Pla de Seguretat de l'Operador (PSO)
Guia simplificada

(DOCUMENT SUBJECTE A MODIFICACIONS)

Abril 2023

Fitxa del document

Títol	Pla de Seguretat de l'Operador (PSO)

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	03/05/23	04/05/23

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. El Pla de Seguretat de l'Operador (PSO) és un document estratègic que estableix les mesures de seguretat necessàries per garantir la continuïtat i la qualitat dels serveis essencials que proporciona un operador crític. Aquest pla té com a objectiu prevenir, detectar, respondre i recuperar-se de possibles incidents de seguretat, i la seva elaboració és fonamental per minimitzar l'impacte d'aquests incidents a la societat i l'economia.
2. L'elaboració d'un PSO implica la identificació i l'avaluació dels riscos a què estan exposats els serveis crítics que proporciona l'operador. Per fer-ho, s'ha de dur a terme una metodologia d'anàlisi de riscos que permeti identificar les possibles amenaces, vulnerabilitats i conseqüències que poden afectar els serveis essencials, així com establir les mesures de seguretat necessàries per minimitzar-ne l'impacte.

1.2. OBJECTE D'AQUEST DOCUMENT

3. Aquesta guia és una versió simplificada que inclou els continguts mínims necessaris per elaborar un Pla de Seguretat de l'Operador (PSO) efectiu. Tot i que hi ha altres temes que poden ser rellevants per a una implementació més exhaustiva del PSO, en aquesta guia ens enfoquem en els aspectes més essencials que cal considerar en l'elaboració d'un PSO.

2. CONTINGUTS MÍNIMS DEL PSO

2.1. INTRODUCCIÓ

4. En aquesta secció, es presenta una breu introducció al Pla de Seguretat de l'Operador (PSO), explicant-ne l'objectiu.

5. Així mateix, cal destacar la importància de l'elaboració d'aquest pla, ja que els serveis essencials que proporciona l'operador crític són vitals per a la societat i la seva interrupció pot tenir conseqüències greus. Per tant, el PSO ha de ser vist com una eina de gestió clau per garantir la prestació ininterrompuda dels serveis essencials.

   - ✓ Objectiu: Presentar el propòsit i els objectius del Pla de Seguretat de l'Operador (PSO). L'objectiu principal del PSO és protegir els serveis crítics que presta l'operador crític. Cal fer esment que el PSO és un document clau per a la gestió de riscos i la protecció de la infraestructura crítica de l'organització.
   - ✓ Abast: Definir l'abast del PSO, és a dir, els serveis crítics que seran protegits a través del pla. S'ha de proporcionar una llista detallada dels serveis crítics essencials per a l'operació de l'organització. A més, cal establir l'àmbit geogràfic del PSO, és a dir, si s'aplicarà a una regió, país o fins i tot internacionalment.
   - ✓ Referències: Enumerar els documents de referència utilitzats en l'elaboració del PSO. Això pot incloure lleis i regulacions rellevants, estàndards de seguretat, polítiques i procediments interns, entre d'altres.

2.2. POLÍTICA GENERAL DE SEGURETAT DE L'OPERADOR I MARC DE GOVERNANÇA

6. En aquest punt, es descriu la política general de seguretat de l'operador i el marc de govern necessari per a l'elaboració del PSO.

7. La política general de seguretat de l'operador ha de ser coherent amb la política de seguretat nacional i europea, i l'ha d'aprovar la direcció de l'organització. El marc de govern ha d'incloure una estructura de gestió de seguretat, amb la identificació de rols i responsabilitats, i la designació d'un responsable de seguretat que coordini totes les activitats de seguretat.

   - ✓ Política de seguretat: Descriure la política de seguretat general de l'organització i com es relaciona amb el PSO. S'han de definir els principis i els objectius de seguretat que s'apliquen a l'organització i com aquests principis s'apliquen a la pràctica a través del PSO.
   - ✓ Marc de govern: Definir l'estructura de gestió de seguretat de l'organització i els rols i les responsabilitats de cadascun dels participants. També cal identificar els recursos necessaris per a la implementació del PSO, com el pressupost, el personal, la formació i la tecnologia. A més, cal establir com es durà a terme la revisió i la millora contínua del PSO.

2.3. RELACIÓ DE SERVEIS ESSENCIALS PRESTATS PER L'OPERADOR CRÍTIC

8. En aquesta part, s'estableix la relació dels serveis essencials prestats per l'operador crític, a fi d'identificar aquells que són prioritaris per a la continuïtat de les operacions i requereixen una protecció especial.
9. S'han d'identificar i classificar els serveis essencials en funció de la seva importància i criticitat, i s'han d'establir objectius de seguretat específics per a cadascun.
    - ✓ Identificació i classificació: Llistar i classificar els serveis essencials prestats per l'operador crític. És important tenir en compte que no tots els serveis són crítics i, per tant, cal identificar aquells que són essencials per a l'operació de l'organització. A més, cal establir els criteris utilitzats per classificar els serveis crítics, com ara l'impacte en la seguretat, la continuïtat del negoci i la reputació.
    - ✓ Objectius de seguretat: Establir objectius de seguretat específics per a cadascun dels serveis identificats. Aquests objectius han de ser coherents amb la política general de seguretat de l'organització i han d'estar en línia amb els requisits legals i reglamentaris. A més, cal definir els indicadors d'exercici fets servir per mesurar el compliment d'aquests objectius.

2.4. METODOLOGIA D'ANÀLISI DE RISCOS

10. En aquest punt, es presenta la metodologia d'anàlisi de riscos que s'utilitzarà per identificar els riscos i les amenaces que poden afectar la seguretat dels serveis essencials de l'operador crític.
11. La metodologia d'anàlisi de riscos ha de ser sistemàtica i cobrir tots els aspectes rellevants, des de la identificació dels actius crítics fins a l'avaluació de la vulnerabilitat i la probabilitat d'ocurrència d'amenaces.
    - ✓ Identificació d'actius crítics: Identificar els actius crítics necessaris per a la prestació dels serveis essencials de l'operador crític. Això pot incloure infraestructura, sistemes d'informació, personal, proveïdors i clients.
    - ✓ Avaluació de riscos: Descriure la metodologia utilitzada per avaluar els riscos associats amb la pèrdua, dany o alteració dels actius crítics identificats. La metodologia ha d'incloure la identificació d'amenaces, vulnerabilitats i potencial impacte en els serveis essencials de l'operador crític. A més, cal establir criteris per classificar els riscos, com ara la probabilitat d'ocurrència i l'impacte potencial.
    - ✓ Mitigació de riscos: Identificar i descriure les mesures de mitigació de riscos que s'aplicaran a cadascun dels riscos identificats. Aquestes mesures han de ser coherents amb la política general de seguretat de l'organització i han d'estar en línia amb els requisits legals i reglamentaris. A més, cal definir els indicadors d'acompliment fets servir per mesurar l'èxit d'aquestes mesures.

2.5. CRITERIS D'APLICACIÓ DE MESURES DE SEGURETAT INTEGRAL

12. En aquesta secció, s'estableixen els criteris d'aplicació de mesures de seguretat integral per garantir la protecció adequada dels serveis essencials de l'operador crític.

13. Els criteris d'aplicació han de considerar els objectius de seguretat establerts, l'avaluació de riscos, els recursos disponibles i les restriccions legals i operatives. Les mesures de seguretat integral han d'incloure mesures preventives i mesures de resposta a incidents.

    - ✓ Identificació de mesures de seguretat integral: Identificar les mesures de seguretat integral que s'aplicaran als serveis essencials de l'operador crític. Aquestes mesures han d'incloure controls físics, controls tècnics i controls organitzatius.
    - ✓ Priorització de mesures de seguretat: Establir criteris per prioritzar les mesures de seguretat integral identificades. Aquests criteris poden incloure el potencial impacte en els serveis essencials de l'operador crític, la probabilitat d'ocurrència i la viabilitat tècnica i econòmica d'implementar les mesures.
    - ✓ Planificació de la implementació: Establir un pla per a la implementació de les mesures de seguretat integral identificades. El pla ha d'incloure un calendari d'implementació, els recursos necessaris per a la implementació i els responsables de la implementació.

2.6. DOCUMENTACIÓ COMPLEMENTÀRIA

14. En aquesta part, es descriuen els documents complementaris necessaris per a l'elaboració i el manteniment del PSO.

15. La documentació complementària pot incloure manuals de procediments, registres d'incidents de seguretat, plans de contingència, plans de recuperació de desastres, entre altres documents necessaris per garantir l'efectivitat i el manteniment del PSO.

    - ✓ Plans de contingència: descriure els plans de contingència necessaris per abordar les possibles interrupcions dels serveis essencials.
    - ✓ Plans de recuperació de desastres: descriure els plans de recuperació necessaris per restaurar la infraestructura crítica en cas de desastre.
    - ✓ Manuals de procediments: descriure els manuals de procediments necessaris per a la implementació i manteniment del PSO.
    - ✓ Registres d'incidents de seguretat: descriure els registres d'incidents de seguretat necessaris per avaluar l'efectivitat del PSO.
    - ✓ Altres documents necessaris per garantir l'efectivitat.

3. VALIDACIÓ DEL PSO

16. El Pla de Seguretat de l'Operador (PSO) ha de ser validat i aprovat conjuntament entre l'autoritat nacional competent (ANC-AD, o AFA) i el cos de Policia d'Andorra, és un element clau per garantir la seguretat i la protecció dels ciutadans i les ciutadanes d'Andorra.
17. A través d'aquest pla es defineixen les estratègies i les mesures que s'han d'adoptar per prevenir i gestionar situacions de risc o d'emergència en diferents àmbits que requereixen la intervenció dels cossos de seguretat. A més, aquest pla també contempla la coordinació entre diferents institucions i organismes per assegurar una resposta eficaç i coordinada en situacions crítiques.
18. En definitiva, la validació i aprovació conjunta del Pla de Seguretat de l'Operador són un pas important per a la seguretat i la protecció dels ciutadans i les ciutadanes d'Andorra en situacions d'emergència i de risc.