CONSELL GENERAL

Lleis

Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació

Atès que el Consell General en la seva sessió del dia 9 de juny del 2022 ha aprovat la següent:

Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació

Dipòsit legal: AND.2-2015

Exposició de motius

És crucial per al nostre país aprofitar tots els avantatges de l'era digital per potenciar el nostre creixement econòmic i reforçar la nostra capacitat d'innovació, dins dels límits segurs i ètics que defineixen conjuntament aquesta Llei, els reglaments que la desenvolupin i la resta de marcs normatius que determini l'Agència Nacional de Ciberseguretat del Principat d'Andorra.

L'enclavament geopolític del Principat d'Andorra, la nostra consciència situacional, la creixent dependència que la nostra economia té de les xarxes i dels sistemes d'informació nacionals i transfronterers, les possibles sinergies en la prevenció d'amenaces i en els desafiaments que suposaran els ciberincidents, i l'anàlisi que s'ha realitzat en relació a les normatives necessàries per regular la correcta transformació digital que s'està projectant per al nostre país, comporten la necessitat d'aproximar les nostres capacitats en matèria de ciberseguretat a les que la Unió Europea exigeix als seus estats membres a través de la seva Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, del 6 de juliol del 2016, relativa a las mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i dels sistemes d'informació a la Unió. Aquesta Llei es basa en l'esmentada directiva, i l'adapta conforme a les particularitats del Principat d'Andorra i a l'experiència que la mateixa Unió Europea ha compilat en relació a la necessitat de reduir la càrrega normativa per als organismes competents i els costos per a les entitats públiques i privades a les que aplica aquesta normativa, prenent en consideració allò que estableix la Proposta de la Comissió Europea COM (2020) 823 final, relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat, la qual proposa la derogació de la referida Directiva (UE) 2016/1148.

Per les mateixes raons esmentades a l'inici del paràgraf anterior, ens és igualment necessari dedicar encara més atenció a les entitats crítiques, enteses com aquelles que, a més de proveir un servei essencial per al Principat d'Andorra, tenen la peculiaritat d'utilitzar una infraestructura que no es pot redundar o reemplaçar per una altra en cas de mal funcionament. El bon funcionament del nostre país requereix exigir a aquestes entitats dues coses: un nivell de protecció mínim per a les denominades infraestructures crítiques, i que es dotin d'una capacitat de recuperació enfront d'incidents en aquest tipus d'infraestructures, molt major que l'exigible a les entitats essencials que sí que compten amb solucions alternatives, per evitar l'alteració del servei essencial en tots els possibles casos en què un incident afecti una única infraestructura. És per tot això que, addicionalment a l'esmentat en el paràgraf anterior, aquesta Llei adapta a les particularitats

Dipòsit legal: AND.2-2015

del Principat d'Andorra la Directiva (UE) 2008/114/CE del Consell, del 8 de desembre del 2008, sobre la identificació i designació d'infraestructures crítiques europees i l'avaluació de la necessitat de millorar-ne la seva protecció, i s'adequa igualment a les lliçons apreses per la Unió Europea en relació a la necessitat d'ampliar el focus en la protecció d'aquestes infraestructures crítiques, amb l'objectiu d'aconseguir la major i més ràpida recuperació de l'entitat que gestiona la infraestructura crítica si les mesures de protecció fallen, lliçons que estan recopilades en la Proposta de Directiva del Parlament europeu i del Consell COM(2020) 829 final, relativa a la resiliència de les entitats crítiques.

Mitjançant aquesta Llei, s'estableixen les obligacions de definir, implementar, i evolucionar una estratègia nacional de ciberseguretat, de gestionar els riscos de ciberseguretat, d'incrementar la cooperació amb altres estats, especialment els propers, i de millorar la ciberresiliència de les entitats públiques i privades que resulten "essencials" o "crítiques" per prestar o tenir el potencial de prestar serveis fonamentals per a l'economia i la societat andorranes en l'àmbit de vuit sectors digitalitzats o en vies de digitalització (energia, transport, banca, infraestructures dels mercats financers, sanitat, aigües potables, residuals i superficials, infraestructures digitals, i administració pública), i de determinades entitats "importants" que operen en altres sectors no essencials però considerats importants (serveis postals i de missatgeria; gestió de residus; fabricació, producció, distribució i comercialització de substàncies i mescles químiques; producció, transformació i distribució d'aliments; i fabricació i prestadors de serveis digitals), i s'exigeix que el nostre país garanteixi que les nostres entitats essencials i importants, ja siguin de naturalesa pública o privada, comptin amb requisits en matèria de ciberseguretat i notifiquin els incidents que pateixin en relació amb aquesta matèria.

Igual que estan fent cada cop més les normatives en matèria de protecció de dades personals i les que regulen els actius digitals, aquesta Llei canvia el paradigma del repartiment de rols i responsabilitats entre les autoritats de control i les entitats incloses en els seus àmbits d'actuació. La creixent transformació digital ha demostrat ineficient el model d'autoritat de control que pretén definir i imposar les mesures tècniques i organitzatives amb les quals s'hauria de reduir l'exposició de tot tipus d'entitats als riscos que tenen el seu origen en els ciberincidents. Per poder preveure l'enorme diversitat de riscos de les ciberincidències i adequar-se a la velocitat amb què canvien tant aquests riscos com les mesures que han d'implantar les entitats, és necessari adoptar una aproximació de responsabilitat descentralitzada. Aquesta Llei estableix, per tant, que sigui cada entitat essencial o important la que quedi obligada demostrar la seva responsabilitat proactiva en la identificació i gestió dels riscos per als serveis que la classifiquen com a essencial o important, de forma proporcionada en relació amb els riscos que presenten les xarxes i els sistemes d'informació que utilitza i tenint en compte l'estat de la tècnica. Són doncs aquestes entitats, independentment de si s'encarreguen elles mateixes del manteniment de les seves xarxes i sistemes d'informació o l'externalitzen, les que es responsabilitzen de determinar els seus propis requisits de seguretat i d'implantar les mesures tècniques i organitzatives que elles mateixes considerin necessàries i suficients per reduir el seu risc de patir ciberincidències greus, fins a un nivell que l'autoritat de control consideri suficient, sobre la base d'uns criteris definits i les que queden obligades a notificar molt ràpidament els seus incidents de ciberseguretat per, entre d'altres raons, evitar la seva propagació i que altres entitats puguin beneficiar-se tant de l'alerta com de les lliçons apreses. I, fins i tot, són les pròpies entitats les que queden obligades a informar els seus usuaris quan aquesta informació pugui reduir el risc de la ciberamenaça per a aquests. En aquest nou paradigma, el paper de l'autoritat de control deixa de ser el de reguladora que dicta mesures suposadament eficients per al conjunt dels sectors i activitats i passa a ser, principalment, el de supervisora de la responsabilitat proactiva de les entitats, amb capacitat per sancionar-les amb, entre d'altres, multes administratives que han de ser efectives, proporcionades i dissuasives, i per, fins i tot, imposar prohibicions temporals per a què determinades persones físiques exerceixin funcions de direcció.

Aquesta nova aproximació s'ha mostrat més eficient que la del regulador clàssic per minimitzar el cost total dels ciberincidents, resultant de sumar els costos associats al compliment de la normativa i els costos associats als danys i perjudicis econòmics i socials que causen els ciberincidents. Així, la seva ràpida i adequada implantació és estrictament necessària per aconseguir els objectius específics de transformació digital del Principat d'Andorra de manera satisfactòria.

Dipòsit legal: AND.2-2015

Aquesta Llei es divideix en un total de quatre títols i dos annexos, en els quals s'hi estableix el seu objecte, àmbit d'aplicació i definicions, el marc estratègic i institucional, les obligacions tant per a les entitats essencials, siguin o no crítiques i importants, com per a les autoritats de control competents i l'equip de referència de resposta del Principat d'Andorra per al tractament d'incidents de ciberseguretat, el règim sancionador, els sectors a considerar per a la identificació d'entitats essencials i els sectors a considerar per a la identificació d'entitats importants

Així mateix, aquesta Llei inclou una disposició addicional i quatre disposicions finals.

La disposició addicional encomana al Govern que, en el termini màxim de divuit mesos, avaluï la conveniència de constituir o no una entitat amb personalitat jurídica pròpia que assumeixi funcions diverses en matèria de digitalització, o relacionades amb aquesta matèria, incloent-hi l'Agència Nacional de Ciberseguretat del Principat d'Andorra (ANC-AD) i l'equip de referència de resposta del Principat d'Andorra per al tractament d'incidents de ciberseguretat (CSIRT-AD).

Pel que fa a les disposicions finals, la primera modifica la Llei 31/2021, del 22 de novembre, de text consolidat qualificada de seguretat pública, modificada per la Llei 4/2022, del 31 de gener, del pressupost per a l'exercici del 2022, especialment per a l'establiment de mesures en cas que el funcionament de les entitats essencials o importants així ho requereixi. Les altres tres disposicions finals, són relatives al desenvolupament reglamentari, la iniciativa de presentar la consolidació d'un text legal i l'entrada en vigor de la Llei.

Títol I. Disposicions generals

Article 1. *Objecte*

1. Aquesta Llei té com a objecte regular el reforç de la resiliència de les entitats crítiques i la seguretat de les xarxes i dels sistemes d'informació utilitzats per a la prestació de serveis essencials i importants al Principat d'Andorra.

2. Per a l'assoliment del seu objecte, aquesta Llei estableix, principalment:

a) Els requisits per a la protecció dels serveis essencials i dels serveis importants, les obligacions de gestió de riscos i d'incidents de ciberseguretat per part de les entitats prestadores d'aquests serveis, i els mecanismes de supervisió del seu compliment, inclòs un sistema de notificació d'incidències;

b) L'obligació de les autoritats nacional competents d'identificar les entitats crítiques i les entitats que han de ser tractades com a equivalents a entitats crítiques en certs aspectes, perquè sense prestar els serveis essencials elles mateixes sí que poden impactar-los;

c) L'obligació de les entitats crítiques d'adoptar determinades mesures, establertes reglamentàriament, destinades a garantir la prestació de serveis essencials;

d) Un marc per a l'elaboració d'un catàleg nacional d'entitats essencials per a la seguretat de les xarxes i dels sistemes d'informació; i

e) Un marc institucional per a l'aplicació de l'Estratègia Nacional de Seguretat de les xarxes i dels sistemes d'informació.

3. El que es disposa en aquesta Llei s'entén sense perjudici de les accions que es puguin emprendre per part de les autoritats públiques corresponents per salvaguardar i garantir la seguretat nacional i les funcions essencials, per protegir la informació reservada d'Estat o la revelació de la qual sigui contrària als interessos essencials del Principat d'Andorra o per al manteniment de l'ordre públic, la detecció, investigació i persecució dels delictes, i l'enjudiciament dels seus autors.

Article 2. *Àmbit d'aplicació*

1. Aquesta Llei s'aplica a les entitats públiques i privades previstes en el marc de les entitats essencials i importants d'acord amb la seva definició a l'article 3, que ocupen a 50 o més persones o que el volum anual de negocis de les quals o el seu balanç general anual supera els deu milions d'euros.

Dipòsit legal: AND.2-2015

2. Addicionalment, aquesta Llei s'aplica a les entitats essencials i importants amb independència de la seva grandària i volum anual de negoci o balanç general anual, quan:

a) els serveis siguin prestats per una de les següents tipologies d'entitats incloses en el sector d'infraestructures digitals de l'Annex I:

i. xarxes públiques de comunicacions electròniques o serveis de comunicacions electròniques disponibles per al públic,

ii. proveïdors de serveis de confiança, i

iii. registres de noms de domini de primer nivell i proveïdors de serveis de sistema de noms de domini (DNS).

b) l'entitat sigui una entitat de l'administració pública tal com es defineix a l'article 3.12;

c) l'entitat sigui l'únic prestador d'un servei al Principat d'Andorra;

d) una possible pertorbació del servei prestat per l'entitat pogués tenir repercussions sobre la seguretat pública, l'ordre públic o la salut pública;

e) una possible pertorbació del servei proveït per l'entitat pogués induir riscos sistèmics, en particular per als sectors en els quals tal pertorbació podria tenir repercussions de caràcter transfronterer;

f) l'entitat sigui crítica en vista de la seva importància específica a nivell nacional o comunal per al sector o tipus de servei en concret o per a altres sectors interdependents al Principat d'Andorra; o

g) l'entitat s'identifiqui com a entitat crítica o com una entitat equivalent a una entitat crítica reglamentàriament.

3. Els reglaments i les altres eventuals normes i actes jurídics de caràcter sectorial en relació amb aquesta Llei que prevegin disposicions relatives a la gestió dels riscos de les tecnologies de la informació i la comunicació (TIC), la gestió o notificació dels incidents associats a les TIC, les proves de la resiliència operativa digital, els mecanismes d'intercanvi d'informació, i el risc de tercers relacionat amb les TIC, que tinguin un efecte almenys equivalent al de les obligacions establertes en aquesta Llei, s'aplicaran de forma prioritària a les entitats essencials i importants incloses en l'àmbit d'aplicació dels dits reglaments, normes i actes jurídics.

4. L'establert en l'apartat anterior s'entén sense perjudici del deure de notificació d'incidents establert a l'article 15, en la mesura que no sigui incompatible amb la normativa sectorial de què es tracti.

Article 3. *Definicions*

A l'efecte d'aquesta Llei, s'entén per:

1. **AFA**: Autoritat Financera Andorrana.

2. **ANC-AD**: Agència Nacional de Ciberseguretat del Principat d'Andorra.

3. **APDA**: Agència Andorrana de Protecció de Dades.

4. **Avaluació de riscos**: una metodologia per determinar la naturalesa i l'abast d'un risc mitjançant l'anàlisi d'amenaces i perills potencials, i l'avaluació de les condicions de vulnerabilitat existents que podrien pertorbar les operacions de l'entitat crítica.

5. **Ciberamenaces**: una circumstància, un esdeveniment o una acció potencial capaç de danyar, interrompre o afectar de manera adversa les xarxes i els sistemes d'informació, així com els seus usuaris i altres parts interessades.

6. **Ciberseguretat**: les activitats necessàries per a la protecció de les xarxes i els sistemes d'informació, dels seus usuaris i d'altres afectats per les ciberamenaces.

7. **CSIRT**: centre de resposta a incidents de seguretat de les xarxes i dels sistemes d'informació.

8. **CSIRT-AD**: CSIRT de referència del Principat d'Andorra.

Dipòsit legal: AND.2-2015

9. DNS, o Sistema de Noms de Domini: un sistema de noms distribuït jeràrquicament que permet als usuaris finals accedir als serveis i recursos d'Internet.

10. Entitat: tota persona física o jurídica constituïda i reconeguda com a tal en virtut del dret nacional del seu lloc d'establiment i que, actuant en nom propi, pot exercir drets i estar subjecta a obligacions.

11. Entitat crítica: una entitat que proporciona un o més serveis essencials la prestació dels quals depèn d'una o més infraestructures crítiques situades al Principat d'Andorra.

12. Entitat de l'administració pública: una entitat del Principat d'Andorra que compleix els següents criteris:

a) s'ha creat per satisfer necessitats d'interès general i no té caràcter industrial o mercantil;

b) està dotada de personalitat jurídica;

c) està majoritàriament finançada pel Govern d'Andorra, els Comuns o entitats de dret públic; o bé, la gestió de la qual es troba sotmesa a un control per part d'aquestes administracions o entitats; o els òrgans d'administració, de direcció o de supervisió de la qual estan composats per membres que, més de la meitat són nomenats pel Govern d'Andorra, els Comuns o entitats de dret públic; i.

d) presta un servei públic.
Queden excloses les entitats de l'administració pública que realitzen activitats en els àmbits de la seguretat pública, la policia, la defensa o la seguretat nacional.

13. Entitat de registre de noms de domini de primer nivell: una entitat en la qual s'ha delegat un domini de primer nivell específic i que és responsable d'administrar aquest domini, inclòs el registre de noms de domini en el de primer nivell i el funcionament tècnic del domini d'aquest nivell, en particular l'explotació dels seus servidors de nom, el manteniment de les seves bases de dades i la distribució dels arxius de zona del domini de primer nivell entre els servidors de nom.

14. Entitat equivalent a entitat crítica: tota entitat que sense ser crítica gestiona una o més infraestructures crítiques situades al Principat d'Andorra.

15. Entitat essencial: tota entitat de l'administració pública o privada, que ofereix un servei essencial d'acord amb la definició de l'apartat 35.

16. Entitat important: tota entitat de l'administració pública o privada que ofereix un servei important d'acord amb la definició de l'apartat 36.

17. Estratègia Nacional de Ciberseguretat: marc coherent del Principat d'Andorra que estableix prioritats i objectius estratègics en matèria de seguretat de les xarxes i dels sistemes d'informació al país.

18. Gestió d'incidents: conjunt de mesures i procediments destinats a detectar, analitzar i limitar un incident i respondre davant aquest.

19. Gestió de riscos: procés de planificar la gestió de riscos, i conjunt d'activitats orientades a identificar, analitzar, respondre, monitorar i controlar els riscos.

20. Incident: qualsevol esdeveniment que pugui pertorbar o que pertorbi les operacions d'una entitat, o que comprometi la disponibilitat, autenticitat, integritat o confidencialitat de les dades emmagatzemades, transmeses o tractades, o els serveis corresponents oferts per xarxes i sistemes d'informació o accessibles per mitjà d'aquests.

21. Infraestructura: un actiu, sistema o part d'aquest, necessari per a la prestació d'un servei essencial.

22. Infraestructures crítiques: infraestructures que són indispensables i no permeten solucions alternatives, pel que la seva pertorbació o destrucció, tindria efectes perjudicials significatius sobre la prestació d'un o més serveis essencials.

23. Mercat en línia: un servei digital que permet als consumidors celebrar contractes a distància mitjançant una interfície en línia.

Dipòsit legal: AND.2-2015

24. Motor de cerca en línia: un servei digital que permet als usuaris introduir consultes per fer recerques, en principi, de tots els llocs web, o de llocs web en un idioma concret, mitjançant una consulta sobre un tema qualsevol en forma de paraula clau, consulta oral, frase o un altre tipus d'entrada i que, en resposta, mostra resultats en qualsevol format en què pot trobar-se informació relacionada amb el contingut sol·licitat.

25. Òrgan de direcció: l'òrgan o òrgans d'administració de l'entitat nomenats de conformitat amb el dret nacional, facultats per fixar l'estratègia, els objectius i l'orientació general de l'administració d'aquesta entitat, o les persones equivalents que dirigeixin efectivament l'entitat o exerceixin funcions clau de conformitat amb la legislació andorrana.

26. Plataforma de serveis de xarxes socials: una plataforma que permet que els usuaris finals es connectin, comparteixin, descobreixin i es comuniquin entre si a través de múltiples dispositius i, en particular, mitjançant xats, publicacions, vídeos i recomanacions;

27. Proveïdor de serveis de DNS: una entitat que proporciona serveis de resolució recursiva de noms de domini a usuaris finals d'Internet i a altres proveïdors de serveis de DNS, o una entitat que proporciona resolució de noms de domini autoritzada com a servei que poden obtenir entitats essencials o importants de tercers.

28. Quasiincident: qualsevol succés que posseeix el potencial per produir un incident i no arriba a produir-lo, ja sigui per l'atzar o per una intervenció oportuna.

29. Resiliència: la capacitat de prevenir, resistir, mitigar, absorbir, adaptar-se i recuperar-se d'un incident que pertorbi o pugui pertorbar les operacions d'una entitat crítica.

30. Risc: qualsevol circumstància o fet que pugui tenir un efecte advers potencial en la resiliència de les entitats crítiques;

31. Seguretat de les xarxes i sistemes d'informació: 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 referides xarxes i sistemes d'informació o accessibles per aquests.

32. Servei de computació en núvol: un servei digital que fa possible l'administració sota demanda i l'accés remot ampli a un conjunt modulable i elàstic de recursos informàtics distribuïts que es poden compartir.

33. Servei de centre de dades: un servei que engloba les estructures, o agrupacions d'estructures, dedicades a l'allotjament, la interconnexió i l'explotació centralitzats de les tecnologies de la informació i els equips de xarxa que proporcionen serveis d'emmagatzematge, tractament i transport de dades, juntament amb totes les instal·lacions i infraestructures necessàries per a la distribució de l'energia i el control ambiental.

34. Servei digital: tot servei de la societat de la informació, és a dir, tot servei proveït normalment a canvi d'una remuneració, a distància, a petició individual d'un destinatari de serveis, i enviat des de la font i rebut pel destinatari mitjançant equips electrònics de tractament (inclosa la compressió digital) i d'emmagatzematge de dades i que es transmet, canalitza i rep completament per fils, ràdio, mitjans òptics o qualsevol altre mitjà electromagnètic.

35. Servei essencial: servei ofert per una entitat quina tipologia s'emmarca en el de les entitats essencials previstes a l'Annex I, que les autoritats nacionals competents designen com tal d'acord amb l'article 6.4.b), en resultar necessari per al manteniment de les funcions socials bàsiques, la salut, la seguretat, el benestar social i econòmic dels ciutadans, o el funcionament eficaç de les institucions de l'Estat i les administracions públiques, que depengui per a la seva provisió de xarxes i sistemes d'informació, i que pot veure greument afectada la continuïtat de les seves prestacions en supòsits de ciberincidents i, en conseqüència, ocasionar un greu perjudici social i econòmic al Principat d'Andorra.

36. Servei important: servei ofert per una entitat de tipologia emmarcada com a entitat important a l'Annex II, que les autoritats nacionals competents designen com tal d'acord amb l'article 6.4.b), en resultar necessari per al manteniment de les funcions socials bàsiques, la salut, la seguretat, el benestar social i econòmic

Dipòsit legal: AND.2-2015

dels ciutadans, o el funcionament eficaç de les institucions de l'Estat i les administracions públiques, que depengui per a la seva provisió de xarxes i sistemes d'informació, i que pot veure greument afectada la continuïtat de les seves prestacions en supòsits de ciberincidents i, en conseqüència, ocasionar un greu perjudici social i econòmic al Principat d'Andorra,

37. Vulnerabilitat: deficiència, susceptibilitat o fallada d'un actiu, sistema, procés o control que pot ser aprofitat per una o més ciberamenaces.

38. Xarxa de distribució de continguts: una xarxa de servidors distribuïts geogràficament a l'efecte de garantir una elevada disponibilitat, accessibilitat o distribució ràpida de continguts i serveis digitals als usuaris d'Internet en nom dels proveïdors de continguts i serveis.

39. Xarxes i sistemes d'informació:

a) Xarxa de comunicacions electròniques, consistent en sistemes de transmissió i, quan sigui procedent, equips de commutació o encaminament i altres recursos, inclosos els elements de xarxa que no són actius, que permetin el transport de senyals mitjançant cables, ones hertzianes, mitjans òptics o altres mitjans electromagnètics amb inclusió de les xarxes de satèl·lits, xarxes terrestres fixes (de commutació de circuits i de paquets, inclòs Internet) i mòbils, sistemes de línia elèctrica, en la mesura que s'utilitzin per a la transmissió de senyals, xarxes utilitzades per a la radiodifusió sonora i televisiva, i xarxes de televisió per cable, amb independència del tipus d'informació transportada;

b) Tot dispositiu o grup de dispositius interconnectats o relacionats entre si en què un o diversos d'ells realitzen, mitjançant un programari, el tractament automàtic de dades digitals; o

c) Dades digitals emmagatzemades, tractades, recuperades o transmeses mitjançant elements previstos a les lletres anteriors, per al seu funcionament, utilització, protecció i manteniment.

Títol II. Marc estratègic i institucional

Capítol Primer. Marc estratègic

Article 4. *Marc estratègic de seguretat de les xarxes i dels sistemes d'informació*

1. L'Estratègia Nacional de Ciberseguretat del Principat d'Andorra comprèn els objectius estratègics i les mesures polítiques i normatives necessàries per aconseguir i mantenir un nivell elevat de seguretat en les xarxes i en els sistemes d'informació, cobrint els sectors operats per les entitats essencials i importants en els termes definits en aquesta Llei, i engloba, a títol enunciatiu i no limitatiu:

a) Una definició dels objectius i les prioritats de l'Estratègia Nacional de Ciberseguretat del Principat d'Andorra.

b) Un marc de governança per aconseguir aquests objectius i prioritats, incloses les polítiques a què es refereix l'apartat 2 i les funcions i responsabilitats de les administracions públiques i les entitats de l'administració pública i d'altres actors pertinents.

c) Una avaluació per determinar els actius pertinents i els riscos de ciberseguretat.

d) Una determinació de les mesures per garantir la preparació, resposta i recuperació enfront d'incidents, inclosa la cooperació entre els sectors públic i privat.

e) Un llistat dels diversos actors i autoritats que participen en l'execució de l'Estratègia Nacional de Ciberseguretat del Principat d'Andorra.

f) Un marc polític per a la coordinació reforçada entre les autoritats competents en virtut d'aquesta Llei a l'efecte de l'intercanvi d'informació sobre incidents i ciberamenaces i l'exercici de les tasques de supervisió i sanció.

g) Una estratègia per reforçar la resiliència de les entitats crítiques que inclogui, com a mínim:

Dipòsit legal: AND.2-2015

i. Objectius estratègics i prioritats per tal de millorar la resiliència general de les entitats crítiques, tenint en compte les interdependències transfrontereres i intersectorials.

ii. Un marc de governança per assolir els objectius estratègics i les prioritats, inclosa una descripció dels rols i les responsabilitats de les autoritats nacionals competents designades en aquesta Llei, entitats crítiques i altres parts implicades en la implementació de l'estratègia.

iii. Una descripció de les mesures necessàries per millorar la resiliència general de les entitats crítiques, inclosa una avaluació del risc nacional, la identificació d'entitats crítiques i d'entitats equivalents a entitats crítiques i les mesures de suport a les entitats crítiques; i

iv. Un marc de polítiques per a una coordinació millorada entre les autoritats nacionals competents designades en aquesta Llei a l'efecte de l'intercanvi d'informació sobre incidents i ciberamenaces i l'exercici de tasques de supervisió.

2. En el marc de l'Estratègia Nacional de Ciberseguretat del Principat d'Andorra, es desenvolupen i adopten reglamentàriament:

a) 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 solucions per als seus serveis essencials o importants i les seves 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 la prestació dels 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 la seva pertinença a organismes o fòrums internacionals en la matèria.
Aquest Esquema Nacional de Seguretat podrà estendre's a totes les entitats de l'administració pública, i contindrà, com a mínim:

i. Una política per abordar la ciberseguretat en la cadena de subministrament de productes i serveis de TIC utilitzats per les entitats essencials o les entitats importants per a la prestació dels seus serveis;

ii. Directrius relatives a la inclusió i l'especificació dels requisits en matèria de ciberseguretat aplicables als productes i serveis de TIC en la contractació pública;

iii. Una política per promoure i facilitar una divulgació coordinada de les vulnerabilitats;

iv. Una política orientada a mantenir la disponibilitat general i la integritat del nucli públic de la Internet oberta;

v. Una política sobre la promoció i el desenvolupament de capacitats de ciberseguretat, incloent la conscienciació i iniciatives de recerca i desenvolupament;

vi. Una política destinada a donar suport a les institucions acadèmiques i de recerca perquè desenvolupin eines de ciberseguretat i infraestructures de xarxa segures;

vii. Les polítiques, els procediments pertinents i les eines apropiades per compartir informació per facilitar i promoure l'intercanvi voluntari d'informació sobre ciberseguretat entre les empreses; i

viii. Una política que englobi les necessitats específiques de les petites i mitjanes empreses, especialment d'aquelles que es troben excloses de l'àmbit d'aplicació d'aquesta Llei, pel que fa a orientacions i suport per millorar la seva resiliència enfront de les amenaces de ciberseguretat.

b) Un Reglament d'Infraestructures Crítiques per a la protecció i el reforç de la resiliència de les infraestructures crítiques que contindrà, com a mínim:

i. Procediments per a la identificació i designació d'infraestructures crítiques per al Principat d'Andorra;

Dipòsit legal: AND.2-2015

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 citades infraestructures i que serà emprat com a base per planificar les actuacions necessàries en matèria de seguretat i protecció d'aquestes, en nodrir-se de les aportacions dels propis operadors;

iii. La regulació d'instruments de planificació per a la protecció de 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; i

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

3. L'Estratègia Nacional de Ciberseguretat del Principat d'Andorra ha de ser objecte de revisió i d'avaluació almenys cada quatre anys, en funció dels indicadors de rendiment clau, procedint en tot cas a la seva modificació quan sigui necessari. S'ha de garantir la consulta als sectors rellevants representats en els diferents comitès i comissions que s'estructuren sota l'Agència Nacional de Ciberseguretat (ANC-AD).

Article 5. *Marc nacional de gestió de crisis de ciberseguretat*

1. L'ANC-AD és la responsable de la gestió dels incidents i de les crisis a gran escala, per als quals:

a) Determinarà les capacitats, els actius i els procediments que es poden desplegar en cas que es produeixi una crisi a l'efecte d'aquesta Llei; i

b) Desenvoluparà un Pla nacional de resposta a incidents i crisis de ciberseguretat, en un termini màxim de nou mesos des de l'entrada en vigor d'aquesta Llei, on es fixaran els objectius i les modalitats de la gestió dels incidents i les crisis de ciberseguretat, que ha de contenir almenys els següents aspectes:

i. Els objectius de les mesures i activitats nacionals en matèria de preparació;

ii. Les tasques i responsabilitats de les autoritats nacionals competents d'acord amb el que es preveu en aquesta Llei;

iii. Els procediments de gestió de crisis i els canals per a l'intercanvi d'informació;

iv. Les mesures de preparació, inclosos els exercicis i les activitats de formació;

v. Les parts interessades pertinents, tant públiques com privades, i la infraestructura implicada; i

vi. Els procediments i mecanismes nacionals entre l'ANC-AD, el CSIRT-AD i altres autoritats o organismes nacionals pertinents per garantir la participació efectiva del Principat d'Andorra en la gestió coordinada d'incidents i crisis de ciberseguretat.

Capítol Segon. Marc institucional

Article 6. *Autoritats nacionals competents*

1. L'ANC-AD és l'autoritat nacional competent encarregada de la ciberseguretat i de les tasques de supervisió a què es refereix el capítol tercer del Títol III per a les xarxes i els sistemes d'informació que cobreixen els sectors esmentats als apartats 1, 2, 5, 6, 7 i 8 de l'Annex I, així com per a totes les entitats importants per a les quals l'AFA no és l'autoritat nacional competent.

2. L'AFA, en coordinació amb l'ANC-AD, és l'autoritat nacional competent encarregada de la ciberseguretat i de les tasques de supervisió a què es refereix el capítol tercer del Títol III per a les xarxes i els sistemes d'informació que cobreixen els sectors de les entitats financeres i del mercat financer tal com es defineixen als apartats 3 i 4 de l'Annex I, així com per als serveis proveïts per les entitats que es trobin sota la supervisió de l'AFA.

3. L'ANC-AD actuarà com a punt de contacte únic en matèria de ciberseguretat per al Principat d'Andorra (Punt de Contacte Nacional Únic), i com a tal serà l'autoritat nacional competent que exercirà la funció

Dipòsit legal: AND.2-2015

d'enllaç per garantir la cooperació transfronterera amb les autoritats competents en matèria de ciberseguretat d'altres països, per garantir la cooperació intersectorial entre l'AFA i l'ANC-AD pel que respecta al previst en aquesta Llei, així com per garantir la cooperació entre el CSIRT-AD i els altres països, incloent-hi la xarxa de CSIRT de la Unió Europea.

4. L'ANC-AD, amb la col·laboració de l'AFA pel que fa al seu àmbit competencial de conformitat amb l'establert en aquesta Llei:

a) Coordinarà la creació i el manteniment del marc estratègic de seguretat de les xarxes i dels sistemes d'informació descrit a l'article 4.

b) Establirà una llista de serveis essencials i serveis importants en els sectors a què es refereixen l'Annex I i l'Annex II. Aquesta llista s'ha de dur a terme en un termini màxim de sis mesos després de l'entrada en vigor d'aquesta Llei. Posteriorment, quan sigui necessari, i almenys una primera vegada en un termini màxim de divuit mesos després de l'entrada en vigor d'aquesta Llei i a partir d'aquell moment cada quatre anys i cada vegada que l'ANC-AD actualitzi la llista, realitzarà una avaluació de tots els riscos rellevants que puguin afectar a la prestació d'aquests serveis essencials, amb la finalitat d'identificar entitats crítiques i entitats equivalents a entitats crítiques i ajudar-les a prendre mesures d'acord amb l'establert a l'article 12. L'avaluació del risc:

i. Haurà de tenir en compte tots els riscos naturals i els originats per l'home, inclosos els accidents, els desastres naturals, les emergències de salut pública, i les amenaces antagòniques, inclosos els delictes de terrorisme.

ii. Els elements rellevants de l'avaluació del risc hauran de posar-se a disposició de les entitats crítiques que s'identifiquin d'acord amb l'establert a l'article 11, per ajudar-les a dur a terme la seva avaluació de riscos d'acord amb l'establert a l'article 13 i a prendre mesures per garantir la seva resiliència d'acord amb l'establert a l'article 12.

c) Donarà suport a les entitats que es troben dins de l'àmbit d'aplicació d'aquesta Llei per millorar la seva ciberseguretat i resiliència. Aquest suport pot incloure, a títol informatiu i no limitatiu:

i. El desenvolupament de materials i metodologies d'orientació;

ii. Donar suport a l'organització d'exercicis per comprovar la seva seguretat i resiliència;

iii. Proporcionar formació al seu personal; i

iv. Establir eines per donar suport a l'intercanvi voluntari d'informació entre entitats i per resoldre qüestions en relació amb aquesta Llei.

d) Adoptarà actes d'execució per establir les especificacions tècniques i metodològiques necessàries relatives a l'aplicació de les mesures esmentades a l'article 12.2.

e) Establirà procediments per a l'expedició, la revisió periòdica i la retirada de certificacions, segells i marques que acrediten el compliment de les obligacions de seguretat en les xarxes i en els sistemes d'informació.

f) Establirà procediments i estructures per tramitar les reclamacions relatives a infraccions de la certificació o a la manera en què una entitat aplica o ha aplicat la certificació, i per fer que aquests procediments i estructures siguin transparents per al públic.

5. L'ANC-AD, amb la col·laboració de l'AFA i el CSIRT-AD, està facultada per adoptar actes delegats establint normes detallades que especifiquin algunes o totes les mesures que s'han de prendre en la mesura que sigui necessari per a l'aplicació eficaç i coherent dels objectius d'aquesta Llei, tenint en compte qualsevol evolució rellevant en riscos, tecnologia o prestació dels serveis afectats per aquesta Llei, així com qualsevol especificitat relacionada amb sectors i tipus d'entitats de l'Annex I i l'Annex II.

6. El Govern d'Andorra ha de vetllar perquè les autoritats nacionals competents disposin dels recursos adequats perquè puguin dur de forma efectiva i eficient les seves funcions per tal de poder complir amb els objectius d'aquesta Llei.

Dipòsit legal: AND.2-2015

Article 7. *Funcions de les autoritats nacionals competents*
Les autoritats nacionals competents exerceixen les següents funcions:

1. Identificar, en col·laboració amb el CSIRT-AD, serveis essencials i importants, entitats crítiques i entitats equivalents a entitats crítiques.

2. Supervisar el compliment per part de les entitats essencials o importants de les obligacions que es determinen de conformitat amb l'establert al capítol tercer del Títol III. En aquest sentit, amb o sense el suport del CSIRT-AD, les autoritats nacionals competents poden realitzar les actuacions inspectores necessàries per al correcte desenvolupament de les seves funcions de control.

3. Analitzar les notificacions que rebin a través del CSIRT-AD sobre incidents notoris que es presentin en el marc d'aquesta Llei.

4. Informar, si s'escau, públicament sobre determinats incidents, quan la difusió d'aquesta informació sigui necessària per evitar un incident o gestionar-ne un que ja s'ha produït.

5. Revisar la declaració d'aplicabilitat de mesures de seguretat inicial a què es refereix l'article 12, i els seus successius canvis.

6. Resoldre les sol·licituds d'informació d'acord amb l'article 12.2.e), sobre personal o candidats a personal que exerceix funcions crítiques.

7. Exercir la potestat sancionadora en els casos que preveu aquesta Llei, en virtut de l'establert al seu Títol IV.

8. Emetre opinions sobre qüestions relacionades amb la ciberseguretat.

9. Desenvolupar les millors pràctiques i metodologies d'implementació de les obligacions a què fa referència aquesta Llei.

10. Desenvolupar activitats i exercicis de formació transfronterers per comprovar la ciberseguretat dels serveis essencials i la resiliència de les entitats crítiques.

11. Emetre, amb la consulta prèvia al CSIRT-AD, a les entitats essencials o importants, certificats que acreditin el compliment de les obligacions de seguretat en les xarxes i els sistemes d'informació.

Article 8. *CSIRT-AD*
1. El CSIRT-AD és l'equip de referència de resposta als incidents de seguretat de les xarxes i els sistemes d'informació dels sectors, subsectors o entitats que figuren en l'Annex I i l'Annex II.

2. L'ANC-AD ha de vetllar perquè el CSIRT-AD disposi dels recursos adequats perquè pugui dur a terme de forma efectiva i eficient les funcions que li assigna aquesta Llei, el seu Reglament de creació i altra eventual normativa.

3. Igualment, l'ANC-AD ha de vetllar perquè el CSIRT-AD tingui a la seva disposició una infraestructura de comunicació i d'informació adequada, segura i resilient per facilitar l'intercanvi d'informació amb les entitats essencials i importants i altres parts interessades pertinents.

Article 9. *Funcions del CSIRT-AD*
1. El CSIRT-AD té com a principals funcions:

a) Cooperar amb l'ANC-AD en tot allò que aquesta li demani en relació amb aquesta Llei.

b) Supervisar les ciberamenaces, les vulnerabilitats i els incidents a escala nacional.

c) Difondre alertes imminents, avisos i informacions sobre les ciberamenaces, les vulnerabilitats i els incidents entre les entitats essencials i importants i altres parts interessades corresponents.

d) Proporcionar a les entitats que notifiquin incidents, informació rellevant sobre el seguiment de la notificació de què es tracti, inclosa informació que pugui donar suport a la resposta efectiva de l'entitat a l'incident.

Dipòsit legal: AND.2-2015

e) Respondre a incidents.

f) Notificar a l'ANC-AD els incidents notoris que es presentin en el marc d'aquesta Llei.

g) Efectuar anàlisis dinàmiques de riscos i d'incidents i de coneixement de la situació en matèria de ciberseguretat.

h) Realitzar, a petició d'entitats, exploracions proactives de la seguretat de les infraestructures crítiques i de les xarxes i els sistemes d'informació utilitzats en la prestació dels serveis essencials o que puguin afectar a serveis essencials per al Principat d'Andorra o altres països.

i) Coordinar-se amb els organismes competents a través dels protocols d'actuació per a l'acompliment d'aquesta Llei que, si escau, es poden desplegar reglamentàriament.

j) Elaborar i fomentar l'adopció i la utilització de pràctiques comunes o normalitzades, sistemes de classificació i taxonomies relatius a:

i. Procediments de gestió d'incidents;

ii. Gestió de crisis de ciberseguretat; i

iii. Divulgació de vulnerabilitats.

Títol III. Obligacions

Capítol primer. Obligacions de ciberseguretat

Article 10. *Obligació d'identificació com entitat essencial o important*

1. Les entitats que conforme a les definicions incloses a l'article 3 es considerin essencials o importants i estiguin dins de l'àmbit d'aplicació descrit a l'article 2 i disposin d'un establiment al Principat d'Andorra o d'un representant d'acord amb l'establert a l'article 19, remetran la següent informació a les seves respectives autoritats nacionals competents a tot tardar sis mesos a comptar de la data de publicació al *Butlletí Oficial del Principat d'Andorra* de la llista de serveis essencials i importants establerta a l'article 6.4.b):

a) El nom de l'entitat i, si escau, del seu representant;

b) L'adreça del seu establiment principal i de la resta dels seus establiments legals al Principat d'Andorra o, de no estar establerta al Principat d'Andorra, del seu representant designat en virtut de l'establert a l'article 19; i

c) Les dades de contacte actualitzades, en particular les adreces de correu electrònic i els números de telèfon de les entitats.

2. Les entitats a què es refereix l'apartat anterior notificaran a les seves respectives autoritats nacionals competents qualsevol canvi en la informació remesa conformement al dit apartat sense demora, i en qualsevol cas, en el termini màxim de tres mesos a comptar de la data en què es produeixi el canvi.

3. Quan, a més del Principat d'Andorra, una entitat a què es refereix l'apartat 1 compti amb el seu establiment principal en altres països, l'ANC-AD també informarà les autoritats competents d'aquests països, de la condició que té aquesta entitat com a essencial o important per al Principat d'Andorra.

Article 11. *Identificació d'entitats crítiques*

1. En el termini màxim de sis mesos a comptar de la conclusió de l'avaluació de riscos que s'especifica a l'article 6.4.b), les autoritats nacionals competents hauran de tenir identificades les entitats crítiques i les equivalents a entitats crítiques per a cada sector i subsector a què es refereix l'Annex I.

Les autoritats nacionals competents hauran de revisar i, si escau, actualitzar aquesta llista d'entitats crítiques i equivalents almenys una primera vegada en un termini màxim de divuit mesos després de l'entrada en vigor d'aquesta Llei i, en qualsevol cas, cada quatre anys com a mínim.

Dipòsit legal: AND.2-2015

2. Quan identifiquin entitats crítiques i equivalents a crítiques de conformitat amb l'apartat 1, les autoritats nacionals competents hauran de tenir en compte els resultats de la seva avaluació dels riscos que poden afectar els serveis essencials de la seva competència, d'acord amb l'establert a l'article 6, i aplicar els criteris que identifiquen a una entitat com entitat crítica d'acord amb la seva definició.

3. L'ANC-AD, amb la col·laboració de l'AFA pel que fa al seu àmbit competencial de conformitat amb l'establert en aquesta Llei, ha d'establir una llista de les entitats identificades com a crítiques o equivalents a crítiques i assegurar-se que es notifiqui a aquestes entitats la seva identificació com a entitats crítiques o equivalents a crítiques en el termini d'un mes després d'aquesta identificació, informant-les de les seves obligacions d'acord amb la resta d'articles d'aquest capítol i la data a partir de la qual els són aplicables les disposicions que estableix aquesta Llei i els reglaments que la desenvolupin, al respecte de les dites obligacions.

Article 12. *Obligacions de ciberseguretat de les entitats essencials i importants*

1. Les entitats essencials i importants sotmeses a l'àmbit d'aplicació d'aquesta Llei han d'adoptar mesures tècniques i d'organització que resultin de gestionar els riscos que es plantegin en relació amb la seguretat de les infraestructures crítiques, i de les xarxes i els sistemes d'informació utilitzats en la prestació dels serveis essencials i importants, tant si es tracta d'infraestructures crítiques, xarxes i sistemes propis, com de proveïdors externs. Així mateix, han de tenir en compte, en particular, la dependència de les infraestructures crítiques, de les xarxes i dels sistemes d'informació amb la continuïtat de serveis o subministraments contractats per l'entitat, així com les interaccions que realitzin amb infraestructures, xarxes i sistemes d'informació de tercers, i els riscos que es derivin del tractament de les dades personals, d'acord amb el que disposi la normativa andorrana vigent en cada moment en matèria de protecció de dades personals i, si escau, la normativa de la Unió Europea vigent en cada moment en matèria de protecció de dades personals.

Sense perjudici del seu deure de notificar incidents de conformitat amb l'establert a l'article 15, les entitats essencials i importants han de prendre les mesures adequades i proporcionals que els siguin aplicables d'acord amb el previst a l'Esquema Nacional de Seguretat a què fa referència aquesta Llei, sense perjudici de poder ser complementades amb mesures d'altres estàndards reconeguts en l'àmbit internacional.

2. Addicionalment, les entitats crítiques han de prendre mesures tècniques i organitzatives adequades i proporcionades per garantir la resiliència de les seves infraestructures crítiques, incloses les mesures necessàries per:

a) Evitar que es produeixin incidents, fins i tot mitjançant mesures de reducció del risc de desastres i d'adaptació climàtica;

b) Garantir una protecció física adequada de les zones, instal·lacions i altres infraestructures sensibles, incloses les tanques, les barreres, les eines i les rutines de control perimetral, així com els equips de detecció i els controls d'accés;

c) Resistir i mitigar les conseqüències dels incidents, inclosa la implementació de procediments i protocols de gestió de riscos i crisis i rutines d'alerta;

d) Recuperar-se dels incidents, incloses les mesures de continuïtat del negoci i la identificació de cadenes de subministrament alternatives;

e) Garantir una gestió adequada de la seguretat dels empleats, inclòs l'establiment de categories de personal que exerceixen funcions crítiques degut als seus drets d'accés a zones, instal·lacions i altres infraestructures sensibles i a informació sensible, sobre les quals cal presentar a l'autoritat nacional competent un informe que inclogui:

i. La identitat de la persona establerta sobre la base de proves documentals;

ii. Qualsevol antecedent penal d'almenys els cinc anys anteriors, i durant un màxim de deu anys, sobre delictes rellevants per a la contractació en un lloc específic, al Principat d'Andorra o tercers països de residència durant aquest període de temps;

Dipòsit legal: AND.2-2015

iii. Ocupacions anteriors, formació i qualsevol manca de formació o ocupació al currículum de la persona durant, com a mínim, els cinc anys anteriors i durant un màxim de deu anys; i

iv. Qualsevol altra informació objectiva disponible que pugui ser necessària per determinar la idoneïtat de la persona interessada per treballar en el lloc en relació amb el qual l'entitat crítica ha sol·licitat informació.

f) Sensibilitzar el personal pertinent sobre les mesures esmentades en les lletres a) a e).

3. Les mesures que s'adoptin han de ser relacionades i formalitzades en una declaració d'aplicabilitat de mesures de seguretat que les entitats han de remetre a l'autoritat nacional competent en el termini de sis mesos a comptar de la identificació de l'entitat com a entitat essencial o important, d'acord amb l'article 10 o des de l'entrada en vigor de l'Esquema Nacional de Seguretat, el que succeeixi més tard, la qual serà objecte de revisió, almenys, cada tres anys.

4. Les entitats essencials i importants han d'adoptar polítiques de seguretat de les infraestructures crítiques, xarxes, i sistemes d'informació necessaris per prestar els seus serveis essencials i importants atesos els principis de seguretat integral, gestió de riscos, prevenció, resposta i recuperació, línies de defensa, reavaluació periòdica i segregació de tasques.

Les polítiques de seguretat de les infraestructures crítiques, les xarxes i sistemes d'informació han de contenir, com a mínim, els següents factors:

a) Anàlisi i gestió de riscos.

b) Gestió de riscos de tercers o proveïdors.

c) Catàleg de mesures de seguretat, organitzatives, tecnològiques i físiques.

d) Gestió del personal i professionalitat.

e) Adquisició de productes o serveis de seguretat.

f) Detecció i gestió d'incidents.

g) Plans de recuperació i assegurament de la continuïtat de les operacions.

h) Millora contínua.

i) Interconnexió de sistemes.

j) Registre de l'activitat dels usuaris.

5. Les autoritats nacionals competents podran establir obligacions específiques per garantir la seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació emprats per les entitats que proveeixen serveis essencials o importants. Així mateix, podran dictar instruccions tècniques i guies orientatives per detallar el contingut d'aquestes instruccions i guies.

6. Per a l'elaboració de disposicions reglamentàries, instruccions i guies, l'autoritat nacional competent tindrà en compte totes aquelles obligacions sectorials i requisits en matèria de seguretat de la informació als quals estiguin sotmesos els operadors als quals els hi són aplicables les disposicions d'aquesta Llei.

Article 13. *Gestió de riscos de ciberseguretat*

1. Les entitats essencials i importants, i molt especialment les que a més d'essencials siguin crítiques, han d'adoptar les mesures tècniques i organitzatives adequades i proporcionades per establir un procés per a la gestió dels riscos que es plantegin a fi d'aconseguir un nivell elevat de resiliència de les infraestructures crítiques i de protecció de les xarxes i dels sistemes d'informació que utilitzen per a la prestació dels seus serveis essencials i importants en relació amb els riscos que es plantegin. Entre les mesures de gestió del risc han de figurar aquelles la finalitat de les quals és determinar tot risc d'incidents, prevenir, detectar i gestionar incidents i reduir les seves repercussions. Aquest procés de gestió dels riscos ha de comprendre la seguretat de les dades emmagatzemades, transmeses i tractades i, en el cas d'entitats essencials, ha

Dipòsit legal: AND.2-2015

de tenir en compte tots els riscos rellevants que hagin trobat les autoritats nacionals competents d'acord amb l'avaluació de riscos a què es refereix l'article 6.4.b), i totes les dependències amb altres sectors i amb entitats crítiques o equivalents a entitats crítiques.

2. L'esforç dedicat per les entitats a la gestió dels riscos de ciberseguretat ha de ser proporcional en relació amb els riscos que presenten la xarxa i els sistemes d'informació que participen en l'oferta dels seus serveis essencials i importants, i tenir en compte l'estat de la tècnica. Entre els criteris per jutjar la proporcionalitat dels esforços en la gestió dels riscos s'hi han de considerar, com a mínim, els següents:

a) La mesura en què les entitats essencials i importants utilitzen serveis, sistemes o productes de TIC crítics i depenen d'ells;

b) La importància de serveis, sistemes o productes de TIC crítics específics per exercir funcions crítiques o sensibles, en particular el tractament de dades personals;

c) La disponibilitat de serveis, sistemes o productes de TIC alternatius;

d) La resiliència de la cadena de subministrament global de serveis, sistemes o productes de TIC enfront de les pertorbacions; i

e) En el cas dels serveis, sistemes o productes de TIC emergents, el pes que poden tenir en el futur per a les activitats de les entitats.

3. Entre les mesures per a la gestió dels riscos que es plantegin, s'hi han d'incloure, almenys, els següents elements:

a) La política de seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació necessaris per a la prestació de serveis essencials o importants;

b) La política de gestió de riscos;

c) La gestió d'incidents (prevenció, detecció i resposta a incidents);

d) La continuïtat de les activitats i la gestió de crisis;

e) La seguretat de la cadena de subministrament, inclosos els aspectes de seguretat relatius a les relacions entre cada entitat i els seus proveïdors o prestadors de serveis com, per exemple, proveïdors de serveis d'emmagatzematge i transformació o anàlisi de dades o de serveis de seguretat administrada;

f) La seguretat en l'adquisició, el desenvolupament i el manteniment d'infraestructures crítiques, xarxes i sistemes d'informació, inclosa la gestió i divulgació de les vulnerabilitats;

g) Les polítiques i els procediments (assaig i auditoria) per avaluar l'eficàcia de les mesures per a la gestió de riscos de ciberseguretat; i

h) La utilització de criptografia i xifratge.

4. Les entitats han de tenir en compte les vulnerabilitats específiques de cada proveïdor i prestador de serveis i la qualitat general dels productes i les pràctiques en matèria de ciberseguretat dels seus proveïdors i prestadors de serveis, inclosos els seus procediments de desenvolupament segur.

5. En cas que una entitat constati que els seus serveis o comeses no s'ajusten als requisits establerts als apartats 1, 2 i 3, com més aviat millor, haurà d'adoptar totes les mesures correctores necessàries per a què el servei o comesa en qüestió, compleixi aquests requisits.

Article 14. *Obligació de resoldre els incidents, d'informació i de col·laboració mútua*

1. En termes de gestió d'incidents de seguretat, detecció de vulnerabilitats o ciberamenaces, les entitats essencials i importants han de:

a) Gestionar i resoldre els incidents de seguretat que afectin les infraestructures crítiques, les xarxes o els sistemes d'informació utilitzats per prestar els seus serveis essencials o importants.

Dipòsit legal: AND.2-2015

Si es tracta d'infraestructures, xarxes o sistemes externs s'ha de garantir que els proveïdors externs compleixen amb l'aplicació de les mesures necessàries per garantir la seguretat.

b) Sol·licitar opinió o suport especialitzat al CSIRT-AD per fer front als incidents, vulnerabilitats o ciberamenaces sorgides i, en tot cas, atendre a les indicacions rebudes per part del CSIRT-AD per resoldre els riscos, mitigar-ne els efectes i reposar els sistemes afectats.
En aquest supòsit, les indicacions emeses pel CSIRT-AD per mitigar els efectes i reposar els sistemes afectats són d'aplicació vinculant.

c) Aplicar la seva política de gestió de la seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació davant del sorgiment de qualsevol incident que afecti la prestació dels seus serveis essencials i importants, així com el conjunt d'obligacions i recomanacions emeses per l'autoritat nacional competent o el CSIRT-AD.

2. Les entitats essencials i importats han de subministrar al CSIRT-AD i a l'autoritat nacional competent que escaigui tota la informació que se'ls requereixi per a l'acompliment de les funcions que els encomana aquesta Llei. En particular, podrà requerir-se informació addicional a les entitats essencials o importants per analitzar la naturalesa, les causes i els efectes dels incidents notificats, i per elaborar estadístiques i reunir les dades necessàries per elaborar els informes anuals considerats a l'article 25.4.e).

Quan les circumstàncies ho permetin, l'autoritat nacional competent o el CSIRT-AD proporcionarà a les entitats essencials o importants afectades per incidents la informació derivada del seu seguiment que pugui ser-los rellevant, en particular, per resoldre l'incident.

Article 15. *Obligació de notificar*
1. Les entitats que presten serveis essencials o importants han de notificar al CSIRT-AD, que al seu torn ho farà a l'autoritat nacional competent que li pertoqui i en tot cas a l'ANC-AD, els incidents que tinguin o puguin tenir efectes significatius en aquests serveis d'acord amb el que s'estableixi reglamentàriament, així com qualsevol informació que permeti a l'autoritat nacional competent o al CSIRT-AD determinar les repercussions transfrontereres que pot tenir l'incident.

Aquesta notificació es farà sense demora i en tot cas en el termini de setanta-dues hores a comptar de la seva detecció. Si en el moment de notificar l'incident o possible incident encara no disposen d'informació en relació amb la seva repercussió sobre serveis essencials o importants, poden ometre aquesta informació, amb el compromís d'enviar-la com més aviat millor, i que transcorregut un termini de setanta-dues hores des de la notificació de l'incident, l'entitat essencial o important que no hagi reunit la informació pertinent enviï al CSIRT-AD un informe justificatiu de les actuacions que hagi dut a terme per obtenir aquesta informació i dels motius pels quals no ha sigut possible obtenir-la.

Quan sigui procedent, aquestes entitats han de notificar, sense demora indeguda, als destinataris dels seus serveis que puguin veure's afectats per l'incident, les mesures o solucions que aquests destinataris poden aplicar en resposta al mateix.

2. Les entitats de serveis essencials o importants han de notificar a l'autoritat nacional competent, per mitjà del CSIRT-AD i sense demora, qualsevol ciberamenaça significativa pels serveis essencials o importants que, al seu parer, pot desembocar en un incident significatiu d'acord amb el que s'estableixi reglamentàriament.

Quan sigui procedent, aquestes entitats han de notificar, sense demora indeguda, als destinataris dels seus serveis que puguin veure's afectats per una ciberamenaça significativa, les mesures o solucions que aquests destinataris poden aplicar en resposta a l'amenaça. Quan sigui procedent, les entitats notificaran als destinataris la pròpia amenaça.

3. Una amenaça significativa és aquella que pot donar lloc a un incident significatiu, i un incident es considerarà significatiu si:

a) L'incident ha causat o pot causar pertorbacions operatives o perjudicis econòmics substancials per a l'entitat afectada; o

Dipòsit legal: AND.2-2015

b) L'incident ha afectat o pot afectar altres persones físiques o jurídiques en causar perjudicis materials o morals considerables en relació amb:

i. El nombre d'usuaris afectats per la pertorbació del servei essencial i la seva quota de mercat.

ii. La duració de l'incident.

iii. La no disponibilitat d'alternatives per mantenir un nivell suficient de prestació del servei.

iv. L'extensió o àrees geogràfiques afectades o que puguin quedar afectades per l'incident.

v. El grau de pertorbació del funcionament del servei.

vi. L'abast de l'impacte en activitats econòmiques i socials crucials.

vii. La importància dels sistemes afectats o de la informació afectada per l'incident per a la prestació del servei essencial.

viii. La dependència d'altres sectors estratègics respecte del servei i la repercussió, en termes de grau i durada, de l'incident en les activitats socials i econòmiques o en la seguretat pública.

ix. El dany a la reputació.

Reglamentàriament es poden afegir factors específics del sector per determinar si un incident pot tenir efectes pertorbadors significatius.

4. En relació a les notificacions indicades en els apartats 1 i 2, les entitats afectades han de presentar al CSIRT-AD:

a) Una notificació inicial sense demora indeguda i en qualsevol cas en el termini de vint-i-quatre hores des que s'hagi tingut constància de l'incident, en la qual s'indicarà, quan s'escaigui, si cal suposar que l'incident respon a una acció il·lícita o malintencionada;

b)Totes aquelles notificacions intermitges que resultin precises o sol·liciti el CSIRT-AD per actualitzar o completar la informació inclosa en la notificació inicial i informar sobre l'evolució de l'incident mentre aquest no es trobi resolt; i

c) Un informe final, a tot tardar un mes després de presentar la notificació inicial prevista a la lletra a), en la qual s'hi recullin almenys els següents elements:

i. una descripció detallada de l'incident, la seva gravetat i el seu impacte;

ii. el tipus d'amenaça o causa principal que probablement va desencadenar l'incident; i

iii. les mesures de mitigació aplicades i en curs.

5. En casos degudament justificats, com ara en supòsits de força major, l'entitat pot incomplir els terminis establerts en els apartats 1 i 2.

6. Les notificacions efectuades a l'empara d'aquest article han d'incloure la informació que permeti determinar qualsevol efecte transfronterer de l'incident.

7. El CSIRT-AD oferirà, en el termini de vint-i-quatre hores després de la recepció de la notificació inicial a què es refereix l'apartat 4.a), una resposta a l'entitat que ha fet la notificació, incloent en particular els seus comentaris inicials sobre l'incident i, a instàncies de l'entitat, una orientació sobre l'aplicació de possibles mesures de mitigació. El CSIRT-AD donarà suport tècnic addicional quan així ho sol·liciti l'entitat afectada. Quan es sospiti que l'incident és de naturalesa delictiva, el CSIRT-AD també proporcionarà orientació a l'efecte de denunciar l'incident davant les autoritats corresponents.

L'obligació de notificació d'incidents prevista en aquest article no allibera del compliment del deure general que té l'entitat que fa la notificació de denúncia davant les autoritats corresponents, sobre aquells fets que puguin revestir caràcter de delicte.

8. Quan el coneixement del públic sigui necessari per evitar un incident o fer front a un incident en curs, o quan la divulgació de l'incident redundi en l'interès públic, l'ANC-AD, amb el suport del CSIRT-AD, podrà

Dipòsit legal: AND.2-2015

informar el públic, després de consultar-ho amb l'entitat afectada, de l'incident, o exigir a l'entitat que ho faci si aquesta no ha actuat prèviament en aquest sentit.

9. Les notificacions d'entitats essencials han de referir-se als incidents que afecten les infraestructures crítiques, les xarxes i els sistemes d'informació emprats en la prestació dels serveis essencials, sent indiferent que es tracti d'infraestructures crítiques, xarxes i sistemes propis o de proveïdors externs.

10. Les entitats essencials o importants han de realitzar les notificacions que corresponguin en virtut d'aquest capítol a través del Delegat de la Seguretat de la Informació (DSI) que hagin designat segons el que es disposa a l'article 18.

11. La notificació d'un incident segons el que es disposa en aquesta Llei no exclou ni substitueix l'obligació de notificació que les entitats hagin de fer a altres organismes conforme a la seva normativa específica.

12. Quan la notificació d'incidents o la seva gestió, anàlisi o resolució requereixi comunicar dades personals, el seu tractament s'ha de restringir a les dades que siguin estrictament adequades, pertinents i limitades en relació amb la finalitat perseguida en cada cas.

Les cessions de dades personals per a aquests fins s'entenen autoritzades en els següents casos:

a) Entre les entitats essencials o importants i l'ANC-AD, el CSIRT-AD o les autoritats nacionals competents.

b) Entre el CSIRT-AD i l'ANC-AD.

c) Entre el CSIRT-AD i altres CSIRT designats internacionalment.

d) Entre l'ANC-AD i altres autoritats competents internacionals.

e) Entre les autoritats nacionals competents i l'ANC-AD.

f) Entre les autoritats nacionals competents i el CSIRT-AD.

Article 16. *Notificació voluntària*

1. Sense perjudici del que es disposa a l'article 2, les entitats excloses de l'àmbit d'aplicació d'aquesta Llei poden presentar voluntàriament notificacions de ciberamenaces, quasiincidents i incidents significatius. Quan tramitin les notificacions al CSIRT-AD, aquestes entitats actuaran de conformitat amb el procediment establert a l'article 15.

2. Així mateix, les entitats essencials o importants poden notificar els incidents o les ciberamenaces per als quals no s'estableixi una obligació de notificació.

3. Aquestes notificacions obliguen a l'entitat que les hagi efectuat a resoldre l'incident d'acord amb el que s'estableix en aquesta Llei. No obstant això, aquest tipus d'entitat notificant no queda subjecta a altres obligacions addicionals a les quals no estaria obligada de no haver presentat aquesta notificació.

4. Les notificacions obligatòries tenen caràcter prioritari sobre les voluntàries a l'efecte de la seva gestió per part del CSIRT-AD.

Capítol Segon. Altres obligacions de les entitats essencials i importants

Article 17. *Governança*

1. Els òrgans de direcció de les entitats essencials i importants han d'aprovar les mesures de gestió dels riscos de ciberseguretat adoptades per aquestes entitats segons el que es disposa a l'article 13, supervisar la seva posada en pràctica i respondre per l'incompliment de les obligacions recollides en dit article per part de les entitats.

2. Els membres de l'òrgan de direcció han d'assistir periòdicament a formacions específiques per adquirir coneixements i destreses suficients que permetin comprendre i avaluar els riscos de ciberseguretat i les pràctiques de gestió i el seu impacte en les operacions de l'entitat.

Dipòsit legal: AND.2-2015

Article 18. *Delegat de la Seguretat de la Informació*

1. Les entitats essencials i les entitats importants, a través dels seus òrgans de direcció, han de designar una persona física, una unitat o un òrgan col·legiat, perquè actuï com a Delegat de la Seguretat de la Informació (DSI) i sigui el punt de contacte i coordinació tècnica entre l'entitat que l'ha designat i l'autoritat nacional competent i el CSIRT-AD.

2. Quan el DSI sigui una unitat o un òrgan col·legiat, es designa una persona física representant del mateix.

3. En tot cas, les entitats essencials o importants també han de designar un substitut del DSI perquè assumeixi les seves funcions en casos d'absència, vacant o malaltia.

4. Les dades de contacte del DSI en funcions s'han de notificar a l'autoritat competent en el termini màxim d'un mes a comptar de la data de designació que s'escaigui. El mateix procediment es realitza en el supòsit de canvis en les dades de contacte, per exemple deguts a cessaments o nomenaments, havent-los de notificar a l'autoritat nacional competent, que al seu torn els compartirà immediatament amb el CSIRT-AD, en el termini màxim d'un mes a comptar de la data del canvi.

5. El DSI actua com a punt de contacte per notificar els incidents conforme a l'article 15, així com per gestionar allò que escaigui en el si de l'entitat que l'hagi nomenat, conforme als articles 13 i 14.

6. Addicionalment, a títol enunciatiu i no limitatiu, el DSI exerceix, sota la responsabilitat de l'entitat que l'ha nomenat, les funcions següents:

a) Elaborar i proposar, de conformitat amb el que estableix l'article 12, polítiques de seguretat, incloent una proposta de mesures tècniques i organitzatives, adequades i proporcionades, per prevenir i gestionar els possibles riscos relatius a la seguretat de les infraestructures crítiques, les xarxes, i els sistemes d'informació necessaris per proveir els serveis essencials o importants, per així reduir al mínim els efectes dels ciberincidents que afectin els dits serveis.

b) Elaborar el document de declaració d'aplicabilitat de mesures de seguretat en relació amb l'Esquema Nacional de Seguretat del Principat d'Andorra.

c) Supervisar l'aplicació de les polítiques de seguretat, protocols i procediments en l'entitat, supervisar-ne la seva efectivitat i establir períodes de control.

d) Fomentar la formació i l'aplicació de bones pràctiques en seguretat de les infraestructures crítiques, les xarxes, i els sistemes d'informació necessaris per proveir els serveis essencials o importants que ofereix l'entitat que els va designar com a DSI.

e) Remetre al CSIRT-AD, que al seu torn informa a l'autoritat nacional competent, sense dilació indeguda, les notificacions d'incidents, vulnerabilitats o ciberamences que tinguin efectes pertorbadors en la prestació dels serveis essencials o importants.

f) Rebre, interpretar, supervisar i transmetre l'aplicació de les instruccions i guies emanades de l'autoritat nacional competent o del CSIRT-AD.

g) Recopilar, preparar i subministrar informació o documentació a l'autoritat nacional competent o al CSIRT-AD quan així ho sol·licitin o per iniciativa pròpia.

h) Intercanviar informació sobre ciberseguretat pertinent directament amb els DSI d'altres entitats essencials i importants autoritzades per l'entitat que l'ha nomenat, o mitjançant els canals de comunicació que l'ANC-AD pugui establir a tal efecte, i en particular, informació referent a ciberamenaces, vulnerabilitats, indicadors de compromís, declaracions d'aplicabilitat, tàctiques, tècniques i procediments, alertes de ciberseguretat i eines de configuració, sempre que aquest intercanvi d'informació:

i. es faci amb l'objectiu de prevenir les possibles ciberamenaces, descoratjar-les, detectar-les, i respondre o mitigar els incidents;

ii. reforci el nivell de ciberseguretat, en particular, en conscienciar sobre les ciberamenaces, limiti o impedeixi la capacitat de tals amenaces per propagar-se, o recolzi una bateria de capacitats de defensa,

Dipòsit legal: AND.2-2015

correcció i divulgació de les vulnerabilitats, tècniques de detecció d'amenaces, estratègies de mitigació o etapes de resposta i recuperació.

Aquest intercanvi es posarà en pràctica mitjançant mecanismes d'intercanvi d'informació que respectin la possible naturalesa delicada de la informació compartida, i amb el que pugui establir-se reglamentàriament.

7. El DSI pot formar part de la plantilla laboral de l'entitat que el nomena o exercir les seves funcions en el marc d'un contracte de serveis.

8. Les entitats essencials i importants han de garantir, a títol enunciatiu i no limitatiu, que el DSI:

a) Sigui una persona o un grup de persones amb coneixements especialitzats i amb experiència en matèria de ciberseguretat, tant des del punt de vista organitzatiu com des del tècnic i jurídic, en virtut de les funcions assignades a l'apartat 6.

b) Se li garanteixen els recursos necessaris per a l'exercici de les seves funcions.

c) Se li atorgui una posició dins de l'organització de l'entitat que faciliti l'exercici de les seves funcions per poder participar de manera adequada, i en temps oportú, en totes les qüestions relatives a la seguretat, així com el manteniment d'una comunicació real i efectiva amb l'alta direcció.

d) S'asseguri la seva independència respecte dels responsables de les infraestructures crítiques, les xarxes i els sistemes d'informació del seu àmbit de treball.

Article 19. *Representant al Principat d'Andorra*

1. Si una entitat que presta serveis essencials o importants al Principat d'Andorra no està establerta en aquest, designarà un representant al Principat d'Andorra que estigui sotmès a la jurisdicció del país. En absència d'aquest representant, l'ANC-AD podrà identificar l'entitat essencial o important, informar-la de les seves obligacions recollides en aquesta Llei i emprendre accions legals contra ella per l'incompliment d'aquestes.

2. La designació d'un representant per una entitat prevista a l'apartat 1 s'entendrà sense perjudici de les accions legals que puguin emprendre's contra la pròpia entitat.

Article 20. *Utilització d'esquemes de certificació de la ciberseguretat*

1. A l'efecte de demostrar la conformitat amb determinats requisits que s'estableixen en aquesta Llei, les autoritats nacionals competents podran exigir a les entitats essencials i importants, o a categories d'entitats essencials o importants, del seu àmbit de competència, que certifiquin determinats productes, serveis i processos de TIC en virtut d'un esquema de certificació de la ciberseguretat específic adoptat reglamentàriament. Els productes, serveis o processos objecte de la certificació poden ser desenvolupats per l'entitat essencial o important o adquirits a tercers.

2. Igualment, una vegada s'hagi establert reglamentàriament un esquema de certificació d'un àmbit de la ciberseguretat, les autoritats nacionals competents podran emetre un certificat en relació amb el dit àmbit per aquelles entitats essencials o importants que acrediten el compliment de les obligacions de seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació corresponents.

Article 21. *Protecció del notificador*

1. La notificació voluntària no donarà lloc a la imposició d'obligacions addicionals a l'entitat notificant a les quals no estaria subjecta de no haver presentat aquesta notificació.

2. El DSI que faci la notificació, tingui relació laboral o mercantil amb l'entitat que l'ha nomenat, o la persona que notifiqui en el cas d'entitats no obligades, en cap cas pot patir conseqüències negatives en el seu lloc de treball o en la seva relació amb l'entitat a causa que procedeixi a notificar un incident d'acord amb el que es disposa en aquesta Llei, a excepció d'aquells casos en els quals quedi acreditada una mala fe en la seva actuació.

Dipòsit legal: AND.2-2015

3. Són nul·les i sense efecte legal totes aquelles decisions del patró que es prenguin en perjudici o detriment dels drets laborals dels treballadors que hagin actuat de conformitat amb el que es disposa a l'article 15 o l'article 16.

Capítol tercer. Obligacions de supervisió

Article 22. *Supervisió del compliment d'obligacions de seguretat i de notificacions d'incidents*

1. Cada autoritat nacional competent s'encarregarà de supervisar el compliment d'aquesta Llei, i en especial les obligacions descrites als articles 13 i 15, que siguin aplicables a les entitats essencials i importants en el seu àmbit d'actuació competent.

2. Cada entitat essencial o important ha de col·laborar amb la seva autoritat nacional competent en la supervisió esmentada, i facilitar les actuacions d'inspecció, proporcionar tota la informació que a aquest efecte se li requereixi i aplicar les instruccions dictades.

3. Cada autoritat nacional competent pot dur a terme les actuacions inspectores que siguin necessàries per a l'exercici de les seves funcions de control en el seu àmbit de competència quan tinguin com a objecte:

a) Controlar el compliment de les normes i instruccions tècniques que, si escau, siguin aplicables a les entitats subjectes a la seva supervisió.

b) Verificar el compliment de les funcions del DSI designat en les entitats de serveis essencials i importants.

c) Fer les inspeccions, comprovacions, proves i revisions necessàries per verificar el compliment de les mesures de seguretat previstes en aquesta Llei i, en particular, de l'aplicabilitat de la política de seguretat de les entitats i l'aplicació de les pertinents mesures de seguretat.

4. Sempre que ho requereixi una autoritat nacional competent, el CSIRT-AD ha de col·laborar en l'exercici de les funcions a les quals es refereix l'apartat anterior. Especialment, el CSIRT-AD ha de facilitar assessorament tècnic sobre la idoneïtat de les mesures de seguretat adoptades per les entitats per proveir els seus serveis essencials o importants.

Article 23. *Supervisió i execució en el cas d'entitats essencials*

1. Cada autoritat nacional competent ha de vetllar perquè les entitats essencials del seu àmbit de competència compleixen amb les obligacions establertes en aquesta Llei de forma efectiva, proporcionada i dissuasiva.

2. Les competències de les autoritats nacionals competents, en cooperació amb el CSIRT-AD si escau, en matèria de supervisió, es fomenten en:

a) Inspeccions *in situ* i supervisió a distància, incloent controls aleatoris;

b) Auditories periòdiques;

c) Auditories de seguretat específiques basades en avaluacions de riscos o en informació disponible sobre riscs;

d) Anàlisis de seguretat a través de criteris d'avaluació de riscs objectius, no discriminatoris, justos i transparents;

e) Sol·licituds de tota la informació necessària per avaluar les mesures de ciberseguretat adoptades per l'entitat, en particular les polítiques de ciberseguretat documentades, així com el compliment del procediment de notificació previst en aquesta Llei, si és necessari;

f) Sol·licituds d'accés a dades, documents o qualsevol informació necessària per al desenvolupament de les seves funcions de supervisió; i

g) Sol·licituds de tota mena de proves necessàries per acreditar l'aplicació de les polítiques de ciberseguretat.

Dipòsit legal: AND.2-2015

Respecte a les lletres e), f) i g), en tot moment l'autoritat nacional competent ha d'indicar la finalitat de la sol·licitud i especificar la informació requerida.

3. Les competències de les autoritats nacionals competents, en cooperació amb el CSIRT-AD si escau, en matèria d'execució, es fomenten en:

a) Advertir a les entitats per l'incompliment de les obligacions establertes en aquesta Llei.

b) Emetre instruccions vinculants perquè les entitats corregeixin les deficiències detectades o les infraccions de les obligacions establertes en aquesta Llei.

c) Exigir a les entitats que posin fi a les conductes que incompleixen les obligacions establertes en aquesta Llei i que s'abstinguin a repetir-les.

d) Exigir a les entitats que adeqüin les seves mesures de gestió de riscos o obligacions de notificació a l'establert en el capítol primer d'aquest Títol.

e) Ordenar a les entitats que informin les persones físiques o jurídiques a les quals presten serveis que es poden veure afectades per una ciberamenaça significativa i de les corresponents mesures correctores o de protecció que les dites persones poden adoptar en resposta a l'amenaça.

f) Ordenar a les entitats l'aplicació, en un termini raonable, de les recomanacions formulades després d'haver realitzat una auditoria de seguretat.

g) Designar a un responsable de supervisió per dur a terme unes funcions clarament definides i perquè supervisi, durant un període determinat, el compliment de les seves obligacions previstes al Títol III.

h) Ordenar a les entitats que facin públics d'una forma concreta els incompliments de les obligacions establertes en aquesta Llei.

i) Emetre comunicats públics en els quals s'identifiqui a les persones físiques i jurídiques responsables d'incompliments d'obligacions establertes en aquesta Llei i la naturalesa dels dits incompliments.

j) Imposar, en el cas de l'ANC-AD, o sol·licitar la imposició per part de l'ANC-AD, en el cas de l'AFA, d'una multa administrativa de conformitat amb el previst al Títol IV, a títol addicional o substitutiu de les mesures referides a les lletres a) a i) d'aquest apartat, en funció de les circumstàncies de cada cas particular.

4. Quan les mesures d'execució exigides per l'autoritat nacional competent no s'adoptin en el termini establert, l'autoritat nacional competent està facultada per:

a) Suspendre la certificació de compliment;

b) Imposar una prohibició temporal sobre qualsevol persona física que exerceixi responsabilitats de direcció o representació legal de l'entitat essencial, i de qualsevol altra persona física responsable de l'incompliment, d'exercir les funcions de direcció en aquesta entitat.

Aquestes suspensions o prohibicions romanen fins que l'entitat referida adopti les mesures necessàries per resoldre les deficiències o compleixi els requisits de l'autoritat nacional competent que hagi aplicat la suspensió o prohibició de què es tracti.

5. Les mesures indicades a l'apartat anterior, s'apliquen sense perjudici de garantir el dret de defensa de la persona afectada, com a mínim en els següents aspectes:

a) La gravetat de l'incompliment i la importància de les obligacions infringides, i en especial les classificades com a greus i molt greus d'acord amb l'article 34;

b) La durada de l'incompliment, en particular si hi ha hagut incompliments reiterats;

c) Els perjudicis o les pèrdues reals originats, o els perjudicis o les pèrdues que podrien haver-se originat, en la mesura en què puguin determinar-se i tot tenint en compte, entre d'altres, les pèrdues financeres o econòmiques reals o potencials, els efectes per a altres serveis i el nombre d'usuaris afectats o potencialment afectats;

Dipòsit legal: AND.2-2015

d) La intencionalitat o negligència en la infracció;

e) Les mesures adoptades per l'entitat per prevenir o reduir els perjudicis o les pèrdues;

f) L'adhesió a codis de conducta o a mecanismes de certificació aprovats; i

g) El grau de cooperació de les persones físiques o jurídiques responsables amb les autoritats nacionals competents.

6. L'autoritat nacional competent ha d'emetre les decisions d'execució de forma detallada i motivada, notificant prèviament a l'emissió definitiva de les mateixes, a les entitats afectades, concedint-les un termini de sis mesos per formular observacions.

Article 24
Supervisió i execució en el cas d'entitats importants

1. Si l'autoritat nacional competent disposa de proves o d'indicis d'incompliment de les obligacions establertes en aquesta Llei, per part d'una entitat de serveis importants, l'autoritat referida pot imposar *a posteriori* les mesures de supervisió corresponents.

2. En aquest sentit, les competències de l'autoritat nacional competent, en cooperació amb el CSIRT-AD, si escau, en matèria de supervisió, es fomenten en:

a) Inspeccions *in situ* i supervisió *a posteriori*;

b) Auditories de seguretat específiques basades en avaluacions de riscos o en la informació disponible sobre els riscos;

c) Anàlisis de seguretat basades en criteris d'avaluació de riscs objectius, justos i transparents;

d) Sol·licituds de tota informació necessària per avaluar *a posteriori* les mesures de ciberseguretat, en particular les polítiques de ciberseguretat documentades, així com el compliment de les obligacions de notificar incidents a l'autoritat nacional competent; i

e) Sol·licitar l'accés a dades o qualsevol informació necessària per al correcte desenvolupament de funcions de supervisió.

Respecte a les lletres d) i e), en tot moment, l'autoritat nacional competent ha d'indicar la finalitat de la sol·licitud i especificar la informació requerida.

3. Les competències de l'autoritat nacional competent, en cooperació amb el CSIRT-AD, si escau, en matèria d'execució, es fomenten en:

a) Advertir a les entitats per l'incompliment de les obligacions establertes en aquesta Llei.

b) Emetre instruccions vinculants perquè les entitats resolguin les deficiències detectades o les infraccions de les obligacions establertes en aquesta Llei.

c) Exigir a les entitats que posin fi a les conductes que incompleixen les obligacions establertes en aquesta Llei i que s'abstinguin a repetir-les;

d) Exigir a les entitats que adeqüin les seves mesures de gestió de riscos o obligacions de notificació a l'establert al Títol III.

e) Ordenar a les entitats que informin les persones físiques o jurídiques a les quals els presten serveis que es poden veure afectades per una ciberamenaça significativa i de les corresponents mesures correctores o de protecció que les persones afectades poden adoptar en resposta a l'amenaça.

f) Ordenar a les entitats l'aplicació, en un termini raonable, de les recomanacions formulades després d'haver realitzat una auditoria de seguretat.

g) Designar un responsable de supervisió per dur a terme unes funcions clarament definides i perquè supervisi, durant un període determinat, el compliment de les obligacions previstes en el Títol III.

Dipòsit legal: AND.2-2015

h) Ordenar a les entitats que facin públics d'una forma concreta els incompliments de les obligacions establertes en aquesta Llei.

i) Emetre comunicats públics en els quals s'identifiqui a les persones físiques i jurídiques responsables d'incompliments d'obligacions establertes en aquesta Llei i la naturalesa dels dits incompliments.

j) Imposar o sol·licitar la imposició d'una multa administrativa de conformitat amb l'establert al Títol IV, a títol addicional o substitutiu de les mesures referides en les lletres a) a i) d'aquest apartat, en funció de les circumstàncies de cada cas particular.

4. És igualment aplicable a les entitats importants, el previst en els apartats 4 a 6 de l'article 23.

Capítol quart. Altres obligacions de les autoritats nacionals competents i del CSIRT-AD

Article 25. *Obligacions de les autoritats nacionals competents*

1. Les autoritats nacionals competents a l'empara d'aquesta Llei han de cooperar i intercanviar informació amb els responsables de redactar els reglaments o altres normes o actes jurídics sectorials, en particular, en relació amb la gestió dels riscos de ciberseguretat i dels incidents que afectin les entitats essencials o importants, així com amb el que respecta a les mesures de ciberseguretat adoptades per aquestes entitats.

2. Les autoritats nacionals competents hauran d'establir els canals que fomentin la comunicació amb les entitats que presten serveis essencials i importants, susceptibles de ser desplegats reglamentàriament.

3. Les autoritats nacionals competents hauran de coordinar-se amb el CSIRT-AD mitjançant els protocols d'actuació que, si escau, es poden desplegar reglamentàriament.

4. L'ANC-AD, en col·laboració amb l'AFA i amb el CSIRT-AD, haurà de:

a) Establir una llista de les entitats identificades a l'empara dels punts b) a f) de l'article 2.2 en el termini de sis mesos a comptar de la data d'entrada en vigor d'aquesta Llei, la qual revisarà periòdicament, almenys cada dos anys, i actualitzarà quan s'escaigui.

b) Crear i mantenir un registre d'entitats essencials i importants.

c) Notificar, sense dilació indeguda, a les agències de ciberseguretat existents en altres països qualsevol incident o ciberamenaça que tingui un impacte transfronterer o els pugui perjudicar o afectar de qualsevol altra forma i el seu nivell es consideri significatiu d'acord amb l'establert a l'article 15.3. En fer-ho, l'ANC-AD preservarà, de conformitat amb la legislació vigent en cada moment, la seguretat i els interessos comercials de l'entitat que ha notificat l'incident, així com la confidencialitat de la informació facilitada.

d) Cooperar, en l'àmbit d'aplicació d'aquesta Llei, amb l'Agència Andorrana de Protecció de Dades (APDA) i les autoritats públiques competents en seguretat pública, seguretat ciutadana i seguretat nacional, incloent-hi la comunicació sense dilació de qualsevol incident que pugui estar en l'àmbit de supervisió de cada autoritat, i mantenir-les informades sobre l'evolució d'aquests incidents.

e) Emetre informes anuals per al Govern d'Andorra sobre els incidents, quasiincidents i ciberamenaces notificats per les entitats essencials i importants, l'estat de l'aplicació de l'Estratègia Nacional de Ciberseguretat i de la situació de la ciberseguretat al Principat d'Andorra. Aquests informes de situació inclouen, a títol informatiu i no limitatiu, entre d'altres:

i. L'evolució de les capacitats de la ciberseguretat al Principat d'Andorra.

ii. Els recursos tècnics, financers i humans disponibles per a les autoritats nacionals competents i el CSIRT-AD.

iii. Les polítiques de ciberseguretat i l'aplicabilitat de les mesures de supervisió i d'execució en funció dels resultats sorgits en l'informe anterior.

iv. Un índex de ciberseguretat que proporcioni una avaluació del nivell de maduresa de les capacitats de ciberseguretat i que estigui establert segons les metodologies reconegudes internacionalment.

f) Emetre i publicar informes anuals sobre la situació de la ciberseguretat al Principat d'Andorra.

Dipòsit legal: AND.2-2015

g) Comparèixer, per mitjà de la seva persona de tutela, davant de la comissió legislativa del Consell General que tracti les qüestions en matèria de ciberseguretat, per tal de presentar els informes anuals previstos en les lletres e) i f), relatius als incidents, quasiincidents i ciberamenaces notificats per les entitats essencials i importants, a l'estat de l'aplicació de l'Estratègia Nacional de Ciberseguretat i a la situació de la ciberseguretat al Principat d'Andorra.

h) Vetllar, a l'efecte de contribuir a la seguretat, estabilitat i resiliència del DNS, perquè els registres de dominis de primer nivell i les entitats que proveeixen serveis de registre de noms de domini de primer nivell:

i. Recopilin i mantinguin dades sobre el registre de noms de domini en una base de dades que:

• Contingui informació pertinent per identificar i contactar amb els titulars dels noms de domini i els punts de contacte que administren els noms de domini en els dominis de primer nivell.

• Compti amb polítiques i procediments, que es trobin a disposició del públic, per garantir que inclogui informació precisa i completa.

ii. Publiquin, sense demora indeguda després del registre d'un nom de domini, les dades de registre de domini que no siguin de caràcter personal.

iii. Concedeixin accés a dades específiques sobre el registre de noms de domini, prèvia sol·licitud lícita i degudament justificada, als sol·licitants d'accés legítims, de conformitat amb la normativa del Principat d'Andorra en matèria de protecció de dades vigent en cada moment.

5. A fi de promoure una aplicació convergent amb la dels estats veïns, les autoritats nacionals competents publicaran un marc normatiu mitjançant el qual fomentin, sense imposar ni afavorir l'ús d'un tipus específic de tecnologia, la utilització de normes i especificacions acceptades a escala internacional que siguin pertinents en matèria de seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació de cada sector del seu àmbit de competència.

6. Addicionalment a les anteriors obligacions, les autoritats nacionals competents podran establir obligacions específiques per garantir la seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació necessaris per prestar serveis essencials o importants i sobre notificació d'incidents, i dictar instruccions tècniques i guies orientatives per detallar el contingut d'aquestes obligacions.

Article 26. *Obligacions del CSIRT-AD*

1. El CSIRT-AD tindrà com a principals obligacions:

a) Garantir la disponibilitat dels seus serveis de comunicació, establint diversos canals de comunicació per ser contactat i contactar-hi directament i en tot moment, evitant errors ocasionals simples.

b) Especificar els canals i les vies de comunicació i donar-los a conèixer als seus grups d'interès.

c) Garantir que les seves instal·lacions i els seus sistemes d'informació necessaris per al compliment de l'objectiu d'aquesta Llei es situen en llocs segurs.

d) Disposar d'un sistema adequat per gestionar i canalitzar les sol·licituds.

e) Disposar de personal suficient per garantir la disponibilitat dels serveis que presta en relació amb aquesta Llei en tot moment.

f) Mantenir l'accés continuat a les infraestructures de comunicació, potenciant els sistemes redundants i els espais de treball de reserva amb l'objectiu de salvaguardar la continuïtat de la seva activitat en relació amb el previst en aquesta Llei.

g) Proporcionar a les entitats essencials o importants que es puguin veure afectades per incidents, la informació que els pugui ser rellevant per prevenir i si escau resoldre els dits incidents.

h) Proporcionar a les entitats essencials o importants notificadores, la informació pertinent respecte al seguiment de la notificació d'un incident, en particular aquella que pugui facilitar la gestió eficaç de l'incident.

i) Garantir la capacitat de participar, si escau, en xarxes de cooperació internacional.

Dipòsit legal: AND.2-2015

Article 27. *Cooperació nacional*

1. L'ANC-AD, l'AFA i el CSIRT-AD cooperaran entre si per vetllar pel compliment de les obligacions establertes en aquesta Llei.

2. L'ANC-AD i el CSIRT-AD cooperaran entre si per garantir la recepció de notificacions d'incidents, quasiincidents, vulnerabilitats o ciberamenaces significatius, en el marc d'aquesta Llei i amb el suport de les autoritats públiques del Principat d'Andorra.

3. L'ANC-AD, l'AFA i el CSIRT-AD han de consultar, quan sigui procedent, als òrgans amb competències en matèria de seguretat nacional, seguretat pública, seguretat ciutadana i protecció de dades de caràcter personal, i hi han de col·laborar en l'exercici de les seves respectives funcions establertes per aquesta Llei.

Article 28. *Cooperació transfronterera*

1. Quan sigui procedent, les autoritats nacionals competents i el CSIRT-AD han de cooperar amb les autoritats competents d'altres països quan aquestes requereixin la supervisió a què es refereixen els articles 23 i 24 i l'adopció de mesures per part d'entitats essencials o importants per als seus països i que tinguin relació amb el Principat d'Andorra. Aquesta cooperació implicarà, com a mínim, el següent:

a) que les autoritats nacionals competents que apliquin mesures de supervisió o execució en el Principat d'Andorra informin i consultin a les autoritats competents dels altres països afectats sobre les mesures de supervisió i execució adoptades i el seu seguiment, de conformitat amb l'establert als articles 23 i 24;

b) que una autoritat competent estrangera pugui sol·licitar a una autoritat nacional competent que adopti les mesures de supervisió o execució a què es refereixen els articles 23 i 24;

c) que una autoritat nacional competent, en rebre una sol·licitud justificada d'una autoritat competent estrangera, presti a aquesta última assistència perquè les mesures de supervisió o execució a què es refereixen els articles 23 i 24 puguin aplicar-se de manera efectiva, eficient i coherent. Aquesta assistència podrà abastar sol·licituds d'informació i mesures de supervisió, incloses les sol·licituds per a la realització d'inspeccions in situ, supervisió a distància o auditories de seguretat específiques.

Les autoritats nacionals competents o el CSIRT-AD podran negar-se a cooperar amb autoritats competents d'altres països quan, després de dialogar amb les altres autoritats nacionals competents i l'ANC-AD, l'ANC-AD determini que o bé l'autoritat competent estrangera manca de competències per demanar l'assistència requerida, o bé aquesta assistència no s'adequa ni a les tasques del CSIRT-AD ni a les tasques de supervisió de l'autoritat nacional competent de què es tracti exercides de conformitat amb els articles 23 i 24.

2. Recíprocament, quan sigui procedent, les autoritats nacionals competents o el CSIRT-AD podran demanar la cooperació d'autoritats competents o CSIRT d'altres països quan requereixin la supervisió a què es refereixen els articles 23 i 24 o l'adopció de mesures per part d'entitats essencials o importants per al Principat d'Andorra i que estiguin establertes o representades en aquests altres països, amb independència que el dit establiment sigui o no l'establiment principal de l'entitat i, en el cas de les entitats que prestin serveis essencials per al Principat d'Andorra, fins i tot quan aquesta estigui representada al país.

3. Quan s'escaigui i de comú acord, les autoritats competents del Principat d'Andorra i les d'altres països podran emprendre conjuntament les mesures de supervisió a què es refereixen els articles 23 i 24.

4. Si el CSIRT-AD o l'ANC-AD o l'AFA reben notificacions per part de països tercers sobre incidents que afecten directament o indirectament a entitats essencials o importants del Principat d'Andorra, s'ho han de notificar de forma immediata i entre aquestes entitats i a les entitats afectades, perquè conjuntament adoptin les mesures pertinents en l'exercici de les seves funcions respectives.

Article 29. *Confidencialitat de la informació sensible*

1. L'ANC-AD, l'AFA i el CSIRT-AD han de preservar la seguretat i els interessos comercials de les entitats essencials o importants, així com la confidencialitat de la informació que obtenen d'aquestes en l'exercici de les funcions que els encomana aquesta Llei.

Dipòsit legal: AND.2-2015

2. Quan l'intercanvi d'informació sigui necessari i es tracti d'informació sensible, s'ha de limitar la cessió d'acord amb la correcta aplicació dels principis de minimització de la informació i de proporcionalitat per a la finalitat d'aquest intercanvi.

Títol IV. Règim sancionador

Article 30. *Potestat sancionadora*
1. Tota actuació que contradigui el que estableix aquesta Llei o les disposicions reglamentàries que la desenvolupin, 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.

2. La potestat per incoar i resoldre els expedients sancionadors per raó de l'establert en aquesta Llei correspon a l'autoritat que en cada moment estigui al capdavant de l'ANC-AD, també pel que fa a les entitats que estiguin sota la supervisió de l'AFA, a petició d'aquesta última. La instrucció dels expedients correspon als tècnics designats per l'ANC-AD.

Article 31. *Responsables de les infraccions*
Són responsables de les infraccions respecte al que regula aquesta Llei, les entitats essencials i importants sotmeses al compliment dels preceptes establerts en la mateixa.

Article 32. *Expedient sancionador*
1. La constatació d'una infracció per part de l'autoritat nacional competent que correspongui comporta la incoació de l'expedient sancionador corresponent per part de l'autoritat que disposa de la potestat sancionadora, d'acord amb el que disposi la normativa vigent en cada moment en matèria de procediments administratius sancionadors. No obstant això, el termini màxim de durada del procediment és d'un any, mentre que el termini d'al·legacions no pot tenir una durada inferior als sis mesos indicats a l'article 23.6.

2. S'atorga a les actes de l'ANC-AD la presumpció d'exactitud, llevat de prova en contra.

3. Contra les resolucions dictades per l'autoritat que disposa de la potestat sancionadora es pot interposar recurs, d'acord amb el que disposi la normativa en vigor en cada moment en matèria de recursos administratius.

Article 33. *Infraccions*
Constitueixen infraccions al que regula aquesta Llei les accions o omissions contràries a l'establert als seus preceptes.

Article 34. *Classificació de les infraccions*
1. Les infraccions dels preceptes continguts en aquesta Llei es classifiquen en molt greus, greus i lleus.

2. Són infraccions molt greus:

a) La falta de remissió de la informació relativa a l'obligació d'identificació com entitat essencial o important, de conformitat amb el previst a l'article 10, quan aquesta disposi d'un establiment al Principat d'Andorra o quan l'ANC-AD ha informat l'entitat que no disposa d'establiments al Principat d'Andorra sobre les seves obligacions d'acord amb l'establert en aquesta Llei

b) La falta d'adopció de mesures per esmenar les deficiències detectades, segons el que es disposa a l'article 23.3.b) i a l'article 24.3.b), quan aquestes deficiències suposin vulnerabilitats a incidents amb efectes pertorbadors significatius sobre un o més serveis essencials o importants, i l'entitat no hagi atès els requeriments dictats per l'autoritat nacional competent amb anterioritat a la producció de l'incident.

c) L'incompliment reiterat de l'obligació de notificar incidents amb efectes pertorbadors significatius en el servei d'acord amb el previst a l'article 15. Es considera que és reiterat a partir del segon incompliment.

Dipòsit legal: AND.2-2015

d) No adoptar les mesures necessàries per resoldre els incidents conformement a l'assenyalat a l'article 14 quan aquests tinguin un efecte pertorbador significatiu en la prestació de serveis essencials o de serveis importants al Principat d'Andorra o en altres països.

3. Són infraccions greus:

a) L'incompliment de la resta d'obligacions que aquesta Llei estableix per a les entitats essencials o importants, que no siguin qualificades com a infraccions molt greus ni lleus de conformitat amb l'establert en aquest article. Queden exemptes les entitats essencials i importants que no disposin d'un establiment al Principat d'Andorra, en tant l'ANC-AD no les hagi notificat la seva condició d'entitat essencial o important per al Principat d'Andorra i les obligacions que els hi són d'aplicació d'acord amb aquesta Llei.

b) L'incompliment de les disposicions reglamentàries o de les instruccions tècniques de seguretat dictades per l'autoritat nacional competent que correspongui sobre les precaucions mínimes que les entitats essencials o importants han d'adoptar per garantir la seguretat de les infraestructures crítiques, les xarxes i els sistemes d'informació necessaris per prestar els dits serveis.

4. Són infraccions lleus:

a) L'incompliment de les disposicions reglamentàries o de les instruccions tècniques de seguretat dictades per l'autoritat nacional competent a l'empara d'aquesta Llei, quan no suposi una infracció greu.

b) No completar la informació que ha de reunir la notificació d'incidents tenint en compte el que es disposa a l'article 15.1, o, si escau, no remetre l'informe justificatiu sobre la impossibilitat de reunir la informació prevista en el dit article.

Article 35. *Infraccions que comporten una violació de la seguretat de les dades personals*

1. Quan l'autoritat nacional competent que correspongui tingui indicis que l'incompliment de les obligacions establertes en aquesta Llei, comès per una entitat essencial o important, comporta una violació de la seguretat de les dades personals, i que, per tant, hagi de notificar-se segons el que es disposa a l'article 27.3, ha d'informar a l'APDA, en un termini de temps raonable.

2. Si l'APDA decideix exercir les seves facultats i imposar una multa administrativa, l'ANC-AD no ha d'imposar una multa administrativa per la mateixa infracció. No obstant això, l'autoritat nacional competent que correspongui pot aplicar les mesures o facultats previstes als apartats 3 (llevat del punt 3.j) i 4 de l'article 23 i als apartats 3 (llevat del punt 3.j) i 4 de l'article 24.

Article 36. *Sancions*

1. Per la comissió de les infraccions tipificades a l'article 34, seguint els principis d'efectivitat, proporcionalitat i dissuasió, s'imposen les següents sancions, que són aplicables amb independència que l'entitat infractora sigui o no una entitat de l'administració pública:

a) Per la comissió d'infraccions molt greus, multa administrativa de 30.001 euros fins a 100.000 euros.

b) Per la comissió d'infraccions greus, multa administrativa de 15.001 euros fins a 30.000 euros.

c) Per la comissió d'infraccions lleus, amonestació o multa administrativa de 500 euros fins a 15.000 euros.

2. Aquestes multes s'han d'imposar atenent les circumstàncies de cada cas individual, a títol addicional o substitutiu de les mesures que hagin d'adoptar-se perquè cessin o es corregeixin els efectes de la infracció. Per a la decisió sobre la imposició de multes administratives i la seva quantia, s'han de tenir en compte, en cada cas particular i com a mínim, els elements previstos a l'article 37.

3. Addicionalment, es poden imposar multes coercitives per obligar una entitat essencial o important a posar fi a una infracció de conformitat amb una decisió prèvia de l'ANC-AD.

4. L'import recaptat en aplicació de les sancions previstes en aquesta Llei es destina a finançar el pressupost propi de l'ANC-AD.

Dipòsit legal: AND.2-2015

Article 37. *Graduació de les sancions*
L'autoritat que disposa de la potestat sancionadora ha de graduar les sancions previstes en aquest Títol atesos els següents criteris:

a) El grau de culpabilitat o l'existència d'intencionalitat.

b) La continuïtat o persistència en la conducta infractora.

c) La naturalesa i quantia dels danys i perjudicis causats.

d) La reincidència, per comissió en l'últim any de més d'una infracció de la mateixa naturalesa, quan així s'hagi declarat per resolució ferma en via administrativa.

e) El nombre d'usuaris afectats.

f) El volum de facturació de l'entitat infractora.

g) La utilització per l'entitat infractora de programes de recompensa pel descobriment de vulnerabilitats en les infraestructures crítiques, les xarxes i els sistemes d'informació, siguin propis o de tercers, que resultin necessaris per prestar els seus serveis.

h) Les accions realitzades per l'entitat infractora per pal·liar els efectes o les conseqüències de la infracció.

Article 38. *Proporcionalitat de les sancions*
1. L'autoritat que disposa de la potestat sancionadora pot graduar la quantia de la sanció aplicant l'escala relativa a la classe d'infraccions anterior en gravetat a aquella en què s'integra la infracció considerada en el cas de què es tracti quan concorrin els següents supòsits:

a) Quan s'aprecïi una qualificada disminució de la culpabilitat de l'entitat infractora conseqüència de la concurrència significativa de diversos dels criteris enunciats a l'article 37.

b) Quan l'entitat infractora hagi regularitzat la situació irregular de manera diligent.

c) Quan l'entitat infractora hagi reconegut espontàniament la seva culpabilitat.

2. Atesa la naturalesa dels fets i la concurrència significativa dels supòsits indicats en l'apartat anterior, l'autoritat que disposa de la potestat sancionadora pot no acordar l'inici del procediment sancionador, procedint, en el seu lloc, a advertir a l'entitat infractora perquè, en el termini que l'autoritat que disposa de la potestat sancionadora determini, acrediti l'adopció de les mesures correctores que, en cada cas, resultin pertinents, sempre que concorrin els següents pressupòsits:

a) Que els fets siguin constitutius d'infracció lleu o greu conforme al que es disposa en aquesta Llei.

b) Que no s'hagi sancionat o advertit a l'entitat infractora en els dos anys previs per la comissió d'infraccions previstes en aquesta Llei.

En cas que l'advertiment no s'atengui en el termini que l'autoritat determini, es procedirà a l'obertura del corresponent procediment sancionador per raó d'aquest incompliment.

Article 39. *Concurrència d'infraccions*
1. No procedeix la imposició de sancions segons el que es preveu en aquesta Llei quan els fets constitutius de la infracció ho siguin també d'una altra tipificada en la normativa sectorial a la qual estigui subjecte el prestador del servei i existeixi identitat del bé jurídic protegit.

2. En cas que, a conseqüència d'una actuació sancionadora, es tingui coneixement de fets que puguin ser constitutius d'infraccions tipificades en altres lleis, s'informa dels mateixos als òrgans o organismes competents per a la seva supervisió i sanció.

Dipòsit legal: AND.2-2015

Article 40. *Prescripció de les infraccions*
1. Les infraccions prescriuen en els terminis següents:

a) Les lleus, al cap d'un any.

b) Les greus, al cap de dos anys.

c) Les molt greus, al cap de tres anys.

2. L'inici d'una activitat inspectora suspèn el termini de prescripció de les infraccions.

3. El termini de prescripció de les infraccions es computa des del dia en què cessa l'acció o l'omissió sancionable.

Article 41. *Prescripció de les sancions*
Les sancions per infraccions lleus prescriuen en el termini d'un any, les greus en el termini de dos anys i les molt greus en el termini de tres anys, a comptar de la data de notificació de la resolució sancionadora esdevinguda ferma.

Disposició addicional. Encomana al Govern

S'encomana al Govern que, en el termini màxim de divuit mesos a comptar de l'entrada en vigor d'aquesta Llei, avaluï la conveniència de constituir o no una entitat amb personalitat jurídica pròpia que assumeixi funcions diverses en matèria de digitalització, o relacionades amb aquesta matèria, incloent-hi l'Agència Nacional de Ciberseguretat del Principat d'Andorra (ANC-AD) i l'equip de referència de resposta del Principat d'Andorra per al tractament d'incidents de ciberseguretat (CSIRT-AD).

Disposició final primera. Modificació de la Llei 31/2021, del 22 de novembre, de text consolidat qualificada de seguretat pública

1. S'addiciona un apartat 3 a l'article 3 de la Llei 31/2021, del 22 de novembre, de text consolidat qualificada de seguretat pública, modificada per la Llei 4/2022, del 31 de gener, del pressupost per a l'exercici del 2022, el qual queda redactat com segueix:

"Article 3. *Deure de col·laboració*
[...]

3. De la mateixa manera, amb la mateixa finalitat, les autoritats i els funcionaris competents poden requerir l'ajuda i la col·laboració de l'Agència de Nacional de Ciberseguretat del Principat d'Andorra, així com la d'altres agències o organismes de control nacionals o d'altres estats amb potestats similars sobre àmbits i sectors concrets."

2. Es modifica l'article 27 de la Llei 31/2021, del 22 de novembre, de text consolidat qualificada de seguretat pública, modificada per la Llei 4/2022, del 31 de gener, del pressupost per a l'exercici del 2022, el qual queda redactat com segueix:

"Article 27. *Establiments i instal·lacions vulnerables*
Les armeries, les joieries, les entitats bancàries, les empreses de seguretat o de venda de material de seguretat, o qualsevol altre establiment o instal·lació que es pugui considerar especialment vulnerable o exposat en matèria de seguretat, incloses les entitats essencials o importants considerades com a tals en virtut de l'establert a la legislació vigent en cada moment en matèria de seguretat de les xarxes i dels sistemes d'informació, han de disposar de les mesures de protecció que s'estableixin per la via reglamentària, per prevenir la comissió d'actes delictius contra aquests establiments o instal·lacions i les persones que hi treballen o s'hi troben, o per evitar que generin riscos pel que fa a aquestes persones o terceres persones."

Disposició final segona. Desenvolupament reglamentari

S'autoritza el Govern per dictar les disposicions reglamentàries necessàries per desplegar i aplicar aquesta Llei.

Dipòsit legal: AND.2-2015

Disposició final tercera. Text consolidat

S'encomana al Govern, en els termes previstos a l'article 116 del Reglament del Consell General, que en el termini màxim de sis mesos des de l'entrada en vigor d'aquesta Llei presenti al Consell General el projecte de text consolidat de la Llei 31/2021, del 22 de novembre, de text consolidat qualificada de seguretat pública.

Disposició final quarta. Entrada en vigor

1. Aquesta Llei entra en vigor l'endemà de ser publicada al *Butlletí Oficial del Principat d'Andorra.*

2. No obstant l'establert en l'apartat anterior, el capítol tercer del Títol III i el Títol IV, entren en vigor en el termini de dos anys a comptar de l'entrada en vigor d'aquesta Llei.

Casa de la Vall, 9 de juny del 2022

Roser Suñé Pascuet
Síndica General

Nosaltres els coprínceps la sancionem i promulguem i n'ordenem la publicació en el *Butlletí Oficial del Principat d'Andorra.*

Joan Enric Vives Sicília
Bisbe d'Urgell
Copríncep d'Andorra

Emmanuel Macron
President de la República Francesa
Copríncep d'Andorra

Annex I. Entitats essencials

Sector	Subsector	Tipus d'entitats
1. Energia	a) Infraestructures energètiques	Infraestructures energètiques de fonts renovables a les quals es refereix el Decret del 16-05-2018 d'aprovació i publicació del Pla sectorial d'infraestructures energètiques d'Andorra.
		Infraestructures de producció de calor centralitzades a les quals es refereix el Decret del 16-05-2018 d'aprovació i publicació del Pla sectorial d'infraestructures energètiques d'Andorra.
		Infraestructures de transport i transformació d'energia elèctrica a les quals es refereix el Decret del 16-05-2018 d'aprovació i publicació del Pla sectorial d'infraestructures energètiques d'Andorra.
		Infraestructures de distribució d'energia tèrmica a les quals es refereix el Decret del 16-05-2018 d'aprovació i publicació del Pla sectorial d'infraestructures energètiques d'Andorra.
	b) Electricitat	Entitat encarregada de la importació, generació, distribució i comercialització d'energia elèctrica d'acord amb la Llei 5-2016, del 10 de març, que regula l'ens públic Forces Elèctriques d'Andorra (FEDA) i el règim de les activitats dels sectors elèctric, del fred i de la calor.
		Empreses productores i distribuïdores d'electricitat.
		Participants del mercat elèctric que proporcionin emmagatzematge de l'energia, agregació o resposta de demanda.
	c) Carburants	Operadors d'instal·lacions de producció, refinació, processament, emmagatzematge i/o transport de petroli en virtut del Decret d'aprovació del Reglament d'emmagatzematge, subministrament, distribució i ús de hidrocarburants, del 28 de febrer del 2018.
	d) Gas	Empreses de subministrament, distribució, transmissió i/o sistemes d'emmagatzematge en virtut de la Llei d'ordenació del sector dels gasos combustibles de 22-6-2000 del Decret d'aprovació del Reglament d'emmagatzematge, subministrament, distribució i ús de gasos combustibles i les seves respectives modificacions.
	e) Calefacció urbana	Entitat encarregada de la importació, generació, distribució i/o comercialització de calefacció urbana.
	f) Hidrogen	Entitat de producció d'hidrogen, emmagatzematge i/o transmissió.

Dipòsit legal: AND.2-2015

2. Transport	a) Transports terrestres	Responsables de les companyies de transports terrestres i/o llicències d'acord amb la Llei 4/2015, del 15 de gener, dels transports per carretera.
		Autoritats públiques responsables de la planificació, el control o la gestió del trànsit.
		Operadors de sistemes de transport intel·ligents.
		Prestadors de serveis del transport sanitari d'acord amb el Decret 74/2021, del 10 de març del 2021.
	b) Transports ferroviaris	Administradors d'infraestructures ferroviàries
	c) Transports aeris	Operadors competents de transport d'aeronaus d'acord amb el Decret del 24-02-2016 pel qual s'aprova el Reglament d'aeronaus no tripulades, pilotades remotament i especialment, aquells que tenen una finalitat pública i/o comercial.
		Autoritat encarregada de regular, controlar, ordenar i verificar les activitats relatives a l'aviació civil dins de les fronteres del Principat d'Andorra.
3. Entitats financeres		Entitats financeres referides en la Llei 7/2013, del 9 de maig, sobre el règim jurídic de les entitats operatives del sistema financer andorrà i altres disposicions que regulen l'exercici de les activitats financeres al Principat d'Andorra i en la Llei 35/2010, del 3 de juny, de règim d'autorització per la creació de noves entitats operatives del sistema financer andorrà.
4. Mercats financers		Entitats operatives del sistema financer que, segons la normativa vigent en cada moment, estiguin autoritzades per actuar al Principat d'Andorra i donin compliment als requisits legals establerts
5. Sanitat	Establiments d'atenció sanitària[1]	Proveïdors de serveis de salut en el sentit exposat en el Decret legislatiu del 30-5-2018 de publicació del text refós de la Llei 6/2014, del 24 d'abril, de serveis socials i sociosanitaris.
		Laboratoris de referència, entitats que realitzen activitats de recerca i desenvolupament de medicaments, entitats que fabriquen productes farmacèutics de base i especialitats farmacèutiques, entitats que fabriquen productes sanitaris que es consideren essencials en situacions d'emergència de salut pública («la llista de productes sanitaris essencials es pot definir o modificar durant l'emergència de salut pública»).
6. Aigua	a) Aigües potables	Encarregats de la captació, el tractament, la distribució i el subministrament d'aigua destinada al consum humà en el sentit de la Llei de policia i protecció de les aigües.
	b) Aigües residuals	Empreses de recollida, disposició o tractament urbà, domèstic i industrial d'aigües residuals.
		Estacions depuradores d'aigües residuals previstes en el Decret del 25-2-2009 d'aprovació del procediment simplificat d'autorització d'abocaments d'aigües i d'obertura d'estacions depuradores d'aigües residuals.
	c) Aigües superficials	L'Administració encarregada del manteniment de l'estat natural de les aigües superficials, establint un règim de protecció i de control de les aigües previst en la Llei de policia i protecció de les aigües.
7. Infraestructures digitals		- Proveïdors de serveis de DNS; - Registres de noms de domini de nivell superior; - Proveïdors de punts d'intercanvi d'Internet; - Proveïdors de serveis de computació al núvol; - Proveïdors de serveis de centres de dades; - Proveïdores de xarxes de distribució de continguts; - Proveïdors de serveis de confiança d'acord amb la Llei 9/2021, del 29 d'abril, de modificació de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica; - Proveïdors de xarxes públiques de comunicacions electròniques i proveïdors de serveis de comunicacions electròniques.
8. Administració pública		Entitats de les administracions públiques del govern central.
		Entitats de les administracions públiques dels comuns o altres nivells organitzatius.

[1] Incloent-hi centres d'atenció primària, centres sociosanitaris, serveis socials, hospitals i clíniques privades.

Dipòsit legal: AND.2-2015

Annex II. Entitats importants

Sector	Subsector	Tipus d'entitats
1. Gestió de residus	a) Gestors	Gestors autoritzats a realitzar operacions de gestió de residus, tant si són productores de residus com si no ho són, previstos en la Llei 25/2004, del 14 de desembre de residus.
	b) Centre de transferència	Centres encarregats de condicionar i emmagatzemar transitòriament els residus abans de ser valoritzats o exportats, previstos en la Llei 25/2004, del 14 de desembre de residus.
	c) Deixalleria	Centres de deixalleria comunals o industrials, previstos en la Llei 25/2004, del 14 de desembre de residus.
	d) Centre de valorització	Centre de valorització destinat exclusivament a la recuperació total o parcial de residus per al seu aprofitament posterior, previst en la Llei 25/2004, del 14 de desembre de residus.
	e) Centre de triatge	Centre destinat a l'emmagatzematge, la classificació, la selecció i/o el condicionament de residus, hagin o no estat separats prèviament en el mateix lloc on s'han generat, amb la finalitat de valorització posterior, previst en la Llei 25/2004, del 14 de desembre de residus.
	f) Centre de transferència	Centre de transferència que condicionen i emmagatzemen transitòriament els residus abans de ser valoritzats o exportats, previst en la Llei 25/2004, del 14 de desembre de residus.
	g) Instal·lació de tractament tèrmic	Unitats tècniques o equips, fixes o mobilitats, dedicades al tractament tèrmic de residus, amb o sense recuperació de la calor originada per la combustió; l'emplaçament i la instal·lació completa, incloses totes les línies d'incineració, les instal·lacions de recepció, emmagatzematge i pretractament in situ dels residus; els sistemes d'alimentació de residus, combustible i aire; la caldera; les instal·lacions de tractament dels gasos de combustió; les instal·lacions de tractament in situ dels residus de la incineració i de les aigües residuals; la xemeneia; així com els dispositius i sistemes de control de les operacions d'incineració, de registre i de seguiment de les condicions d'incineració, previstos en la Llei 25/2004, del 14 de desembre de residus.
	h) Abocador	Entitat gestora de les instal·lacions d'eliminació dels residus mitjançant el seu dipòsit controlat en la superfície o sota terra, prevista en la Llei 25/2004, del 14 de desembre de residus.
2. Correus i missatgeria		Proveïdors de serveis postals i de missatgeria.
3. Fabricació, producció, distribució i comercialització de productes químics		Entitats encarregades de la fabricació de productes químics bàsics, compostos nitrogenats, fertilitzants, plàstics i cautxú sintètic en formes primàries
		Entitats encarregades de la fabricació de plaguicides i altres productes agroquímics.
		Entitats encarregades de la fabricació d'altres productes químics com els explosius, coles, olis essencials.
		Intermediaris del comerç de combustibles, minerals, metalls i productes químics industrials.
		Comerç a l'engròs de productes químics.
4. Producció d'aliments, processament i distribució		Empresa pública o privada que, amb o sense ànim de lucre, dugui a terme qualsevol activitat relacionada en qualsevol de les etapes de la producció, la transformació i la distribució d'aliments.

Dipòsit legal: AND.2-2015

5. Fabricació	a) Fabricació de productes sanitaris, de diagnòstic i de de diagnòstic in vitro	Entitats dedicades a la fabricació de productes sanitaris, entenent com a tals tots aquells instruments, dispositius, equips, programes informàtics, implants, reactius, materials o altres articles destinats pel fabricant a ser utilitzats en persones, per separat o en combinació, amb algun dels següents fins mèdics: - Diagnòstic, prevenció, seguiment, predicció, pronòstic, tractament o alleujament d'una malaltia. - Diagnòstic, seguiment, tractament, alleujament o compensació d'una lesió o d'una discapacitat. - Recerca, substitució o modificació de l'anatomia o d'un procés o estat fisiològic o patològic. - Obtenció d'informació mitjançant l'examen in vitro de mostres procedents del cos humà, incloent donacions d'òrgans, sang i teixits, i que no exerceix la seva acció principal prevista a l'interior o en la superfície del cos humà per mecanismes farmacològics, immunològics ni metabòlics, però a la funció dels quals puguin contribuir tals mecanismes. També s'inclouen les entitats dedicades a la fabricació de productes sanitaris per a diagnòstic in vitro, entenent com a tals aquells productes que, sense ser en si mateix un producte sanitari, estan destinats pel seu fabricant a ser usats de manera conjunta amb un o diversos d'aquests productes, per a permetre específicament que el producte o productes sanitaris pugui utilitzar-se conformement a la seva finalitat prevista o per a contribuir específica i directament a la funcionalitat mèdica dels productes sanitaris a l'efecte de la seva finalitat prevista. S'exclouen les entitats essencials dedicades a la prestació de serveis de salut en el sentit exposat en el Decret legislatiu del 30-5-2018 de publicació del text refós de la Llei 6/2014, del 24 d'abril, de serveis socials i sociosanitaris assenyalades en l'Annex I.
	b) Fabricació de productes informàtics, electrònics i dispositius òptics	Entitats dedicades a la fabricació d'ordinadors, perifèrics d'ordinador, equips de comunicació i productes electrònics, així com la fabricació de components per a aquests productes. S'entenen també incloses les entitats dedicades a la fabricació de productes electrònics de consum, equips de mesurament, prova i navegació, equips d'irradiació, electromèdics i electroterapèutics instruments i equips òptics, i la fabricació de mitjans magnètics i òptics.
	c) Fabricació d'equipament elèctric	Entitats dedicades a la fabricació de productes que generen, distribueixen i utilitzen energia elèctrica així com les dedicades a l'enllumenat elèctric, a la fabricació d'equips de senyalització o d'electrodomèstics. S'exclouen les entitats dedicades a la fabricació de productes informàtics, electrònics i dispositius òptics contingudes en l'Annex II b.
	d) Fabricació de maquinària i equipament que actua de manera independent sobre materials	Entitats dedicades a la fabricació de màquines i equips que actuen de manera independent sobre els materials, ja sigui mecànica o tèrmicament, o que realitzen operacions sobre els materials (com la manipulació, la polvorització, el pesatge o l'envasament), inclosos els components mecànics que produeixen i apliquen força, així com qualsevol peça primària fabricada especialment per a aquests fins. Així mateix, s'inclouen les entitats dedicades a la fabricació de dispositius fixos i mòbils o de mà, independentment que estiguin dissenyats per a un ús industrial, de construcció i d'enginyeria civil, agrícola o domèstic. i l'enginyeria civil, l'agricultura o la llar i les entitats dedicades a la fabricació d'equips especials per al transport de persones o mercaderies. També s'inclouen les entitats dedicades a la fabricació d'altres màquines d'ús especial, utilitzades o no en un procés de fabricació, com els equips d'atraccions de fira, els equips automàtics de pista de bitlles de bitlles, etc. S'exclouen les entitats dedicades a la fabricació de productes metàl·lics d'ús general, de dispositius de control associats, d'equips informàtics, d'equips de mesurament i assaig, dels aparells de distribució i control d'electricitat i de vehicles de motor d'ús general.
	e) Fabricació de vehicles de motor, tràilers y semi-tràilers	Entitats dedicades a la fabricació de vehicles de motor per al transport de passatgers o de mercaderies, incloent la fabricació de les seves peces i accessoris, així com la fabricació de remolcs i semiremolcs. S'exclouen el manteniment i la reparació d'aquests vehicles.
	f) Fabricació d'altres materials de transport	Entitats dedicades a la fabricació d'equips de transport, com la construcció de vaixells i la fabricació de material rodant ferroviari i locomotores, naus aèries i espacials, així com la fabricació de les seves peces.
6. Proveïdors de serveis digitals		- Proveïdors de mercats en línia - Proveïdors de motors de cerca en línia - Proveïdors de plataformes de serveis de xarxes socials

Dipòsit legal: AND.2-2015