

Reglaments

Decret 417/2022, del 12 d'octubre del 2022

Decret 417/2022, del 12-10-2022, pel qual s'aprova el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra.

Exposició de motius

La digitalització genera dos sentiments contraposats en els consumidors dels serveis. D'una banda, les empreses i les administracions han començat la seva particular cursa per a la transformació digital i aprenen els usuaris a reemplaçar els hàbits de consum presencial per uns altres de consum digital, multicanal i exempt d'horaris, el qual genera un sentiment d'urgència i disponibilitat. D'altra banda, els ciberdelinqüents i les amenaces internes (que no només inclouen fallades dels sistemes de la informació, sinó també un altre tipus de factor com és el factor humà) fan que aquests mateixos usuaris se sentin parcialment desemparrats quan en aquest món digital, al qual tan poc estan acostumats, succeeix alguna cosa, cosa que genera un sentiment de desconfiança i desemparrament que pot enquistar-se i provocar rebuig. Per reduir les ocasions en les quals s'experimenta aquest sentiment de desemparrament i desconfiança i eliminar així la barrera que molt sovint preval sobre la necessitat d'utilitzar un servei digital, i que tant alenteix la transformació digital, és absolutament necessari que els serveis digitals siguin segurs i, encara més, els serveis que resulten essencials o importants.

L'objectiu de l'Esquema nacional de seguretat del Principat d'Andorra (d'ara endavant, "ENS-AD" o simplement "Esquema") és garantir un nivell de seguretat suficient per als serveis que, conforme a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (d'ara endavant, "Llei NIS-AD"), resulten essencials o importants per al Principat d'Andorra.

Concretament, d'acord amb el que preveu la lletra a de l'apartat 2 de l'article 4 de la Llei NIS-AD, en el marc de l'Estratègia nacional de ciberseguretat del Principat d'Andorra, s'ha d'adoptar i desenvolupar reglamentàriament un esquema nacional de seguretat constituït pels principis bàsics i requisits mínims necessaris per a una protecció adequada de la informació tractada i els serveis prestats per les entitats essencials i les entitats importants, així com per les entitats que els presten serveis o els proveeixin de solucions per als seus serveis essencials o importants i les respectives cadenes de subministrament, amb l'objectiu d'assegurar l'accés, la confidencialitat, la integritat, la traçabilitat, l'autenticitat, la disponibilitat i la conservació de les dades, les informacions i els serveis utilitzats en mitjans electrònics que gestionin per prestar els serveis essencials o importants, i sense perjudici que pogués resultar necessari complementar les mesures de seguretat previstes en aquest esquema amb altres mesures específiques que puguin derivar-se dels compromisos internacionals contrets pel Principat d'Andorra o de la seva pertinença a organismes o fòrums internacionals en la matèria.

L'Esquema que s'adopta reglamentàriament mitjançant aquest Decret proporciona un mètode, unes instruccions respecte a la implementació de mesures de seguretat físiques, tècniques i organitzatives, unes recomanacions i una ajuda suficient perquè aquestes entitats, que es troben dins l'àmbit d'aplicació de la Llei NIS-AD, i totes les que voluntàriament decideixin implementar-lo aconseguixin el nivell de seguretat mínim necessari ("suficient") perquè els seus usuaris puguin confiar en els mitjans electrònics, sense el suport dels quals resulta inimaginable que avui dia puguin prestar-se quasi qualsevol servei. L'ENS-AD té l'objectiu de desenvolupar capacitats col·lectives per respondre als principals ciberatacs, i permet a aquestes entitats adoptar un enfocament holístic de la seguretat de la informació que inclou, a més dels aspectes

tècnics, els relatius a les infraestructures, l'organització i el personal que intervé en la prestació dels serveis que cal protegir.

L'objectiu últim d'aquest Esquema és, per tant, permetre a les entitats identificar i implementar, de manera sistemàtica i integral, les mesures de seguretat que resulten necessàries per assegurar la prestació dels seus serveis, i facilitar-los procediments per desenvolupar un sistema de gestió per a la seguretat de la informació (SGSI) que garanteixi un nivell de protecció proporcional al nivell de risc al qual estan exposats la informació i els serveis que s'han de protegir.

L'element troncal de l'ENS-AD és, d'acord amb el que especifica la Llei NIS-AD, la gestió de riscos; un procés per identificar els riscos als quals estan exposats les infraestructures, les xarxes, els sistemes d'informació, i les aplicacions que aquests últims executen, i per respondre de manera proporcional a la seva magnitud, mitjançant la planificació i la implantació de mesures de seguretat que, una vegada estiguin operatives, redueixin aquest risc de greu perjudici fins a un nivell que satisfaci els objectius que les entitats persegueixen, igualant o excedint els que els resultin d'obligació per a l'aplicació de la Llei NIS-AD i, en qualsevol cas, aconseguint o superant els objectius de risc que la direcció de cada entitat estigui disposada a acceptar.

L'ENS-AD proporciona un mecanisme per descompondre el problema d'aquesta anàlisi de riscos en la suma de subproblemes la solució dels quals proporciona la mateixa ANC-AD. L'essència d'aquest mecanisme, que ja s'emptra amb èxit en països de grandàries i complexitats tan dispars com són Alemanya i Estònia, és la descomposició del sistema sota estudi en peces cada vegada més petites, fins a arribar a una grandària (la dels servidors i els cables i xarxes d'àrea local, entre altres actius d'informació bàsics) que permeti reemplaçar cada actiu d'informació bàsic per una de les peces que l'ANC-AD ha estudiat i catalogat: els actius d'informació estàndard. Aquest mecanisme permet modelar el sistema sota estudi per tal de veure'l com la suma d'un conjunt d'actius d'informació estàndard, per a cadascun dels quals ja se sap quines mesures de seguretat concretes s'han d'implantar en funció del nivell de seguretat que vulguem donar als serveis que el sistema presta.

L'ENS-AD s'ha dissenyat pensant que l'adoptin entitats de tot tipus de mida, per tal que puguin implementar una protecció estandarditzada suficient per garantir un nivell mínim de seguretat dels serveis que presten, amb un consum de recursos relativament modest, i incloent-hi tant les relacions ad intra (relacions dins de les entitats) com les relacions ad extra (relacions entre diferents entitats i entre aquestes entitats i els usuaris dels seus serveis).

Ateses les consideracions esmentades, a proposta del Cap de Govern, el Govern, en la sessió del 12 d'octubre, aprova aquest Decret amb el contingut següent:

Article únic

S'aprova el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, que entrarà en vigor l'endemà de ser publicat al *Butlletí Oficial del Principat d'Andorra*.

Reglament de l'Esquema nacional de seguretat del Principat d'Andorra

Capítol primer. Consideracions generals

Article 1. *Objecte*

1. Aquest Reglament té per objecte regular l'Esquema nacional de seguretat del Principat d'Andorra (ENS-AD), de conformitat amb el mandat establert a la lletra a de l'apartat 2 de l'article 4 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (Llei NIS-AD), el qual es complementa amb les guies d'implantació i auditoria, les polítiques i els components del catàleg d'actius d'informació estàndard que l'Agència Nacional de Ciberseguretat (ANC-AD) publiqui en relació amb l'Esquema al seu lloc web.

2. Aquest Reglament regula l'establiment del Sistema de gestió de seguretat de la informació (SGSI) i d'un procediment per especificar els requisits de seguretat mínims i les mesures de seguretat tècniques i

organitzatives que, com a mínim, s'han d'aplicar a les xarxes i als sistemes d'informació per assegurar un nivell de seguretat que respecti la confidencialitat, la integritat i la disponibilitat de manera proporcional a la naturalesa de la informació tractada, els serveis que cal prestar i els riscos als quals estiguin exposats.

3. Addicionalment, aquest Reglament aclareix, precisa, simplifica i actualitza alguns dels principals conceptes de la ciberseguretat amb l'objectiu d'homogeneitzar-ne la utilització.

Article 2. Definicions

1. Els termes següents, utilitzats dins el context de l'ENS-AD, tenen el significat següent:

a) Actiu d'informació bàsic: actiu d'informació que no cal descompondre més perquè ja és fàcil analitzar el risc a què està exposat, i determinar quines són les seves amenaces i quins conjunts de salvaguardes caldria implementar per conferir-li un determinat nivell de seguretat. Exemples d'actius d'informació bàsics són l'edifici i el cablejat elèctric, quan el que s'analitza és una infraestructura; les LAN i VPN, quan el que s'analitza és una xarxa; els servidors i els seus sistemes operatius, quan el que s'analitza és un sistema d'informació, o la base de dades i l'aplicació web, quan el que s'analitza és una aplicació.

b) Actiu d'informació estàndard: actiu d'informació bàsic que ha estat analitzat per l'ANC-AD, i per al qual s'han identificat els conjunts de mesures de referència que s'han d'implementar per assolir un determinat nivell de seguretat. L'ANC-AD publica i manté el catàleg d'actius d'informació estàndard.

c) Classe de seguretat: combinació específica de les tres subclasses de seguretat. El símbol de la classe de seguretat es forma a partir dels símbols de les subclasses en aquest ordre: D-I-C (disponibilitat, integritat i confidencialitat). El nombre de totes les combinacions possibles és 4x4x4, per la qual cosa hi ha 64 classes de seguretat diferents.

d) Declaració d'aplicabilitat: llista de mesures de referència que apliquen a una entitat, confeccionada segons s'indica en l'article 12.

e) DSI: delegat de la seguretat de la informació, d'acord amb el que estableix l'article 18 de la Llei NIS-AD

f) Mesures de referència: mesures de seguretat típiques, catalogades, sobre les quals s'han establert mètodes de selecció d'acord amb el nivell de seguretat que es requereixi.

g) Mesures de seguretat: actes i mitjans organitzatius, processos tècnics i implantació de mitjans tècnics per a l'obtenció i la conservació de la seguretat de les xarxes i els sistemes d'informació.

h) Modelar: ajustar a un arquetip format per actius d'informació bàsics.

i) Seguretat de la informació: col·lecció de processos per a la creació, la selecció i la implementació de mesures de seguretat.

j) SGSI: Sistema de gestió de la seguretat de la informació, consistent en un conjunt integral de mesures de gestió que permet garantir la sostenibilitat dels serveis que presta l'entitat i la protecció dels seus actius d'informació.

k) Subclasse de seguretat: nivell de seguretat associat a una de les tres principals dimensions de la seguretat de la informació (disponibilitat, integritat i confidencialitat), expressat en una escala de quatre nivells (0 a 3).

2. La resta de termes emprats en aquest Reglament tenen el significat que defineix l'article 3 de la Llei NIS-AD.

Article 3. Àmbit d'aplicació

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 definits a la Llei NIS-AD, amb la qualitat que cadascun requereix.

Capítol segon. Principis, classes, catàleg i SGSI

Article 4. *Principis bàsics de l'ENS-AD*

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

- a) Seguretat entesa com a procés integral i sistemàtic, que inclou tots els elements tècnics, humans, materials i organitzatius relacionats amb les xarxes i els sistemes d'informació necessaris per prestar els serveis essencials o importants (principi de seguretat integral i sistemàtica).
- b) Gestió de la seguretat basada en la gestió dels riscos als quals estiguin exposats aquests serveis, de forma proporcionada a la naturalesa de la informació tractada i als serveis que s'han de prestar (principi de proporcionalitat).
- c) Modelatge dels actius d'informació bàsics mitjançant actius d'informació estàndard per als quals compten amb mesures estàndard de prevenció, per eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se; mesures estàndard de detecció, per descobrir la presència d'un ciberincident; mesures estàndard de resposta, per restaurar la informació i els serveis que poguessin haver-se vist afectats, i mesures estàndard per garantir la conservació de les dades i informacions en suport electrònic (principi de modelatge estàndard).
- d) Estratificació de la defensa, constituint mesures que formin capes de seguretat, agregant noves mesures a la capa bàsica per construir la capa de nivell de seguretat mitjà, i agregant novament més mesures sobre aquesta última per constituir la capa de seguretat alta, de forma que es redueixi la probabilitat que la bretxa en una capa comprometi tots els actius d'informació que suporten els serveis als quals aplica l'ENS-AD (principi d'estratificació de les mesures).
- e) Vigilància contínua per detectar activitats o comportaments anòmals, i reavaluació periòdica per adequar les mesures d'acord amb l'evolució dels riscos als quals estan exposats en cada moment la informació tractada i els serveis que s'han de prestar (principi de millora contínua).
- f) Diferenciació de responsabilitats sobre la prestació dels serveis i sobre la seguretat dels actius d'informació que suporten aquests serveis (principi de propietat de serveis i actius).

Article 5. *Subclasses de seguretat*

1. S'estableixen tres subclasses de seguretat associades a les tres dimensions de la seguretat de la informació que inclou l'ENS-AD: la disponibilitat, la integritat i la confidencialitat.

2. S'estableixen quatre nivells de seguretat per a cada subclasse, segons quin sigui el nivell d'impacte en la informació o el servei que podria causar un ciberincident (equivalent, pel principi de proporcionalitat, al nivell de protecció que s'ha d'aconseguir en la dimensió de la seguretat corresponent):

- a) Nivell 0 (crític): impacte que impedeix la prestació del servei.
- b) Nivell 1 (important): impacte que degrada la prestació del servei fins al punt que no es pot garantir.
- c) Nivell 2 (mitjà): impacte que permet garantir la prestació del servei, però amb menys qualitat que la requerida.
- d) Nivell 3 (baix): impacte molt reduït en el servei, gairebé inapreciable.

El nivell de seguretat d'una subclasse es descriu amb una lletra, que correspon a la dimensió de la seguretat que dona nom a la subclasse (D per disponibilitat, I per integritat i C per confidencialitat), seguida del nivell de protecció que es necessita assolir, en format numèric.

3. La subclasse Disponibilitat s'assigna d'acord amb l'escala següent, amb el valor que sigui més alt sense excedir els requisits de l'actiu d'informació o el servei:

- 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.

4. La subclasse Integritat s'assigna d'acord amb l'escala següent, amb el valor que sigui més alt sense excedir els requisits de l'actiu d'informació o el servei:

- 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 d'alterar-la o destruir-la, ha de ser identificable, i no és necessari comprovar periòdicament la precisió, la integritat i l'actualitat de la informació.
- I1: quan la font de la informació, o el fet d'alterar-la o destruir-la, ha de ser identificable i és necessari fer comprovacions periòdiques de la precisió, la integritat i l'actualitat de la informació.
- I0: quan la font de la informació, o el fet d'alterar-la o destruir-la, ha de tenir valor probatori, o quan es requereix una verificació en temps real de la precisió, la integritat i l'actualitat de la informació.

5. La subclasse Confidencialitat s'assigna d'acord amb l'escala següent:

- C3 o informació pública: 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 o informació d'ús intern: quan s'ha de concedir l'accés a la informació si la persona que sol·licita l'accés té un interès legítim.
- C1 o informació classificada: 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 o informació altament classificada: 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.

6. S'autoritza les autoritats competents designades a l'article 6 de la Llei NIS-AD a adaptar aquests nivells per a alguna de les entitats sota la seva supervisió o totes.

Article 6. Classe i nivell de seguretat

1. La classe de seguretat d'un actiu d'informació o servei és la concatenació dels nivells de protecció que aquest actiu o servei necessita en cada subclasse: el nivell que s'ha assignat a la subclasse Disponibilitat, el nivell que s'ha assignat a la subclasse Integritat i el nivell que s'ha assignat a la subclasse Confidencialitat (per exemple, D2I3C1).

2. 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 de cada una de les seves subclasses de seguretat, consultant la taula següent:

		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

Complint el principi d'estratificació de les mesures, les mesures de seguretat de cada nivell de seguretat inclouen les del nivell anterior, i afegeixen a aquestes últimes una capa de seguretat addicional. Així, si un actiu d'informació té un nivell de seguretat M, se li han d'aplicar les mesures de seguretat del nivell B i després les que corresponen al nivell M. Igualment, si un actiu d'informació té un nivell de seguretat A, se li han d'aplicar les que correspondrien al nivell M més les mesures addicionals especificades per al nivell A.

3. S'autoritza les autoritats competents designades a l'article 6 de la Llei NIS-AD a adaptar aquesta taula per a alguna de les entitats del seu àmbit de supervisió o totes.

4. La classe de seguretat ha de ser avaluada de nou sempre que es produeixin modificacions significatives en els criteris utilitzats per determinar-la, i com a mínim anualment.

Aquest indicador és la base per establir les mesures de referència obligatòries per a aquest indicador, que se seleccionen sobre la base de les mesures de referència que l'ANC-AD hagi especificat per a la mateixa classe en l'actiu d'informació estàndard que pot modelar el que s'estigui analitzant.

Article 7. *Catàleg d'actius d'informació estàndard*

1. L'ANC-AD analitza els riscos i especifica cadascun dels actius d'informació que resultin necessaris per modelar els serveis als quals aplica aquest Reglament. L'especificació d'aquests actius d'informació estàndard inclou les amenaces a les quals estan exposats i les mesures de seguretat de la informació que, d'acord amb el principi d'estratificació de mesures, els donaria cadascun dels tres nivells de seguretat definits en l'article 6 d'aquest Reglament. Aquestes especificacions formen el Catàleg d'actius d'informació estàndard (d'ara endavant, "el Catàleg").

2. El Catàleg es publica amb una periodicitat mínima anual al lloc web de l'ANC-AD, i cada actualització pot incloure addicions o supressions d'actius d'informació estàndard, així com addicions o canvis en les amenaces o les mesures dels actius d'informació estàndard que ja formaven part del Catàleg en la versió anterior.

3. Les autoritats competents designades a l'article 6 de la Llei NIS-AD comuniquen a totes les entitats essencials i importants que estan sota la seva supervisió la publicació de cada nova versió del Catàleg. Aquesta comunicació es fa sense dilació indeguda i, en tot cas, no més tard d'una setmana després de la data de publicació de la versió del Catàleg de què es tracti.

4. Un any després de la publicació d'una nova versió del Catàleg, les addicions i els canvis s'agreguen a la llista de punts que cal auditar i que les autoritats competents usaran per complir la seva obligació de supervisió.

Article 8. *Sistema de gestió de la seguretat de la informació*

1. El principi de seguretat integral i sistemàtica obliga que la responsabilitat d'iniciar, gestionar i controlar el Sistema de gestió de la seguretat de la informació (SGSI) de l'entitat recaigui sobre l'òrgan de direcció de l'entitat, que delega les tasques associades a aquesta responsabilitat en el DSI de l'entitat, si n'hi ha.

2. El responsable d'implantar l'SGSI de l'entitat ha de garantir-ne l'efectivitat, per la qual cosa ha d'executar les tasques següents:

a) Determinar els lineaments que regularan el marc organitzacional i operacional de la seguretat de la informació de l'entitat, seleccionant-los d'entre els especificats per l'ANC-AD en l'apartat dels Components generals del Catàleg que descriu l'article 7 d'aquest Reglament.

b) Organitzar l'elaboració del pla d'acció per establir els lineaments de la seguretat de l'entitat identificats en el punt anterior, i per gestionar els riscos de seguretat de la informació dels serveis als quals aplica l'ENS-AD, i revisar-lo almenys una vegada a l'any o cada vegada que es faci un canvi en aquests serveis.

3. Per determinar els lineaments que regularan els marcs organitzacional i operacional de la seguretat de la informació de l'entitat i per a l'elaboració del pla d'acció que indica l'apartat 2.b d'aquest article, s'ha de seguir el procediment d'implantació que l'ANC-AD publicarà al seu lloc web.

Capítol tercer. Elements de l'SGSI

Article 9. Àmbit de la implantació de l'ENS-AD

1. L'ENS-AD s'ha d'implantar en cadascun dels actius d'informació necessaris per garantir la prestació dels serveis als quals s'aplica aquest Reglament amb la qualitat que requereixen.

2. No obstant el que estableix l'apartat anterior, es faculta el DSI per proposar a l'òrgan de direcció de l'entitat ampliar l'àmbit d'aplicació de l'ENS-AD a tots els serveis que presta l'entitat. Si l'òrgan de direcció aprova aquesta proposta, l'ENS-AD s'ha d'aplicar a la totalitat dels actius d'informació que l'entitat necessita per garantir la prestació dels seus serveis amb la qualitat requerida.

Article 10. Nivells de seguretat dels serveis

Per a cada servei dins l'àmbit d'implantació de l'ENS-AD, el seu gestor o responsable dins l'entitat (d'ara endavant, "propietari del servei"), en col·laboració amb el DSI de l'entitat, analitza els nivells de confidencialitat, integritat i disponibilitat requerits per garantir una qualitat mínima acceptable del servei del qual és propietari i els riscos als quals està exposat aquest últim, i li assigna les subclasses, la classe i el nivell de seguretat que li pertoquin d'acord amb el que està establert a l'article 5 i l'article 6 d'aquest Reglament.

Article 11. Inventari d'actius

1. Cada servei dins l'àmbit de la implantació de l'ENS-AD ha de modelar-se mitjançant els actius d'informació estàndard d'acord amb el que està establert a l'article 12 d'aquest Reglament. Amb aquest objectiu, les infraestructures, les xarxes, els sistemes d'informació i les aplicacions i el programari que suporten cada un d'aquests serveis s'han de descompondre fins a arribar al nivell de complexitat dels actius d'informació bàsics que puguin modelar-se mitjançant actius d'informació estàndard.

El DSI és responsable del següent:

- a) Dur a terme l'inventari d'actius d'informació bàsics la seguretat dels quals s'ha de gestionar, amb la col·laboració del personal de TIC i d'administració de l'entitat, i amb un nivell de detall suficient per efectuar la resta de funcions que descriu aquest article.
- b) Coordinar per a cada actiu de l'inventari l'assignació de la seva classe de seguretat per part dels seus propietaris (personal de TIC), en col·laboració amb els propietaris dels serveis que suporta l'actiu i amb l'assessorament d'experts en seguretat de la informació.
- c) Afegir als actius d'informació del punt 1.a els que constitueixen el marc organitzatiu i operacional de la seguretat de la informació que permet a l'entitat complir els principis bàsics de l'ENS-AD, i assignar-los les subclasses de seguretat més crítiques de les assignades a la resta d'actius d'informació en el punt anterior.
- d) Determinar el nivell de seguretat requerit per a cada actiu d'informació de l'inventari d'acord amb el que s'indica a l'article 6 d'aquest Reglament.

2. L'inventari d'actius conté per a cada actiu, com a mínim, la informació següent:

- a) Identificació de l'actiu d'informació bàsic.
- b) Els serveis en la prestació dels quals participa.
- c) Classe i nivell de seguretat.
- d) Identificació de l'actiu d'informació estàndard que, conforme a la guia d'implantació de l'ENS-AD, s'ha-gi seleccionat per modelar-lo.

3. Es faculta l'ANC-AD per precisar en la guia d'implantació de l'ENS-AD els criteris necessaris per a una adequada classificació de seguretat dels actius d'informació bàsics que suporten els serveis als quals s'aplica l'ENS-AD, així com per establir perfils de compliment específics per a entitats o sectors concrets, que han d'incloure els reforços addicionals que en cada cas resultin aplicables, o els criteris per determinar-los.

Article 12. *Declaració d'aplicabilitat*

1. El DSI és responsable del següent:

- a) Aplicar a cadascun dels actius d'informació bàsics continguts en l'inventari el procediment de modelatge amb actius d'informació estàndard que s'estableix a la guia d'implementació de l'ENS-AD.
- b) Compilar una llista de mesures de referència per assolir el nivell de seguretat requerit en cada actiu d'informació inventariat, d'acord amb l'especificació dels actius d'informació estàndard amb els quals s'ha-gin modelat i amb les directrius de la guia d'implantació de l'ENS-AD.
- c) Ampliar la llista de mesures de referència de l'apartat 1.b amb les mesures addicionals que es consi-derin necessàries i proporcionals a les noves amenaces que puguin sorgir i no estiguin considerades en el catàleg d'amenaces utilitzat per especificar els actius d'informació estàndard.
- d) Elaborar una proposta de declaració d'aplicabilitat que contingui:
 - i. La llista de mesures de seguretat descrita en l'apartat 1.c.
 - ii. Els actius d'informació estàndard emprats en l'apartat 1.a als quals s'aplica cada mesura de seguretat.
 - iii. Si s'implementen per complet o no; i, en aquest últim cas,
 - iv. La justificació per excloure la implantació de qualsevol de les mesures de referència en qualsevol dels actius d'informació bàsics als quals s'apliquin.

Aquesta exclusió està permesa quan:

- 1. La mesura no es consideri necessària després de fer una avaluació de riscos de seguretat específica per a l'actiu d'informació del qual s'exclou, per verificar que les amenaces previstes en l'especificació del corresponent actiu d'informació estàndard s'ajusten a la seva situació de perill real;
 - 2. S'hagi implementat una altra mesura equivalent a la de referència; o
 - 3. La guia d'implementació de l'ENS-AD així ho indiqui específicament.
2. Aquesta proposta de declaració d'aplicabilitat es presenta a l'òrgan de direcció de l'entitat perquè la modifiqui i aprovi, moment en el qual passa a constituir la declaració d'aplicabilitat de l'entitat que, d'acord amb el que està establert a l'apartat 3 de l'article 12 de la Llei NIS-AD, s'ha de remetre a l'autoritat compe-tent en el termini de sis mesos a comptar de la identificació de l'entitat com a entitat essencial o important.

Article 13. *Gestió del canvi i millora contínua*

1. El DSI és responsable de:

- a) Mantenir la configuració i la gestió de canvis. Qualsevol canvi en els actius d'informació bàsics, actius d'informació estàndard, classes de seguretat, mesures de referència o mesures addicionals s'ha de re-gistrar, i el registre dels canvis ha d'estar a disposició de l'autoritat que supervisa l'entitat. Si l'entitat fa canvis significatius en els serveis o en els actius d'informació inventariats, tot el procés d'im-plantació de l'ENS-AD ha de començar des del principi o des de l'etapa afectada pel canvi.
- b) Verificar sistemàticament la situació de seguretat real dels actius d'informació inventariats tenint en compte les seves amenaces reals.

En cas d'existir perills que no estiguin coberts per l'especificació de seguretat de l'actiu d'informació estàndard, el DSI ha de verificar la idoneïtat de les mesures de seguretat implementades en les condicions reals i, si és necessari, aplicar mesures de seguretat addicionals.

Capítol quart. *Requisits mínims***Article 14.** *Requisits mínims per a l'entitat responsable dels serveis*

1. Per donar compliment als requisits mínims establerts en aquest Reglament, les entitats compreses en el seu àmbit d'aplicació adopten les mesures de seguretat referides en la declaració d'aplicabilitat que descriu l'article 12 d'aquest Reglament.

2. El DSI està autoritzat a no implementar una d'aquestes mesures de seguretat si no redueix els riscos o és massa costosa en comparació amb la reducció dels riscos derivats d'aplicar-la, o si considera que els riscos que cobreix la mesura ja estan coberts per altres mesures tal com indica la mateixa declaració d'aplicabilitat. Si el DSI decideix no implementar alguna de les mesures, ha d'informar els òrgans de direcció de l'entitat que l'ha designat sobre els riscos derivats d'aquesta no implementació, per tal que siguin capaços de prendre la decisió d'aprovar o no les mesures de seguretat proposades, d'acord amb l'obligació que els imposa el que està establert a l'apartat 1 de l'article 17 de la Llei NIS-AD.

3. L'existència d'una referència sobre les mesures de seguretat necessàries per als actius d'informació bàsics no eximeix el DSI de la seva obligació de gestionar els riscos, fins i tot els associats a actius d'informació o amenaces no totalment previstes en el Catàleg que descriu l'article 7 d'aquest Reglament.

4. Quan un actiu d'informació tracti dades personals, li és aplicable el que es disposa en la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD), així com la resta de l'eventual normativa d'aplicació nacional i internacional.

5. Si els serveis als quals s'aplica l'ENS-AD estan suportats per serveis subcontractats a una altra entitat, l'entitat que els presta ha de tenir en compte, quant a la infraestructura i els processos d'aquesta altra entitat proveïdora de serveis, que poden no ser directament auditable (especialment quan es tracta de serveis prestats per empreses internacionals o que presten serveis en el núvol). Per tant, la implantació de l'ENS-AD s'ha de basar en part en els termes del contracte al quals es refereix l'apartat 3 de l'article 15 d'aquest Reglament, així com en les condicions generals per a la prestació del servei subcontractat i en els certificats de seguretat del proveïdor, respecte del servei subcontractat, i això s'ha de reflectir en l'anàlisi de riscos inclòs en l'article 10 d'aquest Reglament i en el principi de proporcionalitat.

Aquesta anàlisi de riscos ha de tenir en compte igualment els riscos potencials, com una interrupció a llarg termini de la xarxa de tercers, la fallida del proveïdor de serveis, i la resta d'amenaces que s'inclouen en l'actiu d'informació estàndard anomenat Subcontractació. Els aspectes legals i de seguretat s'han de tenir en compte per als proveïdors de serveis situats fora d'Andorra i de la Unió Europea. No obstant això, atès que l'entitat que utilitza el programari o el servei administrat és, en qualsevol cas, responsable de la seguretat de la informació dels seus serveis, l'entitat que subcontracta ha de definir clarament les responsabilitats de les parts en el contracte de servei al qual es refereix l'apartat 3 de l'article 15.

6. El DSI ha de signar la declaració d'aplicabilitat i comunicar-la a l'autoritat competent que correspongui a l'entitat.

7. Les mesures a les quals es refereixen els apartats 1 a 4 d'aquest article tenen la condició de mínims exigibles, i poden ser objecte d'auditoria conforme al que està indicat en l'article 16.

Article 15. *Requisits mínims per a les entitats subcontractades*

1. Les entitats essencials i importants tenen el deure d'escollir proveïdors (entitats subcontractades) que ofereixin garanties suficients sobre els serveis subcontractats per aplicar les mesures de seguretat tècniques i organitzatives que siguin adequades al nivell de seguretat que requereixen els serveis als quals s'aplica l'ENS-AD. Entre aquestes garanties, hi pot haver els certificats de seguretat internacionalment reconeguts.

2. L'entitat subcontractada no pot recórrer a una altra subcontracta (independentment que aquesta última sigui una entitat o una persona física) sense l'autorització prèvia, per escrit, específica o general, de l'entitat que presta el servei al qual s'aplica l'ENS-AD. L'entitat subcontractada ha d'informar l'entitat que presta el servei al qual s'aplica l'ENS-AD de qualsevol canvi previst en la incorporació o la substitució d'altres subcontractes en els quals delegar part o la totalitat de la prestació del servei subcontractat. D'aquesta manera, es dona a les entitats que presten serveis als quals s'aplica l'ENS-AD l'oportunitat d'oposar-se a aquests canvis i, si escau, de canviar de proveïdor.

3. El servei que l'entitat subcontractada presta per suportar el servei al qual s'aplica l'ENS-AD s'ha de regir per un contracte per escrit, inclòs el format electrònic, que vincula l'entitat subcontractada a l'entitat que presta el servei al qual s'aplica l'ENS-AD, i estableix, com a mínim:

- a) El nivell de seguretat i l'acord del nivell del servei que l'entitat subcontractada ha de garantir pel servei subcontractat.
- b) Les penalitzacions associades als incompliments en relació amb el punt anterior.
- c) Les restriccions que per raó de jurisdicció pot haver-hi en la ubicació física dels actius d'informació que l'entitat subcontractada necessita per prestar el seu servei. En especial quan aquests actius d'informació són crítics, quan es tracten dades personals o qualsevol altre tipus d'informació igualment sensible, o quan algun dels actius d'informació de l'entitat subcontractada hagi d'ubicar-se fora d'Andorra i de l'espai econòmic europeu.
- d) Garantir que les persones autoritzades per tractar la informació o administrar, mantenir o operar el servei s'han compromès a respectar la confidencialitat de la informació o estan subjectes a una obligació de confidencialitat de naturalesa estatutària, i han rebut la formació adequada en matèria de seguretat de la informació.
- e) Prendre totes les mesures necessàries en matèria de seguretat de la informació.
- f) Respectar les condicions establertes en l'apartat 2, en recórrer a unes altres subcontractes, i obligar-les a complir, mitjançant un contracte escrit, les mateixes obligacions de seguretat de la informació que s'ha-gin estipulat en aquest contracte, especialment la prestació de garanties suficients d'aplicació de mesures tècniques i organitzatives adequades de manera que el servei al qual s'aplica l'ENS-AD sigui conforme amb les disposicions d'aquesta Llei. Addicionalment, s'ha d'especificar que en cap cas aquesta subcontracta no farà que l'entitat subcontractada perdi les seves responsabilitats enfront de l'entitat que presta el servei al qual s'aplica l'ENS-AD.
- g) Assistir l'entitat que presta el servei al qual s'aplica l'ENS-AD en les obligacions que estableixen els articles 12 a 15 de la Llei NIS-AD.
- h) Les condicions per al rescat del servei que presta l'entitat subcontractada.
- i) Posar a disposició de l'entitat que presta el servei al qual s'aplica l'ENS-AD tota la informació necessària per demostrar que compleix les obligacions que estableix aquest article. Així mateix, ha de permetre la realització d'auditories, incloses inspeccions, i contribuir-hi, per part de l'entitat que presta el servei al qual s'aplica l'ENS-AD, per l'autoritat competent que supervisa aquesta última, o per un altre auditor autoritzat per fer aquestes auditories.
- j) L'obligació de l'entitat subcontractada d'informar immediatament l'entitat que presta el servei al qual s'aplica l'ENS-AD si considera que no compleix el nivell de seguretat exigít, encara que sigui temporalment.

4. En l'àmbit del sector públic, poden atribuir-se les competències pròpies d'una entitat subcontractada a un determinat òrgan de l'Administració pública de què es tracti o als seus organismes vinculats o dependents mitjançant l'adopció d'una norma reguladora de les competències referides, que ha d'incorporar el contingut previst a l'apartat anterior.

Capítol cinquè. Auditoria de seguretat

Article 16. Auditoria de seguretat

1. Els actius d'informació necessaris per a la prestació dels serveis als quals s'aplica l'ENS-AD són objecte d'una auditoria interna ordinària anual que verifiqui el compliment dels requisits establerts en aquest Reglament.

Amb caràcter extraordinari, aquesta auditoria s'ha de fer sempre que es produeixin modificacions substancials en els serveis als quals s'aplica l'ENS-AD o en els actius d'informació que els suporten, o en un nombre significatiu de mesures de seguretat requerides d'acord amb el que estableix l'article 14 d'aquest Reglament. La realització d'aquesta auditoria extraordinària determina la data de còmput per al càlcul dels dos anys establerts per efectuar la següent auditoria ordinària, indicats en el paràgraf anterior.

2. L'auditoria es porta a terme 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 als quals s'aplica l'ENS-AD.

3. L'informe d'auditoria serveix a l'òrgan de direcció de l'entitat per identificar les mesures que l'entitat necessita adoptar per corregir la possible falta d'adequació amb l'ENS-AD, i ha d'incloure la metodologia emprada, l'abast i l'objectiu de l'auditoria, el grau de compliment i incompliment d'aquest Reglament, les evidències que suporten els incompliments detectats, i les mesures que s'han d'adoptar per resoldre els incompliments.

4. Els informes d'auditoria poden ser requerits per les autoritats competents designades a l'article 6 de la Llei NIS-AD, en l'exercici de la seva obligació de supervisió d'acord amb el capítol tercer de la Llei NIS-AD.

Capítol sisè. Actualització i certificació de l'Esquema nacional de seguretat

Article 17. *Actualitzacions del Catàleg*

1. En desenvolupament del que es disposa en aquest Reglament, l'ANC-AD aprova les actualitzacions del Catàleg d'actius estàndard que descriu aquest Reglament. L'ANC-AD elabora aquest Catàleg en col·laboració amb el CSIRT-AD i amb la resta d'autoritats competents designades a l'article 6 de la Llei NIS-AD.

2. Un any després de la publicació, les actualitzacions del Catàleg s'incorporen al conjunt documental utilitzat per fer les auditories de l'ENS-AD.

Article 18. *Entitat certificadora, durada i publicació*

1. L'entitat acreditada per a la certificació de l'ENS-AD és l'ANC-AD, la qual després de revisar i auditar la documentació aportada expedeix el certificat corresponent a la classe de seguretat demanada.

2. La durada del certificat és de dos anys a comptar de la data de l'expedició, i en el certificat hi han de figurar les dades següents: entitat, servei, classe de seguretat, data d'expedició i data de finalització.

3. Totes les entitats amb serveis certificats d'acord amb l'ENS-AD es publiquen al lloc web de l'ANC-AD.

Disposició addicional. Formació i conscienciació

Les autoritats competents designades a l'article 6 de la Llei NIS-AD, en col·laboració amb el CSIRT-AD i la Universitat d'Andorra, entre altres, han de desenvolupar programes de sensibilització, conscienciació i formació, dirigits al personal i a l'òrgan de direcció de les entitats a les quals s'aplica la Llei NIS-AD, per assegurar una adequada implantació de l'ENS-AD i un adequat desplegament de la informació i les capacitats jurídiques, organitzatives i tècniques relacionades amb la ciberseguretat dels serveis essencials i els serveis importants, i per garantir el coneixement permanent de l'ENS-AD entre aquestes entitats.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 12 d'octubre del 2022

Xavier Espot Zamora
Cap de Govern