Estratègia nacional de ciberseguretat del Principat d'Andorra 2024-2027

Seguretat de les xarxes i dels sistemes d'informació

Índex

Pròleg

La irrupció de la digitalització en la societat està generant, en termes generals, un canvi de paradigma irreversible respecte a com enteníem fins ara moltes de les pautes quotidianes de relació i interacció existents. Està introduint, sens dubte, una afectació transversal de les maneres de fer en àmbits tan diversos com el cultural, el social, l'econòmic o d'altres.

La consolidació de totes aquestes noves formes de relació i interacció en el nostre dia a dia ha estat possible gràcies a factors com l'evolució ràpida de les noves tecnologies, la proliferació de nous serveis digitals, o l'optimització de les infraestructures que garanteixen la interconnexió de les xarxes. Factors com els referenciats han de ser clarament interpretats com a elements habilitadors del canvi i han de fomentar-ne, si és possible, l'acceleració i l'expansió. Addicionalment no hi ha opció a fer un pas enrere, ni tan sols a plantejar-se un possible estancament evolutiu atenent el ràpid procés de transformació en què estem immersos. Negocis, comunicacions, transport, serveis financers, Administració o la societat en general se sostenen amb algun d'aquests elements i els utilitzen cada dia més com a palanca d'activació. Sembla evident, doncs, que s'ha generat una dependència alta –no únicament evolutiva, sinó també de funcionament– cap a aquest tipus de serveis o components estructurals. Aquest fet comporta consegüentment que la protecció dels serveis i les infraestructures associades que els possibiliten s'hagin convertit en un factor alt de risc.

A la llum del que s'ha exposat, doncs, l'accessibilitat i la utilització d'aquests actius esdevé crítica i, per tant, protegir-los i salvaguardar-los es converteix en objecte d'interès nacional. De fet, la necessitat des d'un entorn segur i estable no té un abast o un impacte únicament local, sinó al contrari. Molts estats treballen per mitigar les possibles amenaces que pot suposar una disfunció o bloqueig d'aquests serveis en la mesura que poden ocasionar importants impactes a l'economia, afectar l'operativitat diària o senzillament posar en qüestió la reputació d'un país.

En el context d'Andorra, com en el context global, també esdevé rellevant tenir en consideració tots aquests canvis profunds en els models i formes de fer. De fet, ja s'està treballant activament en la creació d'un ecosistema digital que promogui i faciliti noves fórmules d'interacció, que permeti introduir una agilitat i una eficiència més grans, que potenciï l'autogestió i, en definitiva, que introdueixi nous formats de relació entre els organismes, les empreses i les persones. Aquest ecosistema s'està construint amb una orientació plena cap a les persones i la societat en general. Per tant, és clau que se'n respecti la seguretat, la privacitat i les llibertats. La interconnexió i la interoperabilitat, així com la transparència d'informació, han d'esdevenir factors clau d'èxit per tal de garantir una societat innovadora, competitiva, però també protegida sota un marc de funcionament segur i estable que minimitzi qualsevol vulnerabilitat o exposició externa i asseguri les llibertats fonamentals. A més, aquesta aproximació ha d'estar absolutament alineada amb les millors pràctiques i recomanacions internacionals, i al mateix temps s'ha de convertir en un avantatge competitiu en el nostre apropament a la Unió Europea.

Cada cop són més els delinqüents professionals que se centren en l'espionatge econòmic i polític digital i en la preparació per al sabotatge digital. També augmenta el nombre de països que desenvolupen capacitats d'atac digital i aquests atacs que es duen a terme són cada cop més complexos.

Aquests fets exigeixen un afany per reforçar la ciberseguretat i així protegir millor els interessos vitals d'Andorra. L'Estratègia nacional de ciberseguretat estableix el marc que cal seguir per a la ciberseguretat. L'Estratègia defineix la posició d'Andorra fixant els principis, les estratègies i les iniciatives per fer front a la vulnerabilitat del ciberespai.

Marc Rossell i Soler
Secretari d´estat de Transformació digital i Telecomunicacions

Resum executiu

Prenent com a objectiu la digitalització del país, per tal de garantir un marc regulador i una infraestructura tecnològica, el Principat d'Andorra, des del 2020, ha definit i ha posat en marxa l'Estratègia nacional de digitalització del 2030. La finalitat d'aquesta Estratègia no només se centra en l'aspecte digital, sinó també en una millora en la qualitat de vida dels ciutadans.

El Govern aposta per un abordatge transversal, mitjançant el Programa de transformació digital, en el qual s'estableixen objectius precisos i comuns en tot el país i en el qual la ciberseguretat és un pilar fonamental per a aquest abordatge. Aquest desenvolupament s'ha començat a executar a través de la implementació de diverses iniciatives durant el període 2021-2024. Així mateix, aquesta Revisió estratègica ha estat actualitzada amb el Programa per al període del 2024 al 2027, i ha fet d'aquesta iniciativa un projecte ambiciós que representa un pas significatiu cap a una societat més connectada, que s'orienta al desenvolupament de les capacitats ja existents del país i que impulsa els canvis que sorgeixen dins del context global i europeu, en el qual el Principat d'Andorra es mou.

En aquest context de digitalització transversal és clau assegurar la seguretat de tots els sistemes. La seguretat de les xarxes i dels sistemes d'informació –i, més generalment, la ciberseguretat– permetrà garantir els principis de disponibilitat, integritat i confidencialitat de la informació durant el seu cicle de vida.

Aquesta Estratègia cerca donar continuïtat a l'entorn digital segur al Principat d'Andorra, considerant iniciatives per a la protecció de les infraestructures crítiques, dels operadors de serveis essencials i dels proveïdors de serveis digitals, ja que la destrucció o interrupció d'aquestes infraestructures generaria greus conseqüències a algunes funcions vitals de la societat.

Andorra ha d'afrontar el repte que suposa abordar la segona part del Programa de transformació digital, la Revisió estratègica 2024-2027, aprovada pel Govern. Aquest programa s'ha centrat en quatre àmbits o línies estratègiques: les administracions públiques, l'empresa, les infraestructures tecnològiques, i la ciutadania i els seus drets digitals. El Govern dona suport a aquest marc de referència com a eina per donar cobertura a aquestes línies estratègiques, fet que permetrà una organització clara i una distribució eficient dels recursos i reforços.

El caràcter transversal i interconnectat de les TIC, que també defineix les seves amenaces i riscos, limita l'eficàcia de les mesures que s'utilitzen per contrarestar-los quan es prenen de manera aïllada. Aquest caràcter transversal també fa que es corri el risc de perdre efectivitat si els requisits en matèria de seguretat de la informació es defineixen de manera independent per a cadascun dels àmbits sectorials afectats.

Per tant, és oportú establir mecanismes que, amb una perspectiva integral, permetin millorar la protecció davant de les amenaces que afecten les xarxes i els sistemes d'informació, i facilitar la coordinació de les actuacions dutes a terme en aquesta matèria tant en l'àmbit nacional com amb els països del nostre entorn i, en particular, dins de la Unió Europea.

Malgrat que les iniciatives de seguretat de les xarxes i dels sistemes de la informació s'han anat desenvolupant internament en organismes estatals i privats i hi ha hagut iniciatives dutes a terme per diverses autoritats en el passat, aquest és el primer enfocament organitzat per donar una resposta coordinada a les amenaces que es manifesten al ciberespai. L'Estratègia nacional de ciberseguretat permetrà continuar treballant sobre les infraestructures i operadors crítics, evolucionant el marc legal que afavoreixi un Pla nacional de contingència per a infraestructures crítiques, reorganitzant les estructures existents i afavorint la col·laboració entre els sectors públic i el privat. La realització d'exercicis de simulació nacionals i internacionals ha de permetre el desenvolupament de les capacitats de les infraestructures crítiques identificades, i augmentar la resposta a incidents.

Aquest document analitza les iniciatives que s'han de dur a terme en una primera fase i els passos següents que s'han de seguir, la planificació, la priorització i planificació de la ciberseguretat nacional i l'avaluació dels resultats de les iniciatives d'estratègia. L'Estratègia nacional de ciberseguretat s'haurà de revisar periòdicament, tenint en compte els resultats del procés d'avaluació, així com les noves amenaces que apareguin (i continuaran apareixent) al ciberespai. Els objectius són fer una avaluació integral dels resultats de les iniciatives anteriors i actualitzar l'Estratègia perquè continuï en condicions de proporcionar el màxim benefici a la societat andorrana.

1. Introducció

1.1. La seguretat de les xarxes i dels sistemes d'informació

L'evolució de les TIC, especialment amb el desenvolupament d'Internet, ha fet que les xarxes i els sistemes d'informació tinguin actualment un paper crucial en la nostra societat, i la seva fiabilitat i seguretat són aspectes essencials per a la pràctica normal de les activitats econòmiques i socials.

Tot sistema bàsic de seguretat ha de cobrir la disponibilitat, la integritat i la confidencialitat de les infraestructures i dels sistemes d'informació i augmentar la resiliència contra amenaces i disfuncionaments que puguin afectar els seus components. S'han de prendre mesures que permetin incrementar els mecanismes de prevenció, d'identificació i de resposta a riscos potencials, així com preparar plans de mitigació i de recuperació de la disponibilitat dels serveis cobrint les situacions d'emergència o de crisi.

La seguretat de les xarxes i dels sistemes d'informació s'aplica a la preservació dels principis de disponibilitat (és a dir, que un sistema pugui proporcionar servei o informació quan se sol·liciti), integritat (és a dir, la protecció de la informació contra qualsevol modificació o destrucció no desitjada) i confidencialitat (és a dir, que un sistema pugui proporcionar servei o informació quan se sol·liciti.). La ciberseguretat fa referència a la seguretat dels sistemes connectats, així com al seu ús segur per part dels usuaris finals.

La ciberseguretat està vinculada directament amb la seguretat nacional. Com a resultat de la digitalització, els interessos de seguretat nacional són vulnerables als atacs digitals i només es pot concebre en cooperació amb la comunitat empresarial i els organismes públics. La ciberseguretat ha de formar part dels processos quotidians de tota organització i, per tant, la cooperació publicoprivada constitueix la base de l'enfocament andorrà de la ciberseguretat. Els ciutadans, les empreses i els governs han de poder confiar en els mitjans de comunicació a través dels quals es transmeten dades importants. L'enfocament de la ciberseguretat ha de tenir en compte la dimensió internacional de les dades, les connexions, el govern d'Internet i els actors que duen a terme atacs digitals. Un espai digital més segur és, per tant, una de les prioritats d'Andorra.

El Govern representa els interessos públics i una Andorra digital segura, que reconegui amenaces a interessos vitals, i així reforci la seva resiliència. Es recomana a la comunitat empresarial i als ciutadans que assumeixin les seves pròpies responsabilitats en matèria de seguretat. A més, el Govern, com a organisme públic, està obligat a tenir la ciberseguretat dels seus propis processos per tal de donar un bon exemple com a iniciador.

Per obtenir les condicions necessàries de confiança en l'ús dels canals telemàtics desenvolupats pel Govern i altres organitzacions és necessari que el nivell de seguretat sigui elevat. Aquesta confiança en els sistemes i la garantia de transaccions segures al ciberespai contribuiran en gran mesura al desenvolupament econòmic del Principat d'Andorra i a l'assoliment dels objectius del Programa de transformació digital.

1.2. Infraestructures crítiques

Molts dels serveis que fan servir els ciutadans i les empreses es recolzen fortament en les infraestructures d'informació. En aquest marc, la dependència que les societats tenen d'aquest sistema d'infraestructures complex que dona suport al desenvolupament normal dels sectors productius, de gestió i de la vida ciutadana en general és cada cop més gran. El fet que aquestes infraestructures siguin altament interdependents entre si propicia que els problemes de seguretat es desencadenin en cascada a través del mateix sistema i ocasionin interrupcions del servei inesperades i cada vegada més greus en els serveis bàsics per a la població.

Fins a tal punt és així que qualsevol interrupció no volguda –fins i tot de curta durada i deguda a causes naturals o tècniques, o bé a atacs deliberats– podria tenir conseqüències greus en els fluxos de subministraments vitals o en el funcionament dels serveis essencials, a més de provocar pertorbacions i disfuncions greus en matèria de seguretat.

Dins de les prioritats estratègiques de la ciberseguretat nacional hi ha les infraestructures crítiques i importants, que estan exposades a una sèrie d'amenaces. Per protegir-les es fa imprescindible continuar catalogant el conjunt de les que presten serveis essencials a la nostra societat i evolucionar els plans que continguin mesures de prevenció i protecció eficaces contra les possibles amenaces que podrien patir aquestes infraestructures, tant en el pla de la seguretat física com en el de la seguretat de les tecnologies de la informació i les comunicacions.

1.3. Visió

L'Estratègia nacional de ciberseguretat vol donar continuïtat a l'equilibri entre llibertat, seguretat i creixement econòmic de les TIC del Principat d'Andorra en benefici de tota la ciutadania basant-se en els principis rectors següents:

- Continuar amb el desenvolupament de noves estratègies i polítiques que afavoreixin la cooperació entre totes les autoritats competents, tenint en compte les seves competències.
- Tenir un enfocament holístic de la seguretat que permeti fer front a les amenaces en el ciberespai.
- Establir objectius ambiciosos perquè l'Estratègia i les seves iniciatives millorin de forma notable el nivell de la ciberseguretat.

1.4. Objectius

El desenvolupament d'aquesta Estratègia i les iniciatives identificades ha de permetre assolir els objectius següents:

1. Donar suport als objectius del Govern identificats en el programa Transformació digital d'Andorra 2.0, emmarcat dins l'Estratègia 2030, per desenvolupar les condicions per a una societat de la informació segura elaborant el marc legal necessari per protegir les infraestructures.
2. Coordinar de manera proactiva la prevenció i la mitigació de les amenaces de ciberseguretat i de telecomunicacions.
3. Afavorir la cooperació entre l'Estat i el sector privat.
4. Afavorir la cooperació internacional Estat-Estat o Estat-sector privat en matèria de ciberseguretat.
5. Buscar la consolidació de les accions anteriors i establir comeses futures.
6. Buscar generar un efecte multiplicador per arribar a més ciutadans i empreses en matèria ciberseguretat.

2. Context estratègic

Per tal de contextualitzar el progrés d'Andorra en la digitalització, des del 2020, s'observa: una millora en els resultats i la posició respecte a la resta de països a l'índex de referència europeu Digital Economy and Society Index; un augment significatiu del nombre de certificats digitals emesos; la creació de l'Agència Nacional de Ciberseguretat i l'equip de resposta a incidents, així com el consegüent compliment normatiu; l'execució de la implantació d'un bus d'interoperabilitat per garantir la interconnexió entre administracions i el llançament de la nova Seu electrònica com a canal de comunicació entre l'administrat i l'Administració; la definició d'un marc regulador en digitalització que comprèn més de 25 lleis i decrets, i el llançament de l'app Andorra Salut, que permet als ciutadans accedir al seu historial mèdic. En definitiva, l'assoliment d'aquestes fites assenta les bases per afrontar els reptes futurs del país.

Per tot això, s'entén que l'Estratègia nacional de transformació digital 2030 d'Andorra és una iniciativa enfocada a millorar el context global del país, amb el suport del Govern, i que segueix una visió estratègica cap a la digitalització. El seu objectiu és capacitar Andorra per afrontar els reptes que sorgeixen, no només en l'àmbit de la ciberseguretat, sinó també en el context global i europeu en què el país es desenvolupa.

2.1. Context normatiu del Principat d'Andorra

En els darrers tres anys, Andorra ha desenvolupat un marc legal sòlid per reforçar la ciberseguretat al país, i en destaquen tres normatives clau. En primer lloc, la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (NIS-AD), estableix les bases per garantir un nivell comú de ciberseguretat, alineant-se amb les directrius europees. Complementant aquesta Llei, el Decret 417/2022, del 12 d'octubre, aprova el Reglament de l'Esquema nacional de seguretat (ENS-AD), que fixa les directrius i els estàndards que han de seguir les entitats públiques i privades per protegir les seves infraestructures digitals. Finalment, el Reglament d'infraestructures crítiques del Principat d'Andorra (RIC-AD) defineix les mesures específiques per garantir la seguretat de les infraestructures i els serveis essencials per al funcionament del país.

Aquest conjunt normatiu representa un pas decisiu cap a la protecció integral de les xarxes i els sistemes d'informació d'Andorra davant les amenaces cibernètiques creixents.

També s'han format el CSIRT-AD (Equip de Resposta a Incidents de Seguretat Informàtica d'Andorra) i l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra)[1] com a organismes rellevants en l'àmbit de la ciberseguretat, encarregats de dur a terme les activitats que prèviament se'ls han assignat.

2.2. La seguretat de les xarxes i dels sistemes d'informació al Principat d'Andorra

El Govern, especialment, reconeix la ciberseguretat com un pilar essencial que permetrà garantir la disponibilitat, la integritat i la confidencialitat dels sistemes i les informacions del mateix Govern i de la resta d'organitzacions públiques i privades, així com de les infraestructures crítiques i de la ciutadania.

Les disposicions d'aquesta Estratègia nacional de ciberseguretat formen part del Programa de transformació digital d'Andorra 2.0 per al desenvolupament d'una societat de la informació i també permetran que el Principat contribueixi activament al procés de protecció de les infraestructures.

2.3. Les amenaces al ciberespai actual

El Principat d'Andorra és un dels països amb més dispositius connectats a Internet per habitant, i les noves tecnologies tenen un paper cada vegada més important en la nostra vida quotidiana. En són exemples el comerç electrònic i la comunicació digital amb el nostre metge, l'escola i els poders públics. A més, una digitalització de gran abast en la salut (història clínica compartida), la mobilitat (e-automòbil), el creixement de dispositius i electrodomèstics connectats a Internet (internet de les coses), tecnologies clau com el big data, el 5G i la intel·ligència artificial fan que la línia que separa el ciberespai del món físic sigui cada vegada més estreta.

La velocitat amb què aquests desenvolupaments tecnològics i socials s'han fet ha conduït a un augment de l'explotació de les vulnerabilitats del ciberespai, una tendència que s'espera que continuï en els anys vinents. Com que cada aspecte de la societat i del desenvolupament econòmic depèn, en major part, dels processos digitals, els atacs a les infraestructures que els suporten poden danyar directament la nostra economia i

[1] ANC-AD

amenaçar la seguretat nacional.

L'increment de la vulnerabilitat és evident i els organismes involucrats en la seguretat dels sistemes d'informació indiquen un augment preocupant de les amenaces digitals. A més, la resiliència es queda per darrere del desenvolupament de l'amenaça i aquesta situació requereix esforços addicionals per part de les autoritats públiques, la comunitat empresarial i els ciutadans per protegir els interessos del Principat i reforçar l'enfocament de la ciberseguretat en benefici de la seguretat nacional.

La digitalització ha impregnat tots els nivells de la societat i de l'economia; en conseqüència, la nostra societat s'ha tornat dependent dels recursos digitals. El funcionament sense interrupció dels recursos tecnològics és cada cop més essencial per als processos vitals de les empreses i del Govern, així com per a la vida quotidiana dels ciutadans. Els incidents dels darrers anys han deixat clar que els atacs digitals poden tenir un impacte important en la societat i poden provocar danys que amenacin la seguretat nacional. L'amenaça dels delinqüents professionals creix i continuarà creixent, ja que els models d'ingressos criminals amb èxit continuen desenvolupant-se i s'estan ampliant. L'escalabilitat gairebé sense cost dels atacs digitals és d'un gran interès per als delinqüents. Els consumidors ja no són les úniques víctimes; les administracions, els hospitals, les empreses i les institucions financeres també són objectius dels delinqüents. La ciberdelinqüència com a servei fa que els mètodes d'atac siguin cada cop més complexos i permeti a actors amb coneixements i recursos, en ocasions quasi il·limitats, poder dur a terme atacs que en alguns casos tenen un impacte social directe.

Exemple: ciberdelinqüènca com a servei *as a service*.

Els ciberdelinqüents no fan tots els passos d'un atac, compren serveis i experiència. Aquests serveis es proporcionen de manera molt professional i completa: des de recursos tècnics fins a la infraestructura i la funcionalitat del servei d'assistència.

2.4. Parts interessades

A banda del Programa de transformació digital d'Andorra, hi ha diverses autoritats i entitats del Principat que actuen en la seguretat de les xarxes, dels sistemes d'informació i dels serveis de tecnologia de la informació. Fan aportacions directes o indirectes en temes crítics de seguretat de la informació i tenen responsabilitats directes o indirectes en matèria de seguretat de les xarxes i dels sistemes d'informació.

Les parts interessades que participen en aquesta etapa són les següents:

- Andorra Digital
- Departament de Transformació Digital (DTD) del Govern
- Cos de Policia
- Andorra Telecom
- Autoritat Financera Andorrana (AFA)
- Agència de Protecció de Dades d'Andorra (APDA)

3. Full de ruta

Prèviament, es va establir una Revisió estratègica que era l'inici del Pla de transformació estratègica, en què la intenció era la formació i creació d'un marc en què s'iniciés el procés al qual està dirigit el Pla. Totes les iniciatives completes, desenvolupades o, posteriorment, identificades són fites que col·laboren en la transformació del país per avançar cap a la convergència amb l'estratègia europea i millorar el nivell de maduresa digital, amb la finalitat d'afrontar els reptes actuals i futurs, mantenint sempre l'esperit de situar l'administrat al centre de l'Administració, i que, amb el seu enfocament holístic, no només busquen la modernització tecnològica, sinó també millorar la qualitat de vida dels ciutadans, garantir la inclusió i l'accessibilitat digital, promoure la sostenibilitat i assegurar un entorn digital segur. Aquest Programa representa un compromís ferm d'Andorra per continuar apostant per la digitalització de la societat, fet que marca el camí cap a un futur més connectat, sostenible i inclusiu.

Aquest full de ruta, primer pas per a la implementació i el desplegament de la Revisió estratègica 2024-2027, s'implementarà a través de les accions oportunes (convenis, acords, aliances, etc.).

Durant la consecució dels objectius es duran a terme accions comunicatives per compartir els avenços del programa, les fites assolides, l'impacte sobre els administrats, la disponibilitat de nous serveis i la divulgació tecnològica i digital per a la ciutadania i les empreses en general. Així mateix, es té en compte el monitoratge del programa, ja que es farà un seguiment constant dels indicadors estratègics derivats dels objectius establerts per al 2030.

3.1. Objectiu 1. Desenvolupar les condicions per a una societat de la informació segura

Iniciativa 1: Millora contínua del marc legal existent

En el marc de la iniciativa de millora contínua del marc legal existent, a més de donar continuïtat al marc legal sòlid existent en matèria de ciberseguretat, es complementarà amb un marc normatiu específic que en faciliti l'adopció efectiva.

Prenent aquesta iniciativa, com a punt de partida, s'implementaran diverses modificacions en l'ENS-AD (Esquema nacional de seguretat d'Andorra) i el RIC-AD (Reglament d'infraestructures crítiques d'Andorra), amb l'objectiu d'augmentar la resiliència i ampliar la llista de serveis essencials, que va ser desenvolupada prèviament el 30 de novembre del 2022, i el desenvolupament de documents i guies associats a les modificacions. Aquestes modificacions i millores dels dos decrets anteriorment descrits s'aniran modificant durant la implementació d'aquests estratègia i augmentarà de forma progressiva el nivell de maduresa, i així s'aconseguirà un nivell de maduresa més elevat.

A més, el Govern impulsarà l'establiment d'un baròmetre de compliment per mesurar el grau d'adopció tant del marc normatiu com del marc legal al país. Aquest baròmetre permetrà avaluar el nivell de conformitat de les entitats públiques i privades amb la normativa vigent, identificant àrees de millora i proporcionant dades que facilitin una aplicació més àmplia i efectiva de les regulacions establertes. Aquest mecanisme contribuirà a un seguiment continu i estimularà una adopció generalitzada de les normatives, fet que enfortirà la seguretat de la societat de la informació.

Com a part complementària del marc legal existent, s'han elaborat diverses guies tècniques, estàndards i guies de bones pràctiques perquè proporcionin directrius concretes als organitzacions i els professionals del sector, per assegurar així que el marc legal és pugui implementar de manera pràctica i eficient.

3.2. Objectiu 2. Coordinar de manera proactiva la prevenció i la mitigació de les amenaces

Iniciativa 2: Seguiment de les interdependències existents per a la evolució de l'Estratègia

Per reforçar la coordinació en la prevenció i la mitigació de les amenaces cibernètiques, Andorra disposarà d'una plataforma de compartició d'informació sobre seguretat cibernètica similar al model de la Cyber Security Information Sharing Partnership (CISP) del Regne Unit.[2] Aquesta plataforma ha de permetre la col·laboració entre els sectors públic i privat del país, oferint un espai segur i confidencial per a l'intercanvi d'informació sobre

[2] Cyber Security Information Sharing Partnership - GOV.UK (www.gov.uk) i About CISP (ncsc.gov.uk)

amenaces i vulnerabilitats.

La plataforma andorrana facilitarà la comunicació i la cooperació entre professionals de la ciberseguretat, empreses i institucions, fet que millorarà la resposta col·lectiva davant de riscos i incidents. A més, es preveu que aquesta plataforma serveixi com a complement o nexe d'unió amb la plataforma EU CyCLONe[3] que la Unió Europea ha establert en el marc de la Directiva NIS2, a la qual s'ha sol·licitat l'entrada i la incorporació. La integració amb EU CyCLONe permetrà a Andorra accedir a una xarxa europea de resposta a incidents, fet que potenciarà la capacitat del país per afrontar amenaces a escala regional i global.

Aquesta iniciativa no només millorarà la coordinació interna, sinó que també reforçarà la col·laboració amb els països veïns i altres membres de la Unió Europea i, per tant, contribuirà a millorar la protecció en l'entorn digital.

Iniciativa 3: Registre d'amenaces i atacs existents a Andorra i en l'àmbit europeu

La protecció de les infraestructures crítiques es pot aconseguir amb mesures globals, però es millorarà molt la resposta si es coneixen les amenaces principals. Això permetrà una millor orientació de les mesures de resposta i un millor cribratge de les amenaces més freqüents, sempre que els controls de protecció necessaris s'implementin a través d'un programa factible per a la consecució d'aquesta estratègia.

Cal una anàlisi de les amenaces i dels atacs per poder aconseguir una millor resposta. Aquesta anàlisi es completarà amb les amenaces que es discuteixin en els fòrums internacionals per a una revisió més exhaustiva.

Es crearan canals de comunicació i relació amb empreses i ciutadans per facilitar la denúncia de ciberatacs, oferir suport i aclarir dubtes sobre ciberamenaçes. Això inclourà l'estudi, viabilitat i posterior implementació d'una Oficina Virtual de Ciberseguretat basada en tecnologia d'IA, que també servirà per alertar sobre comportaments maliciosos.

Es continua treballant en l'enfortiment de les capacitats per obtenir i generar intel·ligència de ciberamenaçes, per assegurar que les mesures de protecció i resposta siguin cada vegada més precises i eficaces. Aquestes millores permetran a Andorra mantenir-se més ben preparada i alineada amb els desafiaments en l'àmbit de la ciberseguretat, tant a escala nacional com internacional.

3.3. Objectiu 3. Cooperació entre l'Estat i el sector privat

Iniciativa 4: Donar continuïtat al PPP (partenariat publicoprivat) i fer-lo evolucionar

Amb l'objectiu de consolidar la protecció d'infraestructures crítiques/importants i reforçar la cooperació entre el sector públic i el privat, es duran a terme les accions clau següents:

Desenvolupament del Fòrum nacional de ciberseguretat

Es crearà un fòrum nacional dedicat a la ciberseguretat que actuarà com a plataforma central per a la col·laboració entre els actors clau dels sectors públic i privat. Aquest fòrum tindrà la funció de facilitar l'intercanvi d'informació, coordinar els esforços en matèria de seguretat cibernètica i proporcionar actualitzacions periòdiques sobre les iniciatives en curs.

Estudi i creació/col·laboració d'un màster en ciberseguretat

Es dissenyarà un programa de màster (o s'hi col·laborarà) amb l'objectiu de captar professionals i talent internacional en el camp de la ciberseguretat. El programa buscarà establir Andorra com un centre centrat en la formació en ciberseguretat, atraient experts internacionals i col·laborant amb institucions acadèmiques i empreses per assegurar que el contingut del màster s'ajusti a les necessitats actuals del sector.

[3] https://www.enisa.europa.eu/topics/incident-response/cyclone

Establiment d'un servei d'intel·ligència nacional

Es proposarà l'estudi, la creació i la viabilitat d'un servei d'intel·ligència nacional dependent del Ministeri d'Interior, i amb col·laboració amb l'ANC-AD, que col·laborarà amb les LEAs (*law enforcement agencies* o agències d'aplicació de la llei), amb entitats encarregades de la seguretat pública i el compliment de les lleis, com ara la Policia i altres organismes responsables de la seguretat pública, i els donarà suport, i oferirà informació crítica sobre campanyes actives i actors rellevants en ciberseguretat.

Aquest servei proporcionarà suport al CSIRT-AD (ANC-AD), fet que millorarà la capacitat de resposta davant de les amenaces cibernètiques. A més, informarà empreses i ciutadans sobre les noves amenaces i les millors pràctiques de seguretat, fet que augmentarà la seguretat global del país.

D'altra banda, proporcionarà sobirania i independència pel que fa a les investigacions en matèria d'intel·ligència i amenaces al país.

Aquest servei d'intel·ligència disposarà d'una llei reguladora pròpia, amb les atribucions corresponents, similar a la dels països veïns (ex: CCN-CERT).

Potenciació de la indústria andorrana de ciberseguretat

Es prendran mesures per incrementar la competitivitat i l'expansió de la indústria de ciberseguretat. Aquestes mesures inclouran el suport a les empreses locals per augmentar les seves capacitats i oportunitats, així com la promoció de la indústria a escala nacional i internacional.

Impuls de programes de finançament públic per a la investigació i la innovació

Es crearan o potenciaran programes amb finançament públic destinats a donar suport a la investigació i la innovació en ciberseguretat. Aquests programes fomentaran la col·laboració entre la part acadèmica, la indústria i el sector públic, promovent projectes innovadors i avançats en seguretat cibernètica. El finançament públic ajudarà a desenvolupar noves tecnologies i solucions de seguretat que beneficiïn tant el sector com la societat en general.

Creació d'un programa d'empreses emergents i incubadores d'empreses de ciberseguretat

Es posarà en marxa un programa específic per a *empreses emergents* i incubadores d'empreses de ciberseguretat. Aquest programa impulsarà l'emprenedoria en ciberseguretat amb una visió internacional i establirà mecanismes de col·laboració amb iniciatives similars a escala internacional. Oferirà suport i recursos per llançar i fer progressar noves empreses en el sector de la ciberseguretat, i facilitarà l'intercanvi de coneixements i oportunitats de creixement global.

Iniciativa 5: Continuïtat i evolució del programa nacional de sensibilització

Amb l'objectiu de consolidar i ampliar l'impacte del programa nacional de sensibilització en matèria de ciberseguretat, s'implementaran diverses accions orientades a millorar la competència i la conscienciació en ciberseguretat tant en la ciutadania com en els professionals del sector.

Aquest esforç s'articularà a través de les línies estratègiques següents:

- Desenvolupar programes educatius en escoles i institucions acadèmiques, per tal d'integrar la ciberseguretat en l'educació des d'edats primerenques per promoure una cultura de seguretat digital en els joves.
- Implementar campanyes de sensibilització dirigides a diferents segments de la població per augmentar la conscienciació sobre els riscos digitals i fomentar bones pràctiques en l'ús de la tecnologia. En aquest context, Andorra demanarà l'adhesió a l'EU Cybersecurity Month[4] amb campanyes de sensibilització, tallers pràctics i recursos educatius per millorar el coneixement en ciberseguretat tant entre ciutadans com organitzacions.
- Impulsar accions per atreure i retenir talent qualificat en ciberseguretat, per enfortir l'ecosistema local.
- Organitzar un esdeveniment de referència internacional sobre ciberseguretat amb la participació de

[4] European Cybersecurity Month — ENISA (europa.eu)

ponents d'Andorra i internacionals, dissenyat per fomentar la col·laboració, l'intercanvi de coneixements i la difusió de pràctiques millors en el sector, fet que posicionarà Andorra com un punt clau a la regió.

Iniciativa 6: Desenvolupament de recursos humans

Prenent com a objectiu el desenvolupament de les capacitats dels recursos humans de l'àrea de ciberseguretat al Principat d'Andorra, la iniciativa es dirigeix cap a la detecció, la promoció i el desenvolupament del talent per respondre a la creixent demanda global de professionals qualificats dins de la ciberseguretat. Aquesta activitat busca potenciar les institucions d'ensenyament superior andorranes per incloure temes de ciberseguretat en els seus plans d'estudi i impulsar programes de recerca rellevants, per tal d'assegurar així una oferta adequada de talent especialitzat en la protecció de xarxes i sistemes d'informació.

Així mateix, aquesta activitat es recolza en la creació d'un ecosistema de col·laboració entre institucions d'ensenyament superior, empreses tecnològiques i centres de recerca per detectar i desenvolupar el talent en ciberseguretat. Per exemple, mitjançant programes de formació pràctica, simulacions d'atacs reals i col·laboració amb experts de la indústria, entre altres exemples, es vol garantir que els futurs professionals estiguin preparats per a les exigències globals en protecció de sistemes d'informació.

3.4. Objectiu 4. Cooperació internacional

Iniciativa 7: Ampliació de les activitats del CSIRT-AD amb enfocament internacional

L'enfortiment de la ciberseguretat a Andorra mitjançant l'expansió i la millora de les capacitats del CSIRT-AD, amb un enfocament internacional, facilitarà la protecció d'infraestructures crítiques i estratègiques, millorarà la resiliència de les organitzacions davant dels ciberatacs i promourà la innovació en ciberseguretat a través de la cooperació internacional. Una de les estratègies clau és la creació d'un centre de connexió (*hub*) d'intel·ligència de ciberamenaces (CTI HUB) que facilitarà la compartició de cabals de continguts (*feeds*) d'intel·ligència entre empreses crítiques i estratègiques. Aquest concentrador es desenvoluparà seguint estàndards internacionals del sector, inspirant-se en models com el Centre Nacional de Ciberseguretat (NCSC)[5] del Regne Unit i la Cybersecurity and Infrastructure Security Agency (CISA)[6] dels EUA, per assegurar la interoperabilitat i l'eficàcia en la compartició de dades.

A més, es potenciarà la creació d'un *cyber blue team*, un equip especialitzat en la simulació de ciberatacs, incloent-hi proves de penetració i avaluacions de vulnerabilitat, amb la finalitat d'entrenar, millorar les capacitats de defensa de les organitzacions i identificar bretxes en els sistemes de les entitats crítiques d'Andorra. Aquest enfocament es basarà en les bones pràctiques adoptades per equips similars a escala internacional.

També es promourà la creació d'un centre de competència en ciberseguretat per consolidar i coordinar la recerca i la innovació en aquest camp, en col·laboració amb organismes de la Unió Europea, com també amb entitats internacionals i estats com el Regne Unit, els Estats Units i l'Organització d'Estats Americans (OEA). Aquest centre servirà com a punt de referència per al desenvolupament de noves tecnologies i solucions en seguretat digital, amb l'objectiu d'atraure empreses de tecnologia i ciberseguretat perquè estableixin operacions a Andorra, oferint un entorn favorable i fomentant la competitivitat del país en l'economia digital.

Iniciativa 8: Planificació i organització d'exercicis cibernètics nacionals i paneuropeus

Totes les parts interessades en la ciberseguretat han de col·laborar, ja que és l'única manera d'incrementar la confiança entre les parts.

Els mecanismes de cooperació creats s'hauran d'avaluar i comprovar regularment simulant situacions de crisi. Aquests exercicis han demostrat ser una eina que permet garantir els nivells de preparació de les autoritats competents per afrontar alguna crisi, com podria ser la pèrdua d'una part important de la xarxa de comunicacions. En l'àmbit europeu, els mecanismes que permeten afrontar aquest tipus de crisi ja existeixen; i s'ha demostrat que la principal mancança és com es pot aconseguir una cooperació ràpida entre les autoritats implicades.

En aquest sentit, es planeja desenvolupar anualment un ciberexercici a escala nacional i, a més i de forma

[5] National Cyber Security Centre - NCSC.GOV.UK

[6] Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA

habitual, la participació en els exercicis organitzats per l'Agència de la Unió Europea per a la Ciberseguretat (ENISA)[7] i altres països. També es preveu la creació d'un *capture the flag* (CTF) a escala nacional, amb possibilitats de participació internacional, la qual cosa permetrà millorar les habilitats tècniques i fomentar la cooperació més enllà de les fronteres nacionals.

Iniciativa 9: Cooperació internacional amb participació en els fòrums i grups de treball europeus

Andorra no pot mitigar tots els problemes i les amenaces del ciberespai, i cal que cooperi amb estats de l'àmbit europeu.

La presència de representants del Principat d'Andorra en grups de treball i fòrums internacionals que operen sota els auspicis de la Comissió Europea, de l'ENISA i l'OSCE[8] és part d'aquesta estratègia, amb l'objectiu de la participació activa i la contribució d'Andorra a les decisions significatives que es prenen en aquests grups de treball. A fi de desenvolupar i millorar contínuament les capacitats de resposta d'Andorra en matèria de ciberseguretat, es crearan vincles estrets amb les respectives autoritats competents d'altres estats membres de la Unió Europea i d'altres països.

3.5. Objectiu 5. Impulsar el desplegament de la IA en matèria de ciberseguretat

Iniciativa 10: El paper de la IA en la ciberseguretat

Amb l'avanç accelerat de la tecnologia, els atacs cibernètics s'han tornat més sofisticats, utilitzant tàctiques i eines innovadores per eludir les defenses tradicionals. En aquest context, la intel·ligència artificial (IA) s'ha posicionat com una eina crucial per enfortir la seguretat digital. Per això, Andorra desenvoluparà una estratègia sòlida per impulsar el desplegament de la IA en ciberseguretat, procurant un enfocament integral que abasti la detecció, la resposta i la mitigació d'atacs.

Amb la condició de millorar i optimitzar els recursos, s'analitzaran els mecanismes de millora de la protecció davant d'amenaces per mitjà d'IA basada en MLE (models de llenguatge extens) –*LLM (large language models)*, en anglès– (GenIA) a partir de la millora de la detecció. Els MLE són coneguts com a models de llenguatge a gran escala, com els que s'utilitzen en la intel·ligència artificial generativa (GenIA). En ciberseguretat, els MLE poden emprar-se per detectar amenaces analitzant patrons en correus electrònics, comunicacions i altres dades, identificant possibles intents de pesca a les xarxes o activitat maliciosa. A més, els MLE poden automatitzar la generació d'informes d'incidents i oferir suport en temps real als analistes de seguretat, fet que millora la presa de decisions i la resposta a incidents.

Per assegurar-ne la implementació de manera ètica i responsable, és crucial establir directrius clares que evitin biaixos i errors, fer auditories periòdiques i garantir la transparència i la privacitat en el maneig de les dades.

[7] ENISA (europa.eu)

[8] Organización para la Seguridad y la Cooperación en Europa | OSCE

4. Objectius acomplerts

A continuació, s'enumeren els objectius o fites que han estat aconseguits en el període 2021-2024:

- Iniciativa 1 - Creació d'un marc legal.
    - Elaboració d'una llei relativa a les mesures destinades per garantir un nivell comú de ciberseguretat (NIS-AD) elevat. Aquest objectiu es va acomplir mitjançant la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació.
    - Creació de l'Agència Nacional de Ciberseguretat, mitjançant el Decret 346/2021, del 20-10-2021, 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, en què es determinen les responsabilitats, les competències i les funcions de l'Agència.
    - Creació del Centre de Resposta a Emergències (CSIRT-AD), mitjançant el Decret 346/2021, del 20-10-2021, 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, en què es determinen les responsabilitats, funcions i obligacions.
    - Desenvolupament, desplegament i primera certificació a les entitats afectades de l'Esquema nacional de seguretat, mitjançant el Decret 417/2022, del 12-10-2022, pel qual s'aprova el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra.
    - Desenvolupament, desplegament i primera certificació a les entitats afectades del RIC-AD, mitjançant el Decret 418/2022, del 12-10-2022, pel qual s'aprova el Reglament d'infraestructures crítiques del Principat d'Andorra.
    - Creació del Comitè Especialitzat en Ciberseguretat, mitjançant el Decret 346/2021, del 20-10-2021, 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. Des de l'inici, s'han dut a terme quatre sessions quadrimestrals, i s'han aconseguit els objectius del Comitè i de les comissions que s'estructuren sota l'ANC-AD.
    - Desenvolupament del Pla nacional de resposta a incidents (PNRI).
    - Desenvolupament de la Guia Nacional de notificació d'incidents.
    - Elaboració de la modificació de la Llei 9/2005, del 21 de febrer, qualificada del Codi penal.
    - Elaboració de la modificació de la Llei 30/2018, del 6 de desembre, qualificada de seguretat pública.
    - Elaboració de la modificació de la Llei 4/2020, del 23 de març, qualificada dels estats d'alarma i d'emergència.
- Iniciativa 2 - Identificació i estudi de les interdependències existents per a la implementació de l'estratègia.
- Iniciativa 4 - Creació d'un PPP (partenariat publicoprivat).
- Iniciativa 5 - Desenvolupament d'un programa nacional de sensibilització.
- Iniciativa 8 - Planificació i organització d'exercicis cibernètics nacionals i paneuropeus.
    - Execució d'un ciberexercici basat en la simulació d'un atac de denegació de servei distribuït (DDoS) –atac que genera un gran volum de trànsit maliciós cap a Andorra Telecom, i com a conseqüència afecta els serveis de les entitats–, en el qual van participar tretze entitats i organismes del Principat d'Andorra considerats com a operadors crítics a causa de la naturalesa de les activitats que duen a terme. Per a això, es va efectuar un procés de coordinació i avaluació de la identificació, resposta i comunicació de l'atac.

5. Propers passos

5.1. Cost de la implementació

El cost d'implementació de cada iniciativa i com es reparteix en els diferents exercicis pressupostaris s'ha d'avaluar amb totes les autoritats competents per veure com es podria fer.

Independentment del seu cost, es prioritzaran les iniciatives que augmentin la seguretat de les xarxes i dels sistemes d'informació, així com l'ús segur dels elements connectats.

5.2. Planificació de les iniciatives 2024-2027

Aquest document proporciona una sinopsi de les línies estratègiques més importants que s'han identificat per garantir una resposta coherent i efectiva en matèria de ciberseguretat, de manera que el ciberespai, així com les xarxes i la informació que s'utilitza diàriament, estiguin degudament protegits en tota la societat andorrana. No obstant això, per a una implementació adequada, és necessari analitzar i desenvolupar cada línia estratègica detalladament, per tal d'identificar totes les activitats associades. Posteriorment, s'elaborarà una anàlisi detallada de cadascun dels eixos d'acció, així com la identificació dels recursos i els processos necessaris perquè siguin implementats.

Les activitats esmentades anteriorment donen suport a la planificació de les iniciatives estratègiques perquè l'Estratègia pugui avançar de manera efectiva, en funció dels recursos que l'Estat destini a posar-la en marxa. Aquesta planificació es basarà en els resultats d'una avaluació detallada, tenint en compte els costos i la priorització de les iniciatives, de manera que la implementació de la resposta estratègica en el seu conjunt es pugui dur a terme de la manera més eficaç possible, atesos els recursos disponibles. El resultat d'aquest procés serà una cronologia detallada que permetrà controlar l'estat d'implantació de totes les iniciatives dins de l'estratègia actual.

5.3. Avaluació de resultats i revisió de l'estratègia

Per aconseguir una resposta estratègica eficaç, s'ha de revisar periòdicament i estrictament el progrés de la seva implementació. Amb aquesta finalitat, s'analitzaran quantitativament i qualitativament els resultats de la implementació de les mesures i les disposicions incloses en les iniciatives estratègiques. Una estratègia de ciberseguretat adequada no es pot considerar com un *pla final*; al contrari, se n'ha d'observar i actualitzar la implementació a intervals regulars. Aquest procés de revisió ha de tenir en compte els resultats de l'avaluació, així com les noves amenaces que apareixen (i continuaran apareixent) al ciberespai i qualsevol altra nova condició que es manifesti en aquesta àrea.

L'ampliació detallada de les iniciatives de l'Estratègia, tal com es descriu a la secció 4.1, inclourà indicadors i criteris per avaluar el rendiment de cada iniciativa, quan sigui possible, i els resultats d'aquesta anàlisi permetran una revisió adequada de l'Estratègia en el futur, amb beneficis substancials per a la societat andorrana.