

Reglaments

Decret 416/2024, del 30-10-2024, de modificació del Decret 418/2022, del 12-10-2022, d'aprovació del Reglament d'infraestructures crítiques del Principat d'Andorra.

Exposició de motius

Des de l'aprovació del Decret 418/2022, del 12-10-2022, d'aprovació del Reglament d'infraestructures crítiques del Principat d'Andorra, com un dels mecanismes per garantir la ciberseguretat al territori 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, "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 sistemes d'informació, ha estat implementada de manera exemplificativa.

Seguint el principi de millora contínua contingut a l'article 12 de la Llei NIS-AND, exigible a les infraestructures crítiques, es considera necessària l'actualització del Reglament de les infraestructures crítiques del Principat d'Andorra, per introduir-hi exigències amb vista a oferir més garanties per millorar-les 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 cal que siguin els que l'Agència Nacional de Ciberseguretat del Principat d'Andorra (en endavant, "ANC-AD") inclou al seu Registre de components certificats.

Aquestes modificacions també afavoreixen que l'ANC-AD continuï sent el punt de referència generador de confiança digital per a les infraestructures crítiques, que representen sectors estratègics per al 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 12 del Reglament d'infraestructures crítiques del Principat d'Andorra*

Es modifica l'article 12 del Reglament d'infraestructures crítiques del Principat d'Andorra, aprovat pel Decret 418/2022, del 12-10-2022, que queda redactat com segueix:

"Article 12. *Auditories de la seguretat i garanties mínimes dels serveis o la tecnologia o els productes*

1. Les entitats crítiques i les entitats equivalents a entitats crítiques són objecte, almenys anualment, d'una auditoria externa ordinària que verifica el compliment dels requisits establerts en aquest Reglament. Amb caràcter extraordinari, ha de fer-se aquesta auditoria sempre que es produeixin modificacions substancials en les infraestructures de l'entitat inscrites en el CNIC, o en un nombre significatiu de mesures de seguretat requerides d'acord amb el PSE corresponent. Aquesta auditoria extraordinària ha de determinar la data de còmput per al càlcul de l'any per efectuar l'auditoria ordinària següent, d'acord amb el que s'indica al paràgraf anterior.

2. L'auditoria es duu a terme d'acord amb la guia d'auditoria d'infraestructures crítiques publicada per l'ANC-AD, i amb els nivells de seguretat que l'ANC-AD hagi assignat als serveis essencials que depenen de cada infraestructura crítica.

Nivell exigít RIC-AD	Nivell mínim RIC-AD	Data lí, it compliment mínim RIC-AD
2,3	2	01/03/2025
3	2,6	30/09/2025
4	3,6	31/03/2027
5	4,6	31/03/2029

Taula de nivells de maduresa exigits per data

L'auditoria externa anual analitza el grau de compliment de les entitats crítiques i les entitats equivalents a entitats crítiques 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 el RIC-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 demostren 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, i els del darrer any han d'estar a disposició, a tot tardar, el primer trimestre de l'any en curs, en l'exercici de la seva obligació de supervisió d'acord amb el que s'estableix al 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 preveu la Llei NIS-AD.

6. Garanties respecte de les subcontractacions:

a) Les entitats crítiques i les entitats equivalents a entitats crítiques han de garantir que els proveïdors subcontractats dels quals disposin tenen garanties suficients sobre els serveis subcontractats, així com sobre la provisió de qualsevol tecnologia o producte. Les entitats crítiques i les entitats equivalents a entitats crítiques resten obligades que aquests serveis, tecnologia o productes oferts constin 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.

b) En cas que una entitat crítica o entitat equivalent a entitat crítica no pugui 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 a la disposició dels serveis o tecnologia o producte que correspongui. Aquesta sol·licitud ha d'estar degudament argumentada i ha de justificar els motius de la necessitat de disposar del servei o tecnologia o producte 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 esmentat, l'autorització s'entén denegada per silenci administratiu negatiu.

c) En els supòsits de processos de contractació de serveis o d'adquisició de tecnologia o productes per part de les entitats crítiques i les entitats equivalents a entitats crítiques, aquestes entitats resten obligades a requerir als proveïdors la presentació d'una auditoria de seguretat externa elaborada amb una data inferior a divuit 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.

d) En cas que una entitat crítica o entitat equivalent a entitat crítica 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 compta 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 referit termini, l'autorització s'entén denegada per silenci administratiu negatiu.

e) No obstant això, les entitats crítiques i les entitats equivalents a entitats crítiques resten obligades a requerir a les entitats subcontractades posteriorment la presentació d'una auditoria de seguretat externa elaborada amb una data inferior a divuit mesos respecte a la data en la qual s'iniciï la subcontractació posterior. En aquest supòsit, també existeix la possibilitat que l'entitat crítica o l'entitat equivalent a entitat crítica 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.

f) Les entitats crítiques i les entitats equivalents a entitats crítiques 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 als components certificats contractats en cada cas. Així mateix, en relació amb les auditories externes esmentades en els apartats anteriors d'aquest article, les entitats crítiques i les entitats equivalents a entitats crítiques han d'informar anualment l'ANC-AD de les empreses responsables de les auditories i dels marcs estàndard utilitzats per aquestes."

Article 2. *Addició d'una disposició transitòria*

S'addiciona una disposició transitòria al Reglament d'infraestructures crítiques del Principat d'Andorra, que queda redactada com segueix:

"Disposició transitòria

1. Les entitats crítiques i les entitats equivalents a entitats crítiques 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 contingudes en aquest Reglament, 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 crítiques i les entitats equivalents a entitats crítiques disposen d'un termini de divuit mesos a comptar de la data d'entrada en vigor d'aquest Reglament per complir les obligacions contingudes en aquest Reglament 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