Esquema Nacional de Seguretat del Principat d'Andorra Simplificat (ENS-AD)

(DOCUMENT SUBJECTE A MODIFICACIONS)

Gener 2023

1. Consideracions generals

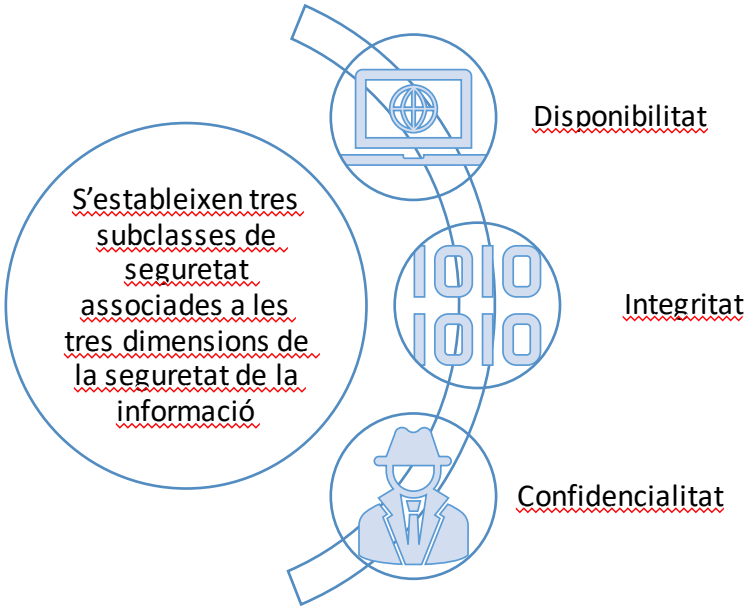
L'àmbit d'aplicació de l'ENS-AD s'estén a la totalitat dels actius d'informació que resulten necessaris per garantir la prestació dels serveis essencials o importants amb la qualitat que cadascú requereix.

Aquest decret regula l'establiment d'un sistema de gestió de seguretat de la informació i els requisits de seguretat mínims que s'han d'aplicar a les xarxes i als sistemes d'informació.

2. Principis, classes, catàleg i SGSI

La seguretat de la informació tractada i dels serveis prestats conforme a l'ENS-AD se sustentarà en els següents principis bàsics:

Seguretat entesa com a procés integral i sistemàtic	Gestió de la seguretat	Modelat dels actius d'informació bàsics	Estratificació de la defensa	Vigilància contínua per a detectar activitats o comportaments anòmals	Diferenciació de responsabilitats



Disponibilitat

D3

Quan la disponibilitat pot ser inferior al 90% i les interrupcions poden durar més de 24 hores

D2

Quan no resulta acceptable una disponibilitat inferior al 90%, ni una interrupció que duri més de 24 hores

D1

Quan no resulta acceptable una disponibilitat inferior al 99% del temps anual, ni una interrupció que duri més de 4 hores

D0

Quan no resulta acceptable una disponibilitat inferior al 99,9% del temps anual, ni una interrupció que duri més d'1 hora

Integritat

I3

Quan la font d'informació, i el fet que s'alteri o destrueixi la informació no són importants

I2

Quan la font de la informació, o el fet de la seva alteració o destrucció ha de ser identificable, i no és necessari comprovar periòdicament la precisió, integritat i actualitat de la informació

I1

Quan la font de la informació, o el fet de la seva alteració o destrucció ha de ser identificable i és necessari fer comprovacions periòdiques de la precisió, integritat i actualitat de la informació

I0

Quan la font de la informació, o el fet de la seva alteració o destrucció ha de tenir valor probatori, o quan es requereix una verificació en temps real de la precisió, integritat i actualitat de la informació

Confidencialitat

C3

Quan l'accés a la informació no està limitat (és a dir, totes les persones interessades tenen accés de lectura, el permís per canviar es determina en funció del requisit d'integritat)

C2

Quan s'ha de concedir l'accés a la informació si la persona que sol·licita l'accés té un interès legítim

C1

Quan la informació només la poden utilitzar determinats grups d'usuaris; l'accés a la informació s'ha de concedir si la persona que sol·licita l'accés té un interès legítim

C0

Quan la informació només la poden utilitzar determinats usuaris; l'accés a la informació s'ha de concedir si la persona que sol·licita l'accés té un interès legítim

Nivells

S'estableixen quatre nivells de seguretat per a cada subclasse, segons sigui el nivell d'impacte en la informació o el servei que podria causar un ciberincident:

N3
Baix

Impacte molt reduït en el servei, casi inapreciable

N2
Mig

Impacte que permet garantir la prestació del servei, però amb menys qualitat que la requerida

N1
Important

Impacte que degrada la prestació del servei fins al punt que aquest no es pot garantir

N0
Crític

Impacte que impedeix la prestació del servei

Nivells de seguretat

El nivell de seguretat d'un actiu d'informació o servei pot ser baix (B), mitjà (M) o alt (A), i es determina en funció del nivell de protecció que cada una de les seves subclasses:

		D3	D2	D1	D0
I3	C3	B	B	M	A
	C2	B	B	M	A
	C1	M	M	M	A
	C0	A	A	A	A
I2	C3	B	B	M	A
	C2	B	B	M	A
	C1	M	M	M	A
	C0	A	A	A	A
I1	C3	M	M	M	A
	C2	M	M	M	A
	C1	M	M	M	A
	C0	A	A	A	A
I0	C3	A	A	A	A
	C2	A	A	A	A
	C1	A	A	A	A
	C0	A	A	A	A

Catàleg d'actius d'informació estàndard

L'ANC-AD analitzarà els riscos i especificarà cadascú dels actius d'informació que resultin necessaris per a modelar els serveis als quals aplica. Inclourà:

Les amenaces a les quals estan exposats	Les mesures de seguretat que li donarien cadscú dels tres nivells de seguretat

Sistema de Gestió de la Seguretat de la Informació

L'òrgan de direcció de l'entitat té la responsabilitat d'iniciar, gestionar i controlar un Sistema de Gestió de la Seguretat de la Informació (SGSI). I haurà:

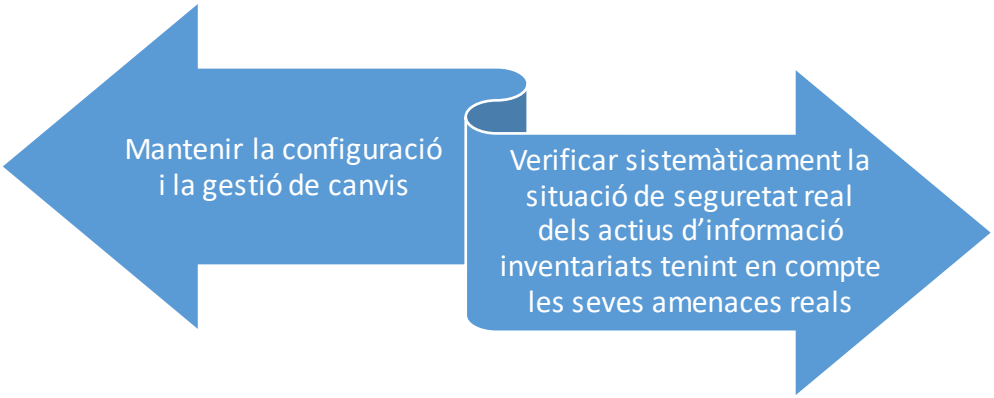
De determinar els lineaments que regularan el marc organitzacional i operacional	Organitzar l'elaboració del pla d'acció i revisar-lo almenys una vegada a l'any

3. Elements del SGSI

Cada servei dins l'àmbit de la implantació de l'ENS-AD haurà de modelar-se mitjançant l'**Inventari d'Actius**. On el Delegat de la Seguretat de la Informació (DSI) és responsable de:			
Dur a terme l'inventari d'actius d'informació bàsics la seguretat	Coordinar per a cada actiu, l'assignació de la seva classe de seguretat per part dels seus propietaris	Afegir la informació que permet a l'entitat complir amb els principis bàsics de l'ENS-AD	Determinar el nivell de seguretat requerit

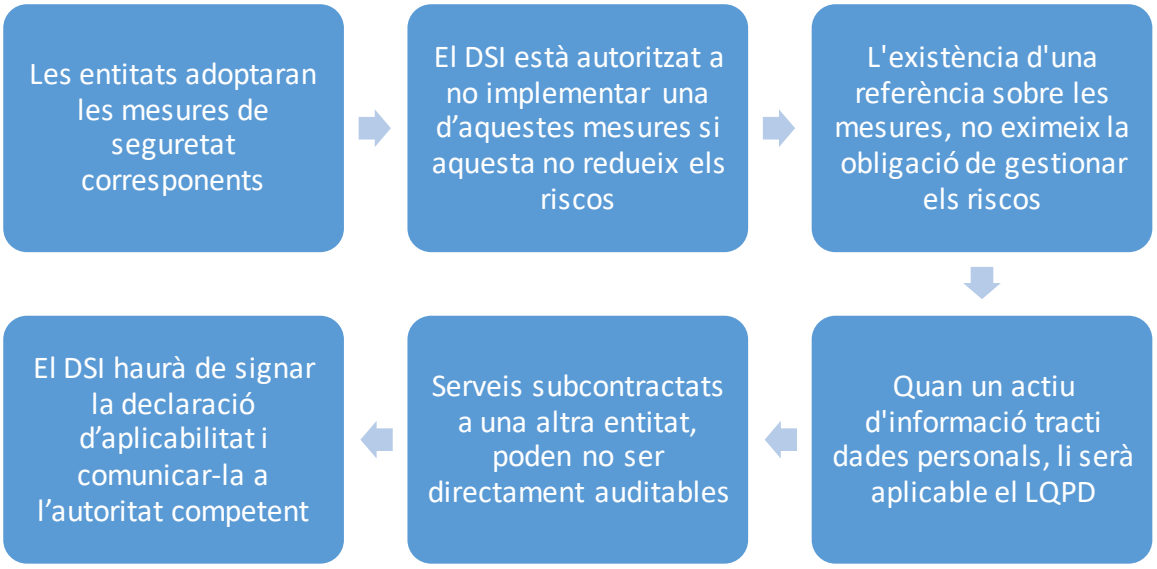
L'**Inventari d'Actius** contindrà per a cada actiu:		
Identificació de l'actiu d'informació bàsic	Serveis en la prestació dels quals participa	Classe i nivell de seguretat

EL DSI és responsable de:

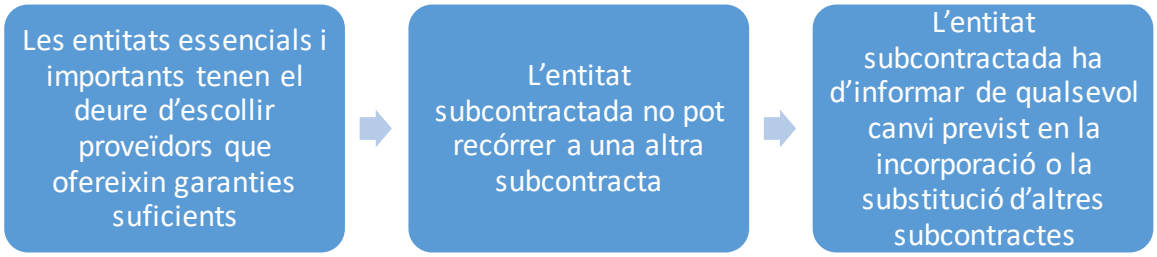


4. Requisits mínims

Per a l'entitat responsable dels serveis



Per a les entitats subcontractades



El servei que l'entitat subcontractada presta, s'ha de regir per un contracte escrit que estableix, com a mínim:

- El nivell de seguretat i l'acord del nivell que ha de garantir
- Les penalitzacions associades als incompliments
- Les restriccions en la ubicació física
- Garantir que les persones autoritzades per a tractar la informació, administrar, mantenir o operar el servei s'han compromès a respectar la confidencialitat
- Prendre totes les mesures necessàries en matèria de seguretat de la informació
- Respectar les condicions establertes
- Assistir l'entitat que presta el servei
- Les condicions per al rescat del servei que presta l'entitat subcontractada
- Posar a disposició tota la informació necessària per a demostrar que compleix les obligacions
- L'obligació d'informar immediatament si considera que no compleix amb el nivell de seguretat exigit

5. Auditoria de seguretat

Els actius d'informació necessaris per a la prestació dels serveis als que aplica l'ENS-AD seran objecte d'una auditoria interna ordinària anual.

Amb caràcter extraordinari, haurà de realitzar-se aquesta auditoria sempre que es produeixin modificacions substancials en els serveis als que aplica l'ENS-AD.

L'auditoria es realitzarà d'acord amb la guia d'auditoria de l'ENS-AD publicada per l'ANC-AD, i amb els nivells de seguretat que l'entitat hagi assignat als serveis.

L'informe d'auditoria servirà a l'òrgan de direcció de l'entitat per identificar les mesures que l'entitat necessita adoptar per a corregir la possible falta d'adequació.

Els informes d'auditoria podran ser requerits per les autoritats competents.