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

Índex

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 apressen 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 desemparats quan en aquest món digital, al qual tan poc estan acostumats, succeeix alguna cosa, cosa que genera un sentiment de desconfiança i desemparament que pot enquistar-se i provocar rebuig. Per reduir les ocasions en les quals s'experimenta aquest sentiment de desemparament 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 prestin 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 aconsegueixin 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 pugui 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'empra 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'homogeneïtzar-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).