DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

CONSELL GENERAL
PRINCIPAT D'ANDORRA

Comissió Legislativa
Economia

Informe de la Ponència relatiu al Projecte de modificació de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació

El M. I. Sr. Pere Marsenyach Bataille, del Grup Parlamentari Demòcrata, nomenat ponent per la Comissió Legislativa d'Economia el dia 16 d'octubre del 2026, en relació al **Projecte de modificació de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació**, exposa el següent:

- El dia 8 de juliol del 2026, d'acord amb el que preveu l'article 97.2 del Reglament del Consell General, es va trametre el Projecte de modificació de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació a la Comissió Legislativa d'Economia, Projecte de llei que havia estat admès a tràmit parlamentari per la Sindicatura l'1 de juliol del 2026.

- Al Projecte de llei esmentat s'hi han presentat 23 esmenes a l'articulat: 15 esmenes per part del Grup Parlamentari Socialdemòcrata (GPS) i 8 esmenes per part del Grup Parlamentari de Concòrdia (GPC).

- El dia 30 de setembre del 2026, la Sindicatura, i als efectes determinats per l'article 18.1.d) del Reglament del Consell General, va constatar que les esmenes formulades pels grups parlamentaris no eren contràries a les disposicions de l'article 117 del Reglament del Consell General, i les va admetre a tràmit i trametre a la Comissió Legislativa d'Economia.

Per aquests fets, el ponent de la Comissió Legislativa d'Economia, en relació al **Projecte de modificació de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació**, proposa, segons el que disposa l'article 102 del Reglament del Consell General, l'informe següent:

PÀGINA: 1 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

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

Exposició de motius

Davant un escenari d'exposició a riscos cibernètics creixents, i tenint en compte els compromisos adquirits en matèria de cooperació internacional i alineament normatiu, especialment amb l'entorn europeu, resulta necessari reforçar el marc jurídic establert per la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (en endavant, "la Llei 22/2022").

D'aquesta manera, els principals objectius d'aquesta modificació de la Llei 22/2022 són ampliar l'abast del marc normatiu per incloure-hi una nova entitat essencial –la ràdio i televisió públiques– subjecta a les obligacions de la Llei, i reforçar les obligacions de gestió de riscos i d'incidents, i de detecció, notificació i resposta en relació amb aquests riscos i incidents.

Amb la modificació legislativa també es pretén consolidar la cooperació internacional i institucional, així com l'intercanvi d'informació, especialment amb organismes de la Unió Europea.

Finalment, s'ha considerat oportú que aquesta modificació legislativa inclogui la possibilitat de reduir per conformitat les sancions consistents en multes administratives per infraccions lleus i greus quan concorrin determinades circumstàncies, combinant un criteri objectiu de reconeixement i pagament voluntari de les sancions amb un criteri tècnic de cooperació i correcció efectiva.

Així, amb aquesta modificació de la Llei 22/2022, es fa un pas addicional per reforçar la resiliència nacional en matèria de ciberseguretat.

Esmena 1	**De modificació**
GPS (1) Es proposa modificar l'exposició de motius de la manera següent: "Exposició de motius Davant un escenari d'exposició a riscos cibernètics creixents, i tenint en compte els compromisos adquirits en matèria de cooperació internacional i alineament normatiu, especialment amb l'entorn europeu, resulta necessari reforçar el marc jurídic establert per la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (en endavant, «la Llei 22/2022»). Aquesta modificació amplia l'àmbit del marc normatiu per incloure-hi com a entitat essencial la ràdio i televisió públiques i reforça les obligacions de gestió dels riscos i dels incidents, així com les capacitats de detecció, notificació, resposta i recuperació. Alhora, introdueix l'obligació de disposar d'un centre d'operacions de seguretat per a les entitats crítiques i les entitats equivalents, que pot ser propi o prestat per un proveïdor especialitzat i que ha de complir els requisits mínims establerts reglamentàriament.	

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

La regulació adopta un enfocament basat en el risc, la proporcionalitat i la neutralitat tecnològica. En particular, les obligacions relatives a l'allotjament i al tractament de les dades s'articulen d'acord amb el nivell efectiu de protecció de la informació, amb independència de la seva ubicació, i se sotmeten a les garanties previstes per la legislació andorrana. Així mateix, es delimiten els sistemes de monitoratge extern i l'intercanvi d'informació de ciberseguretat al que sigui estrictament necessari per prevenir, detectar i gestionar incidents, tot preservant la confidencialitat empresarial, el secret de les comunicacions i la protecció de les dades personals.

Pel que fa a les entitats no incloses en l'àmbit ordinari d'aplicació de la Llei, l'obligació de notificació es vincula a criteris objectius establerts reglamentàriament i a l'existència d'un impacte potencial rellevant sobre la seguretat de les xarxes i dels sistemes d'informació al territori nacional. També es reforcen les garanties aplicables a les mesures extraordinàries davant ciberamenaces greus o sistèmiques, que han de ser necessàries, idònies, proporcionades, temporals i degudament motivades, amb una atenció especial a les persones i entitats no sotmeses ordinàriament a la Llei.

La modificació consolida igualment la cooperació internacional i institucional, així com la participació del Principat d'Andorra en xarxes europees i internacionals de ciberseguretat. Aquesta cooperació s'ha de desenvolupar sobre la base de la reciprocitat, la confiança mútua, la confidencialitat, el respecte a la sobirania institucional i el compliment de la normativa aplicable en matèria de protecció de dades i seguretat de la informació.

Per reforçar la seguretat jurídica, es preveu que les obligacions materials i els requisits tècnics essencials tinguin cobertura legal o reglamentària, mentre que les instruccions tècniques i les guies orientatives n'han de facilitar l'aplicació de manera pública, accessible i, quan sigui possible, amb la participació dels sectors afectats. També s'incorporen criteris basats en el risc per a la identificació i la revisió periòdica de les administracions públiques incloses en l'àmbit de la Llei, i es facilita una implantació progressiva de les noves obligacions mitjançant mecanismes d'acompanyament tècnic.

Finalment, es reforcen els principis de legalitat, culpabilitat i proporcionalitat del règim sancionador i es manté la possibilitat de reduir per conformitat les multes corresponents a infraccions lleus i greus quan concorrin les circumstàncies legalment establertes. En conjunt, aquesta modificació fa un pas addicional per reforçar la resiliència nacional en matèria de ciberseguretat, tot conciliant l'eficàcia de la resposta pública amb la seguretat jurídica, la protecció dels drets i la realitat operativa de les entitats afectades.»

MOTIVACIÓ

L'esmena adapta l'exposició de motius al conjunt de modificacions proposades en les esmenes posteriors del GPS. En concret, explicita l'enfocament basat en el risc, la proporcionalitat i la neutralitat tecnològica; les garanties aplicables al tractament de dades, al monitoratge i a l'intercanvi d'informació; la delimitació de les obligacions de les entitats excloses de l'àmbit ordinari de la Llei; el reforç de les garanties davant les mesures extraordinàries; la cobertura reglamentària dels requisits tècnics; els principis que han de regir la cooperació internacional; i les garanties pròpies del dret administratiu sancionador. D'aquesta manera, l'exposició de motius reflecteix fidelment el contingut i els principis del text resultant de les esmenes del GPS.

PÀGINA: 3 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

Article 1. *Modificació de l'article 9 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

Es modifica l'article 9 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"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 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.

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) Dur a terme, 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 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.

k) Col·laborar amb les autoritats policials competents en matèria de seguretat pública i ciberseguretat per facilitar, amb caràcter tècnic i preventiu, informació rellevant per a la detecció, la notificació i la resposta a incidents de ciberseguretat que puguin afectar dispositius, sistemes o serveis al territori nacional.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

2. Pel que fa a la lletra *k* de l'apartat 1, la col·laboració s'articula mitjançant un protocol d'actuació específic entre el CSIRT-AD i el Cos de Policia que estableix les condicions generals de licitud del tractament, les dades objecte d'intercanvi, les operacions específiques autoritzades (anàlisi, notificació, comunicació), les entitats destinatàries, els terminis de conservació i les mesures de seguretat que cal aplicar.

El tractament de dades personals en aquest context només pot fer-se de conformitat amb el que està establert per la legislació vigent en matèria de protecció de dades personals, i ha de respondre a una finalitat concreta, legítima i determinada en relació amb la gestió d'incidents de ciberseguretat amb possibles implicacions delictives o de seguretat pública, amb l'objectiu de permetre'n la identificació, l'anàlisi, la notificació i, si escau, la transferència a les autoritats competents.

Les dades objecte de tractament poden incloure, entre altres aspectes, l'adreça IP compromesa o atacant, la identitat i les dades de contacte del titular del servei o de l'administrador tècnic (si escau), i altres dades tècniques estrictament necessàries per determinar l'origen i l'abast de l'incident. En tot cas, s'ha de garantir el principi de minimització i s'ha de limitar l'accés a aquestes dades al personal estrictament autoritzat.

Un cop assolit l'objectiu del tractament, les dades són suprimides o, si escau, anonimitzades, d'acord amb els criteris que es defineixen en el protocol d'actuació específic entre el CSIRT-AD i el Cos de Policia. S'estableixen també mecanismes de registre d'accés, auditories internes i mesures adequades per garantir la confidencialitat, la integritat i la disponibilitat de la informació."

Esmena 2	**De modificació**

GPC(1)

Es proposa modificar l'article 1 del Projecte de llei, que modifica l'article 9 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació. La proposta modifica el primer paràgraf de l'apartat 2 de l'article 9, que queda redactat de la següent manera:

"Article 9. *Funcions del CSIRT-AD*

[...]

2. Pel que fa a la lletra k de l'apartat 1, la col·laboració s'articula mitjançant un protocol d'actuació específic entre el CSIRT-AD i el Cos de Policia. **Amb caràcter previ a la seva aprovació, el protocol ha de ser sotmès a informe de l'Agència Andorrana de Protecció de Dades pel que fa als aspectes relatius al tractament de dades personals.** El protocol estableix les condicions generals de licitud del tractament, les dades objecte d'intercanvi, les operacions específiques autoritzades (anàlisi, notificació, comunicació), les entitats destinatàries, els terminis de conservació i les mesures de seguretat que cal aplicar.

[...]"

MOTIVACIÓ

Es considera necessari incorporar la intervenció prèvia de l'Agència Andorrana de Protecció de Dades. L'informe de l'APDA ha de permetre reforçar les garanties de

PÀGINA: 5 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

protecció de dades abans de l'aprovació del protocol i verificar que el tractament previst respecta els principis i les obligacions establerts per la normativa aplicable.

Article 2. *Addició de l'article 12 bis a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

S'addiciona l'article 12 *bis* a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 12 *bis. Obligació de disposar d'un centre d'operacions de seguretat*

1. Les entitats crítiques i les entitats equivalents a entitats crítiques han de disposar, de manera obligatòria, d'un centre d'operacions de seguretat (SOC, per les sigles en anglès, tal com es coneix internacionalment) amb un nivell de capacitat operativa mínim determinat per l'ANC-AD i/o l'AFA, que garanteixi la capacitat d'anàlisi d'incidents, resposta i contenció de manera efectiva. Ha d'estar dotat de recursos humans i tècnics suficients per garantir la vigilància, la detecció i la resposta davant incidents de seguretat de la informació en temps real en les seves infraestructures crítiques, xarxes i sistemes d'informació utilitzats en la prestació dels serveis essencials o importants, mitjançant serveis gestionats.

Els SOC han de disposar d'un certificat conforme a estàndards reconeguts internacionalment en matèria de gestió de la seguretat de la informació i/o de serveis gestionats de seguretat. Alternativament, poden acreditar la seva integració activa en organismes internacionals reconeguts de coordinació de CERT/SOC. En ambdós casos, és requisit estar prèviament acreditat per l'ANC-AD i/o, si escau, per l'AFA, d'acord amb els requisits establerts a la guia corresponent publicada per l'ANC-AD, i degudament registrat a aquest efecte.

2. Totes les dades generades pel SOC, per part de les infraestructures crítiques, han de romandre preferentment dins del territori nacional. Excepcionalment, i amb notificació expressa a l'ANC-AD i/o l'AFA, es poden allotjar fora del territori nacional sempre que es garanteixi un nivell de protecció equivalent al de l'Esquema nacional de seguretat.

3. Les entitats esmentades en aquest article han de permetre la instal·lació de sistemes de monitoratge extern que l'ANC-AD, si escau, els faciliti, amb l'objectiu de reforçar la supervisió per part de l'ANC-AD i/o l'AFA, obtenir una visió agregada de la xarxa nacional i anticipar riscos sistèmics. Les dades recollides per aquests sistemes de monitoratge extern, definits i desplegats segons els criteris establerts per l'ANC-AD en el marc del Comitè d'Experts, tenen caràcter confidencial i s'utilitzen exclusivament amb finalitats de ciberseguretat i intel·ligència nacional. Els terminis d'implantació s'han d'ajustar al grau de maduresa i desplegament de cada entitat, segons les recomanacions de l'ANC-AD.

4. Les entitats afectades per aquest article han de compartir de manera proactiva i sistemàtica la intel·ligència d'incidents de ciberseguretat amb l'ANC-AD i/o l'AFA, mitjançant els canals i les plataformes establerts a aquest efecte. L'ANC-AD determina els formats, la freqüència i els detalls tècnics d'aquest intercanvi a través d'instruccions

PÀGINA: 6 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

tècniques elaborades en col·laboració amb grups de treball interdisciplinaris amb la participació de les entitats crítiques i altres actors rellevants.

5. El compliment de les obligacions establertes en aquest article és objecte de supervisió per part de l'ANC-AD i/o l'AFA, d'acord amb les facultats que els atorga la normativa vigent en matèria de ciberseguretat. L'incompliment d'aquestes obligacions pot donar lloc a l'adopció de mesures correctores i, si escau, a la imposició de sancions en els termes establerts per aquesta Llei i la resta de normativa aplicable."

Esmena 3	**De modificació**

GPS (2)

Es proposa modificar l'article 2 de la forma següent:

"(...)

Article 12 bis. *Obligació de disposar d'un centre d'operacions de seguretat*

1. Les entitats crítiques i les entitats equivalents a entitats crítiques han de disposar, de manera obligatòria, d'un centre d'operacions de seguretat (SOC, per les sigles en anglès, tal com es coneix internacionalment), **que pot ser propi o prestat mitjançant un proveïdor especialitzat,** amb un nivell de capacitat operativa mínim **establert reglamentàriament** ~~determinat per l'ANC-AD i/o l'AFA~~**,** que garanteixi la capacitat d'anàlisi d'incidents, resposta i contenció de manera efectiva.

Ha d'estar dotat de recursos humans i tècnics suficients per garantir la vigilància, la detecció i la resposta davant incidents de seguretat de la informació en temps real en les seves infraestructures crítiques, xarxes i sistemes d'informació utilitzats en la prestació dels serveis essencials o importants~~, mitjançant serveis gestionats~~.

Els SOC han de disposar d'un certificat conforme a estàndards reconeguts internacionalment en matèria de gestió de la seguretat de la informació i/o de serveis gestionats de seguretat. Alternativament, poden acreditar la seva integració activa en organismes internacionals reconeguts de coordinació de CERT/SOC. En ambdós casos, és requisit estar prèviament acreditat per l'ANC-AD i/o, si escau, per l'AFA, ~~d'acord amb els requisits establerts a la guia corresponent publicada per l'ANC-AD~~ **d'acord amb els requisits establerts reglamentàriament**, i degudament registrat a aquest efecte.

~~2. Totes les dades generades pel SOC, per part de les infraestructures crítiques, han de romandre preferentment dins del territori nacional. Excepcionalment, i amb notificació expressa a l'ANC-AD i/o l'AFA, es poden allotjar fora del territori nacional sempre que es garanteixi un nivell de protecció equivalent al de l'Esquema nacional de seguretat.~~ **2. Les dades generades pel SOC s'han de tractar i allotjar de manera que es garanteixi un nivell de protecció equivalent al previst per la legislació andorrana en matèria de seguretat de la informació i protecció de dades, amb independència del lloc on estiguin allotjades.**
Quan les dades s'allotgin fora del territori nacional, l'entitat ho ha de comunicar prèviament a l'ANC-AD i/o a l'AFA i ha d'acreditar que l'allotjament compleix els requisits de seguretat, confidencialitat, disponibilitat, integritat, recuperació i control d'accés establerts reglamentàriament.

3. Les entitats esmentades en aquest article han de permetre la instal·lació de sistemes de monitoratge extern que l'ANC-AD, si escau, els faciliti, amb l'objectiu de reforçar la

PÀGINA: 7 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

supervisió per part de l'ANC-AD i/o l'AFA, obtenir una visió agregada de la xarxa nacional i anticipar riscos sistèmics.

Els sistemes de monitoratge extern s'han de limitar exclusivament a la recopilació de la informació tècnica estrictament necessària per detectar, prevenir o gestionar riscos de ciberseguretat i no poden comportar l'accés al contingut de les comunicacions, ni al tractament de dades personals o informació protegida pel secret empresarial que no siguin estrictament necessàries per a aquestes finalitats.

Les dades recollides per aquests sistemes de monitoratge extern, definits i desplegats segons els criteris establerts per l'ANC-AD en el marc del Comitè d'Experts, tenen caràcter confidencial i s'utilitzen exclusivament amb finalitats de ciberseguretat i intel·ligència nacional.

Els terminis d'implantació s'han d'ajustar al grau de maduresa i desplegament de cada entitat, segons les recomanacions de l'ANC-AD.

4. Les entitats afectades per aquest article han de compartir de manera proactiva i sistemàtica la intel·ligència d'incidents de ciberseguretat amb l'ANC-AD i/o l'AFA, mitjançant els canals i les plataformes establerts a aquest efecte.

Aquest intercanvi s'ha de limitar als indicadors de compromís, vulnerabilitats, tàctiques, tècniques i procediments dels atacants, així com a la informació estrictament necessària per prevenir o gestionar incidents, preservant en tot cas la confidencialitat empresarial i el compliment de la normativa en matèria de protecció de dades.

L'ANC-AD determina els formats, la freqüència i els detalls tècnics d'aquest intercanvi a través ~~d'instruccions tècniques~~ **de disposicions reglamentàries o instruccions tècniques dictades en desenvolupament d'aquestes**, elaborades en col·laboració amb grups de treball interdisciplinaris amb la participació de les entitats crítiques i altres actors rellevants.

5. El compliment de les obligacions establertes en aquest article és objecte de supervisió per part de l'ANC-AD i/o l'AFA, d'acord amb les facultats que els atorga la normativa vigent en matèria de ciberseguretat.

L'incompliment d'aquestes obligacions pot donar lloc a l'adopció de mesures correctores i, si escau, a la imposició de sancions en els termes establerts per aquesta Llei i la resta de normativa aplicable.

MOTIVACIÓ

L'esmena té per objecte reforçar la seguretat jurídica, la proporcionalitat i la neutralitat tecnològica del nou article 12 bis, sense alterar la finalitat perseguida pel Projecte de llei de reforçar la ciberseguretat de les entitats crítiques.

En primer lloc, es clarifica que l'obligació de disposar d'un centre d'operacions de seguretat (SOC) es pot complir tant mitjançant recursos propis com a través de proveïdors especialitzats, evitant limitar l'organització dels operadors i garantint el principi de neutralitat tecnològica.

PÀGINA: 8 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

En segon lloc, es preveu que els requisits mínims exigibles als SOC s'estableixin mitjançant disposicions reglamentàries, en lloc de remetre'ls a una simple guia administrativa, reforçant així els principis de legalitat i de seguretat jurídica.

Igualment, es modifica el règim aplicable a les dades generades pel SOC per substituir el criteri estrictament territorial per un criteri basat en el nivell efectiu de protecció. Quan les dades s'allotgin fora d'Andorra, s'exigeix la comunicació prèvia a l'autoritat competent i l'acreditació del compliment dels requisits de seguretat establerts reglamentàriament.

Així mateix, s'incorporen garanties addicionals respecte als sistemes de monitoratge extern i a l'intercanvi d'intel·ligència de ciberseguretat, delimitant-ne l'abast per assegurar que el tractament de la informació es limiti a les dades estrictament necessàries per a les finalitats de prevenció i resposta davant incidents, preservant la confidencialitat empresarial i el compliment de la normativa de protecció de dades.

En conjunt, l'esmena manté íntegrament els objectius de reforç de la ciberseguretat previstos pel Projecte de llei, però dota el text d'una major precisió jurídica, proporcionalitat i alineament amb els principis que inspiren els marcs europeus de ciberseguretat, especialment la Directiva (UE) 2022/2555 (NIS2).

Esmena 4 **De modificació**

GPC (2)

Es proposa modificar l'article 2 del Projecte de llei, que addiciona l'article 12 bis a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació. La proposta modifica el segon paràgraf de l'apartat 1 i els apartats 2 i 3 de l'article 12 bis, que queden redactats de la manera següent:

"Article 12 bis. *Obligació de disposar d'un centre d'operacions de seguretat*

[...]

Els SOC han de disposar d'un certificat conforme a estàndards reconeguts internacionalment en matèria de gestió de la seguretat de la informació i/o de serveis gestionats de seguretat. Alternativament, poden acreditar la seva integració activa en organismes internacionals reconeguts de coordinació de CERT/SOC. En ambdós casos, és requisit estar prèviament acreditat per l'ANC-AD i/o, si escau, per l'AFA, d'acord amb els requisits establerts ~~a la guia corresponent publicada per l'ANC-AD~~ **reglamentàriament**, i degudament registrat a aquest efecte.

2. ~~Totes les dades generades pel SOC, per part de les infraestructures crítiques, han de romandre preferentment dins del territori nacional. Excepcionalment, i amb notificació expressa a l'ANC-AD i/o l'AFA, es poden allotjar fora del territori nacional sempre que es garanteixi un nivell de protecció equivalent al de l'Esquema nacional de seguretat.~~**Les dades generades pel SOC, així com les claus criptogràfiques vinculades a la gestió de la seguretat de la informació o a la protecció d'infraestructures crítiques, han d'estar allotjades dins del territori del Principat d'Andorra, llevat d'autorització expressa de l'ANC-AD i/o l'AFA.**

3. Les entitats esmentades en aquest article ~~han de permetre la instal·lació de sistemes de monitoratge extern que l'ANC-AD, si escau, els faciliti~~ **han de disposar, almenys, d'una sonda externa de monitoratge gestionada per l'ANC-AD o per l'AFA, segons correspongui**, amb l'objectiu de reforçar la supervisió per part de l'ANC-AD i/o l'AFA, obtenir una visió agregada de la xarxa nacional i anticipar riscos sistèmics. Les dades

PÀGINA: 9 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

recollides per aquests sistemes de monitoratge extern, definits i desplegats segons els criteris establerts per l'ANC-AD en el marc del Comitè d'Experts, tenen caràcter confidencial i s'utilitzen exclusivament amb finalitats de ciberseguretat ~~i intel·ligència nacional,~~ **inclosa la generació i l'anàlisi d'intel·ligència de ciberamenaces**. Els terminis d'implantació s'han d'ajustar al grau de maduresa i desplegament de cada entitat, segons les recomanacions de l'ANC-AD.

[...]"

MOTIVACIÓ

Es reforça la seguretat jurídica en l'acreditació dels SOC establint que els requisits exigibles es determinin reglamentàriament i no mitjançant una guia. Així mateix, s'harmonitza el règim de localització de les dades i de les claus criptogràfiques, així com l'obligació de disposar d'una sonda externa de monitoratge, amb el que estableix la disposició transitòria del Projecte de llei. Finalment, se substitueix l'expressió "intel·ligència nacional" per "intel·ligència de ciberamenaces" per delimitar amb més precisió la finalitat per a la qual poden ser utilitzades les dades recollides pels sistemes de monitoratge.

Article 3. *Modificació de l'article 16 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

Es modifica l'article 16 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 16. *Notificació obligatòria per part de les entitats excloses de l'àmbit d'aplicació d'aquesta Llei*

1. Sense perjudici del que es disposa a l'article 2 respecte a l'àmbit d'aplicació d'aquesta Llei, les entitats no referides al dit article han de presentar notificacions de ciberamenaces, quasiincidents i incidents significatius o que puguin tenir impacte sobre la seguretat de les xarxes i dels sistemes d'informació al territori nacional. Les dites entitats han d'efectuar aquestes notificacions amb la finalitat de contribuir a la detecció precoç de ciberamenaces, facilitar l'intercanvi d'informació sobre riscos emergents i reforçar la resiliència global de l'ecosistema digital nacional.

Quan tramitin les notificacions al CSIRT-AD, aquestes entitats han d'actuar de conformitat amb el procediment establert a l'article 15.

La no realització de les referides notificacions d'acord amb el que està establert als paràgrafs anteriors pot comportar que les entitats de què es tracti siguin objecte de sancions d'acord amb el règim sancionador previst en aquesta Llei.

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. Les notificacions referides als apartats anteriors obliguen l'entitat que les hagi efectuat a resoldre l'incident d'acord amb el que s'estableix en aquesta Llei.

PÀGINA: 10 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

4. Les notificacions obligatòries efectuades per les entitats a què fa referència l'article 2 tenen caràcter prioritari sobre la resta de notificacions previstes en aquesta Llei a l'efecte de gestionar-les per part del CSIRT-AD."

Esmena 5	**De modificació**

GPS (3)

Es proposa modificar l'article 3 de la forma següent:

"(...)

Article 16. *Notificació obligatòria per part de les entitats excloses de l'àmbit d'aplicació d'aquesta Llei*

1. Sense perjudici del que es disposa a l'article 2 respecte a l'àmbit d'aplicació d'aquesta Llei, les entitats no referides al dit article ~~han de presentar notificacions de ciberamenaces, quasiincidents i incidents significatius o que puguin tenir impacte sobre la seguretat de les xarxes i dels sistemes d'informació al territori nacional.~~ **que compleixin els criteris objectius que s'estableixin reglamentàriament, atenent la naturalesa de la seva activitat, la dimensió de les seves infraestructures o el potencial impacte sobre la seguretat de les xarxes i dels sistemes d'informació al territori nacional, han de presentar notificacions de ciberamenaces, quasiincidents i incidents que puguin tenir un impacte rellevant sobre la seguretat de les xarxes i dels sistemes d'informació al territori nacional.**

Les dites entitats han d'efectuar aquestes notificacions amb la finalitat de contribuir a la detecció precoç de ciberamenaces, facilitar l'intercanvi d'informació sobre riscos emergents i reforçar la resiliència global de l'ecosistema digital nacional.

Quan tramitin les notificacions al CSIRT-AD, aquestes entitats han d'actuar de conformitat amb el procediment establert a l'article 15.

La no realització de les referides notificacions d'acord amb el que està establert als paràgrafs anteriors pot comportar que les entitats de què es tracti siguin objecte de sancions d'acord amb el règim sancionador previst en aquesta Llei.

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. ~~Les notificacions referides als apartats anteriors obliguen l'entitat que les hagi efectuat a resoldre l'incident d'acord amb el que s'estableix en aquesta Llei.~~

La presentació d'una notificació d'acord amb aquest article no eximeix l'entitat de continuar adoptant les mesures tècniques i organitzatives necessàries per prevenir, gestionar, contenir i resoldre l'incident de conformitat amb la normativa que li sigui aplicable.

4. Les notificacions obligatòries efectuades per les entitats a què fa referència l'article 2 tenen caràcter prioritari sobre la resta de notificacions previstes en aquesta Llei a l'efecte de gestionar-les per part del CSIRT-AD.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

MOTIVACIÓ

L'esmena té per objecte reforçar la seguretat jurídica i el principi de proporcionalitat en relació amb el règim de notificació obligatòria aplicable a les entitats no incloses en l'àmbit ordinari d'aplicació de la Llei.

En primer lloc, es delimita l'obligació de notificació a les entitats que compleixin criteris objectius establerts reglamentàriament, atenent la naturalesa de la seva activitat, la dimensió de les seves infraestructures o el potencial impacte sobre la seguretat de les xarxes i dels sistemes d'informació. Aquesta modificació evita que una obligació susceptible de comportar un règim sancionador pugui resultar d'aplicació indiscriminada a qualsevol entitat exclosa de l'àmbit de la Llei.

En segon lloc, es precisa que les notificacions han de referir-se a incidents que puguin tenir un impacte rellevant sobre la seguretat de les xarxes i dels sistemes d'informació, substituint una expressió excessivament oberta que pot donar lloc a interpretacions divergents i generar inseguretat jurídica.

Finalment, es modifica l'apartat tercer per aclarir que la notificació constitueix un deure d'informació envers l'autoritat competent, però no és l'acte que origina l'obligació de gestionar o resoldre l'incident. Aquesta obligació deriva dels deures generals de diligència i de la normativa aplicable a cada entitat, de manera que es reforça la coherència jurídica del precepte.

En conjunt, l'esmena manté la finalitat de reforçar la detecció precoç de ciberamenaces i la resiliència de l'ecosistema digital nacional, però ho fa amb una regulació més precisa, proporcionada i respectuosa amb els principis de bona regulació i de seguretat jurídica.

Esmena 6 **De modificació**

GPC (3)

Es proposa modificar l'article 3 del Projecte de llei, que modifica l'article 16 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació. La proposta modifica els apartats 1 i 3 de l'article 16, que queden redactats de la manera següent:

"Article 16. *Notificació obligatòria per part de les entitats excloses de l'àmbit d'aplicació d'aquesta Llei*

1. Sense perjudici del que es disposa a l'article 2 **respecte a l'àmbit d'aplicació d'aquesta Llei, les entitats no referides al dit article han de notificar al CSIRT-AD els incidents significatius i les ciberamenaces significatives que puguin donar lloc a un incident significatiu, d'acord amb els criteris establerts a l'article 15.3, en la mesura que els siguin aplicables.**

Aquestes entitats poden notificar voluntàriament altres ciberamenaces o quasiincidents que considerin rellevants per a la seguretat de les xarxes i dels sistemes d'informació al territori nacional.

Les notificacions s'han d'efectuar de conformitat amb el procediment establert a l'article 15.

[...]

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

3. Les entitats referides a l'apartat 1 han d'adoptar les mesures necessàries per gestionar i resoldre l'incident notificat. La notificació no comporta l'aplicació de les altres obligacions previstes en aquesta Llei per a les entitats essencials o importants, llevat que una disposició estableixi expressament el contrari."

MOTIVACIÓ

Es manté l'obligació de notificació per a les entitats excloses de l'àmbit d'aplicació de la Llei, però es limita als incidents i ciberamenaces de caràcter significatiu. Això evita imposar una obligació potencialment sancionable davant qualsevol ciberamenaça o quasi incident, reforçant la proporcionalitat i la seguretat jurídica. També s'aclareix que aquesta obligació de notificació no comporta l'aplicació automàtica de la resta d'obligacions previstes per a les entitats essencials o importants.

Article 4. ***Addició de l'article 16 bis a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació***

S'addiciona l'article 16 bis a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 16 bis. *Mesures extraordinàries de reforç de la ciberseguretat*

1. Quan l'ANC-AD constati l'existència d'una amenaça cibernètica greu, persistent, generalitzada o susceptible de produir efectes sistèmics sobre la seguretat nacional, l'ordre públic, l'estabilitat econòmica o la confiança en els serveis digitals del Principat d'Andorra, pot proposar l'adopció de mesures extraordinàries de reforç de la ciberseguretat.

2. Les mesures previstes en aquest article poden ser exigides a les entitats subjectes a aquesta Llei de conformitat amb l'article 2 mitjançant una resolució motivada de l'ANC-AD.

3. Excepcionalment, quan la naturalesa, l'abast o els efectes previsibles de la ciberamenaça ho justifiquin, les mesures també poden ser exigides a persones físiques o jurídiques, públiques o privades, no incloses en l'àmbit subjectiu establert a l'article 2 d'aquesta Llei, quan l'ANC-AD motivi que la seva activitat, els serveis que presten, les infraestructures que operen o la seva exposició a la ciberamenaça les converteixen en potencials vectors de propagació, amplificació o materialització del risc detectat.

4. En els supòsits previstos a l'apartat anterior, l'aplicació de les mesures requereix l'aprovació prèvia del Govern mitjançant una resolució motivada, a proposta de l'ANC-AD. La resolució ha de determinar:

a) La naturalesa de la ciberamenaça;

b) Les categories o sectors afectats;

c) Les mesures exigibles;

PÀGINA: 13 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

d) L'abast subjectiu de la seva aplicació;

e) El termini d'implementació;

f) La durada de la seva vigència.

5. Les mesures extraordinàries han de respectar en tot cas els principis de legalitat, necessitat, idoneïtat, proporcionalitat, mínima intervenció i no-discriminació, i han de limitar-se al que sigui estrictament necessari per prevenir o mitigar els riscos identificats.

6. Les mesures extraordinàries poden consistir, entre d'altres, en:

a) La implantació de controls tècnics o organitzatius específics de ciberseguretat;

b) L'adopció de procediments reforçats de gestió de riscos, detecció, resposta i recuperació davant incidents;

c) La realització d'avaluacions de seguretat, auditories o verificacions independents;

d) L'aplicació total o parcial de controls, mesures o requisits previstos en marcs, esquemes o estàndards de ciberseguretat reconeguts per reglament o expressament identificats en la resolució corresponent.

7. Les resolucions adoptades en aplicació d'aquest article han d'especificar de manera precisa les obligacions imposades i els terminis de compliment, i han de ser notificades a les entitats afectades.

8. Amb caràcter general, les entitats afectades disposen d'un tràmit d'audiència previ de cinc dies hàbils. Aquest tràmit pot ometre's quan concorrin circumstàncies d'urgència degudament motivades que puguin comprometre la seguretat de les xarxes i dels sistemes d'informació o l'eficàcia de les mesures adoptades. En aquest cas, l'audiència s'ha de concedir immediatament després de l'adopció de la mesura.

9. Les mesures adoptades en virtut d'aquest article tenen caràcter temporal i han de ser revisades periòdicament per l'ANC-AD. La seva vigència no pot excedir dotze mesos, llevat que una nova resolució motivada del Govern n'acordi la pròrroga per persistència acreditada de les circumstàncies que les van justificar.

10. Respecte de les entitats sotmeses a la supervisió de l'AFA, aquesta autoritat pot exercir les facultats previstes en aquest article dins del seu àmbit competencial, amb la coordinació preceptiva amb l'ANC-AD. Quan les mesures afectin entitats financeres no incloses en l'àmbit subjectiu ordinari d'aquesta Llei, és igualment exigible l'aprovació prèvia del Govern prevista a l'apartat 4.

11. Contra les resolucions adoptades en aplicació d'aquest article es poden interposar els recursos administratius i jurisdiccionals previstos per l'ordenament jurídic."

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

Esmena 7	**De modificació**

GPS (4)

Es proposa modificar l'article 4 de la forma següent:

" (...)

Article 16 bis. *Mesures extraordinàries de reforç de la ciberseguretat*

(...)

3. Excepcionalment, quan la naturalesa, l'abast o els efectes previsibles de la ciberamenaça ho justifiquin, les mesures també poden ser exigides a persones físiques o jurídiques, públiques o privades, no incloses en l'àmbit subjectiu establert a l'article 2 d'aquesta Llei, quan l'ANC-AD motivi que la seva activitat, els serveis que presten, les infraestructures que operen o la seva exposició a la ciberamenaça les converteixen en potencials vectors de propagació, amplificació o materialització del risc detectat~~.~~ **, de manera directa i objectivament acreditada mitjançant un informe tècnic motivat que justifiqui la necessitat de l'adopció de les mesures extraordinàries i la inexistència d'alternatives menys restrictives.**

4. En els supòsits previstos a l'apartat anterior, l'aplicació de les mesures requereix l'aprovació prèvia del Govern mitjançant una resolució motivada, a proposta de l'ANC-AD. La resolució ha de determinar:

a) La naturalesa de la ciberamenaça;

b) Les categories o sectors afectats;

c) Les mesures exigibles;

d) L'abast subjectiu de la seva aplicació;

e) El termini d'implementació;

f) La durada de la seva vigencia.

g) La justificació expressa de la necessitat, la idoneïtat i la proporcionalitat de cadascuna de les mesures adoptades, així com els motius pels quals no resulten suficients altres mesures menys restrictives.

(...)

5. Les mesures extraordinàries han de respectar en tot cas els principis de legalitat, necessitat, idoneïtat, proporcionalitat, mínima intervenció i nodiscriminació, i han de limitar-se al que sigui estrictament necessari per prevenir o mitigar els riscos identificats~~.~~ **, adoptant, sempre que sigui possible, les mesures menys restrictives per assolir la finalitat perseguida i evitant imposar obligacions que excedeixin les estrictament necessàries per gestionar el risc detectat.**

6. Les mesures extraordinàries poden consistir, entre d'altres, en:

a) La implantació de controls tècnics o organitzatius específics de ciberseguretat;

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

b) L'adopció de procediments reforçats de gestió de riscos, detecció, resposta i recuperació davant incidents;

c) La realització d'avaluacions de seguretat, auditories o verificacions independents;

d) L'aplicació total o parcial de controls, mesures o requisits previstos en marcs, esquemes o estàndards de ciberseguretat reconeguts per reglament o expressament identificats en la resolució corresponent~~.~~**, sempre que aquests siguin adequats a la naturalesa, intensitat i abast del risc detectat.**

7. Les resolucions adoptades en aplicació d'aquest article han d'especificar de manera precisa les obligacions imposades i els terminis de compliment, i han de ser notificades a les entitats afectades~~.~~**, incorporant una motivació individualitzada quan les mesures s'adrecin a persones físiques o jurídiques no incloses en l'àmbit subjectiu establert a l'article 2 d'aquesta Llei.**

8. Amb caràcter general, les entitats afectades disposen d'un tràmit d'audiència previ de cinc dies hàbils. Aquest tràmit pot ometre's quan concorrin circumstàncies d'urgència degudament motivades que puguin comprometre la seguretat de les xarxes i dels sistemes d'informació o l'eficàcia de les mesures adoptades. En aquest cas, l'audiència s'ha de concedir immediatament després de l'adopció de la mesura~~.~~**, i les al·legacions formulades per l'entitat afectada han de ser resoltes expressament mitjançant resolució motivada.**

9. Les mesures adoptades en virtut d'aquest article tenen caràcter temporal i han de ser revisades periòdicament per l'ANC-AD. La seva vigència no pot excedir dotze mesos, llevat que una nova resolució motivada del Govern n'acordi la pròrroga per persistència acreditada de les circumstàncies que les van justificar~~.~~ **, incorporant una nova valoració de la necessitat, la idoneïtat i la proporcionalitat del manteniment de les mesures extraordinàries.**

(...) "

MOTIVACIÓ

L'esmena té per objecte reforçar les garanties jurídiques aplicables a l'exercici de les potestats extraordinàries previstes en aquest article, sense limitar la capacitat d'actuació de les autoritats competents davant situacions de risc greu o sistèmic.

En aquest sentit, es reforça el principi de proporcionalitat exigint que les mesures adoptades siguin les menys restrictives possibles per assolir la finalitat perseguida i que existeixi una relació adequada entre la intensitat del risc detectat i les obligacions imposades.

Així mateix, s'exigeix una motivació individualitzada quan les mesures afectin persones o entitats no incloses en l'àmbit ordinari d'aplicació de la Llei, reforçant la seguretat jurídica i el control de la discrecionalitat administrativa.

Igualment, es dota de contingut efectiu el tràmit d'audiència posterior en els supòsits d'urgència, exigint que les al·legacions presentades siguin resoltes expressament mitjançant resolució motivada, i es reforça la justificació de les eventuals pròrrogues de les mesures extraordinàries, que hauran d'anar acompanyades d'una nova valoració sobre la seva necessitat, idoneïtat i proporcionalitat.

PÀGINA: 16 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

En conjunt, l'esmena manté íntegrament els objectius de protecció de la ciberseguretat previstos en el Projecte de llei, però reforça les garanties pròpies d'un estat de dret i assegura una aplicació més proporcionada, motivada i respectuosa amb els principis de bona regulació.

Article 5. *Modificació de l'article 25 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

Es modifica l'article 25 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"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 han 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 han 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, ha de complir el següent:

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 ha de revisar periòdicament, almenys cada dos anys, i ha d'actualitzar quan 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 que tingui un nivell que es consideri significatiu d'acord amb el que està establert a l'article 15.3. En fer-ho, l'ANC-AD ha de preservar, 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.

PÀGINA: 17 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

e) Emetre informes anuals per al Govern d'Andorra sobre els incidents, quasiincidents i ciberamenaces notificats per les entitats essencials i importants, de 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 altres aspectes:

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.

g) Comparèixer, per mitjà de la seva persona de tutela, davant de la comissió legislativa del Consell General competent en matèria de ciberseguretat, a requeriment de la dita comissió o quan les circumstàncies específiques ho justifiquin o aconsellin, 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, l'estabilitat i la 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 els titulars dels noms de domini i els punts de contacte que administren els noms de domini en els dominis de primer nivell, i contactar-hi.

• 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, amb sol·licitud lícita i degudament justificada prèvia, 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.

PÀGINA: 18 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

5. A fi de promoure una aplicació convergent amb la dels estats veïns, les autoritats nacionals competents han de publicar 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 obligacions anteriors, les autoritats nacionals competents poden 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."

Esmena 8	**De modificació**

GPS (5)

Es proposa modificar l'article 5 de la forma següent:

" (...)

Article 25. O*bligacions de les autoritats nacionals competents*

(…)

6. Addicionalment a les obligacions anteriors, les autoritats nacionals competents poden 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~~.~~ **, sempre que aquestes instruccions i guies es dictin en desenvolupament de les disposicions reglamentàries vigents, siguin objecte de consulta prèvia amb els sectors afectats quan la seva naturalesa ho permeti i es publiquin de forma accessible per garantir la seguretat jurídica i la transparència de la seva aplicació.**

(...)"

MOTIVACIÓ

L'esmena reforça els principis de seguretat jurídica, transparència i participació en l'exercici de les potestats de les autoritats nacionals competents. Les instruccions tècniques i les guies orientatives constitueixen instruments útils per adaptar els requisits de ciberseguretat a l'evolució tecnològica, però no haurien de convertir-se en una via per establir obligacions materials desvinculades del marc legal o reglamentari.

Per aquest motiu, es preveu que aquestes instruccions i guies es dictin en desenvolupament de les disposicions reglamentàries vigents, que siguin objecte de consulta amb els sectors afectats sempre que sigui possible i que es publiquin de manera accessible. Aquesta modificació reforça la transparència, afavoreix la col·laboració entre l'Administració i els operadors i contribueix a una aplicació més homogènia i previsible de la normativa.

PÀGINA: 19 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

Esmena 9	**De modificació**

GPC (4)

Es proposa modificar l'article 5 del Projecte de llei, que modifica l'article 25 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació. La proposta modifica la lletra e) i la lletra g) de l'apartat 4 de l'article 25, en les referències a les entitats notificants, que queden redactades de la manera següent:

"Article 25. Obligacions de les autoritats nacionals competents

[...]

e) Emetre informes anuals per al Govern d'Andorra sobre els incidents, quasiincidents i ciberamenaces notificats per les entitats essencials i importants **i per les entitats referides a l'apartat 1 de l'article 16**, de 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 altres aspectes:

[...]

g) Comparèixer, per mitjà de la seva persona de tutela, davant de la comissió legislativa del Consell General competent en matèria de ciberseguretat, a requeriment de la dita comissió o quan les circumstàncies específiques ho justifiquin o aconsellin, 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 **i per les entitats referides a l'apartat 1 de l'article 16**, a l'estat de l'aplicació de l'Estratègia nacional de ciberseguretat i a la situació de la ciberseguretat al Principat d'Andorra.

[...]"

MOTIVACIÓ

Es fa necessari incorporar als informes anuals de l'ANC-AD les notificacions efectuades per les entitats excloses de l'àmbit d'aplicació de la Llei que passen a estar subjectes a obligació de notificació, per tal que els informes reflecteixin de manera completa la situació de la ciberseguretat al Principat.

Article 6. *Addició de l'article 28 bis a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

S'addiciona l'article 28 *bis* a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 28 *bis. Participació en xarxes i cooperació multinivell*

1. Amb l'objectiu d'alinear-se amb les millors pràctiques internacionals i europees en matèria de ciberseguretat, el Principat d'Andorra pot participar, en qualitat de país tercer col·laborador i/o observador, en xarxes i grups de cooperació multinivell com ara el Grup de Cooperació establert per la Directiva (UE) 2022/2555 del Parlament Europeu i del Consell, del 14 de desembre del 2022, relativa a les mesures destinades a garantir

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

un elevat nivell comú de ciberseguretat en tota la Unió, per la qual es modifiquen el Reglament (UE) 910/2014 i la Directiva (UE) 2018/1972 i per la qual es deroga la Directiva (UE) 2016/1148.

2. Les autoritats nacionals competents, incloent-hi l'ANC-AD, l'AFA i el CSIRT-AD i altres organismes designats per llei, poden:

a) Intercanviar bones pràctiques, coneixements tècnics i informació estratègica amb els membres de les xarxes i grups de cooperació multinivell a què es refereix l'apartat 1.

b) Participar en reunions periòdiques amb parts interessades internacionals.

c) Contribuir a l'anàlisi de riscos en cadenes de subministrament crítiques, activitats de sensibilització, capacitació, desenvolupament de competències i exercicis conjunts.

d) Sol·licitar assistència tècnica i estratègica o presentar informes d'experiències compartides en accions transfrontereres o exercicis de supervisió conjunta.

3. El Govern ha d'adoptar les disposicions reglamentàries necessàries per formalitzar la participació del Principat d'Andorra en els grups i xarxes de cooperació multinivell referits, d'acord amb els criteris de reciprocitat, transparència, seguretat i sobirania institucional."

Esmena 10	**De modificació**

GPS (6)

Es proposa modificar l'article 6 de la forma següent:

" (...)

Article 28 bis. *Participació en xarxes i cooperació multinivell*

1. Amb l'objectiu d'alinear-se amb les millors pràctiques internacionals i europees en matèria de ciberseguretat, el Principat d'Andorra pot participar, en qualitat de país tercer col·laborador i/o observador, en xarxes i grups de cooperació multinivell com ara el Grup de Cooperació establert per la Directiva (UE) 2022/2555 del Parlament Europeu i del Consell, del 14 de desembre del 2022, relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat en tota la Unió, per la qual es modifiquen el Reglament (UE) 910/2014 i la Directiva (UE) 2018/1972 i per la qual es deroga la Directiva (UE) 2016/1148.

2. Les autoritats nacionals competents, incloent-hi l'ANC-AD, l'AFA i el CSIRT-AD i altres organismes designats per llei, poden:

a) Intercanviar bones pràctiques, coneixements tècnics i informació estratègica amb els membres de les xarxes i grups de cooperació multinivell a què es refereix l'apartat 1. , **respectant en tot cas la normativa vigent en matèria de protecció de dades, seguretat de la informació, confidencialitat i protecció dels interessos essencials del Principat d'Andorra.**

b) Participar en reunions periòdiques amb parts interessades internacionals.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

c) Contribuir a l'anàlisi de riscos en cadenes de subministrament crítiques, activitats de sensibilització, capacitació, desenvolupament de competències i exercicis conjunts.

d) Sol·licitar assistència tècnica i estratègica o presentar informes d'experiències compartides en accions transfrontereres o exercicis de supervisió conjunta.

3. El Govern ha d'adoptar les disposicions reglamentàries necessàries per formalitzar la participació del Principat d'Andorra en els grups i xarxes de cooperació multinivell referits, d'acord amb els criteris de reciprocitat, transparència, seguretat i sobirania institucional."

MOTIVACIÓ

L'esmena reforça les garanties aplicables a l'intercanvi internacional d'informació en matèria de ciberseguretat. La cooperació internacional constitueix un element essencial per a la prevenció i la resposta davant ciberamenaces, però aquesta ha de desenvolupar-se preservant la confidencialitat de la informació compartida, la protecció de les dades personals i els interessos essencials del Principat d'Andorra. La modificació no limita la cooperació internacional prevista en el Projecte de llei, sinó que n'explicita els principis rectors i reforça la seguretat jurídica en la seva aplicació.

Article 7. *Addició de l'article 28 ter a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

S'addiciona l'article 28 *ter* a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 28 *ter. Desenvolupament de capacitats i interoperabilitat internacional*

1. Les autoritats andorranes competents en matèria de ciberseguretat han de fomentar la col·laboració amb organismes internacionals i europeus en iniciatives de desenvolupament de capacitats i interoperabilitat internacional, incloent-hi la participació en programes de formació i l'harmonització de protocols de resposta a incidents.

2. Es poden establir acords específics amb agències europees com l'Agència de la Unió Europea per la Ciberseguretat (ENISA) o xarxes com, a títol enunciatiu però no limitatiu, la xarxa europea d'organitzacions d'enllaç per a les crisis de ciberseguretat (EU-CyCLONe), entre d'altres, per:

a) Integrar el CSIRT-AD en circuits d'intercanvi d'alertes i informació crítica.

b) Avaluar conjuntament escenaris de crisi cibernètica i contribuir a la definició d'estratègies de resiliència transnacional.

c) Reforçar la interoperabilitat tècnica i la confiança operativa entre equips de resposta i supervisió."

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

Esmena 11	**De modificació**

GPS (7)

Es proposa modificar l'article 7 de la forma següent:

"(...)

Article 28 ter. *Desenvolupament de capacitats i interoperabilitat internacional*

1. Les autoritats andorranes competents en matèria de ciberseguretat han de fomentar la col·laboració amb organismes internacionals i europeus en iniciatives de desenvolupament de capacitats i interoperabilitat internacional, incloent-hi la participació en programes de formació i l'harmonització de protocols de resposta a incidents.

2. Es poden establir acords específics amb agències europees com l'Agència de la Unió Europea per la Ciberseguretat (ENISA) o xarxes com, a títol enunciatiu però no limitatiu, la xarxa europea d'organitzacions d'enllaç per a les crisis de ciberseguretat (EU-CyCLONe), entre d'altres, **sobre la base dels principis de reciprocitat, confiança mútua, respecte a la sobirania nacional i compliment de la normativa aplicable en matèria de protecció de dades i seguretat de la informació,** per:

a) Integrar el CSIRT-AD en circuits d'intercanvi d'alertes i informació crítica.

b) Avaluar conjuntament escenaris de crisi cibernètica i contribuir a la definició d'estratègies de resiliència transnacional.

c) Reforçar la interoperabilitat tècnica i la confiança operativa entre equips de resposta i supervisió."

MOTIVACIÓ

L'esmena reforça les garanties aplicables als acords de cooperació internacional en matèria de ciberseguretat. La participació del Principat d'Andorra en iniciatives impulsades per organismes europeus constitueix un element essencial per millorar les capacitats nacionals i afavorir la interoperabilitat dels sistemes de resposta davant incidents. Tanmateix, aquesta cooperació ha de desenvolupar-se sobre la base dels principis de reciprocitat, respecte a la sobirania nacional, protecció de les dades i seguretat de la informació, garantint així que l'intercanvi d'informació i la col·laboració internacional es duguin a terme amb les garanties jurídiques adequades.

Article 8. *Addició de l'article 28 quarter a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

S'addiciona l'article 28 *quarter* a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 28 *quarter. Xarxa de cooperació operativa del CSIRT-AD*

1. Amb l'objectiu de reforçar la confiança, la seguretat i la cooperació operativa àgil i eficaç en l'àmbit de la ciberseguretat, el CSIRT-AD ha de formar part d'una xarxa de col·laboració amb altres equips nacionals de resposta a emergències informàtiques, en

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

la mesura que sigui possible i adient, en particular amb els CSIRT dels països membres de la Unió Europea i amb Servei de Ciberseguretat per a les Institucions, els Òrgans i els Organismes de la Unió Europea (CERT-UE).

2. Aquesta col·laboració operativa ha d'impulsar els objectius següents:

a) Intercanviar informació sobre les capacitats tècniques i operatives dels CSIRT.

b) Compartir coneixements, bones pràctiques, tecnologies, metodologies i marcs operatius rellevants.

c) Intercanviar informació sobre incidents, quasiincidents, amenaces, riscos i vulnerabilitats.

d) Debatre i, si escau, coordinar respostes comunes davant d'incidents de naturalesa transfronterera.

e) Donar suport a la interoperabilitat dels sistemes d'intercanvi d'informació i als protocols de comunicació segurs.

f) Promoure l'assistència mútua i el suport tècnic, especialment en casos d'incidents que puguin afectar més d'un territori.

g) Col·laborar amb els CSIRT coordinadors en la divulgació coordinada de vulnerabilitats amb impacte potencial multiterritorial.

h) Donar suport en l'elaboració o revisió del pla nacional de resposta a incidents i crisis de ciberseguretat a gran escala.

i) Informar periòdicament l'ANC-AD i altres autoritats competents sobre les activitats desenvolupades en el marc d'aquesta xarxa.

3. El CSIRT-AD pot establir convenis de col·laboració, protocols d'actuació o altres instruments amb organismes equivalents d'altres països o de la Unió Europea per tal de regular aquesta cooperació operativa.

4. El CSIRT-AD pot participar, quan sigui adient, en els exercicis conjunts organitzats per l'ENISA o altres entitats europees especialitzades en ciberseguretat, amb l'objectiu de millorar la preparació i la resposta a incidents de ciberseguretat."

Esmena 12	**De modificació**
GPS (8) Es proposa modificar l'article 8 de la forma següent: " (...) Article 28 quarter. *Xarxa de cooperació operativa del CSIRT-AD* 1. Amb l'objectiu de reforçar la confiança, la seguretat i la cooperació operativa àgil i eficaç en l'àmbit de la ciberseguretat, el CSIRT-AD ha de formar part d'una xarxa de	

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

col·laboració amb altres equips nacionals de resposta a emergències informàtiques, en la mesura que sigui possible i adient, en particular amb els CSIRT dels països membres de la Unió Europea i amb Servei de Ciberseguretat per a les Institucions, els Òrgans i els Organismes de la Unió Europea (CERT-UE).

2. Aquesta col·laboració operativa ha d'impulsar els objectius següents:

a) Intercanviar informació sobre les capacitats tècniques i operatives dels CSIRT.

b) Compartir coneixements, bones pràctiques, tecnologies, metodologies i marcs operatius rellevants.

c) Intercanviar informació sobre incidents, quasiincidents, amenaces, riscos i vulnerabilitats.

d) Debatre i, si escau, coordinar respostes comunes davant d'incidents de naturalesa transfronterera.

e) Donar suport a la interoperabilitat dels sistemes d'intercanvi d'informació i als protocols de comunicació segurs.

f) Promoure l'assistència mútua i el suport tècnic, especialment en casos d'incidents que puguin afectar més d'un territori.

g) Col·laborar amb els CSIRT coordinadors en la divulgació coordinada de vulnerabilitats amb impacte potencial multiterritorial.

h) Donar suport en l'elaboració o revisió del pla nacional de resposta a incidents i crisis de ciberseguretat a gran escala.

i) Informar periòdicament l'ANC-AD i altres autoritats competents sobre les activitats desenvolupades en el marc d'aquesta xarxa.

3. Totes les actuacions d'intercanvi d'informació previstes en aquest article s'han de dur a terme garantint la confidencialitat de la informació compartida, la protecció de les dades personals, el secret empresarial i la preservació dels interessos essencials del Principat d'Andorra.

~~3.~~ **4.** El CSIRT-AD pot establir convenis de col·laboració, protocols d'actuació o altres instruments amb organismes equivalents d'altres països o de la Unió Europea per tal de regular aquesta cooperació operativa.

~~4.~~ **5.** El CSIRT-AD pot participar, quan sigui adient, en els exercicis conjunts organitzats per l'ENISA o altres entitats europees especialitzades en ciberseguretat, amb l'objectiu de millorar la preparació i la resposta a incidents de ciberseguretat.»

PÀGINA: 25 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

MOTIVACIÓ

L'esmena reforça les garanties aplicables al conjunt de les actuacions d'intercanvi d'informació en el marc de la cooperació operativa entre equips de resposta a incidents de ciberseguretat. Tot i que aquesta cooperació constitueix un element essencial per millorar la detecció i la resposta davant ciberamenaces, és convenient establir amb caràcter general que qualsevol intercanvi d'informació ha de respectar la confidencialitat, la normativa de protecció de dades, el secret empresarial i els interessos essencials del Principat d'Andorra.

Aquesta precisió reforça la seguretat jurídica del precepte sense limitar la cooperació internacional ni alterar la seva finalitat.

Article 9. ***Addició de l'article 28 quinquies de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació***

S'addiciona l'article 28 *quinquies* a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article 28 *quinquies. Participació en l'EU-CyCLONe*

1. Per tal de facilitar la gestió coordinada d'incidents i crisis de ciberseguretat a gran escala, el Principat d'Andorra, mitjançant les seves autoritats de gestió de crisis en ciberseguretat, pot col·laborar amb l'EU-CyCLONe, així com amb les eventuals evolucions o derivacions futures d'aquesta última, especialment quan es consideri que un incident pot tenir un impacte significatiu en serveis o activitats del país o vinculats amb el país, mitjançant acords específics de col·laboració, els quals han de tenir com a objectius:

a) Millorar el nivell de preparació del país per a la gestió de crisis de ciberseguretat.

b) Contribuir al coneixement d'incidents amb impacte transfronterer.

c) Avaluar els impactes potencials o reals d'aquests incidents i proposar mesures pal·liatives.

d) Col·laborar, si escau, en la coordinació política i operativa davant de crisis de gran escala.

e) Revisar, a petició pròpia o d'un tercer, el pla nacional de resposta a incidents i crisis de ciberseguretat.

2. El Principat d'Andorra, en el marc de la cooperació internacional, pot establir acords o convenis amb els membres de l'EU-CyCLONe o amb la mateixa ENISA, o amb les eventuals estructures que la puguin substituir o complementar en el futur, per regular la participació, l'intercanvi segur d'informació i el suport mutu davant de situacions de crisi."

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

Esmena 13	**De modificació**

GPS (9)

Es proposa modificar l'article 9 de la forma següent:

"(...)

Article 28 quinquies. *Participació en l'EU-CyCLONe*

1. Per tal de facilitar la gestió coordinada d'incidents i crisis de ciberseguretat a gran escala, el Principat d'Andorra, mitjançant les seves autoritats de gestió de crisis en ciberseguretat, pot col·laborar amb l'EU-CyCLONe, així com amb les eventuals evolucions o derivacions futures d'aquesta última, especialment quan es consideri que un incident pot tenir un impacte significatiu en serveis o activitats del país o vinculats amb el país, mitjançant acords específics de col·laboració, els quals han de tenir com a objectius:

a) Millorar el nivell de preparació del país per a la gestió de crisis de ciberseguretat.

b) Contribuir al coneixement d'incidents amb impacte transfronterer.

c) Avaluar els impactes potencials o reals d'aquests incidents i proposar mesures pal·liatives.

d) Col·laborar, si escau, en la coordinació política i operativa davant de crisis de gran escala. e) Revisar, a petició pròpia o d'un tercer, el pla nacional de resposta a incidents i crisis de ciberseguretat.

2. El Principat d'Andorra, en el marc de la cooperació internacional, pot establir acords o convenis amb els membres de l'EU-CyCLONe o amb la mateixa ENISA, o amb les eventuals estructures que la puguin substituir o complementar en el futur, per regular la participació, l'intercanvi segur d'informació i el suport mutu davant de situacions de crisi~~.~~**, sobre la base dels principis de reciprocitat, proporcionalitat, confidencialitat, respecte a la sobirania institucional del Principat d'Andorra i compliment de la normativa vigent en matèria de protecció de dades i seguretat de la informació."**

MOTIVACIÓ

L'esmena té per objecte reforçar les garanties aplicables als acords de cooperació internacional en matèria de gestió de crisis de ciberseguretat. Tot i que la cooperació amb l'EU-CyCLONe i amb l'ENISA constitueix un instrument essencial per millorar la preparació i la resposta davant incidents transfronterers, és convenient explicitar que aquesta cooperació s'ha de desenvolupar d'acord amb els principis de reciprocitat, proporcionalitat, confidencialitat, respecte a la sobirania institucional del Principat d'Andorra i compliment de la normativa vigent en matèria de protecció de dades i seguretat de la informació.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

La modificació no altera la finalitat del precepte ni limita la capacitat del Principat d'Andorra per participar en mecanismes internacionals de cooperació, sinó que reforça la seguretat jurídica dels futurs acords que es puguin subscriure.

Article 10. *Modificació de l'article 31 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

Es modifica l'article 31 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"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 que hi estan establerts, així com les entitats referides a l'apartat 1 de l'article 16 pel que fa a l'incompliment de les seves obligacions d'acord amb el que està estipulat en el dit article."

Esmena 14	**De modificació**

GPS (10)

Es proposa modificar l'article 10 de la forma següent:

" (...)

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 que hi estan establerts, així com les entitats referides a l'apartat 1 de l'article 16 **que estiguin subjectes a l'obligació de notificació d'acord amb els criteris establerts en aquest article,** pel que fa a l'incompliment de les seves obligacions d'acord amb el que està estipulat en el dit article~~.~~ **, sempre que l'incompliment els sigui imputable a títol de dol o negligència, d'acord amb els principis generals del dret administratiu sancionador."**

MOTIVACIÓ

L'esmena té una doble finalitat. D'una banda, adapta la redacció de l'article 31 a les modificacions introduïdes a l'article 16, aclarint que únicament poden ser responsables les entitats que estiguin efectivament subjectes a l'obligació de notificació d'acord amb els criteris objectius establerts en aquesta Llei.

D'altra banda, incorpora expressament el principi de culpabilitat propi del dret administratiu sancionador, de manera que la responsabilitat només pugui exigir-se quan l'incompliment sigui imputable a títol de dol o negligència. Aquesta precisió reforça la seguretat jurídica i és coherent amb els principis generals que regeixen l'exercici de la potestat sancionadora.

PÀGINA: 28 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

Esmena 15	**De modificació**

GPC (5)

Es proposa modificar l'article 10 del Projecte de llei, que modifica l'article 31 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació. La proposta modifica l'article 31, que queda redactat de la manera següent:

"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 que hi estan establerts, així com les entitats referides a l'apartat 1 de l'article 16 pel que fa a l'incompliment de les seves obligacions d'acord amb el que està estipulat en el dit article~~.~~**, així com les persones físiques o jurídiques, públiques o privades, no incloses en l'àmbit subjectiu establert a l'article 2, a les quals s'hagin imposat mesures extraordinàries en aplicació de l'article 16 bis, pel que fa a l'incompliment de les obligacions establertes en la resolució corresponent.**

Als efectes del règim sancionador previst en aquest títol, les referències a l'entitat infractora s'entenen fetes a qualsevol dels subjectes responsables previstos en aquest article."

MOTIVACIÓ

En coherència amb l'esmena 6 (esmena 3 GPC), es manté la responsabilitat de les entitats excloses de l'àmbit ordinari de la Llei respecte de les obligacions de notificació que els siguin aplicables. Així mateix, s'incorporen les persones físiques o jurídiques a les quals es puguin imposar mesures extraordinàries obligatòries en aplicació de l'article 16 bis, limitant la seva responsabilitat a l'incompliment de les obligacions concretament establertes en la resolució corresponent. Aquesta incorporació s'ha de completar amb la tipificació específica de l'incompliment a l'article 34.

Article 11. *Modificació de l'article 34 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

Es modifica l'article 34 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"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 a entitat essencial o important, de conformitat amb el que preveu l'article 10, quan aquesta entitat 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 el que està establert en aquesta Llei.

PÀGINA: 29 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

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 que està previst a l'article 15. Es considera que és reiterat a partir del segon incompliment.

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

e) L'incompliment de l'obligació de disposar d'un SOC, de conformitat amb el que disposa l'article 12 *bis,* quan aquest incompliment impedeixi garantir la vigilància, la detecció i la resposta davant incidents amb efectes pertorbadors significatius sobre un o més serveis essencials o importants.

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 el que està establert en aquest article. En queden exemptes les entitats essencials i importants que no disposin d'un establiment al Principat d'Andorra, en tant que l'ANC-AD no els hagi notificat la seva condició d'entitat essencial o important per al Principat d'Andorra i les obligacions que els són aplicables 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."

Esmena 16	**De modificació**
GPS (11) Es proposa modificar l'article 11 de la forma següent:	

PÀGINA: 30 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

"(...)

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 a entitat essencial o important, de conformitat amb el que preveu l'article 10, quan aquesta entitat 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 el que està 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 que està previst a l'article 15. Es considera que és reiterat a partir del segon incompliment.

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

~~e) L'incompliment de l'obligació de disposar d'un SOC, de conformitat amb el que disposa l'article 12 bis, quan aquest incompliment impedeixi garantir la vigilància, la detecció i la resposta davant incidents amb efectes pertorbadors significatius sobre un o més serveis essencials o importants.~~

e) L'incompliment de l'obligació de disposar d'un SOC, de conformitat amb el que disposa l'article 12 bis, quan aquest incompliment impedeixi garantir la vigilància, la detecció i la resposta davant incidents amb efectes pertorbadors significatius sobre un o més serveis essencials o importants, sempre que, durant el termini transitori o d'adaptació concedit, no s'hagin adoptat mesures tècniques o organitzatives provisionals que garanteixin un nivell equivalent de protecció.

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 el que està establert en aquest article. En queden exemptes les entitats essencials i importants que no disposin d'un establiment al Principat d'Andorra, en tant que l'ANC-AD no els hagi notificat la seva condició d'entitat essencial o important

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

per al Principat d'Andorra i les obligacions que els són aplicables 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."

MOTIVACIÓ

L'esmena té per objecte reforçar els principis de legalitat, proporcionalitat i seguretat jurídica en l'exercici de la potestat sancionadora.

En primer lloc, es modifica la tipificació de la infracció molt greu relativa al centre d'operacions de seguretat (SOC). Es manté plenament l'obligació de disposar d'un SOC, propi o prestat per un proveïdor especialitzat, però s'evita qualificar automàticament l'incompliment com a molt greu durant el termini transitori o d'adaptació concedit quan l'entitat hagi adoptat mesures provisionals que garanteixin un nivell equivalent de protecció.

En segon lloc, se suprimeix la referència a les instruccions tècniques com a font directa d'infraccions administratives. D'acord amb el principi de legalitat sancionadora, la tipificació de conductes infractores ha de descansar en normes amb rang legal o reglamentari, sense que unes instruccions tècniques o guies administratives puguin ampliar per si mateixes l'àmbit de la responsabilitat sancionadora.

L'esmena manté íntegrament els objectius de la Llei i les facultats de supervisió de les autoritats competents, però reforça les garanties pròpies del dret administratiu sancionador i la coherència del règim d'infraccions amb els principis constitucionals de seguretat jurídica i legalitat.

Esmena 17 **D'addició**

GPC (6)

Es proposa modificar l'article 11 del Projecte de llei, que modifica l'article 34 de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes

PÀGINA: 32 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

d'informació. La proposta addiciona les lletres c) i d) a l'apartat 3 de l'article 34, amb la redacció següent

"Article 34. *Classificació de les infraccions*

(...)

3. Són infraccions greus:

(...)

c) L'incompliment, per part de les entitats referides a l'apartat 1 de l'article 16, de l'obligació de notificar els incidents significatius i les ciberamenaces significatives que puguin donar lloc a un incident significatiu, així com de l'obligació d'adoptar les mesures necessàries per gestionar i resoldre l'incident notificat, d'acord amb el que estableix l'article 16.

d) L'incompliment de les obligacions establertes en una resolució adoptada en aplicació de l'article 16 bis per part de les persones físiques o jurídiques, públiques o privades, no incloses en l'àmbit subjectiu establert a l'article 2, a les quals s'hagin imposat mesures extraordinàries de reforç de la ciberseguretat.

(...)"

MOTIVACIÓ

En coherència amb l'esmena 6 (esmena 3 GPC), es tipifica expressament l'incompliment de les obligacions de notificació i de gestió i resolució dels incidents imposades a les entitats excloses de l'àmbit ordinari de la Llei. Així mateix, es tipifica l'incompliment de les mesures extraordinàries que es puguin imposar, en aplicació de l'article 16 bis, a persones físiques o jurídiques no incloses en l'article 2. D'aquesta manera, es completa el règim de responsabilitat previst a l'article 31 i es determina expressament quines conductes constitueixen infracció greu.

Article 12. *Addició de l'article 38 bis de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

S'addiciona l'article 38 *bis* a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

"Article *38 bis. Reducció per conformitat de les sancions consistents en multes administratives per infraccions lleus o greus*

1. En els procediments sancionadors incoats en aplicació d'aquesta Llei, quan la sanció prevista sigui una multa administrativa per una infracció lleu o greu, l'autoritat que disposa de la potestat sancionadora pot acordar una reducció per conformitat d'un vint per cent (20%) de l'import de la sanció proposada si l'entitat infractora:

a) Reconeix expressament la seva responsabilitat; i

PÀGINA: 33 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

b) Procedeix al pagament voluntari de la multa dins el termini que s'estableixi en la notificació de la proposta de resolució.

2. Addicionalment, l'òrgan competent pot acordar una reducció complementària per conformitat de fins a un vint per cent (20%) de l'import de la multa administrativa quan concorrin, totalment o parcialment, de manera acumulativa a allò que està previst a l'apartat anterior, les circumstàncies següents:

a) Notificació immediata i completa de l'incident de seguretat objecte del procediment sancionador;

b) Cooperació plena i efectiva durant la instrucció del procediment sancionador;

c) Adopció ràpida i verificable de mesures correctores adequades per eliminar o minimitzar el risc o l'impacte de l'incident objecte del procediment sancionador; i

d) Absència de reincidència en infraccions de la mateixa naturalesa.

3. L'aplicació de les reduccions per conformitat previstes en aquest article està condicionada a la renúncia expressa de l'entitat infractora a formular al·legacions durant l'expedient sancionador i a interposar recursos en via administrativa i accions judicials contra la resolució sancionadora.

4. Les reduccions per conformitat regulades en aquest article no són aplicables a les infraccions qualificades com a molt greus.

5. La decisió d'aplicar les reduccions per conformitat ha de ser motivada, amb indicació expressa de les circumstàncies valorades, i s'ha de reflectir en la resolució sancionadora."

Esmena 18	**De modificació**
GPS (12) Es proposa modificar l'article 12 de la forma següent: "(...) Article 38 bis. *Reducció per conformitat de les sancions consistents en multes administratives per infraccions lleus o greus* 1. En els procediments sancionadors incoats en aplicació d'aquesta Llei, quan la sanció prevista sigui una multa administrativa per una infracció lleu o greu, l'autoritat que disposa de la potestat sancionadora pot acordar una reducció per conformitat d'un vint per cent (20%) de l'import de la sanció proposada si l'entitat infractora: a) Reconeix expressament la seva responsabilitat; i b) Procedeix al pagament voluntari de la multa dins el termini que s'estableixi en la notificació de la proposta de resolució.	

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

2. Addicionalment, l'òrgan competent pot acordar una reducció complementària per conformitat de fins a un vint per cent (20%) de l'import de la multa administrativa quan concorrin, totalment o parcialment, de manera acumulativa a allò que està previst a l'apartat anterior, les circumstàncies següents:

a) Notificació immediata i completa de l'incident de seguretat objecte del procediment sancionador;

b) Cooperació plena i efectiva durant la instrucció del procediment sancionador;

c) Adopció ràpida i verificable de mesures correctores adequades per eliminar o minimitzar el risc o l'impacte de l'incident objecte del procediment sancionador; i

d) Absència de reincidència en infraccions de la mateixa naturalesa.

~~3. L'aplicació de les reduccions per conformitat previstes en aquest article està condicionada a la renúncia expressa de l'entitat infractora a formular al·legacions durant l'expedient sancionador i a interposar recursos en via administrativa i accions judicials contra la resolució sancionadora.~~

3. L'aplicació de les reduccions per conformitat previstes en aquest article està condicionada al reconeixement exprés de la responsabilitat, al pagament voluntari de la sanció i a la renúncia a formular al·legacions i recursos en via administrativa contra la resolució sancionadora. Aquesta renúncia no pot impedir l'accés a la jurisdicció ni l'exercici de les accions judicials reconegudes per l'ordenament jurídic.

4. Les reduccions per conformitat regulades en aquest article no són aplicables a les infraccions qualificades com a molt greus.

5. La decisió d'aplicar les reduccions per conformitat ha de ser motivada, amb indicació expressa de les circumstàncies valorades, i s'ha de reflectir en la resolució sancionadora."

MOTIVACIÓ

L'esmena té per objecte compatibilitzar l'eficàcia del règim de reducció per conformitat amb les garanties del procediment administratiu sancionador i el dret fonamental a la tutela judicial efectiva.

La finalitat de les reduccions per conformitat és incentivar el reconeixement de la responsabilitat, el pagament voluntari de la sanció i la ràpida adopció de mesures correctores. Per garantir l'eficàcia de la conformitat, es manté la renúncia a formular al·legacions i recursos en via administrativa, però s'elimina la renúncia anticipada a l'accés a la jurisdicció i a les accions judicials reconegudes per l'ordenament jurídic.

Aquesta solució preserva la utilitat del mecanisme de conformitat i, alhora, evita que l'obtenció de la reducció comporti una renúncia absoluta i anticipada a la tutela judicial.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

Esmena 19	De modificació

GPC (7)

Es proposa modificar l'article 12 del Projecte de llei, que addiciona l'article 38 bis a la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació. La proposta modifica l'apartat 3 de l'article 38 bis, que queda redactat de la manera següent:

"Article 38 bis. *Reducció per conformitat de les sancions consistents en multes administratives per infraccions lleus o greus*

[...]

~~3. L'aplicació de les reduccions per conformitat previstes en aquest article està condicionada a la renúncia expressa de l'entitat infractora a formular al·legacions durant l'expedient sancionador i a interposar recursos en via administrativa i accions judicials contra la resolució sancionadora.~~

3. L'aplicació de les reduccions per conformitat previstes en aquest article està condicionada a la renúncia expressa de l'entitat infractora a formular al·legacions contra la proposta de resolució. Les al·legacions formulades amb anterioritat no impedeixen l'aplicació de les reduccions. La interposició d'un recurs administratiu o jurisdiccional contra la resolució sancionadora comporta la pèrdua de les reduccions aplicades. En aquest cas, l'import a satisfer es calcula sobre la sanció que resulti ferma després de la impugnació, sense aplicar les reduccions previstes en aquest article.

[...] "

MOTIVACIÓ

Es permet que l'entitat exerceixi el seu dret de defensa durant la tramitació de l'expedient i pugui acollir-se posteriorment a la reducció si accepta la proposta de resolució. En cas d'impugnació posterior, es perd la reducció i la sanció que resulti ferma s'abona sense aplicar-la.

Article 13. *Modificació de l'annex I de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació*

Es modifica l'annex I de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que queda redactat com segueix:

Annex I. Entitats essencials

Sector	Subsector	Tipus d'entitats
1. Energia		Infraestructures energètiques de fonts renovables a les quals es refereix el Decret del

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

	a) Infraestructures energètiques	16-5-2018 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 16-5-2018 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 16-5-2018 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 16-5-2018 d'aprovació i publicació del Pla sectorial d'infraestructures energètiques d'Andorra.
	b) Electricitat	Entitat encarregada de la importació, la generació, la distribució i la 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, distribuïdores o comercialitzadores 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

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

		transport de petroli en virtut del Decret d'aprovació del Reglament d'emmagatzematge, subministrament, distribució i ús d'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, del 22-6-2000, i 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.
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.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

	b) Transports ferroviaris	Administradors d'infraestructures ferroviàries.
	c) Transports aeris	Operadors competents de transport d'aeronaus d'acord amb el Decret del 24-2-2016 pel qual s'aprova el Reglament d'aeronaus no tripulades, pilotades remotament, i, especialment, els 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 a 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 efectuen activitats de recerca i desenvolupament de medicaments, entitats que fabriquen productes farmacèutics de base i especialitats

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

		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.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

		- Proveïdors 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.
9. Ràdio i televisió públiques		Entitat pública encarregada dels serveis de radiodifusió i de televisió, que es declaren serveis públics, amb caràcter essencial, de titularitat estatal, regulada a la Llei de la radiodifusió i televisió pública i de creació de la societat pública Ràdio i Televisió d'Andorra SA, del 13 d'abril del 2000.

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

Disposició transitòria. ***Implementació progressiva de les obligacions establertes a l'article 12 bis***

1. Les entitats crítiques i les entitats equivalents a entitats crítiques disposen d'un termini màxim de dotze (12) mesos a comptar de l'entrada en vigor d'aquesta Llei per complir les obligacions següents:

a) Disposar d'un centre d'operacions de seguretat (SOC) amb capacitat nacional i amb el nivell de capacitat operativa mínim establert per l'ANC-AD i/o l'AFA, dotat dels recursos humans i tècnics necessaris per garantir la vigilància, la detecció i la resposta davant incidents de seguretat de la informació en temps real.

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

b) Garantir que les dades generades pel SOC, així com les claus criptogràfiques vinculades a la gestió de la seguretat de la informació o a la protecció d'infraestructures crítiques, estiguin allotjades dins del territori del Principat d'Andorra, llevat d'autorització expressa de l'ANC-AD i/o l'AFA.

c) Disposar, almenys, d'una sonda externa de monitoratge gestionada per l'ANC-AD o per l'AFA, segons correspongui.

2. L'obligació d'intercanvi proactiu i sistemàtic d'intel·ligència d'incidents amb l'ANC-AD i/o l'AFA és exigible a partir del sisè mes des de l'entrada en vigor d'aquesta Llei. Durant aquest període, l'ANC-AD i/o l'AFA ha de coordinar la creació dels grups de treball interdisciplinaris per definir els protocols, els canals, els formats i els requisits tècnics per a l'intercanvi d'informació.

3. L'ANC-AD i/o l'AFA pot concedir, mitjançant resolució motivada i de caràcter excepcional, una pròrroga màxima de sis (6) mesos addicionals per a l'adaptació tècnica o contractual quan concorrin circumstàncies degudament justificades i acreditades documentalment per l'entitat afectada.

4. Durant el període transitori, les entitats han d'informar trimestralment l'ANC-AD i/o l'AFA sobre l'estat d'implementació de cadascuna de les obligacions establertes a l'article 12 *bis*.

Esmena 20	**De modificació**

GPS (13)

Es proposa modificar la disposició transitòria de la forma següent:

"Disposició transitòria. I*mplementació progressiva de les obligacions establertes a l'article 12 bis*

1. Les entitats crítiques i les entitats equivalents a entitats crítiques disposen d'un termini màxim de dotze (12) mesos a comptar de l'entrada en vigor d'aquesta Llei per complir les obligacions següents:

a) Disposar d'un centre d'operacions de seguretat (SOC) amb capacitat nacional ~~i amb el nivell de capacitat operativa mínim establert per l'ANC-AD i/o l'AFA~~ **i amb el nivell de capacitat operativa mínim establert reglamentàriament**, dotat dels recursos humans i tècnics necessaris per garantir la vigilància, la detecció i la resposta davant incidents de seguretat de la informació en temps real.

~~b) Garantir que les dades generades pel SOC, així com les claus criptogràfiques vinculades a la gestió de la seguretat de la informació o a la protecció d'infraestructures crítiques, estiguin allotjades dins del territori del Principat d'Andorra, llevat d'autorització expressa de l'ANC-AD i/o l'AFA.~~

b) Garantir que les dades generades pel SOC, així com les claus criptogràfiques vinculades a la gestió de la seguretat de la informació o a la protecció d'infraestructures crítiques, es tractin i s'allotgin amb el nivell de protecció previst per la legislació andorrana i, quan s'allotgin fora del territori nacional, comunicar-ho

Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

prèviament a l'ANC-AD i/o a l'AFA i acreditar el compliment dels requisits establerts reglamentàriament, d'acord amb el que disposa l'article 12 bis.

c) Disposar, almenys, d'una sonda externa de monitoratge gestionada per l'ANC-AD o per l'AFA, segons correspongui.

2. L'obligació d'intercanvi proactiu i sistemàtic d'intel·ligència d'incidents amb l'ANC-AD i/o l'AFA és exigible a partir del sisè mes des de l'entrada en vigor d'aquesta Llei. Durant aquest període, l'ANC-AD i/o l'AFA ha de coordinar la creació dels grups de treball interdisciplinaris per definir els protocols, els canals, els formats i els requisits tècnics per a l'intercanvi d'informació, **garantint la participació efectiva de les entitats afectades en la seva elaboració**.

3. L'ANC-AD i/o l'AFA pot concedir, mitjançant resolució motivada i de caràcter excepcional, una pròrroga màxima de sis (6) mesos addicionals per a l'adaptació tècnica o contractual quan concorrin circumstàncies degudament justificades i acreditades documentalment per l'entitat afectada**, valorant especialment la complexitat tècnica de la implantació, la disponibilitat de solucions tecnològiques adequades i les actuacions ja desenvolupades per l'entitat per donar compliment a les obligacions establertes en aquesta Llei.**

4. Durant el període transitori, les entitats han d'informar trimestralment l'ANC-AD i/o l'AFA sobre l'estat d'implementació de cadascuna de les obligacions establertes a l'article 12 bis, **i aquestes autoritats han de prestar el suport tècnic necessari per facilitar-ne el compliment, especialment mitjançant la publicació de criteris interpretatius, recomanacions i bones pràctiques.**"

MOTIVACIÓ

L'esmena té per objecte reforçar la seguretat jurídica i facilitar una implantació progressiva, homogènia i efectiva de les noves obligacions introduïdes per l'article 12 bis.

En primer lloc, s'adapta la disposició transitòria a les modificacions proposades a l'article 12 bis, substituint la referència a requisits fixats per l'ANC-AD o l'AFA per un desenvolupament reglamentari i harmonitzant el règim d'allotjament de les dades amb el criteri del nivell equivalent de protecció.

En segon lloc, es reforça la participació de les entitats afectades en la definició dels protocols tècnics d'intercanvi d'informació, afavorint un desplegament consensuat i operativament viable.

Igualment, es concreten els criteris que han de valorar-se per concedir eventuals pròrrogues, reforçant la transparència i la igualtat de tracte entre les entitats obligades.

Finalment, s'incorpora el deure de les autoritats competents d'acompanyar les entitats durant el període transitori mitjançant assistència tècnica, criteris interpretatius i bones

PÀGINA: 43 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

pràctiques, amb l'objectiu de facilitar el compliment efectiu de la Llei i reforçar la resiliència global del sistema de ciberseguretat nacional.

Esmena 21	**De modificació**

GPC (8)

Es proposa modificar la disposició transitòria del Projecte de llei, relativa a la implementació progressiva de les obligacions establertes a l'article 12 bis. La proposta modifica la lletra a) de l'apartat 1 de la disposició transitòria, que queda redactada de la manera següent:

"Disposició transitòria. *Implementació progressiva de les obligacions establertes a l'article 12 bis*

[...]

a) Disposar d'un centre d'operacions de seguretat (SOC) ~~amb capacitat nacional i~~ amb el nivell de capacitat operativa mínim establert per l'ANC-AD i/o l'AFA, dotat dels recursos humans i tècnics necessaris per garantir la vigilància, la detecció i la resposta davant incidents de seguretat de la informació en temps real.

[...] "

MOTIVACIÓ

Se suprimeix l'expressió «capacitat nacional» perquè no se'n concreta el contingut ni l'abast i no forma part de l'obligació material establerta a l'article 12 bis.1. La modificació harmonitza la disposició transitòria amb el règim substantiu, que exigeix un nivell mínim de capacitat operativa determinat per l'ANC-AD i/o l'AFA, evitant introduir durant el període transitori un requisit addicional indeterminat.

Disposició final primera. *Modificacions reglamentàries*

1. El Govern ha d'aprovar, en el termini màxim de sis (6) mesos a partir de la data de publicació d'aquesta Llei, les modificacions reglamentàries necessàries per a l'aplicació efectiva de les modificacions introduïdes per aquesta Llei, així com qualsevol altra disposició reglamentària que sigui necessària a aquest efecte.

2. Mentre no es produeixin aquestes modificacions, les disposicions reglamentàries referides continuen vigents en allò en què no contradiguin la Llei i s'han d'interpretar, en tot cas, d'acord amb els nous principis legals.

Esmena 22	**De modificació**

GPS (14)

Es proposa modificar la disposició final primera de la forma següent:

"Disposició final primera. *Modificacions reglamentàries*

PÀGINA: 44 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

DOCUMENTS
TIPUS: Informe
NOM: 03 Informe ponència xarxes vFINAL
UNITAT: Serveis parlamentaris

ORIGEN: Administració
CODI SEGUR DE VERIFICACIÓ: 85f16539-6f2d-493e-979d-f029ac175be0
IDENTIFICADOR: ES_XXXXXXXXX_2026_00000000000000000000000073851
ESTAT D'ELABORACIÓ: Signat/validat
NIVELL D'ACCÉS:

REFERÈNCIES
EXPEDIENTS: C1210-0281/2026
SIGNATURES
CONSELL GENERAL (SIGNATURA): 11/11/2026 14:56
PERE MARSENYACH BATAILLE: 11/11/2026 17:51

1. El Govern ha d'aprovar, en el termini màxim de sis (6) mesos a partir de la data de publicació d'aquesta Llei, les modificacions reglamentàries necessàries per a l'aplicació efectiva de les modificacions introduïdes per aquesta Llei, així com qualsevol altra disposició reglamentària que sigui necessària a aquest efecte**, prèvia consulta de les autoritats competents i dels sectors afectats quan la naturalesa de la regulació ho requereixi.**

2. Mentre no es produeixin aquestes modificacions, les disposicions reglamentàries referides continuen vigents en allò en què no contradiguin la Llei i s'han d'interpretar, en tot cas, d'acord amb els nous principis legals."

MOTIVACIÓ

L'esmena reforça els principis de bona regulació, transparència i participació en l'elaboració del desenvolupament reglamentari de la Llei. Atès que bona part de les obligacions tècniques previstes en aquesta reforma s'han de concretar mitjançant disposicions reglamentàries, resulta convenient preveure expressament la consulta prèvia de les autoritats competents i dels sectors afectats, afavorint així una regulació més eficaç, proporcional i adaptada a la realitat operativa de les entitats obligades.

Disposició final segona. *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 la publicació d'aquesta Llei al *Butlletí Oficial del Principat d'Andorra* presenti al Consell General el Projecte de consolidació de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, amb la incorporació de totes les modificacions que s'hi han produït.

Esmena 23 **De modificació**

GPS (15)

Es proposa modificar la disposició final segona de la forma següent:

"Disposició final segona. *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 la publicació d'aquesta Llei al Butlletí Oficial del Principat d'Andorra presenti al Consell General el Projecte de consolidació de la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació, amb la incorporació de totes les modificacions que s'hi han produït**, garantint que el text consolidat incorpori les remissions normatives actualitzades i les concordances necessàries per facilitar-ne la interpretació i l'aplicació.**

PÀGINA: 45 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.

MOTIVACIÓ

L'esmena té per objecte reforçar la qualitat tècnica del futur text consolidat, assegurant que aquest no es limiti a integrar les modificacions aprovades, sinó que incorpori també les remissions normatives actualitzades i les concordances necessàries per facilitar la consulta, la interpretació i l'aplicació de la Llei per part dels operadors jurídics i de les entitats afectades.

Disposició final tercera. *Entrada en vigor*

Aquesta Llei entrarà en vigor l'endemà de publicar-se al *Butlletí Oficial del Principat d'Andorra.*

El ponent

PÀGINA: 46 de 46 DATA I HORA DE LA GENERACIÓ DE LA CÒPIA: 25/11/2026 15:06
Aquest document és una còpia autèntica del document electrònic original. Podeu comprovar la seva validesa a https://registre.consellgeneral.ad/Consellers/ValidarDocuments.aspx?csv=85f16539-6f2d-493e-979d-f029ac175be0 emprant el codi segur de verificació.