

Reglaments

Decret 417/2024, del 30-10-2024, de modificació del Decret 417/2022, del 12-10-2022, d'aprovació del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra.

Exposició de motius

Des de l'aprovació del Decret 417/2022, del 12-10-2022, d'aprovació del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, com un dels mecanismes per garantir la ciberseguretat al Principat d'Andorra de conformitat amb la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (en endavant, "la Llei NIS-AND"), la tasca executada en matèria de seguretat pública en el ciberespai, anticipant i prevenint els delictes en matèria de seguretat de les xarxes i els sistemes d'informació, s'ha començat a implementar.

Seguint el principi de millora contínua continguda a l'article 12 de la Llei NIS-AD, exigible a les entitats que prestin serveis essencials i importants, es considera necessària l'actualització de l'Esquema nacional de seguretat del Principat d'Andorra (ENS-AD), a l'efecte d'introduir-hi exigències addicionals per oferir més garanties per millorar la resiliència de les entitats essencials i importants pel que respecta a les empreses que els proveeixin serveis, tecnologia o productes, mitjançant l'exigència de presentar una auditoria de seguretat externa. Així mateix, aquests serveis, tecnologia o productes s'han de correspondre amb els que l'Agència Nacional de Ciberseguretat del Principat d'Andorra (en endavant, "l'ANC-AD") estableix com a certificats segons els seus registres al respecte, incloses les eventuais excepcions que es prevegin.

Aquestes modificacions també afavoreixen que l'ANC-AD continuï sent el punt de referència generador de confiança en matèria de ciberseguretat per a les entitats essencials i importants del Principat d'Andorra.

Finalment, aquesta actualització reforça el compromís nacional de cooperar en l'àmbit nacional i en l'internacional en tot el que sigui necessari per a la seguretat de les xarxes i els sistemes d'informació del Principat d'Andorra.

D'acord amb les consideracions exposades, i a proposta del cap de Govern, el Govern, en la sessió del 30 d'octubre del 2024, aprova aquest Decret amb el contingut següent:

Article 1. *Modificació de l'article 15 del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, relatiu als requisits mínims per a les entitats subcontractades*

Es modifica l'article 15 del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, aprovat pel Decret 417/2022, del 12-10-2022, que queda redactat com segueix:

"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, així com sobre la provisió de qualsevol tecnologia o producte, amb la finalitat d'aplicar les mesures de seguretat tècniques i organitzatives que siguin adequades quant a seguretat que requereixen els serveis, la tecnologia o els productes als quals s'aplica l'ENS-AD. Entre aquestes garanties, hi pot haver l'obligació que es tracti dels serveis, la tecnologia o els productes recollits al registre de components certificats elaborat a aquest efecte per l'ANC-AD en cada moment. El referit registre de components certificats l'elabora l'ANC-AD en funció dels criteris que consideri escaients, incloent-hi els criteris internacionalment reconeguts o aplicats per entitats homòlogues de l'ANC-AD.

En cas que una entitat essencial o important acrediti que no pot disposar de serveis o tecnologia o productes recollits al registre de components certificats referit en el paràgraf anterior, aquesta entitat pot sol·licitar a l'ANC-AD una autorització per contractar els serveis o la tecnologia o els productes que corresponguin. Aquesta sol·licitud ha d'estar degudament argumentada i ha de justificar els motius de la necessitat de disposar del servei o tecnologia o els productes que es proposen, i l'ANC-AD disposa de dos mesos per avaluar-la. En cas de manca de resolució per part de l'ANC-AD dins del termini esmentat, l'autorització s'entén denegada per silenci administratiu negatiu.

En els supòsits de processos de contractació de serveis o d'adquisició de tecnologia o productes per part de les entitats essencials i importants a les quals aplica l'ENS-AD, les dites entitats resten obligades a requerir als proveïdors la presentació d'una auditoria de seguretat externa elaborada amb una data inferior a dotze mesos respecte a la data de la presentació de les seves ofertes, la qual s'ha d'efectuar de conformitat amb els marcs reconeguts internacionalment en matèria de ciberseguretat en cada moment.

En cas que una entitat essencial o important acrediti que no pot disposar d'un proveïdor de serveis o tecnologia o productes que tingui l'auditoria referenciada en el paràgraf anterior, o que el proveïdor ja comptava amb un o diversos certificats reconeguts, pot sol·licitar a l'ANC-AD una autorització per contractar el proveïdor que correspongui. Aquesta sol·licitud ha d'estar degudament argumentada i ha de justificar els motius de la contractació que es proposa, i l'ANC-AD disposa de dos mesos per avaluar-la. En cas de manca de resolució per part de l'ANC-AD dins del termini referit, l'autorització s'entén denegada per silenci administratiu negatiu.

2. El proveïdor seleccionat per l'entitat no pot recórrer a una subcontractació (independentment que subcontracti una entitat o una persona física) sense l'autorització prèvia, per escrit, específica o general, de l'entitat a la qual presta el servei al qual s'aplica l'ENS-AD. El proveïdor ha d'informar a l'entitat a la qual presta el servei i al qual se li aplica l'ENS-AD, de qualsevol canvi previst en la incorporació o la substitució d'altres subcontractes en els quals delegui part o la totalitat de la prestació del servei contractat. 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. No obstant això, les entitats essencials i importants resten obligades a requerir a les entitats subcontractades posteriorment la presentació d'una auditoria de seguretat externa elaborada amb una data inferior a dotze mesos respecte a la data en la qual s'iniciï la subcontractació posterior. En aquests casos, també existeix la possibilitat que l'entitat essencial o important sol·liciti a l'ANC-AD l'excepció regulada a l'apartat anterior, en els supòsits en els quals s'acrediti la manca de disposició d'un proveïdor que pugui tenir aquesta auditoria.

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 que estableix, com a mínim:

- a) El nivell de seguretat i l'acord del nivell del servei que l'entitat subcontractada ha de garantir per al 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) Que es garanteix 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) Que es prendran totes les mesures necessàries en matèria de seguretat de la informació.

f) Que es respecten les condicions establertes en l'apartat 2, en recórrer a unes altres subcontractacions, i que s'obliguen a complir, mitjançant un contracte escrit, les mateixes obligacions de seguretat de la informació que s'hagin 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 subcontractació no fa que l'entitat subcontractada perdi les seves responsabilitats davant de l'entitat que presta el servei al qual s'aplica l'ENS-AD.

g) Que s'assisteix 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) Que es posa 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 l'elaboració 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.

5. Les entitats essencials i importants han de facilitar a l'ANC-AD, amb una periodicitat anual, un resum de les contractacions i subcontractacions efectuades de conformitat amb el que estableixen els apartats anteriors d'aquest article, fent referència al Registre de components certificats contractats en cada cas. Així mateix, en relació amb les auditories externes referides en els apartats anteriors d'aquest article, les entitats essencials i importants han d'informar anualment l'ANC-AD de les empreses responsables de les auditories i dels marcs estàndard utilitzats per aquestes últimes."

Article 2. *Modificació de l'article 16 del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, relatiu a l'auditoria de seguretat*

Es modifica l'article 16 del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, relatiu a l'auditoria de seguretat, que queda redactat com segueix:

"Article 16. *Auditoria de seguretat*

1. Els actius d'informació necessaris per prestar els serveis als quals s'aplica l'ENS-AD són objecte d'una auditoria externa 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. L'elaboració d'aquesta auditoria extraordinària determina la data de còmput per calcular els dos anys fixats 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 maduresa exigits.

Nivell exigit ENS-AD	Nivell mínim ENS-AD	Data límit compliment mínim ENS-AD
2,1	2	01/03/2025
3	2,6	30/09/2025
4	3,4	31/03/2027
5	4,4	31/03/2029

Taula de nivells de maduresa exigits per data

L'auditoria externa anual analitza el grau de compliment dels actius d'informació de conformitat amb els nivells establerts en aquesta guia.

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.

5. La falta d'adopció de mesures per esmenar les deficiències detectades mencionades a l'apartat 3 d'aquest article, quan aquestes deficiències suposin vulnerabilitats a incidents amb efectes perturbadors significatius, pot donar lloc a la incoació d'un expedient sancionador i a la imposició de sancions després de la instrucció prèvia de l'expedient que escaigui de conformitat amb el que estipula la Llei NIS-AD."

Article 3. *Addició d'una disposició transitòria al Reglament de l'Esquema nacional de seguretat del Principat d'Andorra*

S'addiciona una disposició transitòria al Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, que queda redactada com segueix:

"Disposició transitòria

1. Les entitats essencials i importants disposen d'un termini de divuit mesos a comptar de la data d'entrada en vigor d'aquest Reglament per adaptar-se al compliment de les obligacions, exclusivament pel que es refereix a l'exigència de l'auditoria de seguretat externa prevista per a les entitats subcontractades.

2. Així mateix, les entitats essencials i importants disposen d'un termini de divuit mesos a comptar de la data d'entrada en vigor d'aquest Reglament per complir les disposicions relatives a l'obligació d'acreditar que els serveis, les tecnologies o els productes que aquestes entitats adquireixin estan inclosos en el Registre de components certificats elaborat per l'ANC-AD."

Disposició final

Aquest Decret entra en vigor l'endemà de ser publicat al *Butlletí Oficial del Principat d'Andorra*.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 30 d'octubre del 2024

P. d. Conxita Marsol Riart

Ministra de Presidència, Economia, Treball i Habitatge