4. IMPULS I CONTROL DE L'ACCIÓ POLÍTICA DEL GOVERN

4.4.2 Respostes escrites

Edicte

La síndica general, d'acord amb les previsions de l'article 90 del Reglament del Consell General,

Disposa

Publicar la resposta del Govern a les preguntes formulades pel M. I. Sr. Roger Padreny Carmona, conseller general del Grup Parlamentari Socialdemòcrata, per escrit de data 1 de desembre del 2021, relatives **a la ciberdelinqüència i ciberseguretat a Andorra**, i publicada en el Butlletí del Consell General número 138/2021, de l'1 de desembre.

Tot el que es fa públic per a general coneixement i efectes.

Casa de la Vall, 18 de gener del 2022

Roser Suñé Pascuet
Síndica General

Secretaria d'Estat de Transició Digital i Projectes estratègics
Resposta a la pregunta escrita (Reg. núm. 1126/21)

Respostes a les preguntes amb resposta escrita formulades l'01 de desembre del 2021 pel conseller general del Grup Parlamentari Socialdemòcrata Roger Padreny Carmona, relatives a la ciberdelinqüència i la ciberseguretat a Andorra (Reg. núm. 1126)

Vist el Pla d'acció del Govern d'Andorra 2020-2023 (H23), presentat el 27 de juliol del 2020.

Vista la compareixença pública conjunta del ministre de Justícia i Interior, el Sr. Josep Maria Rossell, i el ministre d'Afers Socials, Habitatge i Joventut, el Sr. Víctor Filloy, davant la comissió legislativa de Justícia, Interior i Afers institucionals i davant la comissió legislativa d'Afers Socials i Igualtat del Consell General, del passat 14 de desembre del 2020.

Vist el Programa de Transformació Digital d'Andorra del Govern d'Andorra, presentat el passat 6 de juliol del 2021.

Vista l'Estratègia de Ciberseguretat d'Andorra del Govern d'Andorra, presentada el passat 25 d'octubre del 2021.

Vist el Decret 346/2021, del 20 d'octubre del 2021, de creació de l'Agència Nacional de Ciberseguretat i de l'Equip de Resposta de Referència del Principat d'Andorra per al tractament d'incidents de seguretat de les xarxes i els sistemes d'informació, publicat al Butlletí Oficial del Principat d'Andorra número 111, del 27 d'octubre del 2021.

Vist el Projecte de llei del pressupost per a l'exercici del 2022, publicat al Butlletí del Consell General 128/2021, del 10 de novembre del 2021.

Es demana:

Amb referència a la compareixença pública al Consell General del 14 de desembre del 2020:

1. Quin és el nombre total de ciberdelictes detectats pel Grup de Delictes Tecnològics del Cos de Policia d'Andorra, dividits per tipus delictiu, l'any 2021?

Seguidament s'inclouen el nombre de ciberdelictes detectats pel Grup de Delictes Tecnològics del Cos de Policia d'Andorra, dividits per tipus delictiu, al llarg de l'any 2021:

DENÚNCIES per tipus delictiu	**2021**
Extorsió sexual (*sextorison*)	26
Vulneració d'intimitat	52
Programari de segrest (*ransomware*)	14
Pesca (*phishing*)	16
Estafes	18
Usurpació d'identitat	23
Segrest i bloqueig d'aplicacions (WhatsApp, Instagram, Telegram...)	45
TOTAL	**194**

CASOS DE PORNOGRAFIA INFANTIL (CyberTipline NCMEC)	**2021**
Greu	69
No greu	40
TOTAL	**109**

2. Quin és el percentatge comparatiu del nombre total de ciberdelictes detectats l'any 2021, respecte a l'any 2020? I per tipus de ciberdelictes?

A continuació es facilita el percentatge comparatiu del nombre total de ciberdelictes detectats durant l'any 2021 respecte a l'any 2020, per tipus de ciberdelictes:

DENÚNCIES per tipus delictiu	**2020**	**2021**	**Percentatge de l'any 2021 respecte al 2020**
Extorsió sexual	23	26	13,04%
Vulneració d'intimitat	38	52	36,84%
Programari de segrest	22	14	-36,36%
Pesca	34	16	-52,94%
Estafes	21	18	-14,29%
Usurpació d'identitat	10	23	130,00%
Segrest i bloqueig d'aplicacions (WhatsApp, Instagram, Telegram...)	59	45	-23,73%
TOTAL	**207**	**194**	**-6,28%**

CASOS DE PORNOGRAFIA INFANTIL (CyberTipline NCMEC)	**2020**	**2021**	**Percentatge de l'any 2021 respecte al 2020**
Greu	61	69	13,11%
No greu	32	40	25,00%
TOTAL	**93**	**109**	**17,20%**

3. Quins és el nombre total de "casos forense", dividits per tipus delictiu, detectats l'any 2021?

Seguidament es detalla el nombre total de *casos forense*, dividits per tipus delictiu, detectats al llarg del l'any 2021:

ASSUMPTES AMB ACTUACIONS FORENSES (fets i en curs)	**2021**
Delicte contra el patrimoni	5
Delicte contra la salut pública	14
Delicte contra la llibertat sexual	14
Delicte contra la llibertat	0
Delicte contra l'ordre socioeconòmic	4

Delicte contra la intimitat	3
Delicte contra la funció pública	0
Delicte contra la integritat física	0
Delicte contra la vida humana independent	2
Delicte contra l'Administració de justícia	3
TOTAL	**45**

4. Quin és el percentatge comparatiu del nombre total de "casos forense" de l'any 2021, respecte a l'any 2020?

A continuació es recull el percentatge comparatiu del nombre total de *casos forense* de l'any 2021 respecte a l'any 2020:

ASSUMPTES AMB ACTUACIONS FORENSES (fets i en curs)	**2020**	**2021**	**Percentatge de l'any 2021 respecte al 2020**
Delicte contra el patrimoni	2	5	150,00%
Delicte contra la salut pública	8	14	75,00%
Delicte contra la llibertat sexual	14	14	0,00%
Delicte contra la llibertat	1	0	-100,00%
Delicte contra l'ordre socioeconòmic	4	4	0,00%
Delicte contra la intimitat	2	3	50,00%
Delicte contra la funció pública	1	0	-100,00%
Delicte contra la integritat física	1	0	-100,00%
Delicte contra la vida humana independent	1	2	100,00%
Delicte contra l'Administració de justícia	1	3	200,00%
TOTAL	**35**	**45**	**28,57%**

5. Quin és el nombre total d'extraccions de tipologia delictiva realitzades l'any 2021?

Seguidament es documenta el nombre total d'extraccions de tipologia delictiva efectuades durant l'any 2021:

NOMBRE D'EXTRACCIONS DISPOSITIUS	**2021**
DISPOSITIUS	312
TOTAL	**312**

6. Quin és el percentatge comparatiu del nombre total d'"extraccions" realitzades l'any 2021, respecte a l'any 2020?

A continuació es detalla el percentatge comparatiu del nombre total d'*extraccions* efectuades l'any 2021 respecte a l'any 2020:

NOMBRE D'EXTRACCIONS DISPOSITIUS	**2020**	**2021**	**Percentatge de l'any 2021 respecte al 2020**
DISPOSITIUS	124	312	151,61%
TOTAL	**124**	**312**	**151,61%**

Amb referència al Pla d'acció del Govern d'Andorra 2020-2023 (H23) i al Programa de Transformació Digital d'Andorra del Govern d'Andorra:

Es demana:

7. Al document de presentació del Programa de Transformació Digital s'esmenta que aquest enllaça amb el pilar "Aliances pel canvi" del Pla d'acció del Govern d'Andorra 2020-2023 (H23), presentat el 27 de juliol del 2020. També, al document de presentació del Programa de Transformació Digital s'estableix que una iniciativa d'aquest programa és la "Creació de l'agència de ciberseguretat" al setembre de l'any 2021. En quina acció de la iniciativa 15 ("Cap a una transformació digital") del Pla d'acció del Govern d'Andorra (H23) es preveu la creació de l'Agència de la Ciberseguretat d'Andorra?

Si bé es cert que dins del Pla d'acció del Govern d'Andorra 2020-2023 (H23) no es detallen de forma exhaustiva totes les subaccions vinculades a cada acció, i concretament no detalla la subacció de la creació de l'Agència de Ciberseguretat d'Andorra, la dita subacció és una necessitat vinculada a les accions previstes dins de la iniciativa 15; concretament està vinculada a les accions 15.1- *Prioritzar els projectes públics vinculats a la transformació digital*, 15.2- *Incentivar els projectes privats en l'àmbit de la digitalització del teixit empresarial* i 15.3- *Impulsar la transformació digital a través de la col·laboració d'Andorra Telecom (AT) i ActuaTech*.

L'Agència de Ciberseguretat Nacional d'Andorra haurà de vetllar per garantir un nivell de ciberseguretat adequat en l'ús dels mitjans electrònics en benefici de l'Administració pública, dels ens públics i privats de qualsevol naturalesa establerts o amb establiment

permanent al Principat d'Andorra, així com les persones físiques que es troben al nostre país. Per tant, qualsevol iniciativa o projecte dins del context digital, de naturalesa pública o privada, ha de poder ser desplegat sota un ecosistema segur, fiable i confiable, i l'Agència de Ciberseguretat n'és la responsable.

8. El Pla d'acció del Govern d'Andorra (H23) preveu "Iniciatives legislatives vinculades a l'H23" (pàg. 62 i 63) i "Iniciatives legislatives NO vinculades a l'H23" (pàg. 64), però no es preveu una iniciativa legislativa relacionada amb la ciberseguretat com sí que estableix el Decret 346/2021, del 20 d'octubre del 2021. El citat decret enuncia que "el Govern està treballant en la redacció d'un projecte de llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació, i en una regulació específica dels ciberdelictes". Per què no es va preveure la creació d'una legislació específica sobre ciberseguretat al moment d'elaborar el Pla d'acció del Govern d'Andorra (H23)? Era una prioritat pel Govern d'Andorra en el moment de redacció del "Pla H23"?

Dins el Pla d'acció del Govern d'Andorra (H23) es van incloure un seguit de pilars, iniciatives i accions estratègiques i prioritàries per al Govern. En alguns casos era necessari acabar de detallar el contingut i l'abast final de cadascuna de les iniciatives, accions i subaccions. Particularment, i pel que fa a l'adequació del marc jurídic andorrà a les diferents exigències que comporta en el sentit més ampli el desplegament d'una agència de ciberseguretat, s'han considerat tots els ajustos jurídics requerits tant a les lleis ja existents com l'elaboració de noves lleis en cas de no existir una regulació específica. A tall d'exemple s'ha promogut la revisió el Projecte de llei de modificació del Codi penal (incloent-hi els ciberdelictes en relació amb la pregunta), la Llei qualificada 4/2020, del 23 de març, dels estats d'alarma i d'emergència, i la Llei qualificada 30/2018, del 6 de desembre, de seguretat pública (modificada per la Llei 19/2020, del 23 de desembre, de seguretat pública). Aquests darrers ajustos s'han inclòs com a disposicions addicionals dins del Projecte de llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació, que és una transposició de la directiva europea NIS, recentment entrat a tràmit parlamentari. En el moment de la redacció del pla de Govern H23, la ciberseguretat dins del pla d'evolució cap a un país més digital és una necessitat i una prioritat. En aquell moment, però, no havia finalitzat la definició detallada de l'abast de les modificacions legislatives que cada subacció requeriria, raó per la qual no es va incloure com una llei específica.

Amb referència a l'Estratègia de Ciberseguretat d'Andorra del Govern d'Andorra:

Es demana:

9. L'Estratègia de Ciberseguretat d'Andorra del Govern d'Andorra preveu quatre nivells d'actuació del Govern "per la implementació efectiva d'un marc homologat per fomentar la seguretat de la informació a nivell nacional". El primer és l'anomenat "estratègic", on es preveu elaborar l'Estratègia Nacional de Ciberseguretat d'Andorra; el segon és el titulat com "regulatori", on es preveu elaborar una Llei de ciberseguretat (NIS-AD), la modificació del Codi Penal, la modificació de la Llei 30/2018, del 6 de desembre, qualificada de seguretat pública, i la modificació de la

Llei 4/2020, del 23 de març, qualificada dels estats d'alarma i d'emergència; el tercer nivell, anomenat "tàctic", es basa en la creació de l'Agència de Ciberseguretat Nacional i el Comitè Especialitzat de Ciberseguretat; i el quart nivell, anomenat de "serveis", preveu la creació de l'equip de resposta a incidents (CSIRT-AD). Per què s'ha decidit passar del primer nivell als nivells tres i quatre, sense tenir en vigor el marc regulador previst al nivell dos?

La necessitat de disposar d'un marc regulador vigent que empari tota activitat vinculada al context de la ciberseguerat és necessari perquè l'agència pugui exercir totes les potestats públiques que el seu rol requereix. No obstant això, també s'ha entès com a prioritari poder disposar d'elements i serveis certament més tàctics, però que permetin operativitzar en el més curt termini determinades activitats enteses com a essencials i necessàries, activitats que actualment no s'estan portant a terme o bé no estan reconegudes formalment.

10. L'Estratègia de Ciberseguretat d'Andorra preveu nou iniciatives per tal de complir els seus objectius. Quin és el marc temporal previst de compliment de les nou iniciatives?

El marc temporal previst per a l'acompliment dels objectius establerts dins de l'Estratègia de ciberseguretat d'Andorra, així com per a l'acompliment de les seves iniciatives, queda comprès entre el 2022 i el 2025. Tal com ja s'ha exposat a la pregunta anterior (9), s'ha considerat oportú començar immediatamen algunes de les iniciatives identificades. En concret, les iniciatives que s'han de portar a terme dins d'una primera fase són les incloses dins la Iniciativa 1, de *Creació d'un marc legal*. En particular:

- Elaboració de la Llei relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat.

- Creació de l'Agència Nacional de Ciberseguretat.

- Creació del CSIRT-AD.

- Desenvolupament d'un esquema nacional de seguretat.

- Elaboració del reglament, la identificació i protecció de les infraestructures crítiques.

- Anàlisi d'interdependències.

Les activitats esmentades anteriorment són importants perquè la planificació correcta de les iniciatives de resposta estratègica pugui avançar, de forma alineada amb els recursos que l'Estat posa a disposició per a la implementació d'aquesta estratègia. Aquesta planificació es durà a terme basant-se en els resultats de l'avaluació detallada, el cost i la priorització de les iniciatives, de manera que la implementació de la resposta estratègica en el seu conjunt es pugui assolir de la forma més eficaç i eficient possible. El resultat d'aquest procés serà una cronologia detallada que permetrà controlar l'estat d'implementació de totes les iniciatives de l'estratègia actual.

Finalment cal afegir que l'Estratègia Nacional de ciberseguretat preveu revisions periòdiques per tal d'avaluar el progrés de la seva implementació. Amb aquesta finalitat, es reveu analitzar quantitativament i qualitativament els resultats de la implementació de les mesures i disposicions incloses en les iniciatives estratègiques, així com les noves

amenaces que puguin aparèixer al ciberespai i qualsevol altra nova condició que es manifesti en aquest àmbit.

11. En la primera iniciativa de l'Estratègia de Ciberseguretat d'Andorra es preveu la creació d'un marc legal. A part de l'elaboració de la citada Llei de ciberseguretat i del Decret de creació de l'Agència Nacional de la Ciberseguretat i el CSIRT-AD, es preveu la creació d'un Esquema Nacional de Seguretat (ENS) i un Reglament de protecció d'infraestructures crítiques. Quin contingut es preveu incloure tant a l'"ENS", com al reglament citat?

L'objectiu de l'Esquema nacional de seguretat del Principat d'Andorra (en endavant, l'"ENS-AD", o "Esquema") és garantir un nivell de seguretat suficient per als serveis que resulten essencials o importants per al Principat d'Andorra. Aquest Esquema permet a les entitats que presten serveis essencials o importants identificar i implementar de manera sistemàtica i integral les mesures de seguretat que resulten necessàries per assegurar la prestació dels seus serveis, i els facilita procediments per al desenvolupament d'un sistema de gestió per a la seguretat de la informació (SGSI) que garanteixi un nivell de protecció proporcional al nivell de risc al qual estan exposats la informació i els serveis que cal protegir.

L'element troncal de l'ENS-AD és, d'acord amb el que especifica la Llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació, la gestió de riscos; un procés per identificar els riscos als quals estan exposades les infraestructures, les xarxes, els sistemes d'informació i les aplicacions que aquests últims executen, i per respondre de manera proporcional a la seva magnitud, mitjançant la planificació i la implantació de mesures de seguretat que, una vegada estiguin operatives, redueixin aquest risc de greu perjudici fins a un nivell que satisfaci els objectius que les entitats persegueixen, igualant o excedint els objectius que els resultin d'obligació per l'aplicació de la llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació i, en qualsevol cas, aconseguint o superant els objectius de risc que la Direcció de cada entitat estigui disposada a acceptar.

D'altra banda, i en relació al Reglament de protecció d'infraestructures crítiques, l'avaluació de la protecció de les infraestructures crítiques que la Comissió Europea va dur a terme i que va donar lloc a la proposta de la Comissió Europea COM(2020) 829 final, relativa a la resiliència de les entitats crítiques, que integra el projecte de llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació del Principat d'Andorra, és totalment traslladable al nostre país i demostra una evolució en la naturalesa de les amenaces a les quals s'enfronten les infraestructures crítiques del Principat d'Andorra (ICs).

La Llei NIS-AD, assenyala la necessitat de dedicar a les entitats crítiques una atenció especial en l'àmbit de la seguretat de la informació, per tenir la peculiaritat d'utilitzar infraestructures necessàries per a la prestació de serveis essencials per al Principat d'Andorra i que no es poden redundar o reemplaçar per una altra en cas de mal funcionament.

El Decret del Reglament d'Infraestructures Crítiques del Principat d'Andorra (en endavant, "RIC-AD") d'acord amb la Llei NIS-AD, establirà que s'ha d'exigir a les entitats crítiques i a les equivalents a entitats crítiques: el reforç de la seva resiliència.

12. En la tercera iniciativa de l'Estratègia de Ciberseguretat d'Andorra es preveu la creació d'un "Registre d'amenaces i atacs en context andorrà i àmbit europeu". Qui crearà aquest registre i com es desenvoluparà? Qui es preveu que hi pugui tenir accés?

Des d'un enfocament més estratègic, dins de la missió i diferents funcions que té encomanades l'Agència de Ciberseguretat d'Andorra, dins el decret de la seva creació, en l'article 5, de *Funcions de l'ANC-AD,* al punt número 5 es recull:

> "[...]
>
> 5. Impulsar i aprovar un marc de directrius i normes tècniques de seguretat per a les entitats que proveeixen serveis essencials o serveis importants, per tal d'oferir directrius per assolir una protecció eficaç davant les **ciberamenaces**.
>
> [...]"

Per altra banda, i des d'un pla més operatiu, dins de la missió i els objectius designats per al CSIRT-AD o Equip de Resposta per al Tractament d'Incidents de Seguretat de la Informació, s'especifica el següent articulat dins el decret de creació, en l'article 12, de *Missió i objectius del CSIRT-AD,* al punt número 4:

> "[...]
>
> 4. Així mateix, entre d'altres objectius del CSIRT-AD a assolir s'hi inclouen, a títol enunciatiu i no limitatiu:
>
> a. Centralitzar la coordinació proactiva de la prevenció i la mitigació de les **amenaces** de seguretat en les xarxes i els sistemes d'informació que representin un major risc per al Principat d'Andorra.
>
> b. Operar un equip d'intervenció altament especialitzat i capaç de fer-se càrrec de la prevenció de tot tipus d'incidents de seguretat en les xarxes i els sistemes d'informació, i de determinar l'impacte, l'abast i la naturalesa dels diferents incidents.
>
> c. Difondre informació sobre riscos, **amenaces**, vulnerabilitats, atacs, així com establir les corresponents estratègies de mitigació a través d'alertes, avisos, pàgines web o altres publicacions tècniques.
>
> [...]"

La protecció de les infraestructures crítiques es pot aconseguir amb mesures globals, però es millorarà molt la resposta si es té un coneixement de les principals amenaces. Això permet una millor orientació de les mesures de resposta i un millor cribratge de les amenaces.

Així doncs, considerant que cal una anàlisi de les amenaces i dels atacs per poder aconseguir una millor resposta, serà l'Agència de Ciberseguretat d'Andorra qui garanteixi l'existència d'aquest registre d'amenaces i atacs, i el CSIRT-AD serà qui el gestioni, mantingui i enriqueixi dins de les seves activitats . Addicionalment també serà l'encarregat de difondre aquesta informació d'una forma agregada amb l'objectiu de conscienciar, sensibilitzar i facilitar accés a totes les parts interessades (ciutadania, empreses, sector públic o altres).

13. En la quarta iniciativa de l'Estratègia de Ciberseguretat d'Andorra s'estableix la "creació d'un Partenariat Públic-Privat" (PPP). Quin serà l'objecte d'aquest PPP i quines seran les seves funcions? Quins actors estan previstos que formin part d'aquest PPP? Tant el finançament, com el seu model de gestió, serà de lògica publicoprivada?

La col·laboració entre els sectors públic i privat ha de convertir-se en el catalitzador que contribueixi al desenvolupament d'un entorn de confiança en l'àmbit de la seguretat de les xarxes i dels sistemes d'informació, creant un marc de cooperació que permeti assolir, entre altres aspectes, objectius estratègics comuns en termes de ciberseguretat. La cooperació entre ambdós sectors ha de facilitar l'intercanvi d'informació relacionada amb les noves amenaces al ciberespai i solucions per mitigar-les, així com promoure l'intercanvi de coneixement, la identificació de sinergies i accions que aportin eficiència i economia d'escala en la resolució dels ciberincidents.

Per reforçar aquesta necessitat i d'acord amb el que està especificat dins el Decret de creació de l'Agència Nacional de Ciberseguretat (ANC-AD) i de l'Equip de Resposta per al Tractament d'Incidents de Seguretat de la Informació (CSIRT-AD), en l'article 15, de *Col·laboració externa*, es recull la possibilitat d'establir acords de col·laboració amb qualsevol persona jurídica, pública o privada, quan els objectius i les activitats d'aquesta última siguin d'interès per a les polítiques de ciberseguretat i per al desenvolupament de les funcions de l'ANC-AD i del CSIRT-AD en general.

Cal afegir que totes aquestes activitats han d'afavorir l'atracció i retenció del talent en l'àmbit de coneixement de la ciberseguretat, fomentant el creixement del teixit empresarial nacional andorrà, gràcies als possibles acords amb centres experts de referència, universitats, escoles de negoci o altres, en el marc d'aquesta temàtica.

14. En la novena iniciativa s'estableix la cooperació internacional amb participació en fòrums i grups de treball europeus. Amb quins nous grups internacionals es preveu col·laborar?

Atès que el Principat (o qualsevol altre país) de forma individual no pot encarar les amenaces en el ciberespai, degut al fet que són tan globals, sense una col·laboració internacional, se segueix una bona pràctica més que necessària que consisteix a establir una estreta cooperació amb altres entitats i estats dins l'àmbit de coneixement de la ciberseguretat.

A fi de desenvolupar i millorar de forma contínua les capacitats de resposta del Principat d'Andorra en matèria de ciberseguretat, és necessària la creació de vincles permanents amb autoritats competents d'estats membres de la Unió Europea o d'altres països.

Algunes grups de treball i fòrums internacionals amb els quins té sentit establir relacions o col·laboracions son a títol enunciatiu i no limitatiu) els següents:

• **ENISA.-** Centre de coneixements especialitzats per a la seguretat cibernètica a Europa. Ofereix solucions i assessorament pràctic al sector públic i privat dels països de la UE i a les institucions europees.

• **INCIBE.-** L'INCIBE és el centre de resposta a incidents de seguretat de referència per als ciutadans i entitats de dret privat d'Espanya i que opera sota l'Institut Nacional de Ciberseguretat.

• **Agència de Ciberseguretat de Catalunya.-** L'Agència és l'encarregada d'establir el servei públic de ciberseguretat i treballa per garantir i augmentar el nivell de seguretat de les xarxes i els sistemes d'informació a Catalunya, així com la confiança digital dels ciutadans.

• **esCERT-UPC (Equip de Seguretat per a la Coordinació d'Emergències en Xarxes Telemàtiques).-** Fundat com el primer centre espanyol dedicat a assessorar, prevenir i resoldre incidències de seguretat en entorns telemàtics.

• **FIRST (Fòrum per a Equips de Resposta a Incidents i Seguretat).-** Es tracta d'una de les primeres organitzacions globalment reconeguda en resposta a incidents. El seu principal objectiu és promoure la cooperació i coordinació en la prevenció d'incidents, així com compartir informació entre els seus membres i la Comunitat en el seu conjunt. A través dels seus membres de ple dret, FIRST constitueix una "xarxa de confiança" per a la resposta a incidents globals.

• **Trusted Introducer for CSIRT in Europe.-** Grup de treball creat per TERENA que promou la col·laboració entre CSIRT a nivell Europeu. El seu principal objectiu és proporcionar un fòrum (TF-CSIRT) on els seus membres puguin intercanviar experiències i coneixements en un entorn de confiança.

• **CERT-FR.-** Centre governamental de vigilància, alerta i resposta als atacs informàtics de França. Compta amb InterCERT-FR, que reuneix un conjunt d'organitzacions amb activitats d'IRT (Incident Response Team) al territori francès.

Amb referència al Decret 346/2021, del 20 d'octubre del 2021, de creació de l'Agència Nacional de Ciberseguretat (ANC-AD) i de l'Equip de Resposta de Referència del Principat d'Andorra per al tractament d'incidents de seguretat de les xarxes i els sistemes d'informació (CSIRT-AD):

Es demana:

15. Per què s'ha decidit crear l'Agència Nacional de Ciberseguretat mitjançant Decret i no mitjançant un projecte de llei, com sí que s'ha previst per altres agències de l'ordenament jurídic del Principat d'Andorra?

Després d'analitzar els precedents existents al Principat d'Andorra relatius a agències, oficines, departaments o comissions que han existit o existeixen, sense personalitat jurídica pròpia i dependents directament i jeràrquicament bé del cap de Govern, bé de ministeris, que s'han creat via Decret, es va considerar que l'opció de creació, via decret, de l'Agència Nacional de Ciberseguretat i de l'Equip de Resposta de Referència del Principat d'Andorra per al tractament d'incidents de seguretat de les xarxes i els sistemes d'informació és una forma vàlida.

El projecte de llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació, entrat a tramitació parlamentària, en la disposició addicional encomana al Govern que "en

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

16. El Decret 346/2021 defineix en la lletra i. de l'article 1 la seguretat de les xarxes i els sistemes d'informació, com "la capacitat de resistència de les xarxes i els sistemes d'informació davant de qualsevol acció que comprometi la disponibilitat, l'autenticitat, la integritat o la confidencialitat de les dades emmagatzemades, transmeses o tractades, o els serveis corresponents oferts per aquestes xarxes i sistemes d'informació o accessibles a través seu". Així mateix, en la lletra j. de l'article 1 s'estableix que s'entén per serveis essencials i importants aquells "serveis que resulten necessaris per al manteniment de les funcions socials bàsiques, la salut, la seguretat, el benestar social i econòmic dels ciutadans, o el funcionament eficaç de les entitats de l'Administració pública, que es proveeixin mitjançant xarxes i sistemes d'informació, i que es poden veure greument afectats en supòsits de ciberincidents i, en conseqüència, ocasionar un greu perjudici social i econòmic al Principat d'Andorra". En quin estat es troba actualment la seguretat de les xarxes i sistemes d'informació del sector públic i del sector privat d'Andorra?

La seguretat de les xarxes i els sistemes d'informació es troba en constant desenvolupament i millora; respecte al sector públic, no existeix un barem únic que permeti qualificar l'estat de la seguretat de la informació i de les xarxes. Justament una de les funcions de l'ANC-AD és obtenir visibilitat de l'estat de la seguretat informàtica a escala global d'Andorra. Val a dir que totes les entitats públiques i administracions públiques han fet passes en el sentit de garantir la seguretat dels seus serveis i dades, però les amenaces són canviants i cal una adaptació constant per respondre de forma coordinada a l'evolució dels riscos que cada entitat, pública o privada, ha d'afrontar.

Com a punt de referència inicial es disposa de la classificació efectuada pel GCI - Global Cybersecurity Index (Índex Global de Ciberseguretat)-, indicador que mesura el nivell d'acompliment dels països en termes de ciberseguretat gestionat per la ITU (Unió Internacional de Telecomunicacions), i en el que, l'any 2020, Andorra ocupava la posició 44 dins el rànquing europeu. El rànquing era encapçalat per Regne Unit, Estònia i Espanya en aquest mateix ordre. Cal tenir en compte, però, que aquesta classificació s'estableix en base a qüestionaris efectuats als diferents països.

17. L'article 4.3.i) del Decret 346/2021 preveu que l'ANC-AD sigui "el nexe d'interlocució del Govern amb altres estaments representatius de ciberseguretat nacionals i internacionals." I l'article 5.8 del Decret citat preveu que una de les funcions de l'ANC-AD sigui la de "coordinar la gestió de les crisis amb el Comitè Especialitzat de Ciberseguretat, el Cos de Policia, l'Agència de Protecció de Dades (APDA) i el CSIRT-AD". Com s'estructurarà el protocol d'actuació i resposta conjunta

amb el Grup de Delictes Tecnològics del Cos de Policia d'Andorra i l'APDA, en cas de produir-se incidents de seguretat de les xarxes i els sistemes d'informació?

És responsabilitat dels òrgans de gestió de l'ANC-AD establir els reglaments, procediments i protocols específics d'actuació entre actors rellevants (com ara el Grup de Delictes Tecnològics del Cos de Policia d'Andorra i l'APDA) en cas de produir-se incidents de seguretat de les xarxes i els sistemes d'informació. Amb el benentès que encara es troben en procés de concreció els membres de les diferents comissions i comitès directament vinculats a l'activitat regular de l'ANC-AD; en data d'avui es troben encara pendents de definició els protocols concrets, aspecte que abordarà l'ANC-AD tan bon punt comenci a operar.

18. L'article 7.1 del Decret 346/2021 preveu que la composició de la Comissió de Seguiment de l'ANC-AD sigui "de cinc membres designats en qualitat de representants dels ministeris encarregats d'economia, interior, afers exteriors i gabinet jurídic del Govern i de responsable de l'ANC-AD". Quins són els membres previstos pel Govern per compondre aquesta comissió?

D'acord amb la voluntat que existeixi un òrgan que acompanyi i contribueixi a l'adequat funcionament de l'ANC-AD en el desenvolupament de la seva activitat, i d'acord amb el que especifica el mateix Decret en l'article 8è, els membres de la Comissió seran designats pels ministres responsables dels ministeris afectats, això és, els ministeris encarregats d'economia, interior, afers exteriors i gabinet jurídic del Govern, i de responsable de l'ANC-AD. En aquest sentit, cada ministeri concernit està avaluant la persona més adequada per a aquesta funció.

19. L'article 10.1 del Decret 346/2021 preveu que el Comitè Especialitzat de Ciberseguretat estigui compost per: "a) Experts del Govern, inclòs el Cos de Policia, i d'altres administracions públiques com ara els comuns; b) Representants del sector privat.; c) Representants de les entitats de serveis essencials i de serveis importants; d) Altres representants la intervenció dels quals l'ANC-AD o el ministeri encarregat de la presidència consideri necessària, en funció de les circumstàncies". A quins perfils de "representants del sector privat" es refereix l'apartat b)? A quins perfils de representants de les "entitats de serveis essencials i de serveis importants" es refereix l'apartat c)? A quins perfils de representants es refereix l'apartat d)? Quins criteris objectius justificaran l'entrada d'un membre al Comitè Especialitzat de Ciberseguretat?

En relació amb els participants de cada col·lectiu referenciat a l'enunciat de la pregunta, i únicament a títol enunciatiu, no limitatiu ni vinculant, els participants podrien ser els següents:

- Sector privat

º Entitats privades relacionades amb el món de la ciberseguretat la participació de les quals pugui ser rellevant o determinant a l'efecte d'acomplir les principals funcions del Comitè Especialitat, i derivada per tant també de l'ANC-AD. Per exemple, dins d'aquesta agrupació es podrien trobar els ens privats en disposició de donar suport a la presa de decisions en matèria de ciberseguretat mitjançant l'anàlisi i estudi de propostes d'iniciatives tant en

l'àmbit nacional com en l'internacional, o bé puguin contribuir a l'elaboració de propostes normatives en matèria de ciberseguretat per ser considerades.

- Entitats de serveis essencials i de serveis importants

º S'entén per *servei essencial o important* el servei ofert per una entitat la tipologia del qual s'emmarca en la de les entitats necessàries per al manteniment de les funcions socials bàsiques, la salut, la seguretat, el benestar social i econòmic dels ciutadans, o el funcionament eficaç de les institucions de l'estat i les administracions públiques. Sectors d'activitat entesesos com a essencials son l'energètic, el transport, els mercats financers o el d'infraestructures digitals. Dit això, qualsevol entitat enmarcada dins d'aquests àmbits d'activitat en podria ser un exemple. Per la seva banda, dins els sectors d'activitat entesos com a importants podríem trobar la gestió de residus, correus i missatgeria o proveïdors de serveis digitals.

- Altres representants

º Es tracta d'un apartat de participació que deixa oberta la participació de qualevol entitat que es condieri escaient d'acord amb el criteri de l'ANC-AD, això és, en funció de les circumstàncies, fase o etapa evolutiva de l'ANC-AD o bé d'altres necessitats emergents.

Finalment, en relació amb els criteris objectius que justificaran l'entrada d'un membre al Comitè Especialitzat de Seguretat, aquests seran aquells que contribueixin de forma evident a l'acompliment de les funcions de l'ANC-AD, reforçant si cap en matèria de ciberseguretat aquelles relacions de coordinació, col·laboració i cooperació entre les administracions públiques i el sectors privat, així com aportar informació rellevant per facilitar la presa de decisions estratègiques al mateix Govern dins l'àmbit de seguretat de les xarxes i dels sistemes d'informació. Els membres del Comitè especialitzat han de comptar amb una àmplia experiència en algun dels dominis de la ciberseguretat.

20. El Decret 346/2021 preveu, en l'article 10.4, que el Comitè Especialitzat de Ciberseguretat "es reuneix a iniciativa del seu president com a mínim amb caràcter bimestral o tantes vegades com el president ho consideri necessari ateses les circumstàncies que afecten la ciberseguretat del Principat d'Andorra", però no precisa qui serà el president del comitè. A més a més, l'article 10.5 del mateix Decret estableix que "el detall del règim de funcionament del Comitè s'estableix mitjançant reglament intern". En canvi, pel que fa a la presidència de la Comissió de Seguiment, l'article 9.1 estableix que "la Comissió està presidida pel responsable de l'ANC-AD o per la persona en què delegui". Per què, en el cas del Comitè Especialitzat en Ciberseguretat, no s'ha precisat qui presidirà aquest comitè mitjançant el Decret 346/2021?

A diferència de de la Comissió de Seguiment de l'ANC-AD, el Comitè Especialitzat és un òrgan col·legiat consultiu que té entre altres finalitats donar suport a la presa de decisions a l'ANC-AD sobre qüestions o necessitats que es puguin donar en matèria de ciberseguretat. En aquest sentit i d'acord amb el que s'especifica al Decret 346/2021, serà mitjançant reglament intern com es procedirà a la designació del seu president, amb el benentès que, en funció de la composició final del dit Comitè, segons el moment i les circumstàncies serà més adient la designació de l'ens o persona que presideixi el dit Comitè, així com la rotació del càrrec i la seva temporalitat.

Per contra, la Comissió de Seguiment de l'ANC-AD és l'òrgan que supervisa, gestiona i governa l'Agència en el sentit més ampli, raó per la qual es considera necessari que el rol o funció de la presidència estigui designat de forma predeterminada, i que a més recaigui particularment sobre el responsable de l'ANC-AD o en la persona en què delegui.

Amb referència al Projecte de llei del pressupost per a l'exercici del 2022:

Es demana:

21. L'article 3.1. del Decret 346/2021 preveu que l'ANC-AD "s'estructura jeràrquicament segons les necessitats organitzatives actuals i les resultants de l'evolució en l'acompliment o el desplegament de les seves funcions" i l'article 14 del mateix decret estableix que el CSIRT-AD "s'estructura jeràrquicament segons les necessitats organitzatives actuals i les resultants de l'evolució en l'acompliment o el desplegament de les seves funcions d'acord amb les directrius de l'ANC-AD". Així mateix, la disposició addicional del citat decret estableix que "es faculta el Ministeri de Finances per fer les adaptacions pressupostàries necessàries per acomplir el que s'estableix en aquest Decret". Quins recursos (materials i humans) preveu el Projecte de llei del pressupost per l'any 2022 per al desenvolupament d'ambdues estructures organitzatives?

Dins d'un marc temporal acotat i entès com de consolidació, l'Agència requerirà una estructura mínima de recursos materials i humans que li permetin donar inici a la seva base de funcionament i activitat.

En termes temporals, aquesta fase d'inici de l'activitat i consolidació dels serveis està planificada dins dels dos primers exercicis pressupostaris, i per als quals s'han estimat preliminarment uns costos generals associats que se situarien al voltant dels 400.000 € per exercici.

Les valoracions econòmiques inclouen tant partides satisfer les necessitats estructurals del mateix funcionament de l'Agència (instal·lacions, infraestructura de xarxa, serveis TIC o d'altres de naturalesa similar), com partides per donar cobertura als serveis que l'Agència preveu oferir en aquesta fase inicial. En relació amb la primera agrupació de necessitats econòmiques, s'ha previst una dotació de 150.000 € anuals, mentre pel que fa a la cobertura dels serveis que s'han d'oferir, s'estimen uns 250.00 € per exercici, dins dels quals quedaria inclosa l'operació.

Durant aquesta primera fase de consolidació –2 exercicis– el finançament de l'Agència es farà a través dels recursos de la Fundació Andorra Recerca i Innovació, i més concretament del pressupost d'Andorra Digital.

Posteriorment, una vegada superada aquesta fase inicial de llançament i consolidació de serveis, es requerirà avaluar noves necessitats en funció, entre altres coses, de l'evolució de l'estratègia nacional de ciberseguretat, i de totes les consideracions emergents pròpiament dins l'àmbit de la ciberseguretat. Per tant, dins d'aquest nou cicle s'identificaran, avaluaran i concretaran noves iniciatives que hauran de complementar les activitats en curs.

Així mateix, les dotacions econòmiques hauran de ser ajustades i convenientment introduïdes als pressupostos generals de l'Estat, assignant els mitjans necessaris per garantir-ne la viabilitat i execució, així com per avalar la continuïtat global de les funcions, finalitats i activitats de l'Agència de Ciberseguretat en el temps.

22. Quins dels recursos previstos al Projecte de llei del pressupost per a l'exercici del 2022 per al Departament de Sistemes d'Informació (960), del Ministeri d'Administracions Públiques i Participació Ciutadana (95), van destinats al desenvolupament de l'ANC-AD i el CSIRT-AD?

El pressupost per a l'Agència Nacional de Ciberseguretat serà finançat íntegrament per als seus dos primers exercicis d'acord amb l'exposició de la pregunta anterior, i per tant no es preveu destinar partides específiques ni del Departament de Sistemes d'Informació ni del Ministeri d'Administració Públiques i Participació Ciutadana de forma directa per a l'ANC-AD. No obstant aquesta consideració, no queda descartat que, atenent les possibles sinergies existents entre els departaments i ministeris referenciats i l'ANC-AD, puguin establir-se certes col·laboracions o cooperacions en matèria de ciberseguretat.

23. A on s'esmenta el desenvolupament de l'ANC-AD dins del programa "04.1.1.04" de Digitalització de l'Administració (que inclou el projecte "IN0071-Transformació Digital d'Andorra") del Projecte de llei del pressupost per a l'exercici del 2022? I dins del Departament de la Secretaria d'Estat de Transformació Digital i Projectes Estratègics (145) del Cap de Govern (10)?

Tal com s'ha exposat durant l'argumentació de les respostes als requeriments escrits 21 i 22 sobre els mecanismes de finançament de l'ANC-AD, sempre ha estat voluntat donar cobertura a les necessitats resultants quant a recursos econòmics i humans de l'Agència, mitjançant els pressupostos de la Fundació Andorra Recerca i Innovació, particularment des de la seva branca d'Andorra Digital fins a la consolidació del projecte.

24. Amb quants recursos preveu dotar el Projecte de llei del pressupost per a l'exercici del 2022 al Grup de Delictes Tecnològics del Departament de Policia (420) del Ministeri de Justícia i Interior (40)? Quin és el percentatge comparatiu d'aquests recursos previstos al Projecte de llei del pressupost per a l'exercici del 2022, respecte als previstos a la Llei 18/2020, del 17 de desembre, del pressupost per a l'exercici del 2021?

El Projecte de llei del pressupost per a l'exercici del 2022 preveu els recursos següents per al Grup de Delictes Tecnològics de l'Àrea de Policia Judicial i Investigació Criminal:

a) Despeses de funcionament: manteniment del laboratori d'informàtica forense: 32.000,00 €, 2,40% més que el previst per a l'any 2021 en aquest concepte.

b) Despeses d'inversió: adquisició de dos monitors de 55" : 1.200,00 €, mateixa quantitat que la prevista per a l'any 2021.

En relació amb els recursos humans, a partir d'aquest mes de desembre s'han adscrit definitivament dos nous funcionaris de policia, els quals es troben en espera de rebre durant l'any 2022 les formacions i el material específic.

Així mateix, durant l'any 2022 es faran les formacions inicials, continuades i específiques, que s'aniran ajustant en funció de la dotació pressupostada aprovada per a formació del Cos de Policia, condicionades a les ofertes formatives dels cossos policials o d'empreses privades.

Andorra la Vella, 17 de gener del 2022

César Marquina Pérez de la Cruz
Secretari d'Estat de Transició Digital i Projectes Estratègics

Carrer de la Vall, 9-13 – AD500 Andorra la Vella – Principat d'Andorra – Tel. (376) 877877 – www.consellgeneral.ad

Dipòsit legal: AND.282-2021