

Declaració, Certificació de conformitat ENS-AD



(DOCUMENT SUBJECTE A MODIFICACIONS)

Juny 2023

Fitxa del document

Títol	Declaració, Certificació de conformitat ENS-AD
--------------	--

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	02/06/23	Juny 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. LA CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT D'ANDORRA.....	6
2.1. CRITERIS DE DETERMINACIÓ DE LA CONFORMITAT	6
2.2. PROCEDIMENT DE DETERMINACIÓ DE LA CONFORMITAT	7
3. PUBLICITAT DE LA CONFORMITAT	8
3.1. ESQUEMA DE CERTIFICACIÓ DE LA CONFORMITAT AMB L'ENS-AD.....	8
3.2. DECLARACIÓ, CERTIFICACIÓ DE LA CONFORMITAT	8
3.3. COMUNICACIÓ DE LES CERTIFICACIONS DE CONFORMITAT A L'ANC-AD I LA SEVA PUBLICACIÓ	9

1. INTRODUCCIÓ

1. A continuació, es presenta la guia d'explicació dels criteris i requisits de la Certificació de Conformitat amb el Marc Nacional de Seguretat (ENS-AD). Aquesta guia té com a finalitat proporcionar una guia clara i detallada sobre els criteris que han de ser considerats i els requisits que han de ser complets per a emetre una Certificació de Conformitat vàlida segons l'ENS-AD.
2. Aquesta guia de Certificació de Conformitat amb l'Esquema Nacional de Seguretat d'Andorra (d'ara endavant, l' "ENS-AD"), s'enquadra dins dels requisits de la Llei 22/2022, del 09 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (d'ara endavant la "Llei NIS-AD").
3. Aquesta guia serà d'ús per als sistemes d'informació compresos en els àmbits subjectiu i objectiu d'aplicació segons disposa de l'ENS-AD.
4. La Certificació de Conformitat és un element essencial per acreditar que una organització ha implementat les mesures de seguretat adients i compleix amb les exigències establertes en el marc de referència de l'ENS-AD. Aquesta declaració constitueix una evidència del compromís de l'organització per protegir la informació i els sistemes d'informació d'acord amb les normatives establertes.
5. En aquesta guia, explorarem els criteris que s'han de tenir en compte per avaluar la conformitat amb l'ENS-AD. A més, s'explicaran els requisits específics i les directrius que han de ser completes per emetre una Certificació de Conformitat vàlida.
6. És important destacar que aquesta guia proporciona una visió general i orientativa del procés de Certificació de Conformitat amb l'ENS-AD. Es recomana que les organitzacions consultin les fonts oficials, com l'Agència de Ciberseguretat Andorrana (ANC-AD) per obtenir informació actualitzada i detallada sobre els requisits i les directrius aplicables.
7. Aquesta guia és una eina de referència valuosa per ajudar a les organitzacions a comprendre els criteris i requisits de la Certificació de Conformitat amb l'ENS-AD i a iniciar el procés d'avaluació i certificació de la seva seguretat de la informació. Esperem que aquesta guia sigui d'utilitat i contribueixi a reforçar la seguretat de la informació i la protecció dels sistemes d'informació.

2. LA CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT D'ANDORRA

2.1. CRITERIS DE DETERMINACIÓ DE LA CONFORMITAT

8. La conformitat amb el que disposa l'ENS-AD s'assoleix satisfent els mandats continguts en el seu text articulat i mitjançant la implantació adequada de les mesures de seguretat contemplades a l'Annex A de la Guia d'implementació, prèvia categorització dels sistemes a protegir.
9. Les Guies ENS STIC 802 (Guia d'auditoria), 804 (Guia d'implantació), proporcionen els elements necessaris per definir els criteris de determinació de la conformitat, així com la implantació i verificació de les mesures de seguretat, incloent-hi el procés d'auditoria.
10. La determinació de la conformitat dels sistemes d'informació de l'àmbit d'aplicació de l'ENS-AD es realitzarà mitjançant un procediment d'una auditoria regular ordinària anual, que verifiqui el compliment dels requeriments contemplats a l'ENS-AD anualment. Amb caràcter extraordinari, caldrà fer aquesta auditoria sempre que es produeixin modificacions substancials en els sistemes d'informació, que puguin repercutir en les mesures de seguretat requerides.
11. L'organització titular del sistema d'informació haurà de tenir procediments que permetin detectar les modificacions esmentades i comunicar aquesta circumstància a l'ANC-AD. L'absència de tal comunicació, quan fos necessària, podrà suposar la retirada de la Certificació de Conformitat concedida.
12. Per a la determinació de la conformitat dels sistemes d'informació de l'àmbit d'aplicació de l'Esquema amb categoria ENS-AD, caldrà executar un procediment d'autoavaluació que, amb caràcter ordinari, verifiqui el compliment dels requeriments contemplats a l'ENS-AD, almenys cada any (1). Amb caràcter extraordinari, aquesta autoavaluació haurà de realitzar-se sempre que es produeixin modificacions substancials en els sistemes d'informació, que puguin repercutir en les mesures de seguretat requerides.
13. El termini d'un (1) any assenyalat als paràgrafs anteriors podrà estendre's durant tres (3) mesos quan concorrin impediments de força major no imputables a l'organització titular del sistema o sistemes d'informació concernits.
14. En aquest sentit, l'objectiu de l'auditoria de certificació de l'ENS-AD és aportar la confiança que el sistema la informació ha estat auditat per un tercer independent, imparcial i capacitat. D'altra banda, la finalitat de l'auditoria interna ja sigui la que faci personal independent de la mateixa organització, o bé la facin auditors externs en modalitat de prestació de serveis, és la millora del sistema, ja que es busca confirmar l'eficàcia del sistema de gestió o obtenir informació que permeti llençar-la.

2.2. PROCEDIMENT DE DETERMINACIÓ DE LA CONFORMITAT

15. Com es desprèn del contingut de l'ENS-AD, la conformitat amb la norma d'un sistema d'informació concret passa necessàriament per adoptar i manifestar que s'han implementat les mesures de seguretat requerides per aquest sistema, atenent la seva categoria, i assegurant que aquestes mesures es mantenen al llarg de tot el cicle de vida del sistema.

Procediment d'avaluació	Categoria dels Sistemes Afectats	Manifestació de Conformitat	Resultat de l'avaluació	Anàlisi de l'avaluació
AUTOAVALUACIÓ Realitzada pel mateix personal que administra el sistema d'informació o aquell altre en qui hagués delegat.	ENS-AD	DECLARACIÓ DE CONFORMITAT	Document d'autoavaluació , indicant si cada mesura de seguretat està implementada i subjecta a revisió regular i les evidències que sustenten la valoració anterior.	Els documents d'autoavaluació seran analitzats pel responsable de seguretat competent, que elevarà les conclusions al responsable del sistema perquè adopti les mesures correctores adequades.
AUDITORIA FORMAL Realitzada amb les garanties metodològiques, d'independència, professionalitat i imparcialitat requerides.		CERTIFICACIÓ DE CONFORMITAT	Informe d'auditoria , és imperatiu qualificar adequadament, de conformitat amb el que assenyalava a la ITS d'Auditoria, les desviacions trobades a les auditories, distingint entre No Conformitats Majors, No Conformitats Menors i Observacions. Addicionalment, l'informe d'Auditoria podrà contenir oportunitats de millora que, segons el parer de l'auditor, aportin valor a l'auditoria i puguin contribuir a la millora del sistema de gestió de la seguretat dels sistemes d'informació concernits.	Els informes d'auditoria seran analitzats pel responsable de seguretat competent, que presentarà les vostres conclusions al responsable del sistema perquè adopti les mesures correctores adequades.

3. PUBLICITAT DE LA CONFORMITAT

16. Assolida la conformitat amb l'ENS-AD, i atenent al procediment assenyalat de Certificació de la Conformitat, es descriuen seguidament els continguts de la manifestació de conformitat.

3.1. ESQUEMA DE CERTIFICACIÓ DE LA CONFORMITAT AMB L'ENS-AD

17. L'exhibició d'una Certificació de Conformitat, d'aplicació obligatòria a sistemes d'informació de categoria ENS-AD, són necessaris per mostrar, a tots els interessats, el compromís de l'entitat en qüestió amb la seguretat dels sistemes, respecte de la informació que tracta o els serveis que presta.
18. La Certificació de Conformitat amb l'ENS-AD a què fa referència el punt anterior haurà de ser expedida per l'ANC-AD.
19. D'acord amb el que indica la clàusula 4.2.6 e) de la norma UNE-EN ISO/IEC 17065:2012, l'Entitat de Certificació (l'ANC-AD), ni cap part de l'entitat legal a què pertanyi, ni cap entitat sota el seu control organitzacional, podran oferir ni subministrar consultoria o assistència en el camp dels sistemes de gestió de seguretat de la informació, sistemes de govern de la seguretat de la informació, metodologies o eines associades o altres realitzacions de naturalesa similar, ni auditories internes sobre aquests referents.
20. Qualsevol situació que posi a l'entitat de certificació (ANC-AD) en la necessitat d'avaluar el producte del seu propi treball és una amenaça inacceptable per a la imparcialitat l'entitat de certificació ha de prendre accions per identificar i evitar aquestes situacions.
21. Pel que fa als certificats caducats de les entitats (tant del Sector Públic com del Sector Privat), es prolongarà la publicitat dels mateixos a la pàgina web de l'ANC-AD, llevat de situacions excepcionals justificades, durant dos (2) mesos. Posteriorment, si no s'ha rebut el nou Certificat, se'n procedirà eliminació en aquesta pàgina.

3.2. DECLARACIÓ, CERTIFICACIÓ DE LA CONFORMITAT

22. Quan es tracti de sistemes de categoria ENS-AD, i d'acord amb el que estableix l'ENS-AD, el sistema d'informació haurà de superar l'Auditoria corresponent.
23. El titular de l'òrgan superior en qüestió donarà publicitat a la conformitat dels sistemes d'informació afectats mitjançant l'exhibició d'una Declaració i Certificació de Conformitat.
24. La Declaració de Conformitat amb l'ENS-AD podrà representar-se mitjançant un Segell o Distintiu de Declaració de Conformitat, que serà publicat per l'organització titular, o sota la responsabilitat dels quals es troba el sistema d'informació en qüestió, sempre emprant els models de segells o distintius dissenyats per l'ANC-AD i descarregables des de la seva pàgina web.

25. La Certificació de Conformitat amb l'ENS-AD es podrà representar mitjançant un Segell o Distintiu de Certificació de Conformitat, que serà emès per l'Entitat Certificadora corresponent (ANC-AD), sempre utilitzant els models de segells o distintius dissenyats per l'ANC-AD i descarregables des del seu lloc web. L'ús d'aquest segell o distintiu per part de l'entitat titular o usuària del sistema d'informació en qüestió estarà condicionat a la possessió de la Certificació de Conformitat esmentada.
26. Aquest segell o distintiu de Certificació de Conformitat serà un document electrònic, en format no editable, signat per l'ANC-AD. Inclourà un enllaç que portarà a la Certificació de Conformitat anterior, la qual romandrà accessible a través de la seu electrònica o pàgina web de l'entitat pública o privada, segons el cas. Mentre que per la Declaració de Conformitat, serà el mateix procediment sense haver d'estar signat per l'ANC-AD.

3.3. COMUNICACIÓ DE LES CERTIFICACIONS DE CONFORMITAT A L'ANC-AD I LA SEVA PUBLICACIÓ

27. L'ANC-AD publicarà l'expedició d'aquests Certificats de Conformitat en un termini de quinze (15) dies després de l'expedició del Certificat en qüestió.
28. L'ANC-AD mantindrà al seu lloc web un llistat de les organitzacions públiques o privades que hagin obtingut Certificacions de Conformitat, amb indicació dels sistemes d'informació certificats, els serveis sostenguts o suportats en aquests sistemes i les dates d'expedició i de caducitat de les Certificacions.