RIC-STIC-001
Guia Implementació Infraestructures Crítiques

(DOCUMENT SUBJECTE A MODIFICACIONS)

Desembre 2022

Fitxa del document

Títol	Guia Implementació Infraestructures Essencials

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	20/12/22	20/12/22

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 418/2022, de 19 d´octubre, pel qual es regula el Reglament d´Infraestructures Crítiques d´Andorra en l'àmbit de les entitats que presten serveis "essencials" (RIC-AD, en endavant), al qual es refereix l'article 4-2-a de la Llei 22/2022, de 9 de juny.

En definitiva, la sèrie de documents RIC-STIC s'elaboren (adaptats del CCN-CERT) per donar compliment a les comeses de l´Agència Nacional de Ciberseguretat d´Andorra i al reflectit RIC-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
Secretari d´Estat de Transició Digital i Projectes Estratègics

ÍNDEX

INTRODUCCIÓ

1. Aquesta guia estableix unes pautes de caràcter general que són aplicables a entitats de diferent naturalesa, dimensió i sensibilitat sense entrar en casuístiques particulars. S'espera que cada organització les particularitzi per a adaptar-les al seu entorn singular.
2. Amb el present document es pretén orientar a aquelles infraestructures designades com a essencials en l'elaboració del seu de pla de protecció específic.
3. En aquesta guia s'inclouen una sèrie de mesures organitzatives o gestió, operacionals o procedimentals, protecció o tècniques, que podran ser referents d'ajuda als operadors crítics per a la confecció d'algun dels punts dels continguts mínims del seu pla de protecció específic.

1. ASPECTES ORGANITZATIUS

1.1 ORGANIGRAMA DE SEGURETAT

4. L'operador crític ha de presentar gràficament l'estructura organitzativa funcional que en matèria de seguretat integral existeix en la Infraestructura Essencial o "crítica" (d'ara endavant: IE), amb indicació de tots els actors que participen en aquella, el seu rol de responsabilitat i la seva jerarquia en el procés de presa de decisions.

1.2 DELEGAT DE SEGURETAT DE LA INFORMACIÓ

5. L'operador aportarà la informació sol·licitada en aquest apartat conforme al que s'estableix en el document de continguts mínims del RIC-AD, sent recomanable també d´informar dels mecanismes de contingència i continuïtat adoptats per garantir la comunicació amb el Delegat de Seguretat de la Informació (DSI) en cas d'incidents o que aquesta persona es vegi afectada per qualsevol tipus de succés advers que no li permetin estar accessible, així com els canals de coordinació existents amb els diferents actors afectats.
6. Quant 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).

1.3 MECANISMES DE COORDINACIÓ

7. Per a aclarir els mecanismes de coordinació establerts en relació a la Infraestructura Essencial conforme al que s'estableix al RIC-AD, 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 Infraestructures essencials, tant dins com fora de la pròpia infraestructura.

8. A continuació, s'hauria de recollir per a cadascun d'ells, tant el mecanisme de comunicació principal com el secundari per a casos de contingències (canals que haurien de ser provats periòdicament).
9. 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 / rols, així com els procediments d'actuació prevists davant les diferents situacions crítiques o extraordinàries amb l'objectiu de minimitzar l'impacte d'aquestes eventualitats.
10. Finalment, seria convenient desenvolupar plans de comunicació per a mantenir informats de les novetats a cadascun dels nivells de responsabilitat i funcionalitat entre els diferents actors.

1.4 MECANISMES I RESPONSABLES D'APROVACIÓ

11. Igual que per a altres tipus de polítiques i procediments s'hauria de recollir el procediment que s'utilitza per a l'aprovació i revisió interna del mateix Pla, 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 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 anàlisis realitzades, actualitzacions de les anàlisis de riscos, etc.).

2. DESCRIPCIÓ DE LA INFRAESTRUCTURA ESSENCIAL

2.1 DADES GENERALS

12. L'Operador Essencial, a mode d'introducció de la Infraestructura Essencial hauria d'incloure almenys la informació de context suficient per a descriure els següents aspectes:

- Informació de caràcter estratègic.
  - Descripció del servei essencial que suporta i àmbit geogràfic d´actuació 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 Essencial.
- Localització física i estructura de la infraestructura a protegir.
  - Ubicació geogràfica de la infraestructura.
  - Plans 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.

2.2 ACTIUS / ELEMENTS

13. S'hauria de realitzar una descripció de tots els actius que suporten la Infraestructura Essencial, diferenciant aquells que són vitals dels quals no ho són i detallant les dependències existents entre ells. La informació que es podria incloure almenys seria l'enumerada a continuació:

- Mitjans materials i recursos necessaris per a la prestació del servei essencial.
  - Components de la Infraestructura Essencial.
  - Ubicació dels centres de processament de dades (CPD) que gestionen els diferents elements que conformen la Infraestructura Essencial.
  - Sistemes informàtics (maquinari i programari) utilitzats.
    - Relació de sistemes (HW/SW).

        - Versions.
        - Xarxes de comunicacions que s'utilitzen per a aquesta IE. Tipus.
    - Les xarxes de comunicacions: que permeten intercanviar dades i que s'utilitzin per a aquesta IE.:
        - Arquitectura de xarxa, rangs d'IP públiques i, dominis.
        - Esquema(es) de xarxa complet i detallat, de tipus gràfic i amb descripció literària, on es recullin els fluxos d'intercanvi d'informació que es realitzen en les xarxes, així com els seus perímetres electrònics.
        - Descripció de components de la xarxa (servidors, terminals, hubs, switchos, nodes, enrutadors,firewalls,...) així com la seva ubicació física.
- Mitjans personals per a la prestació del servei essencial.
    - Tipologia.
    - Volum.
- Relació de la IE amb els serveis essencials prestats per l'operador.
- Proveïdors crítics que en general són necessaris per al funcionament d'aquesta IE, i específicament:
    - De subministrament elèctric.
    - De comunicacions (telefonia, internet, etc.…).
    - De tractament i emmagatzematge d'informació (CPDs, etc.).
    - De ciberseguretat (CERTs privats, SOCs, etc.).
- Usuaris finals dels serveis prestats per la IE (particulars, empreses, Sector públic...).
- Sobre els proveïdors nomenats per l'operador, s'especificaran els diferents Acords de Nivell de Serveis que es tenen contractats i que són considerats essencials.

2.3 INTERDEPENDENCIES

14. El que es busca amb aquesta mesura de seguretat és tenir una visió global, íntegra i integradora de com és el sistema d'informació, com es gestiona i com es defensa. Aquesta mesura és bàsicament documental i descriptiva. S'hauria de realitzar una descripció i el motiu que origina les possibles interdependències entre serveis essencials i infraestructures essencials 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 essencials del propi operador.
    - Amb altres infraestructures estratègiques del propi operador que suporten el servei essencial.

- 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, com ara: proveïdor(s) de telecomunicacions, Centres de Processament de dades, serveis de seguretat i qualssevol altres que es consideri, especificant per a cadascun d'ells el nom del proveïdor, els serveis contractats, acords de nivell de servei (ANS) i compliment del servei proveït 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.
- Entre d'altres.

3. RESULTATS DE L'ANÀLISIS DE RISC

3.1 AMENACES CONSIDERADES

15. Per a l'anàlisi de riscos a realitzar es podrien prendre com a punt de partida diferents tipologies d'amenaces que estan definides en diferents catàlegs existents o referents a nivell nacional o internacional.

16. En aquest sentit, s'han d'analitzar les principals amenaces de tipus físic com a la ciberseguretat que poguessin tenir un origen intencionat per part de terceres parts diferents als propis operadors i que poguessin afectar els actius.

3.2 MESURES DE SEGURETAT INTEGRAL EXISTENTS

17. S'entén per mesures de seguretat integral, les mesures de protecció dels actius. Aquestes mesures podran ser, permanents, temporals i graduals.

18. 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 essencials de les quals ells depenen. La llista d'exemples proporcionada no és exhaustiva, però pot servir de punt de partida per a organitzar les necessitats de protecció de l'entorn concret de protecció per al qual siguin aplicables.

19. L'Operador haurà de descriure les mesures de seguretat integral actualment implantades en línia amb l'anàlisi de riscos realitzat. 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.

20. En general les mesures a implementar, o implementades, hauran d´estar alineades amb la Legislació vigent aplicable, tant pel que fa a la documentació exigible, com a la instal·lació i manteniment.

3.2.1 MESURES ORGANITZATIVES O DE GESTIÓ

21. Totes les organitzacions tenen una funció, missió o negoci, que determina els seus objectius (què cal aconseguir) i estratègies (com cal aconseguir-ho). És per això que la seguretat integral d'una organització hauria d'alinear-se per a garantir la consecució d'aquests.

22. Les mesures organitzatives són el conjunt de mesures de seguretat integrades en els processos i estructures organitzatives existents en l'organització i l'objectiu principal de la qual és gestionar la complexitat dels processos de gestió de la seguretat i donar resposta als riscos, condicionants normatius i reguladors de l'entorn.

23. Es poden establir les següents mesures organitzatives o de gestió:

    - 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 Conscienciació
        - Protecció del personal.

3.2.2 MESURES OPERACIONALS O PROCEDIMETALS

24. Derivat del cos normatiu establert en l'organització, les bones pràctiques recomanen la documentació del conjunt indispensable de procediments operacionals o procedimentals amb el seu abast 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.

25. Els procediments d'alt nivell que engloben la tipologia de controls que són aconsellables concordes amb les bones pràctiques de seguretat:

    - 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 (còpia de seguretat)
    - Supervisió contínua i monitoratge
    - Gestió d'accessos
    - 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.

3.2.3 MESURES DE PROTECCIÓ O TÉCNIQUES

26. Les mesures de protecció o tècniques fan referència a aquells conjunts de controls de caràcter tècnic necessàriament implantats en l'organització per a 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.

27. A continuació, de forma no exhaustiva, es proporciona un conjunt d'exemples d'alt nivell de controls i mesures agrupades conforme al que considerem criteris pràctics: facilitat de lectura, catalogació i naturalesa de les mesures. Aquestes agrupacions de controls tenen per objecte el 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 treu 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 manera general per a, conforme a les necessitats, aplicar mesures més concretes derivades o relacionades amb aquestes. Per exemple, si s'indica de manera 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 vídeo vigilància; addicionalment per a la protecció del perímetre lògic seria necessària la segmentació de la xarxa, la creació d'una DMZ, l'aplicació de regles del tallafocs i de sistemes de detecció d'intrusions, etc.

28. Per a 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.

3.3 VALORACIÓ DE RISCOS

29. 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 a poder procedir a aquesta estimació s'haurà de tenir en consideració el grau d'implantació de cadascuna d'aquestes mesures de seguretat, és a dir, caldria avaluar si:

    - Estan correctament implantades
    - Estan operatives
    - Estan sota procediments
    - Estan sota un sistema de gestió i millora contínua
    - Són objecte de proves regulars per a 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.

30. Per a determinar el càlcul final dels riscos als quals es troba exposada la infraestructura s'haurien de prendre 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.

31. S'han de diferenciar en aquesta anàlisi els diferents escenaris de la IE, així com, en el seu cas, els diferents horaris del seu funcionament (instal·lació ocupada o no, etc.).

32. En qualsevol cas, donat l'enfocament de protecció dels serveis essencials que es persegueix, haurà de prestar-se 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.

33. Amb l'objectiu de mostrar la informació de la valoració 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	Amenaces	Risc intrínsec			Controls existents	Risc residual		
		Probabilitat	Impacte	Risc		Probabilitat	Impacte	Risc

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

Actius	Amenaces	Risc intrínsec		Controls existents	Risc residual	
		Probabilitat	Risc		Probabilitat	Risc

34. La interpretació de la informació recollida en les taules prèvies és la següent:

- **Actiu.** Element / component de la Infraestructura Essencial.
- **Amenaça.** Succés que pot afectar el funcionament o a la disponibilitat de l'actiu i, per tant, del servei essencial.
- **Risc intrínsec.** Anàlisi realitzada 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 lligat al 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 realitzada 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.

4. PLA D'ACCIÓ PROPOSAT

35. 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 Essencial com a necessàries per a complementar les existents en l'actualitat, de manera que puguin establir-se unes fites i dates per a la seva implementació.

36. 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 a afrontar els riscos detectats.

37. El Pla d'Acció 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 previ.

38. El Pla d'Acció s'hauria de recollir els següents requisits:

    - Prioritzar les accions, sobre la base del nivell de risc associat, ateses les possibles dependències existents entre elles.
    - Estructurar les diferents mesures de seguretat, associant-les sobre la base de la seva finalitat i naturalesa, en accions que resultin delimitades 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.

39. 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 Essencial.

40. Sobre la base del nivell de prioritat assignat a una determinada mesura de seguretat, l'Operador Crític podria prioritzar la implantació de les mesures en forma d'accions.

4.1 ACCIONS

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

42. 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 esperat 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 IE necessàries per a la prestació del servei essencial. (Codi: INS).
        - Sistemes informàtics, ja siguin maquinari o programari. (Codi: SI).
        - Xarxes de comunicacions que s'utilitzin en aquesta IE. (Codi: XAR).
        - Persones que exploten o operen amb els actius anteriorment citats. (Codi: PER).
        - Proveïdors crítics que són necessaris per al funcionament de la IE. (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 prèvies, 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.

IDENTIFICADOR DE L'ACCIÓ		
CÓDI ÚNIC NOM DESCRIPTIU		
OBJECTIU		
ESPECIFICACIÓ DE LA FINALITAT DE L'ACCIÓ		
DESCRIPCIÓ		
DESCRIPCIÓ DE L'ACCIÓ		
RESPONSABLE		
RESPONSABLE DE L'ACCIÓ		
DEPENDENCIES AMB ALTRES ACCIONS		
ACCIONS AMB LA QUE AQUESTA GUARDA RELACIÓ		
Identificador	Actius Responsables	Tipologia
Identificador de l'Actiu 1 (Codi i Nom Descriptiu)	Responsable de l'Actiu 1	INS / SI / XAR / PER / PRO
Identificador de l'Actiu 2	Responsable de l'Actiu 2	INS / SI / XAR / PER / PRO
Identificador	Mesura de Seguretat Responsable	Tipologia i Caràcter
Mesura de Seguretat 1	Responsable de la Mesura de Seguretat 1	Organitzativa / Operacional / Técnica / Permanent / Gradual
Mesura de Seguretat 2	Responsable de la Mesura de Seguretat 2	Organitzativa / Operacional / Técnica / Permanent / Gradual
MECANISMES DE COORDINACIÓ I SEGUIMENT		
MECANISMES PER L'ACCIÓ		
INVERSIÓ	ESTIMACIÓ TEMPORAL	
ESTIMACIÓ DEL COST DE L'ACCIÓ	TEMPS PREVIST	

Taula.1: Exemple de fitxa de l'acció.

4.2 MESURES DE SEGURETAT

43. La consecució d'una acció va lligada a l'aplicació ordenada d'una o múltiples mesures de seguretat que poden interrelacionar-se. Les mesures de seguretat poden segmentar-se en tasques atòmiques que condueixen a la consecució de la mesura de seguretat.

44. Per a la definició apropiada 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 al càrrec de l'execució de la mesura de seguretat.
- **Identificació de l'Acció:** Mostra l'acció en la qual s'engloba 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 IE necessàries per a la prestació del servei essencial. (Codi: INS).
    - Sistemes informàtics, ja siguin maquinari o programari. (Codi: SI).
    - Xarxes de comunicacions que s'utilitzin en aquesta IE. (Codi: XAR).
    - Persones que exploten o operen amb els actius anteriorment citats. (Codi: PER).
    - Proveïdors crítics que són necessaris per al funcionament de la IE. (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.

IDENTIFICADOR DE LA MESURA DE SEGURETAT		
CÓDI ÚNIC NOM DESCRIPTIU		
DESCRIPCIÓ		
DESCRIPCIÓ DE LA MESURA DE SEGURETAT		
RESPONSABLE		
RESPONSABLE DE LA NESURA DE SEGURETAT		
ACCIÓ		
IDENTIFICADOR DE L'ACCIÓ QUE ENGLOBA AQUESTA MESURA DE SEGURETAT		
CRITICITAT	CARÀCTER	TIPOLOGIA
NIVELL DE CRITICITAT	PERMANENT TEMPORAL / GRADUAL	ORGANITZATIVA O DE GESTIÓ / OPERACIONAL O PRODECIMENTAL / DE PROTECCIÓ O TÉCNICA
Identificador	Actiu Responsable	Tipologia
Identificador de l'Actiu 1 (Codi i Nom Descriptiu)	Responsable de l'Actiu 1	INS / SI / XAR / PER / PRO
Identificador de l'Actiu 2	Responsable de l'Actiu 2	INS / SI / XAR / PER / PRO
TASQUES		
Tasca 1: Descripció de la tasca 1 Tasca 2: Descripció de la tasca 2		

Taula.2: Exemple de Mesura de Seguretat.

5. DETALL MESURES DE SEGURETAT

5.1 MESURES ORGANITZATIVES O DE GESTIÓ

5.1.1 COS DEFINIT NORMATIU

45. És aconsellable establir els processos de seguretat perquè donin cabuda al compliment normatiu, voluntari i regulador que afecta l'organització i els seus actius. Per això és convenient Identificar controls de seguretat derivats de la normativa identificada en el RIC-AD i les normatives o reglamentacions aplicables al RIC-AD.

46. 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 Autoprotecció i Prevenció de Riscos Laborals
    - Seguretat Lògica i de la informació.

47. Per a això és necessari organitzar de manera manejable, proporcionada i documentada tota la informació sobre els controls i mesures de seguretat implementades o que haurien de ser-ho conforme al tractament de riscos.

48. A alt nivell aquesta organització sol incloure:

    - Polítiques i estàndards de Seguretat
    - Criteris de Seguretat
    - Procediments
    - Compliment 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.

5.1.2 ORGANITZACIÓ DE LA SEGURETAT

49. L'organització de seguretat estableix de manera 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.

50. Una de les tasques principals d'organitzar la seguretat consisteix a gestionar el factor humà, embevent en els processos de seguretat tot el referent a la gestió de les persones i les tasques directament realitzades per aquestes.

51. Com a exemple, entre els controls a tenir en compte, podem contemplar-los 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.

52. **Comitè de Seguretat i Crisis:**

53. Com 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 de prioritzar i responsabilitzar les accions necessàries per a la protecció i continuïtat dels serveis i l'organització.

54. La millor manera de progressar és col·laborar. És convenient, la creació de grups de treball en el qual es permeti una col·laboració activa per part de les persones encaminades a eliminar les febleses del sistema o establir protocols comuns d'actuació enfront de situacions de crisis.

55. **Establir Rols:**

56. 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 adequadament segregades.

57. És important tenir en compte el següents punts a l'hora d'assignar responsabilitats:

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

58. **Gestió de Canvis:**

59. 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 mínim mitjançant procediments formals (documentats) de control de canvis que contempli almenys:

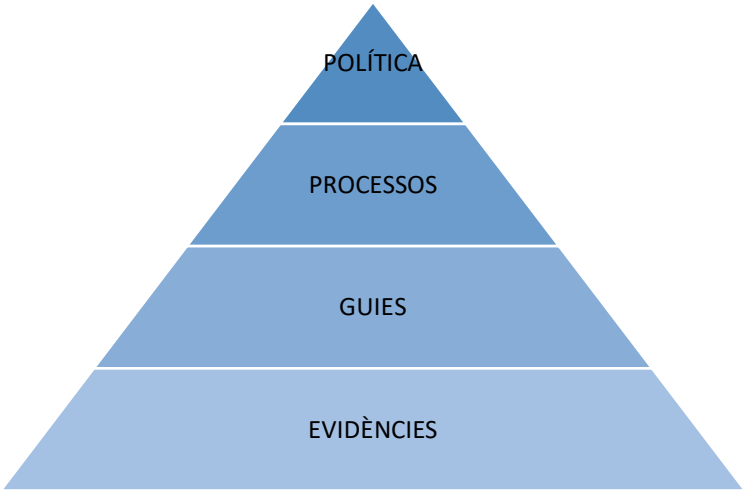
- Avaluació de riscos
- Anàlisi dels efectes dels canvis
- Especificació dels controls de seguretat necessaris.

60. 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.

61. **Gestió de la qualitat i Documentació:**

62. 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.

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



64. Una bona gestió documental i de registres de la informació relativa a la seguretat facilita el control i les activitats de monitoratge i auditoria.

5.1.3 MITJANS HUMANS I SEGURETAT DEL PERSONAL

65. **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 a l'acompliment de la seva funció
- La sensibilització i coneixement de les polítiques i procediments establerts.

67. **Protecció del Personal:**

68. 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 la funció de les quals dins de l'organització pugui suposar un alt risc en cas de compromís de la seva seguretat.

5.2 MESURES OPERACIONALS O PROCEDIMENTALS

5.2.1 PROCEDIMENTS DE GESTIÓ I MANTENIMENT D'ACTIUS CRÍTICS

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

70. D'acord amb aquest model el punt de partida és la identificació dels actius que volem protegir per la qual cosa és convenient comptar amb l'inventari dels elements integrants. A l'hora de classificar els actius sol ser necessari establir una sèrie de paràmetres per a 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.

71. 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.

72. En 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 enfront de 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 talls 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 comptar amb els procediments necessaris relacionats congestió i manteniment d'actius, i de ser possible de manera automatitzada:

    - Procediment d'inventariat (Identificació/Catalogació/Etc.)
    - Actius físics
    - Actius Digitals/ Lògics
    - Procediment de gestió continua d'actius físics i lògics (Alta/Baixa/Modificació).
    - Etc.

5.2.2 GESTIÓ DE LA FORMACIÓ, CONCIENCIACIÓ I CAPACITACIÓ

75. La formació i conscienciació se sol enfocar mitjançant dues vies d'actuació principals:

    - La capacitació per a l'acompliment 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 interna com externament, referit als següents punts:

    - Avaluacions
    - Certificació
    - Auditoria
    - Simulació i Exercicis
    - Formació periòdica
    - Capacitació.

77. En el segon dels casos comprendrien tots aquells procediments de formació, conscienciació i capacitació (tant general com específica) associats als plans definits per a:

    - Emprats/Operaris
    - Vigilants de seguretat
    - Proveïdors
    - Etc.

5.2.3 GESTIÓ DE LA CONTINUÏTAT

78. La continuïtat de l'activitat és un dels objectius generals de la seguretat.

79. 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.

    - Impossibilitat d'accés a algun edifici d'un complex industrial.
    - Indisponiblitat dels sistemes d'informació que operen una infraestructura crítica
    - Etc.

80. Dins de 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
    - Suports
    - Inclusió de seguretat en el procés de gestió de continuïtat de negoci.

5.2.4 SUPERVISIÓ CONTINUA I MONITORITZACIÓ

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

82. Aquest conjunt de procediment solen abastar tots aquells processos operatius per al monitoratge i supervisió dels actius, els sistemes i les persones que els controlen. Especialment 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.

83. De manera general se solen controlar els següents grups d'actius:

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

5.2.5 GESTIÓ DE LA SEGURETAT

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

5.2.6 GESTIÓ D'ACCESSOS

85. La gestió d'accessos és sens dubte la primera línia de defensa per a la protecció dels actius i sol englobar 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 a establir parcel·les d'actuació que permetre una gestió més eficaç, eficient i controlable. Especialment haurien de considerar-se tots aquells procediments i mesures que ens permetin manejar de manera eficaç i eficient les identitats i els seus accessos com per exemple:

- Accessos de 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 (passis, targetes, etc.)
- Control de visites
- Control de claus i combinacions.

5.2.7 GESTIÓ D'EVACUACIÓ I EMERGENCIA

86. És convenient prevenir i anticipar-se a fets que obliguin l'execució de procediments d'emergència, inclosos aquells en els quals 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.

5.2.8 GESTIÓ DE LA INFORMACIÓ

87. 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 a garantir que la incorporació de cada nova font d'informació desencadena el procés d'actualització i classificació d'aquesta, retirant, de ser necessari, aquelles fonts d'informació i/o classificacions pertinents quan ja no són aplicables o necessàries.

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

89. Existeixen alguns criteris comunament utilitzats per al marcatge i classificació de la informació, en els quals a tall d'exemple podem esmentar:

    - Els criteris marcats pel *Traffic Light Protocol* (TLP), creat per l'òrgan CPNI del Regne Unit (Centre Nacional de Protecció d'Infraestructures del Regne Unit), i àmpliament estès en la seva implementació per part grups de treball interdepartamentals.
        - **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.
        - **TARONJA** – Distribució limitada. Els destinataris poden compartir la informació de nivell TARONJA 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 extensament dins d'una comunitat específica. No obstant això, la informació no pot publicar-se en Internet, ni sortir fora de la comunitat.
        - **BLANC** – Informació d'ús no restringit. Subjecte a les regles del copyright que puguin aplicar, la informació de nivell BLANC pot distribuir-se lliurement, sense restriccions.

- Criteri de classificació basats en classificació establerta per la normativa vigent d'aplicació per a determinats organismes de les Administracions Públiques, això sí; suavitzant potser alguns dels requeriments per a ajustar-los a l'entorn i circumstàncies concretes, tret que siguin legalment exigibles. En últims casos és necessari recordar pot ser exigible l'habilitació de seguretat oportuna per a 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

90. En l'àmbit de la gestió de la informació, s'hauran de desenvolupar procediments de comunicació i intercanvi d'informació relatius a la protecció d'IE

- Amb l'ANC-AD:
  - 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.

5.2.9 GESTIÓ DE LA RESPOSTA DEVANT AMENACES I INCIDENTS

91. En general, convé articular una gestió de resposta a incidents graduada que permeti respondre eficaç 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 pròpia seguretat dels sistemes i processos de seguretat.

92. A tall d'exemple les sub-seccions següents indiquen els procediments mínims que haurien de considerar-se.

93. **Procediment per la Catalogació:**

94. Per a poder desplegar i articular una resposta eficaç i proporcionada als riscos derivats d'un incident és necessari catalogar els mateixos d'acord amb els riscos detectats. És necessari considerar el subconjunt específic relatiu a incidents que puguin comprometre la pròpia seguretat dels sistemes i processos de seguretat. Com mínim és aconsellable establir:

- Nivells
- Criticitat
- Protecció de les evidències.

95. Referent a l'elaboració de procediments dels nivells de seguretat tant permanents com excepcionals (temporals/provisionals) ha de tenir-se en compte les circumstàncies especials d'origen operatiu o de risc (amenaça) imminent amb

esment específic a situacions de no operativitat parcial (rellevant) o total dels sistemes de seguretat.

96. **Procediment per l'Escalat:**

97. 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 mínim és aconsellable establir mitjans per a:

- Comunicació
- Seguiment.

98. **Procediment per la Resposta:**

99. En aquest apartat és adequat tenir en compte les relacions amb tercers i la col·laboració als Plans de Suport Operatius, en els quals com a operador d'infraestructura crítica, s'ha de donar suport a les Administracions i organismes públics implicats. És convenient articular prèviament els escenaris de resposta de manera que ens permetin realitzar 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

5.2.10GESTIÓ DEL CONEIXEMENT

100. És necessari articular la retroalimentació de les experiències i situacions esdevingudes tant pròpies com alienes per a realitzar la incorporació de lliçons apreses de manera transversal a la gestió de la seguretat. La gestió del coneixement ens permet augmentar el grau de certitud de les ocurrències d'esdeveniments no desitjats i identificar millor la probabilitat de les amenaces al mateix temps que ens prepara per a oferir una resposta més eficaç i proporcional als incidents.

101. Com mínim és aconsellable establir els següents procediments i mecanismes associats necessaris:

- Recopilar el coneixement
- Processar i correlacionar el coneixement
- Distribuir el coneixement.

5.3 MESURES DE PROTECCIÓ O TÉCNIQUES

5.3.1 PREVENCIÓ I DETECCIÓ

102. **Protecció Multicapa:**

103. 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. 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. Almenys és aconsellable considerar tres capes o zones de protecció, tant en el món físic com en el lògic.

104. Zona exterior o avant-perímetre:

105. Vigilància i Control de les zones més externes al sistema o ubicació per a detectar de manera proactiva possibles amenaces en les zones circumdants a aquest. 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, abocaments, incendis, etc.....), complint sempre amb la legislació vigent en aquest sentit.

106. Perímetre:

107. 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. Al seu torn, dins d'aquesta zona haurien de considerar-se 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.

108. Àrees protegides:

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

110. **Control d'Accés:**

111. És elemental establir controls i mesures de seguretat adequats per a la identificació, la restricció de l'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 manera física i lògica als sistemes i ubicacions objecte de protecció.

- Com a exemples de mesures i elements de seguretat física i electrònica podem indicar tanques, zones de seguretat, càmeres de vídeo vigilància / CCTV, portes i excloses, panys, lectors de matrícules, arcs de seguretat, torns, etc.
- Com exemples de mesures i elements de seguretat lògica relatius als sistemes d'informació podem indicar firewalls, DMZs; IPSs, segmentació i aïllament de xarxes, xifratge, 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 logs, etc.

- Altres mesures específiques concordes amb els riscos més particulars o concrets existents.

112. Identificació i autenticació:

113. És necessari un sistema eficaç d'identificació del personal, que faciliti la categorització i diferenciació dels usuaris, la circulació i l'accés i impedir accessos no autoritzats. Per això s'han d'implementar mitjans tècnics i organitzatius que permetin la identificació de persones, objectes i components. Com a exemple de mesures aplicables podem destacar, les targetes d'accés, targetes d'identificació, biometria, detecció de metalls, escàners corporals, inventaris, etc. Des del punt de vista de l'eficiència, sol ser convenient que els usuaris siguin identificats i autenticats solament una vegada, podent accedir a partir d'allí, a totes les aplicacions i dades als quals el seu perfil els permeti, tant en sistemes locals com en sistemes als quals hagi d'accedir en forma remota

114. Protecció d'àrees o zones:

115. L'estructuració de les zones interiors i exteriors de seguretat ha de realitzar-se coherentment per a 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. Normalment la creació d'una divisió zonal d'aquells actius de major grandària, abast o complexitat afavoreix la gestió eficaç de les mesures i mecanisme implantat per a la seva protecció. Com exemples de caràcter general solen tenir-se en compte els següents elements:

- Control d'accessos tant físics com lògics
- Àrees d'accés públic, lliurament i càrrega
- Assegurar oficines, quarts i instal·lacions
- Control i contenció de la intrusió
- Paraments Horitzontals i Verticals:
  - Murs, sòls, sostres
  - Portes, excloses, i portes d'emergència
  - Conductes
  - Finestres
- Etc.

116. Control de treball en zones segures:

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

118. Com 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.

5.3.2 VIGILANCIA I MONITORITZACIÓ

119. **Monitorització i Alarma:**

120. 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 recol·lecció d'informació, la seva correlació i la detecció de desviacions del que es considera normalitat.

121. Per a això és convenient tenir en compte els alguns elements apropiats com:

- Centres de control d'alarmes, centres de control d'operacions, centre de recepció i visionat 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.

122. **Seguretat del Manteniment i actius de seguretat:**

123. La seguretat del manteniment consisteix a prestar especial atenció a tots els sistemes i ubicacions i, en el seu cas, 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.

124. Per exemple, s'haurien d'assegurar les zones i elements de manteniment com a quadres de llums, claus, caixes fortes, elements anti-incendis, 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. 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, posats de vigilància mòbils o fixos
- Sistema d'alimentació elèctrica, cablejat, manteniment d'equips i reparacions

125. **Auditoria i Responsabilitat:**

126. 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'aquesta, és aconsellable adoptar les accions correctives que corresponguin per a així mitigar els riscos detectats, sempre sota el sota el marc de responsabilitat de l'organització que permeti corregir i donar compliment a les insuficiències detectades en aquestes.

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

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

129. 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.

130. Gestió de registres:

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

132. 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.

133. Anàlisi forense:

134. Es centra principalment a conèixer que ha succeït després d'un incident estudiant els successos 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 perquè han succeït a fi 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.

135. De manera 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 a reconstruir la seqüència de fets
- Informe, lliçons apreses i accions de ser necessàries.

136. **Mètriques:**

137. Indicació de metodologia de mesurament de l'acompliment de la Seguretat: quin tipus d'objectius es mesuren, quina manera de mesurar-los i quins procediments es disposen per al seu estudi i posterior propostes de millora.

5.3.3 COORDINACIÓ I RESPOSTA

138. Davant l'ocurrència d'un incident de seguretat és necessària una reposada efectiva que permeti llançar accions correctores dins del termini i en la forma escaient per a contenir o minimitzar els danys que poguessin produir-se.

139. La gestió adequada de la resposta i la informació relativa als incidents de seguretat és essencial per a complir amb els paràmetres normatius i reguladors que sistematitzen les evidències necessàries per al seu estudi posterior.

140. Com a exemple d'elements a tenir en compte en l'articulació de la coordinació i reposada podríem considerar els següents:

- Gestió d'incidents
- Mesura temporal i gradual
- Reposada davant incidents i mitigació d'atacs
- Coordinació Internes
- Comunicacions externes: Criteris i Models de comunicació interna en cas d'incident comunicable
- Administracions i Ministeris
- Serveis de Alertes de Proveïdors
- Etc.

141. **Interrelació:**

142. En aquest punt s'haurien de tenir en compte les interfícies bé siguin subministradors o consumidors de les entrades i sortides dels processos i/o serveis objecte de protecció necessari entendre al fet que apliquen i el seu nivell de criticitat i/o els riscos que suposen per als actius protegits. Un punt clau és comptar amb

documentació adequada i veraç de l'intercanvi mínim necessari que es comparteix o requereix entre els participants.

143. 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.

5.3.4 CONTINUÏTAT I CONTINGÈNCIA

144. La continuïtat d'una organització depèn directament de complir eficaç 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 quan 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.

145. Per a aconseguir un conjunt mínim de condicions acceptables de continuïtat sol ser útil comptar amb conjunt d'elements mínims per a exercir el servei com per exemple els següents:

- La informació i 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
  - Persones entrenades i motivades
  - Capacitats alternatives del personal.
- Els plans i procediments per a donar una resposta en temps:
  - Pla de contingència i continuïtat
  - Prova, manteniment i reavaluació dels plans
  - Divulgació i formació dels plans
  - Plans de Recuperació i reconstrucció.

ANNEX A. GLOSSARI

DMZ

És una subxarxa d'àrea local situada entre la xarxa privada d'una organització i la xarxa externa.

Hardware

El maquinari (en anglès hardware) d'un ordinador és el conjunt de les seves parts físiques.

Hub

Equip de comunicacions que permet connectar entre si diversos equips en disposició o topologia d'estrella.

Adreça IP

Una adreça IP és un número que identifica inequívocament un dispositiu lògic connectat a la xarxa. Dins d'una mateixa xarxa, cada adreça IP que s'utilitzi ha de ser única.

Software

És el conjunt dels programes informàtics (en anglès software), procediments i documentació que fan alguna tasca en un ordinador.

Switch

Aparell de xarxes que permet agrupar un conjunt d'ordinadors i fer que passin pel mateix cable**.**

VPN

És una tecnologia de xarxa que permet una extensió de la xarxa local sobre una xarxa pública o no controlada, com per exemple Internet.