberseguretat de la teva organització i que esdevingui un negoci competitiu i fiable.
- ✓ També inclou diverses **RECOMANACIONS EN MATÈRIA DE CIBERSEGURETAT**, que es poden implementar i tenir en compte en totes les organitzacions.

Decàleg de ciberseguretat per a totes les organitzacions

1. Anàlisi de riscos

Identifica els processos crítics, els actius essencials, els empleats clau i les possibles amenaces que puguin afectar l'empresa. Aquest diagnòstic és la base per dissenyar un pla de seguretat personalitzat.

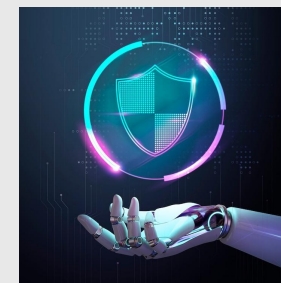


2. Pla director de seguretat

Defineix un pla estratègic que estableixi objectius i mesures concretes per protegir l'empresa. Cal revisar aquest pla periòdicament per adaptar-lo a les noves amenaces.

3. Control d'accés a la informació

Implementa polítiques que regulin qui pot accedir a la informació i a quines dades i recursos, mitjançant una autenticació robusta i una gestió adequada de permisos, per minimitzar riscos interns i externs.



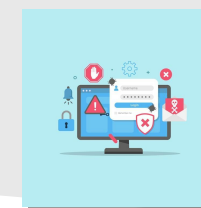
4. Còpies de seguretat

Fes còpies de seguretat de la informació crítica regularment i de manera segura, per tal que es puguin restaurar les dades en cas de pèrdua o després de patir un atac, la qual cosa garanteix la continuïtat del negoci.



5. Eines de protecció contra programari maliciós

Utilitza solucions actualitzades contra virus, programari de segrest i altres tipus de programes maliciosos per protegir els sistemes de l'empresa.



Decàleg de ciberseguretat per a totes les organitzacions

6. Actualitzacions periòdiques dels sistemes

Tingues tots els **sistemes**, les **aplicacions** i els **gestors de contingut actualitzats** per corregir vulnerabilitats i millorar la seguretat.



7. Seguretat de la xarxa

Protegeix les xarxes internes i externes **mitjançant tallafocs, segmentació i polítiques d'ús segur**, incloent-hi la gestió de connexions sense fils i d'accés remot.

8. Gestió segura de dispositius i suports

Controla l'ús, l'emmagatzematge i l'eliminació segura de dispositius físics i digitals per **evitar fuites o pèrdues d'informació**.



9. Registre i auditoria d'activitat

Implementa sistemes que registrin accessos i accions en els sistemes per **detectar incidents de seguretat i respondre-hi**.

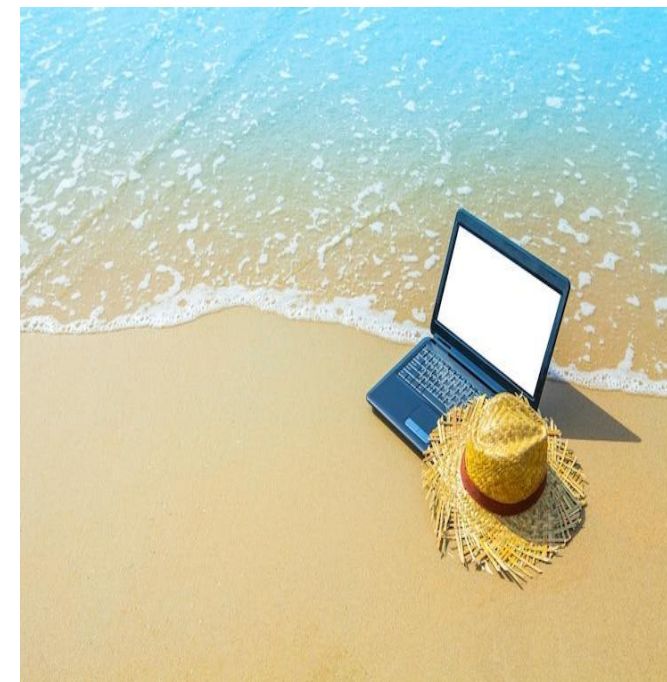
10. Pla de continuïtat del negoci

Prepara procediments per mantenir o recuperar les operacions davant d'incidents greus, per tal de **minimitzar l'impacte econòmic i reputacional**.

2. RECOMANACIONS PER IMPLEMENTAR LA CIBERSEGURETAT

Recomanacions per implementar la ciberseguretat a les organitzacions

- 1.** Fes arribar les **POLÍTIQUES DE SEGURETAT** a tot el personal de l'organització, i assegura't que les conegui i les compleixi.
- 2.** Signa **ACORDS DE CONFIDENCIALITAT** amb treballadors i col·laboradors de l'organització, amb l'objectiu de protegir la informació sensible i crítica i també la documentació confidencial.
- 3.** Fes **FORMACIÓ I CONSCIENCIACIÓ** de manera habitual entre els treballadors de la teva organització, i duu a terme les **ACTUALITZACIONS PERIÒDIQUES** que siguin necessàries i oportunes per evitar possibles riscos i vulnerabilitats.
- 4.** Estableix un protocol clar per **GESTIONAR INCIDENTS DE SEGURETAT** i **RESPONDRE** de manera ràpida en cas de possibles ciberatacs.



3. ■ DECÀLEG DE CIBERSEGURETAT: 10 PASSOS

Decàleg de ciberseguretat: 10 passos

1. Anàlisi de riscos

- ✓ Avalua els riscos i les vulnerabilitats actuals.
- ✓ Estableix objectius clars de ciberseguretat segons les necessitats de l'organització.

2. Pla director de ciberseguretat

- ✓ Defineix regles d'ús de sistemes, dispositius i dades.
- ✓ Assegura't del compliment legal i ètic en el tractament de la informació.

3. Control d'accés a la informació

- ✓ Limita l'accés a la informació només a aquelles persones que el necessitin.
- ✓ Implementa sistemes d'autenticació robustos i polítiques de contrasenyes segures.



Decàleg de ciberseguretat: 10 passos

4. Còpies de seguretat

- ✓ Fes **còpies de seguretat** de la informació crítica periòdicament.
- ✓ Verifica que es poden restaurar les dades i fer còpies de seguretat.



5. Eines de protecció contra programari maliciós

- ✓ Instal·la i actualitza solucions de protecció en tots els dispositius de l'organització.
- ✓ Fes anàlisis de manera freqüent per detectar amenaces.

6. Actualitzacions periòdiques dels sistemes, aplicacions, etc.

- ✓ Aplica pedaços i actualitzacions de seguretat de manera regular.



Decàleg de ciberseguretat: 10 passos

7. Seguretat de la xarxa

- ✓ Protegeix la xarxa interna amb tallafocs i segmentació.
- ✓ Usa connexions segures (VPN, xifratge) per a l'accés remot a la xarxa i la transmissió d'informació delicada.

8. Gestió segura de dispositius i suports

- ✓ Controla l'ús d'USB, discos durs i altres dispositius extraïbles.
- ✓ Aplica polítiques d'esborrament segur i destrucció d'informació quan calgui.

9. Registre i auditoria d'activitat

- ✓ Implementa sistemes de registre d'accessos i activitats rellevants.

10. Pla de continuïtat del negoci

- ✓ Defineix procediments per actuar davant d'esdeveniments disruptius que puguin afectar la continuïtat del negoci.



4. CONCLUSIONS



Conclusions

- ✓ El **decàleg de ciberseguretat** estableix els passos clau per enfortir la seguretat de la informació a les organitzacions.
- ✓ La **gestió d'accessos i l'autenticació robusta** és fonamental per prevenir intrusions.
- ✓ Les **còpies de seguretat i les actualitzacions periòdiques** garanteixen la continuïtat del negoci.
- ✓ La **formació i la conscienciació** dels empleats i col·laboradors són clau per reduir possibles riscos humans.
- ✓ Un **pla de continuïtat del negoci** i les **auditories constants** ens permeten respondre de manera eficaç en cas de possibles incidents de seguretat.

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.