# Pla de Seguretat de l'Entitat (PSE)

## Guia de bones pràctiques


**(DOCUMENT SUBJECTE A MODIFICACIONS)**

**Abril 2023**

Fitxa del document

| **Títol** | Pla de Seguretat de l'Entitat (PSE) |
|---|---|

| Versió | Redactat/Revisat per | Aprovat per | Data aprovació | Data publicació |
|---|---|---|---|---|
| | | | | |
| 1.0 | ANC-AD | ANC-AD | 26/4/23 | 27/4/23 |

| Registre de canvis | | | |
|---|---|---|---|
| Versió | Pàgines | Data de modificació | Motiu del canvi |
| | | | |
| | | | |
| | | | |

| **Propietari del document**: ANC-AD |
|---|

# PRÒLEG

L'ús massiu de les tecnologies de la informació i les telecomunicacions (TIC), en tots els àmbits de la societat, ha creat un nou espai, el ciberespai, on es produiran conflictes i agressions, i on hi ha ciberamenaces que atemptaran contra la seguretat nacional, l'estat de dret, la prosperitat econòmica, l'estat de benestar i el normal funcionament de la societat i de les administracions públiques.

La Llei 22/2022, de 9 de juny, , encomana a l´Agència Nacional de Ciberseguretat d´Andorra (ANC-AD) l'exercici de les funcions relatives a la seguretat de les tecnologies de la informació, i de protecció de les xarxes d´ informació alhora que confereix Secretari d'Estat de Transició Digital i Projectes Estratègics la responsabilitat de dirigir l´ANC-AD.

El Decret 417/2022, de 19 d´octubre, pel qual es regula l'Esquema Nacional de Seguretat d´Andorra en l'àmbit de les entitats que presten serveis "importants" (ENS-AD, en endavant), al qual es refereix l'article 4-2-a de la Llei 22/2022, de 9 de juny , estableix la política de seguretat en la utilització de mitjans electrònics que permeti una protecció adequada de la informació.

En definitiva, la sèrie de documents ENS-STIC s'elaboren (adaptats del CCN-CERT) per donar compliment a les comeses de l´Agència Nacional de Ciberseguretat d´Andorra i al reflectit en l' Esquema Nacional de Seguretat d´Andorra, conscients de la importància que té l' establiment d' un marc de referència en aquesta matèria que serveixi de suport perquè el personal de les entitats afectades, i en ocasions, ingrata tasca de proporcionar seguretat als sistemes de les TIC sota la seva responsabilitat.

César Marquina Pérez de la Cruz
Ministre de Finances i portaveu del Govern

# ÍNDEX

# 1. INTRODUCCIÓ

## 1.1. MARC DE REFERÈNCIA

1. Segons l'establert a la Llei 22/2022, de 9 de juny, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques, l'operador designat com a crític, ja sigui aquest pertanyent al sector públic o al privat, s'integrarà com a agent del sistema de protecció d'infraestructures crítiques, havent de complir amb una sèrie de responsabilitats recollides en l'article 12.
2. Actualment, la seguretat, entesa en el sentit més ampli, s'ha convertit en una part crítica per a la immensa majoria de les entitats pel que han d'estar preparades per gestionar-la correctament i afrontar amb el mínim impacte possible les incidències que es vagin produint.

## 1.2. OBJECTE D'AQUEST DOCUMENT

3. Aquest document té per objecte el disseny d'un Pla de Seguretat de l'Entitat (d'ara endavant, PSE) que permeti controlar i minimitzar els nivells de risc associats a les instal·lacions, serveis i sistemes d'informació de l'entitat d'acord amb la criticitat dels seus processos de negoci.
4. El pla servirà de referència per assolir i mantenir, mitjançant la implantació dels projectes i accions definits en aquest, el nivell de seguretat objectiu de l'entitat al curt, mitjà i llarg termini.

# 2. ANÀLISI DE L'ENTORN

5. L'anàlisi de l'entorn és una tasca important en la gestió de la seguretat, ja que permet identificar possibles amenaces i vulnerabilitats en l'entorn extern de l'entitat. Això inclou l'avaluació de riscos externs, com les amenaces econòmiques i socials, així com la identificació de possibles amenaces cibernètiques provinents de hackers, grups de delictes informàtics i ciberterrorismes.

    - ✓ Elaborar una anàlisi periòdica de l'entorn per identificar possibles amenaces i vulnerabilitats externes.
    - ✓ Avaluar els riscos i establir mesures de seguretat adequades per prevenir o mitigar els riscos externs.
    - ✓ Establir un pla de comunicació i col·laboració amb els *stakeholders* rellevants, incloent-hi les autoritats locals i altres actors del sector, per millorar la seguretat de l'entorn empresarial.
    - ✓ Mantenir-se actualitzat sobre les últimes tendències i desenvolupaments en l'entorn de seguretat per garantir la protecció de l'entitat contra noves amenaces.

## 3. IDENTIFICACIÓ I ANÀLISI DE RISCOS

6. La identificació i anàlisi de riscos és el primer pas per a la implementació d'una estratègia de seguretat efectiva. Aquest procés consisteix a identificar les amenaces potencials i avaluar la seva probabilitat i impacte, per determinar les mesures de seguretat necessàries per mitigar-los.

   - ✓ Elaborar una anàlisi exhaustiva dels actius i sistemes crítics de l'entitat, identificant els possibles riscos i amenaces als quals estan exposats, incloent-hi riscos interns i externs.
   - ✓ Avaluar la probabilitat i l'impacte de cada risc identificat, així com la vulnerabilitat actual dels sistemes i actius enfront d'ells.
   - ✓ Prioritzar els riscos segons el seu impacte i probabilitat, i definir estratègies de mitigació específiques per a cada un d'ells.
   - ✓ Establir un pla de seguiment i avaluació continus per assegurar que els riscos estiguin controlats i mitigats de manera efectiva.

## 4. POLÍTICA DE SEGURETAT

7. La política de seguretat és un conjunt de normes i directrius que estableixen com es deuen protegir els actius i la informació de l'entitat. Aquestes polítiques han de ser clares, coherents i aplicades de manera uniforme en tota l'entitat.

   - ✓ Definir una política clara i concisa de seguretat de la informació que estableixi els objectius, principis i mesures necessàries per garantir la protecció dels actius crítics de l'entitat.
   - ✓ Establir mesures de control i seguretat per garantir la confidencialitat, integritat i disponibilitat de la informació, així com el compliment de les regulacions i normatives aplicables.
   - ✓ Definir un pla de contingència i recuperació davant desastres que garanteixi la continuïtat de les operacions crítiques en cas d'una interrupció o incident de seguretat.

## 5. ESTRUCTURA ORGANITZATIVA

8. L'estructura organitzativa és clau per a la implementació efectiva d'una estratègia de seguretat. L'entitat ha de tenir un equip dedicat a la seguretat de la informació, liderat per un responsable de seguretat de la informació (CISO), i els membres de l'equip han de tenir rols i responsabilitats clarament definits.

   - ✓ Crear un equip dedicat i capacitats en ciberseguretat, amb rols i responsabilitats clarament definits per a cada membre.
   - ✓ Establir un comitè de seguretat que supervisi i controli la implementació i el compliment de les polítiques i procediments de seguretat.
   - ✓ Establir un protocol de comunicació i resposta davant incidents de seguretat, que permeti una ràpida identificació, resposta i recuperació davant possibles amenaces.

## 6. GESTIÓ D'ACCESSOS

9. La gestió d'accés es refereix a la implementació de mesures de seguretat per controlar l'accés als actius i la informació de l'entitat. Això inclou l'autenticació d'usuaris, l'assignació de permisos i la gestió de contrasenyes.

    - ✓ Establir mesures d'autenticació i autorització per limitar l'accés a la informació i sistemes crítics de l'entitat, segons la necessitat i perfil de cada usuari.
    - ✓ Establir controls d'accés físics i lògics per restringir l'accés no autoritzat als actius i sistemes crítics.
    - ✓ Definir un pla de gestió de contrasenyes per garantir la seva seguretat i evitar el seu ús inapropiat o filtració.

## 7. PROTECCIÓ DE LA XARXA

10. La protecció de la xarxa és essencial per garantir la seguretat de la informació. Això inclou la implementació de mesures de seguretat en la infraestructura de xarxa, com ara tallafocs, detecció d'intrusions i filtratge de contingut.

    - ✓ Establir mesures de seguretat a la xarxa, com ara tallafocs, detecció d'intrusos, prevenció d'atacs de denegació de servei (DDoS), entre d'altres, per protegir els sistemes i les dades crítiques de l'entitat.
    - ✓ Implementar solucions de xifrat i autenticació de la xarxa, per garantir la confidencialitat i integritat de la informació transmesa a través d'ella.
    - ✓ Definir un pla de monitoratge continua de la xarxa per detectar possibles amenaces o atacs, i establir mesures de resposta i recuperació davant d'ells.

## 8. PROTECCIÓ DELS DISPOSITIUS

11. La protecció dels dispositius és fonamental per protegir la informació de l'entitat. Això inclou la implementació de mesures de seguretat en els dispositius, com ara antivirus, antimalware i actualitzacions regulars, per garantir la seva protecció davant possibles amenaces. També s'ha d'establir un pla de gestió de pegats per mantenir els dispositius actualitzats i protegits.

    - ✓ Establir mesures de seguretat en els dispositius, com ara antivirus, antimalware, actualitzacions regulars, entre altres, per garantir la seva protecció davant possibles amenaces.
    - ✓ Definir un pla de gestió de pegats i actualitzacions de programari, que estableixi la periodicitat i el procés per dur a terme aquestes tasques.
    - ✓ En el cas de dispositius mòbils, implementar mesures com ara el xifrat de dades, l'autenticació d'usuari i la configuració de polítiques de seguretat per a l'ús de dispositius personals a l'empresa.

## 9. MONITORATGE DE LA XARXA I DETECCIÓ D'AMENACES

12. Disposar d'eines de monitoratge de la xarxa i detecció d'amenaces que permetin identificar i respondre ràpidament als incidents de seguretat. Això inclou la implementació de sistemes de detecció d'intrusions, anàlisi de registres d'activitat i alertes de seguretat en temps real. A més, és necessari disposar d'un equip de resposta a incidents (intern o extern) i un pla d'acció en cas que es produeixi un atac o una violació de la seguretat.

    - ✓ Establir un sistema de monitoratge constant dels sistemes i xarxes de l'entitat.
    - ✓ Configurar alertes per notificar en temps real qualsevol incident o activitat sospitosa.
    - ✓ Implementar un sistema de registre i gestió d'incidents per documentar i analitzar les causes d'aquests.
    - ✓ Definir un procés de resposta a incidents per actuar de manera ràpida i efectiva davant qualsevol problema de seguretat.

## 10. CONTINUÏTAT DEL NEGOCI

13. La continuïtat del negoci és un aspecte clau en la gestió de la seguretat. És important comptar amb plans i procediments per garantir que l'entitat pugui seguir operant en cas d'un desastre natural, una fallada tècnica o un atac de seguretat. Això inclou la realització de proves periòdiques de recuperació davant desastres, la implementació de plans de contingència i la identificació dels recursos necessaris per garantir la continuïtat del negoci en cas d'una interrupció.

    - ✓ Identificar els processos i sistemes crítics per al negoci i establir plans de contingència per a la seva recuperació en cas d'interrupcions.
    - ✓ Realitzar proves periòdiques dels plans de contingència per garantir-ne l'efectivitat.
    - ✓ Definir un equip de resposta a desastres per actuar ràpidament davant situacions crítiques.
    - ✓ Establir un pla de comunicació per mantenir informats els empleats, clients i proveïdors sobre la situació i les mesures adoptades.

## 11. AVALUACIÓ I MILLORA CONTÍNUA

14. L'avaluació i millora contínua de la seguretat és fonamental per garantir que el pla de seguretat sigui efectiu. És important dur a terme auditories i revisions periòdiques del pla de seguretat per identificar possibles debilitats o àrees de millora. Això inclou l'avaluació de l'eficàcia de les mesures de seguretat implementades, la revisió de les polítiques i procediments de seguretat i la identificació de noves amenaces o vulnerabilitats que puguin sorgir.

    - ✓ Realitzar auditories regulars per avaluar el compliment de les polítiques i procediments de seguretat.
    - ✓ Analitzar els resultats de les auditories i establir plans d'acció per corregir qualsevol problema detectat.
    - ✓ Realitzar avaluacions de riscos periòdiques per identificar noves amenaces i establir mesures de protecció adequades.
    - ✓ Establir un sistema de retroalimentació per recopilar comentaris i suggeriments dels empleats i usuaris i millorar contínuament el PSE.

## 12. CONSCIENCIACIÓ I FORMACIÓ

15. Els empleats són una part fonamental de la seguretat de l'entitat. És important conscienciar i capacitar els empleats sobre les millors pràctiques de seguretat, així com sobre les amenaces i riscos potencials. Això inclou la implementació de programes de formació i conscienciació en seguretat, la realització de proves de phishing i la promoció d'una cultura de seguretat en tota l'entitat.

    - ✓ Establir un programa de formació en seguretat de la informació per a tots els empleats, incloent-hi sessions de conscienciació i entrenament sobre millors pràctiques de seguretat.
    - ✓ Realitzar proves periòdiques de phishing per avaluar la capacitat dels empleats per detectar i informar intents de frau.
    - ✓ Definir polítiques clares de seguretat de la informació i assegurar-se que siguin enteses i seguides per tots els membres de l'entitat.
    - ✓ Establir un sistema de recompenses i reconeixements per fomentar una cultura de seguretat en l'entitat.

## 13. COMPLIMENT NORMATIU LQPD

16. La Llei Qualificada de Protecció de Dades Personals (LQPD) és la normativa que regula el tractament de dades personals a Andorra. En el context de la ciberseguretat, és important complir amb la LQPD per garantir la protecció de les dades personals dels ciutadans i minimitzar els riscos de ciberatacs.

17. El compliment de la LQPD en ciberseguretat implica implementar mesures tècniques i organitzatives per garantir la confidencialitat, integritat i disponibilitat de les dades personals, i establir procediments per notificar les violacions de seguretat a l'autoritat de protecció de dades.

18. Per complir amb la LQPD en ciberseguretat a Andorra, es poden seguir les següents mesures:

    - ✓ Identificar i classificar les dades personals: És crucial realitzar una auditoria de les dades personals que es manegen en l'entitat i classificar-les segons el seu nivell de sensibilitat.
    - ✓ Implementar mesures tècniques i organitzatives: En funció de la classificació anterior, cal implementar mesures tècniques i organitzatives adequades per garantir la confidencialitat, integritat i disponibilitat de les dades personals. Això pot incloure la implementació de sistemes de xifrat, controls d'accés, còpies de seguretat, polítiques de seguretat, entre altres.
    - ✓ Establir procediments per notificar violacions de seguretat: En cas que es produeixi una violació de seguretat, és important comptar amb procediments clars per notificar a l'autoritat de protecció de dades i als titulars de les dades personals afectats.
    - ✓ Designar un responsable de protecció de dades: Segons la LQPD, és obligatori designar un responsable de protecció de dades a les entitats. Aquest responsable ha de ser una persona encarregada de vetllar pel compliment de la normativa en matèria de protecció de dades personals i actuar com a punt de contacte amb l'autoritat de protecció de dades.

## 14. LLISTA DE VERIFICACIÓ

19. A continuació, es facilita una llista de verificació per garantir que es compleixin els requisits necessaris i es minimitzin els riscos.

| Preguntes de verificació | Si | No |
|---|---|---|
| **Anàlisi de l'entorn** | | |
| S'avalua periòdica de l'entorn extern per identificar possibles amenaces i vulnerabilitats? | | |
| S'han avaluat els riscos externs, incloent-hi les amenaces econòmiques i socials, així com les possibles amenaces cibernètiques? | | |
| S'han establert mesures de seguretat adequades per prevenir o mitigar els riscos externs identificats? | | |
| S'ha establert un pla de comunicació i col·laboració amb els *stakeholders* rellevants, incloent-hi les autoritats locals i altres actors del sector, per millorar la seguretat en l'entorn empresarial? | | |
| Es manté actualitzat el coneixement sobre les últimes tendències i desenvolupaments en l'entorn de seguretat per garantir la protecció de l'entitat contra noves amenaces? | | |
| **Identificació i anàlisi de riscos** | | |
| S'ha elaborat una anàlisi exhaustiva dels actius i sistemes crítics de l'entitat, identificant els possibles riscos i amenaces als quals estan exposats, incloent-hi riscos interns i externs? | | |
| S'ha avaluat la probabilitat i l'impacte de cada risc identificat, així com la vulnerabilitat actual dels sistemes i actius davant ells? | | |
| S'han prioritzat els riscos segons el seu impacte i probabilitat, i s'han definit estratègies de mitigació específiques per a cada un d'ells? | | |
| S'ha establert un pla de seguiment i avaluació contínua per assegurar que els riscos estiguin controlats i mitigats de manera efectiva? | | |
| **Política de seguretat** | | |
| S'ha definit una política clara i concisa de seguretat de la informació que estableixi els objectius, principis i mesures necessàries per garantir la protecció dels actius crítics de l'entitat? | | |
| S'han establert mesures de control i seguretat per garantir la confidencialitat, integritat i disponibilitat de la informació, així com el compliment de les regulacions i normatives aplicables? | | |

| | | |
|---|---|---|
| **S'ha definit un pla de contingència i recuperació davant desastres que garanteixi la continuïtat de les operacions crítiques en cas d'una interrupció o incident de seguretat?** | | |
| **La política de seguretat s'aplica de manera uniforme en tota l'entitat i s'actualitza regularment per adaptar-se als canvis en l'entorn de seguretat?** | | |
| **Es realitzen auditories regulars per assegurar el compliment de la política de seguretat i es prenen mesures correctives quan sigui necessari?** | | |
| **Estructura organitzativa** | | |
| **S'ha creat un equip dedicat a la seguretat de la informació?** | | |
| **L'equip està liderat per un responsable de seguretat de la informació (CISO)?** | | |
| **Cada membre de l'equip té rols i responsabilitats clarament definits?** | | |
| **S'ha establert un comitè de seguretat per supervisar la implementació i compliment de les polítiques i procediments de seguretat?** | | |
| **S'ha establert un protocol de comunicació i resposta davant incidents de seguretat que permeti una ràpida identificació, resposta i recuperació davant possibles amenaces?** | | |
| **Gestió d'accessos** | | |
| **S'han establert mesures d'autenticació i autorització per limitar l'accés a la informació i sistemes crítics de l'entitat, segons la necessitat i perfil de cada usuari?** | | |
| **S'han establert controls d'accés físics i lògics per restringir l'accés no autoritzat als actius i sistemes crítics?** | | |
| **S'ha definit un pla de gestió de contrasenyes per garantir-ne la seguretat i evitar-ne l'ús inapropiat o filtració?** | | |
| **Protecció de la xarxa** | | |
| **S'han establert mesures de seguretat a la xarxa, com a tallafocs, detecció d'intrusos, prevenció d'atacs de denegació de servei (DDoS), entre altres, per protegir els sistemes i les dades crítiques de l'entitat?** | | |
| **S'han implementat solucions de xifrat i autenticació de la xarxa per garantir la confidencialitat i integritat de la informació transmesa a través d'ella?** | | |
| **S'ha definit un pla de monitoratge contínua de la xarxa per detectar possibles amenaces o atacs i s'han establert mesures de resposta i recuperació davant d'ells?** | | |

| | | |
|---|---|---|
| **Protecció dels dispositius** | | |
| **S'han establert mesures de seguretat en els dispositius, com ara antivirus, antimalware, actualitzacions regulars, entre altres, per garantir la seva protecció davant possibles amenaces?** | | |
| **S'ha definit un pla de gestió de pegats i actualitzacions de programari, que estableixi la periodicitat i el procés per dur a terme aquestes tasques?** | | |
| **En el cas de dispositius mòbils, s'han implementat mesures com el xifrat de dades, l'autenticació d'usuari i la configuració de polítiques de seguretat per a l'ús de dispositius personals a l'empresa?** | | |
| **Monitoratge de la xarxa i detecció d'amenaces** | | |
| **S'ha implementat un sistema de monitoratge constant dels sistemes i xarxes de l'entitat?** | | |
| **S'han configurat alertes per notificar en temps real qualsevol incident o activitat sospitosa?** | | |
| **S'ha implementat un sistema de registre i gestió d'incidents per documentar i analitzar les causes dels mateixos?** | | |
| **S'ha definit un procés de resposta a incidents per actuar de manera ràpida i efectiva davant qualsevol problema de seguretat?** | | |
| **Continuïtat del negoci** | | |
| **S'han identificat els processos i sistemes crítics per al negoci i s'han establert plans de contingència per a la seva recuperació en cas d'interrupcions?** | | |
| **S'han realitzat proves periòdiques dels plans de contingència per garantir la seva efectivitat?** | | |
| **S'ha definit un equip de resposta a desastres per actuar ràpidament davant situacions crítiques?** | | |
| **S'ha establert un pla de comunicació per mantenir informats als empleats, clients i proveïdors sobre la situació i les mesures adoptades en cas d'interrupcions?** | | |
| **Avaluació i millora contínua** | | |
| **S'ha dut a terme una revisió del pla de seguretat en els últims 12 mesos?** | | |
| **S'han identificat debilitats o àrees de millora en el pla de seguretat?** | | |
| **S'han establert plans d'acció per abordar les debilitats o àrees de millora identificades?** | | |
| **S'han avaluat els riscos en els últims 12 mesos per identificar noves amenaces o vulnerabilitats?** | | |

| | | |
|---|---|---|
| **Conscienciació i formació** | | |
| **S'ha establert un programa de formació en seguretat de la informació per a tots els empleats, incloent-hi sessions de conscienciació i entrenament sobre les millors pràctiques de seguretat?** | | |
| **S'han realitzat proves periòdiques de phishing per avaluar la capacitat dels empleats per detectar i informar intents de frau?** | | |
| **S'han definit polítiques clares de seguretat de la informació i s'assegura que siguin enteses i seguides per tots els membres de l'entitat?** | | |
| **S'ha establert un sistema de recompenses i reconeixements per fomentar una cultura de seguretat en l'entitat?** | | |
| **Compliment normatiu LQPD** | | |
| S'ha dut a terme una auditoria de les dades personals que es manegen a l'entitat? | | |
| S'han classificat les dades personals segons el seu nivell de sensibilitat? | | |
| S'han implementat mesures tècniques i organitzatives per garantir la confidencialitat, integritat i disponibilitat de les dades personals? | | |
| S'ha implementat el xifrat als sistemes on es troben les dades personals? | | |
| S'han establert procediments clars per notificar les violacions de seguretat a l'autoritat de protecció de dades i als titulars de les dades personals afectats? | | |
| S'ha designat un responsable de protecció de dades a l'entitat? | | |