ENS-STIC-001

Catàleg d´actius d´informació estàndard

Gener 2023

Fitxa del document

Títol	Catàleg d´actius d´informació estàndard (Catàleg de Components)

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	25/01/23	26/01/23

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document: ANC-AD

PRÒLEG

L'ús massiu de les tecnologies de la informació i les telecomunicacions (TIC), en tots els àmbits de la societat, ha creat un nou espai, el ciberespai, on es produiran conflictes i agressions, i on hi ha ciberamenaces que atemptaran contra la seguretat nacional, l'estat de dret, la prosperitat econòmica, l'estat de benestar i el normal funcionament de la societat i de les administracions públiques i entitats privades.

La Llei 22/2022, de 9 de juny, , encomana a l´Agència Nacional de Ciberseguretat d´Andorra (ANC-AD, en endavant) l'exercici de les funcions relatives a la seguretat de les tecnologies de la informació, i de protecció de les xarxes d´ informació alhora que confereix Secretari d'Estat de Transició Digital i Projectes Estratègics la responsabilitat de dirigir l´ANC-AD.

El Decret 417/2022, de 19 d´octubre, pel qual es regula l'Esquema Nacional de Seguretat d´Andorra en l'àmbit de les entitats que presten serveis "importants" (ENS-AD, en endavant), al qual es refereix l'article 4-2-a de la Llei 22/2022, de 9 de juny , estableix la política de seguretat en la utilització de mitjans electrònics que permeti una protecció adequada de la informació.

En definitiva, la sèrie de documents ENS-STIC s'elaboren (adaptats i autoritzada la seva modificació i distribució per part del CCN-CERT) per donar compliment a les comeses de l´ANC-AD i al reflectit en l' ENS-AD, conscients de la importància que té l' establiment d' un marc de referència en aquesta matèria que serveixi de suport perquè el personal de les entitats afectades, i en ocasions, ingrata tasca de proporcionar seguretat als sistemes de les TIC sota la seva responsabilitat.

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

ÍNDEX

1. INTRODUCCIÓ

1. L'adquisició d'un producte o la contractació d'un servei de seguretat TIC que utilitzarà informació classificada o informació sensible ha d'estar precedida d'un procés de comprovació que els mecanismes de seguretat implementats en el producte o servei són adequats per a protegir aquesta informació.
2. L'avaluació i certificació (si la te) d'un producte o servei de seguretat TIC és l'únic objectiu que permet valorar i acreditar la seva capacitat per tractar informació de manera segura.
3. Aquest catàleg estableix unes pautes de caràcter general que són aplicables a entitats de diferent naturalesa, dimensió i sensibilitat sense entrar en casuístiques particulars. S'espera que cada organització l´adapti per a adaptar-les al seu entorn singular.

2. OBJECTIU

4. L'objecte d'aquest document és el de presentar el Catàleg d´actius que recull un llistat de productes pel maneig de la seguretat de la informació (SI) i serveis associats així com productes i serveis qualificats pel tractament d'informació sensible, de manera que pugui servir de referència a les entitats afectades per l´ENS-AD.

3. CATEGORIA: CONTROL D'ACCÉS

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Control d'accés a xarxa (NAC)	D1	I1	C1	M
Dispositius biomètrics	D2	I3	C0	A
Dispositius Single Sign-On	D3	I3	C3	B
Servidors d'autenticació	D0	I0	C1	A
Dispositius One-Time Password (OTP)	D1	I2	C3	M
Gestió d'accés privilegiat (PAM)	D1	I0	C1	A
Gestió d'identitats (IM)	D0	I0	C1	A

Taula 1. Nivell de seguretat de les diferents famílies o actius de la categoria Control d'Accés, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

3.1 FAMÍLIA: CONTROL D'ACCÉS A XARXA (NAC)

5. El **NAC (Network Acces Control) permet a les entitats obtenir informació completa sobre l'estat dels seus entorns ampliats** i orquestrar mesures destinades a reduir el risc operatiu i de ciberseguretat. Les solucions de control d'accés a la xarxa (admeten la visibilitat de xarxa i l'administració d'accés mitjançant l'aplicació de polítiques en dispositius i usuaris de la xarxa corporativa.
6. Les plataformes solen incorporar tant elements de perfilat de xarxa com de compliment de polítiques de seguretat corporativa (NAC) . Aquest control d'accés a xarxa ofereix descobriment, classificació en temps real i avaluació contínua d'estat, sense necessitat d'agents.

3.2 FAMÍLIA: DISPOSITIUS DE CONTROL BIOMÈTRIC

7. La biometria permet identificar a les persones en funció de característiques úniques. Els exemples inclouen escanejos d'empremtes dactilars, escanejos d'iris i reconeixement de veu. Els dispositius biomètrics utilitzen tecnologia per a capturar i processar aquest tipus d'informació.
8. Els dos usos principals dels dispositius biomètrics són la identificació i la verificació.

3.3 FAMÍLIA: DISPOSITIUS SINGLE SIGN-ON

9. El Single Sign On conegut també com SSO, permet als usuaris tenir accés a múltiples aplicacions ingressant només amb un compte als diferents sistemes i recursos. El

SSO és de gran utilitat quan existeixen diferents sistemes als que és possible accedir mitjançant una única contrasenya i es desitja evitar l'ingrés repetitiu d'aquestes cada vegada que l'usuari es desconnecti del servei.

3.4 FAMÍLIA: SERVIDORS D'AUTENTICACIÓ

10. Un servidor d'autenticació és un dispositiu que controla qui pot accedir a una xarxa informàtica. Els objectius de l'autenticació són l'autorització i la privacitat. L'autorització determina a quins objectes o dades pot tenir accés un usuari en la xarxa, si correspon. La privacitat evita que la informació es divulgui a persones no autoritzades. El no repudi és sovint un requisit legal i es refereix al fet que el servidor d'autenticació pot registrar tots els accessos a la xarxa juntament amb les dades d'identificació, de manera que un usuari no pot repudiar o negar el fet que ha accedit o modificat les dades en qüestió. Un servidor d'autenticació pot ser un servidor independent, una aplicació de firewall, integrat amb un commutador o servidor d'accés a la xarxa.

3.5 FAMÍLIA: DISPOSITIUS ONE-TIME PASSWORD (OTP)

11. Si una contrasenya s'usa de manera regular, existeix el risc que hi hagi persones no autoritzades que puguin accedir a ella. Una de les opcions és canviar la contrasenya amb regularitat, a poder ser, cada poc temps (aquesta directiva normalment està especificada dins les polítiques de seguretat de l´entitat). Una altra solució bastant més senzilla és la One-Time Password (contrasenya d'un sol ús). Una One-Time Password (OTP) és una contrasenya que només es pot usar una vegada i després perd la seva vigència.
12. Primer s'introdueixen les dades d'inici de sessió convencionals. Després, l'usuari genera una contrasenya dinàmica d'un sol ús, per exemple, amb un generador de codis, que també és necessari per a l'autenticació.
13. Les One-Time Passwords són molt recomanables en totes les pàgines web i serveis en línia que usin dades especialment sensibles i importants. Per exemple:
    - Banca electrònica
    - Serveis financers com a dipòsits d'accions en línia o mercats de valors per a criptomonedes
    - Dades sensibles d'entitats
    - Canals de comunicació confidencials

3.6 FAMÍLIA: GESTIÓ D'ACCÉS PRIVILEGIAT (PAM)

14. Una solució de gestió de comptes privilegiats (Privileged Access Management) permet descobrir, securitzar, administrar i auditar contrasenyes, credencials així com monitorar i gravar les sessions privilegiades. Permet gestionar l'accés a cada compte privilegiat i actiu crític, automatitzar les millors pràctiques de seguretat i complir les regulacions normatives.

15. Les capacitats de PAM de Secret Server per a l'administració dels comptes privilegiats inclouen:

    - Gestió del Cicle de Vida de les credencials amb privilegis:
        - Descobriment Automatitzat de comptes privilegiats i “onboarding” de les mateixes en un repositori central segur
        - Control i auditoria de les sessions privilegiades
    - Anàlisis del comportament de l'usuari privilegiat
    - Gestió de comptes de servei
    - Polítiques d'accés basades en RBAC i gestió de polítiques de seguretat.
    - Arquitectura escalable. Alta Disponibilitat (HA) i Disaster Recovery (DR). Integració amb múltiples plataformes Out-Of-The-Box
    - Mòdul de Reporting capaç de generar informes totalment a mesura
    - Securització dels processos de DevOps

3.7 FAMÍLIA: GESTIÓ D'IDENTITATS (IM)

16. La gestió d'identitats (IDM), també anomenada «gestió d'identitats i accessos» (IAM), garanteix que tan sols les persones autoritzades tinguin accés als recursos tecnològics que necessiten per a fer el seu treball. Inclou les polítiques i tecnologies que abasta tota l'organització, per identificar, autenticar i autoritzar adequadament persones o aplicacions de programari a través d'atributs com els drets d'accés dels usuaris i les restriccions basades en les seves identitats.

17. Un sistema de gestió d'identitats evita l'accés no autoritzat a sistemes i recursos, ajuda a evitar el robatori de dades protegides, i genera alertes i alarmes quan persones o programes no autoritzats intenten accedir a aquests.

4. CATEGORIA: EXPLOTACIÓ DE LA SEGURETAT

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Anti-virus / Endpoint Protection Plan	D0	I3	C3	A
Endpoint Detection and Response (EDR)	D1	I3	C3	M
Eines de Gestió de Xarxa	D2	I1	C3	M
Actualització de Sistemes	D3	I3	C3	B
Filtrat de navegació	D2	I3	C3	B
Sistemes de Gestió d'Esdeveniments de Seguretat	D1	I1	C1	M
Dispositius per a Gestió de Claus Criptogràfiques	D2	I1	C1	M
Eines de Gestió de Dispositius Mòbils	D1	I1	C1	M

Taula 2. Nivell de seguretat de les diferents famílies o actius de la categoria Explotació de la Seguretat, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

5.1 FAMÍLIA: ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)

18. L'Endpoint Protection Platform o EPP és una solució de seguretat per a endpoints amb l'objectiu de detectar i bloquejar amenaces i que prové del món dels antivirus de nova generació. Un agent d'aquest tipus és capaç de prevenir molts ciberatacs (per exemple, atacs de programari basat en arxius o activitats malicioses) i té una funcionalitat específica contra molts problemes de seguretat com el phishing, l'explotació 0-day i els atacs de xarxa.

5.2 FAMÍLIA: EDR (ENDPOINT DETECTION AND RESPONSE)

19. Les tècniques emprades pels cibercriminals cada vegada són més dirigides i sofisticades. Per això, no és suficient protegir el endpoint i el perímetre de la xarxa. Aquí, és on entra en joc l'eina EDR, una evolució de l'antivirus tradicional. Serveix per a donar visibilitat i respondre a les amenaces avançades.

20. Endpoint Detection and Response (o EDR) és una eina que proporciona monitoratge i anàlisi contínua de l´endpoint i la xarxa. La finalitat és identificar, detectar i prevenir amenaces avançades (APT) amb major facilitat.

21. La pròpia evolució del mercat ha portat al fet que els diferents fabricants vagin integrant en els seus EPP funcionalitats EDR.

22. Beneficis de l´EDR:

    - Major anticipació als atacs dirigits.
    - Menor temps d'exposició a incidents de seguretat.
    - Proporcionen una visibilitat completa de les amenaces.

5.3 FAMÍLIA: EINES DE GESTIÓ DE XARXA

23. Es pot sintetitzar en tasques de "desplegament, integració i coordinació del maquinari, programari i els elements humans per a monitorar, provar, sondejar, configurar, analitzar, avaluar i controlar els recursos "d'una xarxa per a aconseguir nivells de treball i de servei adequats als objectius d'una instal·lació i d'una organització.

24. Les eines més importants per una correcta gestió de xarxes són, entre d'altres:

    - Monitoratge de xarxa per a reduir les caigudes de la xarxa
    - Programari de monitoratge de l'amplada de banda i analitzador de NetFlow
    - Intel·ligència aplicada a la xarxa, núvol, infraestructura, aplicació i base de dades
    - Programari d'administració d'adreces IP, DHCP i DNS
    - Programari de rastreig de dispositius de xarxa
    - Analitzador de logs

5.4 FAMÍLIA: ACTUALITZACIÓ DE SISTEMES

25. Les actualitzacions estan per a garantir el funcionament i rendiment del nostre ordinador. Les actualitzacions d'un sistema són necessàries per dues raons:

    - Millorar la funcionalitat d'un programa amb una nova versió.
    - Mantenir la seguretat d'un sistema al mateix temps que es van descobrint vulnerabilitats

26. El principal objectiu de les actualitzacions és estar en constant cerca de vulnerabilitats de seguretat d'un sistema i posar-les pegats per a evitar així, que un equip pugui ser ciberatacat.

5.5 FAMÍLIA: FILTRAT DE NAVEGACIÓ

27. Un filtre web és una aplicació que bloqueja la navegació cap a algunes categories de llocs web. L'eina s'utilitza per a denegar l'accés a llocs web perillosos o llocs web que incloguin continguts sensibles o ofensius. És la solució perfecta per a mantenir la navegació dins de la xarxa d'una entitat. Dins de les entitats, s'utilitza un filtre web, també anomenat programari de control de contingut, per a evitar que els empleats utilitzin la xarxa de l'entitat per a fins diferents a l'activitat laboral.

28. L'algorisme del filtre web monitoritza la navegació des d'un dispositiu connectat. Tan aviat com un dispositiu requereix accés a un lloc web que forma part d'una llista negra, es denega l'accés.

5.6 FAMÍLIA: SISTEMES DE GESTIÓ D'ESDEVENIMENTS DE SEGURETAT

29. La informació sobre seguretat i gestió d'esdeveniments o SIEM (Security Information and Event Management) és un sistema de seguretat que té com a objectiu proporcionar a les entitats una resposta ràpida i precisa per a detectar i respondre davant qualsevol amenaça sobre els seus sistemes informàtics.
30. Els sistemes SIEM tenen un control total sobre tots els esdeveniments que succeeixen en l'entitat per a poder detectar qualsevol tendència o patró fora del comú i així actuar de manera immediata. SIEM és l'evolució de dues tecnologies de seguretat anteriors.
31. Les funcions principals que realitza un sistema SIEM són la d'emmagatzemar i interpretar els registres.
32. Els sistemes SIEM són una de les millors solucions per a aconseguir que els recursos TI d'una entitat estiguin a resguard de qualsevol atac extern i intern.

5.7 FAMÍLIA: DISPOSITIUS PER A GESTIÓ DE CLAUS CRIPTOGRÀFIQUES

33. La gestió de claus de xifratge és administrar el cicle de vida complet de les claus criptogràfiques. Això inclou: generar, usar, emmagatzemar, arxivar i eliminar claus. La protecció de les claus de xifratge inclou limitar l'accés a les claus física, lògica i mitjançant l'accés d'usuari / rol. Per tant, un sistema robust d'administració de claus de xifratge i polítiques inclou:
    - Cicle de vida de la clau: generació de claus, preactivació, activació, caducitat, postactivació, custòdia i destrucció.
    - Accés físic i lògic als servidors clau.
    - Accés d'usuari a les claus de xifratge.

5.8 FAMÍLIA: EINES DE GESTIÓ DE DISPOSITIUS MÒBILS (MDM)

34. La gestió de dispositius mòbils (MDM) és un conjunt d'eines i una metodologia provada que s'utilitzen per a proporcionar eines i aplicacions de gran productivitat per als dispositius mòbils dels empleats, alhora que es garanteix la seguretat de les dades corporatives. Com el treball remot s'ha tornat essencial, els dispositius mòbils s'han convertit en una part integral de la majoria de les entitats: eines vitals per a garantir la productivitat i l'eficiència.
35. No obstant això, com els dispositius mòbils de l'entitat accedeixen a dades crítiques, poden suposar una amenaça per a la seguretat si es pirategen, roben o perden.
36. Amb una plataforma MDM consolidada, els departaments d'IT i Seguretat poden gestionar tots els dispositius d'una entitat, independentment del tipus o el sistema operatiu.

6. CATEGORIA: MONITORATGE DE LA SEGURETAT

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Dispositius de Prevenció d'intrusos	D1	I3	C2	M
Sistemes HoneyPot / HoneyNet	D3	I3	C2	B
Captura, Monitoratge i Anàlisi de Trànsit	D2	I3	C2	B
Eines de Sandbox	D3	I3	C2	B

Taula 3. Nivell de seguretat de les diferents famílies o actius de la categoria Monitoratge de la Seguretat, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

7.1 FAMÍLIA: DISPOSITIUS DE PREVENCIÓ D'INTRUSIONS

37. Un sistema de detecció d'intrusions (IDS) és una aplicació usada per a detectar accessos no autoritzats a un ordinador o a una xarxa, és a dir, són sistemes que monitoren el trànsit entrant i es compara amb una base de dades actualitzada de signatures d'atac conegudes. Davant qualsevol activitat sospitosa, emeten una alerta als administradors del sistema els qui han de prendre les mesures oportunes. Aquests sistemes només detecten els accessos sospitosos emetent alertes anticipades de possibles intrusions, però no tracten de mitigar la intrusió.

38. En canvi, un sistema de prevenció d'intrusions (IPS) ajuda a les entitats a identificar el trànsit maliciós i bloqueja de manera proactiva l'ingrés d'aquest trànsit a la seva xarxa. Els productes que utilitzen tecnologia IPS poden implementar-se en línia per a monitorar el trànsit entrant i inspeccionar aquest trànsit a la recerca de vulnerabilitats i/o exploits. En cas de detectar-se amenaces, permeten prendre les mesures adequades segons es defineix en la política de seguretat, com bloquejar l'accés, posar en quarantena als hosts o bloquejar l'accés a llocs web externs que puguin resultar en una possible filtració de seguretat.

7.2 FAMÍLIA: SISTEMES HONEYPOT / HONEYNET

39. Un honeypot és un sistema o component de maquinari o programari utilitzat com una trampa o esquer amb finalitats de protecció contra atacs de ciberdelinqüents. En general, consisteix en una equipa o un lloc que sembla ser part de la xarxa i conté informació valuosa, però que en realitat està ben aïllat i no té contingut sensible o crític; també podria ser un arxiu, registre o una adreça IP no utilitzada. Dos o més honeypots en una xarxa formen una honeynet. Típicament, una honeynet s'usa per a monitorar una xarxa més gran i / o més diversa on un honeypot pot no ser suficient. Honeynets i honeypots s'utilitzen generalment com a parts de sistemes de detecció d'intrusions de xarxa més grans.

7.3 FAMÍLIA: CAPTURA, MONITORATGE I ANÀLISI DEL TRÀNSIT

40. Monitoratge dels trànsits de xarxa per a detectar amenaces o comportaments anòmals. Supervisió contínua de tots els elements actius relacionats amb la Ciberseguretat mitjançant sondes i agents interrogant als actius (Pot realitzar-se aquest anàlisi tant en xarxes IT com en xarxes OT (equips SCADA, PLCs, switchos industrials, PCs, encaminadors, impressores, etc).

7.4 FAMÍLIA: EINES DE SANDBOX

41. És una màquina virtual aïllada o un entorn dins una maquina, en la qual es pot executar codi de programari potencialment insegur sense afectar els recursos de xarxa o a les aplicacions locals.

42. En ciberseguretat les sandbox s'utilitzen per a executar codis sospitosos provinents d'arxius adjunts i URL desconeguts, i observar el seu comportament. Alguns indicadors molt reveladors són: si el codi s'autoreplica, si intenta contactar a un servidor de comanda i control (C&C), si descarrega programari addicional, si xifra dades delicades, etc. Com l'entorn de proves és un entorn emulat sense accés a la xarxa, dades o altres aplicacions, els equips de seguretat poden "detonar" el codi amb seguretat per a determinar com funciona i si és malintencionat.

8. CATEGORIA: PROTECCIÓ DE LES COMUNICACIONS

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Encaminadors (Router)	D0	I1	C2	A
Switch	D1	I1	C2	M
Tallafocs	D1	I2	C2	M
Proxies	D1	I2	C2	M
Dispositius de Xarxes Sense Fils	D1	I2	C2	M
Passarel·les segures d'Intercanvi de Dades	D0	I2	C2	A
Xarxes Privades Virtuals	D1	I2	C2	M
Eines per a Comunicacions Mòbil Segures	D3	I3	C2	B
Xifradors IP	D3	I3	C2	B
Web Application Firewall	D2	I3	C2	B

Taula 4. Nivell de seguretat de les diferents famílies o actius de la categoria Protecció de les Comunicacions, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

9.1 FAMÍLIA: ENCAMINADORS (ROUTER)

43. Els encaminadors guien i dirigeixen les dades de xarxa mitjançant paquets que contenen diversos tipus de dades, com a arxius, comunicacions i transmissions simples com a interaccions web.

44. Els encaminadors també poden proporcionar seguretat. El programari de firewall i filtrat de contingut integrat proporciona una protecció addicional contra el contingut no desitjat i els llocs web maliciosos.

45. Generalment l'encaminador està connectat a un router i envia informació d'Internet als dispositius de l´entitat o de l´usuari,

46. Podem trobar diferents tipus d'encaminadors:

- Encaminador principal
- Encaminador perimetral
- Encaminador de distribució
- Encaminador sense fil
- Encaminador virtual

9.2 FAMÍLIA: SWITCH

47. Un switch és un dispositiu d'interconnexió de dispositius dins d'una mateixa xarxa. En català es coneix com a commutador de xarxa d´àrea local LAN. Aquest tipus de connexió sempre es realitza de manera física i mitjançant cablejat perquè el seu objectiu és crear xarxes locals o connectar molts equips a única xarxa. Actualment les xarxes locals o LAN s'entrellacen mitjançant un sistema de cablejat amb l'estàndard de connexió Ethernet. Els switch ofereixen un alt nivell d'escalabilitat.

48. Un switch està pensat per a connectar entre si dispositius dins d'una mateixa xarxa. Per tant, no està pensat per a connectar-se a Internet. Si volem connectar-nos a internet hem d'utilitzar un encaminador o un servei de virtualització que permeti la connexió amb xarxes externes.

9.3 FAMÍLIA: TALLAFOCS

49. Un tallafocs o firewall és un sistema de seguretat (HW o SW) que controla el trànsit d'Internet en una xarxa, per a evitar intrusions malicioses. Aquests actuen de barreres entre una xarxa interna privada i pública. Es tracta d'un element dedicat que s'instal·la en el sistema operatiu i permet o no l'accés a la xarxa per part d'altres programes i aplicacions. També existeixen firewalls físics, és a dir, un maquinari específic que s´usen generalment per la seguretat perimetral.

9.4 FAMÍLIA: PROXIES

50. Un proxie és un equip informàtic que fa d'intermediari entre les connexions d'un client i un servidor de destí, filtrant tots els paquets entre tots dos. El proxie rep les peticions d'accedir a la pàgina sol·licitada, i s'encarrega de transmetre al servidor d web perquè aquesta no sàpiga qui les està sol·licitant. Les consultes del Proxie, poden quedar emmagatzemades a la caché.

51. D'aquesta manera, quan es visita una pàgina web, en comptes d'establir una connexió directa entre el navegador i la pàgina farà l´enviament i la rebuda de dades a través del proxie. La pàgina visitada no sabrà la IP de l´usuari sinó la del proxie.

9.5 FAMÍLIA: DISPOSITIUS DE XARXA SENSE FILS

52. Un primer element que ha de ser considerat en implementar és la connexió pel mitjà aeri (WLANs) ja que és l'element fonamental per a la propagació dels senyals sense fils. L'aire és el “conducte” a través del qual la informació flueix entre els dispositius d'usuari i la infraestructura de xarxa. Similar al comportament en les comunicacions “parlades”, a mesura que els dispositius s'allunyen és difícil mantenir la comunicació especialment en ambients d'alt soroll i interferència radioelèctrica.

53. Les xarxes sense fils utilitzen components similars a les xarxes LANs cablejades. Aquests components disposen de dues diferents classes de dispositius:

- Dispositius d'accés al mitjà com a targetes sense fils i estacions base (punts d'accés, encaminadors sense fils).
- Dispositius d'usuari final com a equips personals, portàtils, agendes digitals, càmeres web, impressores, etc.

9.6 FAMÍLIA: PASSAREL·LES SEGURES D'INTERCANVI DE DADES

54. Les passarel·les d'intercanvi segur d'informació són dispositius de protecció perimetral especialment dissenyats per controlar l'intercanvi d'informació entre sistemes amb diferents nivells de classificació i evitar així que s'estableixin fluxos d'informació no autoritzats.

55. Com a dispositius de protecció perimetrals, són més segurs que un tallafocs o un proxie, ja que separen físicament dos sistemes, impedeixen que s'estableixin connexions de cap nivell dins de les capes del model OSI i analitzen el contingut de la informació d'acord amb unes regles prèviament definides.

9.7 FAMÍLIA: XARXES PRIVADES VIRTUALS

56. **IPsec** (Seguretat del Protocol d'Internet) és un marc normalitzat per a assegurar les comunicacions d'IP mitjançant el xifratge i autenticació de cada paquet IP en un flux de dades. La norma IPsec s'utilitza normalment per a establir una VPN IPsec a través d'Internet entre terminals fixos i també per a crear una connexió client-servidor VPN xifrada entre dispositius remots i una xarxa fixa.

57. **PPTP** (o Point to Point Tunneling Protocol), és un protocol de comunicacions obsolet que permet implementar xarxes privades virtuals o VPN. Aquest protocol PPTOP va ser substituït pel protocol L2TP.

58. Les connexions **L2TP** (Layer 2 Tunneling Protocol), també denominades línies virtuals, ofereixen accés als usuaris remots a baix preu, en permetre que un sistema de xarxa de l'entitat gestioni les adreces IP assignades als seus usuaris remots. A més, les connexions L2TP ofereixen un accés segur al seu sistema o xarxa quan les utilitzi conjuntament amb IPSec (IP Security).

59. **Open VPN** és una eina de connectivitat que ofereix una combinació de seguretat, facilitat d'ús i riquesa. Està basada en programari lliure: SSL (Secure Sockets Layer) i VPN Virtual Private Network (xarxa virtual privada). OpenVPN ofereix connectivitat punt-a-punt amb validació jeràrquica d'usuaris i host connectats remotament.

60. **IKE** o intercanvi de claus d'Internet és un protocol de tunelització basat en IPSec que proporciona un canal de comunicació VPN segur i defineix els mitjans automàtics de negociació i autenticació per a les associacions de seguretat IPSec de manera segura.

61. Una **VPN SSL** és un tipus de xarxa privada virtual (VPN) que utilitza el protocol Secure Sockets Layer (SSL) en navegadors web estàndard per a proporcionar capacitat VPN d'accés remot i segur. SSL VPN permet que els dispositius amb

connexió a internet estableixin una connexió VPN segura d'accés remot amb un navegador web. Una connexió SSL VPN utilitza xifratge d'extrem a extrem (E2EE) per a protegir les dades transmeses entre el programari del client del dispositiu de punt final i el servidor SSL VPN a través del qual el client es connecta de manera segura a internet. Les entitats utilitzen VPN SSL per a permetre que els usuaris remots accedeixin de manera segura als recursos de l'organització, així com per a protegir les sessions d'internet dels usuaris que accedeixen a internet des de fora de l'entitat.

62. **Secure Socket Tunneling Protocol** és una forma de túnel de xarxa privada virtual que proporciona un mecanisme per a transportar trànsit PPP a través d'un canal SSL/TLS. SSL/TLS brinda seguretat a nivell de transport amb negociació de claus, encriptació i verificació d'integritat del trànsit.

9.8 FAMÍLIA: EINES PER A COMUNICACIONS MÒBILS SEGURES

63. Els productes associats a aquesta família permeten establir comunicacions de manera segura com veu i vídeo sobre IP (VVoIP) o missatgeria instantània,) a través de túnels segurs amb altres dispositius o amb servidors remots.

64. Una aplicació VVOIP executada sobre un dispositiu mòbil estableix un túnel segur amb un servidor controlador de sessió (ESC) o amb una altra aplicació VVOIP executada sobre un dispositiu mòbil.

9.9 FAMÍLIA: XIFRADORS IP

65. Els xifradors d´IP s'utilitzen per a crear xarxes privades virtuals (VPN) i per exemple, permetre l'accés dels dispositius mòbils a la xarxa a través d'Internet mitjançant una connexió segura.

9.10 FAMÍLIA: WEB APPLICATION FIREWALL (WAF)

66. Un Web Application Firewall (WAF) protegeix de múltiples atacs al servidor d'aplicacions web a la capa de backend. La funció del WAF és garantir la seguretat del servidor web mitjançant l'anàlisi de paquets de petició HTTP / HTTPS i modelat del trànsit.

67. El WAF examina cada petició enviada al servidor, abans que arribi a l'aplicació, per a assegurar-se que compleix amb les regles del Firewall definides per l´administrador del sistema. Les característiques WAF poden ser implementades:

    - En el programari (SW): instal·lant una aplicació en el sistema operatiu.
    - En el maquinari(HW): integrant les funcionalitats en una solució d´appliance.

10. CATEGORIA: PROTECCIÓ DE LA INFORMACIÓ I SUPORTS D'INFORMACIÓ

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Servidors	D0	I0	C1	A
Servidors NAS	D0	I0	C1	A
Emmagatzematge Xifrat de Dades	D0	I0	C1	A
Xifrat Offline	D2	I1	C1	M
Esborrat Segur	D2	I1	C1	M
Prevenció de Fugides de Dades	D0	I1	C0	A
Eines per a Signatura Electrònica	D3	I3	C2	B
Maquinari Security Moduli (HSM)	D3	I2	C1	M
Cabines de Disc	D0	I0	C1	A
Núvol Híbrid	D0	I0	C1	A

Taula 5. Nivell de seguretat de les diferents famílies o actius de la categoria Protecció de la Informació i Suports d'Informació, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

11.1 FAMÍLIA: SERVIDORS

68. Un servidor és un aparell informàtic que emmagatzema, distribueix i subministra informació. Els servidors funcionen basant-se en el model "client-servidor". El client pot ser tant un ordinador com una aplicació que requereix informació del servidor per a funcionar. Per tant, un servidor oferirà la informació demandada pel client sempre que el client estigui autoritzat. Els servidors poden ser físics o virtuals.

69. En el cas del servidor físic, es tracta d'un maquinari, també conegut com host (amfitrió), és una màquina integrada a una xarxa de nodes basats en programari. D'altra banda, els servidors de virtuals (VPS, Virtual Private Server) són softwares que proporcionen serveis a altres programes (clients).

70. Els servidors poder ser Cloud, es a dir al núvol, o *on-premise* (en local). A més també es pot diferenciar entre si es vol servidor propi, o si es vol llogar a un proveïdor (SAAS o Software as a Service).

11.2 FAMILIA: SERVIDORS NAS

71. Un servidor NAS és un dispositiu d'emmagatzematge connectat a la xarxa. La seva funció és la de fer còpies de seguretat dels arxius que tu li indiquis en la configuració, tant els del teu ordinador personal com els de qualsevol altre dispositiu mòbil.

72. A efectes pràctics la funció principal d'aquests dispositius és la d'actuar com a unitat d'emmagatzematge, fent les vegades de disc dur extern o permetent-te crear el teu propi emmagatzematge en el núvol. La diferència amb els núvols d'altres entitats és que en aquest cas els discos durs on s'emmagatzemen les teves dades estan en la teva pròpia casa, i no en els servidors pertanyents a l'entitat que et presta l'emmagatzematge.

11.3 FAMÍLIA: EMMAGATZEMATGE XIFRAT DE DADES

73. L'encriptació de l'emmagatzematge d'arxius és l'encriptació de les dades emmagatzemades, generalment amb el propòsit de protegir la informació confidencial perquè no sigui vista per persones que no haurien de tenir accés a ella, o en cas d´accés no autoritzat, aquesta informació xifrada no tingui cap valor.

74. És més probable que s'utilitzi el xifratge d'emmagatzematge d'arxius si les dades s'emmagatzemen en línia o en una ubicació de fàcil accés, com en una unitat externa o una unitat flash.

75. Gairebé tots els serveis de còpia de seguretat en línia utilitzen el xifratge d'emmagatzematge d'arxius. Això és necessari tenint en compte que les dades privades com a vídeos, imatges i documents s'emmagatzemen en servidors accessibles a través d'Internet.

76. Una vegada encriptades, les dades no poden ser llegides per ningú tret que la contrasenya utilitzada per a encriptar-los s'utilitzi per a revertir l'encriptació, o desxifrar-la, concedint-li accés als arxius.

11.4 FAMÍLIA: XIFRAT OFFLINE

77. Els dispositius o eines de xifrat fora de línia (offline) són productes que permeten el xifrat d'informació per al seu posterior emmagatzematge o transport quan no es disposa d'una infraestructura de comunicacions o d'intercanvi d'informació segura (veure família VPN).

78. En aquesta mena d'eina els fitxers es xifren localment, des de la plataforma a la qual està connectat el dispositiu o des de la qual s'executa (eina), per a després ser emmagatzemats, enviats o transportats utilitzant un mitjà no segur.

11.5 FAMÍLIA: ESBORRAT SEGUR

79. Les entitats, sense importar la seva grandària o el seu sector, basen la seva activitat en la informació: bases de dades, documents de text, arxius, imatges, etc. El cicle

de vida de la informació, de forma simplificada, consta de tres fases: generació, transformació i destrucció.

80. Amb l'esborrat i destrucció de suports d'informació (discos durs, memòries flash, cintes, paper…), no sols es busca protegir la difusió d'informació confidencial d'una organització. Les entitats poden trobar diversos motius per a eliminar la informació que guarden. A més, són les encarregades de vetllar per l'adequada gestió de dades personals, estratègics, legals o comptables, entre altres, i estan obligades a conservar aquestes dades durant un període de temps, després del qual se solen eliminar.

11.6 FAMÍLIA: PREVENCIÓ D´EXFILTRACIÓ O PÈRDUA DE DADES

81. Una pèrdua o exfiltració de dades es produeix quan dades catalogades com a sensibles o confidencials queden exposats públicament de forma involuntària (s'origina generalment per un error humà). Aquesta exposició de dades pot succeir en trànsit, en repòs o en ús.

82. La majoria de les estratègies per a prevenir la pèrdua o exfiltració de dades sensibles comencen amb la realització d'avaluacions de risc i la creació de polítiques i procediments basats en aquestes avaluacions.

11.7 FAMÍLIA: EINES PER A SIGNATURA ELECTRÒNICA

83. Els beneficis que les eines de signatura digital poden aportar als processos de l´entitat els següents beneficis:

- Millorar la productivitat
- Encaminar el negoci a la transformació digital
- Atorgar seguretat i control
- Permetre reestructurar els fluxos de treball
- Converteixen l´entitat en amigable amb l'ambient
- Facilitar el signar de manera digital des de qualsevol ubicació
- Brinda celeritat, reduint els temps burocràtics
- Redueix despeses de diners i de temps en el trasllat

11.8 FAMÍLIA: MÒDUL DE SEGURETAT DE MAQUINARI (HSM)

84. Els mòduls de seguretat de Maquinari (HSM) són dispositius de maquinari sòlid i resistent a manipulacions que asseguren els processos criptogràfics generant, protegint i administrant claus utilitzades per a xifrar i desxifrar dades, i crear signatures i certificats digitals. Els sistemes HSM es proven, validen i certifiquen amb els estàndards de seguretat més elevats.

85. HSM com a servei és una oferta basada en subscripció perquè els clients generin, utilitzin i protegeixin les seves claus amb un HSM al núvol. Tot això al marge de les

dades confidencials. Aquesta oferta de serveis proporciona la mateixa protecció que un desplegament on-premise i garanteix major flexibilitat.

11.9 FAMÍLIA: CABINES DE DISCOS

86. Una cabina de discos és un dispositiu que compta amb diversos discos durs que li permeten compartir informació. Al comptar amb diversos discos, li permet oferir funcions avançades com crear RAIDs, donar servei a diversos equips, etc.
87. Els equips NAS (Network Attached Storage) són dispositius que compten amb un o diversos discos durs i que són capaços de proveir emmagatzematge a la xarxa.
88. Un equip SANT o xarxa SAN (Storage Area Network) està formada, igual que en el cas anterior, per una cabina de discos.

11.10 FAMÍLIA: NÚVOL HÍBRID

89. Un **núvol híbrid** és la combinació de tots dos models d'implementació del núvol privat i públic. A l´usar un núvol híbrid, es poden escalar recursos de computació i limitar els enormes costos de gestionar els pics de demanda. A més, els núvols híbrids donen la flexibilitat d'alliberar recursos locals per a emmagatzemar i executar més aplicacions i dades confidencials quan és necessari.
90. Els núvols híbrids també brinden un mitjà per a limitar l'accés de núvol públic a tot el seu pool de dades, ja que reserven l'ús de núvol públic específicament per a gestionar desbordaments, i així garantir una ciberseguretat més sòlida.

12. CATEGORIA: PROTECCIÓ D'EQUIPS I SERVEIS

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Protecció de Correu Electrònic	D1	I1	C0	A
Targetes Intel·ligents	D1	I0	C1	A
Còpies de Seguretat	D1	I0	C1	A
Virtualització	D1	I2	C1	M
Equilibrador de Càrrega	D2	I2	C2	B
Eines CASB	D2	I2	C2	B
Hiperconvergencia	D2	I1	C2	M
Eines de Videoidentificació	D1	I1	C1	M
Eines de Videoconferència	D1	I2	C1	M
Lloc de Treball	D0	D0	CO	A

Taula 6. Nivell de seguretat de les diferents famílies o actius de la categoria Protecció d'Equips i Serveis, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

13.1 FAMÍLIA: PROTECCIÓ DE CORREU ELECTRÒNIC

91. Una exfiltració de dades es produeix quan dades sensibles queden exposats en públic involuntàriament (s'origina per un error humà). Aquesta exposició de dades pot succeir en trànsit, en repòs o en ús

92. Si algú aconsegueix l´adreça de correu electrònic —perquè està publicada en alguna xarxa social o blog; pel reenviament de correus en cadena; participació en portals de falsos concursos— i, a més, s´utilitza una contrasenya que no és segura per a accedir a la bústia, és relativament senzill que algú entri a la bústia de l´usuari i pugui llegir, modificar i esborrar correus privats, enviar emails amb el seu nom propi, canviar les opcions de privacitat i seguretat associades al compte. Per tant, és molt important conèixer els riscos als quals s´exposa l´usuari i tenir en compte les recomanacions per a protegir el compte de correu. Les converses privades quedaran exposades. A traves del correu es pot tenir accés als documents enviats i rebuts, entre d'altres:

    - Factures
    - Nòmines
    - Avisos de lliuraments de documents d'identitat

- Fotografies i vídeos
- Contactes
- Documentació interna o confidencial

13.2 FAMÍLIA: TARGES INTEL·LIGENTS

93. Un aspecte crucial de les targes intel·ligents virtuals és la seva capacitat per a emmagatzemar i usar dades secretes de forma segura, específicament que les dades protegides no es poden exportar. Es pot accedir a les dades i usar-les dins del sistema de targes intel·ligents virtuals, però no tenen sentit fora del seu entorn previst. A les targes intel·ligents virtuals, la seguretat es garanteix amb una jerarquia de claus segura, que inclou diverses cadenes de xifratge. És imprescindible evitar la pèrdua o robatori de la tarja intel·ligent per evitar una exfiltració involuntària de dades.

13.3 FAMÍLIA: CÒPIES DE SEGURETAT

94. El xifrat de la còpia de seguretat ha de formar part de l'estratègia de seguretat. En molts entorns, l'emmagatzematge s'ha realitzat fora de la supervisió dels responsables de seguretat, ja que aquests es centren en àrees com la seguretat perimetral, la detecció i prevenció d'intrusions i la protecció de sistemes.
95. Algunes recomanacions per protegir la còpia de seguretat són:
    - Assignar responsabilitat i autoritat
    - Avaluar el risc d'emmagatzematge
    - Desenvolupar un programa de protecció de la informació
    - Comunicar els processos de protecció de la informació i seguretat
    - Executar i Provar el pla de seguretat de protecció de la informació
    - Provar de forma programada la recuperació de còpies
    - Xifrat de les còpies

13.4 FAMÍLIA: VIRTUALITZACIÓ

96. La virtualització és el procés d'executar diverses instàncies virtuals d'un dispositiu en un sol recurs de maquinari físic. La virtualització de la seguretat fa referència al procés, al procediment i a les polítiques que garanteixen que la infraestructura de maquinari virtualitzada estigui segura i protegida.
97. La virtualització també planteja desafiaments de seguretat per als quals els sistemes de seguretat físics no estan preparats:
    - L'intercanvi d'arxius entre hosts i convidats no és segur.
    - Es consoliden diversos servidors, la qual cosa suposa un major risc que una vulneració pugui propagar-se des de les aplicacions d'un mateix host.

13.5 FAMÍLIA: EQUILIBRADOR DE CÀRREGA

98. Un equilibrador de càrrega actua com a únic punt de contacte per als clients. L'equilibrador de càrrega distribueix el trànsit entrant entre diversos destins, això augmenta la disponibilitat de l'aplicació. Pot agregar un o diversos agents pel control l'equilibrador de càrrega.
99. Un agent d'escolta comprova les sol·licituds de connexió dels clients, utilitzant el protocol i el port configurats, i reenvia les sol·licituds a un grup de destí.

13.6 FAMÍLIA: EINES CASB

100. Un CASB és un intermediari entre els usuaris i les plataformes basades en el núvol que protegeixen les dades en el núvol i alhora aborden les inquietuds en matèria d'autoritzacions i visibilitat de les corporacions que usen serveis basats en el núvol. Es pot considerar al CASB com un punt central en el qual tots els controls d'accés i regles d'autorització es validen enfront de polítiques establertes per l´organització.

13.7 FAMÍLIA: HIPERCONVERGENCIA

101. La infraestructura hiperconvergent (HCI) és un sistema unificat i definit per programari que reuneix tots els elements d'un centre de dades tradicional: emmagatzematge, recursos informàtics, xarxa i gestió. Aquesta consta de quatre components de programari integrat:
    - Virtualització de l'emmagatzematge
    - Virtualització de recursos informàtics
    - Virtualització de la xarxa
    - Gestió avançada amb automatització
102. El programari de virtualització desvincula i agrupa els recursos, i després els assigna dinàmicament a aplicacions en màquines virtuals. Això brinda possibilitats com:
    - Crear un núvol privat
    - Estendre l'entorn al núvol privat a públic
    - Aconseguir un núvol veritablement híbrid

13.8 FAMÍLIA: EINES DE VIDEOIDENTIFICACIÓ

103. Els productes associats a la família eines de videoidentificació sorgeixen per a donar resposta a la necessitat d'establir mecanismes d'autenticació i identificació remota, amb la finalitat de contribuir en la reducció dels desplaçaments dels usuaris dels sistemes (generalment externs a l'organització, per ex: tràmits en línia) per a realitzar tràmits, sense minvar els seus drets.
104. Avui dia, els productes de videoidentificació, i de biometria en general, són productes complexos en els quals la fiabilitat, privacitat i seguretat són claus. Algunes de les característiques d'aquests productes són les següents:

- Composició modular
- Procés assistit o desatès
- Enregistrament i emmagatzematge d'evidències

13.9 FAMÍLIA: EINES DE VIDEOCONFERÈNCIA

105. El confinament, el distanciament social i l'adopció del teletreball com a mesura adoptada en moltes entitats han convertit les videoconferències en un recurs "imprescindible", amb un increment del seu ús en tots els àmbits utilitzant diferents aplicacions (apps) i eines. L'augment de l'ús d'aquestes eines ha vingut acompanyat de l'aparició de noves vulnerabilitats.

106. Per això es recomanen prendre entre d'altres, les següents mesures:

- Protegir les reunions virtuals amb contrasenyes
- Verificar els assistents
- Vigilar la divulgació dels enllaços per a accedir a aquestes reunions
- Reportar activitats sospitoses
- Doble factor d´autenticació per accedir a les reunions(2FA)

13.10 FAMÍLIA: LLOC DE TREBALL

107. **PC**: Un ordinador personal, o PC, és un tipus de microordinador dissenyat en principi per a ser utilitzat per una sola persona. Sol denominar-se ordenador de sobretaula, a causa de la seva posició estàtica i impossibilitat de transport a diferència d'un ordinador portàtil. Un ordinador personal sol estar equipat per a complir tasques comunes de la informàtica moderna, és a dir, permet navegar per Internet, estudiar, escriure textos i fer altres treballs d'oficina o educatius, com editar textos i bases de dades, a més d'activitats d'oci, com escoltar música, veure vídeos, jugar, etc.

108. **Portàtil**: Es denomina computadora portàtil o ordinador portàtil, a vegades simplement portàtil, a un determinat dispositiu informàtic que es pot moure o transportar amb relativa facilitat. Els ordinadors portàtils són capaços de realitzar totes les tasques que realitzen els ordinadors d'escriptori, també dits «de torre» o simplement PC.

109. **Perifèrics**: Un perifèric és la denominació genèrica per a designar a l'aparell o dispositiu auxiliar i independent connectat a la placa base d'una computadora. Es a dir, són dispositius de hardware a través dels quals l'ordinador es comunica amb l'exterior, i també als sistemes que emmagatzemen o arxiven la informació, servint de memòria auxiliar de la memòria principal.

- Dispositius d'entrada: teclat, ratolí, escàner, micròfon, etc.
- Dispositius de sortida: monitor, impressora, altaveu o auriculars, etc.
- Perifèrics d'entrada/sortida: Pantalla tàctil, equips multifunció, etc.
- Perifèrics de comunicació: Targes de xarxa, mòdems, hubs, routers, etc.

14. CATEGORIA: DISPOSITIUS OT

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
PLC	D3	D3	D3	B
HMI	D3	D3	D3	B
SCADA	D3	D3	D3	B
Controladors	D2		D3	B
Sensors	D3	D3	D3	B
Actuadors	D3	D3	D3	B
Xarxes Intel·ligents	D3	D3	D3	B
Protocol de Protecció de Comunicació	D2	I2	C2	B

Taula 7. Nivell de seguretat de les diferents famílies o actius de la categoria Dispositius OT, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

15.1 FAMÍLIA: PLC

110. Un Controlador Lògic Programable o PLC (Programmable Logic Controller) és una computadora que s'utilitza en l'enginyeria d'automatització per a les indústries, és a dir, es tracta de dispositius electrònics programables encarregats d'accionar a altres components de maquinària perquè realitzin accions que poguessin ser perilloses per als éssers humans o molt lentes si es fa manualment.

111. Bàsicament els PLC resolen requeriments de control de processos i seqüències de la maquinària dins del sector indústries

15.2 FAMÍLIA: HMI

112. HMI (human machine interface) es refereixen a un panell que permet a un usuari comunicar-se amb una màquina, programari o sistema. Tècnicament, es pot referir a qualsevol pantalla que s'usi per a interactuar amb un equip, però s'utilitza normalment per a les d'entorns industrials. Les HMI mostren dades en temps real i permeten a l'usuari controlar les màquines amb una interfície gràfica d'usuari.

15.3 FAMÍLIA: SCADA

113. El sistema SCADA és una eina d'automatització i control industrial utilitzada en els processos productius que pot controlar, supervisar, recopilar dades, analitzar dades

i generar informes a distància mitjançant una aplicació informàtica. La seva principal funció és la d'avaluar les dades amb el propòsit d'esmenar possibles errors.

114. Un SCADA, és una agrupació d'aplicacions informàtiques instal·lades en un ordinador denominat Màster o MTU, destinat al control automàtic d'una activitat productiva a distància que està interconnectada amb altres instruments anomenats de camp com són els autòmats programables (PLC) i les unitats terminals remotes (RTU).

15.4 FAMÍLIA: CONTROLADORS

115. Un controlador o driver és el programari que controla un dispositiu en un PC; per exemple, una tarja de vídeo o de so. Els controladors actuen com a "ponts" entre les aplicacions i els dispositius, encarregant-se que tots dos interactuïn. Existeixen tres tipus de controladors utilitzats en l'automatització industrial: controladors lògics programables (PLC), sistemes de control distribuït (DCSs) i controladors programables d'automatització (PACS).

15.5 FAMÍLIA: SENSORS

116. Un sensor és un dispositiu que detecta el canvi en l'entorn i respon a alguna sortida en l'altre sistema. Un sensor converteix un fenomen físic en un voltatge analògic mesurable (o, a vegades, un senyal digital) convertit en una pantalla llegible per a humans o transmesa per a lectura o processament addicional. Actualment els sensors, a part de la connexió física de sempre, disposen de connectivitat wifi, nfc o Bluetooth.

15.6 FAMÍLIA: XARXES INTEL·LIGENTS

117. Es coneix com a xarxa intel·ligent a un sistema de distribució d'energia recolzat en els avanços tecnològics que combina tres elements: els equips elèctrics tradicionals, els comptadors electrònics i els sistemes d'informació i telecomunicacions que permeten rebre la informació a distància. D'aquesta manera, es poden detectar amb més rapidesa i precisió quan una línia pateix una incidència i solucionar-la en un temps inferior o, fins i tot, anticipar-se a situacions de sobrecàrrega.

118. L'adaptació a una xarxa intel·ligent permet monitorar i actuar a distància i de manera instantània i automàtica sobre la xarxa elèctrica i, gràcies a això, avançar-se a possibles incidències, gestionar més ràpidament les que es produeixin i millorar la qualitat del servei als consumidors. D'igual manera, la valuosa informació proporcionada pels comptadors intel·ligents afavoreix, d'una banda, a les necessitats dels clients respecte a tot el relacionat al seu punt de subministrament, perquè pugui prendre decisions a partir de la seva informació detallada.

15.7 FAMÍLIA: PROTOCOL DE PROTECCIÓ DE COMUNICACIÓ

119. **Profinet**: PROFINET (Process Field Network) és un protocol de comunicació Ethernet industrial basat en estàndards oberts TCP/IP i IT i desenvolupat amb un enfocament en la semblança a PROFIBUS DP. Així mateix, és un mecanisme per a intercanviar dades entre controladors i dispositius. Els controladors, per norma general, són autòmats programables (PLC) i Sistemes de Control Distribuït (DCS), mentre que els dispositius poden ser mòduls de E/S, sistemes de visió artificial, lectors de sistemes RFID, accionaments varis, instruments de procés, proxies, o fins i tot altres autòmats.
120. **Profibus**: PROFIBUS és un estàndard de xarxa digital de camp obert (bus de camp) que s'encarrega de la comunicació entre els sensors de camp i el sistema de control o els controladors. És important conèixer que PROFIBUS són les sigles de Process Field Bus. La possibilitat de comunicació entre els dispositius i l'ús de mecanismes estandarditzats, oberts i flexibles són components essencials del concepte d'automatització actual.
121. **Modbus**: Modbus és el protocol de comunicacions més estès en l'automatització industrial i el mitjà més comú per a connectar dispositius electrònics automatitzats. utilitzat per a transmetre informació a través de xarxes en sèrie entre dispositius electrònics. El dispositiu que sol·licita la informació es diu mestre(master) Modbus i els dispositius que subministren la informació són els esclaus(slave) Modbus. Això significa que un dispositiu esclau no pot oferir informació; ha d'esperar que se li demani. El mestre escriurà dades en els registres d'un dispositiu esclau i llegirà les dades dels registres d'un dispositiu esclau. Per tant, en una xarxa Modbus estàndard, hi ha un mestre i fins a 247 esclaus, cadascun amb una direcció d'esclau única d'1 a 247. El mestre també pot escriure informació als esclaus.

16. CATEGORIA: CAPA FÍSICA

Família	Subclasse de seguretat			Nivell de seguretat
	Disponibilitat	Integritat	Confidencialitat	
Sistema de Videovigilància	D1	I0	C0	A
SAI	D0	I3	C1	A
Duplicitat de Línies Elèctriques	D0	I3	C1	A
Duplicitat de Línies de Telecomunicacions	D0	I3	C1	A

Taula 8. Nivell de seguretat de les diferents famílies o actius de la categoria Capa Física, determinat en funció del nivell de protecció de cada una de les seves subclasses de seguretat (Article 6 de l'ENS-AD).

17.1 FAMÍLIA: SISTEMA DE VIDEOVIGILÀNCIA

122. Les entitats han de protegir els seus recursos, tant materials com humans, per la qual cosa implementar un bon sistema de videovigilància. Aquest tipus de sistemes són ideals per a controlar perímetres i accessos, evitar robatoris d'informació interns, i per a dissuadir a delinqüents.

17.2 FAMÍLIA: SAI

123. Sistemes d'alimentació ininterrompuda (SAI), en anglès uninterruptible power supply (UPS), és un dispositiu que gràcies als seus bateries i altres elements emmagatzemadors d'energia, durant una apagada elèctrica pot proporcionar energia elèctrica per un temps limitat a tots els dispositius que tingui connectats.

124. Una altra funció que es pot afegir a aquests equips és millorar la qualitat de l'energia elèctrica que arriba a les càrregues, filtrant pujades i baixades de tensió i eliminant harmònics de la xarxa en cas d'usar corrent altern.

17.3 FAMÍLIA: DUPLICITAT DE LÍNIES ELÈCTRIQUES

125. Totes les opcions amb les quals aconseguir que es dugui a terme la continuïtat en el subministrament d'energia inclou l'alimentació múltiple evitant així que existeixi un únic punt en el qual es pot produir la fallada.

17.4 FAMÍLIA: DUPLICITAT DE LÍNIES DE TELECOMUNICACIONS

126. Els equips de telecomunicació han d'estar connectats al proveïdor mitjançant dues rutes diferents prevenint així que si falla una es pugui comptar amb l'altra. Aquest servei ha de ser adequat per a satisfer els requisits legals amb els quals comunicar les emergències que es produeixin en l'organització.

18. ANNEX A: GLOSSARI

IKE

Internet Key Exchange

OSI

OSI és el protocol de referència d'Interconnexió de Sistemes Oberts, definit en set capes, cada una amb la seva funció (aplicació, presentació, sessió, transport, xarxa, enllaç, física).

RAIDs

El RAID és un acrònim que significa *Redundant Array of Independent Disks,* o matriu de discos independents redundants. La seva finalitat d'un sistema RAID de discos és la de protegir les dades en cas que un disc dur falli, o en alguns casos té com a funció principal millorar la velocitat de lectura de diversos discos que conformen un únic volum..

RBAC

El RBAC o role based accés control es un model de seguretat permet assignar funcions i autoritzacions en la infraestructura informàtica d'una organització.

WLANs

WLAN és l'abreviatura de *Wireless Local Area Network*, i es refereix a una xarxa de computadores a distància d'unes poques desenes o centenars de metres, que utilitza senyals de radio d'alta freqüència per a transmetre i rebre dades.

19. ANNEX B: AMENACES

128. Les amenaces a les quals estan exposats els actius prèviament esmentats poden ser de diferent naturalesa i amb diferents objectius. Els més comuns son:

- **Explotació de vulnerabilitats SW**: Molts dels intents d'intrusió resulten de l'explotació de vulnerabilitats ja identificades i per a les quals es disposava de correctius: actualitzacions i pegats que únicament requereixen la seva aplicació.
- **Injecció SQL**: És un tipus de ciberatac encobert en el qual un hacker insereix codi propi en un lloc web amb la finalitat d'infringir les mesures de seguretat i accedir a dades protegides.
- **Intrusions**: En molts casos d'intrusió en la xarxa, l'atac implica inundar o sobrecarregar la xarxa, recopilar dades sobre la xarxa per a atacar-la des d'un punt feble més tard o inserir informació en la xarxa per a propagar-se i obtenir accés des d'endins.
- **Malware**: És un terme general per a referir-se a qualsevol tipus de “malicious software” (programari maliciós) dissenyat per a infiltrar-se en els dispositiu sense el coneixement de l’afectat.
- **Remote File Inclusion (RFI)**: És un tipus de vulnerabilitat web que afecta aplicacions web que depenen d'un temps d'execució de scripts.
- **Spyware**: L´spyware és una forma de malware que s'oculta en el seu dispositiu, controla la seva activitat i li roba informació confidencial i contrasenyes.
- **DoS / DDoS**: Atac de denegació de servei, té com a objectiu inhabilitar l'ús d'un sistema, una aplicació o una màquina, amb la finalitat de bloquejar el servei per al qual està destinat. És realitzen peticions o connexions emprant un gran nombre d'ordinadors o adreces IP.
- **Atacs de força bruta**: És un intent d'esbrinar una contrasenya o un nom d'usuari, o de trobar una pàgina web oculta o la clau utilitzada per a xifrar un missatge, mitjançant un enfocament de prova i error, amb l'esperança d'encertar.
- **RAT**: És una eina que es pot utilitzar per a controlar i administrar de manera remota algun sistema o dispositiu.
- **Accessos a serveis no autoritzats:** Usuaris malintencionats poden intentar infringir la seguretat o afectar el rendiment del sistema mitjançant atacs als processos d'inici de sessió, contrasenya oblidada i autoregistre.
- **Phishing**: És una suplantació d'identitat per part dels hackers. Amb aquesta tècnica maliciosa ens fan picar en l'ham amb la finalitat d'aconseguir les nostres credencials per a suplantar la nostra identitat.
- **Ransomware**: És una forma de malware que bloqueja els arxius o dispositius de l'usuari i després reclama un pagament en línia anònim per a restaurar l'accés.
- **Exfiltració d’informació**: Ocorre quan s'incorre en la còpia, transferència o recuperació no autoritzades de dades d'un servidor o l'ordinador d'un individu.
- **Cucs**: Un cuc informàtic és un tipus enganyós de malware, dissenyat per a propagar-se a través de diversos dispositius mentre roman actiu en tots ells.
- **Rootkit**: És un sigil·lós i perillós tipus de malware que permet als hackers accedir al seu equip sense el seu coneixement.

	Amenaces														
Família	Explotació de vulnerabilitat SW	Injecció SQL	Intrusions	Malware	RFI	Spyware	DoS / DDoS	Atac de força bruta	RAT	Accessos a serveis no autoritzats	Phishing	Ransomware	Exfiltració d'informació	Cucs	Rootkit
Control d'accés a xarxa (NAC)			✓	✓		✓	✓	✓	✓	✓		✓			✓
Dispositius biomètrics				✓		✓		✓		✓		✓			
Dispositius Single Sign-On				✓		✓	✓	✓		✓		✓			
Servidors d'autenticació				✓		✓	✓	✓	✓	✓		✓			
Dispositius One-Time Password (OTP)				✓		✓	✓	✓		✓		✓			
Gestió d'accés privilegiat (PAM)				✓		✓	✓	✓	✓	✓		✓			✓
Gestió d'identitats (IM)				✓		✓	✓	✓	✓	✓		✓			✓
Anti-virus / Endpoint Protection Plan	✓		✓	✓			✓			✓					
Endpoint Detection and Response (EDR)	✓		✓	✓			✓			✓					
Eines de Gestió de Xarxa		✓	✓	✓			✓		✓	✓				✓	
Actualització de Sistemes	✓		✓	✓										✓	
Filtrat de navegació	✓	✓		✓	✓										✓
Sistemes de Gestió d'Esdeveniments de Seguretat	✓		✓	✓					✓	✓					✓

Dispositius per a Gestió de Claus Criptogràfiques				✓						✓					
Eines de Gestió de Dispositius Mòbils	✓	✓		✓			✓			✓	✓			✓	
Dispositius de Prevenció d'intrusos	✓		✓	✓			✓		✓	✓					✓
Sistemes HoneyPot / HoneyNet	✓		✓	✓			✓		✓	✓					✓
Captura, Monitoratge i Anàlisi de Trànsit	✓		✓	✓			✓		✓	✓					
Eines de Sandbox	✓		✓	✓			✓		✓	✓					✓
Encaminadors (Router)	✓	✓	✓	✓			✓			✓			✓	✓	
Switchos	✓	✓	✓	✓			✓			✓			✓	✓	
Tallafocs	✓	✓	✓	✓			✓			✓			✓	✓	✓
Proxies	✓	✓	✓	✓			✓			✓			✓	✓	✓
Dispositius de Xarxes Sense Fils	✓	✓	✓	✓			✓			✓			✓	✓	
Passarel·les segures d'Intercanvi de Dades	✓	✓	✓	✓			✓			✓			✓	✓	✓
Xarxes Privades Virtuals	✓	✓	✓	✓			✓			✓			✓	✓	✓
Eines per a Comunicacions Mòbil Segures	✓		✓	✓			✓	✓		✓			✓	✓	
Xifradors IP	✓	✓	✓	✓			✓			✓			✓	✓	✓
Web Application Firewall	✓	✓	✓	✓	✓		✓			✓			✓	✓	

Servidors	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓
Servidors NAS	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓
Emmagatzematge Xifrat de Dades	✓	✓	✓	✓		✓				✓		✓			
Xifrat Offline				✓		✓				✓					
Esborrat Segur				✓						✓			✓		
Prevenció de Fugides de Dades	✓	✓	✓	✓		✓				✓		✓	✓	✓	✓
Eines per a Signatura Electrònica	✓			✓		✓	✓	✓		✓					
Maquinari Security Moduli (HSM)	✓	✓		✓		✓	✓			✓		✓	✓		✓
Cabines de Disc		✓	✓	✓		✓	✓		✓	✓		✓	✓	✓	✓
Núvol Híbrid		✓	✓	✓		✓	✓		✓	✓		✓	✓	✓	✓
Protecció de Correu Electrònic		✓		✓		✓		✓		✓	✓	✓	✓	✓	✓
Targetes Intel·ligents		✓	✓	✓		✓	✓			✓	✓	✓			
Còpies de Seguretat		✓	✓	✓		✓			✓	✓		✓	✓	✓	✓
Virtualització		✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓
Equilibrador de Càrrega		✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓
Eines CASB		✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓
Hiperconvergencia		✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓

Eines de Videoidentificació				✓			✓	✓	✓	✓	✓			✓	✓
Eines de Videoconferència				✓		✓	✓	✓	✓	✓	✓			✓	
Lloc de Treball	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PLC	✓		✓	✓					✓	✓		✓			
HMI	✓		✓	✓					✓	✓		✓			
SCADA	✓		✓	✓					✓	✓		✓			
Controladors	✓		✓	✓					✓	✓		✓			
Sensors	✓		✓	✓					✓	✓		✓			
Actuadors	✓		✓	✓					✓	✓		✓			
Xarxes Intel·ligents	✓	✓	✓	✓			✓		✓	✓			✓	✓	✓
Protocol de Protecció de Comunicació	✓	✓	✓	✓			✓		✓	✓	✓		✓	✓	✓
Sistema de Videovigilància	✓		✓					✓		✓					
SAI			✓					✓		✓					
Duplicitat de Línies Elèctriques			✓					✓		✓					
Duplicitat de Línies de Telecomunicacions			✓					✓		✓					

Taula 9. Llistat d'amenaces a les que es poden afrontar les diferents famílies.