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

Índex

[Mostra/Amaga]

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

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 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.

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.

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.

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.

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 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:

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;
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).