RIC-STIC-001_S
Guia Simplificada Implementació Infraestructures Crítiques

(DOCUMENT SUBJECTE A MODIFICACIONS)

Gener 2023

Fitxa del document

Títol	Guia Simplificada Implementació Infraestructures Crítiques

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	25/1/23	26/1/23

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document: ANC-AD

PRÒLEG

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

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

El Decret 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
Ministre de Finances i portaveu del Govern

ÍNDEX

1. INTRODUCCIÓ

1. Aquesta guia simplificada, 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.

2. ASPECTES ORGANITZATIUS

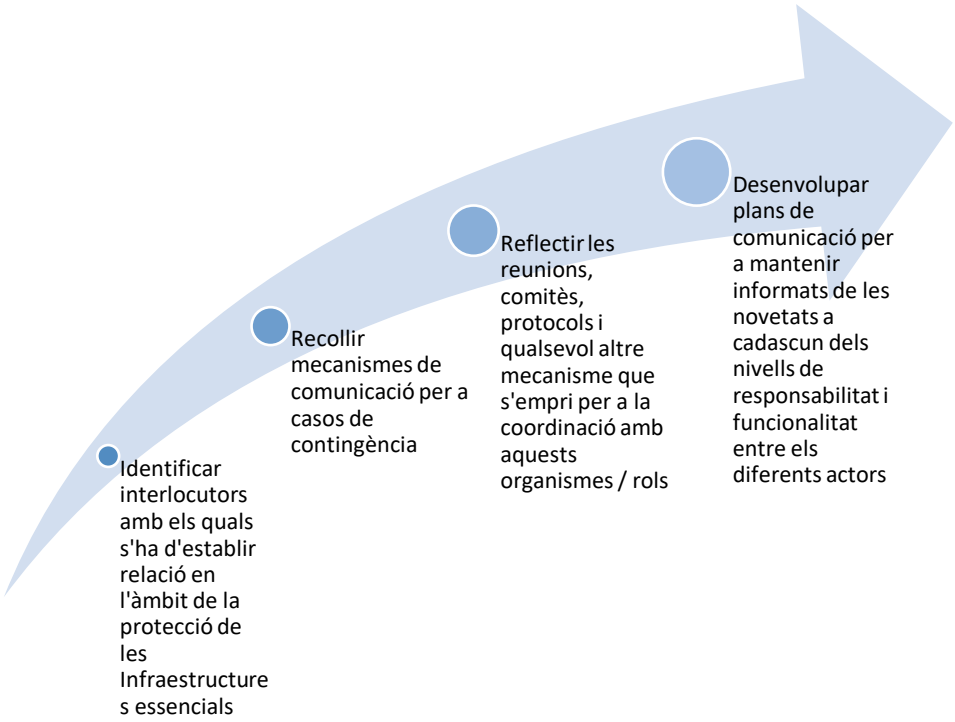
2.1 ORGANIGRAMA DE SEGURETAT

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.

2.2 DELEGAT DE SEGURETAT DE LA INFORMACIÓ

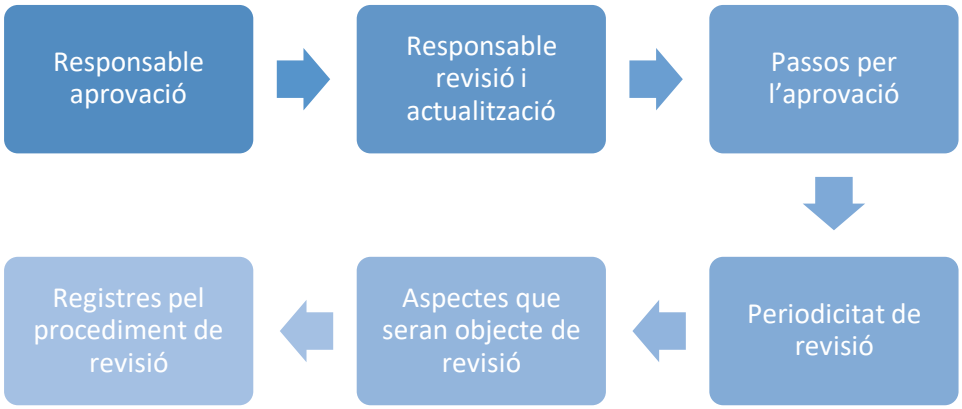
5. L'operador aportarà la informació sol·licitada en aquest apartat conforme al que s'estableix en el document de continguts mínims del RIC-AD, sent recomanable també d´informar dels mecanismes de contingència i continuïtat adoptats per garantir la comunicació amb el Delegat de Seguretat de la Informació (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).

2.3 MECANISMES DE COORDINACIÓ



2.4 MECANISMES I RESPONSABLES D'APROVACIÓ

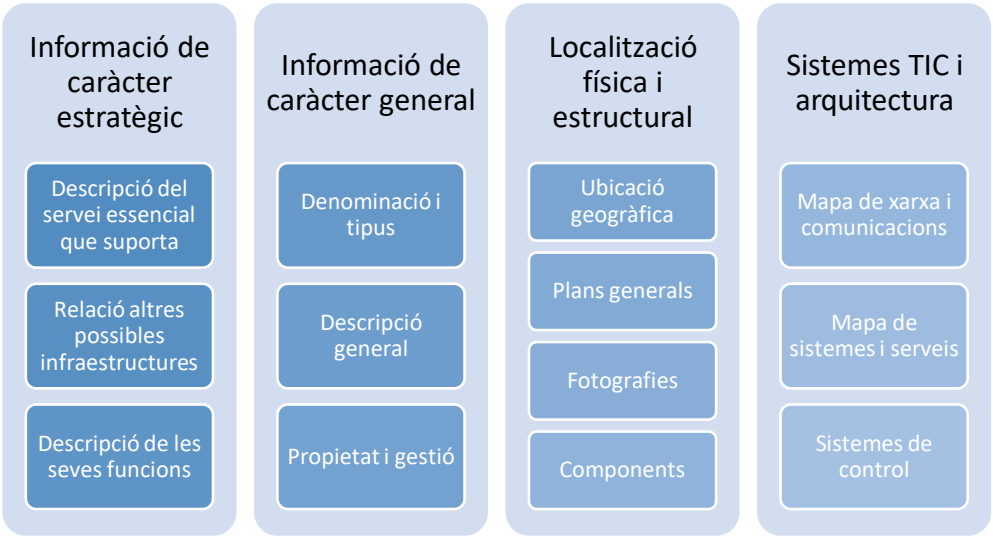
Igual que per a altres tipus de polítiques i procediments s'hauria de recollir el procediment que s'utilitza per a l'aprovació i revisió interna del mateix Pla, és a dir:



3. DESCRIPCIÓ DE LA INFRAESTRUCTURA ESSENCIAL

3.1 DADES GENERALS

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



3.2 ACTIUS / ELEMENTS

8. 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:

Mitjans materials i recursos

- Components
- Ubicació dels centres de processament de dades
- Sistemes informàtics
- Les xarxes de comunicacions

Mitjans personals per a la prestació del servei

- Tipologia
- Volum

Relació de la IE amb els serveis essencials

Proveïdors crítics

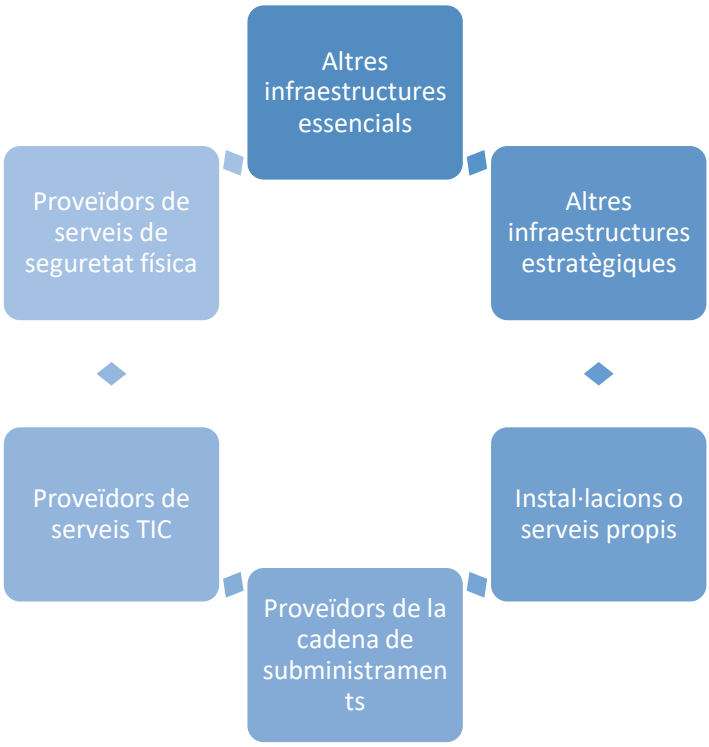
- De subministrament elèctric
- De comunicacions
- De tractament i emmagatzematge d'informació
- De ciberseguretat

Usuaris finals

Proveïdors

3.3 INTERDEPENDENCIES

9. Alguns exemples d'interdependències serien:



4. RESULTATS DE L'ANÀLISIS DE RISC

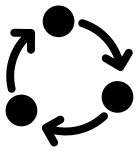
4.1 AMENACES CONSIDERADES

10. 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.

11. 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.

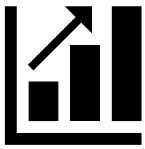
4.2 MESURES DE SEGURETAT INTEGRAL EXISTENTS

12. S'entén per mesures de seguretat integral, les mesures de protecció dels actius. Aquestes mesures podran ser:



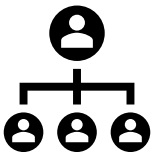
Permanents

Temporals



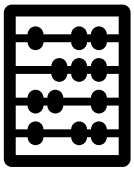
Graduals

13. Es recomana seguir una organització de les mesures en tres nivells:



Organitzatives

Protecció



Operacionals

4.2.1 ORGANITZATIVES O DE GESTIÓ

14. 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.

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

- Definició d'un cos normatiu
- Organització de la seguretat
  - Comité de Seguretat i Crisis
  - 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

4.2.2 OPERACIONALS O PROCEDIMETALS

16. Els procediments aconsellables concordes amb les bones pràctiques de seguretat són:

- Procediments per a la realització, gestió i manteniment d'actius
- Gestió de la formació, conscienciació i capacitació.
- Gestió de la continuïtat
- 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

4.2.3 DE PROTECCIÓ O TÉCNIQUES

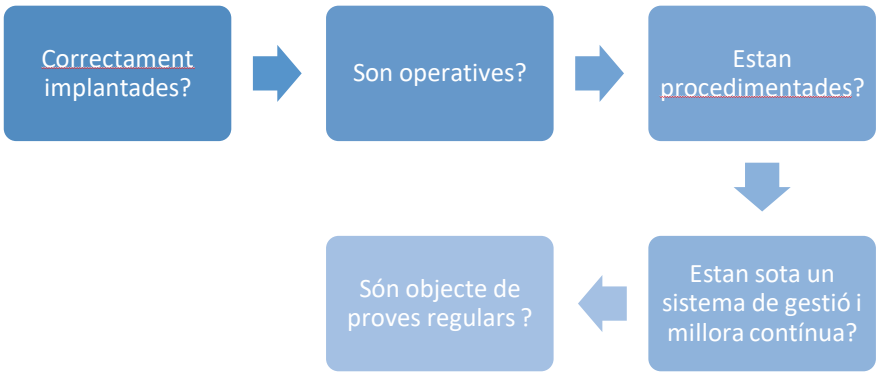
17. Les mesures de protecció o tècniques fan referència a aquells conjunts de controls de caràcter tècnic necessàriament implantats en l'organització per a aconseguir un nivell de risc acceptable.

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

Prevenció | Vigilància | Coordinació | Continuïtat

4.3 VALORACIÓ DE RISCOS

19. 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,:



20. 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

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

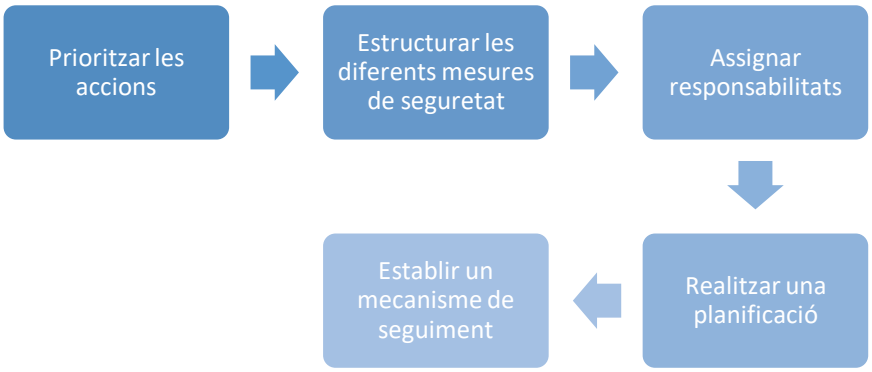
- **Actiu.** Element / component de la Infraestructura Essencial.
- **Amenaça.** Succés que pot afectar el funcionament o a la disponibilitat de l'actiu i, per tant, del servei essencial.
- **Risc intrínsec.** Anàlisi realitzada amb caràcter previ a l'aplicació de mesures de seguretat.
- **Probabilitat.** 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.

5. PLA D'ACCIÓ PROPOSAT

22. 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.

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



5.1 ACCIONS

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.

5.2 MESURES DE SEGURETAT

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.