Pla de Protecció Específic (PPE)

Guia de bones pràctiques

(DOCUMENT SUBJECTE A MODIFICACIONS)

Abril 2023

Fitxa del document

Títol	Pla de Protecció Específic (PPE)

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 i entitats privades.

La Llei 22/2022, de 9 de juny, , encomana a l´Agència Nacional de Ciberseguretat d´Andorra (ANC-AD, en endavant) 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 i autoritzada la seva modificació i distribució per part del CCN-CERT) per donar compliment a les comeses de l´ANC-AD i al reflectit en l' ENS-AD, 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. En el PPE, la Infraestructura Crítica (d'ara endavant IC), són aquelles instal·lacions, sistemes, serveis i xarxes que són essencials per al funcionament de la societat i la interrupció o destrucció dels quals podria tenir un impacte greu en la salut, la seguretat o el benestar econòmic de la població.
3. Mentre que l'Operador Crític (d'ara endavant OC) públic o privat recollirà de forma pràctica els següents aspectes i criteris inclosos en el seu Pla de Seguretat de l'Operador (d'ara endavant PSO), que afecten de manera específica a aquesta instal·lació:
   - ✓ Aspectes relatius a la seva política general de seguretat.
   - ✓ Desenvolupament de la metodologia d'anàlisi de riscos que garanteixi la continuïtat dels serveis proporcionats per aquest operador a través d'aquesta IC. L'OC és el responsable de garantir la seguretat de la IC, però no és el mateix que la mateixa IC.
   - ✓ Desenvolupament dels criteris d'aplicació de les diferents mesures de seguretat que s'implantin per fer front a les amenaces, tan físiques com aquelles que afectin la ciberseguretat, identificades en relació amb cada una de les tipologies dels actius existents en aquesta infraestructura.

1.2. OBJECTE D'AQUEST DOCUMENT

4. Amb el present document es pretén orientar aquells operadors designats com a crítics en l'elaboració dels seus PPE´s. Per tant, es tracta d'un document de caràcter obligatori. Per facilitar l'aplicació d'aquestes bones pràctiques s'han inclòs diferents exemples en aquest document.
5. En aquesta guia s'inclouen una sèrie d'annexos (detall de mesures organitzatives o gestió, operacionals o procedimentals, protecció o tècniques, etc.) que podran ser referents d'ajuda als operadors crítics per a la confecció d'un dels punts dels continguts mínims del PPE.

1.3. PROTECCIÓ DE LA INFORMACIÓ

6. Després de l'aprovació del PPE, el seu grau de classificació serà, com es sap, de difusió limitada, sent necessari que l'Operador Crític i la Infraestructura Crítica defineixin els seus procediments de gestió i tractament de la informació d'acord amb uns estàndards de seguretat que garanteixin una adequada i eficaç protecció d'aquesta informació.

Per a això, l'OC prendrà com a referència les orientacions dictades per l'Autoritat Nacional de Seguretat, entre les quals cal destacar:

2. ASPECTES ORGANITZATIUS

2.1. ORGANIGRAMA DE SEGURETAT

7. L'operador crític ha de presentar gràficament l'estructura organitzativa funcional que existeix en matèria de seguretat integral en la infraestructura crítica, amb indicació de tots els actors que hi participen, el seu rol de responsabilitat i la seva jerarquia en el procés de presa de decisions. De la mateixa manera, s'ha d'establir la dependència d'aquesta estructura amb la qual està definida en el corresponent Pla de Seguretat de l'Operador.

2.2. DELEGATS DE SEGURETAT DE LES INFRAESTRUCTURES CRÍTIQUES

8. L'operador aportarà la informació sol·licitada en aquest apartat, sent recomanable informar també dels mecanismes de contingència i continuïtat adoptats per garantir la comunicació amb el delegat de seguretat en cas d'incidents o que aquesta persona es vegi afectada per qualsevol mena de succés advers que no li permetin estar accessible, així com els canals de coordinació existents amb els diferents actors afectats.
9. Pel que fa a la formació que haurà de reflectir, en funció del pla de formació, hauria d'incloure aspectes tant tècnics com de gestió en l'àmbit de la seguretat i, en les seves dues dimensions més tradicionals (física i ciberseguretat). Seria recomanable incloure la formació que ha rebut d'acord amb el que està previst en el Pla de Formació recollit en el PSO.

2.3. MECANISMES DE COORDINACIÓ

10. Per clarificar els mecanismes de coordinació establerts amb relació a la IC conforme al que s'estableix en el document de continguts mínims del PPE, es recomana identificar, en primer lloc, tots aquells interlocutors amb els quals s'ha d'establir relació en l'àmbit de la protecció de les IC, tant dins com fora de la mateixa infraestructura.
11. A continuació, s'hauria de recollir per a cada un d'ells, tant el mecanisme de comunicació principal com el secundari per a casos de contingències (canals que haurien de ser provats periòdicament, com és lògic).
12. Així mateix, s'haurien de reflectir també les reunions, comitès, protocols i qualsevol altre mecanisme que s'empri per a la coordinació amb aquests organismes/roles, així com els procediments d'actuació previstos davant les diferents situacions crítiques o extraordinàries amb l'objectiu de minimitzar l'impacte d'aquestes eventualitats.
13. Finalment, seria convenient desenvolupar plans de comunicació per mantenir informats de les novetats a cada un dels nivells de responsabilitat i funcionalitat entre els diferents actors.

2.4. MECANISMES I RESPONSABLES D'APROVACIÓ

14. Igual que per altres tipus de polítiques i procediments, s'hauria de recollir el procediment que s'utilitza per a l'aprovació i revisió interna del mateix PPE, és a dir:

- ✓ Qui és el responsable de la seva aprovació.
- ✓ Qui és el responsable de la seva revisió i actualització si fos necessari.
- ✓ Quins són els passos per a la seva aprovació i a qui es comuniquen les modificacions en el pla (incloent-hi qualsevol tercer afectat per aquestes modificacions).
- ✓ Periodicitat amb la qual es revisa el pla (que ha de complir, en qualsevol cas, amb els requisits legals establerts) i data de l'última revisió.
- ✓ Aspectes que seran objecte de revisió.
- ✓ Registres generats pel procediment de revisió que permetran comprovar que el Pla ha estat revisat, encara que no s'hagi traduït en modificacions del pla (reunions, actes del comitè corresponent, estudis i anàlisi elaborada, actualitzacions de l'anàlisi de riscos, etc.)

3. DESCRIPCIÓ DE LA INFRAESTRUCTURA CRÍTICA

3.1. DADES GENERALS

15. L'Operador Crític, com a introducció de la Infraestructura Crítica, hauria d'incloure com a mínim la informació de context suficient per descriure els següents aspectes:

- ✓ Informació de caràcter estratègic
  - Descripció del servei essencial que suporta i àmbit geogràfic d'aquest.
  - Relació amb altres possibles infraestructures necessàries per a la prestació d'aquest servei essencial.
    - Del mateix sector
    - D'altres sectors
  - Descripció de les seves funcions i de la seva relació amb els serveis essencials suportats.
- ✓ Informació de caràcter general
  - Denominació i tipus d'instal·lació
  - Descripció general de la infraestructura a protegir
  - Propietat i gestió de la Infraestructura Crítica
- ✓ Localització física i estructura de la infraestructura a protegir
  - Ubicació geogràfica de la infraestructura
  - Plànols generals de la infraestructura amb referència a tots els elements, així com la seva ubicació relativa i absoluta.
  - Fotografies rellevants de la infraestructura i els elements que la componen.
  - Components (Edificis/Instal·lacions/etc.)
- ✓ Sistemes TIC i arquitectura
  - Mapa de xarxa i comunicacions
  - Mapa de sistemes i serveis
  - Sistemes de control

3.2. ACTIUS / ELEMENTS

16. S'hauria de fer una descripció de tots els actius que suporten la infraestructura crítica, diferenciant aquells que són vitals dels que no ho són i detallant les dependències existents entre ells. La informació que es podria incloure seria l'enumerada a l'ENS-STIC-001 (Catàleg d'actius d'informació estàndard).

3.3. INTERDEPENDÈNCIES

17. S'hauria de realitzar una descripció i el motiu que origina les possibles interdependències entre serveis essencials i infraestructures crítiques pròpies, així com, amb les d'altres operadors dins del mateix sector o diferent, que hagin de ser considerades en l'anàlisi de riscos en el marc global de l'organització. En aquest sentit, cal tenir en compte l'anàlisi de risc del marc global de l'organització així com la manera en què afecten el servei, analitzant les possibles dependències d'entrada,

de sortida i de procés, sense oblidar tant l'àmbit intern com extern a l'organització de la dependència. Alguns exemples d'interdependències serien:

- ✓ Amb altres infraestructures crítiques del mateix operador.
- ✓ Amb altres infraestructures estratègiques del mateix operador.
- ✓ Entre les seves pròpies instal·lacions o serveis.
- ✓ Amb els seus proveïdors dins de la cadena de subministraments.
- ✓ Amb els proveïdors de serveis TIC contractats per a aquesta infraestructura, tals com: proveïdor(s) de telecomunicacions, Centres de Procés de Dades, serveis de seguretat (Centre d'Operacions de Seguretat, CERT privat, etcètera) i qualsevol altre que es consideri, especificant per a cada un d'ells el nom del proveïdor, els serveis contractats, acords de nivell de servei (SLA) i compliment del servei prestat amb la política general de seguretat de l'operador.
- ✓ Amb els proveïdors de serveis de seguretat física, indicant els serveis prestats i el personal i mitjans emprats.
- ✓ Etc.

4. RESULTATS DE L'ANÀLISI DE RISCOS

4.1. AMENACES CONSIDERADES

18. Per a l'anàlisi de riscos a realitzar es podrien prendre com a punt de partida diferents tipologies d'amenaces que estan definides a l'ENS-STIC-804 o en diferents catàlegs referents en l'àmbit nacional o internacional.
19. En aquest sentit, s'han d'analitzar les principals amenaces tipus físic com a la ciberseguretat que poguessin tenir un origen intencionat per part de tercers diferents dels mateixos operadors i que poguessin afectar els actius.
20. Els OC podran dirigir-se a l'Agència de Ciberseguretat Andorrana per obtenir l'arbre d'amenaces que haurà de tenir com a guia per a la realització d'aquesta activitat.

4.2. MESURES DE SEGURETAT INTEGRAL EXISTENTS

21. Es consideren mesures de seguretat integral, les mesures de protecció dels actius. Aquestes mesures poden ser permanents, temporals i graduades.
22. En les seccions següents es proporcionen recomanacions i exemples generals a partir dels quals es podria estructurar la seguretat integral dels serveis essencials i les infraestructures crítiques de les quals depèn. La llista d'exemples proporcionada no és exhaustiva, però pot servir com a punt de partida per a organitzar les necessitats de protecció de l'entorn concret de protecció per al qual siguin aplicables.
23. L'Operador haurà de descriure les mesures de seguretat integral actualment implantades en línia amb l'anàlisi de riscos realitzada. Es recomana seguir una organització de les mesures en tres nivells:
    - ✓ Mesures organitzatives o de gestió
    - ✓ Mesures operacionals o procedimentals
    - ✓ Mesures de protecció o tècniques
24. En general, les mesures a implementar, o implementades, hauran de ser acordes amb la legislació vigent i aplicable, tant pel que fa a la documentació exigible com a la instal·lació i manteniment.

4.2.1. ORGANITZATIVES O DE GESTIÓ

25. Totes les organitzacions tenen una funció, missió o negoci, que determina els seus objectius (què s'ha d'aconseguir) i estratègies (com s'ha d'aconseguir). És per això que la seguretat integral d'una organització hauria d'alinear-se per garantir la consecució d'aquests.
26. Les mesures organitzatives són el conjunt de mesures de seguretat incrustades en els processos i estructures organitzatives existents en l'organització i el seu objectiu principal és gestionar la complexitat de les operacions de gestió de la seguretat i donar resposta als riscos, factors normatius i reguladors de l'entorn.

27. A l'Annex I (secció 7.1) s'inclou informació addicional sobre les següents mesures organitzatives o de gestió que es poden establir:

    - ✓ Definició d'un cos normatiu
    - ✓ Organització de la seguretat
        - Comitè de seguretat i crisi
        - Establiment de rols
        - Gestió de canvis
        - Gestió de la qualitat i de la documentació
    - ✓ Mitjans Humans i seguretat del personal
        - Formació i consciència
        - Protecció del personal

4.2.2. OPERACIONALS O PROCEDIMENTALS

28. Derivats del cos normatiu establert en l'organització, les bones pràctiques recomanen la documentació del conjunt indispensable de procediments operacionals o procedimentals amb el seu àmbit concret que permeti realitzar una gestió integral del procés de seguretat i l'adequada gestió dels controls implantats. Tot això amb l'objectiu d'aconseguir l'eficàcia i l'eficiència dels mateixos d'acord amb els riscos contemplats i la racionalitat i proporcionalitat de la protecció requerida.

29. A l'Annex (secció 7.2) es descriuen els procediments d'alt nivell que inclouen la tipologia de controls que són aconsellables d'acord amb les bones pràctiques de seguretat. En concret, en aquest Annex s'inclou informació sobre els següents:

    - ✓ Procediments per a la realització, gestió i manteniment d'actius crítics (cicle de vida).
    - ✓ Gestió de la formació, conscienciació i capacitació.
    - ✓ Gestió de la continuïtat, detallant a més els mètodes i polítiques de còpies de seguretat (backup).
    - ✓ Supervisió contínua i monitoratge
    - ✓ Gestió d'accés
    - ✓ Gestió d'evacuació i emergències
    - ✓ Gestió de la informació i comunicació
    - ✓ Gestió de la resposta davant amenaces i incidents
        - Procediment per a la catalogació
        - Procediment per a l'escalat
        - Procediment per a la resposta
    - ✓ Gestió del coneixement
    - ✓ Revisió

4.2.3. DE PROTECCIÓ O TÈCNIQUES

30. Les mesures de protecció o tècniques fan referència a aquells conjunts de controls de caràcter tècnic necessàriament implantats a l'organització per aconseguir un nivell de risc acceptable. La forma més recomanable d'implementació és mitjançant

l'establiment de mesures automatitzades que permetin crear registres d'evidències fiables.

31. A continuació, de forma no exhaustiva, es proporciona un conjunt d'exemples d'alt nivell de controls i mesures agrupades d'acord amb el que considerem criteris pràctics: facilitat de lectura, catalogació i naturalesa de les mesures. Aquestes agrupacions de controls tenen per objecte facilitar la seva inclusió en un cicle de gestió contínua de la seguretat que permeti major eficàcia i eficiència en la implementació i manteniment de la seguretat. Això no impedeix que algunes de les mesures poguessin ser classificades en més d'un grup. No obstant això, l'objectiu és facilitar la seva identificació i comprensió de forma general per, conforme a les necessitats, aplicar mesures més concretes derivades o relacionades amb aquestes. Per exemple, si s'indica de forma general mesures de control de perímetre de seguretat, hi ha diversos grups de mesures que poden ser implantats conforme a les necessitats de defensa en profunditat: hipotèticament conforme als riscos seria necessari implementar una tanca, un volumètric i una càmera de videovigilància; addicionalment per a la protecció del perímetre lògic seria necessària la segmentació de la xarxa, la creació d'una DMZ, l'aplicació de regles de firewall i de sistemes de detecció d'intrusions, etc.

32. Per organitzar un cicle de gestió contínua de la seguretat les agrupacions proposades són les següents:

    - ✓ Prevenció i detecció
    - ✓ Vigilància i monitoratge
    - ✓ Coordinació i resposta
    - ✓ Continuïtat i contingència

33. En l'Annex I (apartat 7.3) s'inclou informació addicional sobre cada un dels tipus de mesures que es poden aplicar en cada cas.

4.3. AVALUACIÓ DE RISCOS

34. A partir de la selecció de les diferents mesures de seguretat que hagin estat implantades, es procedirà a estimar el risc residual al qual es troba exposada una infraestructura. Per poder procedir a aquesta estimació, s'haurà de tenir en consideració el grau d'implantació de cada una d'aquestes mesures de seguretat, és a dir, s'hauria d'avaluar si:

    - ✓ Estan correctament implantades
    - ✓ Estan operatives
    - ✓ Estan protocol·litzats
    - ✓ Estan sota un sistema de gestió i millora contínua
    - ✓ Són objecte de proves regulars per verificar el seu correcte funcionament i que el personal encarregat d'usar-les està format en les seves funcions i respon en els temps previstos

35. Per determinar el càlcul final dels riscos als quals es troba exposada la infraestructura, s'haurien de tenir en consideració les probabilitats que existeixen

que el conjunt d'amenaces identificades puguin arribar a afectar la infraestructura, així com el potencial impacte que podrien provocar. A partir d'aquest càlcul, s'hauria de contemplar la reducció del risc a partir de les mesures de seguretat que s'hagin pogut implantar, ja sigui per la reducció en les probabilitats que arribessin a succeir o bé per la reducció de l'impacte que provocaria aquesta determinada amenaça en el supòsit que es materialitzés.

36. S'han de diferenciar en aquesta anàlisi els diferents escenaris de la IC, així com, si escau, els diferents horaris del seu funcionament (instal·lació ocupada o no, etc.).

37. En qualsevol cas, donat l'enfocament de protecció dels serveis essencials que es persegueix, s'haurà de prestar especial atenció a les amenaces d'alt impacte i baixa probabilitat d'ocurrència que poguessin afectar el servei essencial i dotar-se de les mesures de protecció pertinents.

38. Amb l'objectiu de mostrar la informació de l'avaluació de riscos realitzada, es podrien elaborar dues taules similars a les següents que resumeixen les principals dades de l'anàlisi:

Per als actius amb nivells de risc alts o molt alts

Actius	Amenaça	Risc intrínsec			Controls existents	Risc residual		
		Probabilitat	Impacte	Risc		Probabilitat	Impacte	Risc

Per als actius amb nivells d'impacte alts o molt alts

Actius	Amenaça	Risc intrínsec		Controls existents	Risc residual	
		Probabilitat	Risc		Probabilitat	Risc

39. La interpretació de la informació recollida a les taules anteriors és la següent:

- ✓ Actiu. Element / component de la infraestructura crítica.
- ✓ Amenaça. Esdeveniment que pot afectar el funcionament o la disponibilitat de l'actiu i, per tant, del servei essencial.
- ✓ Risc intrínsec. Anàlisi elaborada amb caràcter previ a l'aplicació de mesures de seguretat.
  - Probabilitat. Possibilitat que l'amenaça es materialitzi sobre l'actiu.
  - Impacte. Estimació de les conseqüències de l'ocurrència de l'amenaça (està relacionat amb el valor de l'actiu).
  - Risc. Resultat de la combinació dels valors previs de probabilitat i impacte.
- ✓ Controls existents. Mesures de seguretat que s'apliquen en l'actualitat i que redueixen, bé la probabilitat, bé l'impacte.
- ✓ Risc residual. Anàlisi elaborada considerant ja els controls aplicats. Per tant, hauran de ser valors inferiors als intrínsecs.
  - Probabilitat. Possibilitat que l'amenaça es materialitzi considerant les mesures de seguretat existents (només les mesures preventives redueixen la probabilitat).

- Impacte. Estimació de les conseqüències de l'ocurrència de l'amenaça, considerant les mesures de seguretat aplicades (només les mesures de detecció i les correctives redueixen l'impacte).
- Risc. Resultat dels valors de probabilitat i impacte residuals previs.

5. PLA D'ACCIÓ PROPOSAT

40. El pla d'acció consisteix en la planificació completa per a la implementació de les mesures de seguretat identificades en l'anàlisi de riscos de la infraestructura crítica com a necessàries per a complementar les existents en l'actualitat, de forma que puguin establir-se dates per a la seva implementació.

41. El pla d'acció es constitueix en un nombre d'accions on s'agruparien les mesures de seguretat d'índole organitzativa, operacional i tècnica, que s'haurien d'implantar, monitorar i gestionar per afrontar els riscos detectats.

42. El pla d'acció és part del PPE i hauria de ser implementat en el termini màxim de tres anys. La seva revisió s'hauria de realitzar basant-se sempre en una anàlisi de riscos prèvia.

43. El pla d'acció hauria de recollir els següents requisits:

- ✓ Prioritzar les accions, d'acord amb- el nivell de risc associat, tenint en compte les possibles dependències existents entre elles.
- ✓ Estructurar les distintes mesures de seguretat, associant-les d'acord amb la seva finalitat i naturalesa, en accions que resultin acotades i viables.
- ✓ Assignar responsabilitats en la implantació de les accions.
- ✓ Realitzar una planificació completa i detallada on s'inclogui l'estimació sobre les inversions i els terminis necessaris per a la seva implantació.
- ✓ Establir un mecanisme de seguiment per mitjà de mètriques que permeti conèixer l'estat de les accions.

44. A cada mesura de seguretat resultant de l'anàlisi de riscos, l'Operador Crític hauria d'assignar-li un nivell de prioritat de cara a la reducció del risc que la implantació d'aquesta mesura de seguretat provocaria en l'avaluació general dels riscos que afecten la Infraestructura Crítica.

45. D'acord amb el nivell de prioritat assignat a una determinada mesura de seguretat, l'Operador Crític podria prioritzar la implantació de les mesures en forma d'accions.

5.1. ACCIONS

46. Les accions abasten un conjunt de mesures de seguretat que s'hauran d'implementar conjuntament.

47. L'Operador Crític podria definir, per a cada acció, les següents dades:

- ✓ Identificació de l'acció: Consisteix en un codi únic i un nom descriptiu per a l'acció.
- ✓ Objectius: Especificació, incloent-hi àmbit i abast, de la finalitat cap a la qual s'orienta el conjunt de mesures de seguretat que componen l'acció i la reducció del risc esperada a la implantació d'aquesta.
- ✓ Descripció: Resum dels continguts i implicacions de l'acció de manera descriptiva.

- ✓ Responsable: Identifica el departament o persona al càrrec de l'execució de l'acció.
- ✓ Dependències: Reflecteix les possibles relacions existents entre altres accions i la que es desenvolupa.
- ✓ Actius: Actius sobre els quals s'aplica l'acció.
  - Identificador de l'Actiu: Consisteix en un codi únic i un nom descriptiu per a l'actiu.
  - Tipologia de l'Actiu: Defineix la tipologia de l'actiu sobre el qual s'aplica l'acció. Aquesta podria ser, per exemple:
    - Instal·lacions de la IC necessàries per a la prestació del servei essencial. (Codi: INS).
    - Sistemes informàtics, ja sigui hardware o software. (Codi: SI).
    - Xarxes de comunicacions que s'utilitzen en aquesta IC. (Codi: RED).
    - Persones que exploten o operen amb els actius anteriorment esmentats. (Codi: PER).
    - Proveïdors crítics que són necessaris per al funcionament de la IC. (Codi: PRO).
  - Responsable de l'Actiu: Responsable a càrrec de l'actiu sobre el qual s'aplica l'acció.
- ✓ Llistat de les mesures de seguretat: Recull les diferents mesures de seguretat agrupades com a part integrant de l'acció, el responsable d'aquesta mesura de seguretat i la seva tipologia.
- ✓ Inversió estimada: Estimació de cost de l'acció, basat en l'experiència en pressupostos per a accions anteriors, anàlogues i en entorns similars. S'adjuntarà a més un breu desglossament de l'esforç en recursos estimat, així com les tecnologies i solucions que s'han tingut en consideració.
- ✓ Estimació temporal: Data en la qual està previst que es desenvoluparà l'acció.
- ✓ Mecanismes de coordinació i seguiment: Mecanismes que s'aplicaran per a la coordinació i seguiment en l'execució de l'acció sobre un o diversos actius.

Taula 1. Exemple de fitxa d'actiu

IDENTIFICADOR DE L'ACCIÓ:		
CODI ÚNIC		
NOM DESCRIPTIU		
OBJECTIU:		
ESPECIFICACIÓ DE LA FINALITAT DE L'ACCIÓ.		
DESCRIPCIÓ:		
DESCRIPCIÓ DE L'ACCIÓ.		
RESPONSABLE:		
RESPONSABLE DE L'ACCIÓ.		
DEPENDÈNCIES AMB ALTRES ACCIONS:		
ACCIONS AMB LES QUALS AQUESTA GUARDA RELACIÓ.		
Actius		
Identificador:	**Responsable:**	**Tipologia:**
Identificador de l'actiu 1 (Codi i Nom Descriptiu)	Responsable de l'actiu 1	INS / SI / XARXA / PER / PRO
Identificador de l'actiu 2	Responsable de l'actiu 2	INS / SI / XARXA / PER / PRO
Mesures de Seguretat		
Identificador:	**Responsable:**	**Tipologia i Caràcter:**
Mesura de seguretat 1	Responsable de la mesura de seguretat 1	Organitzativa / Operacional / Tècnica / Permanent / Gradual
Mesura de seguretat 2	Responsable de la mesura de seguretat 2	Organitzativa / Operacional / Tècnica / Permanent / Gradual
MECANISMES DE COORDINACIÓ I SEGUIMENT:		
MECANISMES PER A L'ACCIÓ.		
INVERSIÓ:	**ESTIMACIÓ TEMPORAL:**	
ESTIMACIÓ DEL COST DE L'ACCIÓ.		

5.2. MESURES DE SEGURETAT

48. L'èxit d'una acció està lligat a l'aplicació ordenada d'una o múltiples mesures de seguretat que poden interrelacionar-se. Les mesures de seguretat es poden segmentar en tasques atòmiques que porten a la consecució de la mesura de seguretat.

49. Per a la definició adequada de les mesures de seguretat es podrien definir les següents dades:

- ✓ Identificació de la mesura de seguretat: Consistent en un codi únic i un nom descriptiu de la mesura de seguretat.
- ✓ Descripció: Resumeix els continguts i implicacions de la mesura de seguretat de manera descriptiva.

- ✓ Responsable: Identifica el departament o persona encarregada de l'execució de la mesura de seguretat.
- ✓ Identificació de l'acció: Mostra l'acció en la qual s'emmarca la mesura de seguretat.
- ✓ Criticitat: Marca el nivell d'importància de la mesura de seguretat. L'execució d'una mesura de seguretat de nivell de criticitat més alt tindrà un major impacte en la gestió de riscos.
- ✓ Caràcter: El caràcter distingeix entre mesura de seguretat permanent o gradual.
  - Permanent: Mesura de seguretat que s'aplica en qualsevol circumstància.
  - Gradual: S'activarà en funció dels diferents nivells d'amenaça. S'haurà d'indicar les circumstàncies d'activació.
- ✓ Tipologia: La tipologia de la mesura de seguretat serà relativa a les següents.
  - Organitzatives o de gestió.
  - Operacionals o procedimentals.
  - De protecció o tècniques.
- ✓ Actius: Actius sobre els quals s'aplica la mesura de seguretat.
  - Identificador: Consisteix en un codi únic i un nom descriptiu de l'actiu.
  - Responsable: Responsable a càrrec de l'actiu sobre el qual s'aplica la mesura de seguretat.
  - Tipologia: Defineix la tipologia de l'actiu:
- ✓ Instal·lacions de la IC necessàries per a la prestació del servei essencial. (Codi: INS).
- ✓ Sistemes informàtics, ja siguin hardware o software. (Codi: SI).
- ✓ Xarxes de comunicacions que s'utilitzin en aquesta IC. (Codi: RED).
- ✓ Persones que exploten o operen amb els actius anteriorment esmentats. (Codi: PER).
- ✓ Proveïdors crítics que són necessaris per al funcionament de la IC. (Codi: PRO).
- ✓ Llistat de tasques: Recull les diferents tasques unitàries a desenvolupar que podrien considerar-se necessàries, si bé no suficients, per a la consecució de la mesura de seguretat. Així com una descripció d'aquesta tasca.

Taula 2. Exemple de Mesura de seguretat

IDENTIFICADOR DE LA MESURA DE SEGURETAT:		
CODI ÚNIC		
NOM DESCRIPTIU		
DESCRIPCIÓ:		
DESCRIPCIÓ DE LA MESURA DE SEGURETAT.		
RESPONSABLE:		
RESPONSABLE DE LA MESURA DE SEGURETAT.		
ACCIÓ:		
IDENTIFICADOR DE L'ACCIÓ QUE ENGLOBA AQUESTA MESURA DE SEGURETAT.		
CRITICITAT:	**CARÀCTER:**	**TIPOLOGIA:**
NIVELL DE CRITICITAT.	☐ PERMANENT ☐ TEMPORAL / GRADUAL NIVELL D'AMENAÇA INDICA EL NIVELL D'AMENAÇA O CIRCUMSTÀNCIA PER A LA ACTIVACIÓ DE LA MESURA TEMPORAL O GRADUAL.	ORGANITZATIVA O DE GESTIÓ / OPERACIONAL O PROCEDIMENTAL / DE PROTECCIÓ O TÈCNICA.
Identificador de l'actiu 2	Responsable de l'actiu 2	INS / SI / XARXA / PER / PRO
Actius		
Identificador:	**Responsable:**	**Tipologia**
Identificador de l'actiu 1 (Codi i Nom Descriptiu)	Responsable de l'actiu 1	INS / SI / XARXA / PER / PRO
Identificador de l'actiu 2	Responsable de l'actiu 2	INS / SI / XARXA / PER / PRO
TASQUES:		
Tasca 1: Descripció de la tasca 1. Tasca 2: Descripció de la tasca 2		

6. DOCUMENTACIÓ COMPLEMENTÀRIA

50. L'Operador Crític incorporarà com a Annex la planimetria general de la instal·lació i també aquells altres plànols que incorporin la ubicació de les mesures de seguretat implementades. Així mateix, també es podrà adjuntar aquella altra informació que es pugui generar dels diferents apartats d'aquest document.

51. Es farà una breu referència a tots aquells plans de diferent tipus (emergència, autoprotecció, ciberseguretat, etc.), que afectin la instal·lació amb la finalitat d'establir una adequada coordinació entre ells, així com tota aquella normativa i bones pràctiques que regulin el bon funcionament del servei essencial prestat per aquesta infraestructura i els motius pels quals li són d'aplicació.

52. Les normatives a incloure comprendran tant les de rangs nacionals, autonòmics, europeus i internacionals, com les sectorials, relatives a:

- ✓ Seguretat Física.
- ✓ Ciberseguretat.
- ✓ Seguretat de la Informació en qualsevol dels seus àmbits.
- ✓ Seguretat Personal.
- ✓ Seguretat Ambiental.
- ✓ Autoprotecció i Prevenció de Riscos Laborals.

7. ANNEX 1: DETALL DE MESURES DE SEGURETAT

7.1. DETALL DE MESURES ORGANITZATIVES O DE GESTIÓ

7.1.1. COS DEFINIT NORMATIU

53. És aconsellable establir els processos de seguretat perquè donin cabuda al compliment normatiu, i regulador que afecta l'organització i els seus actius. Per això és convenient identificar els controls de seguretat derivats de la normativa identificada o reglamentacions aplicables al PPE.

54. Generalment, solen ser aplicables els següents conjunts de processos en la definició i estructuració del cos normatiu:

- ✓ Relació amb normativa interna i corporativa
- ✓ Seguretat física
- ✓ Protecció civil
- ✓ Seguretat ambiental
- ✓ Seguretat personal
- ✓ Seguretat d'autoprotecció i prevenció de riscos laborals
- ✓ Seguretat lògica i de la informació

55. Per això és necessari organitzar de forma manejable, proporcionada i documentada tota la informació sobre els controls i mesures de seguretat implementades o que haurien de ser-ho d'acord amb el tractament de riscos.

56. A alt nivell aquesta organització sol incloure:

- ✓ Polítiques i estàndards de seguretat
- ✓ Criteris de seguretat
- ✓ Procediments
- ✓ Compliment de normes i/o regulacions d'aplicació a la infraestructura crítica, així com identificació del seu nivell de compliment.
- ✓ Certificacions, acreditacions i avaluacions de seguretat obtingudes per a la infraestructura crítica.
- ✓ Plans d'acció i millora de la seguretat
- ✓ Definició de rols i responsabilitats: Segregació de tasques.
- ✓ Jerarquia i responsabilitats de llocs de treball
- ✓ Relacions amb tercers
- ✓ Gestió de la documentació i estructura de dependència i del procés d'elaboració i presentació d'informes.
- ✓ Gestió de canvis

7.1.2. ORGANITZACIÓ DE LA SEGURETAT

57. L'organització de seguretat estableix de forma general les estructures organitzatives adequades i les directrius de seguretat a tenir en compte per a l'elaboració dels diferents processos que es desenvolupen en les funcions de seguretat i els criteris aplicables a aquests.

58. Una de les tasques principals d'organitzar la seguretat consisteix a gestionar el factor humà, capacitant-se en els processos de seguretat tot el que fa referència a la gestió de les persones i les tasques directament executades per aquestes.

59. Com a exemple, entre els controls a tenir en compte, podem contemplar els següents:

- ✓ Selecció i contractació del personal de seguretat
- ✓ Els accessos de persones
- ✓ La vigilància de la instal·lació
- ✓ Operació dels sistemes de seguretat
- ✓ Formació i entrenament
- ✓ Classificació de la informació
- ✓ Acords de confidencialitat
- ✓ Simulacres.

7.1.2.1. COMITÈ DE SEGURETAT I CRISI

60. Ja que la seguretat és un procés transversal a l'organització, les millors pràctiques per a la seva gestió recomanen la creació d'un comitè de seguretat i crisi amb capacitat per a prioritzar i responsabilitzar-se de les accions necessàries per a la protecció i continuïtat dels serveis i l'organització. La millor forma de progressar és col·laborar. És convenient la creació de grups de treball en què es permeti una col·laboració activa per part de les persones encaminades a eliminar les debilitats del sistema o establir protocols comuns d'actuació davant situacions de crisi.

7.1.2.2. ESTABLIMENT DE ROLS

61. El factor humà és el que realment determina l'efectivitat de qualsevol sistema de seguretat. És per això que ha d'existir un conjunt clar de funcions de seguretat i responsabilitats adequades segregades. És important tenir en compte els següents punts a l'hora d'assignar responsabilitats:

- ✓ Assignar i documentar les responsabilitats.
- ✓ Documentar i definir clarament els nivells d'autorització dins del sistema.

7.1.2.3. GESTIÓ DE CANVIS

62. La implantació del control dels canvis realitzats en qualsevol sistema, especialment els relacionats amb la seguretat i les infraestructures crítiques, hauria de realitzar-se

com a mínim mitjançant procediments formals (documentats) de control de canvis que contemplin almenys:

- ✓ Avaluació de riscos
- ✓ Anàlisi dels efectes dels canvis
- ✓ Especificació dels controls de seguretat necessaris

63. Com a recomanació de bones pràctiques, és aconsellable la implementació automatitzada de controls de canvis, de procediments de marxa enrere i la generació dels registres d'auditories pertinents.

7.1.2.4. GESTIÓ DE LA QUALITAT I DOCUMENTACIÓ

64. És essencial una bona gestió de la documentació relacionada amb els sistemes i ubicacions de les infraestructures crítiques de les quals depenen els serveis essencials.

65. Específicament, les referències i normes aplicables concretament al servei essencial han d'estar identificades per extreure'n els controls de seguretat específics que són necessaris per a la instal·lació / servei.

7.1.3. MITJANS HUMANS I SEGURETAT DEL PERSONAL

7.1.3.1. FORMACIÓ I CONSCIENCIACIÓ

66. Partint d'una estratègia planificada de formació: entrenament, reentrenament i conscienciació, és convenient sensibilitzar i formar al personal, almenys, en les següents funcions:

- ✓ Els seus rols i responsabilitats.
- ✓ Els coneixements tècnics necessaris per al desenvolupament de la seva funció.
- ✓ La sensibilització i coneixement de les polítiques i procediments establerts.

7.1.3.2. PROTECCIÓ DEL PERSONAL

67. El personal és el principal actiu de tota organització. Les condicions de salut, ambientals i seguretat personal són determinants en tots els processos de seguretat establerts; per la qual cosa és adequat establir protocols de protecció per a aquelles persones que, per la seva funció dins de l'organització, puguin suposar un alt risc en cas de comprometre's la seva seguretat.

7.2. DETALL DE MESURES OPERACIONALS O PROCEDIMENTALS

7.2.1. PROCEDIMENT DE GESTIÓ I MANTENIMENT D'ACTIUS CRÍTICS

68. Una de les formes més eficients de protegir les Infraestructures crítiques d'una organització és mitjançant el modelatge de les mateixes prenent com a base el servei i/o els sistemes que la conformen.

69. D'acord amb aquest model, el punt de partida és la identificació dels actius que volem protegir, per la qual cosa és convenient disposar de l'inventari dels elements integrants. A l'hora de classificar els actius, sovint és necessari establir una sèrie de paràmetres per poder determinar el seu nivell i/o la seva agrupació en sectors o conjunts d'elements. Com a exemple d'alguns paràmetres a tenir en compte, podríem destacar els següents:

    - ✓ Impacte de l'incident en actius que afectin el funcionament general del sistema.
    - ✓ Impacte del problema en actius que afectin els usuaris del sector.
    - ✓ Impacte del problema en actius que afectin la resta de sectors.
    - ✓ Capacitat de resolució del problema en un determinat actiu.
    - ✓ Temps estimat per a la resolució del problema en un determinat actiu.
    - ✓ Possibilitat de propagació del problema en el mateix sector a través d'un determinat actiu.
    - ✓ Cost de la resolució del problema o substitució de l'actiu.

70. Per exemple, els actius més crítics d'un sector podrien ser els centres de control, ja que normalment controlen la resta d'elements, però caldrà tenir en compte els diferents sectors, perquè cadascun tindrà les seves particularitats.

71. En una central nuclear, potser el subsistema encarregat del seu control directe sigui el més crític, perquè el dany que pot causar qualsevol problema en l'entorn pot ser incalculable.

72. De la mateixa manera, a les subestacions encarregades de proveir d'energia a les diferents àrees geogràfiques també seran molt importants, però a mesura que ens acostem al destí final (usuari) la criticitat serà menor, ja que haurien d'existir camins redundants a l'hora de proveir a l'usuari final o una capacitat de reacció davant contingències més immediates.

73. Respecte als sectors de telecomunicacions, la possibilitat d'establir camins secundaris a través d'antenes i un control immediat de les xarxes provocarien que els tallats de subministrament no fossin molt llargs, sempre que es disposés d'un servei d'acció ràpid i eficient.

74. Dins d'aquest apartat és convenient disposar dels procediments necessaris relacionats amb la gestió i manteniment d'actius, i si és possible, de forma automatitzada:

    - ✓ Procediment d'inventari (Identificació/Catalogació/etc.)
    - ✓ Actius físics.

- ✓ Actius Digitals/Lògics

7.2.2. GESTIÓ DE LA FORMACIÓ, CONSCIENCIACIÓ I CAPACITACIÓ

75. La formació i conscienciació es solen enfocar mitjançant dues vies d'actuació principals:
    - ✓ La capacitació per al desenvolupament de les funcions.
    - ✓ La sensibilització per als llocs de treball i processos operatius existents.
76. En el primer cas s'inclouria el cronograma aplicable, tant internament com externament, referit als punts següents:
    - ✓ Avaluacions
    - ✓ Certificació
    - ✓ Auditoria
    - ✓ Simulació i exercicis
    - ✓ Formació periòdica
    - ✓ Capacitació.
77. En el segon dels casos comprenen tots aquells procediments de formació, conscienciació i capacitació (tant general com específica) associats als plans definits per a:
    - ✓ Empleats/Operaris
    - ✓ Vigilants de seguretat
    - ✓ Proveïdors, etc.

7.2.3. GESTIÓ DE LA CONTINUÏTAT

78. La continuïtat de l'activitat és un dels objectius generals de la seguretat. Per tant, és aconsellable abastar tots aquells procediments que vetllen per la supervivència i continuïtat de l'organització i els serveis prestats. Especialment, els plans i procediments de Contingències i Recuperació en funció dels escenaris derivats dels riscos.
    - ✓ Impossible accés a algun edifici d'un complex industrial.
    - ✓ Indisponibilitat dels sistemes d'informació que operen una infraestructura crítica
    - ✓ Etc.
79. Dins les necessitats de la gestió de la continuïtat podem indicar els següents conjunts de controls:
    - ✓ Pla Continuïtat del negoci
    - ✓ Pla de continuïtat i Pla de Contingència
    - ✓ Prova, manteniment i reavaluació dels plans de continuïtat
    - ✓ Proves periòdiques
    - ✓ Resguards
    - ✓ Inclusió de seguretat en el procés de gestió de continuïtat de negoci.

7.2.4. SUPERVISIÓ CONTINUA I MONITORATGE

80. L'objectiu del monitoratge i la supervisió contínua sol ser doble: per una banda, permetre la detecció d'anomalies de comportament i la seva correcció; i, per altra banda, servir com a base per a l'adquisició de la informació necessària que permeti el registre de l'activitat i la presa de decisions

81. Aquest conjunt de procediments solen abastar tots aquells processos operatius per al monitoratge i supervisió dels actius, els sistemes i les persones que els controlen. En especial, tots aquells que ens permetin recollir la informació necessària per a la mesura i millora de la gestió, els controls de seguretat i la minimització del risc dels actius afectats.

82. De forma general, solen controlar-se els següents grups d'actius:

- ✓ Actius Físics de la infraestructura
- ✓ Actius Lògics i/o de sistemes d'operació.

7.2.5. GESTIÓ DE LA SEGURETAT

83. S'identificaran tots aquells procediments de seguretat existents en els quals es reflectiran les activitats requerides davant de qualsevol esdeveniment de seguretat, els rols i responsabilitats de les persones encarregades de dur-los a terme, etc.

7.2.6. GESTIÓ D'ACCÉS

84. La gestió d'accés és sens dubte la primera línia de defensa per a la protecció dels actius i sol incloure tots aquells procediments operatius relacionats amb l'accés als sistemes i ubicacions de l'organització. Sol ser convenient estructurar els accessos conforme a les bones pràctiques de zonificació i segmentació de seguretat per establir parcel·les d'actuació que permetin una gestió més eficaç, eficient i controlable. En especial, s'haurien de considerar tots aquells procediments i mesures que ens permetin manejar de forma eficaç i eficient les identitats i els seus accessos, com per exemple:

- ✓ Accessos d'usuaris i persones (altes/baixes/modificacions), incloent-hi accessos temporals.
- ✓ Accés de vehicles, mercaderies, correspondència, suports tècnics, equipament, etc. (entrades/sortides).
- ✓ Control d'accessos temporals.
- ✓ Control d'entrades i sortides.
- ✓ Control de rondes.
- ✓ Identificació de seguretat (passes, targetes, etc.).
- ✓ Control de visites.
- ✓ Control de claus i combinacions.

7.2.7. GESTIÓ D'EVACUACIÓ I EMERGÈNCIA

85. És convenient prevenir i anticipar-se a fets que obliguin l'execució de procediments d'emergència, inclosos aquells en què sigui necessària l'evacuació de les instal·lacions. Fonamentalment en aquest apartat és útil establir procediments per a:

- ✓ Gestionar l'evacuació de les persones
- ✓ Gestionar la coordinació amb tercers
- ✓ La gestió i escalat de les emergències.
- ✓ Protecció extraordinària d'actius durant l'estat d'emergència.

7.2.8. GESTIÓ DE LA INFORMACIÓ

86. En la societat actual, la informació sol ser el principal actiu d'una organització, per la qual cosa és necessari aplicar normes i procediments per garantir que la incorporació de cada nova font d'informació desencadena el procés d'actualització i classificació d'aquesta, retirant, si és necessari, aquelles fonts d'informació i/o classificacions pertinents quan ja no són aplicables o necessàries.

87. Normalment, la classificació de la informació és quelcom inherent a l'organització segons aquelles característiques com confidencialitat, disponibilitat, integritat o traçabilitat conforme a la "necessitat de conèixer"; per la qual cosa és convenient parametritzar i establir els nivells necessaris d'ús.

88. Hi ha alguns criteris comunament utilitzats per a l'etiquetatge i classificació de la informació, en els quals com d'exemple podem esmentar:

- ✓ Els criteris marcats pel Traffic Light Protocol (TLP), creat per l'organisme CPNI del Regne Unit (Centre Nacional de Protecció d'Infraestructures del Regne Unit), i àmpliament estès en la seva implementació per part de grups de treball interdepartamentals.
- ✓ A més a més, l'INCIBE també reconeix els criteris de classificació basats Traffic Light Protocol (TLP). - https://www.incibe-cert.es/tlp
  - VERMELL - D'ús privat, per a destinataris concrets únicament. En el context d'una reunió, per exemple, la informació de nivell VERMELL es limita a aquells presents en aquesta. En la majoria de les circumstàncies la informació de nivell VERMELL es comunicarà verbalment o en persona.
  - GROC - Distribució limitada. Els destinataris poden compartir la informació de nivell GROC amb altres membres de l'organització, sota el criteri de "necessitat de conèixer".
  - VERD - D'àmbit comunitari. La informació manejada en aquesta categoria pot circular àmpliament dins d'una comunitat específica. Tanmateix, la informació no pot publicar-se a Internet, ni sortir fora de la comunitat.
  - BLANC - Informació d'ús no restringit. Sotmès a les regles del copyright que puguin aplicar, la informació de nivell BLANC es pot distribuir lliurement, sense restriccions.

- ✓ Criteris de classificació basats en classificació establerta per la normativa vigent d'aplicació per a determinats organismes de les administracions públiques, tot i que suavitzant potser alguns dels requisits per ajustar-los a l'entorn i circumstàncies concretes, llevat que siguin legalment exigibles. En últims casos és necessari recordar que pot ser exigible l'habilitació de seguretat oportuna per poder tenir accés a la informació. Com a exemple de nivells en aquesta classificació podem esmentar els següents:
  - Secret
  - Reservat
  - Confidencial
  - Difusió limitada
  - Sense classificar

89. En l'àmbit de la gestió de la informació, cal desenvolupar procediments de comunicació i intercanvi d'informació relatius a la protecció d'infraestructures crítiques (d'acord amb el protocol d'intercanvi d'informació i incidents PIC):
    - ✓ Amb l'Agència de Ciberseguretat Andorrana:
      - Sobre incidents o situacions que puguin posar en risc o comprometre la seguretat integral de la infraestructura.
      - Sobre variació de dades sobre l'organització i mesures de seguretat, dades de descripció de la infraestructura, etc.

7.2.9. GESTIÓ DE LA RESPOSTA DAVANT AMENACES I INCIDENTS

90. En general, convé articular una gestió de resposta a incidents graduada que permeti respondre eficaçment i proporcionalment als esdeveniments no desitjats que impactin en l'operativa normal de l'organització. Cal no oblidar considerar el subconjunt específic relatiu a incidents que puguin comprometre la mateixa seguretat dels sistemes i processos de seguretat.
91. Com a exemple, les subseccions següents indiquen els procediments mínims que haurien de ser considerats.

7.2.9.1. PROCEDIMENT PER A LA CATALOGACIÓ

92. Per poder desplegar i articular una resposta eficaç i proporcionada als riscos derivats d'un incident és necessari catalogar els mateixos segons els riscos detectats. És necessari considerar el subconjunt específic relatiu a incidents que puguin comprometre la mateixa seguretat dels sistemes i processos de seguretat. Com a mínim és aconsellable establir:
    - ✓ Nivells.
    - ✓ Criticitat.
    - ✓ Protecció de les evidències.
93. Pel que fa a l'elaboració de procediments dels nivells de seguretat tant permanents com excepcionals (temporals/provisionals), cal tenir en compte les circumstàncies especials d'origen operatiu o de risc (amenaces) imminent amb menció específica a situacions de no operativitat parcial (rellevant) o total dels sistemes de seguretat.

7.2.9.2. PROCEDIMENT PER A L'ESCALAT

94. Aquest conjunt de procediments permet definir la graduació, responsabilitats i necessitats d'informació i el flux de la mateixa que ha d'establir-se per a la presa de decisions i la gestió del coneixement. Com a mínim, és aconsellable establir mitjans per a:
    - ✓ Comunicació
    - ✓ Seguiment.

7.2.9.3. PROCEDIMENT PER A LA RESPOSTA

95. En aquest apartat és adequat tenir en compte les relacions amb tercers i la col·laboració als Plans de Suport Operatius (si s´escau), en els quals com a operador d'infraestructura crítica, s'ha de prestar suport a les administracions i organismes públics implicats. És convenient articular prèviament els escenaris de resposta de manera que ens permetin elaborar l'anàlisi, resolució, tancament i aprenentatge d'aquests, per al que hem de tenir almenys en compte els següents entorns d'operació:
    - ✓ Intern
    - ✓ Locals
    - ✓ Externs
    - ✓ Forces i Cossos de Seguretat del Principat

7.2.9.4. GESTIÓ DEL CONEIXEMENT

96. És necessari articular la retroalimentació de les experiències i situacions esdevingudes tant pròpies com alienes per a realitzar la incorporació de lliçons apreses de forma transversal a la gestió de la seguretat. La gestió del coneixement ens permet augmentar el grau de certesa de les ocurrències d'esdeveniments no desitjats i identificar millor la probabilitat de les amenaces alhora que ens prepara per a oferir una resposta més eficaç i proporcional als incidents.
97. Com a mínim, és aconsellable establir els següents procediments i mecanismes associats necessaris:
    - ✓ Recopilar el coneixement.
    - ✓ Processar i correlacionar el coneixement
    - ✓ Distribuir el coneixement.

7.3. DETALL DE MESURES DE PROTECCIÓ O TÈCNIQUES

7.3.1. PREVENCIÓ I DETECCIÓ

7.3.1.1. PROTECCIÓ MULTICAPA

98. És útil per a la defensa en general i davant la intrusió en particular aplicar un model de protecció d'acord amb el principi de "defensa en profunditat" en el qual

s'apliquen controls complementaris i superposats per a aconseguir un major grau de protecció.

99. S'haurien d'implementar les mesures necessàries de protecció, detecció i resposta davant les intrusions. Per això és convenient articular la compartimentació de zones de protecció conforme a les necessitats. Com a mínim és aconsellable considerar tres capes o zones de protecció, tant en el món físic com en el lògic.

Zona exterior o pre-perímetre

100. Vigilància i control de les zones més externes al sistema o ubicació per a detectar de forma proactiva possibles amenaces en les zones circumdants al mateix. És convenient tenir en compte els paràmetres ambientals i socials que poden augmentar els riscos i provocar incidents que indirectament afectin la seguretat (vagues, manifestacions, vessaments, incendis, etc. ...), complint sempre amb la legislació vigent en aquest sentit.

Perímetre

101. És recomanable controlar tot el perímetre de l'organització, considerant aquest tant des del punt de vista interior com exterior conforme a la segmentació en zones de gestió.

102. Al seu torn, dins d'aquesta zonificació s'haurien de considerar zones més generals d'aquelles altres més vitals i/o importants; monitorant i registrant la seva activitat convenientment per a anticipar circumstàncies de risc i anomalies.

Àrees protegides

103. Són les àrees en les quals l'accés ha d'estar restringit fins i tot per a usuaris interns segons la necessitat d'accedir-hi. Serien àrees en les quals, per la seva sensibilitat, poques o molt poques persones haurien de tenir accés.

7.3.1.2. CONTROL D'ACCÉS

104. És elemental establir controls i mesures de seguretat adequats per a la identificació, la restricció d'accés, l'assegurament i monitoratge de l'entorn de sistemes i ubicacions sota protecció. El control d'accés ha de fonamentar-se en la "necessitat de conèixer" i pot aplicar-se de forma física i lògica als sistemes i ubicacions objecte de protecció.

105. Alguns exemples de mesures de control d'accés aplicables podrien ser les següents:

- ✓ Com a exemples de mesures i elements de seguretat física i electrònica, podem indicar tanques, zones de seguretat, càmeres de vigilància / CCTV, portes i encluses, panys, lectors de matrícules, arcs de seguretat, torns, etc.
- ✓ Com a exemples de mesures i elements de seguretat lògica relacionats amb els sistemes d'informació, podem indicar firewalls, DMZs; IPSs, segmentació i aïllament de xarxes, xifrat, VPNs, elements i mesures de control d'accés d'usuaris (tokens, controls biomètrics, etc.), mesures d'instal·lació i configuració segura d'elements tècnics, eines de correlació d'esdeveniments i registres, etc.
- ✓ Altres mesures específiques d'acord amb els riscos més particulars o concrets existents.

Identificació i autenticació

106. És necessari un sistema eficaç d'identificació del personal, que faciliti la categorització i diferenciació dels usuaris, la circulació i l'accés i impedeixi accés no autoritzats. Per això, s'han d'implementar mitjans tècnics i organitzatius que permetin la identificació de persones, objectes i components.

107. Com a exemple de mesures aplicables, podem destacar les targetes d'accés, les targetes d'identificació, la biometria, la detecció de metalls, els escàners corporals, els inventaris, etc.

108. Des del punt de vista de l'eficiència, sol ser convenient que els usuaris siguin identificats i autenticats només una vegada, podent accedir a partir d'allà, a totes les aplicacions i dades a les quals el seu perfil els permeti, tant en sistemes locals com en sistemes als quals hagin d'accedir de forma remota.

Protecció d'àrees o zones

109. L'estructuració de les zones interiors i exteriors de seguretat ha de realitzar-se coherentment per aconseguir l'assegurament, vigilància i monitoratge de les mateixes en funció dels riscos sense oblidar aquelles zones internes vitals el compromís de les quals pot produir un impacte altament advers en les persones, els processos de negoci i els actius / recursos de l'organització.

110. Normalment, la creació d'una divisió zonal d'aquells actius de major mida, abast o complexitat afavoreix la gestió eficaç de les mesures i mecanismes implantats per a la seva protecció.

111. Com a exemples de caràcter general, solen tenir-se en compte els següents elements.

- ✓ Control d'accés tant físics com lògics
- ✓ Àrees d'accés públic, lliurament i càrrega
- ✓ Assegurar oficines, sales i instal·lacions
- ✓ Control i contenció de la intrusió
- ✓ Paraments horitzontals i verticals:
  - Murs, sòls, sostres
  - Portes, encluses, i portes d'emergència
  - Conductes
  - Finestres
- ✓ Etc.

Control de treball en zones segures

112. Un dels elements més importants a controlar són les zones segures, fonamentalment aquelles destinades al control i supervisió de la seguretat.

113. Com a exemples de caràcter general solen tenir-se en compte els següents elements:

- ✓ Control ambiental de l'entorn de la instal·lació: Il·luminació de seguretat, operadors, etc.
- ✓ Vigilant de seguretat o recepcionista.
- ✓ Control d'accés automatitzat.
- ✓ Control de vehicles i mercaderies.
- ✓ Circuit tancat de televisió (CCTV).
- ✓ Protecció contra incendis.
- ✓ Contenidors de seguretat, caixes fortes, fitxers de claus, armaris blindats, etc.

- ✓ Sistemes i elements de suport.

7.3.2. VIGILÀNCIA I MONITORATGE

7.3.2.1. MONITORATGE I ALARMA

114. Un component important de la seguretat es basa en el coneixement i és, per tant aconsellable establir totes aquelles mesures requerides que condueixen a la recopilació d'informació, la seva correlació i la detecció de desviacions del que es considera normalitat.
115. Per això és convenient tenir en compte alguns elements apropiats com:
    - ✓ Centres de control d'alarmes, centres de control d'operacions, centre de recepció i visualització d'imatges.
    - ✓ Equips de vigilància (torns, rondes, dotació, etc.).
    - ✓ Megafonia i ràdio.
    - ✓ Sistemes de detecció i alarma d'incendis.
    - ✓ Sistemes de revisió d'incidències i incidents.
    - ✓ Altres.

7.3.2.2. SEGURETAT DEL MANTENIMENT I ACTIUS DE SEGURETAT

116. La seguretat del manteniment consisteix a prestar especial atenció a tots els sistemes i ubicacions i, si escau, entorns no directament relacionats amb els actius a protegir; però que per la seva naturalesa estan imbricats en l'estructura de l'organització i/o són processos bàsics de manteniment de l'estat operatiu de l'organització.
117. Per exemple, s'haurien d'assegurar les zones i elements de manteniment com ara quadres de llums, claus, caixes fortes, elements antiincendis, dispositius d'alarma i seguretat, material i substàncies perilloses, generadors, etc. que encara que no estan directament relacionats amb els actius identificats del negoci; però que el seu compromís pot ser indici o causa d'un incident de seguretat.
118. Com a exemple d'aquests elements podríem considerar els següents:
    - ✓ Subsistemes de Seguretat Electrònica
    - ✓ Centralització i Control d'Alarmes
    - ✓ Manteniment del sistema de seguretat
    - ✓ Manteniment de la infraestructura
    - ✓ Manteniment de sistemes digitals crítics i comunicacions
    - ✓ Cablejat, línies d'alimentació, etc.
    - ✓ Sistema de comunicacions de seguretat física
    - ✓ Enllaços amb els centres de control, llocs de vigilància mòbils o fixos
    - ✓ Sistema d'alimentació elèctrica, cablejat, manteniment d'equips i reparacions.

7.3.2.3. AUDITORIA I RESPONSABILITAT

119. La gestió de la seguretat i la seva implantació (és a dir, els objectius de control, els controls, les polítiques, els processos i els procediments de seguretat) haurien de sotmetre's a una revisió independent a intervals planificats o sempre que es produeixin canvis significatius en la implantació de la seguretat. Després d'això, és aconsellable adoptar les accions correctives que corresponguin per mitigar els riscos detectats, sempre sota el marc de responsabilitat de l'organització que permeti corregir i donar compliment a les insuficiències detectades en aquestes.

120. És una bona pràctica aconsellable establir els controls d'auditories necessaris per determinar el grau de compliment enfront a les polítiques i regulacions establertes, així com l'eficàcia i eficiència dels controls de seguretat implantats; al mateix temps que es consciencia al personal sobre la responsabilitat dels processos dels quals formen part.

121. De forma general, el conjunt d'auditories a planificar sol ser de dues tipologies: de compliment i tècniques. Les primeres es realitzen enfront les regulacions i normatives aplicables i la segona enfront dels requisits documentats i comportament esperat dels sistemes auditats.

122. Com a exemples de conjunts d'auditoria podem destacar:

- ✓ Compliment de normativa i legislació aplicable
- ✓ Eficàcia de les mesures tècniques aplicades
- ✓ Compliment dels plans d'acció acordats

Gestió de registres

123. La gestió de coneixement i l'auditoria no és possible si no es registren evidències dels fets succeïts; per la qual cosa és necessari establir una política de registres d'evidències d'acord amb les necessitats tant de compliment com de coneixement lligat a l'eficàcia i eficiència dels processos de seguretat.

124. Entre els elements a controlar sol ser útil comptar amb:

- ✓ Gestió de registres en general
- ✓ Registre d'incidències de seguretat
- ✓ Registres d'avisos i alertes
- ✓ Registres o logs d'auditoria
- ✓ Protecció de logs
- ✓ Revisió d'ús de sistemes
- ✓ Logs d'administradors i operadors
- ✓ Logs de fallada del sistema
- ✓ Etc.

Anàlisi forense

125. Es centra principalment a conèixer què ha succeït després d'un incident estudiant els esdeveniments iniciadors que poden donar lloc a l'activació de determinades mesures o actuacions de seguretat. Davant qualsevol incident haurien d'aplicar-se les tècniques metodològiques preestablertes adequades per a reconstruir els fets, descobrir les relacions entre ells i comprendre per què han succeït amb l'objectiu d'assimilar la lliçó apresa. Per exemple, el mètode arbre de causes persegueix

evidenciar les relacions entre els fets que han contribuït en la producció d'un incident.

126. De forma general en qualsevol anàlisi forense d'uns fets s'haurien de contemplar els següents punts:
- ✓ Identificació i caracterització dels fets
- ✓ Preservació de l'evidència
- ✓ Anàlisi i correlació d'esdeveniments per reconstruir la seqüència de fets
- ✓ Informe, lliçons apreses i accions si són necessàries.

7.3.2.4. MÈTRIQUES

127. Indicació de metodologia de mesurament del rendiment de la Seguretat: quin tipus d'objectius es mesuren, què forma de mesurar-los i quins procediments es disposen per al seu estudi i posteriors propostes de millora.

7.3.3. COORDINACIÓ I RESPOSTA

128. Enfront d'un incident de seguretat, és necessària una resposta efectiva que permeti llançar accions correctores en temps i forma per contenir o minimitzar els danys que puguin produir-se. La gestió adequada de la resposta i la informació relativa als incidents de seguretat és essencial per complir amb els paràmetres normatius i reguladors que sistematitzen les evidències necessàries per al seu estudi posterior.

129. Com a exemple d'elements a tenir en compte en l'articulació de la coordinació i resposta, podríem considerar els següents:
- ✓ Gestió d'incidents.
- ✓ Mesura temporal i gradual.
- ✓ Resposta davant d'incidents i mitigació d'atacs.
- ✓ Coordinació interna.
- ✓ Comunicacions externes: criteris i models de comunicació interna en cas d'incident comunicable.
- ✓ Administracions i ministeris.
- ✓ Serveis d'alertes de proveïdors.
- ✓ Agència de Ciberseguretat Andorrana
- ✓ Etc.

7.3.3.1. INTERRELACIÓ

130. En aquest punt s'haurien de tenir en compte les interfícies, tant si són proveïdors com consumidors de les entrades i sortides dels processos i/o serveis objecte de protecció. És necessari entendre a què s'apliquen, el seu nivell de criticitat i/o els riscos que suposen per als actius protegits. Un punt clau és comptar amb documentació adequada i veritable de l'intercanvi mínim necessari que es comparteix o es requereix entre els participants.

131. Entre els punts a tenir en compte en aquest apartat podríem destacar les necessitats tècniques i organitzatives relatives als següents elements:

- ✓ Entorn ambiental.
- ✓ Entorn funcional.
- ✓ Serveis dels quals depèn.
- ✓ Serveis que depenen.
- ✓ Etc.

7.3.4. CONTINUÏTAT I CONTINGÈNCIA

132. La continuïtat d'una organització depèn directament de complir eficaçment i eficientment amb la missió que s'ha imposat i la caracteritza; per això, normalment els serveis identificats com a essencials constitueixen el punt central de la seva activitat. És necessari donar continuïtat als mateixos malgrat les circumstàncies i, quan aquestes són adverses, s'haurien de prestar en condicions mínimes acceptables i tornar a la normalitat tan aviat com sigui possible. Per tant, és convenient definir els controls necessaris que, amb una perspectiva d'abast adequada als serveis afectats, permetin organitzar els processos de continuïtat i contingència aplicables segons la granularitat necessària.

133. Per aconseguir un conjunt mínim de condicions acceptables de continuïtat, sol ser útil comptar amb un conjunt d'elements mínims per a desenvolupar el servei, com ara els següents:

- ✓ La informació i les dades necessàries:
  - Suport de les dades.
  - Suport de les informacions.
  - Suport de les dependències externes i internes.
  - Suport del coneixement.
- ✓ La infraestructura i les persones
  - Entorns alternatius.
  - Elements de suport i suport tècnic.
  - Persones entrenades i motivades.
  - Capacitats alternatives del personal.
- ✓ Els plans i procediments per donar una resposta en temps
  - Pla de contingència i continuïtat.
  - Prova, manteniment i reavaluació dels plans.
  - Difusió i formació dels plans.
  - Plans de Recuperació i reconstrucció.