ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Memòria anual ANC-AD / CSIRT-AD 2022

Gener del 2023

Fitxa del document

Títol	Memòria anual 2022 ANC-AD / CSIRT-AD

Versió	Redactat/Revisat per	Aprovat per	Data d'aprovació	Data de publicació
1.0		ANC-AD	01/23	

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document: ANC-AD

ÍNDEX

Pròleg

La irrupció de la digitalització a 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. Introdueix sens dubte una afectació transversal en les maneres de fer en àmbits tan diversos com el cultural, el social, l'econòmic o 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 la ràpida evolució 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 esmentats han de ser clarament interpretats com a elements habilitadors del canvi i n'han fomentar, si és possible, l'acceleració i l'expansió. Addicionalment no hi ha l'opció de fer un pas enrere, ni tan sols de plantejar-se un possible estancament evolutiu atenent al ràpid procés de transformació en el qual estem immersos. Els negocis, les comunicacions, el transport, els serveis financers, l'administració o la societat en general se sostenen sobre algun d'aquests elements i els utilitzen cada dia més com a palanca d'activació. Sembla evident, doncs, que s'ha generat una alta dependència no únicament evolutiva, sinó també de funcionament, cap a aquest tipus de serveis o components estructurals. Aquest fet comporta, conseqüentment, que la protecció dels serveis i les infraestructures associades que els possibiliten s'hagin convertit en un factor d'alt risc.

A la llum del que s'ha exposat, doncs, l'accessibilitat i 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 d'un entorn segur i estable no té un abast o impacte únicament locals, ans al contrari. Molts estats treballen per mitigar les possibles amenaces que pot suposar una disfunció o un bloqueig d'aquests serveis en la mesura que poden ocasionar impactes importants en l'economia, afectar les operacions diàries 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 les formes de fer. De fet, ja es treballa activament en la creació d'un ecosistema digital que promogui i faciliti noves fórmules d'interacció, permeti introduir més agilitat i eficiència, potenciï l'autogestió i, en definitiva, introdueixi nous formats de relació entre els diversos organismes, les empreses i les persones. Aquest ecosistema s'està construint amb una plena orientació cap a les persones i la societat en general i, per tant, és clau que se'n respecti la seguretat, la privacitat i les llibertats. La interconnexió, la interoperabilitat i

la transparència d'informació han d'esdevenir factors clau d'èxit per tal de garantir una societat innovadora i 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, així mateix, s'ha de convertir en un avantatge competitiu en el nostre acostament a la Unió Europea.

Cada cop hi ha més 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 esforç 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 nacional de ciberseguretat defineix la posició d'Andorra fixant els principis, les estratègies i les iniciatives per fer front a la vulnerabilitat del ciberespai.

César Marquina Pérez de la Cruz
Ministre de Finances i portaveu del Govern

Resum executiu

Andorra es troba en un moment en què té el repte d'abordar un programa de transformació digital holística per al país a través d'un pla integral en què la ciberseguretat és un pilar molt important, amb objectius precisos i comuns a tot el país. Les tecnologies de la informació i de la comunicació (TIC) són un motor rellevant del desenvolupament econòmic i social, alhora que són eines necessàries per al funcionament de les estructures funcionals i socials del Principat. 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.

L´estratègia Nacional de Ciberseguretat pretén obtenir un entorn digital segur al Principat d'Andorra, considerant iniciatives per protegir les infraestructures crítiques, els operadors de serveis essencials i els proveïdors de serveis digitals, ja que la destrucció o interrupció d'aquests serveis i infraestructures generaria greus conseqüències per a algunes de les funcions vitals de la societat.

El caràcter transversal i interconnectat de les TIC, que també caracteritza les seves amenaces i riscos, limita l'eficàcia de les mesures que s'utilitzen per contrarestar-los quan aquestes mesures 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 contra les amenaces que afecten les xarxes i els sistemes d'informació, i facilitin la coordinació de les actuacions dutes a terme en aquesta matèria tant en l'àmbit nacional com amb els països del nostre entorn, 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 promogudes per part de 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 identificar les infraestructures i els operadors crítics, establir un marc legal que afavoreixi un Pla nacional de contingència per a infraestructures crítiques, reorganitzar les estructures existents al Principat i afavorir la col·laboració entre els sectors públic i privat. La realització d'exercicis de simulació nacionals i internacionals ha de permetre

desenvolupar les capacitats de les infraestructures crítiques identificades, augmentar la resposta a incidents dins l'Esquema nacional de seguretat i analitzar les amenaces.

Aquest document analitza les iniciatives que s'han de dur a terme en una primera fase així com els passos següents que s'han de seguir, la priorització i planificació de la ciberseguretat nacional i l'avaluació dels resultats de les iniciatives d'estratègia. L'Estratègia nacional de ciberseguretat del Principat d'Andorra 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 en conseqüència de manera que continuï en condicions de proporcionar el màxim benefici a la societat andorrana.

El 2022 en xifres

835
Alertes de vulnerabilitats publicades

217
Notícies Web / XXSS publicades

87
Subscriptors Butlletí

35
Butlletins distribuïts

12
Playbooks elaborats

8
Píndoles conscienciació publicades

21
Incidents gestionats 2022

1572
Visites site web 2022

98
Descàrregues píndoles i informes site web 2022

Segrest de comptes d'Instagram

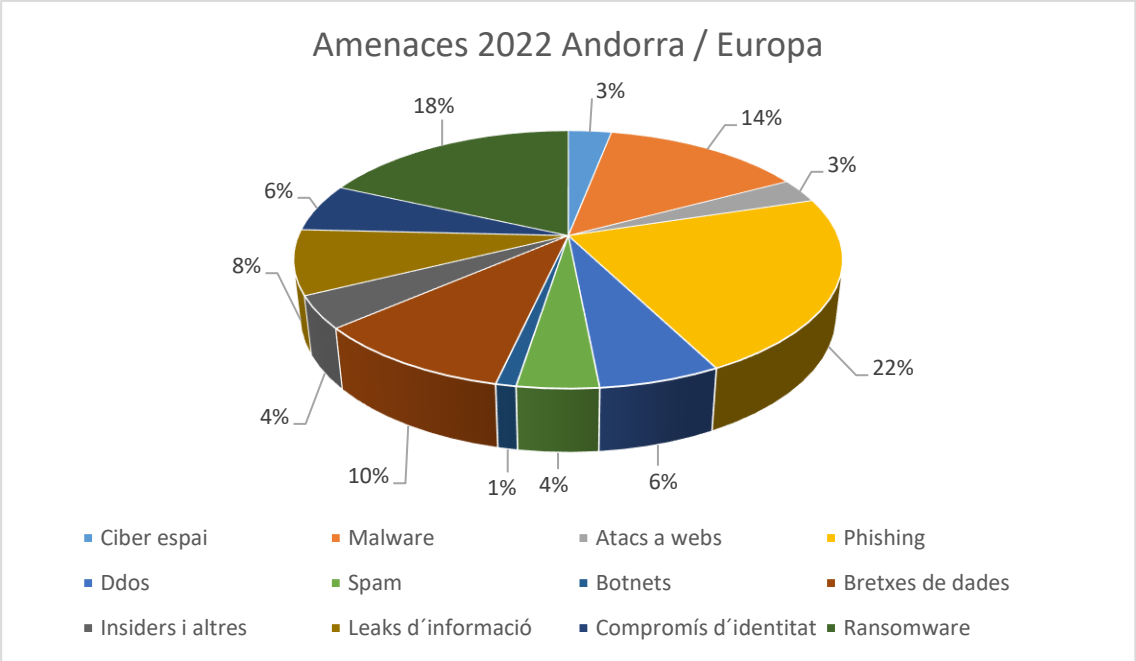
Durant l'any 2022, s'han detectat tres campanyes d'intent de segrest de comptes d'Instagram al Principat, amb un balanç de més de 50 denúncies (segons dades oficials de la Policia), en què s'ha pogut observar un mateix patró inicial, aprofitant diferents publicacions de credencials al *dark web*[7] (web fosc).
Aquestes dades han estat recopilades mitjançant diferents vectors d'atac: *malware*[17],

Programari maliciós Redline

RedLine és una família d'*information stealers*[13] que va emergir a principis del 2020 i que, en data abril del 2022, se situa com un dels *stealers* més populars i amb més percentatge d'adopció per actors de tots els nivells i racons del món. Inicialment el programa es va llançar com un model de *malware as a service* (MaaS) en què l'actor responsable del desenvolupament oferia el paquet a canvi d'una subscripció mensual. Un dels motius que ha disparat l'ús de RedLine per tota mena de cibercriminals i que el cataloga avui dia com a *commodity malware* és la seva facilitat d'accés. Nombroses versions del tauler de control es troben disponibles de forma gratuïta a través d'escletxes i filtracions, baixant el llistó d'entrada per a actors menys experimentats. A més, el tauler de control és una aplicació per a Windows que només requereix el marc .NET i un doble clic per desplegar-lo, fet que en facilita també la instal·lació per a usuaris amb menys nivell tècnic.

Leaks[16] i filtracions de dades

Durant l'any 2022, ha augmentat un 38% la publicació i filtració de dades personals d'usuaris. Aquest augment deriva de l'alt nivell d'atacs deguts a la COVID-19 i el teletreball, provocat per una relaxació de l'usuari i la falta de mesures de prevenció contra intrusions.



Disminució dels casos de *ransomware*

Tot i que el nombre d'atacs ha augmentat en un percentatge significatiu, l'amenaça per programari de segrest ha baixat puntualment durant l'últim trimestre de l'any, i s'ha reduït així el nombre de casos reportats per aquest tipus d'atac.
Encara que el nombre d'infeccions ha disminuït, sí que s'ha incrementat la tendència de tipus segrestador, passant d'un 80% de primera generació i un 20% de segona generació (xifres del 2021) a un 60% de primera generació i un 40% de segona generació.

Xarxes socials i missatgeria

S'han detectat múltiples intents d'estafa a través de contactes directes i aplicacions de missatgeria instantània amb diferents formats:

- Ofertes promocionals de comerços (físics i en línia).
- Compra de criptomoneda.
- Entrega de paqueteria.
- Donacions i herències.

Pesca per SMS (*smishing*) i pesca per veu (*vishing*)

Encara que es pugui pensar que són amenaces poc freqüents, a la pràctica se segueixen utilitzant per intentar que l'usuari faciliti dades personals, de contacte o directament dades bancàries. Generalment aquests tipus d'atacs van associats o combinats amb possibles campanyes de *phishing*[19].

1. Estratègia de seguretat d'Andorra

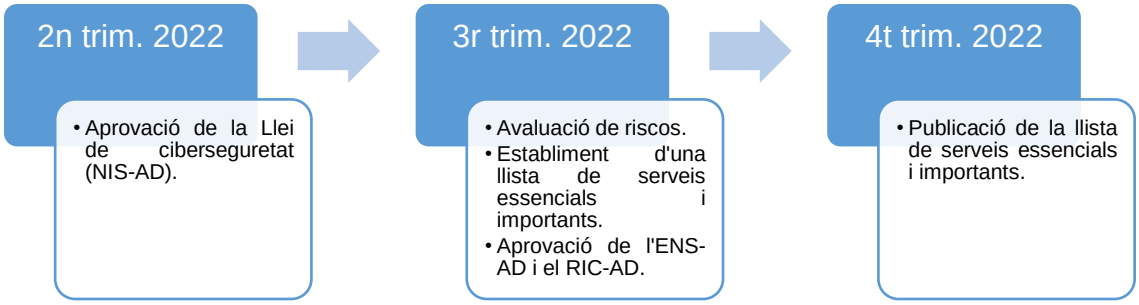
L'Estratègia nacional de ciberseguretat del Principat d'Andorra comprèn els objectius estratègics i les mesures polítiques i normatives necessàries per aconseguir i mantenir un nivell elevat de seguretat en les xarxes i en els sistemes d'informació, cobrint els sectors operats per les entitats essencials i importants en els termes definits a la Llei NIS-AD (22/2022).

Fig. 1. Nivells d'actuació i les nou iniciatives de l'Estratègia nacional de ciberseguretat

2.1 Iniciativa 1. Creació del marc legal

La creació del marc legal ha permès aprovar la Llei de ciberseguretat (NIS-AD), que és l'eix vertebrador de l'Estratègia de ciberseguretat d'Andorra. Aquesta Llei va acompanyada de dos reglaments: l'Esquema nacional de seguretat (ENS-AD) i el Reglament d'infraestructures crítiques (RIC-AD).

D'altra banda, l'aprovació d'aquests dos reglaments comporta que s'hagin de desenvolupar una sèrie de tasques associades, tant per part de l'ANC-AD com per part de les entitats implicades en els reglaments.



2.1.1 Què és l'ANC-AD

L'ANC-AD és l'encarregada de planificar, coordinar, gestionar i controlar la ciberseguretat de xarxes i sistemes d'informació, com a pol tecnològic de referència i confiança, líder en l'estratègia de ciberseguretat del país en un sentit nacional i global. Sense perjudici del que estableixi qualsevol altra normativa que li sigui aplicable, l'ANC-AD té per missió:

- Garantir la ciberseguretat al territori del Principat d'Andorra.
- Protegir la seguretat pública en el ciberespai, anticipant i combatent els delictes en matèria de seguretat de les xarxes i els sistemes d'informació.
- Ser el punt de referència generador de confiança digital per a les entitats de les administracions públiques i entitats privades, especialment per als sectors estratègics representats per les entitats proveïdores de serveis essencials i de serveis importants.

- Cooperar en l'àmbit nacional i en l'internacional en tot el que sigui necessari per a la seguretat de les xarxes i els sistemes d'informació del Principat d'Andorra.

Pel que fa als objectius que ha d'assolir l'ANC-AD s'hi inclouen, a títol enunciatiu i no limitador:

- Fomentar el desenvolupament de la ciberseguretat al Principat d'Andorra com a pilar fonamental de la transformació digital de la societat.
- Reforçar les capacitats del Principat d'Andorra a l'hora de prevenir i gestionar els problemes vinculats a la seguretat de les xarxes i els sistemes d'informació i reaccionar quan apareguin aquests problemes.
- Impulsar l'atenció al criteri de ciberseguretat en els processos de selecció i implantació de les tecnologies de la informació i la comunicació.
- Promoure la consecució i el manteniment d'un nivell de seguretat suficient de les xarxes i els sistemes d'informació, en especial en les entitats proveïdores de serveis essencials i serveis importants.

Per complir la seva missió i els seus objectius, l'ANC-AD porta a terme, a títol enunciatiu i no limitador, les funcions següents a escala nacional:

- Identifica els serveis essencials i importants, juntament amb el CSIRT(-AD i amb el vistiplau de la Comissió de Seguiment.
- Serveix de punt de contacte únic amb les autoritats competents en matèria de ciberseguretat d'altres països, i entre aquestes autoritats i el CSIRT-AD.
- Impulsa la formació professional especialitzada en seguretat de la informació a les institucions públiques i privades, i afavoreix l'atracció i la retenció de talent en l'àmbit de la ciberseguretat i la qualitat en la gestió de la seguretat de la informació.

- Ofereix i dona assessorament a institucions públiques i privades que ho requereixin per desenvolupar capacitats pròpies per a la gestió d'incidents, amb la col·laboració del CSIRT-AD.

Difon informació sobre riscos, amenaces, vulnerabilitats i atacs, i estableix les estratègies de mitigació corresponents a través d'alertes, avisos, pàgines web o altres publicacions tècniques:

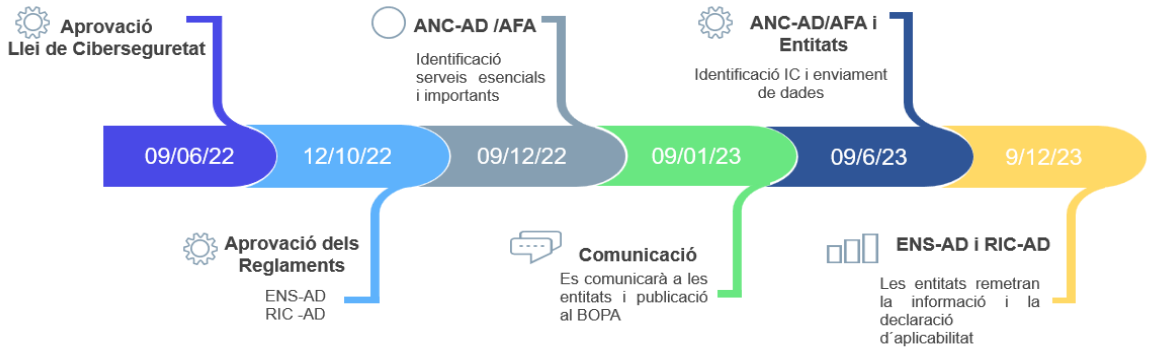
- Dona resposta a incidents de seguretat en les xarxes i els sistemes d'informació.
- Supervisa la resolució dels incidents de seguretat en les xarxes i els sistemes d'informació.
- Difon alertes imminents, avisos i informacions sobre incidents de seguretat en les xarxes i els sistemes d'informació, incloent-hi els atacs i les llacunes de seguretat que s'hagin descobert en els sistemes i aplicacions més utilitzats al Principat d'Andorra quan aquests sistemes i aplicacions tenen un alt nivell de criticitat, i fa possibles recomanacions en relació amb virus extremadament estesos.

2.1.2 Què és el CSIRT-AD

El CSIRT-AD és el principal òrgan competent per coordinar la resposta i respondre als incidents de seguretat en les xarxes i els sistemes d'informació que afectin l'Administració pública, els 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 Principat. El que es promou principalment amb la creació del CSIRT-AD és disposar dels mitjans i recursos necessaris per poder:

- Coordinar de forma centralitzada les qüestions relacionades amb els incidents de seguretat de la informació.
- Prevenir incidents de seguretat de la informació i reaccionar quan apareguin.
- Fer costat als afectats que necessitin recuperar-se d'incidents de seguretat de la informació i assistir-los.
- Ser un mecanisme per respondre sistemàticament als incidents de seguretat en les xarxes i sistemes d'informació i adoptar les accions més adequades per mitigar-ne els efectes.
- Promoure la seguretat de les xarxes i sistemes d'informació, proporcionant un servei de supervisió, detecció, alerta i resposta als incidents de seguretat en les xarxes i els sistemes d'informació.
- Cooperar en l'àmbit nacional i en l'internacional en la identificació i resolució d'incidents de seguretat en les xarxes i els sistemes d'informació i en tot el que sigui necessari per a la seguretat de les xarxes i els sistemes d'informació al Principat d'Andorra en general.

2.1.3 Calendari d'aplicació de la Llei



2.1.4 Reglaments ENS-AD i RIC-AD

Objectiu de l'ENS-AD:

Garantir un nivell de seguretat suficient per als serveis que resulten essencials o importants per al Principat d'Andorra.

Benefici:

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, facilitant 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 s'han de protegir.

Model:

D'acord amb el que s'especifica en la Llei NIS-AD, l'element troncal de l'ENS-AD és la gestió de riscos.

Es proporcionarà un procés ja emprat amb èxit en països com Alemanya i Estònia per identificar els riscos als quals estan exposats les infraestructures, les xarxes i els sistemes d'informació.

Es tracta d'un mecanisme de descomposició del risc en subriscos que permet modelar el sistema sota estudi com la suma d'un conjunt d'actius d'informació estàndard per a cadascun dels quals ja se sap quines mesures de seguretat concretes s'han implantat en funció del nivell de seguretat que vulguem donar als serveis que el sistema proporciona.

Objectiu del RIC-AD:

Reforçar la resiliència de les entitats crítiques i equivalents a crítiques.

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

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

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

Benefici:

D'acord amb el que s'especifica en la Llei NIS-AD, l'element troncal de l'ENS-AD és la gestió de riscos.

Es proporcionarà un procés ja emprat amb èxit en països com Alemanya i Estònia per identificar els riscos als quals estan exposats les infraestructures, les xarxes i els sistemes d'informació.

Model:

Es trasllada a la Llei NIS-AD del Principat d'Andorra la proposta final d'avaluació de la protecció d'infraestructures crítiques de la Comissió Europea COM(2020) 829, relativa a la resiliència de les entitats crítiques, que també adoptaran països com Espanya.

2.1.5 Seguiment i control de l'ANC-AD

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

COMISSIÓ DE SEGUIMENT

Reforçar les relacions de coordinació, col·laboració i cooperació entre les diverses administracions públiques.
Donar suport a la presa de decisions de l'ANC-AD en matèria de ciberseguretat.
Verificar el grau de compliment de l'Estratègia nacional de ciberseguretat i informar-ne l'ANC-AD.

COMITÈ ESPECIALITZAT DE CIBERSEGURETAT

Garantir el funcionament i les actuacions de l'ANC-AD i del CSIRT-AD.
Coordinar els criteris i les actuacions de seguiment i avaluació impulsats per la Llei NIS-AD i pels decrets ENS-AD i RIC-AD.
Consulta i seguiment de les actes de cada reunió del Comitè.

2.2 Iniciativa 2. Identificació i estudi de les interdependències existents per a la implementació de l'estratègia

Dins la identificació, i per implementar inicialment l'estratègia, s'ha de desenvolupar una sèrie de tasques i implementacions de serveis, que van des del portal web (el punt principal d'entrada als serveis de l'ANC/CSIRT) fins a la creació de diferents plans operatius i de seguretat dels operadors crítics, en què han d'intervenir tots els implicats en la col·laboració de l'ANC-AD i la Policia d'Andorra.

D'altra banda, s'iniciarà el càlcul de l'índex (indicadors internacionals, que cal definir segons les característiques del Principat) en matèria de ciberseguretat actual, amb una posterior revisió passat un any des del primer càlcul.

3r trim. 2022

- Inici dels serveis de l'ANC-AD i el CSIRT-AD.

4t trim. 2022

- Inici del càlcul GCI(11).

2.3 Iniciativa 3. Registre d'amenaces i atacs

Per gestionar el registre d'amenaces i atacs i els incidents, es focalitzaran els serveis sobre la gestió inicial de les alertes rebudes i serveis per a la gestió d'incidents enfocats a entitats i a la ciutadania, s'establiran campanyes de *phishing* (19)controlat, per tal d'avaluar el nivell de maduresa de les entitats que ho sol·licitin, i posteriorment l'ANC-AD oferirà serveis de *reversing*(21) i *forensic*(9), molt especialitzats i lligats directament a incidents soferts per les entitats del país, amb total coordinació entre l'ANC-AD, l'entitat i la Policia.

2n trim. 2022

- *Playbooks* associats als serveis.
- Notificació d'incidents.
- XS.
- Alerta precoç.

4t trim. 2022

- Gestió d'incidents amb entitats i ciutadania.

2.4 Iniciativa 4. Creació d'un partenariat públic-privat (PPP)

L'Estat buscarà la cooperació amb les autoritats competents existents que determinin el funcionament de sectors importants: l'Andorra Banking pel que fa al sector bancari, l'Associació de transportistes pel que fa al transport de mercaderies, etc. Es posarà en marxa un mecanisme per proporcionar actualitzacions periòdiques al sector privat, pel que fa als avenços fets en les iniciatives previstes, per ajudar a aconseguir la convergència en les activitats dels sectors públic i privat respecte a les disposicions d'aquesta estratègia.

4t trim. 2022

- Desenvolupar confiança entre el sector públic i el privat.
- Crear un marc de cooperació segur.
- Facilitar l'intercanvi d'informació relacionada amb noves amenaces.

2.5 Iniciativa 5. Desenvolupament d'un programa nacional de sensibilització

En aquest apartat es pretén desenvolupar i teixir un programa per tal de sensibilitzar entitats i població en matèria de ciberseguretat, ja sigui amb la publicació recurrent de píndoles de conscienciació, xerrades genèriques sobre diferents temes que poden afectar la ciberseguretat, formacions que se sol·licitin a mida o sobre alguna matèria específica, preparant un curs d'entrenament intensiu (*bootcamp*[1]) de ciberseguretat i col·laborant en matèria de ciberseguretat a la UdA.

2n trim. 2022
- Publicació de píndoles formatives.

3r trim. 2022
- Xerrades destinades a entitats.
- Xerrades destinades a la població en general.

2n trim. 2023
- Preparació del *bootcamp*(1) de ciberseguretat.
- Formació en l'àmbit universitari.

2.5.1 Píndoles formatives per a la ciutadania

2.5.2 Sensibilització i formació

L'ANC-AD ha anat desenvolupant des dels inicis serveis de sensibilització en matèria de ciberseguretat.

Referent a això, durant el 2022 l'ANC-AD ha participat en diverses jornades de sensibilització i formació per a diferents entitats.

Les xarxes socials afecten de diferents formes la ciutadania, i aquest impacte es multiplica quan es parla de les famílies. A través de les píndoles de conscienciació l'ANC-AD vol ajudar a donar a conèixer quina és la manera de fer-ne un ús segur i saludable i tracta altres temes relacionats, ja que la tecnologia pot servir com a eina per fomentar la relació i el desenvolupament dels més vulnerables, però també ha d'incloure i tocar altres qüestions d'importància que tinguin a veure amb els factors de risc i les amenaces existents.

Els principals usuaris d'Internet són els adolescents i els joves. Aquest és un col·lectiu que cal tenir en compte a causa de la seva alta vulnerabilitat.

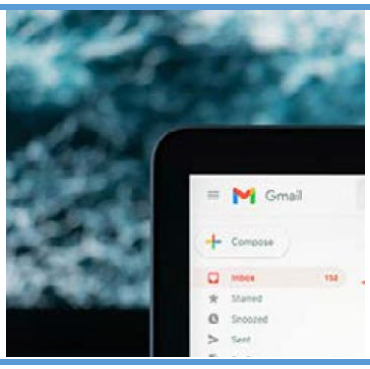
2.5.3 Sortides professionals en matèria de ciberseguretat

La ciberseguretat cada vegada és més present i avui dia és una de les poques professions en què l'oferta supera la demanda. L'Institut Nacional d'Estàndards i Tecnologia dels Estats Units (NIST) classifica les possibilitats de professió en quatre pilars:

2.5.4 Consells de ciberseguretat

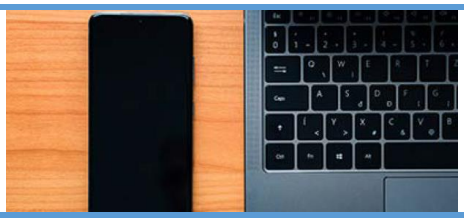
Programari segrestador (*ransomware*[20]): què és, com es propaga i què cal fer en cas d'atac per protegir l'empresa

Un simple descuit pot convertir una empresa en una víctima de *ransomware*[20]. És igual la mida i el sector en què operi: n'hi ha prou que una persona de l'organització obri un correu fraudulent, entri en una pàgina web desconeguda o faci clic en un arxiu infectat perquè un troià s'introdueixi al sistema i impedeix accedir a les dades. En aquell moment, l'empresa s'haurà convertit en un "blanc" digital d'un ciberdelinqüent, que exigirà el pagament d'un rescat perquè es pugui recuperar la informació.
A l'ANC-AD, conscients d'aquest problema, s'avisa i es dona suport tant a pimes com a la gran empresa a través de diferents serveis.



El mètode de transmissió és summament senzill. En moltes ocasions, els ciberdelinqüents envien de manera massiva correus electrònics amb enllaços a URL falsos o amb arxius adjunts maliciosos en diversos formats en espera que alguna persona pateixi un descuit i l'obri per error. En el moment en el qual l'usuari fa clic a l'arxiu o a l'enllaç, s'activa la descàrrega de *ransomware*[20], que encripta el sistema i el manté segrestat amb una contrasenya fins que la víctima paga el rescat.

Xarxes socials o missatgeria instantània. Les xarxes i la missatgeria instantània permeten a la ciberdelinqüència arribar a les seves víctimes de forma massiva i amb senzillesa mitjançant enllaços falsos o arxius que contenen fitxers.



Forats de seguretat. Algunes aplicacions i sistemes operatius sense actualitzar tenen vulnerabilitats o forats de seguretat, que poden arribar a ser un focus per als ciberdelinqüents.

En cas que l'empresa s'hagi vist infectada per *ransomware*[20] cal adoptar determinades mesures i, sobretot, no pagar mai el rescat. Si es fa, no només es contribueix a perpetuar aquest tipus de delictes, sinó que no es tindrà mai la certesa d'haver acabat amb el problema, ni garanties per poder recuperar les dades. Aquestes són algunes de les accions que s'han de dur a terme:

- Desconnectar l'equip de la xarxa per intentar evitar l'expansió del troià.
- Canviar les contrasenyes des d'un dispositiu diferent i, si pot ser, connectat a una altra xarxa.
- Conservar els arxius xifrats perquè és possible que més endavant hi hagi alguna eina que aconsegueixi desencriptar-los.

Jocs en línia

Cada dia són més les persones que juguen en línia. Però són tots els videojocs en línia segurs? Quines mesures hem de prendre per no caure en les xarxes d'un ciberdelinqüent?.

És molt divertit jugar amb la colla en línia, però això comporta uns riscos que han de conèixer tant els jugadors com els seus progenitors. La indústria dels videojocs està en alça i les seves xifres així ho corroboren. Les dades d'alguns estudis de videojocs sostenen que aquesta indústria ja supera la del cinema o la de la música i que, a més, s'ha vist impulsada per la pandèmia. El 2020 el nombre total de jugadors va ser de 15,9 milions i una de cada quatre persones jugadores (26%) té entre 6 i 14 anys.

La seva arribada a les llars es produeix cada vegada a edats més primerenques, ja que el seu caràcter lúdic i social resulta ideal per a les persones més joves. No obstant

això, aquesta pràctica també porta associats certs perills, per la qual cosa convé aplicar mesures de seguretat.

Per tot això és important conèixer les possibles amenaces que hi pot haver en una partida en línia, encara que sigui entre persones del mateix entorn. Es juga per divertir-se i evadir-se en el temps de lleure, però això no implica que s'hagin de relaxar les precaucions. Per evitar problemes, és important tenir en compte els consells següents:

Utilitzar un correu electrònic nou per registrar-se a les plataformes en línia. Així es limita i controla la informació personal que es vol compartir.

No vincular targetes de crèdit a plataformes de joc. Utilitzar una targeta virtual amb saldo limitat que es pugui desconnectar quan no s'utilitzi.

Revisar les app i els comptes connectats a les XS.

Accés a continguts per part dels menors

Pel que fa als riscos, no es tracta d'escandalitzar les famílies, sinó d'escoltar les inquietuds en matèria de ciberseguretat i menors, partir dels seus coneixements i experiències, per complementar-les i millorar-ne la perspectiva en aquest àmbit. L'objectiu és que puguin ser més eficaces a l'hora de detectar aviat o resoldre un incident en línia.

Així mateix, és fonamental rebatre la idea estesa que "això al meu fill/a no li passarà". N'hi ha prou a reflexionar breument sobre algunes dades: segons l'estudi Net Children Go Mobile1, un 18% dels menors s'havien sentit molestos per alguna cosa succeïda a Internet, un 32% havia patit assetjament, un 31% havia rebut missatges sexuals d'alguna mena, un 21% havia contactat en línia amb persones desconegudes, un 32% havia vist continguts inapropiats i potencialment perjudicials, etc.

Es pot dir que el nostre objectiu és implicar les famílies en l'educació digital dels seus fills i filles. Tot i això, la forma de concretar aquesta tasca pot variar notablement segons l'edat i el grau de maduresa de cada menor: des d'un acompanyament continu, en un entorn acotat, per progressivament anar guanyant autonomia demostrant responsabilitat, fins a desenvolupar-se lliurement a Internet, amb una supervisió basada en el diàleg i la confiança.

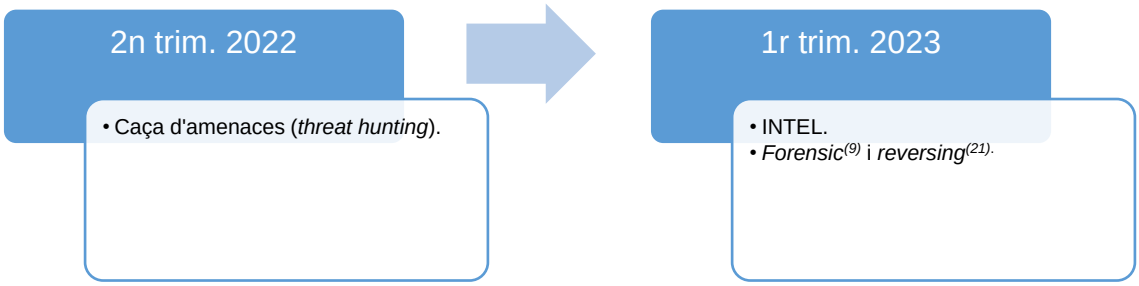
És imprescindible acompanyar els nostres fills i filles en l'ús d'Internet per poder aprendre junts a gaudir-lo de manera segura. Es tracta d'un aprenentatge per a les dos parts, perquè ells veuran en nosaltres una guia o model que cal seguir (per exemple, com reaccionem davant d'un problema, de quins resultats de cerca ens fiem més, com gestionem la publicitat, etc.), però nosaltres també comprendrem millor l'entorn en què es mouen (quines aplicacions i activitats estan de moda, amb qui es relacionen, com s'exposen a la xarxa, etc.).

Lògicament, el nostre acompanyament haurà d'adaptar-se de mica en mica a les seves necessitats, grau de maduresa i autonomia.

Amb els més petits, haurem d'estar al seu costat cada vegada que es connectin per, a poc a poc, ajudar-los a créixer amb responsabilitat i a guanyar autonomia, i anar acompanyant-los de manera més ocasional (per exemple, navegant junts de tant en tant, demanant-los que ens ensenyin a utilitzar una nova app o un joc, etc.).

2.6 Iniciativa 6. Desenvolupament de recursos humans / capacitació

L'ANC-AD i el CSIRT-AD, amb els principals serveis publicats i en funcionament, per anar avançant amb la resta de serveis per prestar, siguin interns o externs, ofereixen serveis enfocats principalment a les entitats essencials dirigides a la part proactiva i a la resposta immediata, així com al control i les auditories anuals de les diverses infraestructures, en què hi ha personal tècnic especialitzat en cadascun dels sectors que serà complementari i donarà suport a les tasques que duu a terme de forma interna cada entitat.



2.6.1 Serveis proactius de gestió, comunicació i formació

Serveis proactius de gestió, comunicació i formació

Alertes i advertiments	• L'objectiu d'aquest servei serà proveir el CSIRT-AD d'informes estratègics (de vigilància activa) així com la generació d'alertes respecte a actius crítics representats mitjançant paraules clau definides per dur a terme recerques sobre actors, campanyes, amenaces, etcètera.
Comunicats	• S'identifiquen les publicacions més representatives de l'àmbit de la seguretat informàtica, tant en revistes especialitzades com en mitjans de comunicació generalistes. Entre els mitjans més rellevants es prioritzen les temàtiques o notícies que puguin resultar de valor per al públic objectiu subscrit en la llista de distribució.
Difusió d'informació	• El servei de difusió d'informació té per objectiu mantenir els canals de comunicació per informar els consumidors de serveis de ciberseguretat, així com canalitzar continguts generats per altres serveis, com la notificació de vulnerabilitats, i donar visibilitat contínua a l'activitat de l'ANC-AD i el CSIRT-AD.

Suport a la resposta d´incidents	• L'objectiu d'aquest servei és mantenir i crear noves guies de resolució (d'ara endavant, "*playbooks*"), entenent que abasta l'elaboració d'instruccions, guies i recomanacions per solucionar incidents de ciberseguretat i garanteix que es prenguin decisions encertades en el moment d'una crisi.
Sensibilització i formació	• El servei consisteix en la provisió i elaboració de píndoles formatives amb l'objectiu de promoure la conscienciació i formació de manera recurrent per part dels usuaris i entitats. Mensualment es publica una píndola de conscienciació. A més, el servei disposa de formacions per a les entitats que ho sol·licitin.
Llistes d'IOC	• L'IOC(14) és la descripció d'un incident de ciberseguretat(4), activitat i/o artefacte maliciós mitjançant patrons, per identificar-lo en una xarxa o *endpoint* i poder millorar així les capacitats davant la gestió d'incidents. El procés preveu la intel·ligència contra amenaces aplicada de fonts d´informació estratègiques.

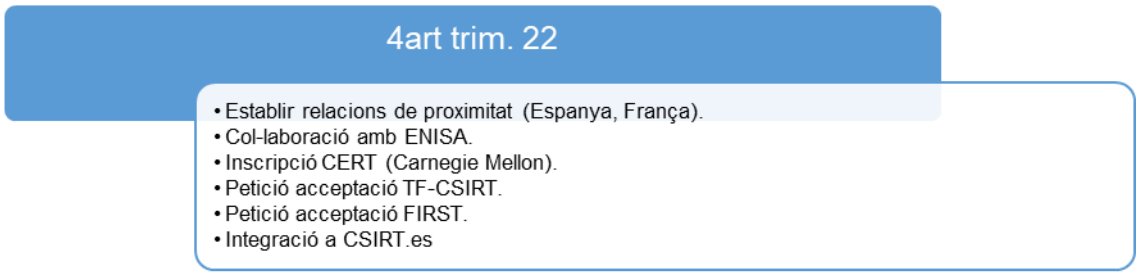
Serveis reactius d'assessorament, gestió de vulnerabilitats i incidències

Coordinació de resposta a vulnerabilitats	• Igual que al servei Comunicats setmanals, es consideren les sol·licituds de subscripció al butlletí del CSIRT-AD com a entrada que origina el consum del servei. Aquesta gestió se suportarà a través de dos elements principals: • Formulari de subscripció ubicat a la web del CSIRT-AD. • Gestor de butlletins i llistes de distribució.
Tractament d'incidents	• El procés de resposta davant d'incidents, considerant tant l'assessorament com la documentació de l'incident per part del personal del CSIRT-AD, considera una entrada clara única, que és la sol·licitud d'assessorament.

2.7 Iniciativa 7. Avaluació i ampliació de les activitats del CSIRT-AD amb enfocament internacional

Pel que fa a l'establiment de relacions internacionals amb diversos organismes en matèria de ciberseguretat, es definiran els passos que s'han de seguir per tal de formular les peticions corresponents a cada organisme.

Tots aquests organismes estan dividits en públics i privats. Un cop cadascun d'ells accepti la petició d'entrada, intercanviaran informació entre ambdós parts, fet que donarà un ampli ventall de possibilitats davant possibles incidents i una resposta ràpida .



2.7.1 CARNEGIE MELLON

La divisió CERT és líder en ciberseguretat. Col·laboren amb el Govern, la indústria, les forces de l'ordre i el món acadèmic per millorar la seguretat i la resistència dels sistemes i xarxes informàtics. Estudien problemes que tenen implicacions generalitzades en la ciberseguretat i desenvolupen mètodes i eines avançades per contrarestar les ciberamenaces sofisticades i a gran escala.
Durant l'últim trimestre el CSIRT-AD ha sol·licitat l'accés a la xarxa CERT(3), i durant el mes de novembre s'ha rebut l'acceptació oficial.

2.7.2 TF-CSIRT

El TF-CSIRT és el principal fòrum europeu de CERT(3) (les sigles en anglès d'*equip de resposta a emergències informàtiques*) en què col·laboren, innoven i comparteixen informació els CERT(3) més destacats del món.

Actualment, el CSIRT-AD està en procés d'inscripció al TF-CSIRT, finalitzant l'autoavaluació (*self-assessment*(22)) per tal de formalitzar la inscripció i la validació per part de l'organització.

2.7.3 CSIRT.ES

El CSIRT.es té com a objectiu protegir el ciberespai espanyol, intercanviant informació sobre incidents de ciberseguretat per actuar de forma ràpida i coordinada davant de qualsevol situació que pugui afectar simultàniament diferents entitats a Espanya o en el context europeu.

Aquest fòrum és una plataforma independent de confiança i sense ànim de lucre compost pels equips de resposta a incidents de seguretat CSIRT/CERT(3), l'àmbit d'actuació dels quals i la comunitat d'usuaris en què operen es troben dins del territori espanyol.

Actualment, el CSIRT-AD està en procés d'acceptació, ja que en tractar-se d'un país veí és important disposar d'informació de primera mà.

2.7.4 FIRST.ORG

El FIRST és el Fòrum d'equips de seguretat i resposta a incidents. La idea de FIRST es remunta a l'any 1989, només un any després de la creació del Centre de Coordinació CERT(3) després del famós cuc d'Internet. Aleshores, els incidents ja afectaven no només a un grup o organització tancat d'usuaris, sinó a qualsevol nombre de xarxes interconnectades per Internet.

A partir d'aleshores va quedar clar que l'intercanvi d'informació i la cooperació en qüestions d'interès mutu com ara noves vulnerabilitats o atacs d'ampli abast, especialment en sistemes bàsics com els servidors DNS o Internet com a infraestructura crítica en si mateixa, eren els problemes clau per a la seguretat i la resposta a incidents.

Des de l'any 1990, quan es va fundar el FIRST, els seus membres han resolt un flux gairebé continu d'atacs i incidents relacionats amb la seguretat, incloent-hi la gestió de milers de vulnerabilitats de seguretat que afecten gairebé tots els milions de sistemes informàtics i xarxes d'arreu del món connectats per Internet, en constant creixement.

El FIRST reuneix una gran varietat d'equips de seguretat i de resposta a incidents, incloent-hi especialment equips de seguretat de productes dels sectors governamental, comercial i acadèmic.
Actualment, el CSIRT-AD està en procés d'inscripció al FIRST i es troba en l'estadi inicial de facilitar la documentació d'inscripció.

2.7.5 COMJIB

La Conferència de Ministres de Justícia dels Països Iberoamericans (COMJIB) és una organització internacional que agrupa els ministeris de Justícia i institucions homòlogues dels 22 països de la Comunitat Iberoamericana, de què forma part Espanya, que té per objecte l'estudi i la promoció de formes de cooperació jurídica entre els estats membres.

Va néixer a Madrid el 1970 com una estructura informal de col·laboració, però ja el 1992 va adquirir carta de natura amb l'adopció del Tractat de Madrid, que la va dotar de personalitat jurídica pròpia i la va convertir en una organització internacional. Aquest tractat constitutiu ha estat ratificat fins ara per 18 dels 22 països signants, entre ells Andorra. Durant l'any 2022, l'ANC-AD va participar sobre temes d'estratègia nacional de ciberseguretat i mesures de protecció contra atacs exteriors.

2.7.6 CYBERFIRE

Fòrum dels EUA destinat a ciberexercicis, debats i cursos col·laboratius patrocinats per l'Oficina del Director d'Informació (OCIO) del Departament d'Energia (DOE) en col·laboració amb el Laboratori Nacional de Los Alamos (LANL) i altres laboratoris nacionals del DOE.

Es fan exercicis de ciberresiliència (entorn real i simulació d'incidents) en els àmbits següents:

- Arquitectura de xarxes
- OT
- Coordinació davant incidents
- Forense de sistemes
- Anàlisi de *malware*(17)

Avantatges de les aliances

Aquesta aliança en l'àmbit internacional no només reforma el compromís del Principat per crear un entorn més segur per a les entitats i els ciutadans, sinó que permet obtenir coneixement del que passa a escala global. Així mateix, dota el país d'una capacitat de resposta més ràpida, en el cas de patir algun incident de ciberseguretat, i de tota la capacitat d'actuació i resposta ràpida.

2.8 Iniciativa 8. Planificació i organització d'exercicis cibernètics nacionals i paneuropeus

Pel que fa a la planificació d'exercicis a escala nacional o en l'entorn europeu, es crearan una sèrie de proves de concepte com els de *phishing*[19] controlat, el qual evidencia l'estat de la seguretat en l'esglaó final de la cadena de ciberseguretat, que és l'usuari. També es col·laborarà en una hackató[12] anual al Principat, per tal que les entitats puguin presentar reptes per resoldre, ja sigui pels resultats de millora obtinguts o per captar talent.

D'altra banda, s'establiran ponts de col·laboració en l'àmbit internacional, per poder participar com a país en diferents exercicis en matèria de ciberdefensa.

2n trim. 2023

- Petició d'acceptació d'exercicis de ciberdefensa anuals a escala europea.
- Altres exercicis en l'àmbit global.

2.9 Iniciativa 9. Cooperació internacional amb participació als fòrums i grups de treball europeus

El CSIRT-AD elaborarà, anyalment i en cooperació amb les altres autoritats competents, un informe sobre les activitats que li permeten coordinar plenament els esforços del Principat d'Andorra per implementar, aplicar i supervisar de manera òptima totes les accions i la resposta efectiva a les amenaces que prevalen actualment al ciberespai, així com a les amenaces creixents que apareixeran al futur. Aquest estudi presentarà recomanacions al ministeri encarregat de la presidència, per permetre al CSIRT-AD coordinar plenament el gran volum de treball associat a les àrees de seguretat de la xarxa i dels sistemes d'informació i la ciberseguretat. Així mateix, formarà part de grups de treball europeus, als quals també proporcionarà informació anualment.

4t trim. 2022

- Informe anual AND-AD/CSIRT-AD.
- Participació en fòrums.

4t trim. 2023

- Informe per als grups de treball europeus.

3. Presència als mitjans de comunicació

El 20% dels ciberatacs consisteixen a 'robar' dades utilitzant l'engany

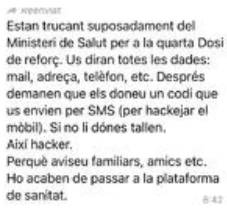
06/10/2022 Dolors Moreno Andorra la Vella

Els experts insten les empreses a invertir en formació i recursos per protegir-se

Alerta per missatges fraudulents de premis de Mercadona

30/09/2022 Redacció Andorra la Vella

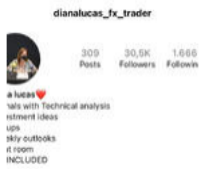
El missatge indica que la cadena de supermercats celebra el seu 45è aniversari i que es pot optar a diversos premis



Avís de trucades fraudulentes per hackejar el mòbil

28/09/2022 Redacció Andorra la Vella

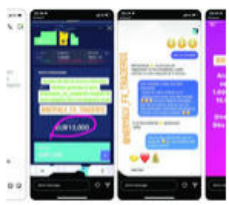
La policia assegura que a Andorra, de moment, no s'estan rebent aquestes trucades



Hackegen l'Instagram de la cònsol menor

13/09/2022 Redacció Andorra la Vella

La cònsol menor de Sant Julià de Lòria, Mireia Codina, ha estat víctima del hackeig del compte d'Instagram



Alerta pel hackeig a comptes d'Instagram

21/07/2022 Cristina Pantebre Andorra la Vella

El cos de Policia acumula nou denúncies formals de persones i càrrecs polítics del país

Alerta per intent de 'phishing' a través de Dropbox

15/06/2022 Redacció Andorra la Vella

La campanya detectada és un correu fraudulent que et redirigeix a una pàgina falsa on se't demanen les credencials per accedir a la plataforma d'emmagatzematge

L'Agència de Ciberseguretat alerta de la creació de nous virus encara més problemàtics

Notícies - 12 de juny, 2022

Atacs més avançats i complexos de defensar. Aquest és el futur que preveu l'Agència Nacional de ... [llegir més]

L'Agència de Ciberseguretat centralitzarà els atacs i garantirà els serveis essencials

Notícies - 07 d'abril, 2022

L'Agència de Ciberseguretat ha accelerat el treball amb empreses i institucions pel context geopolític actual. ... [llegir més]

SOCIETAT

Es constitueix la Comissió de seguiment del funcionament de l'Agència de Ciberseguretat

27/04/2022

SOCIETAT

L'Agència de Ciberseguretat admet que els 'atacs' als membres del Govern són habituals

07/04/2022

4. Línies d'acció de millora

4.1 Reforç de les capacitats enfront amenaces del ciberespai

Incrementar les capacitats de prevenció, defensa, detecció, anàlisi, resposta, recuperació i coordinació davant les ciberamenaces.

- Ampliar i millorar les capacitats de detecció i anàlisi de ciberamenaces.
- Potenciar la col·laboració amb els centres d'excel·lència i investigació.
- Potenciar i millorar la creació i la difusió de bones pràctiques.

4.2 Impulsar la ciberseguretat en les empreses

S'hi inclouen els serveis proactius necessaris per incrementar la resiliència del teixit empresarial del país, així com la creació d'un fòrum on hi hagi representats els diferents sectors.

- Impulsar la ciberseguretat.
- Promoure la ciberseguretat.
- Crear un fòrum nacional de ciberseguretat.

4.3 Desenvolupar una cultura de ciberseguretat

Conscienciar els ciutadans, els professionals i les empreses de la importància de la ciberseguretat.

- Incrementar les campanyes de conscienciació.
- Impulsar iniciatives i plans d'alfabetització digital.
- Promoure la conscienciació i formació.

4.4 Monitoratge i vigilància

Principalment es tracta de fer el desplegament de sondes arreu de la xarxa del país, sobretot a les infraestructures principals.

- Desplegament de *honeypots* (sondes) a les principals IC del país.
- Monitoratge i vigilància de les infraestructures.
- Implantació de sistemes de protecció.

4.5 Iniciar el desplegament d'un SOC de nivell 1 (1a fase)

Iniciar el desplegament nacional d'un SOC(23) de nivell 1 (1a fase).

- Desplegament inicial (quatre infraestructures).
- Monitoratges i advertiments.

La finalitat principal del SOC(23) és donar servei en l'àmbit de país, monitorant els esdeveniments i les amenaces que es produeixen a les principals xarxes i infraestructures del país, i donar així una capacitat de resposta molt més ràpida per tal de prevenir qualsevol intent d'accés o atac a les infraestructures i xarxes.

5. GLOSSARI DE TERMES

1. ***Bootcamp***: són programes intensius de curta durada (dies, setmanes o mesos), encara que això pot variar depenent del nivell de complexitat del curs. L'ensenyament es fa en un entorn d'aprenentatge pràctic en què s'introdueixen situacions reals de treball.
2. ***Botnet***: una xarxa de zombis (*botnet*) és una xarxa d'equips infectats que es poden controlar a distància i als quals es pot obligar a enviar correu brossa, propagar codi maliciós o dur a terme un atac DDoS, i tot sense l'autorització de l'amo del dispositiu.
3. **CERT**: un equip de resposta a emergències informàtiques o CERT (*computer emergency response team*) és un equip de persones dedicat a prevenir i detectar eficaçment els incidents de seguretat que es puguin materialitzar sobre els sistemes informàtics i a respondre-hi. L'objectiu és limitar el dany en aquests sistemes i garantir la continuïtat dels serveis que suporten.
4. **Ciberamenaça**: el concepte de *ciberamenaces* es refereix a les activitats "malignes" que tenen lloc en un entorn digital, ja sigui en un ordinador de sobretaula o portàtil, en un mòbil o en una tauleta.
5. **Ciberseguretat**: la ciberseguretat fa referència a la protecció dels dispositius connectats a Internet, com ara ordinadors, dispositius mòbils i electrònics, servidors, xarxes i dades, dels atacs cibernètics
6. **CSIRT**: un equip de resposta a incidents de seguretat (CSIRT) és una organització responsable de rebre i revisar informes i activitat sobre incidents de seguretat i de respondre-hi.
7. ***Dark web***: el web fosc (*dark web*) és el conjunt ocult de llocs d'Internet als quals només es pot accedir mitjançant un navegador web especialitzat. S'utilitza per

mantenir l'activitat d'Internet privada i l'anonimat, cosa que pot ser útil tant en aplicacions legals com il·legals.

8. **DDos:** un atac DDoS, o atac distribuït de denegació de servei, és un tipus de ciberatac que intenta fer que un lloc web o recurs de xarxa no estigui disponible col·lapsant-lo amb trànsit malintencionat perquè no pugui funcionar correctament.
9. ***Forensic***: la informàtica forense és una disciplina que consisteix a extreure, preservar i analitzar evidències quan es produeix una bretxa de seguretat en sistemes informàtics, xarxes, dispositius mòbils, correus electrònics o discos durs, entre d'altres.
10. ***Framework***: un *framework* és un entorn o marc de treball, un conjunt de pràctiques, conceptes i criteris estandarditzats que cal seguir. Seguint unes regles, el *framework* ens obliga a fer servir bones pràctiques per al nostre codi. D'altra banda, els *frameworks* també ens proporcionen una sèrie d'eines ja desenvolupades.
11. **GCI**: l'Índex de ciberseguretat global (Global Cybersecurity Index – GCI) és una iniciativa de la Unió Internacional de Telecomunicacions (UIT). És un índex compost per mesurar el compromís dels estats membres de la UIT.
12. **Hackató**: en el significat més pràctic, una hackató és un esdeveniment d'innovació en què diferents persones es reuneixen per crear i dissenyar solucions a una o més problemàtiques que hi ha en la societat actualment o dins d'una empresa o organització.
13. ***Information stealers***: un tipus de programa maliciós (*malware*) dedicat a robar la nostra informació és el conegut com a *stealer* o *infostealer*.
14. **IOC**: un indicador de compromís o *indicator of compromise* (IOC) és un terme que s'utilitza per parlar de qualsevol rastre o evidència que indiqui que s'ha accedit sense autorització a un sistema de dades.
15. ***Insider*:** podem definir un atac d'*insider* com el que es fa mitjançant un empleat intern d'una empresa. Aquest tipus d'atac es pot produir perquè el ciberatacant s'ha posat en contacte per subornar l'empleat o la iniciativa pròpia.
16. **Filtració d'informació (*leak*)**: en aquest cas ens referim a una fugida d'informació i dades, que es poden publicar a Internet. Podria afectar lògicament la privadesa dels usuaris i d'organitzacions o empreses.
17. ***Malware***: el terme *malware* fa referència al programari maliciós i inclou qualsevol sistema de programari que afecti els interessos de l'usuari. No només

pot afectar l'ordinador o el dispositiu infectat, sinó també qualsevol altre amb què es comuniqui.

18. **OT**: la tecnologia operativa (TO/OT) consisteix a utilitzar el programari i el maquinari per controlar els equips industrials, i inclou els sistemes especialitzats que s'utilitzen als sectors de la fabricació, l'energia, la medicina i la gestió dels edificis, entre d'altres.
19. ***Phishing***: suplantació d'identitat o pesca per correu electrònic. El *phishing* és un mètode per enganyar i fer que l'usuari comparteixi contrasenyes, números de targeta de crèdit i altra informació confidencial fent-se passar per una institució de confiança en un missatge de correu electrònic.
20. ***Ransomware***: el programari de segrest o *ransomware* és un tipus de codi maliciós que xifra els arxius i fins i tot sistemes informàtics sencers per després demanar el pagament d'un rescat a canvi de tornar l'accés, que generalment s'ha de fer amb criptomoneda.
21. ***Reversing***: la inversió o *reversing* és la tècnica per excel·lència per analitzar el comportament de les aplicacions malicioses quan no es disposa del codi font.
22. ***Self-assessment***: l'avaluació de la qualitat, i especialment l'autoavaluació de les escoles, constitueix un element clau en el desenvolupament d'un ensenyament de qualitat.
23. **SOC**: un centre d'operacions de seguretat (*security operations center* en anglès) s'encarrega de protegir una organització contra les amenaces cibernètiques. Els analistes del SOC fan un seguiment permanent de la xarxa d'una organització i investiguen qualsevol possible incident de seguretat.
24. ***Spam***: el correu brossa és qualsevol forma de comunicació no sol·licitada que s'envia de forma massiva (correu electrònic massiu no sol·licitat).
25. **TLP**: TLP és un esquema simple i intuïtiu per indicar com n'és de sensible la informació sobre ciberseguretat que serà compartida i per facilitar la col·laboració amb altres entitats o organitzacions a escala nacional i internacional.