

Declaració d'aplicabilitat a l'ENS-AD



(DOCUMENT SUBJECTE A MODIFICACIONS)

Maig 2023

Fitxa del document

Títol	Declaració d'aplicabilitat a l'ENS
--------------	------------------------------------

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	23/5/23	MAIG 2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document: ANC-AD
--

PRÒLEG

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

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

El Decret 417/2022, de 19 d'octubre, pel qual es regula l'Esquema Nacional de Seguretat d'Andorra en l'àmbit de les entitats que presten serveis " importants " (ENS-AD, en endavant), al qual es refereix l'article 4-2-a de la Llei 22/2022, de 9 de juny , estableix la política de seguretat en la utilització de mitjans electrònics que permeti una protecció adequada de la informació.

En definitiva, la sèrie de documents ENS-STIC s'elaboren (adaptats del CCN-CERT) per donar compliment a les comeses de l'Agència Nacional de Ciberseguretat d'Andorra i al reflectit en l' Esquema Nacional de Seguretat d'Andorra, conscients de la importància que té l' establiment d' un marc de referència en aquesta matèria que serveixi de suport perquè el personal de les entitats afectades, i en ocasions, ingrata tasca de proporcionar seguretat als sistemes de les TIC sota la seva responsabilitat.

Marc Rossell

Secretari d'Estat de Transformació Digital i Telecomunicacions

ÍNDEX

1. INTRODUCCIÓ	5
2. PROCEDIMENT PER DEFINIR LA DECLARACIÓ DE APLICABILITAT	6
2.1. CATEGORITZACIÓ	6
2.1.1. DETERMINACIÓ DE LA CATEGORIA	7
2.2. DETERMINACIÓ DE LES MESURES D'APLICACIÓ	7
3. RECOMANACIONS.....	8
3.1. RESPECTE AL FORMAT DE LA DECLARACIÓ D'APLICABILITAT	8
3.2. DECÀLEG DE RECOMANACIONS GENERALS	8

1. INTRODUCCIÓ

1. La Declaració d'Aplicabilitat, en l'àmbit de l'ENS-AD, és el document en el qual es formalitza la relació de mesures de seguretat que resulten d'aplicació al sistema d'informació de què es tracti.
2. Com es determina a l'ENS-AD, les mesures de seguretat referenciades a l'Annex A de la guia ENS-STIC-804 podran ser reemplaçades per altres mesures compensatòries sempre que es justifiqui documentalment que protegeixen igual o millor el risc sobre els actius i es satisfan els principis bàsics i els requisits mínims previstos.
3. Com a part integral de la Declaració d'Aplicabilitat, s'indicarà de forma detallada la correspondència entre les mesures compensatòries implementades i les mesures de l'Annex A que compensen, igual que s'especificaran les mesures complementàries de vigència que s'hagin pogut precisar, sent objecte d'aprovació formal per part del responsable de seguretat.
4. El document formalitzat de Declaració d'Aplicabilitat serà essencial per a l'elaboració del pla d'adequació i la posterior implementació de les mesures contemplades, i podrà ser analitzat per l'entitat certificadora i emprat com a document de suport durant el procés d'auditoria per a la validació del compliment de l'ENS-AD. Per a aquest fi, és important que la Declaració d'Aplicabilitat indiqui per a cadascuna de les mesures de seguretat que contempla l'ENS-AD, no només si s'aplica o no s'aplica al sistema d'informació o a l'organització, sinó, de forma molt resumida, com s'aplica i/o la documentació on es detalla i, si escau, per què no s'aplica.

2. PROCEDIMENT PER DEFINIR LA DECLARACIÓ DE APLICABILITAT

5. Per aconseguir l'adequació d'un sistema d'informació al que disposa l'ENS-AD i poder determinar quines mesures són d'aplicació, és necessari procedir a la seva categorització i seguir les indicacions especificades a l'Annex A de la guia ENS-STIC-804.
6. El procés de categorització té com a objecte assignar la categoria BÀSICA als sistemes d'informació. La categoria d'un sistema d'informació, en matèria de seguretat, busca l'equilibri entre la importància de la informació que maneja, els serveis que presta i l'esforç de seguretat requerit, i els riscos als quals està exposat, sota el criteri del principi de proporcionalitat.
7. Dit en altres paraules, les mesures de seguretat que s'aplicaran al sistema d'informació, i així constaran a la Declaració d'Aplicabilitat, procediran principalment de la categorització del sistema.
8. La determinació de la categoria s'efectua en funció de les indicacions establertes a l'ENS-AD.

2.1. CATEGORITZACIÓ

9. La categoria BÀSICA d'un sistema es determina mitjançant la valoració de l'impacte que tindria sobre l'organització un incident que afectés la seguretat del sistema d'informació esmentat, amb repercussió en la capacitat organitzativa per complir les seves obligacions diàries de servei i respectar la legalitat vigent.
10. Per fer-ho, es fa una valoració individualitzada per cada actiu del sistema d'informació, per la qual cosa cal disposar d'un inventari actualitzat. Es recomana, en primer lloc, procedir a la valoració dels actius essencials (informació i serveis) que són els que exigiran una valoració més exhaustiva a l'hora d'establir els nivells de seguretat i determinar-ne la categoria del sistema.
11. Els actius essencials són aquells que concentren el valor del sistema en matèria de seguretat i són l'essència i la raó de ser del sistema. La resta d'actius donaran suport als actius essencials referits, i hereten les valoracions d'aquests d'acord amb la seva relació de dependència.
12. En conclusió, la categoria BÀSICA d'un sistema es determina mitjançant la valoració de l'impacte que tindria sobre l'organització un incident que afectés la seguretat del sistema, amb repercussió en la capacitat organitzativa per complir les obligacions diàries de servei i respectar la legalitat vigent. Aquesta valoració es realitza de forma individualitzada per cada actiu del sistema, i els actius essencials són els que exigiran una valoració més exhaustiva per establir els nivells de seguretat necessaris.

2.1.1. DETERMINACIÓ DE LA CATEGORIA

13. L'Esquema Nacional de Seguretat estableix una (1) categoria de seguretat per als sistemes d'informació: BÀSICA.

- ✓ Tots els sistemes d'informació seran de categoria bàsica, ja que és el nivell exigít per l'ENS-AD.

2.2. DETERMINACIÓ DE LES MESURES D'APLICACIÓ

14. Per assolir el compliment dels principis bàsics i requisits mínims establerts a l'Esquema Nacional de Seguretat, cal aplicar un conjunt de mesures de seguretat, que seran proporcionals a les dimensions de seguretat rellevants al sistema a protegir i la seva categoria.

15. L'Annex A de la guia ENS-STIC-804 recull la correspondència entre els nivells de seguretat exigits i les mesures de seguretat aplicables.

16. En concret, per cada mesura de seguretat s'indica:

- ✓ Si és aplicable o no per a un determinat nivell de seguretat. En cas que l'aplicació de la mesura no sigui necessària per obtenir l'adequació amb l'ENS-AD, a la taula de l'Annex A es recull el valor "n.a."

D'altra banda, en cas que sigui necessària la seva aplicació, apareixerà el següent valor:

- "aplica": indica que els requisits base d'una mesura de seguretat han de ser aplicats a una o diverses dimensions de la seguretat en algun nivell.

A continuació, es recull un exemple del que s'ha indicat anteriorment:

- a) La mesura [org.1] s'aplica als sistemes de categoria bàsica. El nivell d'exigència únicament s'apliquen els requisits bàsics.

Afectades	BÀSICA	Mesura de seguretat	
Marc organitzatiu	aplica	[org.1]	Política de seguretat

3. RECOMANACIONS

3.1. RESPECTE AL FORMAT DE LA DECLARACIÓ D'APLICABILITAT

17. Per a més claredat i utilitat de la Declaració d'Aplicabilitat, és una bona pràctica afegir dues (2) columnes addicionals: el grau d'implementació de cadascuna de les mesures que apliquin, així com el nivell de maduresa amb una breu descripció de com aplica cada mesura al Sistema d'Informació de l'Organització.
18. En aquesta descripció, si s'ha substituït alguna mesura de seguretat mitjançant una mesura compensatòria, haurà de constar referència a aquesta.
19. A més, disposeu d'una plantilla estàndard proporcionada per l'ANC-AD.

DECLARACIÓ D'APLICABILITAT ENS-AD						
Bàsic	Mesura	Descripció	Aplica	Grau d'implem.	Nivell de Maduresa	Detall de com aplica, o perquè no aplica
Marc organitzatiu						
APL	org.1	Política de seguretat	SI	G2	L3	Es disposa del document "POL-001 Política de seguretat" que al control de versions està referenciat com última versió la v1.2 en data de 03/02/2023. S'ha comunicat internament a l'organització a través d'Internet.
APL	org.2	Normativa de seguretat	SI	G1	L1	...
APL	org.3	Procediments de seguretat	SI	G1	L1	...
APL	org.4	Procés d'autorització	SI	G0	L0	...
Marc operacional						
	op.pl	Planificació				
APL	op.pl.1	Anàlisi de riscos	SI	G2	L3	...
APL	op.pl.2	Arquitectura de seguretat	SI	G1	L1	...
APL	op.pl.3	Adquisició de nous components	SI	G1	L1	...
APL	op.pl.4	Dimensionament/gestió de la capacitat	SI	G0	L0	...
n.a	op.pl.5	Components certificats	NO			No aplica pel nivell exigít a l'ENS-AD.

Il·lustració 1. - Extracte d'una possible declaració d'aplicabilitat

20. S'aprecia a l'extracte exemple de la figura superior, que representa un sistema de categoria BÀSICA, com es descriu l'aplicabilitat concreta per a les mesures [org.1] i [org.2]. A la columna 'Grau d'implementació', G0 significa que la mesura no està implementada, G1 que està en procés d'implementació i G2 que està implementada.

3.2. DECÀLEG DE RECOMANACIONS GENERALS

21. A continuació, es mostra un decàleg de recomanacions a tenir en compte per determinar una Declaració d'Aplicabilitat a l'àmbit de l'ENS-AD

Decàleg de recomanacions per a la Declaració d'Aplicabilitat (ENS-AD)	
1	Comprovar que es troben totes les mesures que apareixen a l'Annex A de la guia ENS-STIC-804
2	En cas que a la Declaració d'Aplicabilitat s'inclogui alguna mesura compensatòria, detallar, per cadascuna, els paràmetres següents: àmbit d'aplicació, limitacions o restriccions, objectiu, risc identificat, definició de la compensatòria, validació de la mesura compensatòria i manteniment.
3	Per a la redacció del document de Declaració d'Aplicabilitat, fer ús d'un document d'elaboració pròpia que sigui comprensible .