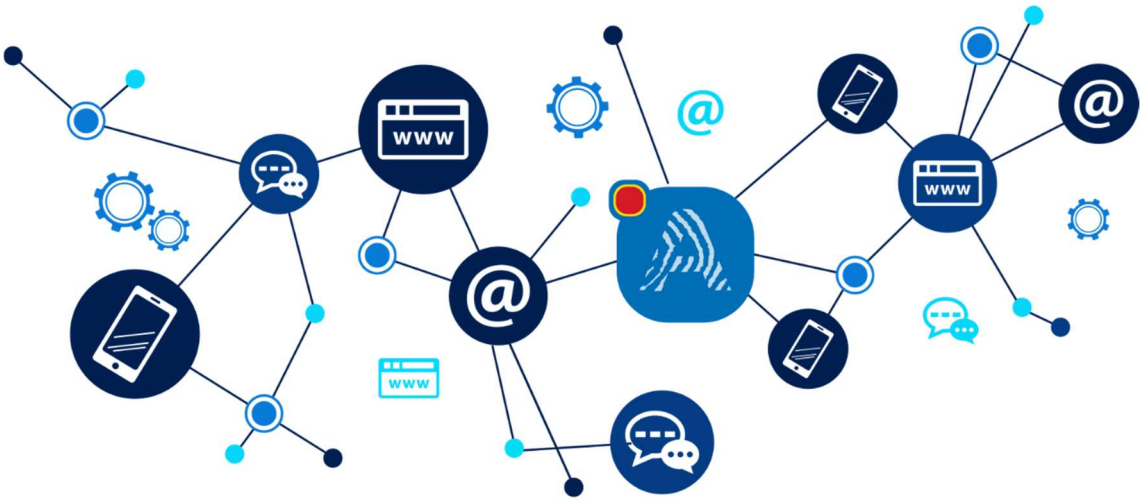
ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

# Memòria anual ANC-AD / CSIRT-AD 2023




Abril del 2024

Fitxa del document

| **Títol** | Memòria anual 2023 ANC-AD / CSIRT-AD |
|---|---|

| Versió | Redactat/revisat per | Aprovat per | Data d'aprovació | Data de publicació |
|---|---|---|---|---|
| | | | | |
| 1.0 | ANC-AD | ANC-AD | 3-2024 | 4-2024 |

| Registre de canvis | | | |
|---|---|---|---|
| Versió | Pàgines | Data de modificació | Motiu del canvi |
| | | | |
| | | | |
| | | | |

**Propietari del document**: ANC-AD

# ÍNDEX

## Pròleg

La irrupció de la digitalització ha provocat un canvi de paradigma irreversible en la manera com ens relacionem i interactuem, i afecta transversalment tots els àmbits de la nostra vida, des del cultural i el social fins a l'econòmic. Aquesta transformació comporta noves formes de comunicació, consum, treball i oci, i presenta tant oportunitats com reptes que cal afrontar per construir una societat més justa, sostenible i equitativa.

La consolidació de les noves formes de relació i interacció en el nostre dia a dia s'ha vist impulsada per diversos factors. Entre ells destaca la ràpida evolució de les tecnologies, que ha donat lloc a noves eines i plataformes digitals. A més, la proliferació de serveis digitals ha facilitat l'accés a aquestes tecnologies per a un públic més ampli. Finalment, l'optimització de les infraestructures de xarxa ha garantit una interconnexió fiable i de gran velocitat, indispensable per a l'ús fluid d'aquestes noves formes de relació i interacció.

Els factors que impulsen el canvi digital són elements imprescindibles per a la nostra evolució i no podem plantejar-nos un retrocés. La seva acceleració i expansió són necessàries per seguir avançant en la transformació digital, que ja ha impregnat tots els àmbits de la nostra vida. La dependència d'aquests elements és cada vegada més gran, tant en termes d'evolució com de funcionament, per a negocis, comunicacions, transport, finances, l'Administració i la societat en general. La protecció dels serveis i les infraestructures associades es converteix, per tant, en un factor d'alt risc que hem d'abordar de manera responsable per garantir un futur digital segur i pròsper.

L'accessibilitat i la utilització dels actius digitals esdevenen crítiques, i converteixen la seva protecció i salvaguarda en un objectiu d'interès nacional. La necessitat d'un entorn segur i estable no es limita a l'àmbit local, ja que la disfunció o el bloqueig d'aquests serveis pot tenir un impacte important en l'economia global, afectar les operacions diàries i fins i tot danyar la reputació d'un país. Per tant, la protecció d'aquests elements és una responsabilitat compartida que exigeix la col·laboració internacional per garantir un futur digital segur i pròsper per a tothom.

Andorra, com el món sencer, està experimentant canvis profunds en els seus models i formes de fer. La creació d'un ecosistema digital és crucial per promoure noves formes d'interacció, agilitzar i fer més eficients els processos, potenciar l'autogestió i, en definitiva, crear nous formats de relació entre organismes, empreses i persones.

Aquest ecosistema digital ha de tenir com a centre la persona i la societat, respectant la seva seguretat, privacitat i llibertats. La interconnexió, la interoperabilitat i la transparència de la informació són claus per garantir una societat innovadora i competitiva, però protegida sota un marc segur i estable que minimitzi vulnerabilitats externes i asseguri les llibertats fonamentals.

A més, l'ecosistema ha d'estar alineat amb les millors pràctiques internacionals i convertir-se en un avantatge competitiu en l'acostament d'Andorra a la Unió Europea.

En resum, la construcció d'un ecosistema digital segur, transparent i centrat en la persona és crucial per garantir el futur pròsper i competitiu d'Andorra en el context global.

L'augment de la delinqüència professional en l'espionatge econòmic i polític digital, juntament amb el creixement de països que desenvolupen capacitats d'atac digital, exigeix un reforç de la ciberseguretat per protegir els interessos vitals d'Andorra. L'Estratègia nacional de ciberseguretat defineix el marc que s'ha de seguir, establint els principis, les estratègies i les iniciatives necessàries per fer front a la

vulnerabilitat del ciberespai. Aquesta estratègia fixa la posició d'Andorra davant les amenaces digitals, garantint la protecció dels seus ciutadans i infraestructures crítiques.

Durant l'any 2023, Andorra ha assolit una fita important en matèria de ciberseguretat amb la certificació de totes les empreses afectades per la Llei 22/2022, de ciberseguretat i els decrets associats 417/2022 (ENS-AD) i 418/2022 (RIC-AD).

Aquesta fita s'ha aconseguit gràcies al treball conjunt de l'Agència Nacional de Ciberseguretat amb les empreses i els professionals del sector.

Cal destacar el gran esforç tècnic, econòmic i humà fet per totes les entitats i administracions públiques, parapúbliques i del sector privat subjectes a la Llei, per assolir el nivell de maduresa en ciberseguretat exigit en el marc legal abans de la data límit, el 9 de desembre del 2023.

Aquesta certificació garanteix que les entitats essencials i importants del país disposen dels estàndards de seguretat necessaris per protegir-se dels ciberatacs, a la vegada que augmenta la confiança dels clients i usuaris en els seus serveis digitals.

Val a dir que aquest és el primer pas obligatori per assolir un augment del nivell de ciberresiliència d'Andorra en el seu conjunt.

Això significa que Andorra està avui més preparada per afrontar els reptes de la ciberseguretat actual i futura, més que ahir però menys que demà. I cal continuar treballant de forma activa per millorar el nostre grau de maduresa en ciberseguretat en aquestes entitats essencials i importants, però també en la resta del teixit empresarial del país.

Marc Rossell Soler
Secretari d'Estat de Transformació Digital i Telecomunicacions

# Resum executiu

Andorra es troba en un moment en què té el repte de continuar amb la segona part del programa de transformació digital (PdTDA), de forma holística per al país a través d'un dels pilars fonamentals: la ciberseguretat, 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 proveeix d'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 a escala global, 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. Aquesta característica 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, així com per protegir la ciutadania, 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, i de la resta del món.

Malgrat que les iniciatives de seguretat de les xarxes i dels sistemes d'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 ha permès identificar les infraestructures i els operadors crítics, establir un marc legal que afavoreix 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 diferents iniciatives dutes a terme durant l'any 2023, així com els propers passos a seguir, la priorització i la planificació de la ciberseguretat nacional, i l'avaluació dels resultats de les diferents iniciatives de l'Estratègia. L'Estratègia nacional de ciberseguretat del Principat d'Andorra s'ha de revisar periòdicament, almenys un cop cada quatre anys, tal com es detalla a la Llei 22/2022, tenint en compte els resultats del procés d'avaluació, així com les noves amenaces que apareguin (i continuïn apareixent) al ciberespai. Els objectius són fer una avaluació integral dels resultats de les iniciatives anteriors i actualitzar l'Estratègia per tal que continuï en condicions de proporcionar el màxim benefici a la societat andorrana.

## El 2023 en xifres

**3077**
Visites al lloc web

**287**
Notícies web / XS publicades


**2092**
Alertes de vulnerabilitats publicades

**164**
Subscriptors Butlletí

**32**
Subscriptors alertes vulnerabilitats

**24**
Píndoles de conscienciació disponibles al lloc web

**630**
Descàrregues del lloc web

**32**
Materials de suport disponibles

**277**
Incidents gestionats (30 crítics)

### Segrest de comptes de xarxes socials

Durant l'any 2023, s'han detectat sis campanyes d'intent de segrest de comptes de xarxes socials al Principat, 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], *phishing*, pèrdua de dades, etc.

### Programari maliciós Racoon

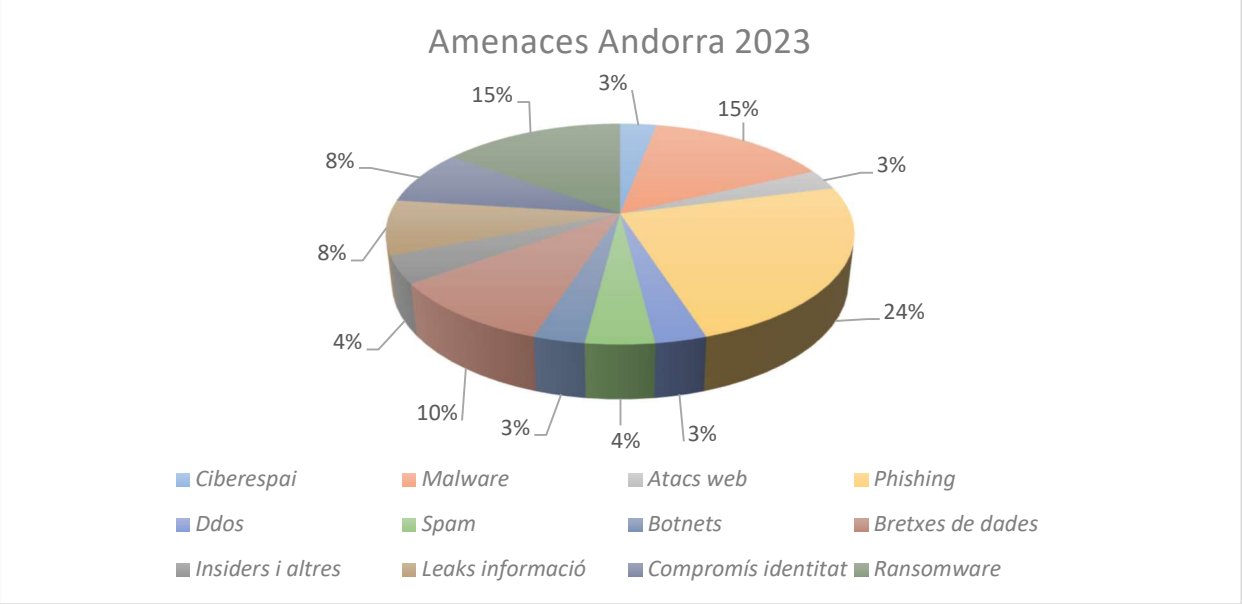
Racoon, una variant recent del *stealer* RedLine, ha guanyat popularitat l'any 2023. A diferència de RedLine, Racoon s'ofereix de forma gratuïta, i així facilita l'accés a actors de tots els nivells. A més de les funcions de RedLine, com el robatori de contrasenyes, dades de navegació i informació personal, Racoon incorpora noves capacitats com la captura de captures de pantalla i l'enregistrament de vídeo. La seva facilitat d'ús i eficiència en la recopilació de dades sensibles converteixen Racoon en una amenaça important per a la privacitat i la seguretat dels usuaris.

Com protegir-se de Racoon:

Actualitza el teu software: mantenir actualitzat el sistema operatiu i el programari antivirus és crucial per protegir-se de les amenaces més recents.
Implementa una política de contrasenyes segura: utilitza contrasenyes úniques i complexes per a cada compte per mitigar el risc d'accés no autoritzat.
Evita descàrregues sospitoses: no descarreguis fitxers de fonts no fiables ni cliquis en enllaços sospitosos per prevenir la infecció per Racoon.
En resum, Racoon és un *stealer* en auge que representa un risc important per a la privacitat i la seguretat dels usuaris. La implementació de mesures de protecció i la conscienciació sobre els riscos són crucials per mitigar l'impacte d'aquesta amenaça.

### *Leaks*[16] i filtracions de dades

Durant l'any 2023, ha augmentat un 38% la publicació i la filtració de dades personals d'usuaris. Aquest augment deriva de la infecció de dispositius personals per *malware*.




**Continua la disminució dels casos de *ransomware***

Tot i que el nombre d'atacs ha augmentat en un percentatge moderat, l'amenaça per programari de segrest ha baixat puntualment durant l'últim 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 2022) a un 70% de primera generació i un 30% 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).

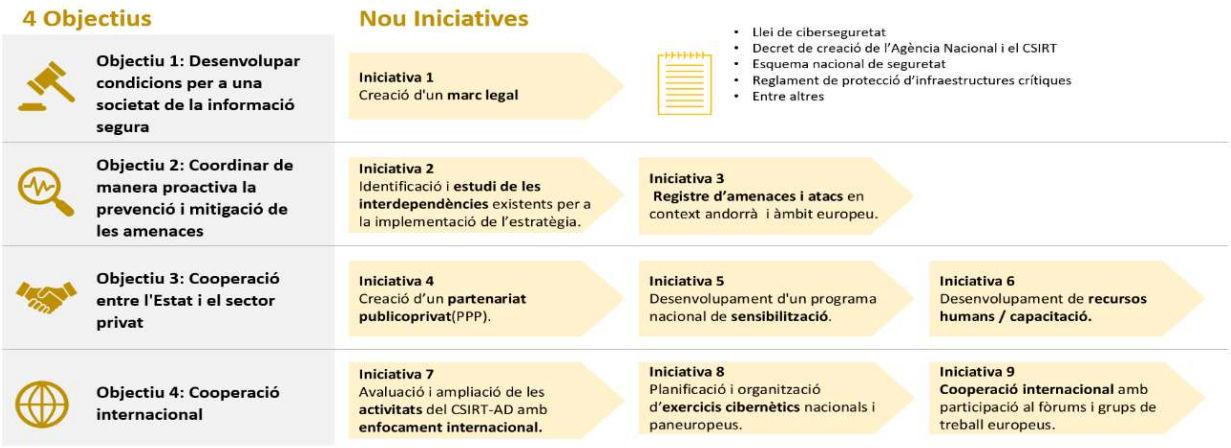




Fig. 1. Nivells d'actuació i les nou iniciatives de l'Estratègia nacional de ciberseguretat

# 2. Estat de les iniciatives

## 2.1 Iniciativa 1. Aplicació del marc legal

L'aplicació del marc legal ha permès que les entitats afectades per la Llei 22/2022 hagin arribat a la data 9-12-2023 amb l'acompliment dels requeriments marcats, el total de les entitats ha assolit el nivell de maduresa exigit per l'Esquema nacional de seguretat (ENS-AD) i han dotat el conjunt del país d'un nivell de ciberresiliència molt més elevat.

### 2.1.1 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 ciberdelictes 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:

- Vetlla en matèria de ciberseguretat nacional pels serveis essencials i importants, juntament amb el CSIRT-AD i amb el vistiplau de la Comissió de Seguiment.
- Actua com a 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 de professionals en l'àmbit educatiu 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, així com també hi col·labora, 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.

A més a més, 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:

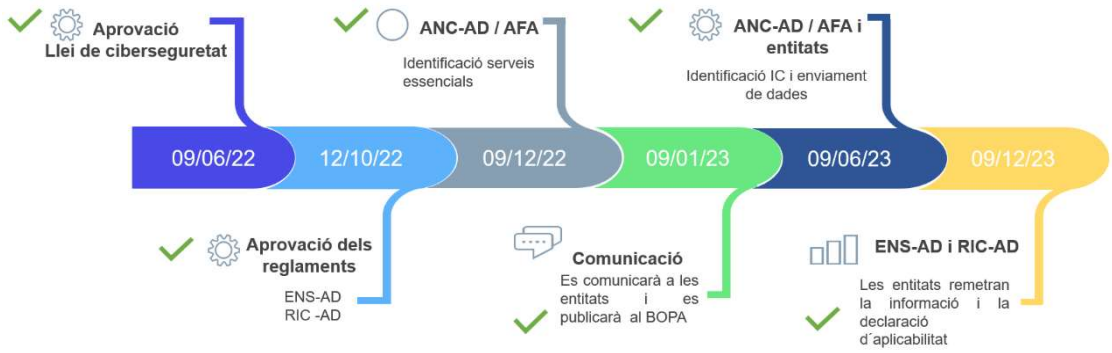
- Dona resposta a incidents de seguretat en les xarxes i els sistemes d'informació.
- Supervisa i dona suport a la resolució dels incidents de seguretat en les xarxes i els sistemes d'informació.
- Difon alertes imminents, avisos i informacions sobre incidents de seguretat en les xarxes i els sistemes 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 recomanacions amb relació a virus extremadament estesos.

### 2.1.2 Què és el CSIRT-AD

El CSIRT-AD és l'òrgan competent principal 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 el 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 dels mecanismes 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 la 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 són 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 és objecte de revisió i d'avaluació almenys cada quatre anys (prevista, tal com detalla la Llei 22/2022, durant aquest 2024), 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

Dins la identificació, i per seguir amb l'Estratègia nacional de seguretat, es continuen desenvolupant les tasques i les implementacions de serveis, que van des del portal web (el punt principal d'entrada als serveis de l'ANC-AD / CSIRT-AD) 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 el Cos de Policia d'Andorra.

D'altra banda, durant el 2023 s'ha iniciat el càlcul de l'índex de ciberseguretat (GCI) de l'organització ITU (agafant els principals indicadors segons les característiques del Principat) en matèria de ciberseguretat actual, amb una revisió posterior passat un any des del primer càlcul.

| Nom del país | Puntuació | Classificació |
|---|---|---|
| EUA | 100 | 1 |
| GB | 99,54 | 2 |
| Aràbia Saudita | 99,54 | 2 |
| Estònia | 99,48 | 3 |
| República de Corea | 98,52 | 4 |
| Singapur | 98,52 | 4 |
| Espanya | 98,52 | 4 |
| | ..... | ..... |
| Andorra | 26,38 | 117 |

Font: ITU 2021

Objectiu 2023-2024: posicionar Andorra al top 50 (>80 punts)

## 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 de les alertes rebudes i els serveis per a la gestió d'incidents enfocats a entitats i a la ciutadania, i posteriorment l'ANC-AD complementarà amb 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 el Cos de Policia d'Andorra.

## 2.4 Iniciativa 4. Creació d'un partenariat publicoprivat (PPP)

Continuem la cooperació amb les autoritats competents existents que determinen 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.

L'Agència Nacional de Ciberseguretat d'Andorra (ANC-AD) ha impulsat la formalització d'un protocol per gestionar de forma eficient i efectiva la gestió d'incidents relacionats amb la ciberseguretat. L'entesa, que s'ha signat juntament amb Andorra Telecom i el Cos de Policia, formalitza uns mecanismes que fins a la data ja es portaven a terme.

Així, el protocol estableix els mecanismes i els passos que cal seguir quan es rebi una notificació sobre un possible incident. En cas que apliqui la gestió conjunta de l'incident per dos de les parts, es registrarà la informació reportada i s'establirà una prioritat al cas i posteriorment s'iniciaran les accions necessàries per a la resolució de l'incident.

D'altra banda el CCN-CERT i l'Agència Nacional de Ciberseguretat d'Andorra (ANC-AD) han signat un acord de col·laboració amb l'objectiu d'intercanviar informació tècnica en matèria de ciberseguretat.

L'aliança pretén regular la col·laboració entre totes dos entitats i intercanviar sinergies durant els incidents de seguretat dels sistemes, serveis i xarxes, compartint informació tècnica i procediments de resolució.

L'acord, que també preveu l'intercanvi de formació i bones pràctiques en aquesta matèria, estableix que el CCN-CERT i l'ANC-AD es donin suport mútuament en el desenvolupament de programes i projectes relacionats amb la ciberseguretat.

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

En aquest apartat es pretén avançar i teixir un programa per tal de sensibilitzar entitats i població en matèria de ciberseguretat, amb l'ampliació de les publicacions recurrents 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, mitjançant exercicis tipus CTF (capture the flag).

## 2.5.1 Píndoles formatives per a empreses i 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 2023 l'ANC-AD ha participat en diverses jornades de sensibilització i formació per a diferents entitats.

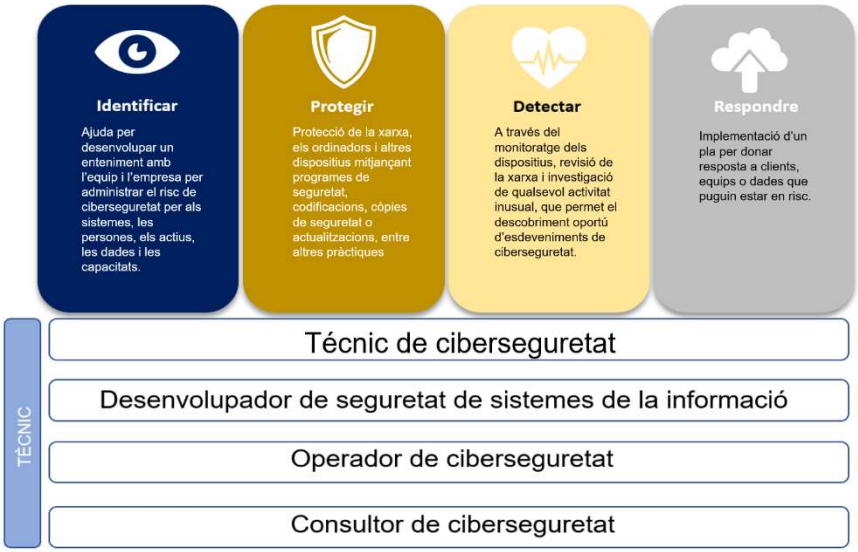
Les xarxes socials afecten de diferents formes la ciutadania, i aquest impacte es multiplica quan es parla de les famílies. A través de les píndoles de conscienciació l'ANC-AD, per una banda, vol ajudar a donar a conèixer quina és la manera de fer-ne un ús segur i saludable i, per l'altra, tracta altres 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.

Durant el 2023, també s'ha posat especial atenció en el col·lectiu de la gent gran i el de les persones amb discapacitat a través de la publicació de continguts específics en l'apartat de píndoles de conscienciació.

### 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:

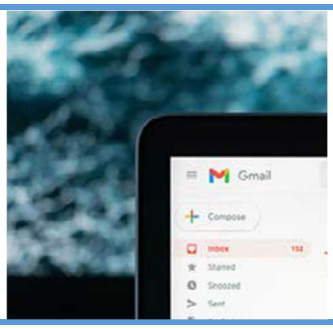



## 2.5.4 Consells de ciberseguretat

### 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 impedeixi 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, conscient 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 2022 el nombre total de jugadors va ser de 18,9 milions i una de cada quatre persones jugadores (26%) té entre 6 i 14 anys.

La proliferació 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-hi 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-los 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.

Actualització de dades sobre l'accés a continguts inapropiats per a menors a Europa (2023)

- Estudi EU Kids Online 2022:
  - 29% dels nens i adolescents europeus (9-16 anys) han estat exposats a contingut pornogràfic a internet.
  - 18% han estat exposats a contingut violent a internet.
  - 12% han estat exposats a discursos d'odi a internet.

- Informe d'UNICEF sobre la situació dels infants a Europa 2021:
  - Els nens i adolescents europeus estan cada vegada més exposats a continguts inapropiats a internet.
  - La pornografia, la violència i els discursos d'odi són els continguts inapropiats més comuns als quals s'exposen els nens i adolescents a internet.
  - Aquesta exposició pot tenir un impacte negatiu en el desenvolupament dels nens i adolescents.

**Tendències**:

- Augment de l'exposició a continguts inapropiats a internet entre els nens i adolescents.
- Augment del risc d'exposició a continguts inapropiats per a menors a través de les xarxes socials.
- Augment de la ciberseducció de menors (*grooming*) a través de internet.

**Consells per a famílies i educadors**:

- Parleu amb els vostres fills sobre els riscos d'internet.
- Ensenyeu-los a navegar per internet de manera segura.
- Utilitzeu controls parentals per limitar l'accés a continguts inapropiats.
- Superviseu l'activitat dels vostres fills a internet.
- Denuncieu qualsevol contingut inapropiat que vegeu a internet.

És important recordar que l'accés a continguts inapropiats per a menors a internet és un problema greu que requereix una resposta conjunta a escala europea. Cal que governs, escoles, famílies i tota la societat treballin plegats per prevenir-lo i abordar-lo de manera efectiva.

Recursos addicionals específics per a Europa:

- Guia de la Comissió Europea sobre els drets dels nens en l'entorn digital.
- Xarxa europea per a la seguretat dels infants a internet.

Recordeu que la protecció dels nens i adolescents a internet és una responsabilitat de tots.

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 en 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.).

### Augment de casos de *malware*:

Durant l'últim any ens hem trobat davant d'un augment preocupant de les infeccions per dos tipus de *malware* especialment perillosos: Racoon i Lumma. Aquestes variants de programari maliciós tenen com a objectiu principal robar dades sensibles dels usuaris, com ara contrasenyes, informació bancària i dades personals, fet que pot causar greus perjudicis a l'usuari.

Racoon actua com un troià, infiltrant-se silenciosament en dispositius mòbils o ordinadors a través d'aplicacions aparentment inofensives descarregades de fonts no fiables o enllaços maliciosos camuflats en correus electrònics fraudulents. Un cop instal·lat, opera en la clandestinitat robant

contactes, fotos, missatges de text i, el més preocupant, accés a dades bancàries per realitzar transaccions no autoritzades.

D'altra banda, Lumma és un tipus de *ransomware*, un programari maliciós que pren els fitxers de la víctima com a ostatges, xifrant-los i fent-los inaccessibles. Els ciberdelinqüents exigeixen posteriorment un pagament a canvi de desxifrar la informació segrestada, i causen un gran impacte personal i empresarial en impedir l'accés a documents crucials, fotos irreemplaçables i altres arxius valuosos. Per tal de protegir-se d'aquestes amenaces, els experts recomanen als usuaris extremar les precaucions i seguir una sèrie de passos fonamentals: instal·lar un antivirus i un *antispyware* de confiança i mantenir-los sempre actualitzats, baixar aplicacions únicament de fonts oficials, desconfiar de correus electrònics sospitosos i no clicar en enllaços o adjunts desconeguts, actualitzar regularment el sistema operatiu i les aplicacions amb els últims pegats de seguretat per cobrir vulnerabilitats, i finalment, però no menys important, realitzar còpies de seguretat periòdiques dels arxius importants per disposar sempre d'un pla de contingència en cas d'infecció.

No obstant, si malgrat totes les precaucions un dispositiu resulta infectat, cal actuar amb rapidesa per minimitzar els danys. En primer lloc, cal desconnectar immediatament el dispositiu d'internet per evitar que el *malware* pugui transmetre les dades robades. Seguidament, s'ha d'escanejar el dispositiu amb un antivirus potent per eliminar el programari maliciós. Un cop eliminat, és imprescindible canviar les contrasenyes de tots els comptes compromesos, tant bancaris com de correu electrònic i xarxes socials per garantir-ne la seguretat. Finalment, davant d'un atac d'aquestes característiques, és recomanable denunciar l'incident a les autoritats competents per tal de fer front a aquest tipus de ciberdelinqüència. La ciberseguretat és una responsabilitat compartida i si seguim aquestes consells i mantenim una actitud prudent a la xarxa, podem minimitzar els riscos associats al *malware* Racoon, Lumma i a altres amenaces que ronden constantment per l'espai digital.

## 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

Per combatre les amenaces digitals en constant evolució, els serveis proactius de gestió, comunicació i formació en ciberseguretat ofereixen una protecció multicapa. Implementen un sistema basat en normes internacionals per gestionar la seguretat de la informació. Auditories regulars i avaluacions de vulnerabilitats identifiquen i mitiguen riscos abans d'un atac. La comunicació és clau: s'elabora un pla per a tota l'organització amb campanyes de sensibilització i un canal de report d'incidents sospitosos.

La formació és essencial. S'ofereixen programes adaptats a cada nivell, tallers i simulacres per mantenir els empleats preparats. Actualitzats constantment, aquests programes garanteixen la protecció davant les últimes tàctiques dels ciberdelinqüents. En resum, aquests serveis no només redueixen el risc d'incidents sinó que fomenten una cultura de ciberseguretat sòlida, protegint dades, augmentant la confiança i garantint el compliment legal.

| | |
|---|---|
| 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.<br>• Durant el 2024 es posarà en funcionament un servei de MISP per a les empreses i entitats del país. |

### Serveis reactius d'assessorament, gestió de vulnerabilitats i incidències

Quan s'inicia un incident de ciberseguretat, els serveis reactius d'assessorament, gestió de vulnerabilitats i incidències entren en acció. Els experts avaluen els danys i recomanen mesures per contenir-los, a més d'oferir assessorament legal. S'identifiquen i es corregeixen les vulnerabilitats que

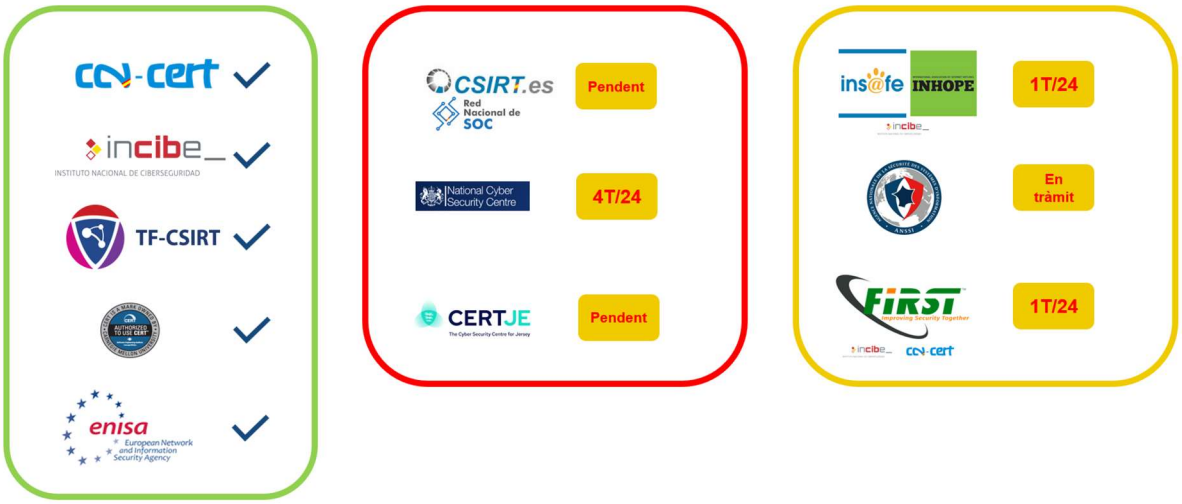
van permetre l'atac per prevenir futures intrusions. La investigació de l'incident i la recuperació dels sistemes afectats són accions prioritàries, cal assegurar una resposta ràpida per minimitzar l'impacte i salvaguardar la imatge de l'organització.

| | |
|---|---|
| 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:<br>• El formulari de subscripció ubicat a la web del CSIRT-AD.<br>• El gestor de butlletins i llistes de distribució. |
| Tractament d'incidents | • El procés de resposta davant d'incidents, 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

Pel que fa a l'establiment de relacions internacionals amb diversos organismes en matèria de ciberseguretat, es segueix amb els passos definits per a la formulació de les peticions que corresponen 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·labora 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. Estudia problemes que tenen implicacions generalitzades en la ciberseguretat i desenvolupa mètodes i eines avançades per contrarestar les ciberamenaces sofisticades i a gran escala.
Actualment es disposa de l'adhesió a aquest organisme.

## 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 inscrit al TF-CSIRT.

## 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 un grup o organització tancat d'usuaris, sinó 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'abast ampli, 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.

CONFERENCIA DE MINISTROS DE JUSTICIA
DE LOS PAÍSES IBEROAMERICANOS
COMJIB

### 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]

### 2.7.7 OSCE

Durant l'any 2023, l'ANC-AD ha participat en diferents sessions i fòrums tècnics a l'OSCE.

L'Organització per a la Seguretat i la Cooperació a Europa (OSCE) reconeix la ciberseguretat com un pilar fonamental per a la seguretat i la cooperació en l'era digital. En aquest context, l'OSCE ha desenvolupat un marc integral per abordar els desafiaments de la ciberseguretat, que inclou:

**1. Promoció de normes i principis**:

- L'OSCE ha adoptat diversos documents que defineixen normes i principis de comportament responsable en l'espai cibernètic, com el Document de Viena sobre ciberseguretat (2013) i les Directrius de l'OSCE sobre la implementació del Document de Viena (2015). Aquests documents promouen la cooperació entre els estats membres, la confiança mútua i la prevenció de conflictes en l'espai digital.

**2. Assistència tècnica i capacitació**:

- L'OSCE ofereix assistència tècnica i programes de capacitació als seus estats membres per enfortir les seves capacitats nacionals en ciberseguretat.
- Això inclou assessorament en legislació, creació d'equips de resposta a incidents cibernètics i formació en investigació de delictes cibernètics.

**3. Diàleg i cooperació:**

- L'OSCE facilita el diàleg i la cooperació entre els seus estats membres sobre qüestions de ciberseguretat.

- Això es fa a través de fòrums, reunions d'experts i grups de treball, com el Fòrum OSCE sobre ciberseguretat.
- L'objectiu és fomentar la confiança mútua, compartir informació i coordinar respostes a incidents cibernètics.

**4. Lluita contra el cibercrim**:

- L'OSCE treballa per combatre el cibercrim, incloent el ciberterrorisme, la distribució de contingut il·legal en línia i els atacs a infraestructures crítiques.
- L'OSCE coopera amb altres organitzacions internacionals, com la Interpol i l'Agència Europea de Seguretat de les Xarxes i la Informació (ENISA), per perseguir els delinqüents cibernètics i prevenir els delictes cibernètics.

**5. Protecció de la infraestructura crítica**:

- L'OSCE reconeix la importància de protegir la infraestructura crítica, com ara les xarxes elèctriques i els sistemes de transport, dels atacs cibernètics.
- L'OSCE treballa amb els seus estats membres per desenvolupar estratègies i plans de protecció de la infraestructura crítica.

En resum, l'OSCE juga un paper important en la promoció de la ciberseguretat a Europa i Àsia. La seva tasca es basa en la cooperació internacional, la promoció de normes i principis, la capacitació i el diàleg. L'objectiu final és crear un espai cibernètic més segur i estable per a tots.

**Avantatges de les aliances**
Aquesta aliança en l'àmbit internacional no només referma 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

Pel que fa a la planificació d'exercicis a escala nacional o en l'entorn europeu, es crearan una sèrie de proves de concepte, que evidenciaran l'estat de la seguretat en l'esglaó final de la cadena de ciberseguretat.

Durant el 2023 es va participar als exercicis Cyberex, organitzats per Incibe, i amb més de 82 equips a escala mundial.

Per part del Principat d'Andorra, es van presentar quatre equips i després de sis hores d'exercicis i reptes, un d'ells va aconseguir una molt bona setena posició.

| Pos. | Name | Country | Points | Challenges completed |
|---|---|---|---|---|
| 1 | YoloSw4g | | 6187 | 10 |
| 2 | CERTUNLP | | 3600 | 7 |
| 3 | KMH | | 3600 | 7 |
| 4 | F4ctum-H4ckr0cks | | 2850 | 6 |
| 5 | Rhampholeon | | 2550 | 6 |
| 6 | Moose Marauders | | 1800 | 4 |
| 7 | TamarrouLand | | 1800 | 5 |
| 8 | NullSec | | 1800 | 5 |
| 9 | AIR Security | | 1762 | 5 |
| 10 | Cossacks Blade | | 1650 | 3 |

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.

## 2.9 Iniciativa 9. Cooperació internacional

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 en el 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.

## 3. Presència als mitjans de comunicació

### Una quarantena d'experts en ciberseguretat assisteixen a la jornada CISO

*Divendres, 16 Desembre 2022*

---

Actualitzada 06/02/2023 a les 21:26 Redacció Andorra la Vella

La policia informa que l'Agència Nacional de Ciberseguretat d'Itàlia alerta d'un atac global de pirateria de *ransomware*, que pot afectar principalment empreses. Per això, el cos de seguretat recorda que si es té un empresa s'ha de mantenir els sistemes actualitzats.

En aquest sentit, l'atac de pirateria buscava explotar una vulnerabilitat de programari. Per això, és probable que dotzenes d'organitzacions italianes s'hagin vist afectades i es va advertir a moltes més que prenguessin mesures per evitar ser bloquejades dels seus sistemes. A més del país transalpí, també es van veure afectats els Estats Units, França, Finlàndia i el Canadà. En aquesta línia, funcionaris de seguretat cibernètica dels EUA van dir que estaven avaluant l'impacte dels incidents reportats.

---

### Andorra va patir l'any passat més de 4.500 atacs hacker

Noticies » Societat 06 de febrer, 2023

---

### Creixen els delictes relacionats amb la publicació i filtració de dades personals a internet

Noticies » Societat 11 d'abril, 2023

---

**L'Agència Nacional de Ciberseguretat alerta d'una onada d'atacs conegut com a botnet a Europa. Són ofensives que infecten dispositius que hi ha a casa i que després provoquen atacs com el que va viure Andorra Telecom.**

La **televisió**, la **càmera de vigilància** o, fins i tot, la **impressora** que tenim a casa podrien ser les causants de milers d'atacs **hacker arreu del món**. Així ho ha alertat el responsable de l'Agència Nacional de Ciberseguretat, **Jordi Ubach**, a l'Obert per Vacances on ha explicat que Europa està vivint una onada massiva d'atacs **botnet**. Què és això? Respon Ubach:

---

### Andorra Telecom organitza, el 27 d'abril, una jornada dedicada al Dia de les noies a les TIC

Noticies 12 d'abril, 2023

CIBERSEGURETAT

## 'Spear phishing' l'estafa que afecta les empreses

Andorra Digital va organitzar una sessió informativa en línia per a les PIMES



## L'ANC posa en marxa un servei d'alertes sobre vulnerabilitats per a les empreses

1/6/2023

S'accedeix via subscripció i és gratuït

> NACIONAL

TECNOLOGIA

## Servei d'alertes de ciberseguretat dirigit a l'empresa

L'Agència Nacional posa a disposició del sector empresarial una eina d'informació

SUCCESSOS | 07/08/2023

## Intent d'estafa amb un fals missatge de Netflix

El correu indica que s'ha caducat la subscripció i es demanen dades bancàries

ARA Andorra

## L'Agència Nacional de Ciberseguretat d'Andorra publica 11 consells per no patir ciberatacs a l'estiu

Noticies » Societat 16 de juliol, 2023

SOCIETAT | 09/04/2023

# La publicació i filtració de dades personals s'incrementen un 38%

Deriva de l'alt nivell d'atacs deguts a la Covid-19 i el teletreball, que van provocar una relaxació dels usuaris i una falta de mesures de prevenció contra intrusions

ANA

---

> NACIONAL

GOVERN

# Protocol per a la gestió d'incidents de ciberseguretat

L'Agència de ciberseguretat ha arribat a una entesa amb el CNI per intercanviar sinergies, formació i bones pràctiques

---

## Entrevista amb Jordi Ubach, responsable de l'Agència Nacional de Ciberseguretat

El responsable de l'ANC, Jordi Ubach, ens parla de la importància de la ciberseguretat i l'actualitat dels atacs al país. Fem referència al Botnet Mairai, que s'ha escampat a Europa, i coneixem les seves afectacions a Andorra. Repassem alguns consells que hem de tenir en compte i la participació del país a l'International Cyberex.

---

# Webinar: 'Els desafiaments de la IA per a les empreses'

16/11/2023

*Recupera la sessió organitzada per Andorra Digital amb l'Agència Nacional de Ciberseguretat*

---

L'ANC i Andorra Digital participen a la jornada 'Obligacions tècniques i legals en ciberseguretat al Principat d'Andorra

14/9/2023

El 21 de Setembre, la Universitat d'Andorra i la Cambra de Comerç Indústria i Serveis organitzen una jornada sobre obligacions tècniques i legals en ciberseguretat al Principat. **Jordi Ubach, de l'Agència Nacional de Ciberseguretat i David Vicente, director del Programa de transformació digital** hi intervindran amb la conferència "Aspectes essencials de la normativa NIS i Reglaments de l'ENS. Terminis d'obligat compliment. Serveis i recursos.

# 4. Línies d'acció de millora

## 4.1 Reforç de les capacitats enfront d'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 Impulsió de la ciberseguretat a 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 en què hi hagi representats els diferents sectors.

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

## 4.3 Desenvolupament d'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 la 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 del nivell d'exposició de les infraestructures.
- Implantació de sistemes de protecció.

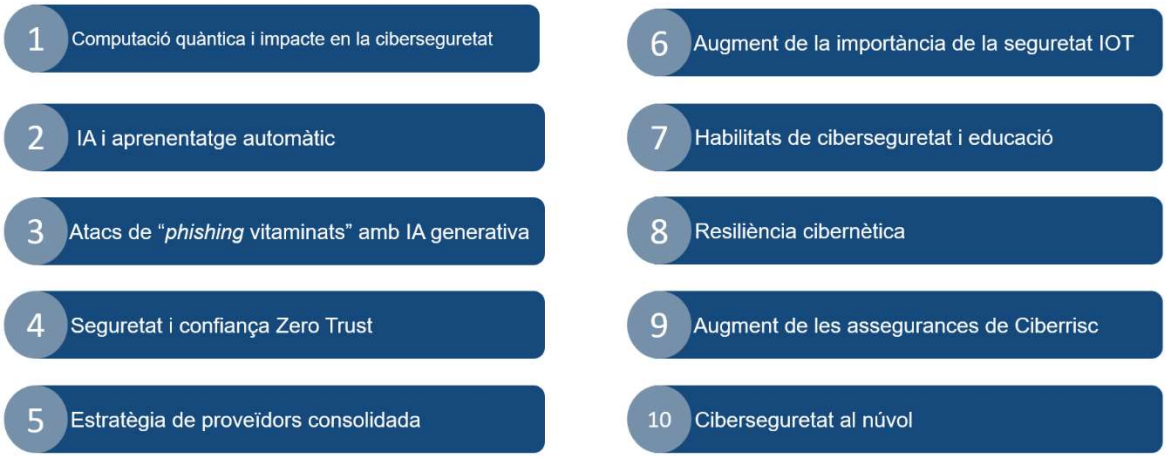
### 4.5 Ampliació del servei de resposta a incidents

Ampliar el servei actual L1(inicial) a L2 (avançat):

- Desplegament inicial 24 x 7

## 5. Tendències 2024

El resum de tendències elaborat per l'ANC-AD, el qual ja es pot descarregar i consultar des del lloc web de l'Agència, a través de : https://www.anc.ad/prediccions-i-tendencies-clau-pel-2024/, es resumeix de la forma següent:




## 6. 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**: aquest terme 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 activitats 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. Complint 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 que mesura 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, també es coneix 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 mitjà 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.
26. **MISP**: són les sigles en anglès de Mechanism for Sharing Indicator and STIX Packages, que és una plataforma gratuïta i oberta per a l'intercanvi d'informació sobre ciberamenaces. Funciona com un centre comunitari en què experts en seguretat comparteixen indicadors de compromís (IOCs) i paquets STIX (Structured Threat Information eXchange) per ajudar a altres a identificar i mitigar les amenaces de manera més eficient.