

Reglaments

Decret 418/2022, del 12 d'octubre del 2022

Decret 418/2022, del 12-10-2022, pel qual s'aprova el Reglament d'infraestructures crítiques del Principat d'Andorra.

Exposició de motius

L'avaluació de la protecció de les infraestructures crítiques que la Comissió Europea va dur a terme durant la primera meitat del 2019, i que va donar lloc a la proposta de la Comissió Europea COM(2020) 829 final, relativa a la resiliència de les entitats crítiques, que 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-AD") adapta a les peculiaritats del nostre país, demostra una evolució en la naturalesa de les amenaces a les quals s'enfronten les infraestructures crítiques. Algunes d'aquestes amenaces (com és el cas de les que exploten la informació privilegiada o les associades al canvi climàtic) estan evolucionant, mentre que d'altres (com les que introdueixen els vehicles aeris no tripulats o la intel·ligència artificial) són noves i, si bé és probable que la introducció d'algunes tecnologies millori la capacitat per protegir les infraestructures crítiques (com serà, per exemple, el cas del 5G a les infraestructures crítiques on fins ara no era possible una redundància en les xarxes per garantir la seguretat de les comunicacions), és igualment probable que aquestes mateixes tecnologies exacerbin vulnerabilitats preexistents o en creïn de noves. En aquest context d'increment continuat de les amenaces, canvis accelerats i incertesa, és utòpic pensar que l'esforç dedicat a la protecció de les infraestructures crítiques serà suficient per garantir la prestació dels serveis essencials amb la qualitat que requereixen.

La Llei NIS-AD assenyala la necessitat de dedicar a les entitats crítiques una atenció especial en l'àmbit de la seguretat de la informació, perquè tenen la peculiaritat d'utilitzar infraestructures necessàries per prestar serveis essencials per al Principat d'Andorra i per a les quals no hi pot haver una redundància o no es poden reemplaçar per unes altres en cas de mal funcionament. El bon funcionament del nostre país requereix exigir a aquestes entitats dos coses: d'una banda, es requereix un nivell de seguretat mínim per a totes les infraestructures que participen en la prestació dels serveis importants i essencials, regulat dins l'Esquema de seguretat nacional del Principat d'Andorra; i, d'altra banda, tenint en compte que, de manera realista, les infraestructures crítiques no poden estar completament protegides tot el temps, i per evitar l'alteració dels serveis essencials en tots els possibles casos en què un incident afecti una única infraestructura, cal que les entitats crítiques es dotin d'una capacitat de recuperació enfront d'incidents molt més grans que l'exigible a la resta d'entitats essencials que sí que compten amb solucions alternatives.

Concretament, per assolir això últim, la lletra b de l'apartat 2 de l'article 4 de la Llei NIS-AD requereix que, en el marc de l'Estratègia nacional de ciberseguretat del Principat d'Andorra, es desenvolupi i s'adopti un reglament que ha de contenir, com a mínim:

- i. Els procediments per identificar i designar infraestructures crítiques per al Principat d'Andorra.
- ii. Les condicions per a la creació d'un catàleg nacional d'infraestructures crítiques, que ha d'aglutinar totes les dades i la valoració de la criticitat de les infraestructures mencionades i que serà emprat com a base per planificar les actuacions necessàries en matèria de seguretat i protecció d'aquestes infraestructures, en nodrir-se de les aportacions dels mateixos operadors.
- iii. La regulació d'instruments de planificació per protegir les infraestructures crítiques de les entitats essencials i les entitats importants.

iv. Les obligacions per a les entitats crítiques, incloent-hi els requisits de seguretat de les comunicacions, amb la finalitat d'augmentar la seva resiliència i millorar la seva capacitat per proveir els seus serveis al Principat d'Andorra.

iv. Les normes sobre supervisió d'entitats crítiques i l'aplicació d'obligacions a les mateixes entitats.

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 d'infraestructures crítiques del Principat d'Andorra, que entra en vigor l'endemà de ser publicat al *Butlletí Oficial del Principat d'Andorra*.

Reglament d'infraestructures crítiques del Principat d'Andorra

Capítol primer. Consideracions generals

Article 1. *Objecte*

1. Aquest Reglament (en endavant, el "RIC-AD" o "el Reglament") regula l'establiment d'instruments de planificació per mesurar i millorar el nivell de protecció i resiliència de les entitats crítiques i les entitats equivalents a entitats crítiques, de conformitat amb el precepte establert a la lletra b de l'apartat 2 de l'article 4 de la Llei NIS-AD.

2. Aquest Reglament estableix el dret de les entitats crítiques a rebre de l'Agència Nacional de Ciberseguretat del Principat d'Andorra (en endavant, "l'ANC-AD") suport i orientació específics destinats a aconseguir un alt nivell de resiliència enfront de tots els riscos pertinents.

Article 2. *Definicions*

1. Els termes següents, utilitzats dins el context del RIC-AD, tenen el significat següent:

- a) ANC-AD: Agència Nacional de Ciberseguretat del Principat d'Andorra.
- b) CSIRT-AD: centre de resposta a incidents de seguretat de les xarxes i dels sistemes d'informació de referència al Principat d'Andorra.
- c) Catàleg nacional d'infraestructures crítiques (CNIC): instrument que conté la valoració i tota la informació completa, actualitzada i contrastada de les infraestructures crítiques per al Principat d'Andorra. El CNIC inclou les infraestructures crítiques de les entitats crítiques, les de les entitats equivalents a entitats crítiques i les situades fora del Principat d'Andorra.
- d) CID i DIC: tots dos són sigles de les paraules confidencialitat, integritat i disponibilitat, ordenades segons la dimensió que, en principi, té més rellevància per a la seguretat. En l'àmbit de les tecnologies de la informació és habitual utilitzar el terme CID, mentre que en l'àmbit la tecnologia d'operació se sol utilitzar el terme DIC.
- e) DSI: delegat de la seguretat de la informació, d'acord amb el que s'estableix a l'article 18 de la Llei NIS-AD.
- f) Informació sensible sobre infraestructures crítiques: dades específiques sobre infraestructures crítiques que, en cas de revelar-se, podrien utilitzar-se per planejar i dur a terme accions l'objectiu de les quals sigui provocar la pertorbació o la destrucció d'aquestes infraestructures.
- g) Pla de suport operatiu: plans elaborats pel Cos de Policia del Principat d'Andorra amb la col·laboració de les entitats crítiques i les entitats equivalents a entitats crítiques que els necessitin, per recollir les mesures de vigilància, prevenció i protecció que han d'adoptar les unitats policials en relació amb amenaces com, per exemple, la delinqüència o el terrorisme que puguin afectar les infraestructures crítiques, així com la reacció per a la qual han d'estar preparades si el risc associat a alguna d'aquestes amenaces es materialitza.

h) Seguretat: la capacitat de les xarxes i dels sistemes d'informació de resistir, amb un nivell determinat de fiabilitat, tota acció que comprometi la disponibilitat, autenticitat, integritat o confidencialitat de les dades emmagatzemades, transmeses o tractades, o els serveis corresponents oferts per les xarxes i sistemes d'informació esmentats o que són accessibles per aquests darrers.

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

Article 3. Àmbit d'aplicació

1. L'àmbit d'aplicació d'aquest Reglament s'estén a les infraestructures crítiques de les entitats crítiques i les entitats equivalents a entitats crítiques, a aquestes entitats i a les autoritats competents, d'acord amb les definicions que s'inclouen a l'article 3 de la Llei NIS-AD.

2. Addicionalment, i només a l'efecte de col·laboració amb l'ANC-AD d'acord amb el que s'estableix a l'article 4 i a l'article 7 d'aquest Reglament, s'inclouen en el seu àmbit d'aplicació les entitats essencials els serveis essencials de les quals depenen d'infraestructures crítiques.

3. Finalment, i només als efectes del que s'estableix a l'article 11 d'aquest Reglament, s'inclou en el seu àmbit d'aplicació el Cos de Policia del Principat d'Andorra.

Capítol segon. Procediments per a la identificació i la designació d'infraestructures crítiques

Article 4. Identificació d'infraestructures crítiques

1. Les autoritats competents designades a l'article 6 de la Llei NIS-AD proposen les infraestructures crítiques en funció dels resultats de la seva avaluació dels riscos que poden afectar els serveis essencials de la seva competència, d'acord amb els seus criteris sectorials, com ara la durada permesa per a les pertorbacions o el temps de recuperació.

2. Per dur a terme la proposta d'infraestructures crítiques esmentada a l'apartat anterior, les autoritats competents poden comptar amb la participació i l'assessorament tècnic de les entitats essencials dels sectors de la seva competència, les quals han de col·laborar en la valoració i la descripció de les infraestructures que gestionen o de les quals depenen.

3. L'ANC-AD és responsable d'identificar les infraestructures crítiques en la prestació dels serveis essencials per al Principat d'Andorra, per a la qual cosa aplica els criteris de criticitat horitzontals adients en cada moment, com ara les possibles víctimes, l'impacte econòmic i l'impacte públic, sobre la proposta d'infraestructures crítiques a què es refereixen els apartats 1 i 2 anteriors.

Article 5. Designació d'entitats crítiques i entitats equivalents a entitats crítiques

1. L'ANC-AD és responsable d'aprovar la designació d'una entitat com a entitat crítica o entitat equivalent a entitat crítica.

2. Per designar una entitat com a entitat crítica o entitat equivalent a entitat crítica, d'acord amb les definicions d'ambdós conceptes que ofereix l'article 3 de la Llei NIS-AD, n'hi ha prou que almenys una de les infraestructures situades al territori del Principat d'Andorra gestionades per aquesta entitat tingui la consideració d'infraestructura crítica identificada d'acord amb el que s'estableix a l'article 4 d'aquest Reglament.

3. L'ANC-AD s'assegura que l'autoritat competent corresponent, o ella mateixa, notifiqui a aquestes entitats que han estat identificades com a entitats crítiques o equivalents a crítiques en el termini d'un mes després d'aquesta identificació, i les informa de les seves obligacions d'acord amb la Llei NIS-AD i aquest Reglament, així com de la data a partir de la qual els són aplicables les disposicions que estableixen la Llei NIS-AD i el RIC-AD respecte a les obligacions mencionades.

Article 6. *Designació d'infraestructures crítiques estrangeres*

1. L'ANC-AD és responsable d'aprovar la designació de les infraestructures crítiques per al Principat d'Andorra, identificades en aplicació dels criteris enumerats a l'article 4 d'aquest Reglament, que estiguin situades a l'estranger, a proposta de les autoritats competents designades a l'article 6 de la Llei NIS-AD.

2. L'ANC-AD es comunica amb les agències nacionals que escaigui dels països en els quals es trobin les infraestructures crítiques designades d'acord amb el que s'estableix a l'apartat anterior, per tal de recollir la informació necessària per incloure aquestes infraestructures al Catàleg nacional d'infraestructures crítiques i coordinar els procediments de notificació d'amenaques i incidents que afectin aquestes infraestructures crítiques per al Principat d'Andorra, i acordar plans de comunicació i d'actuació conjunta.

Capítol tercer. Catàleg nacional d'infraestructures crítiques**Article 7.** *Catàleg nacional d'infraestructures crítiques*

1. El Catàleg nacional d'infraestructures crítiques (d'ara endavant, "el CNIC" o "el Catàleg") és el registre de caràcter administratiu que conté informació completa, actualitzada i contrastada de les infraestructures crítiques designades conforme a l'article 5 i l'article 6 d'aquest Reglament, que suporten serveis essencials per al Principat d'Andorra. El Catàleg:

a) Conté, entre altres dades, les relatives a la descripció de les infraestructures, la seva ubicació, l'administració i la titularitat (incloent-hi si es tracta d'una entitat crítica, una entitat equivalent a una entitat crítica o una entitat estrangera que gestiona una infraestructura crítica per la prestació d'un servei essencial al Principat d'Andorra), els serveis que presten, els mitjans de contacte, el nivell de seguretat que necessiten en funció dels riscos avaluats i el pla de seguretat de l'entitat, així com la informació obtinguda de les forces i els cossos de seguretat.

b) És secret, i la informació sensible sobre infraestructures crítiques s'hi inclou únicament quan sigui necessària per a la finalitat principal del Catàleg i es limita a aquella que sigui pertinent i proporcionada per a aquestes finalitats, i cal preservar-ne la confidencialitat i protegir-la d'interessos aliens als previstos per al CNIC.

c) Les xarxes i els sistemes d'informació que allotgin el Catàleg i hi donin accés, i la informació continguda en el Catàleg, comptaran amb les mesures de seguretat necessàries que en garanteixin la confidencialitat, integritat i disponibilitat (CID) o la disponibilitat, integritat i confidencialitat (DIC), depenent en cada cas de la tipologia de l'entitat, d'acord amb els requisits de seguretat establerts en l'Esquema nacional de seguretat del Principat d'Andorra per al nivell de seguretat alt.

2. La finalitat principal del Catàleg és valorar i gestionar les dades disponibles de les diferents infraestructures crítiques, amb l'objectiu de dissenyar els mecanismes de planificació, prevenció, protecció i reacció davant una eventual amenaça contra les dades i, en cas de ser necessari, activar, conforme al que es preveu en el Pla de les infraestructures crítiques del Principat d'Andorra mencionat en l'article 8 d'aquest Reglament, una resposta àgil, oportuna i proporcionada, d'acord amb el nivell i les característiques de l'amenaça de què es tracti.

3. La competència per classificar una infraestructura com a crítica, així com per incloure-la en el Catàleg, correspon a l'ANC-AD. Així:

a) Correspon a l'ANC-AD efectuar les altes, baixes i modificacions d'infraestructures crítiques en el Catàleg, així com determinar el nivell de seguretat que requereixen. Per complir aquest punt, l'ANC-AD pot comptar amb la participació i l'assessorament de l'entitat que allotja la infraestructura crítica.

b) A l'efecte de determinar el nivell de seguretat de cada infraestructura crítica, l'ANC-AD pot sol·licitar a les entitats essencials que en depenen la seva pròpia anàlisi de riscos dels serveis essencials afectats per la infraestructura crítica.

4. El CNIC és custodiat, gestionat i mantingut per l'ANC-AD, i es nodreix de la informació que faciliten a l'ANC-AD tant les entitats crítiques i equivalents a entitats crítiques com les entitats essencials que depenen

d'infraestructures crítiques ubicades a l'estranger, i ha d'actualitzar-se amb una periodicitat anual i, en tot cas, a requeriment de l'ANC-AD i sempre que es produeixi una modificació rellevant que afecti les infraestructures inscrites del Catàleg i que sigui d'interès als efectes previstos en aquest Reglament.

Capítol quart. Instruments de planificació de la protecció i la millora de la resiliència de les infraestructures crítiques

Article 8. *El Pla de les infraestructures crítiques del Principat d'Andorra*

1. El Pla de les infraestructures crítiques del Principat d'Andorra (en endavant, "PIC-AD") és un compendi de documents, la majoria confidencials, que descriuen com s'ha d'organitzar el país, controlar, motivar, liderar i prendre decisions per aconseguir els objectius de protecció i resiliència d'infraestructures crítiques per als serveis essencials per al Principat d'Andorra que estableixi l'Estratègia de ciberseguretat del Principat d'Andorra, descrita l'article 4 de la Llei NIS-AD. El PIC-AD:

- a) Estableix els criteris i les directrius precises per articular les mesures preventives necessàries per assegurar, de forma actualitzada i homogènia, la protecció permanent i la resiliència de les infraestructures crítiques que formen part del CNIC enfront de les amenaces provinents d'atacs deliberats contra elles.
- b) Preveu diferents nivells de seguretat i intervenció de les forces i els cossos de seguretat, que s'han d'activar, en cada cas, en funció dels resultats de l'avaluació del nivell i del tipus de l'amenaça a què en cada moment s'enfrontin les infraestructures crítiques que formen part del CNIC.
- c) S'ha d'actualitzar com a mínim amb cada edició nova de l'Estratègia de ciberseguretat del Principat d'Andorra i, si escau, quan resulti necessari modificar alguna de les dades o instruccions incloses en el pla.

2. L'ANC-AD és responsable de:

- a) Coordinar l'elaboració, sense dilació indeguda, de cada proposta de PIC-AD que consideri necessària la mateixa ANC-AD, la secretaria d'Estat a la qual s'adscriu o el Comitè Especialitzat de Seguretat descrit a l'article 10 del Decret 346/2021, del 20 d'octubre del 2021, de creació de l'Agència Nacional de Ciberseguretat i de l'Equip de Resposta de Referència del Principat d'Andorra per al tractament d'incidents de seguretat de les xarxes i els sistemes d'informació.
- b) Custodiar els documents que formen el PIC-AD i controlar-hi l'accés d'acord amb els nivells de seguretat associats als seus continguts, fins i tot mentre es creen o modifiquen.
- c) Executar el PIC-AD.
- d) Monitorar i controlar l'execució del PIC-AD.
- e) Coordinar l'anàlisi de les propostes de canvis que en cada moment pugui requerir el PIC-AD.

3. L'ANC-AD és responsable d'aprovar totes les versions del PIC-AD.

Article 9. *Plans estratègics sectorials*

1. Els plans estratègics sectorials del Principat d'Andorra (en endavant, "els PES-AD") descriuen, en cadascun dels sectors essencials de l'annex I de la Llei NIS-AD, quins són els serveis essencials proporcionats a la societat dins el sector que cobreix el PES-AD corresponent, el funcionament general d'aquests serveis, els seus riscos, les infraestructures crítiques per garantir la prestació de cada servei essencial amb la qualitat requerida, les conseqüències potencials de la materialització dels riscos identificats per a cada servei essencial i les mesures tècniques i organitzatives que, d'acord amb el PIC-AD i amb el que sigui específic del servei essencial corresponent, sigui necessari implantar per a la protecció i la resiliència de les infraestructures crítiques de les quals depenen.

2. L'ANC-AD, amb la col·laboració de l'Autoritat Financera Andorrana pel que fa al seu àmbit competencial de conformitat amb el que s'estableix en la Llei NIS-AD, i tenint en compte l'avaluació de riscos que d'acord amb l'apartat 4.b de l'article 6 de la Llei NIS-AD ha de fer per a cada servei essencial, és responsable de:

- a) Crear sense dilació indeguda els PES-AD de cada sector essencial.

b) Custodiar els documents que formen cada PES-AD i controlar-hi l'accés d'acord amb els nivells de seguretat associats als seus continguts, fins i tot mentre es creen o modifiquen.

c) Executar els PES-AD.

d) Monitorar i controlar l'execució de cada PES-AD.

e) Adequar els PES-AD com correspongui a la realitat del sector corresponent en cada moment i als plans de seguretat de les infraestructures crítiques dels quals depengui cada sector.

3. Per dur a terme els PES-AD, l'ANC-AD pot comptar amb la participació i l'assessorament tècnic de les entitats crítiques i les entitats equivalents a entitats crítiques.

Article 10. *Pla de seguretat de l'entitat*

1. El Pla de seguretat de l'entitat (en endavant, "PSE") és el conjunt de documents estratègics definidors de les polítiques generals d'una entitat crítica o una entitat equivalent a entitat crítica per garantir la protecció i la resiliència de les infraestructures crítiques que posseeix o gestiona. El PSE ha de contenir com a mínim els documents següents:

a) La política general de seguretat de l'entitat, que inclou, com a mínim:

i. La descripció de les infraestructures crítiques compartida amb l'ANC-AD per incloure-les al CNIC.

ii. Els procediments de gestió i manteniment de la seguretat.

iii. Els procediments establerts per a la comunicació i l'intercanvi d'informació relativa a la protecció d'infraestructures crítiques.

iv. La metodologia d'anàlisi de risc (amenaces físiques i de ciberseguretat).

v. L'estructura de govern de la seguretat de l'entitat juntament amb la descripció de les funcions i les responsabilitats de cada rol de l'organigrama corresponent.

vi. Les dades de contacte del seu DSI, o de l'equivalent en el cas d'entitats equivalents a entitats crítiques, i dels DSI de les entitats que presten els serveis essencials que depenen d'aquestes darreres, així com de les persones que els substituïran quan no estiguin disponibles.

b) La relació de serveis essencials que depenen de cadascuna de les infraestructures crítiques que posseeix o gestiona l'entitat.

c) La relació de dependències de cada infraestructura crítica amb altres infraestructures crítiques posseïdes o gestionades per la mateixa entitat o una altra entitat.

d) El resultat de l'anàlisi de risc de cadascuna de les infraestructures crítiques posseïdes o gestionades per l'entitat.

e) L'inventari dels serveis subcontractats que puguin impactar de qualsevol manera en les infraestructures crítiques. Per a cadascun d'aquests serveis, juntament amb la descripció del possible impacte i la descripció del servei subcontractat, s'ha d'identificar l'entitat subcontractada, els certificats que té en matèria de seguretat i la seu des de la qual presta el servei subcontractat, així com els nivells de servei acordats. D'igual forma, s'ha de descriure la metodologia mitjançant la qual es duu a terme la comprovació del compliment per part de l'entitat crítica o equivalent a entitat crítica dels protocols de seguretat implementats en el seu cas.

f) La relació de mesures tècniques i organitzatives (inclosos els procediments d'alertes i de gestió de crisi) que es consideren adequades i proporcionades per garantir la seguretat i resiliència de cada infraestructura crítica, documentades amb un nivell de detall suficient per aconseguir els objectius de l'entitat, tenint en compte els riscos detectats. S'ha d'indicar quines d'aquestes mesures són permanents, i quines són graduals i només s'activaran a partir d'un determinat nivell de risc i d'amenaça.

g) La relació de mesures tècniques i organitzatives que ja estan implementades o preparades per activar-se en cada infraestructura crítica, fent referència, si escau, a les esmentades en el punt anterior.

2. S'autoritza l'ANC-AD a ampliar el contingut mínim dels PSE per a alguna o totes les entitats o equivalents a entitats crítiques.

3. L'òrgan de direcció de l'entitat, si escau, amb la col·laboració del seu DSI, és responsable de:

- a) Crear sense dilació indeguda el PSE de l'entitat.
- b) Custodiar els documents que formen el seu PSE i controlar-hi l'accés d'acord amb els nivells de seguretat associats als seus continguts, fins i tot mentre es creen o modifiquen.
- c) Executar el PSE.
- d) Monitorar i controlar l'execució del PSE.
- e) Adequar el PSE com correspongui a la seva realitat i a les directrius que rebi de la seva autoritat competent o de l'ANC-AD.
- f) Posar el PSE a disposició de l'autoritat competent corresponent.
- g) Comunicar cada nova versió del PSE a l'ANC-AD sense demora indeguda i, en qualsevol cas, en el termini màxim d'una setmana a comptar de l'endemà de l'aprovació del PSE, i amb independència de les circumstàncies que hagin donat lloc a la nova versió i de si els documents han estat o no objecte de modificacions.
- h) Comunicar a l'ANC-AD, sense dilació indeguda, l'adopció de qualsevol mesura de seguretat que no s'hagi inclòs en el PSE per tenir naturalesa temporal.

4. L'ANC-AD és responsable d'aprovar els PSE de les entitats crítiques i les entitats equivalents a entitats crítiques i, si escau, de proposar actualitzacions per a aquests plans.

Article 11. *Plans de suport operatiu*

1. El Cos de Policia del Principat d'Andorra, a instància de l'ANC-AD, és l'encarregat de dissenyar el pla de suport operatiu que requereixi cada infraestructura crítica del CNIC, i n'assumeix la responsabilitat.

2. Aquests plans preveuen les mesures de vigilància, prevenció, protecció o reacció que s'han d'aplicar, de manera complementària a les previstes per les mateixes entitats crítiques i entitats equivalents a entitats crítiques.

Capítol cinquè. Auditoria d'infraestructures crítiques

Article 12. *Auditoria de la seguretat*

1. Les entitats crítiques i les entitats equivalents a entitats crítiques són objecte, almenys anualment, d'una auditoria interna 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 el nivell més alt dels nivells de seguretat que les entitats essencials hagin assignat als serveis essencials que depenen de cada infraestructura crítica.

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, com a molt tard, 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.

Article 13. *Incidents de ciberseguretat*

1. En cas d'incident de ciberseguretat de nivell mitjà o alt, l'entitat crítica o equivalent a entitat crítica està obligada a proporcionar totes les dades i proves de l'incident que li requereixin l'ANC-AD, el CSIRT-AD o el Cos de Policia del Principat d'Andorra.

2. Les entitats crítiques i equivalents a entitats crítiques estan obligades a notificar els seus incidents de seguretat d'acord amb el que s'estableix en la Llei NIS-AD per al cas d'entitats essencials.

Disposició addicional primera. Suport, orientació i exercicis

L'ANC-AD, en col·laboració amb el CSIRT-AD i la Universitat d'Andorra, entre altres entitats, desenvolupa materials i metodologies d'orientació, dona suport a l'organització d'exercicis per comprovar la resiliència de les entitats crítiques i proporciona formació al seu personal.

Adicionalment, l'ANC-AD, en col·laboració amb el CSIRT-AD, assessora les entitats crítiques en el compliment de les seves obligacions i ha d'emprendre, quan ho consideri necessari, activitats de suport destinades a facilitar el compliment d'aquestes obligacions.

Disposició addicional segona. Actes delegats

A fi de tenir en compte els nous riscos, els avenços tecnològics o les especificitats d'un o diversos sectors o entitats, es deleguen en l'ANC-AD les competències necessàries per definir, mitjançant l'especificació de normes que han de ser prèviament aprovades per l'ANC-AD, mesures de resiliència de compliment obligatori per les entitats crítiques i les entitats equivalents a entitats crítiques, així com per descriure en major mesura algunes d'aquestes mesures o totes elles amb l'objectiu de garantir-ne l'aplicació efectiva i coherent.

Disposició final. Competències en matèria de protecció civil

El que es disposa en aquest Reglament s'entén sense perjudici del que estableixi la normativa del Principat d'Andorra en matèria de protecció civil.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 12 d'octubre del 2022

Xavier Espot Zamora
Cap de Govern