# ENS-STIC-804
# Guia d'implementació de l'ENS


**(DOCUMENT SUBJECTE A MODIFICACIONS)**

**Desembre 2025**

Fitxa del document

| **Títol** | Guia d'implementació ENS-STIC-804 |
|---|---|

| Versió | Redactat/Revisat per | Aprovat per | Data aprovació | Data publicació |
|---|---|---|---|---|
| | | | | |
| 1.0 | ANC-AD | ANC-AD | 20/12/22 | 20/12/22 |

| Registre de canvis | | | |
|---|---|---|---|
| Versió | Pàgines | Data de modificació | Motiu del canvi |
| 1.1 | 88 | 20/03/2023 | Afegit Annex A |
| 1.2 | 92 | 08/01/2025 | Inclusió dels requeriments per la categoria mitjana |
| 2.21 | 132 | 22/12/2025 | Afegit "Marc comú" per canvi legislatiu, actualització d'índex (OP.PL.6–7), annexos reordenats (nou Annex tècnic) i taula d'equivalència CMMI. |

| **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.

La Llei 22/2022, de 9 de juny, encomana a l'Agència Nacional de Ciberseguretat d'Andorra (ara endavant, ANC-AD) 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 al 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, d'ara 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'elabora per donar compliment a les comeses de l'Agència Nacional de Ciberseguretat d'Andorra (ANC-AD) i al que estableix l'Esquema Nacional de Seguretat d'Andorra (ENS-AD), amb la finalitat de proporcionar un marc de referència en matèria de seguretat de la informació que serveixi de suport al personal de les entitats afectades en la seva tasca d'assegurar els sistemes i serveis TIC sota la seva responsabilitat.

Marc Rossell i Soler
Ministre de Funció Pública i transformació digital

# ÍNDEX

**1. INTRODUCCIÓ ..... 7**
**2. NIVELLS DE MADURESA ..... 7**
**3. MARC COMÚ ..... 10**
3.1 INTRODUCCIÓ DE L'ENTITAT I ABAST DE L'ENS-AD ..... 10
3.2. SISTEMA DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ (SGSI) ..... 10
3.3 PLANIFICACIÓ DE REVISIONS DEL SGSI ..... 11
3.4 DELEGAT DE LA SEGURETAT DE LA INFORMACIÓ (DSI) ..... 11
3.5 ROL DE LA DIRECCIÓ EN LA SEGURETAT DE LA INFORMACIÓ ..... 12
3.6 AUDITORIA DE SEGURETAT I PLA D'ACCIONS CORRECTORES (PAC) ..... 12
**4. DIFERENCIACIÓ DE LES CATEGORIES ..... 13**
**5. [ORG] MARC ORGANIZATIU ..... 14**
5.1 [ORG.1] POLÍTICA DE SEGURETAT ..... 14
5.3 [ORG.2] NORMATIVA DE SEGURETAT ..... 15
5.4 [ORG.3] PROCEDIMENTS OPERATIUS DE SEGURETAT ..... 18
5.5 [ORG.4] PROCÉS D'AUTORITZACIÓ ..... 20
**6 MARC OPERACIONAL ..... 22**
6.3 [OP.PL] PLANIFICACIÓ ..... 22
6.3.1 [OP.PL.1] ANÀLISI DE RISCOS ..... 22
6.3.2 [OP.PL.2] ARQUITECTURA DE SEGURETAT ..... 24
6.3.3 [OP.PL.3] ADQUISICIÓ DE NOUS COMPONENTS ..... 24
6.3.4 [OP.PL.4] DIMENSIONAMENT / GESTIÓ DE CAPACITATS ..... 25
6.3.5 [OP.PL.5] COMPONENTS CERTIFICATS ..... 26
6.3.6 [OP.PL.6] PLA DE SEGURETAT ..... 29
6.3.7 [OP.PL.7] DECLARACIÓ D'APLICABILITAT ..... 31
6.4 [OP.ACC] CONTROL D'ACCÉS ..... 32
6.4.1 [OP.ACC.1] IDENTIFICACIÓ ..... 32
6.4.2 [OP.ACC.2] REQUISITS D'ACCÉS ..... 34
6.4.3 [OP.ACC.3] SEGREGACIÓ DE FUNCIONS I TASQUES ..... 35
6.4.4 [OP.ACC.4] PROCÉS DE GESTIÓ DE DRETS D'ACCÉS ..... 36
6.4.5 [OP.ACC.5] MECANISME D'AUTENTICACIÓ (USUARIS EXTERNS) ..... 37
6.4.6 [OP.ACC.6] MECANISMES D'AUTENTICACIÓ (USUARIS DE L'ORGANITZACIÓ) .43
6.5 [OP.EXP] EXPLOTACIÓ ..... 46
6.5.1 [OP.EXP.1] INVENTARI D'ACTIUS ..... 46
6.5.2 [OP.EXP.2] CONFIGURACIÓ DE SEGURETAT ..... 48
6.5.3 [OP.EXP.3] GESTIÓ DE LA CONFIGURACIÓ DE SEGURETAT ..... 49
6.5.4 [OP.EXP.4] MANTENIMENT I ACTUALITZACIONS DE SEGURETAT ..... 50
6.5.5 [OP.EXP.5] GESTIÓ DE CANVIS ..... 51
6.5.6 [OP.EXP.6] PROTECCIÓ ENFRONT DE CODI NOCIU ..... 52
6.5.7 [OP.EXP.7] GESTIÓ D'INCIDENTS ..... 53
6.5.8 [OP.EXP.8] REGISTRE DE L'ACTIVITAT DELS USUARIS ..... 57
6.5.9 [OP.EXP.9] REGISTRE DE LA GESTIÓ D'INCIDENTS ..... 57
6.5.10 [OP.EXP.10] PROTECCIÓ DE LES CLAUS CRIPTOGRÀFIQUES ..... 58

6.6 [OP.EXT] RECURSOS EXTERNS ..... 59
6.6.1 [OP.EXT.1] CONTRACTACIÓ I ACORDS DE NIVELL DE SERVEI ..... 60
6.6.2 [OP.EXT.2] GESTIÓ DIÀRIA ..... 64
6.6.3 [OP.EXT.3] INTERCONNEXIÓ DE SISTEMES ..... 65
6.7 [OP.NUB] SERVEIS EN EL NÚVOL ..... 66
6.8 [OP.CONT] CONTINUÏTAT DEL SERVEI ..... 67
6.8.1 [OP.CONT.1] ANÀLISI D'IMPACTE ..... 67
6.8.2 [OP.CONT.2] PLA DE CONTINUÏTAT ..... 68
6.8.3 [OP.CONT.3] PROVES PERIÒDIQUES ..... 70
6.8.4 [OP.CONT.4] MITJANS ALTERNATIUS ..... 71
6.9 [OP.MON] MONITORATGE DEL SISTEMA ..... 73
6.9.1 [OP.MON.1] DETECCIÓ D'INTRUSIÓ ..... 73
6.9.2 [OP.MON.2] SISTEMA DE MÈTRIQUES ..... 75
6.9.3 [OP.MON.3] VIGILÀNCIA ..... 76
6.9.4 [OP.MON.4] REGISTRE D'ESDEVENIMENTS ..... 78
**7 [MP] MESURES DE PROTECCIÓ ..... 83**
7.9 [MP.IF] PROTECCIÓ DE LES INSTAL·LACIONS I INFRAESTRUCTURES ..... 83
7.9.2 [MP.IF.1] ÀREES SEPARADES I AMB CONTROL D'ACCÉS ..... 83
7.9.3 [MP.IF.2] IDENTIFICACIÓ DE LES PERSONES ..... 83
7.9.4 [MP.IF.3] ACONDICIONAMIENT DELS LOCALS ..... 84
7.9.5 [MP.IF.4] ENERGIA ELÈCTRICA ..... 85
7.9.6 [MP.IF.5] PROTECCIÓ ENFRONT D'INCENDIS ..... 86
7.9.7 [MP.IF.6] PROTECCIÓ ENFRONT DE INUNDACIONS ..... 86
7.9.8 [MP.IF.7] REGISTRE D'ENTRADA I SORTIDA D'EQUIPAMENT ..... 87
7.10 [MP.PER] GESTIÓ DEL PERSONAL ..... 87
7.10.2 [MP.PER.1] CARACTERITZACIÓ DEL LLOC DE TREBALL ..... 87
7.10.3 [MP.PER.2] DEURES I OBLIGACIONS ..... 88
7.10.4 [MP.PER.3] CONSCIENCIACIÓ ..... 89
7.10.5 [MP.PER.4] FORMACIÓ ..... 90
7.11 [MP.EQ] PROTECCIÓ DELS EQUIPS ..... 91
7.11.2 [MP.EQ.1] LLOC DE TREBALL ORDENAT ..... 91
7.11.3 [MP.EQ.2] BLOQUEIG DE LLOC DE TREBALL ..... 91
7.11.4 [MP.EQ.3] PROTECCIÓ D'EQUIPS PORTÀTILS ..... 92
7.11.5 [MP.EQ.4] ALTRES DISPOSITIUS CONNECTATS A LA XARXA ..... 93
7.12 [MP.COM] PROTECCIÓ DE LES COMUNICACIONS ..... 94
7.12.2 [MP.COM.1] PERÍMETRE SEGUR ..... 94
7.12.3 [MP.COM.2] PROTECCIÓ DE LA CONFIDENCIALITAT ..... 95
7.12.4 [MP.COM.3] PROTECCIÓ DE L'AUTENTICITAT I DE LA INTEGRITAT ..... 96
7.12.5 [MP.COM.4] SEGREGACIÓ DE XARXES ..... 97
7.13 [MP.SI] PROTECCIÓ DELS SUPORTS D'INFORMACIÓ ..... 99
7.13.2 [MP.SI.1] ETIQUETAT DE SUPORTS ..... 99
7.13.3 [MP.SI.2] CRIPTOGRAFIA ..... 100
7.13.4 [MP.SI.3] CUSTÒDIA ..... 100
7.13.5 [MP.SI.4] TRANSPORT ..... 101

7.13.6 [MP.SI.5] BORRAT I DESTRUCCIÓ ..... 101
7.14 [MP.SW] PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES ..... 103
7.14.2 [MP.SW.1] DESENVOLUPAMENT D'APLICACIONS ..... 103
7.14.3 [MP.SW.2] ACCEPTACIÓ I POSADA EN SERVEI ..... 106
7.15 [MP.INFO] PROTECCIÓ DE LA INFORMACIÓ ..... 107
7.15.2 [MP.INFO.1] DADES DE CARÀCTER PERSONAL ..... 107
7.15.3 [MP.INFO.2] QUALIFICACIÓ DE LA INFORMACIÓ ..... 110
7.15.4 [MP.INFO.3] SIGNATURA ELECTRÒNICA ..... 111
7.15.5 [MP.INFO.4] SEGELLS DE TEMPS ..... 112
7.15.6 [MP.INFO.5] NETEJA DE DOCUMENTS ..... 114
7.15.7 [MP.INFO.6] CÒPIES DE SEGURETAT (BACKUP) ..... 114
7.16 [MP.S] PROTECCIÓ DELS SERVEIS ..... 115
7.16.2 [MP.S.1] PROTECCIÓ DEL CORREU ELECTRÒNIC (E-MAIL) ..... 115
7.16.3 [MP.S.2] PROTECCIÓ DE SERVEIS I APLICACIONS WEB ..... 117
7.16.4 [MP.S.3] PROTECCIÓ DE LA NAVEGACIÓ DE WEB ..... 119
7.16.5 [MP.S.4] PROTECCIÓ ENFRONT DE LA DENEGACIÓ DE SERVEI ..... 119
**ANNEX A. MESURES DE SEGURETAT ..... 122**
**ANNEX B. ESPECIFICACIONS TÈCNIQUES ..... 126**
**ANNEX C. GLOSSARI ..... 129**
**ANNEX D. REFERÈNCIES ..... 132**

# 1. INTRODUCCIÓ

1. Aquesta guia 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 entitat les particularitzi per a adaptar-les al seu entorn singular.
2. L'Esquema Nacional de Seguretat d'Andorra (d'ara endavant, ENS-AD) estableix una sèrie de mesures de seguretat en què estan condicionades a la valoració del nivell de seguretat en cada dimensió, i a la categoria del sistema d'informació de què es tracti. Al seu torn, la categoria del sistema es calcula en funció del nivell de seguretat en cada dimensió.
3. Aquestes mesures constitueixen un mínim que s'ha d'implementar, o justificar els motius pels quals no s'implementen o se substitueixen per altres mesures de seguretat que aconsegueixin els mateixos efectes protectors sobre la informació i els serveis.
4. Aquesta guia busca ajudar els responsables dels sistemes perquè puguin implantar ràpidament i efectivament les mesures requerides, sense perjudici que emprin recursos propis o recorrin a proveïdors i productes externs.
5. Per a cada mesura es proporciona:
   - una descripció més àmplia que la proporcionada a l'ENS-AD,
   - referències externes que ajuden a la seva comprensió i realització,
   - relació amb mesures o controls en altres esquemes de seguretat,
   - i la relació amb els principis bàsics recollits a l'ENS-AD.

# 2. NIVELLS DE MADURESA

6. És habitual l'ús de nivells de maduresa per a caracteritzar la implementació d'un procés. El model de maduresa permet descriure les característiques que fan un procés efectiu, mesurant el grau o nivell de professionalització de l'activitat.
7. Els nivells identificats són els següents:

| Nivell | Descripció |
|---|---|
| N/A | **No aplica** |
| | No es reconeix la necessitat d'implementar aquest control. El control no és part de la cultura o missió de l'organització. |
| L1 | **Inicial / ad hoc** |
| | En el nivell L1 de maduresa, el procés existeix, però no es gestiona. L'entitat no proporciona un entorn estable. L'èxit o fracàs del procés depèn de la competència i bona voluntat de les persones i és difícil preveure la reacció davant una situació d'emergència. En aquest cas, les entitats excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell L1 depèn de tenir personal d'alta qualitat. |

| Nivell | Descripció |
|---|---|
| L2 | **Repetible, però intuïtiu** |
| | En el nivell L2 de maduresa, l'eficàcia del procés depèn de la bona sort i de la bona voluntat de les persones. Hi ha un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps. |
| L3 | **Procés definit** |
| | Es disposa un catàleg de processos que es manté actualitzat. Aquests processos garanteixen la consistència de les actuacions entre les diferents parts de l'entitat, que adapten els seus processos particulars al procés general. Hi ha normativa establerta i procediments per a garantir la reacció professional davant els incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor del desconegut (o no planificat). L'èxit és una mica més que bona sort: es mereix.<br>Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2, i que es gestiona en el nivell 3. |
| L4 | **Gestió quantitativa** |
| | Es disposa d'un conjunt de mètriques de qualitat i productivitat significatives que s'utilitzen sistemàticament per la presa de decisions i la gestió de riscos. La confiança és quantitativa al contrari que al nivell 3 que era només qualitativa.<br>Els processos que es realitzen per arribar als objectius van acompanyats d'una gran recopilació de dades i mesures estudiades estadísticament que faciliten una millor presa de decisions. |

Taula 1. Nivells de maduresa

8. Com a regla general, s'exigirà un nivell de maduresa en les mesures de seguretat en proporció al nivell de les dimensions afectades o de la categoria del sistema:

| Nivell de maduresa mesures de seguretat | Categoria del sistema de les tecnologies de la informació i la comunicació | Nivell de maduresa mínim exigit |
|---|---|---|
| ENS-AD | Mitjana | L4 |

Taula 2. Nivells de maduresa exigits en funció de la categoria del sistema o nivell de la dimensió de seguretat.

9. Per tal d'assegurar la coherència amb marcs de maduresa reconeguts internacionalment, la taula següent presenta una correspondència entre els nivells de maduresa definits en aquest document i els nivells del model **Capability Maturity**

**Model Integration (CMMI)**. Aquesta equivalència no implica una relació de certificació directa, sinó que actua com una guia interpretativa per entendre com s'ajusta l'escala de maduresa interna als nivells estàndard del CMMI.

| Nivell de maduresa de l'ENS | CMMI |
|---|---|
| L1 | 1 |
| L2 | 2 |
| L3 | 3 |
| L4 | 3,5 |
| L5 | 4 |

# 3. MARC COMÚ

## 3.1 Introducció de l'entitat i abast de l'ENS-AD

11. Aquest apartat s'ha d'adaptar a cada entitat i descriure de manera sintètica el seu context organitzatiu, el paper que exerceix en el teixit econòmic i social del Principat d'Andorra i els serveis que presta. En el cas de les entitats identificades com a essencials o importants d'acord amb la Llei 22/2022, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (Llei NIS-AD), s'ha d'especificar clarament quins serveis entren dins de l'àmbit d'aplicació de l'ENS-AD i per què són crítics per a la continuïtat de l'activitat del país.
12. L'entitat és, en tot cas, la responsable última de la seguretat de la informació dels serveis inclosos en l'ENS-AD, amb independència que determini subcontractacions o serveis prestats per tercers. Aquesta responsabilitat s'exerceix a través de l'òrgan de direcció, que ha de definir l'estratègia de seguretat, aprovar el Sistema de gestió de la seguretat de la informació (SGSI) i designar el delegat de la seguretat de la informació (DSI), de conformitat amb el Reglament aprovat pel Decret 417/2022, del 12 d'octubre, pel qual s'aprova l'Esquema nacional de seguretat del Principat d'Andorra (ENS-AD).
13. L'abast de l'ENS-AD dins l'entitat ha de quedar definit explícitament, indicant els serveis, processos, unitats organitzatives i actius d'informació que en formen part, així com les principals dependències tecnològiques i de proveïdors. Quan l'entitat opti per estendre voluntàriament l'ENS-AD a altres serveis no classificats com a essencials o importants, aquesta ampliació també s'ha de descriure en aquest apartat, deixant constància que l'objectiu és aplicar un nivell de protecció coherent i proporcional als riscos i al rol que l'organització exerceix en l'ecosistema digital andorrà.

## 3.2. Sistema de gestió de la seguretat de la informació (SGSI)

14. El Sistema de gestió de la seguretat de la informació (SGSI) és l'eix vertebrador de la implantació de l'ENS-AD dins de l'entitat. D'acord amb el Decret 417/2022, el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra estableix que l'SGSI ha de permetre identificar, implantar i mantenir, de manera sistemàtica i integral, les mesures de seguretat necessàries per garantir la prestació dels serveis essencials o importants amb un nivell de risc acceptable.
15. L'SGSI ha de cobrir, com a mínim, tots els serveis que l'entitat hagi declarat dins l'àmbit d'aplicació de l'ENS-AD, així com els actius d'informació bàsics i estàndard associats, incloent-hi infraestructures, xarxes, sistemes d'informació, aplicacions i processos de negoci relacionats. El seu disseny ha d'estar basat en la gestió de riscos, en els principis bàsics de l'ENS-AD (proporcionalitat, estratificació de mesures, vigilància contínua, modelatge estàndard, etc.) i en un cicle de millora contínua que garanteixi l'adequació permanent de les mesures a l'evolució de les amenaces, de la tecnologia i del context de l'entitat.
16. En aquest marc, l'SGSI no és només un conjunt de documents, sinó un sistema de governança que integra polítiques i normativa interna, procediments operatius,

inventaris d'actius, declaracions d'aplicabilitat, plans de seguretat, plans de formació i conscienciació, i mecanismes de seguiment, auditoria i revisió periòdica, tal com preveu el Reglament aprovat pel Decret 417/2022.

## 3.3 Planificació de revisions del SGSI

17. La planificació de revisions del SGSI dona compliment al principi de vigilància contínua i millora contínua recollit a l'ENS-AD i al Reglament aprovat pel Decret 417/2022. L'entitat ha d'establir un calendari formal de revisions periòdiques que abasti, com a mínim, la política i la normativa de seguretat, l'anàlisi i el tractament de riscos, l'inventari d'actius, la declaració d'aplicabilitat, els plans de seguretat, el PAC i els procediments d'actuació davant incidents.
18. Aquestes revisions s'han de dur a terme, com a mínim, amb una periodicitat anual, i sempre que es produeixin canvis rellevants en els serveis, en el context tecnològic, en el model organitzatiu o en el marc legal i regulador. Igualment, la planificació de revisions s'ha d'alinear amb les actualitzacions del Catàleg d'actius d'informació estàndard i amb els resultats de les auditories, de manera que els canvis normatius o tècnics es tradueixin en actualitzacions oportunes del SGSI.
19. El DSI és l'encarregat de coordinar aquesta planificació, recollir els resultats de les revisions i elaborar els informes corresponents perquè l'òrgan de direcció pugui valorar-ne les conclusions, ajustar l'estratègia de seguretat, prioritzar accions de millora i, si escau, actualitzar la declaració d'aplicabilitat i els plans de seguretat de l'entitat.

## 3.4 Delegat de la seguretat de la informació (DSI)

20. El delegat de la seguretat de la informació (DSI), definit a la Llei NIS-AD i desenvolupat pel Decret 417/2022, és la figura designada per l'òrgan de direcció per coordinar i supervisar l'SGSI i la implantació de l'ENS-AD dins de l'entitat. El DSI actua com a punt de referència intern en matèria de seguretat de la informació i com a interlocutor davant l'Agència Nacional de Ciberseguretat d'Andorra (ANC-AD) i la resta d'autoritats competents.
21. Entre les seves funcions principals destaquen: impulsar i coordinar l'anàlisi i la gestió de riscos; promoure i mantenir l'inventari d'actius d'informació; elaborar i actualitzar la declaració d'aplicabilitat; proposar i fer el seguiment dels plans d'acció i dels plans d'accions correctores (PAC); coordinar la resposta davant incidents de seguretat; i vetllar pel compliment de les obligacions establertes al Reglament de l'ENS-AD i en la normativa interna de l'entitat. Així mateix, el DSI ha de garantir que la seguretat de la informació es considera en els projectes, els canvis i les decisions estratègiques que afecten els serveis essencials o importants.
22. L'entitat ha de dotar el DSI de l'autoritat, la independència funcional i els recursos humans i materials necessaris per exercir les seves responsabilitats amb eficàcia, assegurant que pot accedir a la informació rellevant, convocar els actors implicats i elevar recomanacions i informes l'òrgan de direcció.

## 3.5 Rol de la direcció en la seguretat de la informació

23. L'òrgan de direcció és el màxim responsable de la seguretat de la informació i de la correcta implantació de l'ENS-AD dins de l'entitat. D'acord amb el que estableixen la Llei NIS-AD i el Decret 417/2022, li correspon definir l'estratègia i els objectius de seguretat, aprovar el marc organitzatiu i operacional de la seguretat, designar el DSI i validar els documents clau de l'SGSI (política de seguretat, anàlisi de riscos, declaració d'aplicabilitat, pla de seguretat, PAC, etc.).
24. La direcció ha de garantir que es destinen recursos suficients —humans, tecnològics i econòmics— per complir els requisits mínims i les mesures de referència que deriven del Reglament de l'ENS-AD, així per atendre els reforços necessaris segons la categoria i el nivell de seguretat dels serveis afectats. Igualment, ha d'impulsar una cultura de seguretat dins l'entitat, promovent la formació i la conscienciació del personal i assegurant que la seguretat de la informació s'integra en la presa de decisions i en la planificació estratègica.
25. Finalment, l'òrgan de direcció ha de revisar periòdicament els informes del DSI, els resultats de les auditories i els indicadors de seguretat, i assumir formalment les decisions sobre acceptació de riscos, priorització d'inversions i aprovació dels plans d'accions correctores i de millora contínua.

## 3.6 Auditoria de seguretat i Pla d'Accions Correctores (PAC)

26. Les auditories de seguretat previstes al Reglament de l'ENS-AD, aprovat pel Decret 417/2022, constitueixen un mecanisme clau per verificar el grau d'adequació de l'entitat als requisits mínims i a les mesures de referència aplicables. Com a mínim, els actius d'informació necessaris per a la prestació dels serveis essencials o importants s'han de sotmetre a una auditoria interna ordinària amb la periodicitat establerta, i sempre que es produeixin canvis significatius en els serveis, en l'arquitectura tecnològica o en el conjunt de mesures de seguretat implantades.
27. Aquestes auditories s'han de realitzar d'acord amb la guia d'auditoria de l'ENS-AD publicada per l'ANC-AD i han d'avaluar, entre d'altres, el compliment dels requisits reglamentaris, l'adequació de la declaració d'aplicabilitat, el nivell d'implantació de les mesures, l'eficàcia dels controls i l'existència de desviacions o no conformitats. L'informe d'auditoria, adreçat a l'òrgan de direcció i al DSI, ha d'incloure les evidències, les conclusions i les recomanacions.
28. A partir d'aquest informe, l'entitat ha de definir i aprovar un Pla d'Accions Correctores (PAC), en què es recullin, per a cada desviació detectada, les mesures a adoptar, els responsables, els terminis, els recursos necessaris i els mecanismes de seguiment i tancament. El DSI és responsable de coordinar l'execució i el seguiment del PAC, i d'informar periòdicament la direcció sobre el seu grau d'avanç i sobre les possibles necessitats addicionals de millora.

## 4. DIFERENCIACIÓ DE LES CATEGORIES

29. D'ara endavant es presentaran els diversos controls de la guia classificats en marcs organitzatiu, operacional i mesures de protecció. Cada control especifica les mesures que s'han d'aplicar per tal d'assolir-los correctament, a més a més s'han diferenciat dos apartats depenent de la categoria a la qual aplica cada mesura: categoria bàsica i/o mitjana.

30. Per assolir la categoria bàsica s'han de complir els punts introduïts dins de la classificació, i per assolir categoria mitjana s'han de tenir en compte tant els de categoria bàsica com els de categoria mitjana.

31. A continuació es presenta un exemple per observar-ne el funcionament.

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits + [R1 o R2 o R3 o R4] | Requisits + [R2 o R3 o R4] + R5 |

Els requisits que es presenten en el control s'hauran d'aplicar a les dues categories, per poder assolir la bàsica a més a més s'haurà de triar un reforç d'entre Reforç 1 (R1), Reforç 2 (R2), Reforç 3 (R3) i Reforç 4 (R4). Per altra banda, per poder arribar a categoria mitjana serà essencial triar un entre Reforç 2 (R2), Reforç 3 (R3) i Reforç 4 (R4) i complir el Reforç 5 (R5).

# 5. [ORG] MARC ORGANIZATIU

32. Tota entitat necessita poder assegurar l'abast dels seus objectius, definint funcions i establint responsabilitats i canals de coordinació. Aquesta estructura permet la gestió del dia a dia de les activitats rutinàries i la resolució ordenada dels incidents que puguin sobrevenir.
33. Tota estructura organitzativa necessita una avaluació constant i una anàlisi de la resposta als incidents de manera que s'aprèn de l'experiència, es corregeixen defectes o febleses i es busca l'excel·lència per mitjà de la millora contínua.
34. L'entitat en matèria de seguretat no pot sinó estar alineada i servir a la missió de l'organisme, ajustant-se a les necessitats dels serveis que es presten.
35. La manca d'una organització formal i efectiva es tradueix en unes prestacions incertes, el resultat de les quals depèn de la fortuna i el bon encert dels membres de l'entitat, sense poder assegurar que es vagin a aconseguir els objectius proposats, ni tan sols pugui dir-se que l'Entitat està sota control.

## 5.1 [ORG.1] POLÍTICA DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

36. És un document d'alt nivell que defineix el significat de "seguretat de la informació (SI)" en una entitat. El document ha d'estar accessible i ser conegut per tots els membres de l'entitat i redactat de manera senzilla, precisa i comprensible. Convé que sigui breu, deixant els detalls tècnics per a altres documents normatius.
37. Ha de contemplar-se els objectius de l'organització, el marc legal on es desenvoluparan les diverses activitats, les funcions i rols de seguretat i les directrius per a estructurar la documentació de seguretat.
38. Estableix les autoritats dins de l'entitat: rols i funcions. La política té caràcter d'obligat compliment. En cas de ser necessari es pot utilitzar la següent guia externa:
    - Guies d'implantació i d'auditoria de l'ENS-AD publicades per l'Agència Nacional de Ciberseguretat d'Andorra (ANC-AD), així com els Components generals del Registre de Productes Certificats i Serveis de Seguretat de les T.I.C, d'acord amb el Reglament aprovat pel Decret 417/2022.
39. Són d'especial rellevància els següents principis bàsics:
    - La seguretat com a procés integral.
    - Revaluació periòdica.
    - Validació per l'alta direcció i/o dels rols responsables de la seguretat de la informació.
40. El principi de seguretat integral i sistemàtica obliga que la responsabilitat d'iniciar, gestionar i controlar el Sistema de gestió de la seguretat de la informació (SGSI) de

l'entitat recaigui sobre l'òrgan de direcció de l'entitat, que delega les tasques associades a aquesta responsabilitat en el DSI de l'entitat, si n'hi ha.

41. El responsable d'implantar l'SGSI de l'entitat ha de garantir-ne l'efectivitat, per la qual cosa ha d'executar les tasques següents:

    - Determinar els lineaments que regularan el marc organitzacional i operacional de la seguretat de la informació de l'entitat, seleccionant-los d'entre els especificats per l'ANC-AD en l'apartat dels Components generals del Registre de Productes Certificats i Serveis de Seguretat de les T.I.C que descriu l'article 7 d'aquest Reglament.
    - Organitzar l'elaboració del pla d'acció per establir els lineaments de la seguretat de l'entitat identificats en el punt anterior, i per gestionar els riscos de seguretat de la informació dels serveis als quals aplica l'ENS-AD, i revisar-lo almenys una vegada a l'any o cada vegada que es faci un canvi en aquests serveis.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27001:2022 | - 4 – Context de l'Entitat |
| ISO/IEC 27002:2022 | - A.5.1 – Política de Seguretat de la Informació<br>- A.5.4 – Responsabilitats de la direcció<br>- A.5.6 – Contacte amb grups d'interès especial<br>- A.5.31 – Identificació de requisits legals, reglamentaris i contractuals<br>- A.5.32 – Drets de propietat intel·lectual<br>- A.6.4 – Procés disciplinari |
| NIST SP 800-53 rev.4 | - [PM-2] Senior Information Security Officer<br>- [PM-11] Mission/Business Process Definition |
| Altres referències | - NIST SP 800-12 - An Introduction to Computer Security. |

## 5.3 [ORG.2] NORMATIVA DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

42. Conjunt de documents que, sense entrar en els detalls, estableixen la manera d'afrontar un cert tema en matèria de seguretat. Defineixen la posició de l'organisme en aspectes concrets i serveixen per a indicar com s'ha d'actuar en cas que una certa circumstància no estigui recollida en un procediment explícit o que el procediment pugui ser imprecís o contradictori en els seus termes.

43. Es disposarà d'una documentació de seguretat seguint els criteris de les guies ANC-STIC.
44. A vegades es denominen "policies" o "standards" (en anglès).
45. Les normes han de centrar-se en els objectius que es desitgen aconseguir, abans que en la manera d'aconseguir-ho. Els detalls els proporcionaran els procediments. Les normes ajuden a prendre la decisió correcta en cas de dubte.
46. Les normes han de descriure el que es considera ús correcte, així com el que es considera ús incorrecte.
47. La normativa té caràcter d'obligat compliment. Això ha de destacar-se, així com les conseqüències derivades del seu incompliment (mesures disciplinàries).
48. Cada norma ha d'indicar la manera de localitzar els procediments que s'han desenvolupat en la matèria tractada. És difícil que la norma cobreixi tots els procediments desenvolupats, però els procediments han d'indicar la norma o normes que desenvolupen.
49. Les normes les han d'escriure persones expertes en la matèria, coneixedores de la postura de la Direcció, de les possibilitats i limitacions de la tecnologia corresponent i amb experiència en els incidents o situacions típiques que poden trobar-se els usuaris. Les normes han de ser revisades pel departament d'assessoria legal, tant per a evitar l'incompliment d'alguna norma de rang superior, com per a introduir registres que puguin ser requerits com a evidències en cas de conflicte.
50. Les normes han de ser realistes i viables. Han de ser concises (sense perdre precisió) i sense ambigüitats. Han d'estar motivades, ser descriptives i definir punts de contacte per a la seva interpretació correcta.
51. Possibles àmbits per a cada normativa:
    - Control d'accés: protecció dels elements d'autenticació i autorització (contrasenyes, targetes, etc.)
    - Lloc de treball net i equips desatesos
    - Protecció enfront de programari maliciós: virus, spyware, adware, entre altres.
    - Desenvolupament d'aplicacions (software)
    - Instal·lació d'aplicacions (software)
    - Accés remot
    - Tele-treball
    - Ús de portàtils
    - Gestió de suports d'informació extraïbles (com cd, claus usb, etc.)
    - Tractament de la informació impresa: copies, emmagatzematge i destrucció
    - Ús del correu electrònic
    - Ús de la web
    - Problemes d'enginyeria social
    - Criteris de classificació de la informació
    - Tractament d'informació de caràcter personal
    - Còpies de seguretat (backups)

- Ús de la criptografia:
  - Gestió de claus
  - Gestió de dispositius
  - Xifrat, signatura i verificació
- Seguretat física:
  - Ús de les instal·lacions
- Relacions amb tercers (proveïdors externs):
  - Acords de confidencialitat
  - Cooperació preventiva
  - Resolució d'incidències
- Formació i conscienciació
- Contrasenyes

52. Són d'especial rellevància els següents principis bàsics:

- Prevenció, reacció i recuperació.
- Revaluació periòdica.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.1 – Polítiques per a la seguretat de la informació<br>- A.5.10 – Ús acceptable de la informació i actius associats<br>- A.5.11 – Devolució d'actius<br>- A.5.14 – Transferència de la informació<br>- A.5.32 – Drets de propietat intel·lectual (IPR)<br>- A.6.6 – Acords de confidencialitat o no divulgació<br>- A.6.7 – Teletreball<br>- A.7.6 – El treball en àrees segures |
| NIST SP 800-53 rev.4 | - Tots els apartats, primer control (XX-1). Per exemple, AC-1 "Access Control Policy and Procedures".<br>- PM-15 - Contacts with Security Groups and Associations |
| Altres referències | - The SANS Security Policy Project http://www.sans.org/resources/policies/<br>- NIST SP800-12 - An Introduction to Computer Security<br>- NSA - Manageable Network Plan |

## 5.4 [ORG.3] PROCEDIMENTS OPERATIUS DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

53. Conjunt de documents que descriuen pas a pas com acomplir una certa activitat. Faciliten les tasques rutinàries, evitant que s'oblidin passos importants. El que mai pot passar és que una certa activitat només sàpiga fer-la una determinada persona; ha d'estar escrit formalment el procediment perquè la persona pugui ser reemplaçada.
54. Un procediment pot estar definit (és comunicat als organismes implicats, es comprèn per la seva part i s'executa regularment conforme al definit) i un procediment pot estar documentat (a més de l'anterior, consta en un document escrit). No tots els procediments es requereixen que estiguin documentats, però sí que haurien d'estar-ho els més crítics per a l'entitat.
55. A vegades es denominen "guies" o "instruccions".
56. Cada procediment ha de detallar:
    - en quines condicions ha d'aplicar-se;
    - qui és el que ha de dur-ho a terme;
    - què és el que cal fer a cada moment, incloent-hi el registre de l'activitat acomplerta;
    - i com es reporten deficiències en els procediments.
57. El conjunt de procediments ha de cobrir un alt percentatge (almenys el 80%) de les activitats rutinàries, així com aquelles tasques que es realitzen amb poca freqüència, però exigeixen seguir uns passos determinats molt precisos.
58. La quantitat de procediments operatius de seguretat dependrà de les activitats que té l'organització, per la qual cosa ha de cobrir cada una. No obstant això, és millor no tenir un procediment que tenir un procediment erroni o antiquat.
59. Ha d'existir un mecanisme perquè els usuaris accedeixin ràpidament a una versió actualitzada dels procediments que els afecten. L'ús de la intranet com a repositori de documents és molt eficaç, encara que cal preveure algunes còpies en paper per a aquelles activitats que cal realitzar quan existeixi un incident o fallada en la intranet.
60. Ha d'existir un procediment perquè els usuaris puguin informar d'errors, inexactituds o mancances en els procediments i es tingui en compte aquestes comunicacions en el procés de millora contínua.
61. Es despondrà d'una sèrie de documents que detallen de forma clara com operar els elements del sistema d'informació.
62. Es requerirà la validació dels procediments de seguretat per l'autoritat corresponent.
63. En la forma que s'ha de tractar la informació s'ha de precisar:
    - El seu control d'accés

- El seu emmagatzematge
- La realització de còpies
- L'etiqueta ment de suports
- La transmissió telemàtica
- Qualsevol altra activitat relacionada amb la informació

64. És d'especial rellevància el següent principi bàsic:
    - Revaluació periòdica.
65. El principi de seguretat integral i sistemàtica obliga que la responsabilitat d'iniciar, gestionar i controlar el Sistema de gestió de la seguretat de la informació (SGSI) de l'entitat recaigui sobre l'òrgan de direcció de l'entitat, que delega les tasques associades a aquesta responsabilitat en el DSI de l'entitat, si n'hi ha.
66. El responsable d'implantar l'SGSI de l'entitat ha de garantir-ne l'efectivitat, per la qual cosa ha d'executar les tasques següents:
    - Determinar els lineaments que regularan el marc organitzacional i operacional de la seguretat de la informació de l'entitat, seleccionant-los d'entre els especificats per l'ANC-AD en l'apartat dels Components generals del Catàleg que descriu l'article 7 del Reglament de l'Esquema nacional de seguretat del Principat d'Andorra.
    - Organitzar l'elaboració del pla d'acció per establir els lineaments de la seguretat de l'entitat identificats en el punt anterior, i per gestionar els riscos de seguretat de la informació dels serveis als quals aplica l'ENS-AD, i revisar-lo almenys una vegada a l'any o cada vegada que es faci un canvi en aquests serveis.
67. Per determinar els lineaments que regularan els marcs organitzacional i operacional de la seguretat de la informació de l'entitat i per a l'elaboració del pla d'acció, s'ha de seguir el procediment d'implantació que l'ANC-AD publicarà al seu lloc web.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.10 – Ús acceptable de la informació i actius associats<br>- A.5.14 – Transferència de la informació<br>- A.5.37 – Documentació de procediments operacionals |
| NIST SP 800-53 rev.4 | - Tots els apartats, primer control (XX-1). Per exemple, AC-1 "Access Control Policy and Procedures".<br>- PM-15 - Contacts with Security Groups and Associations |

## 5.5 [ORG.4] PROCÉS D'AUTORITZACIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

68. Cap sistema d'informació amb responsabilitats sobre la informació que tracta o els serveis que dona, hauria d'admetre elements no autoritzats. La lliure incorporació d'elements acabaria amb la confiança del sistema, en modificar la superfície d'atac i donar lloc a noves vulnerabilitats susceptibles de ser explotades.

69. L'ENS-AD singularitza una sèrie d'elements, sense perjudici que s'apliqui sempre la regla d'"es requereix autorització prèvia" amb caràcter general a tots els components durant tot el seu cicle de vida:

    - Utilització d'instal·lacions, habituals i alternatives.
    - Entrada d'equips en producció, en particular, equips que involucren criptografia.
    - Entrada d'aplicacions en producció.
    - Establiment d'enllaços de comunicacions amb altres sistemes.
    - Utilització de mitjans de comunicació, habituals i alternatius.
    - Utilització de suports d'informació.
    - Utilització d'equips mòbils. S'entendrà per equips mòbils: ordinadors portàtils, PDA, i altres de naturalesa anàloga.
    - Utilització de serveis de tercers, sota contracte o conveni.
    - Utilització d'equips propietat de l'usuari (BYOD – Bring Your Own Device).

70. El procés d'autorització requereix:

    - Que estigui definit en la normativa de seguretat la persona o punt de contacte per a autoritzar un determinat component o actuació.
    - Que existeixi un mecanisme (per exemple, un formulari) per a sol·licitar l'autorització, indicant el que es desitja i la motivació; aquesta sol·licitud haurà d'incorporar els següents elements:
        - descripció precisa de l'element o actuació per al qual se sol·licita autorització,
        - descripció precisa de les activitats per a les quals es requereix el nou component,
        - justificació que el nou component no afecta altres funcionalitats del sistema,
        - si el nou component introdueix possibles vulnerabilitats (és a dir, si exposa al sistema a noves o renovades amenaces), haurà d'annexar-se una anàlisi de riscos i les mesures que es prenen per a gestionar-lo; aquesta anàlisi de riscos tindrà la intensitat proporcionada a la categoria del sistema, com s'estableix en [op.pl.1],
        - justificació que no es viola cap normativa de seguretat,

- i informació dels procediments de seguretat que són aplicables al cas o, si calgués, la necessitat de desenvolupar algun nou procediment específic.

- Que es requereixi l'aprovació formal de la petició (és a dir, la signatura del responsable) abans de l'actuació.

71. Si es requereixen nous procediments, l'autorització pot ser temporal amb un termini límit per a desenvolupar els nous procediments i formalitzar l'autorització definitiva.

72. L'autorització només cobrirà la utilització dels nous recursos per als objectius explícitament aprovats.

73. És d'especial rellevància el següent principi bàsic:

- Revaluació periòdica.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.2 – Rols i responsabilitats en seguretat de la informació<br>- A.5.36 – Compliment de les polítiques, i normes de seguretat de la informació |
| NIST SP 800-53 rev.4 | - [PM-10] Security Authorization Process |
| Altres referències | - NIST SP800-12 - An Introduction to Computer Security<br>- Manageable Network Plan |

# 6 MARC OPERACIONAL

74. Mesures a prendre per a protegir l'operació del sistema com a conjunt integral de components per a un fi.

## 6.3 [OP.PL] PLANIFICACIÓ

75. En els controls de planificació es contempla els punts febles del sistema i tot allò que els protegeix. Tindríem com a actius les eines d'anàlisi de riscs com podrien ser les plataformes ERM (gestió de riscs empresarials) o alguna aplicació especialitzada per mantenir registre i seguiments dels riscs identificats. També es troba el personal especialitzat que s'encarrega de fer avaluacions i proposar mesures de seguretat. Entra dins de la classificació tota la documentació referent a les situacions de vulnerabilitat i els components que s'adquireixen, i totes les polítiques de seguretat, els procediments i diferents informes d'avaluació.
76. Activitats prèvies a la posada en explotació.
77. Són d'especial rellevància els següents principis bàsics:
    - La seguretat com un procés integral.
    - Gestió de la seguretat basada en els riscos.

### 6.3.1 [OP.PL.1] ANÀLISI DE RISCOS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits+R1 |

78. Emprem l'expressió "anàlisi de riscs" en el sentit de "risk assessment" en la terminologia d'ISO.
79. L'anàlisi de riscos permet:
    - validar el conjunt de mesures de seguretat implantat,
    - detectar la necessitat de mesures addicionals
    - i justificar l'ús de mesures de protecció alternatives.
80. Tota anàlisi de riscos ha d'identificar i prioritzar els riscos més significatius a fi de conèixer els riscos als quals estem sotmesos i prendre les mesures oportunes, tècniques o d'un altre tipus.
81. L'anàlisi de riscos ha de ser una activitat recurrent; és a dir, s'ha de mantenir actualitzada.
82. L'aspecte formal exigeix que l'anàlisi estigui documentada i aprovada. La documentació ha d'incloure els criteris utilitzats per a seleccionar i valorar actius, amenaces i salvaguardes.
83. Una anàlisi de riscos ha de ser realitzada:

- durant l'especificació d'un nou sistema, per a determinar els requisits de seguretat que han d'incorporar-se a la solució,
- durant el desenvolupament d'un nou sistema, per a analitzar opcions,
- i durant l'operació del sistema, per a ajustar a nous actius, noves amenaces, noves vulnerabilitats i noves salvaguardes.

84. Tot sistema opera sota una situació d'un cert risc residual. El risc residual ha d'estar documentat i aprovat pel responsable de la informació i del servei corresponent(s).

85. R1: realització d'una anàlisi de riscos semiformal, usant un llenguatge específic, amb un catàleg bàsic d'amenaces i una semàntica definida. Una presentació amb taules que:

    - Valori qualitativament els actius més valuosos.
    - Quantifiqui les amenaces més probables.
    - Valori les salvaguardes que protegeixen d'aquestes amenaces.
    - Valori el risc residual.

86. Són d'especial rellevància els següents principis bàsics:

    - La seguretat com a procés integral.
    - Gestió de la seguretat basada en els riscos.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27001:2022 | - 6.1 – Accions per abordar riscos i oportunitats<br>- 6.1.1 - General<br>- 6.1.2 – Avaluació de riscos<br>- 6.1.3 – Tractament dels riscos<br>- 8.2 – Avaluació de riscos<br>- 8.3 – Tractament dels riscos |
| NIST SP 800-53 rev.4 | - [RA] Risk Assessment<br>- [PM-9] Risk Management Strategy |
| Altres referències | - NIST SP 800-30 - Risk Management Guide for Information Technology Systems<br>- NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach<br>- NIST SP 800-39 - Managing Risk from Information Systems: An Organizational Perspective<br>- ISO/IEC 27005 - Information security risk management<br>- ISO/IEC 31000 – Gestió del risc – Principis i directrius |

### 6.3.2 [OP.PL.2] ARQUITECTURA DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits+R1 |

87. El que es busca amb aquesta mesura de seguretat és tenir una visió global, íntegra i integradora de com és el sistema d'informació, com es gestiona i com es defensa. Aquesta mesura és bàsicament documental i descriptiva.
88. L'arquitectura de seguretat és elaborada sota la direcció del Responsable del Sistema, i és aprovada pel Responsable de la Seguretat.
89. R1: sistema de gestió, relatiu a la planificació, organització i control dels recursos relatius a la seguretat de la informació.
90. Són d'especial rellevància els següents principis bàsics:
    - Prevenció, reacció i recuperació.
    - Línies de defensa.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.9 - Inventari d'informació i altres actius associats<br>- A.8.27 - Arquitectura segura de sistemes i principis d'enginyeria |
| NIST SP 800-53 rev.4 | - [CM-8] Information system Component Inventory<br>- [PM-5] Information Systems Inventory<br>- [PM-7] Enterprise Architecture<br>- [PM-8] Critical Infrastucture Plan<br>- [SA-5] Information System Documentation<br>- [SA-8] Security Engineering Principles<br>- [PL-8] Information Security Architecture |
| Altres referències | - Manageable Network Plan |

### 6.3.3 [OP.PL.3] ADQUISICIÓ DE NOUS COMPONENTS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

91. L'adquisició de nous components ha de:
    - tenir en compte l'anàlisi de riscos [op.pl.1];
    - ajustar-se a l'arquitectura de seguretat [op.pl.2];
    - preveure els recursos necessaris, esforç i mitjans econòmics per a:
        - La implantació inicial.

- El manteniment al llarg de la seva vida útil.
- Atendre a l'evolució de la tecnologia.

- i, en tot moment, s'atendrà tant les necessitats tècniques com a la conscienciació i formació de les persones que treballaran amb els components.

92. En el cas de categoria mitjana, si es volen adquirir nous components, s'ha de tenir en compte el Guia ANC-STIC-100 "Registre de Productes Certificats i Serveis de Seguretat de les T.I.C." per a veure si són components certificats.

93. És d'especial rellevància el següent principi bàsic:

- Revaluació periòdica.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.8 – Seguretat de la informació en la gestió de projectes |
| NIST SP 800-53 rev.4 | - [PL-1] Security Planning Policy and Procedures<br>- [PL-2] System Security Plan<br>- [PL-7] Security Concept of Operations<br>- [PL-8] Information Security Architecture<br>- [SA-1] System and Services Acquisition Policy and Procedures<br>- [SA-3] System Development Life Cycle<br>- [SA-4] Acquisition Process<br>- [SA-8] Security Engineering Principles<br>- [SA-12] Supply Chain Protection |
| Altres referències | - NIST SP 800-18 - Guide for Developing Security Plans for Federal Information Systems<br>- NIST SP 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process |

### 6.3.4 [OP.PL.4] DIMENSIONAMENT / GESTIÓ DE CAPACITATS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

94. Convé destacar que aquesta mesura de seguretat no és merament tècnica, sinó que té implicacions pressupostàries i per això ha de gestionar-se amb temps perquè les necessitats quedin degudament recollides en els pressupostos. Si en totes les mesures de seguretat cal fugir de la improvisació, en aquesta amb més raó.

95. Cal fer veure que en entorns flexibles com és l'ús de recursos en el núvol, el dimensionament efectiu del sistema pot ser dinàmic, adequant-se a les necessitats del servei.

96. R1: millora contínua de la gestió de la capacitat:

    - Realitzar una previsió de la capacitat i mantenir-la actualitzada durant tot el cicle de vida del sistema.
    - Utilitzar eines i recursos pel monitoratge de la capacitat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.6 – Gestió de capacitats |
| NIST SP 800-53 rev.4 | - [SA-2] Allocation of Resources<br>- [AU-4] Audit Storage Capacity |

### 6.3.5 [OP.PL.5] COMPONENTS CERTIFICATS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

97. Totes les paraules es queden curtes per tal d'insistir en la necessitat de recórrer a components provats, avaluats i certificats. Desenvolupar els mateixos components exigeix un apreciable nivell de formació, un considerable esforç i una capacitat de manteniment de la seguretat enfront de vulnerabilitats, defectes i noves amenaces. Tot això se simplifica notablement recorrent a components de terceres parts sempre que aquests components estiguin assegurats per a protegir-nos d'acord amb les nostres necessitats i enfront de les nostres amenaces. Això vol dir que abans d'adquirir un producte, per molt acreditat que estigui, cal cerciorar-se que cobreix les nostres necessitats específiques.

98. L'ús de components certificats requereix

    - un esforç preliminar de validació: idoneïtat per al cas;
    - un esforç d'implantació: adquisició i formació;
    - i un esforç continu d'actualitzacions per a no perdre les garanties inicials.

99. Quan s'avaluen productes, és freqüent establir una escala de nivells. En el cas de Criteris Comuns (ISO 15408), aquesta és l'escala:

    **EAL1 – Provat funcionalment**
    EAL1 és aplicable quan es necessita alguna confiança en el funcionament correcte, però les amenaces a la seguretat no són importants. Serà útil quan es necessiti garantia independent en la controvèrsia entre la deguda cura que s'ha exercit i la protecció de la informació personal o similar.

    EAL1 proporciona una avaluació del TOE disponible per al client, incloent-hi proves independents sobre una especificació i un examen dels manuals proporcionats. És

pensa que una avaluació EAL1 pugui ser realitzada amb èxit sense l'ajuda del fabricant del TOE i amb una despesa mínima.

Una avaluació a aquest nivell ha de proporcionar evidència que el TOE funciona d'una manera consistent amb la seva documentació i que proporciona protecció útil contra les amenaces identificades.

**EAL2 – Provat estructuralment**
EAL2 necessita la cooperació del fabricant pel que fa a lliurar informació de disseny i resultats de proves, però no ha d'exigir més esforç per part del fabricant del qual suposa una pràctica comercial bona. Per tant, no ha de requerir una inversió substancialment major en costos o temps.

EAL2 és, per consegüent, aplicable en aquelles circumstàncies en les quals fabricants o usuaris necessiten un nivell de seguretat, entre baix i moderat, garantit independentment davant la falta de disponibilitat immediata del registre de desenvolupament complet. Aquesta situació pot sorgir en donar seguretat a sistemes heretats o en els quals l'accés al fabricador pot estar limitat.

**EAL3 – Provat i verificat metòdicament**
EAL3 permet a un fabricant conscienciós obtenir garantia màxima de l'enginyeria de seguretat en la fase de disseny sense l'alteració substancial de les pràctiques de desenvolupament vàlides existents.

EAL3 és aplicable en aquelles circumstàncies en les quals fabricants o usuaris necessiten un nivell moderat de seguretat garantit independentment i una completa recerca del TOE i el seu desenvolupament sense necessitat de reenginyeria substancial.

**EAL4 – Dissenyat, provat i revisat metòdicament**
EAL4 permet a un fabricant obtenir garantia màxima de l'enginyeria de seguretat basada en correctes pràctiques de desenvolupament comercial que, fins i tot sent rigorós, no requereix un coneixement o destresa especialitzats substancials ni altres recursos. EAL4 és el nivell més alt que permet que sigui econòmicament factible aplicar CC a una línia de producte ja existent.

EAL4 és, per consegüent, aplicable en aquelles circumstàncies en les quals fabricants o usuaris necessiten un nivell de seguretat, entre moderat i alt, garantit independentment de TOEs convencionals i estan disposats a costejar despeses addicionals d'enginyeria específica de seguretat.

**EAL5 – Dissenyat i provat semiformalment**
EAL5 permet a un fabricant obtenir garantia màxima de l'enginyeria de seguretat basada en pràctiques de desenvolupament comercial rigoroses secundades per una

moderada aplicació de tècniques específiques d'enginyeria de seguretat. En aquest cas el TOE probablement es dissenya i desenvolupi amb la intenció d'aconseguir el nivell de garantia EAL5. És probable que el cost addicional atribuïble als requisits d'EAL5, comparat al cost que suposa un desenvolupament rigorós sense l'aplicació de tècniques especialitzades, no sigui gran.

EAL5 és, per consegüent, aplicable en aquelles circumstàncies en les quals fabricants o usuaris necessitin un nivell alt de seguretat, garantit independentment, en un desenvolupament previst i requereix un enfocament de desenvolupament rigorós sense incórrer en despeses no raonables atribuïbles a les tècniques d'enginyeria específica de seguretat.

**EAL6 – Dissenyat, provat i revisat semiformalment**
EAL6 permet als fabricants obtenir alta garantia de l'aplicació de tècniques d'enginyeria de seguretat en un entorn de desenvolupament rigorós per a produir un TOE específic per a protegir els recursos d'alt valor contra riscos significatius.

EAL6 és, per consegüent, aplicable al desenvolupament de TOEs de seguretat per a la seva aplicació en situacions d'alt risc on el valor dels recursos protegits justifica el cost addicional.

**EAL7 – Dissenyat, provat i revisat formalment**
EAL7 és aplicable al desenvolupament de TOEs de seguretat per a la seva aplicació en situacions de risc extremadament alt i/o on l'alt valor dels recursos justifica el cost més gran. L'aplicació pràctica d'EAL7 es limita actualment a TOEs amb una funcionalitat estrictament dirigida a la seguretat que permet una extensa anàlisi formal.

100. L'ENS-AD només requereix la consideració de productes certificats. No obstant això, cal fer les següents indicacions:

- Un nivell EAL1, EAL2 seria recomanable per a qualsevol sistema.
- Nivells per sobre d'EAL3 són sempre interessants, però probablement desproporcionats per a sistemes adscrits a l'ENS-AD, excepte enfront d'amenaces extremes

101. Guies ajuda ENS-AD:

- Guia ANC-STIC-100 "Registre de Productes Certificats i Serveis de Seguretat de les T.I.C." (es tracta d'una guia amb constants modificacions i actualitzacions, cal mirar sempre l'última versió).

102. S'utilitzarà el ANC-STIC-100 per seleccionar els productes i serveis subministrats per un tercer que formin part de l'arquitectura de seguretat del sistema.

103. La informació ha de ser protegida enfront de les amenaces TEMPEST d'acord amb la normativa en vigor.

104. Cada producte i serveis inclourà en la seva descripció una llista de components de software.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| Altres referències | - NIST SP 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products<br>- NIST SP 800-36 – Guide to Selecting Information Technology Security Products<br>- ISO/IEC 15408-1:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model<br>- ISO/IEC 15408-2:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements<br>- ISO/IEC 15408-3:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements<br>- ISO/IEC 18045:2005 - Information technology – Security techniques – Methodology for IT security evaluation<br>- ISO/IEC TR 19791:2006 - Information technology – Security techniques – Security assessment of operational systems |

### 6.3.6 [OP.PL.6] PLA DE SEGURETAT

105. El Pla de seguretat de l'entitat (d'ara endavant, "PSE") és el conjunt de documents estratègics definidors de les polítiques generals d'una entitat crítica o una entitat equivalent a entitat crítica per garantir la protecció i la resiliència de les infraestructures crítiques que posseeix o gestiona. El PSE ha de contenir com a mínim els documents següents:

- La política general de seguretat de l'entitat, que inclou, com a mínim:
  - La descripció de les infraestructures crítiques compartida amb l'ANC-AD per incloure-les al CNIC.
  - Els procediments de gestió i manteniment de la seguretat.
  - Els procediments establerts per a la comunicació i l'intercanvi d'informació relativa a la protecció d'infraestructures crítiques.
  - La metodologia d'anàlisi de risc (amenaces físiques i de ciberseguretat).

- L'estructura de govern de la seguretat de l'entitat juntament amb la descripció de les funcions i les responsabilitats de cada rol de l'organigrama corresponent.
- Les dades de contacte del seu DSI, o de l'equivalent en el cas d'entitats equivalents a entitats crítiques, i dels DSI de les entitats que presten els serveis essencials que depenen d'aquestes darreres, així com de les persones que els substituiran quan no estiguin disponibles.

- La relació de serveis essencials que depenen de cadascuna de les infraestructures crítiques que posseeix o gestiona l'entitat.
- La relació de dependències de cada infraestructura crítica amb altres infraestructures crítiques posseïdes o gestionades per la mateixa entitat o una altra entitat.
- El resultat de l'anàlisi de risc de cadascuna de les infraestructures crítiques posseïdes o gestionades per l'entitat.
- L'inventari dels serveis subcontractats que puguin impactar de qualsevol manera en les infraestructures crítiques. Per a cadascun d'aquests serveis, juntament amb la descripció del possible impacte i la descripció del servei subcontractat, s'ha d'identificar l'entitat subcontractada, els certificats que té en matèria de seguretat i la seu des de la qual presta el servei subcontractat, així com els nivells de servei acordats. D'igual forma, s'ha de descriure la metodologia mitjançant la qual es duu a terme la comprovació del compliment per part de l'entitat crítica o equivalent a entitat crítica dels protocols de seguretat implementats en el seu cas.
- La relació de mesures tècniques i organitzatives (inclosos els procediments d'alertes i de gestió de crisi) que es consideren adequades i proporcionades per garantir la seguretat i resiliència de cada infraestructura crítica, documentades amb un nivell de detall suficient per aconseguir els objectius de l'entitat, tenint en compte els riscos detectats. S'ha d'indicar quines d'aquestes mesures són permanents, i quines són graduals i només s'activaran a partir d'un determinat nivell de risc i d'amenaça.

  Aquestes mesures han d'incloure, específicament, els controls d'accés segur dels usuaris, amb requisits com l'autenticació multifactor, controls de sessió, política de canvis de credencials, control d'accessos privilegiats, així com procediments d'accés en situacions d'emergència.
- La relació de mesures tècniques i organitzatives que ja estan implementades o preparades per activar-se en cada infraestructura crítica, fent referència, si escau, a les esmentades en el punt anterior.
- La descripció de les mesures complementàries de seguretat adoptades voluntàriament per l'entitat per reforçar la protecció de les infraestructures crítiques, especialment en cas de situacions excepcionals, com canvis sobtats en l'amenaça, vulnerabilitats descobertes, o alertes de seguretat de les autoritats

competents. Aquestes mesures poden incloure controls addicionals, mecanismes de supervisió reforçada, plans de redundància, accions de sensibilització interna o auditories internes addicionals.

106. S'autoritza l'ANC-AD a ampliar el contingut mínim dels PSE per a alguna o totes les entitats o equivalents a entitats crítiques.

107. L'òrgan de direcció de l'entitat, si escau, amb la col·laboració del seu DSI, és responsable de:

- Crear sense dilació indeguda el PSE de l'entitat.
- Custodiar els documents que formen el seu PSE i controlar-hi l'accés d'acord amb els nivells de seguretat associats als seus continguts, fins i tot mentre es creen o modifiquen.
- Executar el PSE.
- Monitorar i controlar l'execució del PSE.
- Adequar el PSE com correspongui a la seva realitat i a les directrius que rebi de la seva autoritat competent o de l'ANC-AD.
- Posar el PSE a disposició de l'autoritat competent corresponent.
- Comunicar cada nova versió del PSE a l'ANC-AD sense demora indeguda i, en qualsevol cas, en el termini màxim d'una setmana a comptar de l'endemà de l'aprovació del PSE, i amb independència de les circumstàncies que hagin donat lloc a la nova versió i de si els documents han estat o no objecte de modificacions.
- Comunicar a l'ANC-AD, sense dilació indeguda, l'adopció de qualsevol mesura de seguretat que no s'hagi inclòs en el PSE per tenir naturalesa temporal.

108. L'ANC-AD és responsable d'aprovar els PSE de les entitats crítiques i les entitats equivalents a entitats crítiques i, si escau, de proposar actualitzacions per a aquests plans.

### 6.3.7 [OP.PL.7] DECLARACIÓ D'APLICABILITAT

109. Per donar compliment als requisits mínims establerts en el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra, les entitats compreses en el seu àmbit d'aplicació adopten les mesures de seguretat referides en la declaració d'aplicabilitat que descriu l'article 12 d'aquest Reglament.

110. El DSI està autoritzat a no implementar una d'aquestes mesures de seguretat si no redueix els riscos o és massa costosa en comparació amb la reducció dels riscos derivats d'aplicar-la, o si considera que els riscos que cobreix la mesura ja estan coberts per altres mesures tal com indica la mateixa declaració d'aplicabilitat. Si el DSI decideix no implementar alguna de les mesures, ha d'informar els òrgans de direcció

de l'entitat que l'ha designat sobre els riscos derivats d'aquesta no implementació, per tal que siguin capaços de prendre la decisió d'aprovar o no les mesures de seguretat proposades, d'acord amb l'obligació que els imposa el que està establert a l'apartat 1 de l'article 17 de la Llei NIS-AD.

111. L'existència d'una referència sobre les mesures de seguretat necessàries per als actius d'informació bàsics no eximeix el DSI de la seva obligació de gestionar els riscos, fins i tot els associats a actius d'informació o amenaces no totalment previstes en el Catàleg que descriu l'article 7 del Reglament mencionat.

112. El DSI ha de signar la declaració d'aplicabilitat i comunicar-la a l'autoritat competent que correspongui a l'entitat.

## 6.4 [OP.ACC] CONTROL D'ACCÉS

113. El control d'accés cobreix el conjunt d'activitats preparatòries i executives perquè una determinada entitat pugui, o no, accedir a un recurs del sistema per a realitzar una determinada acció.

114. Amb el compliment de totes aquestes mesures es garanteix que ningú accedirà a recursos sense autorització. A més, ha de quedar registrat l'ús del sistema ([op.exp.8]) per a poder detectar i reaccionar a qualsevol fallada accidental o deliberada.

115. El control d'accés que s'implanta en un sistema real és un punt d'equilibri entre la comoditat d'ús i la protecció de la informació. En sistemes de categoria bàsica, es preval la comoditat, mentre que en sistemes de categoria alta es preval la protecció.

116. Com a actius dels diferents controls d'accés es troba els diferents sistemes de Gestió d'Identitat i accés (IAM), que gestionen la creació, ús i desactivació dels diferents comptes dels usuaris, també les eines d'autenticació multifactor (MFA) que inclou mètodes biomètrics, targetes intel·ligents, contrasenyes segures… Els mateixos usuaris i tots els permisos als quals tenen accés i el personal amb l'autoritat corresponent per donar-los.

117. Aquestes mesures solen venir recollides en la literatura de seguretat sota els epígrafs:

- I&A- Identificació i Autenticació
- Control d'Accés

### 6.4.1 [OP.ACC.1] IDENTIFICACIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits +R1 |

118. S'ha d'assignar un identificador singular per a cada entitat (usuari o procés) que accedeix al sistema i per a cada rol de cada entitat enfront del sistema (administrador, usuari, etc.).

119. D'aquesta manera:

- es pot saber qui rep quins drets d'accés,
- i es pot saber qui ha fet que, i quin ha fet per a corregir o per a perseguir.

120. La identificació d'usuaris sol anar associada a un "compte d'usuari". Sovint es parla de "drets d'un compte" per a referir-se als drets del titular del compte. Es diu que els drets d'un usuari són els del seu compte en el sistema.

121. S'han de gestionar els comptes d'usuari:

- Els comptes han de ser inhabilitats quan:
  - l'usuari deixa l'entitat;
  - cessa en la funció per a la qual es requeria el compte d'usuari;
  - la persona que ho va autoritzar dona ordre en contra.
- Els comptes inhabilitats han de ser retinguts durant el període necessari per a atendre les necessitats de traçabilitat dels registres d'activitat associats a un compte (període de retenció).
- No han d'existir 2 comptes amb el mateix identificador, de manera que no es puguin confondre dos usuaris ni es puguin imputar activitats a usuaris diferents.

122. R1: identificació avançada:

- La identificació de l'usuari permetrà al responsable del sistema singularitzar a la persona associada i les seves responsabilitats en el sistema.
- Les dades d'identificació seran utilitzades pel sistema per determinar els privilegis de l'usuari d'acord amb els requisits de control d'accés establerts en la documentació de seguretat.
- S'assegurarà l'existència d'una llista actualitzada dels usuaris autoritzats.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.16 – Gestió de la identitat<br>- A.5.17 – Informació d'autenticació<br>- A.8.2 – Gestió de privilegis d'accés |
| NIST SP 800-53 rev. 4 | - [AC-2] Account Management<br>- [AC-14] Permitted Actions without Identification or Authentication<br>- [IA-2] Identification and Authentication (Organizational Users)<br>- [IA-3] Device Identification and Authentication<br>- [IA-4] Identifier Management<br>- [IA-5] Authenticator Management |

| | |
|---|---|
| | - [IA-8] Identification and Authentication (Non-Organizational Users) |

### 6.4.2 [OP.ACC.2] REQUISITS D'ACCÉS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

123. És necessari que tant els sistemes en producció com els previs a la seva posada en explotació comptin amb un mecanisme de control d'accés, basat en l'identificador assignat a cada entitat (usuari o procés) i un mecanisme d'autenticació.

124. Per a definir aquest control d'accessos, ha de definir-se un document o matriu on s'especifiqui quins són els components del sistema i els seus fitxers o registres de configuració i es relacionin amb els diferents permisos d'usuari, de manera que únicament puguin accedir als recursos els usuaris autoritzats.

125. Serà el responsable de cada informació o servei, qui especifiqui els drets d'accés a aquests, responsabilitzant-se de l'assignació d'autorització i nivell d'accés a aquest.

126. Accés autenticat amb certificat digital /cartera digital o altres mètodes segurs.

Els usuaris interns i externs que accedeixin a aplicatius, serveis o entorns de gestió afectats per l'ENS-AD hauran de fer-ho mitjançant certificat digital, cartera digital o altres mitjans robustos. En cas de voler utilitzar una altra alternativa, aquesta serà sol·licitada i posteriorment aprovada/denegada per part de l'ANC-AD o l'AFA segons correspongui.

127. Requisits del mecanisme d'autenticació.

El mecanisme d'autenticació ha de garantir el principi de no-repudi, ser compatible amb normatives com eIDAS o equivalents locals, i integrar-se amb la infraestructura de clau pública (PKI) de l'entitat o proveïdor de confiança autoritzat.

128. Registre i control d'accessos digitals.

Tots els accessos realitzats mitjançant certificats han de quedar registrats, incloent-hi moment d'accés, aplicació consultada i operacions crítiques efectuades. Aquest registre s'ha de conservar segons el termini legal establert.

129. Guies d'ajuda ENS-AD:

- Guia ANC-STIC-100 "Registre de Productes Certificats i Serveis de Seguretat de les T.I.C." (es tracta d'una guia amb constants modificacions i actualitzacions, cal mirar sempre l'última versió).

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.15 – Control d'accés<br>- A.5.17 – Informació d'autenticació<br>- A.8.3 – Restricció de l'accés a la informació |

| | |
|---|---|
| | - A.8.4 – Accés al codi font<br>- A.8.18 – Ús dels recursos del sistema amb privilegis especials |
| NIST SP 800-53 rev. 4 | - [AC-3] Access Enforcement<br>- [AC-4] Information Flow Enforcement<br>- [AC-6] Least Privilege<br>- [AC-24] Access Control Decisions<br>- [CM-5] Access Restrictions for Change<br>- [MP-2] Media Access |
| Altres referències | - Manageable Network Plan<br>○ Milestone 5: Control Your Network (User Access) |

### 6.4.3 [OP.ACC.3] SEGREGACIÓ DE FUNCIONS I TASQUES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

130. La segregació de funcions té dos objectius:

- prevenir errors;
- i impedir l'abús de privilegis per part dels usuaris autoritzats.

131. Ha de documentar-se un esquema de funcions i tasques en el qual es contemplen les que són incompatibles en una mateixa persona. La incompatibilitat ha de garantir que per a dur a terme un procés o activitat crítica sempre es requereixen almenys 2 persones.

132. Ha d'establir-se un procediment d'assignació de persones a funcions i tasques a persones que garanteixi que no es viola l'esquema anterior, ni quan s'assignen responsabilitats inicialment, ni quan s'actualitzen.

133. Cal evitar que les persones que treballen en l'operació diària del sistema participin en el desenvolupament d'aplicacions (desenvolupadors) o en la seva configuració (administradors):

- Ningú pot autoritzar-se a si mateix
- Els desenvolupadors no poden modificar dades d'explotació
- Els desenvolupadors no poden passar programari a explotació
- Els desenvolupadors no poden configurar programari en explotació
- Els operadors ni desenvolupen programari ni poden modificar els desenvolupaments
- Els usuaris ni desenvolupen ni poden modificar els desenvolupaments
- Els usuaris ni configuren ni poden modificar la configuració

134. Cal evitar que les persones que treballen en l'auditoria o supervisió participin en qualsevol altra funció.

135. Sempre que es pugui les persones que autoritzin i les que controlen l'ús seran diferents.

136. Haurà de prestar-se una especial atenció als rols associats a comptes d'administració del sistema (administració d'equips, d'aplicacions, de comunicacions, de seguretat), fragmentant les funcions administratives entre diverses persones quan la categoria del sistema el requereixi. En tot cas el nombre de persones amb drets d'administració ha de ser el més reduït possible sense menyscapte de la usabilitat del sistema.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.3 – Segregació de funcions<br>- A.8.3 – Restricció de l'accés a la informació<br>- A.8.19 – Instal·lació del software en sistemes de producció |
| NIST SP 800-53 rev. 4 | - [AC-5] Separation of Duties |

### 6.4.4 [OP.ACC.4] PROCÉS DE GESTIÓ DE DRETS D'ACCÉS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

137. Tot accés estarà prohibit excepte autorització expressa.

138. Es tindrà en compte el principi de mínim privilegi. Els privilegis de cada entitat es reduiran al mínim per complir les seves obligacions i funcions.

139. La necessitat d'accés ha de venir per escrit de part del responsable de la informació o procés al qual se li concedirà accés.

140. En l'estructuració dels drets d'accés es tenen en compte les necessitats de cada usuari segons la seva funció en l'entitat i les tasques que té encomanades.

141. El reconeixement de la necessitat d'accés ha de ser reassegurat periòdicament, extingint-se quan no es demostri positivament que la necessitat perdura.

142. Haurà de prestar-se una especial atenció als comptes d'administració del sistema (administració d'equips, d'aplicacions, de comunicacions, de seguretat), establint procediments àgils de cancel·lació i mecanismes de monitoratge de l'ús que es fa d'elles.

143. S'establirà una política específica d'accés remot, requerint autorització expressa.

144. Per un servei d'accés remot segur s'haurà d'implementar el sistema amb equipament especialitzat que permeti als usuaris remots accedir a la seva entitat i a les aplicacions indicades en cada cas. S'han d'incloure almenys aquestes capacitats:

- Servei d'acabament de túnels VPN.
- Suport de VPN-SSL/TLS, Ipsec i ActiveSync.

145. L'estat de l'equip dels usuaris ha de comptar amb mecanismes de seguretat i protecció (antivirus instal·lat, antivirus actualitzat...) d'acord amb les polítiques de seguretat.

146. Els accessos que s'han de contemplar són:

- Accés sense client.
- Accés amb client lleuger, entenent com a tal, l'afegit que s'executa sobre el mateix navegador.
- Accés amb client pesant.

147. S'ha de poder respondre automàticament els problemes de connectivitat dels usuaris en remot.

148. Es pot utilitzar split tunneling, per separar el trànsit destinat a la xarxa interna que passaria per a la VPN, de l'externa.

149. Suport de múltiples plataformes de client: Windows, Mac, Linux, iOS, Android, així com aquelles altres que poguessin estar àmpliament esteses al mercat durant la durada de l'acord marc.

150. Autenticació mitjançant diversos mecanismes: certificats, targetes intel·ligents, tokens, programari, etc.

151. Possibilitat d'autenticació mitjançant doble factor. Els equips hauran de tenir capacitat d'integració amb els sistemes d'autenticació d'usuaris més comuns del mercat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.18 – Drets d'accés<br>- A.8.3 - Restricció de l'accés a la informació |
| NIST SP 800-53 rev. 4 | - [AC-3] Access Enforcement<br>- [AC-24] Access Control Decisions<br>- [CM-5] Access Restrictions for Change |
| Altres referències | - Manageable Network Plan<br>o Milestone 5: Control Your Network (User Access) |

### 6.4.5 [OP.ACC.5] MECANISME D'AUTENTICACIÓ (USUARIS EXTERNS)

| Categoria | Bàsica | Mitjana |
|---|---|---|

| | | |
|---|---|---|
| | Requisits + [R1 o R2 o R3 o R4] | Requisits + [R2 o R3 o R4] + R5 |

152. És el mecanisme que permet validar la identitat d'un usuari. És crític ja que la identificació de l'usuari és, en general, fàcilment accessible.

153. Típicament els mecanismes d'autenticació recorren:

- A alguna cosa que es coneix (un secret, per exemple, una contrasenya)
- A alguna cosa que es té (un objecte, per exemple, una targeta o una clau)
- A alguna cosa que és propi de l'usuari (característiques biomètriques)

154. A vegades aquests mecanismes s'empren per parells per a dificultar la falsificació i guanyar temps enfront de la pèrdua d'algun dels mecanismes. Com, per exemple:

- Una targeta + un PIN
- Una targeta + una característica biomètrica
- Una característica biomètrica + una contrasenya

155. Cada mecanisme té els seus punts febles que han d'atallar-se per mitjà de normativa i procediments que regulin el seu ús, període de validesa i gestió d'incidències com ara la pèrdua per part de l'usuari legítim.

| Nivell de les dimensions de seguretat | | ENS-AD | |
|---|---|---|---|
| Factors d'autenticació | | Doble factor d'autenticació | |
| Alguna cosa que se sap | contrasenyes<br>claus concertades<br>PIN | amb cautela | amb cautela |
| Alguna cosa que es té | *tokens*<br>targeta | ok | criptogràfics |
| Alguna cosa que s'és | biometria | ok | ok |

Taula 3. Mecanismes d'autenticació segons nivell de dimensions de seguretat.

156. Les credencials hauran d'activar-se una vegada estiguin sota control efectiu de l'usuari (per exemple, contrasenya temporal d'un sol ús) i seran exclusivament per a aquest usuari, prohibint-se la seva divulgació o ús compartit. És a dir, l'usuari haurà de reconèixer que ha rebut les credencials i que coneix i accepta les obligacions que implica la seva tinença, en particular, el deure de custòdia diligent, protecció de la seva confidencialitat i informació immediata en cas de pèrdua.

157. Les credencials caducaran amb una periodicitat marcada per la política de l'entitat, encara que l'entitat (persona, equip o procés) faci ús habitual d'elles.

158. Les credencials es retiraran i seran inhabilitades quan l'entitat (persona, equip o procés) que autentiquen:

- Acaba la seva relació amb el sistema
- Després d'un període definit de no utilització

159. A més, ha de contemplar-se la possibilitat que les aplicacions i altres elements tecnològics de seguretat dels quals es faci ús, sobretot si s'usen productes comercials, no tinguin la capacitat per a permetre una adequada configuració dels mecanismes d'autenticació atès l'ENS-AD i a la categoria del sistema. Per això hauran de tenir-se en compte les següents opcions:

- Adquirir productes amb la capacitat de complir els requisits exigits.
- Disposar d'altres elements o mesures prèvies que supleixin les mancances dels requisits exigits (per exemple, autenticació contra LDAP o Directori Actiu (AD), màquines de salt per a autenticar-se en elements de seguretat amb configuració limitada, etc.).
- Reemplaçar les mesures de seguretat per altres compensatòries sempre que es justifiqui documentalment que protegeixen igual o millor el risc sobre els actius i sigui aprovat formalment pel Responsable de la Seguretat.

**Contrasenyes (secrets compartits en general)**

160. Característiques:

- Es poden oblidar.
- A vegades els usuaris les escriuen obrint una oportunitat al coneixement per robatori.
- Si el nombre de possibilitats és reduït i el mecanisme de validació permet provar ràpidament, un atacant pot descobrir el secret a base de proves.
- Noti's que la revelació d'un secret pot produir-se sense el coneixement de la part afectada pel que el lladre disposa d'una àmplia finestra de temps per a actuar maximitzant les seves oportunitats.
- El principal avantatge és que són barates d'implantar i fàcils de reemplaçar en cas de pèrdua.

161. S'ha de conscienciar als usuaris dels riscos de l'ús de contrasenyes i instruir-los en com generar-les i custodiar-les.

162. L'expressió "amb cautela" emprada més amunt indica que hem d'establir una política rigorosa d'ús de contrasenyes com a mecanisme d'autenticació. Una política inclou els següents elements:

- La Política de contrasenyes ha de formalitzar-se en normativa [org.2] i procediments operatius de seguretat [org.3].
- Ha de diferenciar entre contrasenyes d'usuari i contrasenyes amb privilegis d'administrador.
- Ha de tenir en compte si s'empra aïlladament o en combinació amb un altre factor d'autenticació.
- Ha de fixar els processos de creació, distribució, custòdia i terminació.

- Ha d'establir les característiques (patrons) de les contrasenyes per a considerar-se vàlides. Per exemple, nombre de caràcters i conjunt admès i requerit de caràcters.
- Ha d'establir un període màxim de validesa i un temps mínim de no repetició (per exemple, cal renovar-la almenys cada 6 mesos i no es pot establir una contrasenya ja utilitzada en l'últim any o entre les N últimes contrasenyes, on N és el nombre de contrasenyes històriques que l'entitat conserva i aplica com a política).
- Han de detectar-se els intents repetits d'utilització i tractar-los com a possibles atacs de descobriment pel mètode de prova-error. I ha d'establir-se un procediment d'actuació que pot anar des de la introducció d'un retard creixent en el mecanisme de validació, fins a la suspensió cautelar del compte.
- Ha d'executar-se regularment una aplicació de descobriment de contrasenyes per força bruta (*password cracker*), suspenent-se d'ofici totes les contrasenyes trencades.
- Han de suspendre's les contrasenyes que hagin estat utilitzades amb èxit en un procés d'autenticació de doble factor, fins i tot si el segon factor ha bloquejat l'accés.
- Han d'establir-se plans de conscienciació i formació dels usuaris i administradors que empren contrasenyes.

163. S'ha d'implementar un procediment de resolució d'incidències relacionades amb contrasenyes; en particular ha d'haver-hi un procediment urgent de suspensió de compte després d'un robatori.

**Claus concertades**

164. Les claus concertades són una variant de les contrasenyes, que se suposen més còmodes d'establir per al ciutadà usuari.

165. S'entenen per claus concertades codis generats prèvia identificació i autenticació del ciutadà per altres mitjans. Jurídicament, el ciutadà expressa la seva voluntat d'utilitzar aquest mecanisme en el procés de sol·licitud. Les claus concertades hauran de garantir que l'usuari no pot ser suplantat, ni per un altre usuari, ni per la mateixa Administració. Per això deuran:

- ser raonablement robustes enfront d'atacs d'endevinació, tant per estar associades a dades àmpliament coneguts del ciutadà, com per falta d'aleatorietat suficient en la generació;
- ser raonablement robustes enfront d'atacs de diccionari;
- ser raonablement robustes enfront d'atacs de força bruta; és a dir, han de disposar de prou entropia;
- impedir que l'usuari pugui ser suplantat;
- seguir un procediment de generació que garanteixi l'autenticitat de l'usuari;
- seguir un procediment de comunicació a l'interessat que garanteixi que arriba a la persona correcta;

- disposar d'un procediment de comunicació de pèrdua o robatori que suspengui immediatament l'operativitat de la clau;
- i disposar de procediments de custòdia de les dades de signatura i verificació de la signatura durant el període de validesa de la informació signada, incloent-hi els instants de temps en què es genera, se suspèn i s'extingeix la validesa de la clau concertada.

166. A fi de garantir la robustesa, l'Administració de sistemes haurà de recórrer a generadors aleatoris que proporcionin prou entropia (que hi hagi tantes claus possibles que sigui impossible provar-les totes una per una).

167. És responsabilitat de l'usuari custodiar aquestes claus de manera segura.

168. El procés de generació ha de garantir la identitat del subjecte i deixar evidència documental de les proves d'identitat emprades.

169. El procediment de distribució ha de garantir que només se li facilita al titular legítim. Per exemple:

- Usant una xarxa privada virtual xifrada i autenticada (mp.com.2 i mp.com.3).
- Per doble canal; ex. Internet + telèfon mòbil.
- Per escrit en sobre tancat.

170. Han de generar-se de manera aleatòria per a:

- Resistir atacs aleatoris.
- Resistir atacs de diccionari.

**Claus o targetes (físiques)**

171. Característiques:

- Es poden perdre, accidental o deliberadament
- Es poden robar
- Es poden fer còpies

172. Ús habitual:

- Autenticació enfront de terminals (*logon*)
- Accés remot i establiment de canals segurs
- Activació de dispositius criptogràfics
- Ús de dues o més targetes d'activació
- Accés a instal·lacions

173. Sembla natural que es potenciï l'ús de la signatura electrònica com a mecanisme d'autenticació de la persona. Aquest dispositiu proporciona mitjans d'autenticació criptogràfics acreditats. Enfront del seu ús no autoritzat es protegeix amb un PIN d'activació. Noti's que la signatura electrònica només està capacitada per política per a identificar a la persona; la resta del sistema de control i registre d'accés ha d'implementar-se a part.

**Biometria**

174. Característiques:
    - Normalment, no són secretes, i la seva robustesa depèn del fet que no es pugui suplantar a l'usuari; això depèn molt del mecanisme concret, però alguns permeten tècniques de reproducció una miqueta avançades.
    - En general, els dispositius són costosos.
    - És difícil de reemplaçar en cas de pèrdua del control per part de l'usuari legítim.
175. Ús habitual:
    - En l'autenticació enfront de terminals:
        - reconeixement d'empremta digital;
        - reconeixement facial;
        - com a doble factor es pot utilitzar una contrasenya o un PIN.
    - En l'accés a locals o àrees:
        - reconeixement de la mà;
        - reconeixement de l'iris o del fons de l'ull;
        - com a doble factor es pot fer servir una targeta o un PIN.
    - R1: S'utilitzarà una contrasenya com a mecanisme d'autenticació i s'imposaran normes de complexitat mínima.
    - R2: Es requereix una contrasenya d'un sol ús (OTP) com a complement a la contrasenya d'usuari.
    - R3: Certificats:
        - S'usaran certificats qualificats de mecanismes d'autenticació.
        - L'ús del certificat estarà protegit per un segon factor de tipus PIN o biomètric.
        - Les credencials usades hauran de ser obtingudes després d'un registre presencial o bé telemàtic.
    - R4: Certificats en dispositiu físic:
        - S'usaran certificats qualificats de mecanisme d'autenticació, en suport físic (targeta o similar) usant algoritmes, paràmetres i dispositius autoritzats.
        - L'ús del certificat estarà protegit per un segon factor, del tipus PIN o biomètric.
        - Les credencials usades hauran de ser obtingudes després d'un registre presencial o bé telemàtic.
    - R5: els registres:
        - Es registraran els accessos exitosos i fallits.
        - S'informarà l'usuari de l'últim accés efectuat amb la seva identitat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.17 - Informació d'autentificació |
| NIST SP 800-53 rev. 4 | - IA-2] Identification and Authentication (Organizational Users)<br>- [IA-3] Device Identification and Authentication<br>- [IA-5] Authenticator Management<br>- [IA-7] Cryptographic Module Authentication<br>- [IA-8] Identification and Authentication (Non-Organizational Users) |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>o CSC.5 - Controlled Use of Administrative Privileges<br>o CSC.14 - Controlled Access Based on the Need to Know<br>- Password Policy, SANS Institute<br>- https://www.sans.org/ |

### 6.4.6 [OP.ACC.6] MECANISMES D'AUTENTICACIÓ (USUARIS DE L'ORGANITZACIÓ)

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits + [R1 o R2 o R3 o R4] + R8 + R9 | Requisits + [R1 o R2 o R3 o R4] + R5 + R8 + R9 |

176. La major part de les mesures requerides es poden aconseguir simplement configurant els llocs d'usuari segons s'indica.

- Com a manera preventiva, la informació que es visualitza abans d'accedir a un sistema haurà de procurar ser la menys possible, per evitar donar a conèixer quina informació pot trobar dins algú que pugui estar temptat de vulnerar el sistema. Per exemple, haurà d'evitar-se text de tipus advertiment per estar a punt d'entrar en un portal o aplicació que conté informació confidencial d'un determinat tipus, ja que habitualment aquests advertiments poden atreure a usuaris no autoritzats.
- Limitar el nombre d'intents d'accés per a bloquejar l'oportunitat d'accés una vegada efectuats un cert nombre de fallades consecutives, sigui mitjançant bloqueig del compte o retard de la sol·licitud de contrasenya.

- Desar un registre o *log* dels accessos realitzats a un sistema, tant els accessos correctes com aquells realitzats erròniament. Això últim és especialment important de cara a detectar continuats intents de vulnerar el sistema (mitjançant per exemple atacs de força bruta), ja sigui mitjançant revisions periòdiques dels registres (logs) o amb eines automatitzades que detectin aquest tipus d'esdeveniments.
- L'usuari haurà de tenir coneixement de les obligacions després d'accedir satisfactòriament a un sistema (per exemple, una finestra emergent). En cas que el sistema no permeti notificar immediatament després de l'accés, haurà de notificar-se-li per altres vies compensatòries (per exemple, un correu electrònic després de l'alta en el sistema).

177. El sistema ha d'informar i detectar si el seu compte d'usuari ha estat compromès i pugui activar el procediment de resolució d'incidents relacionats amb contrasenyes. Per exemple, després d'un període d'inactivitat en el compte (vacances, baixes, etc.), si a l'usuari se li notifica un accés recent sabrà immediatament que algú ha suplantat la seva identitat en el sistema.

178. En cas de no ser possible la implementació d'aquest avís de manera proactiva per part del sistema, s'hauran d'establir els mecanismes necessaris perquè l'usuari pugui consultar/sol·licitar el registre d'accessos.

179. S'haurà de controlar que l'accés als sistemes es restringeixi en determinats moments (per exemple, dies festius, fi de la jornada laboral, etc.) i llocs (adreces IP fora del domini de seguretat, teletreball, equips no autoritzats, etc.), per a evitar accessos no supervisats que puguin generar modificacions o fraus clandestins o no autoritzats.

180. No obstant això, és possible que existeixin sistemes que no requereixin limitar l'accés (per exemple, perquè precisament el propòsit del sistema sigui ser accessible en qualsevol moment i lloc), però haurà d'estar degudament documentada aquesta casuística.

181. El requisit que en uns certs punts es requereixi una identificació singular no és assolible per mitjà de configuració del lloc de l'usuari, sinó que requereix instrumentar *workflow* dels processos. Com a regla general, aquests punts han de ser pocs i el sistema no ha de memoritzar la identitat de l'usuari, sinó que ha de verificar-la cada vegada.

182. Aprovisionar serveis de monitoratge de suplantació d'identitat d'entitats en llocs web, registre de dominis, comptes en xarxes socials, correus electrònics... S'ha de monitoritzar especialment:

- Campanyes de phising, pharming o spam per detectar les campanyes en les quals els correus no passin per sistemes de gestió de correu de les entitats.
- Suplantació de dominis, tant mitjançant l'elecció de noms de domini similars o que puguin portar a confusió com en suplantació de dominis reals.
- Suplantació de llocs web de serveis "oficials" com cites prèvies, tramitació, etc.

- Llocs web oferint serveis no existents o serveis similars o iguals als existents en webs oficials.
- Ús de la imatge de "marca", logotip, nom, etc., d'alguna entitat en llocs web no autoritzats.
- Aplicacions mòbils fraudulentes que intentin suplantar la identitat d'alguna entitat, oferir serveis de les entitats, obtenir dades d'usuaris relacionats amb les entitats, distribuir malware utilitzant la imatge d'alguna entitat, etc.
- Malware relacionat amb entitats, tant en l'àmbit de logotip, imatge de marca, URL, noms de domini, etc., que faci servir qualsevol element de les entitats per obtenir la confiança del ciutadà o de l'usuari de les entitats

183. També s'ha de prestar assistència en els processos de resolució d'aquest tipus d'incidents:
    - Gestionar el tancament de dominis relacionats amb els casos de "phishing" o "pharming".
    - Gestionar el tancament de dominis i webs fraudulents.
    - Gestionar la retirada d'aplicacions mòbils fraudulentes.
184. Les accions necessàries hauran de poder realitzar-se tant davant autoritzades nacionals com de tercers països, per la qual cosa l'adjudicatari haurà de comptar amb capacitat per actuar-hi.
185. R1: Contrasenyes:
    - S'utilitzarà una contrasenya com a mecanisme d'autenticació quan l'accés es realitzi des de zones controlades i sense travessar zones no controlades.
    - S'imposaran normes de complexitat mínima enfront d'atacs d'endevinació
186. R2: Contrasenya + un altre factor d'autenticació: Es requereix un segon factor tal com "alguna cosa que es té", és a dir, un dispositiu, una contrasenya d'un sol com a complement a la contrasenya d'usuari, o "alguna cosa que s'és".
187. R3: Certificats:
    - S'utilitzaran certificats qualificats de mecanisme d'autenticació.
    - L'ús del certificat estarà protegit per un segon factor, tipus PIN o biomètric.
188. R4: Certificats en dispositiu físic:
    - S'utilitzaran certificats qualificats de mecanisme d'autenticació, en suport físic (targeta o similar) utilitzant algoritmes, paràmetres i dispositius autoritzats per ANC-AD.
    - L'ús del certificat estarà protegit per un segon factor, de tipus PIN o biomètric.
189. R5: Registre:

- Es registraran els accessos amb èxit i fallida.
- S'informarà l'usuari de l'últim accés efectuat amb la seva identitat

190. R8: Doble factor per accés des de o a través de zones no controlades: Es denomina "zona controlada" aquella que no és d'accés públic, requerint-se que l'usuari, abans de tenir accés a l'equip, s'hagi autenticat prèviament d'alguna forma (control d'accés a les instal·lacions), diferent del mecanisme d'autenticació lògica enfront del sistema. Un exemple de zona no controlada és Internet. Per a l'accés des de o a través de zones no controlades es requerirà un doble factor d'autenticació: R2, R3 o R4.

191. R9: Accés remot (tots els nivells):

- Serà aplicable la ITS d'Interconnexió de sistemes d'informació.
- L'accés remot haurà de considerar els següents aspectes:
  - Ser autoritzat per l'autoritat corresponent
  - El trànsit haurà de ser xifrat
  - Si l'ús no es produeix de manera constant, l'accés remot haurà de trobar-se inhabilitat i habilitar-se únicament quan sigui necessari.
  - Hauran de recollir-se registres d'auditoria d'aquesta mena de connexions.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.5 – Autenticació segura |
| NIST SP 800-53 rev. 4 | - [AC-7] Unsuccessful Login Attempts<br>- [AC-8] System Use Notification<br>- [AC-9] Previous Login Notification<br>- [IA-5] Authenticator Management<br>- [IA-6] Authenticator Feedback<br>- [SI-11] Error Handling |

## 6.5 [OP.EXP] EXPLOTACIÓ

192. En els controls d'explotació es contempla els components i dispositius dels quals es disposa i la seva seguretat. Els actius són tots els elements del sistema que han d'estar recollits en un inventari. També ho és la documentació que exposi les diferents polítiques o processos per garantir-ne un bon ús, una correcta configuració i protegeixi les seves vulnerabilitats. Quedarà registrada qualsevol actualització tant de noves incorporacions com de manteniment, incidents i canvis.

### 6.5.1 [OP.EXP.1] INVENTARI D'ACTIUS

| Categoria | Bàsica | Mitjana |
|---|---|---|

193. L'inventari d'actius ha de cobrir tot el domini de seguretat del responsable de la seguretat del sistema d'informació, fins a aconseguir els punts d'interconnexió i els serveis prestats per tercers. La granularitat ha de ser suficient per a cobrir les necessitats de report d'incidents i per a fer un seguiment, tan formal (auditories) com a reactiu en el procés de gestió d'incidents.

- Identificació de l'actiu: fabricant, model, número de sèrie
- Configuració de l'actiu: perfil, política, programari instal·lat
- Programari instal·lat: fabricant, producte, versió i pegats aplicats
- Equipament de xarxa: MAC, IP assignada (o rang)
- Ubicació de l'actiu: on està?
- Propietat de l'actiu: persona responsable del mateix

194. L'etiquetatge de l'equipament i del cablejat formarà part de l'inventari. Es disposarà d'eines que permetin visualitzar i fer un seguiment de l'estat de tots els equips en la xarxa, particularment els servidors i els dispositius de xarxa i comunicacions.

195. Es disposarà d'eines que permetin categoritzar els actius crítics per context de l'organització i riscs de seguretat.

196. Quan un actiu d'informació tracti dades personals, li és aplicable el que es disposa en la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD), així com la resta de l'eventual normativa d'aplicació nacional i internacional.

197. Es mantindrà actualitzada una relació formal dels components software dels treballadors. Aquesta llista inclourà llibreries i els serveis requerits pel seu ús.

198. Verificar sistemàticament la situació de seguretat real dels actius d'informació inventariats tenint en compte les seves amenaces reals, mitjançant l'anàlisi de registres d'activitat, indicadors d'alerta i resultats de monitoratge de seguretat.

199. En cas d'existir perills que no estiguin coberts per l'especificació de seguretat de l'actiu d'informació estàndard, el DSI ha de verificar la idoneïtat de les mesures de seguretat implementades en les condicions reals i, si cal, aplicar mesures de seguretat addicionals.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.9 – Inventari d'informació i altres actius associats<br>- A.5.32 – Drets de propietat intel·lectual |
| NIST SP 800-53 rev. 4 | - [CM-8] Information System Component Inventory<br>- [PM-5] Information System Inventory |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1 |

| | |
|---|---|
| | ○ CSC.1 - Inventory of Authorized and Unauthorized Devices<br>○ CSC.2 - Inventory of Authorized and Unauthorized Software |

### 6.5.2 [OP.EXP.2] CONFIGURACIÓ DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

200. Tots els sistemes han de ser configurats de manera sistemàtica abans d'entrar en producció. L'entitat ha d'elaborar uns pocs perfils de configuració per a les diferents activitats al fet que poden ser dedicats, sent típics els següents:

- Usuaris normals (ús administratiu)
- Atenció a clients
- Gestió de proveïdors (inclosos bancs)
- Desenvolupament
- Operadors i administradors (tècnics de sistemes)
- Responsable de seguretat (consola de configuració)
- Auditoria

201. La mesura s'instrumenta per mitjà d'una llista de verificació (*checklists*) que s'ha d'aplicar sistemàticament a cada equip abans d'entrar en producció.

202. En tots els perfils d'usuari, excepte en els d'administrador, s'ha de bloquejar l'opció que aquest pugui canviar la configuració del sistema o pugui instal·lar nous programes o nous perifèrics (*drivers*).

203. La configuració de seguretat ha d'incloure un perfil bàsic d'auditoria d'ús de l'equip.

204. Les màquines virtuals estaran configurades i gestionades d'una forma segura. La gestió de la resolució d'errors, comptes d'usuaris, software antivirus... Es realitzarà com si es tractés de màquines físiques, incloent la màquina amfitriona.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.9 – Gestió de la configuració<br>- A.8.19 – Instal·lació del software en sistemes de producció<br>- A.8.34 – Protecció dels sistemes d'informació durant proves d'auditoria |
| NIST SP 800-53 rev. 4 | - [CM-2] Baseline Configuration<br>- [CM-6] Configuration Settings<br>- [CM-7] Least Functionality |

| | |
|---|---|
| | - [SI-5] Security Alerts, Advisories, and Directives |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>  ○ CSC.3 - Secure Configurations for Hardware and Software<br>  ○ CSC.9 - Limitation and Control of Network Ports<br>  ○ CSC.18 - Application Software Security<br>- FDCC - Federal Desktop Core Configuration<br>- http://nvd.nist.gov/fdcc/index.cfm<br>- USGCB - The United States Government Configuration Baseline<br>- https://csrc.nist.gov/h<br>- Manageable Network Plan<br>- Milestone 7: Manage Your Network, Part II (Baseline Management) |

### 6.5.3 [OP.EXP.3] GESTIÓ DE LA CONFIGURACIÓ DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

205. Per sobre de la configuració de cada equip, cal tenir una visió integral del sistema, dels equips que treballen coordinadament, de l'estructura de línies de defensa en profunditat i de la dinàmica del sistema: la seva evolució temporal des del punt de vista d'arquitectura del sistema i des del punt de vista d'actualitzacions dels components.

206. Els canvis han de ser controlats i la configuració ha d'anar en la mateixa línia.

207. R1: manteniment regular de la configuració:

- Es mantindran i autoritzaran regularment les configuracions de hardware/software per als servidors, elements de xarxa i estacions de treball.
- Es verificarà periòdicament la configuració de hardware/software del sistema per a notificar que no hi ha hagut cap introducció d'elements no autoritzats.
- Llista de serveis autoritzats per a servidors i estacions de treball.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.36 – Compliment de les polítiques, i normes de seguretat de la informació |

| | |
|---|---|
| | - A.8.9 – Gestió de la configuració<br>- A.8.34 – Protecció dels sistemes d'informació durant proves d'auditoria |
| NIST SP 800-53 rev. 4 | - [CM-3] Configuration Change Control<br>- [CM-9] Configuration Management Plan |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>  ○ CSC.3 - Secure Configurations for Hardware and Software<br>- NIST 800-128 Guide for Security-Focused Configuration Management of Information Systems |

### 6.5.4 [OP.EXP.4] MANTENIMENT I ACTUALITZACIONS DE SEGURETAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

208. Proactivament, s'haurà d'estar informat dels defectes anunciats per part del fabricant o proveïdor (com per exemple mitjançant subscripcions a llistes de correu o RSS, consultant notícies en webs de tecnologia, seguretat o fabricants, etc.) o des del site de l'ANC-AD mitjançant la subscripció al servei de defectes. El manteniment s'haurà de realitzar únicament pel personal autoritzat.

209. R1: proves en preproducció. Abans de posar en producció una nova versió aquesta serà comprovada en un entorn de prova controlat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.36 – Compliment de les polítiques, i normes de seguretat de la informació<br>- A.7.13 – Manteniment dels equips<br>- A.8.8 – Gestió de les vulnerabilitats tècniques<br>- A.8.34 – Protecció dels sistemes d'informació durant proves d'auditoria |
| NIST SP 800-53 rev. 4 | - [CA-2] Security Assessments<br>- [CA-7] Continuous Monitoring<br>- [CA-8] Penetration Testing<br>- [MA-2] Controlled Maintenance<br>- [MA-3] Maintenance Tools<br>- [MA-4] Nonlocal Maintenance<br>- [MA-5] Maintenance Personnel |

| | |
|---|---|
| | - [MA-6] Timely Maintenance<br>- [RA-5] Vulnerability Scanning<br>- [SI-2] Flaw Remediation<br>- [SI-4] Information System Monitoring<br>- [SI-5] Security Alerts, Advisories, and Directives |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>  ○ CSC.4 - Continuous Vulnerability Assessment and Remediation<br>  ○ CSC.20 - Penetration Tests and Red Team Exercises<br>- NIST SP 800-40 - Creating a Patch and Vulnerability Management Program<br>- Manageable Network Plan<br>  ○ Milestone 6: Manage Your Network, Part I (Patch Management) |

### 6.5.5 [OP.EXP.5] GESTIÓ DE CANVIS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

210. Es mantindrà un control continu dels canvis realitzats en el sistema, de forma que:

- Els canvis es planificaran per reduir l'impacte sobre la prestació dels serveis afectat. Totes les peticions de canvi es registraran assignant un número de referència que permeti el seu seguiment de forma equivalent al registre dels incidents.
- La informació a registrar per a cada petició de canvi serà suficient per a qui hagi d'autoritzar-los no tingui cap dubte i permeti gestionar-ho fins a la seva desestimació o implementació.
- Les proves de preproducció, sempre que sigui possible realitzar-les, s'efectuaran en equips equivalents als de producció, almenys en els aspectes específics del canvi.
- Mitjançant una anàlisi de riscs es determinarà si els canvis són rellevants per a la seguretat del sistema. Aquells canvis que impliquin un risc de nivell alt hauran de ser aprovats explícitament de forma prèvia a la seva implementació, pel responsable de Seguretat.
- Un cop implementat el canvi es faran les proves d'acceptació convenients. Si són positives s'actualitzarà la documentació de configuració.
- Mantenir la configuració i la gestió de canvis. Qualsevol canvi en els actius d'informació bàsics, actius d'informació estàndard, classes de seguretat,

mesures de referència o mesures addicionals s'ha de registrar, mitjançant mecanismes de registre (logs) que permetin auditar la traçabilitat dels canvis. Aquests registres han d'incloure com a mínim l'identificador de l'usuari, el moment del canvi, l'actiu afectat i la naturalesa del canvi, i han d'estar a disposició de l'autoritat competent que supervisa l'entitat.

- Impulsar la millora contínua del sistema de gestió mitjançant la revisió periòdica de les dades obtingudes dels registres, informes d'auditoria, incidents i canvis, amb l'objectiu de detectar oportunitats de millora i planificar accions correctives o preventives.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.32- Gestió de canvis |
| NIST SP 800-53 rev. 4 | - [CA-5] Plan of Action and Milestones<br>- [CM-4] Security Impact Analysis<br>- [CM-5] Access Restrictions for Change<br>- [MA-2] Controlled Maintenance<br>- [SI-2] Flaw Remediation<br>- [SI-7] Software, Firmware, and Information Integrity |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>○ CSC.4 - Continuous Vulnerability Assessment and Remediation |

### 6.5.6 [OP.EXP.6] PROTECCIÓ ENFRONT DE CODI NOCIU

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 + R2 |

211. Han de monitorar-se els punts d'entrada i de sortida de codi nociu, primer per a no veure'ns afectats i segon per a no expandir la infecció.

212. Ha de conscienciar-se al personal per a detectar comportament sospitós i establir canals per a reportar-lo.

213. Han d'establir-se procediments per a reaccionar a deteccions o simples sospites, aïllar el problema recopilant prou evidències per a l'anàlisi forense i que es reporti a les autoritats pertinents. És a dir, connectar amb el procés de gestió d'incidències.

214. S'ha d'instal·lar software de protecció enfront codi maliciós en tots els equips. Les bases de dades de detecció del codi han d'estar permanentment actualitzades. Les entitats han de comptar amb tots els elements de maquinari i programari per a la creació d'un laboratori d'anàlisi de malware.

215. S'ha d'incloure la capacitat de sandboxing per a l'anàlisi automàtica d'executables, documents ofimàtics, etc que permeti l'anàlisi automàtica dels correus electrònics, navegació per internet entre d'altres.

216. El sistema ha d'incloure totes les eines necessàries perquè un equip de recerca de malware pugui realitzar anàlisis manuals en profunditat de mostres de malware.

217. R1: Escaneig periòdic: tot el sistema serà escanejat per detectar codi maliciós.

218. R2: Revisió preventiva del sistema: les funcions crítiques s'analitzaran en arrancar el sistema per a prevenir modificacions no autoritzades.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.7 – Controls contra el codi nociu |
| NIST SP 800-53 rev. 4 | - [SC-18] Mobile Code<br>- [SI-3] Malicious Code Protection |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>o CSC.8 - Malware Defenses<br>- NIST SP 800-28 - Guidelines on Active Content and Mobile Code<br>- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling |

### 6.5.7 [OP.EXP.7] GESTIÓ D'INCIDENTS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 + R2 |

219. Cal establir un procés de gestió que instrumenti les següents activitats:

- Reporti esdeveniments de seguretat i febleses detectats pels usuaris, detallant els criteris de classificació i l'escalat de la notificació.
- Reporti incidents reportats per proveïdors externs (terceres parts).
- S'informi els usuaris potencialment afectats.
- S'informi els proveïdors potencialment afectats.
- Es prenen mesures urgents per a contenir el problema, evitar que creixi dins de l'entitat i impedir que es transmeti a altres entitats.
- Es reparen danys.

220. També cal executar una sèrie d'activitats de caràcter administratiu:

- Recopilació
- Recopilació d'evidències per a analitzar, aprendre i reportar als òrgans de gestió
- Es documenta l'incident, la seva anàlisi i els passos seguits per a la seva resolució

- S'actualitzen els procediments operatius de seguretat afectats per a evitar que es repeteixi l'incident incloent informació a l'usuari per a la correcta identificació i manera de tractar l'incident
- S'actualitzen els plans de continuïtat afectats
- S'inclou la notificació a l'ANC-AD quan l'incident sigui d'impacte significatiu en la seguretat de la informació manejada i dels serveis prestats (l'ENS-AD)

221. Procediment que estableix identificar si l'incident afecta fitxers amb dades de caràcter personal i, en cas que així sigui, està alineat o integrat amb el procés de gestió d'incidents de dades personals.

222. Es recopilaran dades sobre el temps de tancament dels incidents que permetin poder valorar posteriorment el sistema de gestió d'incidents.

223. En l'anàlisi de l'incident convé identificar la causa arrel o causa última per la qual ha estat origen de l'incident. Aquesta caracterització s'incorporarà a les mètriques d'eficàcia, identificant-se febleses recurrents i elaborant un pla per al seu remei.

224. Es requereix que les entitats s'aprovisionin d'un sistema EDR que ha de posseir diferent fonts d'actualització, de vulnerabilitats, regles de comportament, etc., perquè el sistema estigui actualitzat i pugui detectar la majoria d'anomalies.

225. L'EDR ha de poder interaccionar amb la plataforma de detecció i resposta a incidents per poder-ne gestionar la contesta. I les capacitats de monitoratge i registre han de ser de mínim un any.

226. L'EDR s'ha de configurar per enviar la seva activitat a les plataformes de detecció de les entitats i a les eines de l'ANC-AD.

227. Ha de complir les següents característiques:

- La solució proposada ha d'aparèixer com a líder en l'últim quadrant màgic de Gartner
- Ha d'aparèixer en última versió de Mitre ATT&CK Enterprise evaluations, de productes avaluats.
- Consola totalment APIficada. Qualsevol acció que es pot realitzar a través de la interfície gràfica també s'ha de poder fer via API amb la finalitat d'automatitzar processos.
- Execució de scripts des de la consola a qualsevol plataforma, Windows en PowerShell, Linux i Mac a Shell, registrant la seva execució (auditoria) al SIEM
- Capacitat per remeiar artefactes digitals (rastres o elements generats per les amenaces, com malware, ransomware o atacs dirigits en un sistema), en plataformes Windows i MacOS.
- Capacitat per descobrir equips desprotegits en el seu mateix segment de xarxa.

228. Les entitats hauran d'aprovisionar-se dels sistemes d'informació que prestin els serveis dels actuals Sistemes d'Alerta Primerenca d'ANC-AD, que hauran de quedar integrats en la infraestructura de les entitats.

229. S'hauran de seguir les recomanacions d'ANC-AD per al traspàs d'aquests sistemes a la seva infraestructura.

230. S'ha d'instal·lar almenys els següents sistemes d'alerta primerenca.
   - Sistema d'alerta primerenca per als sistemes exposats a internet.
   - Sistema d'alerta primerenca per als sistemes exposats en xarxa compartida amb entitats i ANC-AD
   - Sistema d'alerta primerenca per als sistemes de control industrial (si tinguessin).

231. És important comptar amb un Centre d'Operacions de Seguretat (SOC) que pugui fer front als desafiaments creixents.

232. Les entitats han d'implementar un SOC que inclogui plataformes d'intel·ligència artificial per poder funcionar amb el menor nombre de persones possibles. Aquesta eina també pot ajudar a automatitzar els nivells 1 i 2 d'atenció a incidents.

233. Els sistemes de detecció han d'evolucionar en sondes per poder actuar de forma automàtica davant d'atacs i poder donar una resposta adient. En el cas d'incidents comuns la IA ha de poder donar resposta de forma automàtica i discernir si és necessària la presència d'un analista.

234. El sistema IA ha de proporcionar informació sobre les noves tendències d'atacs agafant la informació del sistema de sondes i de l'EDR. També s'ha de poder identificar incidents nous i notificar-ho.

235. El sistema IA també haurà de tractar els temes de fuita de dades i donar suport en les tasques d'anàlisis de malware.

236. Els elements de la plataforma de detecció d'incidents s'implantarà en dependències d'Andorra, de l'Agència o punts intermedis de comunicacions, depenent de la necessitat.

237. La plataforma ha de ser en modalitat Cloud i amb la possibilitat de créixer d'acord amb els actius i fonts de les entitats.

238. Es requereix que el sistema treballi amb unes estadístiques de menys d'un 2% de falsos positius a l'hora de detectar incidents mitjançant casos d'ús.

239. La plataforma haurà de contenir un Portal accessible per als responsables de les entitats on la informació s'adapti respecte a l'evolució tant de les amenaces com dels actius de l'organització. En aquest portal s'ha de mostrar quin percentatge de la Matriu MITRE ATT&CK s'està cobrint amb els actuals casos d'ús que el proveïdor té implantats a les entitats.

240. R1: notificació. Es disposarà de solucions per a la notificació d'incidents a l'ANC-AD, que permeti la distribució de notificacions a les diferents entitats de manera federada.

241. R2: detecció i resposta. Aquest reforç integra un procés per fer front als incidents que puguin tenir un impacte en la seguretat del sistema. Inclou les següents mesures:

- Implantació de mesures urgents, inclòs la detecció de serveis, l'aïllament del sistema afectat, la recollida d'evidències i protecció dels registres, segons convingui al cas.
- Assignació de recursos per investigar les causes, analitzar les conseqüències i resoldre l'incident.
- Informar de l'incident als responsables de la informació i serveis afectats i de les actuacions per a resoldre'ls.
- Mesures per a:
  - Prevenir que es repeteixi l'incident
  - Incloure en els procediments d'usuari la identificació i forma de tractar l'incident
  - Actualitzar, estendre i millorar els procediments de resolució d'incidents.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.5 – Contacte amb les autoritats<br>- A.5.24 – Planificació i preparació de la gestió d'incidents de seguretat de la informació<br>- A.5.25 – Avaluació i decisió sobre els esdeveniments de seguretat de la informació<br>- A.5.27 – Aprendre dels incidents de seguretat de la informació<br>- A.5.28 – Recopilació d'evidències<br>- A.6.8 – Notificació dels esdeveniments de seguretat de la informació |
| NIST SP 800-53 rev. 4 | - [IR] Incident Response<br>- [PM-15] Contacts with Security Groups and Associations<br>- [SI-5] Security Alerts, Advisories, and Directives |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>  - CSC.19 - Incident Response and Management<br>- NIST SP 800-61 – Computer Security Incident Handling Guide<br>- ISO/IEC TR 18044:2004 - Information technology – Security techniques – Information security incident management |

### 6.5.8 [OP.EXP.8] REGISTRE DE L'ACTIVITAT DELS USUARIS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 + R2 + R3 + R4 |

204. Es realitza una inspecció regular dels registres per a identificar anomalies en l'ús dels sistemes (ús irregular o no previst).

205. S'utilitzen eines automàtiques per a recollir i analitzar els registres a la recerca d'activitats fora del normal (per exemple: consola de seguretat centralitzada, SIEM).

206. R1: Revisió de registres: Es revisen informalment, de forma periòdica, els registres d'activitat.

207. R2: Sincronització del rellotge del sistema: El sistema disposa d'una referència de temps per facilitar les funcions de registre d'esdeveniments.

208. R3: Retenció de registres: En la documentació de seguretat s'inclouen els esdeveniments de seguretat que seran auditats i el temps de retenció dels registres abans de ser eliminats.

209. R4: Control d'accés: Als registres d'activitat només hi pot accedir el personal autoritzat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.33 – Protecció dels registres<br>- A.8.15 – Registre d'esdeveniments<br>- A.8.17 – Sincronització del rellotge |
| NIST SP 800-53 rev. 4 | - [AU] Audit and Accountability |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>○ CSC.16 - Account Monitoring and Control |

### 6.5.9 [OP.EXP.9] REGISTRE DE LA GESTIÓ D'INCIDENTS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

210. Es registraran totes les actuacions relacionades amb la gestió d'incidents: el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident. Especialment, quan l'incident pugui comportar accions disciplinàries sobre el personal intern o proveïdors externs.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.26 – Resposta a incidents de seguretat de la informació |

| | |
|---|---|
| | - A.5.27 – Aprendre dels incidents de seguretat de la informació<br>- A.5.28 – Recopilació d'evidències |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>  ○ CSC.19 - Incident Response and Management |

### 6.5.10 [OP.EXP.10] PROTECCIÓ DE LES CLAUS CRIPTOGRÀFIQUES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

211. Les claus han de generar-se en un equip i després traslladar-se a l'equip en el qual s'usaran. Els elements de generació que no són necessaris per a l'ús, es quedaran en l'equip de generació. És molt recomanable emprar un suport d'informació (per exemple, un disc USB o una targeta de memòria) per a traslladar les claus.

212. Quan una clau es retira d'explotació, la política marcarà durant quant temps s'ha de retenir, bé per raons operatives, bé com a prova d'auditoria. El motiu operacional més habitual es dona en claus de desxifrat quan es requereix poder desxifrar informació xifrada amb claus antigues.

213. És molt recomanable que les claus que es retenen estiguin en equips separats (mitjans aïllats d'explotació). Per al seu ús es traslladarà la informació a l'equip on estiguin.

214. En resum, s'han de protegir les claus criptogràfiques durant tot el seu cicle de vida:

- Generació
  - S'ha de garantir que les claus generades són imprevisibles
  - amb programes avaluats o dispositius criptogràfics certificats conforme a [op.pl.5]
  - els mitjans de generació han d'estar aïllats dels mitjans d'explotació
- Transport o distribució al punt d'utilització
  - S'ha d'assegurar la confidencialitat de la clau i l'autenticitat del receptor
  - Lliurament en mà
  - Ús de contenidors físics segurs
  - Ús de contenidors criptogràfics
  - Doble canal: clau i dades d'activació per separat
- Custòdia en explotació
  - S'ha de garantir la confidencialitat de la clau en els dispositius o aplicacions que l'empren

- S'ha de procurar el seu canvi quan el volum de dades xifrades o el temps que porta en ús superin els paràmetres recomanats abans que un atacant pugui descobrir-la per anàlisi de les dades xifrades
- En targeta intel·ligent protegida per contrasenya

- En dispositiu criptogràfic certificat amb control d'accés arxiu: còpies de seguretat de claus actives i retenció de claus retirades d'explotació activa
  - En contenidors físics segurs (per exemple, caixa forta)
  - En contenidors criptogràfics
  - En mitjans alternatius aïllats dels mitjans d'explotació
- Destrucció
  - Eliminació d'original i còpies
  - S'ha de garantir la seva destrucció, encara que per política pot requerir-se la seva retenció durant un període a l'efecte d'auditoria
  - En el cas de retenció, ha de garantir-se la confidencialitat de la clau controlant el seu accés

215. Totes les dades generades pel SOC, així com qualsevol clau criptogràfica relacionada amb la gestió de la seguretat o la protecció d'infraestructures crítiques, han de romandre dins el territori del Principat d'Andorra. Només es permet el seu allotjament fora del territori nacional en cas d'autorització expressa per part de l'ANC-AD, sempre que es garanteixi un nivell de protecció equivalent al de l'Esquema nacional de seguretat del Principat d'Andorra.

216. Aquestes garanties permeten establir un marc mínim d'homogeneïtat, confiança i interoperabilitat per a l'actuació del SOC dins del territori nacional i, si escau, en coordinació internacional.

217. R1: algoritmes autoritzats: Es fa ús d'algoritmes i paràmetres autoritzats per l'ANC-AD.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.24 – Ús de la criptografia |
| NIST SP 800-53 rev4 | - [SC-12] Cryptographic Key Establishment and Management<br>- [SC-17] Public Key Infrastructure Certificates |
| Altres referències | - NIST SP 800-57 Recommendation for Key Management |

## 6.6 [OP.EXT] RECURSOS EXTERNS

204. Mesures per a protegir el sistema de possibles perjudicis derivats de la contractació de determinats serveis a proveïdors externs.

205. L'Entitat pot delegar funcions, però mai la responsabilitat sobre la informació i els serveis.

206. Un problema que ha de quedar resolt és el d'alineament dels processos de l'entitat contractant i els processos del proveïdor extern, establint punts de contacte i protocols de comunicació. Això inclou tant els processos organitzatius com els processos operacionals.

207. Els actius dels següents controls és principalment la informació que s'intercanvia i tota la documentació que descriu les característiques referents als diversos processos.

### 6.6.1 [OP.EXT.1] CONTRACTACIÓ I ACORDS DE NIVELL DE SERVEI

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

208. Ha de realitzar-se una anàlisi de riscos que identifiqui els riscos associats al proveïdor extern.

209. Ha d'establir-se un contracte formal, acord de nivell de servei, aprovat per totes dues parts i actualitzat periòdicament establint:

- detall per part del proveïdor de les característiques del servei a prestar, de manera que quedi constància que inclou els requisits de servei i seguretat requerits
- rols i funcions en totes dues parts, en matèria de seguretat, incloent-hi els mecanismes de contacte (telèfon, e-mail, etc.)
- obligacions de cada part
- responsabilitats de cada part
- detalli de l'acord de nivell de servei (ANS/SLA) i conseqüències del seu incompliment
- protocol d'avís previ d'actuacions que puguin impactar a l'altra part
- mecanismes i procediments per a la sincronització de les activitats de gestió d'incidències
- un conjunt d'indicadors per a avaluar el servei prestat

210. També cal tenir preparat un procediment de desconnexió o finalització de la provisió del servei. En aquest escenari és especialment important la recuperació de la informació dins del RPO establert i la destrucció de la informació en els equips del proveïdor sortint (segons [mp.si.5]).

211. Les entitats essencials i importants tenen el deure d'escollir proveïdors (entitats subcontractades) que ofereixin garanties suficients sobre els serveis subcontractats, així com sobre la provisió de qualsevol tecnologia o producte, amb la finalitat d'aplicar les mesures de seguretat tècniques i organitzatives que siguin adequades quant a seguretat que requereixen els serveis, la tecnologia o els productes als quals s'aplica l'ENS-AD. Entre aquestes garanties, hi pot haver l'obligació que es tracti dels serveis, la tecnologia o els productes recollits al registre de components certificats elaborat a aquest efecte per l'ANC-AD en cada moment. El referit registre de components certificats l'elabora l'ANC-AD en funció dels criteris que consideri escaients, incloent-

hi els criteris internacionalment reconeguts o aplicats per entitats homòlogues de l'ANC-AD.

212. En cas que una entitat essencial o important acrediti que no pot disposar de serveis o tecnologia o productes recollits al registre de components certificats referit en el paràgraf anterior, aquesta entitat pot sol·licitar a l'ANC-AD una autorització per contractar els serveis o la tecnologia o els productes que corresponguin. Aquesta sol·licitud ha d'estar degudament argumentada i ha de justificar els motius de la necessitat de disposar del servei o tecnologia o els productes que es proposen, i l'ANC-AD disposa de dos mesos per avaluar-la. En cas de manca de resolució per part de l'ANC-AD dins del termini esmentat, l'autorització s'entén denegada per silenci administratiu negatiu.

213. En els supòsits de processos de contractació de serveis o d'adquisició de tecnologia o productes per part de les entitats essencials i importants a les quals aplica l'ENS-AD, les dites entitats resten obligades a requerir als proveïdors la presentació d'una auditoria de seguretat externa elaborada amb una data inferior a dotze mesos respecte a la data de la presentació de les seves ofertes, la qual s'ha d'efectuar de conformitat amb els marcs reconeguts internacionalment en matèria de ciberseguretat en cada moment.

214. En cas que una entitat essencial o important acrediti que no pot disposar d'un proveïdor de serveis o tecnologia o productes que tingui l'auditoria referenciada en el paràgraf anterior, o que el proveïdor ja comptava amb un o diversos certificats reconeguts, pot sol·licitar a l'ANC-AD una autorització per contractar el proveïdor que correspongui. Aquesta sol·licitud ha d'estar degudament argumentada i ha de justificar els motius de la contractació que es proposa, i l'ANC-AD disposa de dos mesos per avaluar-la. En cas de manca de resolució per part de l'ANC-AD dins del termini referit, l'autorització s'entén denegada per silenci administratiu negatiu.

215. L'accés remot per part de proveïdors o terceres parts als sistemes, serveis o dades de les entitats essencials i importants haurà d'efectuar-se a través de connexions segures que compleixin, com a mínim, els següents requisits:

- Autenticació multifactor (MFA) basada en certificats digitals, claus criptogràfiques o codis temporals (OTP) generats per sistemes acreditats o de confiança de l'entitat.
- Registre de totes les sessions remotes en sistemes de logs integrats amb solucions SIEM o equivalents, en compliment de la política definida per l'ENS-AD i el RIC-AD.
- Inclusió dels elements mínims de traçabilitat: identitat de l'usuari autenticat, mètode d'autenticació, adreça IP d'origen i ubicació, sistema operatiu, data, hora i durada de la sessió, recursos accedits, activitat acomplerta i registres d'anomalies o accessos denegats.
- Per a rols privilegiats o accés a entorns crítics, serà obligatori l'ús de bastions d'accés o jump servers amb enregistrament en vídeo i monitoratge.

- Es recomana la implantació de solucions de tipus Zero Trust Network Access (ZTNA) i arquitectures SASE per garantir la validació contínua de la identitat, control d'accés basat en el principi de mínim privilegi i supervisió del dispositiu.
- S'aplicarà verificació contínua durant la sessió activa, amb revalidacions de la identitat i monitoratge del dispositiu. La sessió s'interromprà immediatament en cas de canvis no autoritzats, desconnexió del canal segur o activitat sospitosa.
- Qualsevol sistema de connexió remota nou, alternatiu o tecnologia equivalent haurà de ser autoritzat prèviament per escrit per l'ANC-AD o, si escau, per l'AFA, abans del seu desplegament en entorns productius o de proves. Aquesta obligació inclou tecnologies que substitueixin VPN tradicionals o plataformes de control remot de tercers.
- Els accessos hauran d'estar limitats per rol i funció i només actius durant el període de la intervenció contractada, estant prohibit l'accés generalitzat o indefinit a recursos.

216. El proveïdor seleccionat per l'entitat no pot recórrer a una subcontractació (independentment que subcontracti una entitat o una persona física) sense l'autorització prèvia, per escrit, específica o general, de l'entitat a la qual presta el servei al qual s'aplica l'ENS-AD. El proveïdor ha d'informar a l'entitat a la qual presta el servei i al qual se li aplica l'ENS-AD, de qualsevol canvi previst en la incorporació o la substitució d'altres subcontractes en els quals delegui part o la totalitat de la prestació del servei contractat. D'aquesta manera, es dona a les entitats que presten serveis als quals s'aplica l'ENS-AD l'oportunitat d'oposar-se a aquests canvis i, si escau, de canviar de proveïdor. No obstant això, les entitats essencials i importants resten obligades a requerir a les entitats subcontractades posteriorment la presentació d'una auditoria de seguretat externa elaborada amb una data inferior a dotze mesos respecte a la data en la qual s'iniciï la subcontractació posterior. En aquests casos, també existeix la possibilitat que l'entitat essencial o important sol·liciti a l'ANC-AD l'excepció regulada a l'apartat anterior, en els supòsits en els quals s'acrediti la manca de disposició d'un proveïdor que pugui tenir aquesta auditoria.

217. El servei que l'entitat subcontractada presta per suportar el servei al qual s'aplica l'ENS-AD s'ha de regir per un contracte per escrit, inclòs el format electrònic, que vincula l'entitat subcontractada a l'entitat que presta el servei al qual s'aplica l'ENS-AD i que estableix, com a mínim:

- El nivell de seguretat i l'acord del nivell del servei que l'entitat subcontractada ha de garantir per al servei subcontractat.
- Les penalitzacions associades als incompliments en relació amb el punt anterior.
- Les restriccions que per raó de jurisdicció pot haver-hi en la ubicació física dels actius d'informació que l'entitat subcontractada necessita per prestar el seu servei, en especial quan aquests actius d'informació són crítics, quan es tracten dades personals o qualsevol altre tipus d'informació igualment sensible, o quan algun dels actius d'informació de l'entitat subcontractada hagi d'ubicar-se fora d'Andorra i de l'Espai Econòmic Europeu.
- Que es garanteix que les persones autoritzades per tractar la informació o administrar, mantenir o operar el servei s'han compromès a respectar la

confidencialitat de la informació o estan subjectes a una obligació de confidencialitat de naturalesa estatutària, i han rebut la formació adequada en matèria de seguretat de la informació.

- Que es prendran totes les mesures necessàries en matèria de seguretat de la informació.
- Que es respecten les condicions establertes en l'apartat 2, en recórrer a unes altres subcontractacions, i que s'obliguen a complir, mitjançant un contracte escrit, les mateixes obligacions de seguretat de la informació que s'hagin estipulat en aquest contracte, especialment la prestació de garanties suficients d'aplicació de mesures tècniques i organitzatives adequades de manera que el servei al qual s'aplica l'ENS-AD sigui conforme amb les disposicions d'aquesta Llei. Addicionalment, s'ha d'especificar que en cap cas aquesta subcontractació no fa que l'entitat subcontractada perdi les seves responsabilitats davant de l'entitat que presta el servei al qual s'aplica l'ENS-AD.
- Que s'assisteix l'entitat que presta el servei al qual s'aplica l'ENS-AD en les obligacions que estableixen els articles 12 a 15 de la Llei NIS-AD.
- Les condicions per al rescat del servei que presta l'entitat subcontractada.
- Que es posa a disposició de l'entitat que presta el servei al qual s'aplica l'ENS-AD tota la informació necessària per demostrar que compleix les obligacions que estableix aquest article. Així mateix, ha de permetre l'elaboració d'auditories, incloses inspeccions, i contribuir-hi, per part de l'entitat que presta el servei al qual s'aplica l'ENS-AD, per l'autoritat competent que supervisa aquesta última o per un altre auditor autoritzat per fer aquestes auditories.
- L'obligació de l'entitat subcontractada d'informar immediatament l'entitat que presta el servei al qual s'aplica l'ENS-AD si considera que no compleix el nivell de seguretat exigit, encara que sigui temporalment.

218. En l'àmbit del sector públic, poden atribuir-se les competències pròpies d'una entitat subcontractada a un determinat òrgan de l'Administració pública de què es tracti o als seus organismes vinculats o dependents mitjançant l'adopció d'una norma reguladora de les competències referides, que ha d'incorporar el contingut previst a l'apartat anterior.

219. Les entitats essencials i importants han de facilitar a l'ANC-AD, amb una periodicitat anual, un resum de les contractacions i subcontractacions efectuades de conformitat amb el que estableixen els apartats anteriors d'aquest article, fent referència al Registre de components certificats contractats en cada cas. Així mateix, han d'incloure un registre actualitzat dels proveïdors externs amb accés remot, la tecnologia segura de connexió emprada, i les auditories o controls aplicats.

220. L'inventari dels serveis subcontractats que puguin impactar de qualsevol manera en les infraestructures crítiques. Per a cadascun d'aquests serveis, juntament amb la descripció del possible impacte i la descripció del servei subcontractat, s'ha d'identificar l'entitat subcontractada, els certificats que té en matèria de seguretat i la seu des de la qual presta el servei subcontractat, així com els nivells de servei acordats. D'igual forma, s'ha de descriure la metodologia mitjançant la qual es duu a

terme la comprovació del compliment per part de l'entitat crítica o equivalent a entitat crítica dels protocols de seguretat implementats en el seu cas.

221. S'ha d'incloure també la política d'accés segur per part dels proveïdors externs, que ha de contemplar, com a mínim, l'ús de canals xifrats, autenticació multifactor, assignació de rols amb privilegis mínims, horaris i durades limitades per a les connexions remotes, així com mecanismes de control i revocació d'aquests accessos.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.14 – Transferència d'informació<br>- A.5.19 – Seguretat de la informació en la relació amb proveïdors<br>- A.5.20 – Abordar la seguretat de la informació dins dels acords de proveïdors<br>- A.6.6 – Acords de confidencialitat o no revelació<br>- A.8.30 – Externalització del desenvolupament |
| NIST SP 800-53 rev4 | - [SA-9] External Information System Services |
| Altres referències | - NIST SP 800-35 – Guide to Information Technology Security Services |

### 6.6.2 [OP.EXT.2] GESTIÓ DIÀRIA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

222. A partir d'una sèrie d'indicadors, s'estableix un pla de report i seguiment amb punts d'alarma quan se superin uns certs llindars. Aquestes alarmes dispararan procediments de resolució i d'escalat, tractant-se com una incidència que ha de resoldre's.

223. S'estableix un sistema rutinari per a mesurar el compliment de les obligacions del servei, incloent-hi el procediment per a neutralitzar qualsevol desviació fora de l'acord previ.

224. El procés de resolució de la incidència aixecada per una alarma es regirà segons [op.exp.7] i [op.exp.9].

| Marc de referència | Controls d'aplicabilitat |
|---|---|

| | |
|---|---|
| ISO/IEC 27002:2022 | - A.5.22 – Seguiment, revisió i gestió dels canvis dels serveis del proveïdor |
| NIST SP 800-53 rev4 | - [SA-9] External Information System Services |
| Altres referències | - NIST SP 800-35 – Guide to Information Technology Security Services |

### 6.6.3 [OP.EXT.3] INTERCONNEXIÓ DE SISTEMES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

225. Es denomina interconnexió a l'establiment d'enllaços amb altres sistemes d'informació per a l'intercanvi d'informació i serveis.

226. Tots els intercanvis d'informació i prestació de serveis amb altres sistemes hauran de ser objecte d'una autorització prèvia. Tot flux d'informació estarà prohibit excepte autorització expressa.

227. Per a cada interconnexió es documentarà explícitament: les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada.

228. La connexió segura per part de proveïdors o terceres parts, amb la finalitat de protegir la cadena de subministrament, haurà de requerir doble autenticació (MFA) basada en certificats digitals, claus criptogràfiques o tokens temporals (OTP), generats per sistemes acreditats, o de confiança de l'entitat. L'activitat associada a cada sessió s'haurà de registrar en sistemes de logs que compleixin la política definida per l'ENS-AD ([OP.MON.4] Registre d'esdeveniments) i el RIC-AD, amb integració amb solucions de Security Information and Event Management (SIEM) o equivalents que permetin una gestió centralitzada, correlació d'esdeveniments i generació d'alertes.

229. Els elements mínims de traçabilitat exigits són:

- Identitat de l'usuari autenticat.
- Mètode d'autenticació emprat.
- Adreça IP d'origen, ubicació geogràfica i sistema operatiu utilitzat.
- Data, hora i durada de la connexió.
- Recursos o serveis accedits.
- Activitat acomplerta durant la sessió.
- Registre de qualsevol anomalia o accés denegat.

230. Per reforçar la seguretat i garantir el control continuat d'accés remot, es recomana l'adopció dels següents sistemes i tecnologies:

- Solucions de Zero Trust Network Access (ZTNA):
  Permeten validar contínuament la identitat de l'usuari i la postura de seguretat del dispositiu abans de concedir accés específic a recursos. L'accés es concedeix sota el principi del mínim privilegi i només mentre es mantinguin les condicions definides.
- Bastions d'accés o Jump Servers monitorats:
  Per a usuaris amb rols privilegiats o tècnics amb accés a entorns crítics, es requereix l'ús de bastions que registri en vídeo la sessió remota i permetin la supervisió posterior per part dels responsables de seguretat.
- Integració amb arquitectures SASE (Secure Access Service Edge):
  És recomanable que les connexions remotes utilitzin plataformes que combinin seguretat de xarxa, control d'accés i optimització del trànsit per a garantir rendiment, traçabilitat i seguretat en entorns híbrids o en el núvol.
- Supervisió i verificació contínua de la sessió activa:
  Els sistemes hauran d'aplicar revalidacions periòdiques de la identitat i de la configuració del dispositiu durant la sessió. La connexió haurà de ser interrompuda immediatament si es detecta un canvi d'estat no autoritzat, desconnexió del canal segur, o qualsevol activitat sospitosa.

## 6.7 [OP.NUB] SERVEIS EN EL NÚVOL

231. El següent control té com a actius tots els serveis en el núvol i la informació que hi està relacionada.

### 6.7.1 [OP.NUB.1] PROTECCIÓ DE SERVEIS EN EL NÚVOL

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

232. Els sistemes que subministren un servei en el núvol a organismes del sector públic hauran de complir amb un conjunt de mesures de seguretat en funció del model de servei:
    - Software com a servei
    - Plataforma com a servei
    - Infraestructura com a servei
233. Quan s'utilitzen serveis en el núvol subministrats per tercers, els sistemes d'informació que els suporten hauran de ser conformes amb l'ENS o complir amb les mesures descrites en altres guies que inclourà punts com:
    - Auditoria de proves de penetració.
    - Transparència.

- Xifrat i gestió de contrasenyes.
- Jurisdicció de les dades.

234. R1: Serveis certificats.
    - Quan s'utilitzin serveis en el núvol subministrats per tercers, aquests hauran d'estar certificats sota una metodologia de certificació reconeguda per l'Organisme de Certificació de l'Esquema Nacional d'Avaluació i Certificació de Seguretat de les Tecnologies de la Informació.
    - Si el servei en el núvol és un servei de seguretat haurà de complir amb els requisits establerts en [op.pl.5].

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.22 – Segregació en xarxes |

## 6.8 [OP.CONT] CONTINUÏTAT DEL SERVEI

235. Aquestes activitats permeten instrumentar els principis de seguretat:
    - Prevenció, reacció i recuperació.
236. Mesures per a frenar incidents desastrosos i permetre que els serveis es continuïn prestant en unes condicions mínimes després de l'ocurrència d'un desastre.
237. S'entén per desastre qualsevol esdeveniment accidental, natural o malintencionat que interromp les operacions o serveis habituals d'una entitat durant el prou temps per a veure la mateixa afectada de manera significativa.
238. Les mesures d'aquesta secció s'entenen com a complement holístic de les mesures requerides en altres punts relatives a mitjans alternatius i còpies de seguretat de la informació.

### 6.8.1 [OP.CONT.1] ANÀLISI D'IMPACTE

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

239. Una anàlisi d'impacte és un estudi detallat de com afectaria un desastre a la prestació de serveis, identificant els elements del sistema d'informació que són necessaris per a la prestació de cada servei.
240. Una anàlisi d'impacte és una activitat metòdica que segueix els següents passos:
    - S'identifiquen els serveis, processos o activitats crítics,
    - Es valora l'impacte de la interrupció d'aquests serveis, processos o activitats en funció del temps que duri la interrupció; sense perjudici que en cada cas es triï l'escala més adequada, són escales típiques de valoració les següents:
        - Dies: 1, 2, 3..., 10 dies

- Hores: 1, 2, 4, 8, 24, 48..., 120 hores

- S'identifiquen els recursos necessaris per a donar continuïtat a cada servei: instal·lacions, persones, equipament, comunicacions, programari i proveïdors
- S'estableix un temps de recuperació objectiu (**RTO**), bé per a cada servei, bé per a tots els sistemes d'informació de l'organisme, bé per famílies de serveis (crítics, normals, secundaris...) els sistemes que intervinguin en la prestació dels serveis heretaran el rto més restrictiu dels serveis en què intervinguin, podent segmentar-se per subsistemes.

241. Per a la informació, cal analitzar quanta és acceptable que es perdi en cas de desastre. Sobre la base d'aquest càlcul s'estableix, un punt de recuperació objectiu (RPO), que marcarà la freqüència de còpies de seguretat. Per exemple, si es fan còpies cada 24 hores, en el pitjor dels casos perdrem les actualitzacions de les últimes 24 hores, dient-se que el RPO = 24h. Si no es pot admetre aquesta pèrdua, cal establir objectius més ambiciosos, augmentant la freqüència de realització de còpies. En última instància es pot arribar a un RPO pràcticament igual a zero emprant tècniques d'emmagatzematge redundant.

242. L'anàlisi d'impacte ha d'incloure les implicacions sobre els proveïdors de serveis externs.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.29 – Seguretat de la informació durant la interrupció. |
| NIST SP 800-53 rev4 | - [CP] Contingency Planning |

### 6.8.2 [OP.CONT.2] PLA DE CONTINUÏTAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

243. S'han d'identificar funcions, responsabilitats i activitats a realitzar en cas de desastre que impedeixi prestar el servei en les condicions habituals i amb els mitjans habituals, podent diferenciar-se per als diferents escenaris de continuïtat que s'identifiquin.

244. En particular:

- Qui componen el comitè de crisi que pren la decisió d'aplicar els plans de continuïtat després d'analitzar el desastre i avaluar les conseqüències
- Qui s'encarregarà de la comunicació amb les parts afectades en cas de crisi
- Qui s'encarrega de reconstruir el sistema d'informació (recuperació de desastre)
- Les persones designades a les funcions dels punts anteriors seran conscients del seu rol en el pla de continuïtat

- En cas que les funcions s'hagin assignat a rols de l'entitat, existeix un document que permet identificar els rols amb les persones nominals

245. Ha d'existir una previsió dels mitjans alternatius que es conjugaran per a poder continuar prestant els serveis en cas de no poder fer-se amb els mitjans habituals:
    - Instal·lacions alternatives (veure [mp.if.9])
    - Comunicacions alternatives (veure [mp.com.9])
    - Equipament alternatiu (veure [mp.eq.9])
    - Personal alternatiu (veure [mp.per.9])
    - Proveïdors alternatius
    - Recuperació de la informació amb una antiguitat no superior a un topall determinat a la llum de l'anàlisi d'impacte (veure [mp.info.9] i [mp.cont.1.1])
246. Tots els mitjans alternatius han d'estar planificats i materialitzats en acords o contractes amb els proveïdors corresponents. El pla ha de determinar la coordinació de tots els elements per a aconseguir la restauració dels serveis en els terminis estipulats, així com punts de contacte, obligacions i canals de comunicació amb els proveïdors per a la sincronització de la recuperació d'un desastre.
247. Les persones afectades pel pla han de rebre formació específica relativa al seu paper en aquest pla.
248. El pla de continuïtat ha de ser part íntegra i harmònica amb els plans de continuïtat de l'entitat en altres matèries alienes a la seguretat.
249. Han d'establir-se procediments per a sincronitzar el pla de continuïtat amb les actualitzacions del sistema referent a arquitectura, elements components i serveis i qualitat dels serveis prestats. En altres paraules, els procediments operatius de seguretat referents a canvis i actualitzacions han d'incloure un punt per a actualitzar els plans de continuïtat.
250. El DSI és responsable de:
    - Mantenir la configuració i la gestió de canvis. Qualsevol canvi en els actius d'informació bàsics, actius d'informació estàndard, classes de seguretat, mesures de referència o mesures addicionals s'ha de registrar, mitjançant mecanismes de registre (logs) que permetin auditar la traçabilitat dels canvis. Aquests registres han d'incloure com a mínim l'identificador de l'usuari, el moment del canvi, l'actiu afectat i la naturalesa del canvi, i han d'estar a disposició de l'autoritat competent que supervisa l'entitat.
    - Si l'entitat fa canvis significatius en els serveis o en els actius d'informació inventariats, tot el procés d'implantació de l'ENS-AD ha de començar des del principi o des de l'etapa afectada pel canvi.

- Verificar sistemàticament la situació de seguretat real dels actius d'informació inventariats tenint en compte les seves amenaces reals, mitjançant l'anàlisi de registres d'activitat, indicadors d'alerta i resultats de monitoratge de seguretat.
- Garantir que els accessos als sistemes per part d'usuaris interns i proveïdors externs es realitzin de forma segura, mitjançant l'ús de mecanismes d'autenticació robusta, control d'accessos basat en rols, connexions protegides i registre d'activitat.
- Aplicar mesures de seguretat complementàries quan es detectin vulnerabilitats, mancances de protecció o noves amenaces que no estiguin cobertes per les mesures de referència, tenint en compte el context de l'actiu i la seva exposició.
- Impulsar la millora contínua del sistema de gestió mitjançant la revisió periòdica de les dades obtingudes dels registres, informes d'auditoria, incidents i canvis, amb l'objectiu de detectar oportunitats de millora i planificar accions correctives o preventives.

251. En cas d'existir perills que no estiguin coberts per l'especificació de seguretat de l'actiu d'informació estàndard, el DSI ha de verificar la idoneïtat de les mesures de seguretat implementades en les condicions reals i, si cal, aplicar mesures de seguretat addicionals.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.29 – Seguretat de la informació durant la interrupció. |
| NIST SP 800-53 rev4 | - [CP] Contingency Planning |

### 6.8.3 [OP.CONT.3] PROVES PERIÒDIQUES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

252. S'han de fer proves periòdiques per a localitzar (i corregir en el seu cas) els errors o deficiències que puguin existir en el pla d'acció en cas de desastre.

253. Es dissenyaran proves que, encara que tractin les accions a realitzar sobre la base de proves parcials independents, acabin cobrint tot l'espectre d'accions que haurien de realitzar-se en cas d'una situació de continuïtat. Aquestes proves hauran d'involucrar als responsables de la seva execució en cas de produir-se i podran ser de diversa tipologia com:

- Proves de validació: Validen el coneixement del personal involucrat respecte a les decisions i comunicacions (crides, correus, eines, etc.) que s'han de realitzar en cas de situació de continuïtat.

- Simulacres: Validen l'activació total o parcial del Pla de Continuïtat del Negoci (PCN) mitjançant proves unitàries (proves pràctiques d'accions concretes que s'haurien de realitzar).
- Prova d'entorn alternatiu: Validen el funcionament dels sistemes en la situació alternativa de contingència.
- Prova d'interrupció completa: Prova real executada en entorn de producció requerint treballar en situació alternativa.

254. Totes les entitats subjectes a l'ENS-AD o amb infraestructures crítiques regulades pel RIC-AD han de participar de forma activa en, com a mínim, un ciberexercici nacional cada dos anys, organitzat o coordinat per l'Agència Nacional de Ciberseguretat, l'AFA, o qualsevol altre organisme internacional sota normatives reconegudes.

255. La participació en els ciberexercicis ha d'integrar-se dins la planificació de proves del SGSI i constar com a activitat formal en el Pla Anual de Ciberseguretat. Les lliçons apreses han de quedar documentades i formar part del pla de millora contínua.

256. Cada entitat haurà d'emetre un informe d'avaluació interna, amb identificació de vulnerabilitats detectades, temps de resposta, coordinació entre equips i millores proposades.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.30 – Preparació per a les TIC per a la continuïtat de negoci |
| NIST SP 800-53 rev4 | - [CP] Contingency Planning |

### 6.8.4 [OP.CONT.4] MITJANS ALTERNATIUS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

257. La provisió de serveis externs serà part dels plans de continuïtat de l'entitat ([op.cont]).

258. Tots els canvis d'informació i prestació de serveis amb altres sistemes s'han de realitzar amb una autorització prèvia.

259. Per a cada interconnexió queda documentat les característiques, els requisits de seguretat, la protecció de dades i la naturalesa de la informació intercanviada.

260. S'ha establert un protocol de comunicació amb el proveïdor per a avisar de desastres i escalar el problema.

261. S'ha definit un procediment de reacció i recuperació (RTO) davant fallades prolongades del servei per part del proveïdor.

262. S'ha definit un procediment per a recuperar la informació amb l'antiguitat (RTPO) determinada per la política de l'Entitat.

263. Els processos d'actuació en cas de desastre es proven dins del pla de proves periòdiques ([op.cont.3]) de l'Entitat.

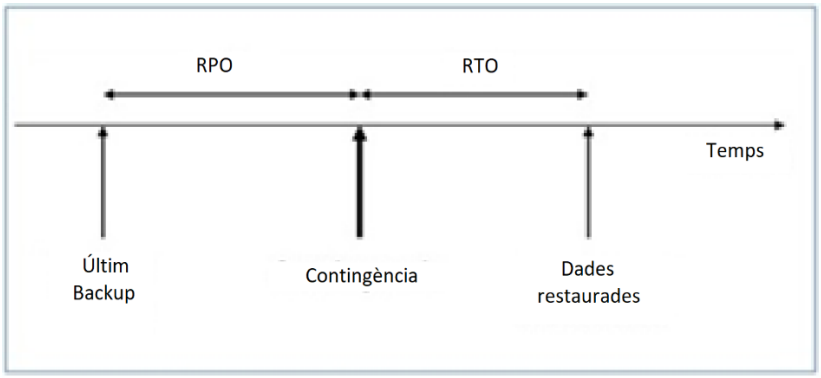


Fig.1: Punt de recuperació objectiu (RPO) i temps de recuperació objectiu (RTO).

264. Hi ha una àmplia varietat d'opcions alternatives a un servei prestat per un tercer:

- El mateix proveïdor proporciona els mitjans alternatius, en estar inclosos uns nivells mínims de SLA que estableixen l'obligatorietat de mantenir la continuïtat del proveïdor per a obtenir sempre el nivell de disponibilitat establert en el contracte, de manera que el client només ha de commutar l'accés. És aconsellable seleccionar adequadament aquells proveïdors que realment són crítics per a la continuïtat de l'operació del servei.
- Si el proveïdor alternatiu en realitat està funcionant sempre i simplement es fa càrrec de tota la càrrega de treball, cal establir un procediment per a ampliar la contractació i mantenir un nivell mínim de qualitat del servei

265. L'entitat pot recórrer a mitjans, havent de preveure els procediments citats en els punts anteriors.

266. La disponibilitat de mitjans alternatius estarà prevista per poder continuar prestant servei quan els mitjans habituals no estiguin disponibles. En concret, es cobriran els següents elements del sistema:

- Serveis contractats a tercers
- Instal·lacions alternatives
- Personal alternatiu
- Equipament informàtic alternatiu
- Mitjans de comunicació alternatiu

267. S'establirà un temps màxim perquè els Mitjans alternatius entrin en funcionament.

268. Els Mitjans alternatius estaran sotmesos a les mateixes garanties de seguretat que els originals.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.14 Redundància dels recursos de tractament de la informació |

## 6.9 [OP.MON] MONITORATGE DEL SISTEMA

269. L'actiu principal dels següents tres controls és la seguretat i tot el que es relaciona per garantir-la. Els diferents principis i eines que s'utilitzen com podrien ser els sistemes de monitoratge, mètriques per predir anomalies entre altres mesures.

### 6.9.1 [OP.MON.1] DETECCIÓ D'INTRUSIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

270. Aquestes activitats permeten instrumentar els principis de seguretat:
    - Prevenció, reacció i recuperació.
    - Línies de defensa.
271. El monitoratge del sistema permet detectar atacs i incidents en general habilitant les mesures de reacció i recopilant informació per a analitzar l'incident.
272. Les eines de monitoratge poden observar el trànsit en la xarxa o els registres d'activitat en els equips. En aquest segon cas, cal organitzar un sistema de recopilació d'informació des dels punts en què es genera.
273. És necessari instal·lar un sistema de monitoratge en la xarxa corporativa. Si existeixen punts d'interconnexió, han d'instal·lar-se sistemes de monitoratge en aquests punts, en particular si ens connectem a xarxes públiques com a Internet i si es permet l'accés remot amb dispositius on no es pot garantir la configuració de seguretat.
274. Es monitoraran aquells punts on l'anàlisi de riscos ha identificat un risc elevat.
275. El sistema de monitoratge buscarà tot allò que suposi un ús no autoritzat del sistema o un ús sospitós; per exemple:
    - descàrregues massives d'informació,
    - escombrat de ports,
    - accessos fora d'horari habitual,
    - accessos amb drets d'administrador,
    - freqüències anormals d'ús del sistema,
    - enviament d'informació a servidors externs,
    - trànsit xifrat,
    - descàrregues de servidors externs,
    - etc.
276. Cal detectar activitats d'atacants interns i externs, així com l'existència de troians o APT que poguessin haver-se introduït en el sistema.

277. Les entitats han de tenir un sistema automàtic de monitoratge que controli la infraestructura, les aplicacions i els serveis oferts. També han de documentar la informació sobre aquests entorns (aplicacions en producció, informació d'accés, usuaris i dades de prova) en un document normalitzat d'autorització de proves d'anàlisi de vulnerabilitats.

278. S'han d'abordar i monitorar els següents elements:

- Aplicacions específiques desenvolupades per a les entitats.
- Aplicacions o serveis comercials implantats per les entitats.
- Serveis d'infraestructura (correu electrònic, accés remot...)
- Aparició sobtada d'IPs, ports, serveis o aplicacions no contemplades en els inventaris proporcionats per les entitats.

279. La informació obtinguda de les anàlisis de vulnerabilitats s'utilitzarà com a entrada al procés intern d'intel·ligència d'amenaces i per a mantenir el servei actualitzat.

280. El servei de gestió de vulnerabilitats ha de tenir les següents característiques:

- Inventariat d'actius actualitzat.
- Monitoratge continu d'explotacions potencials.
- Haurà de comptar amb una gestió de troballes que es realitzarà de la següent manera: Les deficiències de seguretat constitueixen, principalment, vulnerabilitats o errors de configuració presents en els recursos de l'entorn de les entitats detectades gràcies als escanejos realitzats pels motors d'anàlisi. Aquesta informació, creuada amb la base de coneixement de vulnerabilitats, i amb la capacitat de verificació mitjançant consultes actives als mateixos recursos, hauran de tenir com a resultat troballes associades a les configuracions de serveis i recursos de l'entorn. Totes les deficiències de configuració hauran de ser gestionades seguint un sistema de priorització basat en severitat (Baix, Mitjà, Alt i Crític), a més d'un indicador de si és un actiu exposat a internet.

281. Com a resultat de la gestió de troballes s'ha de proporcionar un Pla de Remediació generant un full de ruta clar i manejable per poder abordar les diverses deficiències trobades d'acord amb una priorització personalitzada.

282. Totes les entitats afectades pel Reglament de l'Esquema nacional de seguretat del Principat d'Andorra estaran obligades a compartir de manera proactiva i sistemàtica la intel·ligència d'incidents de ciberseguretat amb l'ANC-AD, utilitzant els canals i plataformes establerts a aquest efecte. La definició dels formats, freqüència i detalls tècnics d'aquest intercanvi es farà mitjançant instruccions tècniques elaborades per grups de treball interdisciplinaris liderats per l'ANC-AD, amb participació de les entitats crítiques i altres actors rellevants.

283. R1: procediments de resposta. Han d'estar estipulats procediments de resposta a les alertes generades pel sistema de detecció o prevenció d'intrusions.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| NIST SP 800-53 rev4 | - [SI-4] Information System Monitoring |
| Altres referències | - NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS) |

### 6.9.2 [OP.MON.2] SISTEMA DE MÈTRIQUES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1+R2 |

284. Aquestes activitats permeten instrumentar els principis de seguretat.
    - Prevenció, reacció i recuperació.
    - Revaluació periòdica.
285. S'ha de disposar de mètriques predictives que anuncien possibles incidents abans que aquests es produeixin. Típicament, es recorre a indicadors de compliment i mesures dels recursos dedicats a la seguretat del sistema i als resultats de les auditories o autoavaluacions realitzades.
286. S'ha de disposar de mètriques d'eficiència que mesuren si els recursos dedicats a la seguretat són d'un volum adequat i prudent. Típicament, són mesures de recursos humans i de dotació econòmica.
287. És recomanable formalitzar el procés de generació d'indicadors, havent d'estar aprovat un conjunt d'indicadors, indicant per a cadascun:
    - L'objectiu que es pretén mesurar
    - El responsable de l'indicador
    - L'origen de la informació
    - El procediment de recollida i tractament de dades (mesuraments)
    - La freqüència de recollida de dades
    - El mètode d'elaboració d'indicadors a partir de les mesures
    - L'elaboració d'indicadors agregats a partir d'altres indicadors
    - Els criteris de valoració de l'indicador a l'efecte de reaccionar i prendre decisions
288. El procés d'avaluació dels indicadors és aconsellable complementar-lo amb un procés de report als diferents nivells que han de prendre decisions en l'Entitat:
    - Ha d'establir-se una llista formal de les persones o òrgans que rebran els indicadors
    - Ha d'establir-se el conjunt d'indicadors (probablement agregats) que rebrà cada destinatari

- Cada indicador vindrà acompanyat d'una explicació del seu objectiu i els criteris d'interpretació, emprant els termes adequats a l'activitat del receptor
- Ha d'establir-se la freqüència amb què se subministrarà cada indicador
- Ha de formalitzar-se el canal de report

289. Pot resultar d'utilitat l'ús d'eines automatitzades que permetin l'obtenció i visualització d'indicadors de manera transparent, a partir de dades d'entrada d'altres eines o inventaris.

290. S'ha de disposar de mètriques d'eficàcia, que indiquin que el sistema de protecció està protegint realment la seguretat de la informació i els serveis. Típicament, s'analitzen dades del procés de gestió d'incidents de seguretat. En concret:

- El nombre d'incidents de seguretat tractats
- El temps emprat per a tancar el 50% dels incidents
- El temps emprat per a tancar el 90% dels incidents

291. S'ha de disposar de mètriques d'eficiència que mesuren si els recursos dedicats a la seguretat són d'un volum adequat i prudent. Típicament mesurades de la fracció de recursos humans (hores) i de dotació econòmica (pressupost) dedicada a la seguretat dels sistemes TIC en relació amb el total de recursos dedicats a les Tecnologies de la Informació i la Comunicació.

292. R1: Efectivitat del sistema de gestió d'incidents. Es recopilen les dades precises que possibiliten avaluar el comportament del sistema de gestió d'incidents.

293. R2: Eficiència del sistema de gestió de la seguretat. Es recopilen les dades per conèixer l'eficiència del sistema de seguretat en relació amb els recursos consumits (temps i pressupost).

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| NIST SP 800-53 rev4 | - [PM-6] Information Security Measures of Performance |
| Altres referències | - NIST SP 800-55 - Performance Measurement Guide for Information Security<br>- NIST SP 800-80 - Guide for Developing Performance Metrics for Information Security<br>- ISO/IEC 27004 - Information technology – Security techniques – Information security management – Measurement |

### 6.9.3 [OP.MON.3] VIGILÀNCIA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 +R2 |

294. Es disposarà d'un sistema automàtic de recol·lecció d'esdeveniments de seguretat.

295. Les entitats hauran d'implementar serveis de monitoratge de xarxes socials, fòrums, web, deep web... per detectar possibles riscos i amenaces.

296. Vigilància de les fonts obertes per detectar amb antelació possibles atacs.

- Prestar especial atenció a campanyes que puguin organitzar-se al voltant de situacions especials, tant detectades per les mateixes entitats com comunicades per l'ANC-AD.
- Robatori de credencials. Publicació en fòrums públics o restringits, al web "oberta" o a la "deep web", d'informació sobre credencials de comptes de les entitats o de ciutadans en els serveis proporcionats per les entitats.
- Robatori de dades i fuites d'informació. Presència a internet. En fòrums públics o restringits, al web "oberta" o a la "Deep web", d'informació, documents, etc., de les entitats que no tinguin caràcter públic.
- Atacs de denegació de servei o de qualsevol altre tipus organitzats contra alguna entitat.

297. Les entitats hauran de col·laborar amb l'ANC-AD i aportar tota la informació necessària per elaborar la CMDB d'actius de l'entitat que permeti particularitzar al seu context la informació generada.

298. Les entitats hauran de facilitar a l'ANC-AD els dominis web, dominis de correu, xarxes socials, etc., gestionats per l'entitat per al seu correcte monitoratge, així com col·laborar amb l'ANC-AD proporcionant la informació de context relativa al negoci de l'entitat que sigui necessària per poder particularitzar l'activitat de vigilància digital.

299. Les entitats crítiques i les entitats equivalents a entitats crítiques hauran de disposar, de manera obligatòria, d'un Centre d'Operacions de Seguretat (SOC) amb capacitat nacional, de nivell mínim L2, amb recursos humans i prou tècnics per garantir la vigilància, detecció i resposta davant incidents de seguretat de la informació en temps real.

300. Per assegurar l'eficàcia i la fiabilitat d'aquests SOC, s'estableix que han d'estar certificats conforme a estàndards reconeguts internacionalment o bé formar part activa d'organismes internacionals acreditats en la coordinació de CERT/SOC. Es consideren vàlids, entre altres:

- Certificacions de gestió de serveis de seguretat de la informació, com ara ISO/IEC 27001, ISO/IEC 27035 (gestió d'incidents), o ISO/IEC 20000-1 (gestió de serveis TI).
- Certificacions SOC Type II conforme a l'estàndard SSAE 18 (Estats Units) o ISAE 3402 (àmbit internacional).

- Participació activa com a membres d'organismes internacionals com el FIRST (Forum of Incident Response and Security Teams), el Trusted Introducer (TF-CSIRT), RNS (Red nacional de SOC) o el CSIRT Europeu (ENISA).

301. Les entitats esmentades hauran de disposar obligatòriament d'almenys una sonda de monitoratge externa, gestionada per l'ANC-AD o per l'Autoritat Financera Andorrana (AFA), en funció de la seva competència sectorial. Aquesta sonda tindrà per objecte reforçar la supervisió, obtenir una visió agregada del que succeeix a la xarxa nacional i anticipar riscos sistèmics. Les dades recollides per aquesta sonda tindran caràcter confidencial i s'utilitzaran exclusivament amb finalitats de ciberseguretat nacional.

302. R1: Correlació d'esdeveniments: Es disposa d'un sistema automàtic de recol·lecció d'esdeveniments de seguretat que permeti la correlació.

303. R2: Anàlisi dinàmica: Es disposarà de solucions de vigilància que permetin determinar la superfície d'exposició amb relació amb les vulnerabilitats i deficiències de configuració.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.7 – Intel·ligència d'amenaces<br>- A.5.33 – Protecció dels registres<br>- A.8.8 – Gestió de vulnerabilitats tècniques<br>- A.8.16 – Seguiment d'activitats |
| NIST SP 800-53 rev4 | - [AC] Access Control<br>- [IR] Incident Response<br>- [AU] Audit and Accountability |

### 6.9.4 [OP.MON.4] REGISTRE D'ESDEVENIMENTS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

204. Les entitats han de garantir la generació, conservació i protecció dels logs següents:

Registres de Logs i Auditoria

- Logs d'accés i autenticació:
  - Inicis i tancaments de sessió.
  - ID d'usuari, rols, adreces IP, dispositius.
- Logs de seguretat:

- Alertes i esdeveniments de sistemes SIEM, IDS/IPS i firewalls.

- Logs de servidors i sistemes operatius:
  - Activitat crítica en servidors web, bases de dades i serveis.
  - Errors, accessos i accions administratives.
- Logs d'activitat d'aplicacions i bases de dades:
  - Consultes, modificacions, accés a APIs.
  - Ús de sistemes crítics i aplicacions empresarials.
- Logs de configuració i canvis:
  - Modificacions a sistemes, permisos, polítiques i aplicació de pegats
- Logs de connexions de xarxa i accessos segurs:
  - Connexions VPN i altres fluxos de comunicació amb dades sensibles

Registres de Xarxa

- Connexions de xarxa:
  - Dispositius connectats, IPs, horaris de connexió.
  - Activitat de connexions entrants i sortints.
- Xarxes privades virtuals (VPN):
  - Detalls de connexió d'usuaris (connexió i desconnexió).
- Captures de trànsit crítiques (si ho permet la normativa):
  - Fluxos rellevants de xarxa.

Configuracions i Canvis

- Configuració inicial i actualitzacions de:
  - Firewalls, routers, switches.
  - Sistemes operatius, servidors i aplicacions.
- Registres de canvis:
  - Implementació de polítiques noves.
  - Modificacions en permisos, rols i sistemes.
  - Aplicació de pegats de seguretat.

Informació sobre Comptes i Identitats

- Activitat d'usuaris:
    - Intents d'accés reeixits i fallits.
- Gestió de comptes:
    - Creació, modificació i eliminació de comptes.
- Accessos privilegiats:
    - Registre de sessions administratives.

Còpies de Seguretat (Backups)

- Backups de sistemes i dades crítiques:
    - Còpies completes i diferencials.
    - Retenció periòdica (setmanal, mensual).
- Verificació d'integritat:
    - Proves de restauració periòdiques.

Comunicacions i Fitxers Clau

- Correus electrònics:
    - Historial de comunicacions rellevants (internes i externes).
- Xats interns:
    - Converses operatives i sobre projectes sensibles.
- Documents corporatius:
    - Polítiques de seguretat, registres de projectes i desplegaments.

Activitats de Tercers i Proveïdors

- Accessos concedits a tercers i proveïdors.
- Activitat en sistemes compartits o externalitzats.
- Transferències de dades amb proveïdors externs.

Documentació i Polítiques Internes

- Documents de polítiques vigents.
- Historial d'auditories (internes i externes).
- Registres de formació i simulacres de ciberseguretat.

205. Segons els principis de l'article 4 de l'ENS-AD i els nivells de seguretat dels actius (articles 5 i 6):

- Xifratge de tots els logs i accés restringit.
- Duració mínima de conservació: 12 mesos (prorrogables segons normativa o risc).
- Sistemes d'emmagatzematge que garanteixin:
    - Integritat, Confidencialitat i Disponibilitat (CID/DIC).
    - Classificació de seguretat adequada (ex. D0-I0-C0 en infraestructures crítiques).
- Verificacions periòdiques:
    - Registre digital de les comprovacions d'integritat.

206. Tot accés als logs ha de quedar registrat i auditat. Només hi pot accedir personal autoritzat, amb responsabilitat assignada pel DSI i la direcció. L'accés pot ser requerit per autoritats competents, dins el termini establert per la normativa.

207. L'auditoria dels logs ha de formar part del Pla de Revisió anual del SGSI (ENS-AD, art. 8).

- Per a infraestructures crítiques:
    - Els logs s'integren en el Pla de Seguretat de l'Entitat (PSE) (RIC-AD, art. 10).

208. Compliment Normatiu i Protecció de Dades.

- Es garanteix el compliment de la Llei 29/2021 de protecció de dades (LQPD).
- Els logs amb dades personals es tractaran seguint els principis de:
    - Minimització, limitació de la finalitat i confidencialitat.
- Aquesta clàusula s'integra dins del Pla de Seguretat i del SGSI.

242. El SGSI de l'entitat ha de garantir la generació, conservació, protecció i revisió regular dels registres (logs) relacionats amb la seguretat de la informació. En concret, s'han de conservar, com a mínim, els tipus de registres següents:

- Registres d'accés i autenticació, incloent-hi inicis i finalitzacions de sessió, identificador d'usuari, adreça IP, dispositiu d'accés i rol associat.
- Registres de seguretat, com ara alertes dels sistemes SIEM, esdeveniments dels sistemes de detecció i prevenció d'intrusions (IDS/IPS), i incidències dels tallafocs.
- Registres dels servidors i sistemes operatius, incloent-hi activitat crítica, errors, accessos i accions administratives.

- Registres de configuració i canvis, que incloguin modificacions a sistemes, permisos, polítiques i aplicació de pegats.
- Registres de connexions de xarxa i accessos segurs, incloent-hi connexions VPN i altres fluxos de comunicació amb dades sensibles.
- Registres d'activitat d'aplicacions i bases de dades, incloent-hi consultes, canvis i accessos a APIs o informació protegida.

243. Aquests registres han de conservar-se durant el període mínim establert pel Catàleg i estar protegits contra manipulacions i accessos no autoritzats. La seva revisió ha d'estar contemplada dins els procediments regulars del SGSI i de les auditories de seguretat.

# 7 [MP] MESURES DE PROTECCIÓ

## 7.9 [MP.IF] PROTECCIÓ DE LES INSTAL·LACIONS I INFRAESTRUCTURES

209. Els següents controls especifiquen les mesures que s'han d'adoptar per garantir la protecció dels diversos equips i infraestructures davant d'incidents externs.

### 7.9.2 [MP.IF.1] ÀREES SEPARADES I AMB CONTROL D'ACCÉS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

210. S'han de delimitar les àrees de treball i d'equips, disposant d'un inventari actualitzat que per a cada àrea determini la seva funció i les persones responsables de la seva seguretat i d'autoritzar l'accés.

211. Quan l'accés es controli per mitjà de claus o dispositius equivalents, es disposarà d'un inventari de claus juntament amb un registre de qui les pren, qui les retorna i en mans de qui hi ha còpies a cada moment. En cas de sostracció o pèrdua, es procedirà al canvi amb diligència per a evitar el risc.

212. Es disposarà de mitjans que evitin l'accés per punts diferents del que disposa del control d'accés. S'evitaran finestres accessibles i portes desprotegides. En particular cal vigilar portes d'evacuació d'emergència perquè no permetin l'entrada ni en condicions normals ni quan s'utilitzen com a via d'evacuació (per exemple, càmeres de vigilància, panys electrònics que registren cada accés, etc.).

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.1 – Perímetre de seguretat física<br>- A.7.3 – Seguretat d'oficines, despatxos i recursos<br>- A.7.4 – Monitoratge de la seguretat física<br>- A.7.6 – El treball en àrees segures<br>- A.7.8 – Ubicació i protecció d'equips |
| NIST SP 800-53 rev4 | - [PE-18] Location of Information System Components<br>- [PE-3] Physical Access Control<br>- [PE-4] Access Control for Transmission Medium<br>- [PE-5] Access Control for Output Devices |

### 7.9.3 [MP.IF.2] IDENTIFICACIÓ DE LES PERSONES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

213. Per a les àrees d'accés restringit, s'ha de mantenir una relació de persones autoritzades i un sistema de control d'accés que verifiqui la identitat i l'autorització i deixi registre de tots els accessos de persones (per exemple, persona o identificador corporatiu, data i hora de cada entrada i sortida).

214. Es recomana que existeixi segregació de funcions en el procés de gestió d'accés als locals amb equipament (sol·licitud i autorització). Aquestes funcions han de recaure en almenys dues persones.

215. Ha de realitzar-se periòdicament una revisió de les autoritzacions, identificant si continua existint la necessitat d'accés que va motivar l'autorització.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.2 – Controls físics d'entrada |
| NIST SP 800-53 rev4 | - [PE-2] Physical Access Authorizations<br>- [PE-6] Monitoring Physical Access<br>- [PE-8] Visitor Access Records |

### 7.9.4 [MP.IF.3] ACONDICIONAMIENT DELS LOCALS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

216. S'ha de disposar d'unes instal·lacions adequades per a l'eficaç acompliment de l'equipament que s'instal·la en elles.

217. Sense perjudici del que es disposa en altres mesures més específiques, els locals han de:

- Garantir que la temperatura es troba en el marge especificat pels fabricants dels equips
- Garantir que la humitat es troba dins del marge especificat pels fabricants dels equips
- S'ha de protegir el local enfront de les amenaces identificades en l'anàlisi de riscos, tant d'índole natural, com a derivades de l'entorn o amb origen humà, accidental o deliberat (complementant [mp.if.1], [mp.if4], [mp.if.5], [mp.if.6] i [mp.if.7])
- S'ha d'evitar que el propi local sigui una amenaça en si mateix, o factor determinant d'altres amenaces, com l'existència de material innecessari o inflamable en el local (paper, caixes, etc.) O que pugui ser causa d'altres incidents (elements amb aigua, etc.)
- El cablejat ha d'estar:

- Etiquetat: es pot identificar cada cable físic i la seva correspondència als plans de la instal·lació
- Controlat: per a identificar el cablejat fora d'ús
- Protegit enfront d'accidents: per exemple, per a evitar que les persones ensopeguin amb els cables
- Protegit enfront d'accessos no autoritzats: protegint armaris de distribució

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.3 – Seguretat d'oficines, despatxos i recursos<br>- A.7.5 – Protecció contra les amenaces externes i ambientals<br>- A.7.12 – Seguretat del cablejat |
| NIST SP 800-53 rev4 | - [PE-14] Temperature and Humidity Controls |

### 7.9.5 [MP.IF.4] ENERGIA ELÈCTRICA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

218. S'han de preveure mesures per a atallar un possible tall de subministrament elèctric i un correcte funcionament de les llums d'emergència.

219. Prevenció de problemes d'origen intern:

    - Dimensionament i protecció del cablejat de potència
    - Dimensionat i protecció dels quadres i armaris de potència

220. Reacció a problemes d'origen extern:

    - Subministrament alternatiu: UPS, generadors, proveïdor alternatiu

221. S'ha de disposar d'un pla d'emergència, de reacció i de recuperació de desastres.

222. Cal disposar d'una alimentació suficient per a apagar els equips de forma ordenada. Normalment, això suposa una alimentació local (SAI, o UPS per les seves sigles en anglès) que garanteixi el subministrament elèctric durant els minuts necessaris per a activar i concloure el procediment d'apagat d'emergència, i grups electrògens en cas de ser necessari.

223. R1: Subministrament elèctric d'emergència: En cas de fallada del subministrament principal, el proveïment elèctric haurà d'estar garantit durant prou temps per a una terminació ordenada dels processos i la salvaguarda de la informació.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.11 – Instal·lacions de subministrament |
| NIST SP 800-53 rev4 | - [PE-9] Power Equipment and Cabling |

| | |
|---|---|
| | - [PE-10] Emergency Shutoff<br>- [PE-11] Emergency Power<br>- [PE-12] Emergency Lighting |

### 7.9.6 [MP.IF.5] PROTECCIÓ ENFRONT D'INCENDIS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

224. S'ha de realitzar un estudi del risc d'incendis, tant d'origen natural com industrial:
    - Entorn natural procliu a incendis
    - Entorn industrial que pogués incendiar-se
    - Instal·lacions pròpies amb el risc d'incendi
225. Si el foc no es pot evitar, cal desplegar mesures de prevenció, monitoratge i limitació de l'impacte.
    - Disposar de cartells per a evacuació
    - Evitar l'ús de materials inflamables
    - Aïllament (tallafocs, portes ignífugues)
    - Sistema de detecció connectat a central d'alarmes 24x7
    - Mitjans de reacció: mitjans d'extinció
    - Pla d'emergència, de reacció i de recuperació de desastres

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.5 - Protecció contra les amenaces externes i ambientals |
| NIST SP 800-53 rev4 | - [PE-13] Fire Protection |

### 7.9.7 [MP.IF.6] PROTECCIÓ ENFRONT DE INUNDACIONS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

226. S'ha de realitzar un estudi del risc d'inundacions, tant d'origen natural com indústria:
    - Proximitat a rius o corrents d'aigua
    - Canalitzacions d'aigua (canonades) especialment damunt dels equips
227. Si el risc no es pot evitar, cal desplegar mesures de prevenció, monitoratge i limitació de l'impacte.
    - Aïllament d'humitats
    - Canalització de desguàs amb procediments regulars de neteja
    - Sistema de detecció connectat a central d'alarmes 24x7

- Pla de reacció i recuperació de desastres; en el cas de canalitzacions industrials, el pla de reacció pot incloure el tancament de claus o vàlvules que atallin l'abocament.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.5 - Protecció contra les amenaces externes i ambientals |
| NIST SP 800-53 rev4 | - [PE-15] Water Damage Protection |

### 7.9.8 [MP.IF.7] REGISTRE D'ENTRADA I SORTIDA D'EQUIPAMENT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

228. S'ha de portar un registre detallat de tota entrada i sortida d'equipament, fent constar en aquest:
    - Data i hora
    - Identificació inequívoca de l'equipament (servidors, portàtils, equips de comunicacions, suports d'informació, etc.)
    - Persona que realitza l'entrada o sortida
    - Persona que autoritza l'entrada o sortida
    - Persona que realitza el registre
229. Es recomana que existeixi segregació de funcions en el procés de gestió d'entrada i sortida d'equipament en els locals (sol·licitud i autorització). Aquestes funcions han de recaure en almenys dues persones.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.2 – Controls físics d'entrada |
| NIST SP 800-53 rev4 | - [PE-16] Delivery and Removal |

## 7.10 [MP.PER] GESTIÓ DEL PERSONAL

230. Mesures per a protegir el sistema de problemes que poguessin ser causats per les persones que gaudeixen d'accés a aquest.

### 7.10.2 [MP.PER.1] CARACTERITZACIÓ DEL LLOC DE TREBALL

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

231. S'han de definir les responsabilitats relacionades amb cada lloc de treball en matèria de seguretat. La definició ha de venir recolzada per l'anàlisi de riscos en la mesura en què afecta cada lloc de treball.

232. S'han de definir els requisits que han de satisfer les persones que vagin a ocupar el lloc de treball, en particular en termes de confidencialitat.

233. S'han de tenir en compte aquests requisits en la selecció de la persona que ho ocuparà, incloent-hi la verificació dels seus antecedents laborals, formació i altres referències: dins del marc de la llei.

234. Els administradors de seguretat tindran una Habilitació Personal de Seguretat (PHS) donada per l'autoritat competent a conseqüència dels resultats de l'anàlisi de riscs previs.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.6.1 - Comprovació |
| NIST SP 800-53 rev4 | - [PS-2] Position Risk Designation<br>- [PS-3] Personnel Screening<br>- [SA-21] Developer Screening |

### 7.10.3 [MP.PER.2] DEURES I OBLIGACIONS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

235. S'ha d'informar cada persona relacionada amb el sistema dels deures i responsabilitats del seu lloc de treball en matèria de seguretat, incloent-hi les mesures disciplinàries al fet que pertoqui.

236. S'ha de cobrir tant el període durant el qual s'exerceix el lloc com les obligacions en cas de terminació de l'assignació, incloent-hi el cas de trasllat a un altre lloc de treball.

237. És d'especial rellevància el deure de confidencialitat respecte de les dades als quals tinguin accés, tant durant el període durant el qual estiguin adscrits al lloc de treball, com la seva prolongació posterior a la terminació de la funció per a la qual va tenir accés a la informació confidencial.

238. En el cas de personal contractat a través d'una tercera part:

- S'han de determinar deures i obligacions de la persona
- S'han de determinar deures i obligacions de la part contractant
- S'ha de determinar el procediment de resolució d'incidents relacionats amb l'incompliment de les obligacions, involucrant a la part contractant

239. R1: Confirmació expressa. S'ha d'obtenir la confirmació expressa que els usuaris coneixen les instruccions de seguretat necessàries i obligatòries i la seva acceptació. També els procediments necessaris per realitzar-les de forma adequada.

| Marc de referència | Controls d'aplicabilitat |
|---|---|

| | |
|---|---|
| ISO/IEC 27002:2022 | - A.6.2 – Condicions de contractació<br>- A.6.5 – Responsabilitats davant la finalització o canvi<br>- A.6.6 – Acords de confidencialitat o no divulgació<br>- A.6.7 – Teletreball |
| NIST SP 800-53 rev4 | - [PL-4] Rules of Behavior<br>- [PS-6] Access Agreements<br>- [PS-7] Third-Party Personnel Security<br>- [PS-4] Personnel Termination<br>- [PS-5] Personnel Transfer<br>- [PS-8] Personnel Sanctions |

### 7.10.4 [MP.PER.3] CONSCIENCIACIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

240. S'ha de conscienciar regularment al personal sobre el seu paper i responsabilitat perquè la seguretat del sistema aconsegueixi els nivells exigits.

241. En particular cal refrescar regularment:

- La normativa de seguretat relativa al bon ús dels sistemes i les tècniques d'enginyeria social més habituals.
- La identificació d'incidents, activitats o comportaments sospitosos que hagin de ser reportats per al seu tractament per personal especialitzat
- El procediment de report d'incidents de seguretat, siguin reals o falses alarmes

242. Tot el personal ha de rebre inicialment i regularment informació sobre els punts a dalt descrits.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.6.3 – Conscienciació, educació i formació en seguretat de la informació |
| NIST SP 800-53 rev4 | - [AT-2] Security Awareness Training<br>- [AT-3] Role-Based Security Training<br>- [CP-3] Contingency Training<br>- [IR-2] Incident Response Training<br>- [PM-13] Information Security Resources |
| Altres referències | - NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program |

### 7.10.5 [MP.PER.4] FORMACIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

243. S'ha de formar regularment a les persones en aquelles tècniques que requereixin per a l'acompliment de les seves funcions.

244. Cal destacar, sense perjudici d'altres aspectes:

- Configuració de sistemes
- Gestió d'incidents (detecció i reacció)
- Procediments relatius a les seves funcions sobre la gestió de la informació (emmagatzematge, transferència, còpies, distribució i destrucció)
- S'avaluarà l'eficàcia de les accions formatives

245. La formació ha d'actualitzar-se cada vegada que canvien els components del sistema d'informació, introduint-se nous equips, nou programari, noves instal·lacions, etc.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27001:2022 | - 7.2 – Competències |
| ISO/IEC 27002:2022 | - A.6.3 – Conscienciació, educació i formació en seguretat de la informació |
| NIST SP 800-53 rev4 | - [AT-2] Security Awareness Training<br>- [AT-3] Role-Based Security Training<br>- [AT-4] Security Training Records<br>- [CP-3] Contingency Training<br>- [IR-2] Incident Response Training<br>- [PM-13] Information Security Resources |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>o CSC.17 - Security Skills Assessment and Appropriate Training to Fill Gaps<br>- NIST SP 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model<br>- NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program |

## 7.11 [MP.EQ] PROTECCIÓ DELS EQUIPS

246. Els controls d'aquesta secció es centren més en els dispositius i en els equips que utilitzen els treballadors. Les polítiques i mesures que s'han d'adoptar per evitar incidents i controlar-ne la seguretat.

### 7.11.2 [MP.EQ.1] LLOC DE TREBALL ORDENAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

247. S'ha d'exigir que els llocs de treball estiguin nets, sense més material damunt de la taula que el requerit per a l'activitat que s'està realitzant a cada moment. Segons s'acabi una tasca, el material es retirarà a una altra zona: calaixos, prestatgeries personals o comunes, magatzem, etc.

248. R1: Emmagatzematge del material. El material de treball es guardarà en un lloc tancat. Poden ser calaixos o armaris amb clau, o una habitació separada tancada amb clau almenys fora de l'horari de treball.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.7 – Lloc de treball buidat i pantalla neta |

### 7.11.3 [MP.EQ.2] BLOQUEIG DE LLOC DE TREBALL

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

249. S'ha de bloquejar automàticament el lloc de treball des del qual s'accedeix a serveis o dades de nivell mitjà o superior al cap d'un temps d'inactivitat, que es marcarà per part de l'entitat o companyia.

250. S'ha de requerir a l'usuari autenticar-se de nou per a reprendre l'activitat en curs.

251. El temps esmentat serà part de la configuració de l'equip i no podrà ser alterat per l'usuari.

252. Es cancel·laran les sessions obertes tant des d'aquest lloc de treball com les remotes al cap d'un temps d'inactivitat (superior al bloqueig del lloc de treball).

253. El temps esmentat serà part de la configuració de l'equip i no podrà ser alterat per l'usuari.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.7 – Lloc de treball buidat i pantalla neta |
| NIST SP 800-53 rev. 4 | - [AC-11] Session Lock |

| | |
|---|---|
| | - [AC-12] Session Termination |

### 7.11.4 [MP.EQ.3] PROTECCIÓ D'EQUIPS PORTÀTILS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

254. Ha d'existir un inventari dels equips portàtils, que identifiqui l'equip portàtil al costat de la persona responsable d'aquest. S'ha de verificar regularment en l'inventari que l'equip roman sota control de l'usuari al qual està assignat.

255. Es recomana que els equips portàtils tinguin instal·lat i activat un sistema de protecció perimetral (tallafocs personal) configurat per a bloquejar accessos excepte els autoritzats. Els accessos autoritzats seguiran els procediments d'autorització de l'organisme (veure [org.4]).

256. Els accessos realitzats remotament hauran de ser distingits pel servidor perquè pugui limitar i autoritzar la informació i els serveis accessibles quan es connectin remotament a través de xarxes que no pugui controlar l'entitat.

257. El mecanisme de control de l'equip formarà part de la configuració de l'equip i no podrà ser modificat per l'usuari.

258. Els usuaris rebran instruccions sobre l'ús admissible de l'equip, sobre els aspectes que ha de contemplar en el seu ús diari i del canal de comunicació per a informar el servei de gestió d'incidents en cas d'avaria, pèrdua, robatori o terminació.

259. S'haurà de comunicar al personal que els equips portàtils no han de contenir claus d'accés remot a l'entitat i s'identificarà i aprovarà formalment aquells casos en els quals no pot aplicar-se.

260. Els equips portàtils hauran de disposar de detectors de violació que permetin saber si l'equip ha estat manipulat i, en cas afirmatiu, activar els procediments de gestió d'incidents. Els detectors de violació podran ser:

    - Físics: per exemple, adhesius que s'alteren en manipular-los, brides de protecció, etc.
    - Lògics: per exemple, eines automatitzades que detectin si algun component del portàtil ha estat extret o substituït

261. Es recomana protegir l'accés a la informació que contenen els equips portàtils que siguin susceptibles de sortir de les instal·lacions de l'entitat (per exemple, amb cadenats, discos durs xifrats, etc.).

262. S'evitarà que el dispositiu portàtil tingui claus d'accés remot a l'organització que no siguin imprescindibles. Les claus són aquelles que són capaces d'habilitar un accés a altres equips de l'organització.

263. S'ha de protegir la informació continguda de nivell alt per mitjans criptogràfics: [mp.si.2].

264. Les claus criptogràfiques han de protegir-se segons [op.exp.11].

265. Quan l'equip és desmantellat, s'ha d'aplicar el que es preveu en [mp.si.5].

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.8 – Ubicació i protecció d'equips<br>- A.7.9 – Seguretat dels equips fora de les instal·lacions<br>- A.8.1 – Dispositius de punt final de l'usuari<br>- A.8.12 – Prevenció de fuita de dades |
| NIST SP 800-53 rev. 4 | - [AC-19] Access Control for Mobile Devices |

### 7.11.5 [MP.EQ.4] ALTRES DISPOSITIUS CONNECTATS A LA XARXA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

266. Aquesta mesura afecta a tota mena de dispositius connectats a la xarxa i que puguin tenir accés a la informació. En són exemples:
    - Dispositius multifunció: Impressores, escàners, etc
    - Dispositius multimedia: projectors, altaveus intel·ligents, etc
    - Dispositius internet de les coses (IoT)
    - Dispositius de convidats i personals dels mateixos treballadors (BYOD)

267. S'ha de preveure mitjans alternatius de tractament de la informació per al cas que fallin els equips de personal habituals. Aquests mitjans alternatius estaran subjectes a les mateixes garanties de protecció.

268. S'ha d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

269. Els equips alternatius poden estar disposats per a entrar en servei immediatament (és a dir, configurats) o requerir un temps de personalització (es pot disposar d'ells en el temps preestablert; però cal configurar-los i carregar les dades). En tot cas el temps d'entrada en servei ha d'estar sostingut per una anàlisi d'impacte (veure [op.cont.1]).

270. Els dispositius presents en la xarxa que disposin d'algun tipus d'emmagatzematge temporal o permanent d'informació proporcionaran la funcionalitat necessària per a eliminar la informació del suport.

271. R1: Productes certificats. Quan sigui possible, utilitzar, productes o serveis que compleixin [op.pl.5]

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.1 – Dispositius finals d'usuari |

## 7.12 [MP.COM] PROTECCIÓ DE LES COMUNICACIONS

### 7.12.2 [MP.COM.1] PERÍMETRE SEGUR

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

272. S'ha de delimitar el perímetre lògic del sistema; és a dir, els punts d'interconnexió amb l'exterior. Aquest perímetre haurà d'estar reflectit en la documentació de l'arquitectura del sistema (per exemple, l'esquema de xarxa).

273. S'ha de disposar de tallafocs que separin la xarxa interna de l'exterior. Tot el trànsit haurà de travessar aquests tallafocs que només deixessin transitar els fluxos prèviament autoritzats.

274. Els atacs de denegació de servei poden ser afrontats en el perímetre, encara que poden requerir la intervenció d'altres elements. En el perímetre es poden detectar patrons sospitosos de comportament: allaus de peticions, peticions trucades i, en general, un ús maliciós dels protocols de comunicacions. Algunes d'aquestes peticions poden ser denegades directament per l'equip perimetral, en altres ocasions cal aixecar una alarma per a actuar on correspongui (servidors web, servidors de bases de dades... o contactant amb els centres de resposta a incidents).

275. Tots els fluxos d'informació a través del perímetre han d'estar autoritzats prèviament. La Instrucció Tècnica de Seguretat d'Interconnexió de Sistemes d'Informació determinarà els requisits establerts en el perímetre que han de complir tots els components del sistema.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.12 – Prevenció de fuita de dades<br>- A.8.20 – Seguretat de xarxes |
| NIST SP 800-53 rev. 4 | - [AC-4] Information Flow Enforcement<br>- [CA-3] System Interconnections<br>- [SC-7] Boundary Protection |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>○ CSC.8 - Malware Defenses<br>○ CSC.9 – Limitation and Control of Network Ports<br>○ CSC.11 – Secure Configurations for Network Devices<br>○ CSC.12 – Boundary Defense |

| | |
|---|---|
| | ○ CSC.13 – Data Protection<br>○ CSC.15 - Wireless Access Control<br>- NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy |

### 7.12.3 [MP.COM.2] PROTECCIÓ DE LA CONFIDENCIALITAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

276. S'utilitzaran xarxes privades xifrades quan la comunicació discorri per xarxes fora del domini de la seguretat.

277. R1: algoritmes i paràmetres autoritzats. Es faran servir aquells autoritzats per l'ANC-AD.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.12 – Prevenció de fuita de dades<br>- A.8.21 – Seguretat dels serveis de xarxa |
| NIST SP 800-53 rev. 4 | - [AC-4] Information Flow Enforcement<br>- [AC-18] Wireless Access<br>- [SC-8] Transmission Confidentiality and Integrity<br>- [SC-12] Cryptographic Key Establishment and Management<br>- [SC-13] Cryptographic Protection<br>- [SC-40] Wireless Link Protection |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>○ CSC.15 - Wireless Access Control<br>- NIST SP 800-48 - Wireless Network Security for IEEE 802.11a/b/g and Bluetooth<br>- NIST SP 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations<br>- NIST SP 800-77 - Guide to IPsec VPNs<br>- NIST SP 800-113 - Guide to SSL VPNs<br>- NIST SP 800-121 - Guide to Bluetooth Security<br>- NIST SP 800-127 - Guide to Securing WiMAX Wireless Communications<br>- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs) |

| | |
|---|---|
| | - SSL – Secure Sockets Layer<br>  ○ [RFC 6101] The Secure Sockets Layer (SSL) Protocol Version 3.0<br>  ○ TLS – Transport Layer Security<br>  ○ [RFC 5246] The Transport Layer Security (TLS) Protocol – Version 1.2<br>  ○ [RFC 6176] Prohibiting Secure Sockets Layer (SSL) Version 2.0<br>- SSH – Secure Shell<br>- SCP – Secure copy<br>- SFTP – SSH File Transfer Protocol |

### 7.12.4 [MP.COM.3] PROTECCIÓ DE L'AUTENTICITAT I DE LA INTEGRITAT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1+R2 |

278. És freqüent que autenticitat, integritat i confidencialitat es tractin de manera conjunta negociant els protocols, els paràmetres i les claus en la fase d'establiment. És per això que aquesta mesura sol implementar-se al mateix temps que [mp.com.2].

279. S'ha d'establir de manera fefaent l'autenticitat de l'altre extrem d'un canal de comunicació abans d'intercanviar cap informació.

280. S'ha d'evitar la utilització de mecanismes d'autenticació i protocols no contemplats en la normativa de l'entitat.

281. S'han d'usar protocols que garanteixin o almenys comprovin i detectin violacions en la integritat de les dades intercanviades i en la seqüència dels paquets.

282. La forma més habitual d'establir aquesta mesura és establir una xarxa privada virtual que:

    - Garanteixi l'autenticació de les parts a l'inici de sessió, quan la xarxa s'estableix
    - Controli que la sessió no pot ser segrestada per una tercera part
    - Que no permeti realitzar atacs actius (alteració de la informació en trànsit o injecció d'informació espúria) sense que sigui, almenys, detectada

283. Cal seleccionar algoritmes avaluats o acreditats que garanteixin el secret de les dades transmeses. Sovint n'hi ha prou amb seleccionar els algoritmes i els paràmetres adequats dins de les opcions possibles.

284. S'ha d'evitar la utilització de mecanismes d'autenticació i protocols no contemplats en la normativa d'aplicació. A més, en cas d'utilitzar claus concertades, hauran de fer-se servir amb cautela aplicant exigències mitjanes de qualitat.

285. En connexions establertes fora del domini de seguretat de l'entitat, es pot recórrer a xarxes privades virtuals que, amb mètodes criptogràfics i després d'una autenticació fiable, estableixen una clau de xifratge per a la sessió.

286. El xifratge de les comunicacions és especialment adequat en xarxes sense fils (Wifi). Els equips sense fils porten incorporats mecanismes de xifratge de les comunicacions, que hauran de ser configurats de manera segura (veure [op.exp.2] i [op.exp.3]) emprant mecanismes actualitzats.

287. Cal atendre el secret de les claus de xifratge segons s'indica en [op.exp.11]. En el cas de xarxes privades virtuals, el secret ha de ser impredictible, mantenir-se sota custòdia mentre duri la sessió, i ser destruït en acabar. En el cas d'altres procediments de xifratge, cal cuidar les claus de xifratge durant el seu cicle de vida: generació, distribució, ocupació, retirada del servei i retenció si n'hi hagués.

288. Cal procurar que les tasques de xifratge en els extrems es realitzin en equips maquinari especialitzat i certificats, conforme a [op.pl.5], evitant el xifratge per programari.

289. S'ha d'evitar la utilització de mecanismes d'autenticació i protocols no contemplats en la normativa d'aplicació. A més, en cas d'utilitzar claus concertades, hauran de fer-se servir amb cautela aplicant exigències altes de qualitat.

290. R1: Xarxes privades virtuals. Es faran servir xarxes privades virtuals xifrades quan la comunicació discorri per xarxes fora del mateix domini de seguretat.

291. R2: Algoritmes i paràmetres autoritzats. Es faran servir algoritmes i paràmetres autoritzats per ANC-AD

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.21 - Seguretat dels serveis de xarxa<br>- A.8.26 Requisits de seguretat de les aplicacions |
| NIST SP 800-53 rev. 4 | - [AC-18] Wireless Access<br>- [SC-8] Transmission Confidentiality and Integrity<br>- [SC-13] Cryptographic Protection<br>- [SC-23] Session Authenticity<br>- [SC-40] Wireless Link Protection |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>o CSC.15 - Wireless Access Control |

### 7.12.5 [MP.COM.4] SEGREGACIÓ DE XARXES

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits + [R1 o R2 o R3] |

292. La segregació de xarxes delimita l'accés a la informació i delimita la propagació dels incidents de seguretat que queden restringits a l'entorn on ocorren. Aquesta haurà de quedar reflectida en documentació de l'arquitectura del sistema (per exemple, l'esquema de xarxa) [op.pl.2].

293. S'ha de segmentar la xarxa de manera que hi hagi:

- control (d'entrada) dels usuaris que poden treballar en cada segment, en particular si l'accés es realitza des de l'exterior del segment, tant si és des d'un altre segment de la xarxa corporativa com si l'accés prové de l'exterior de la xarxa, extremant les precaucions en aquest últim escenari.
- control (de sortida) de la informació disponible en cada segment
- control (d'entrada) de les aplicacions utilitzables en cada segment

294. El punt d'interconnexió ha d'estar particularment assegurat, mantingut i monitorat (veure [mp.com.1]). Aquests punts d'interconnexió interna són una defensa crítica enfront d'intrusos que han aconseguit superar les barreres exteriors i s'allotgen a l'interior. Sovint l'objectiu d'aquestes intrusions és extreure informació i enviar-la a l'exterior, la qual cosa es tradueix en el fet que cal vigilar els protocols de comunicacions que s'estableixen i les dades que es transmeten.

295. No hauria de permetre's cap protocol directe entre els segments interns i l'exterior, mitjançant tots els intercanvis d'informació.

296. Les xarxes es poden segmentar per dispositius físics o lògics.

297. Aquesta mesura pot establir-se dinàmicament com a reacció enfront d'intrusions (suposades o detectades) i que requeriran un cert període de temps (dies) a poder ser erradicades. Els primers serveis a aïllar serien els servidors de dades i els servidors d'autenticació per a monitorar i controlar el seu ús. Altres candidats a ser aïllats són els serveis d'administració del mateix sistema per a evitar que es capturin credencials amb privilegis d'administració o es pugui suplantar la identitat dels administradors.

298. R1: Segmentació lògica bàsica. Els segments de xarxa s'implementaran per mitjà de xarxes d'àrea local virtuals. La xarxa haurà de segregar-se en diverses subxarxes contemplant usuaris, serveis i administració.

299. R2: Segmentació lògica avançada: Els segments de xarxa s'implementaran per mitjà de xarxes privades virtuals (VPN).

300. R3: Segmentació física: Els segments de xarxa s'implementaran amb mitjans físics separats.

| Marc de referència | Controls d'aplicabilitat |
|---|---|

| | |
|---|---|
| ISO/IEC 27002:2022 | - A.8.22 – Segregació en xarxes |
| NIST SP 800-53 rev. 4 | - [SC-32] Information System Partitioning |

## 7.13 [MP.SI] PROTECCIÓ DELS SUPORTS D'INFORMACIÓ

301. Els suports d'informació inclouen:

- discos dels servidors i equips d'usuari final, amb especial consideració a equips portàtils i discos amovibles
- PDAs
- disquets, cintes, CD, DVD...
- discos USB
- targetes de memòria i targetes intel·ligents
- components d'impressores
- material imprès
- altres mitjans d'emmagatzematge d'informació amb capacitat que la informació pugui ser recuperada de formar automàtica o manual

### 7.13.2 [MP.SI.1] ETIQUETAT DE SUPORTS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

302. S'ha d'etiquetar de manera que, sense revelar el seu contingut, s'indiqui el nivell de qualificació més alt de la informació continguda.

303. Una opció és que el mateix suport, en el seu exterior, porti escrit el nivell d'informació que conté o pot contenir.

304. Una alternativa és que el suport sigui identificable per mitjà d'algun codi o referència i que l'usuari pugui accedir a un repositori d'informació on s'indica el nivell d'informació que el suport conté o pot contenir.

305. L'etiqueta del suport determina les normatives i els procediments que han d'aplicar-se a aquest, concretament referent a:

- control d'accés
- xifrat del contingut
- entrada i sortida de les instal·lacions
- mitjans de transport

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.13 – Etiquetatge de la informació<br>- A.7.10 – Suports d'emmagatzematge |
| NIST SP 800-53 rev. 4 | - [MP-3] Media Marking |

### 7.13.3 [MP.SI.2] CRIPTOGRAFIA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

306. Aquest requisit s'aplica, en particular, a tots els dispositius removibles (com CD, DVD, discos USB, etc.).
307. Referent a claus criptogràfiques, s'ha d'aplicar [op.exp.11].
308. Una opció és assegurar-se que les dades es protegeixen abans de copiar-se al suport; és a dir, es xifren o se signen exteriorment.
309. Una altra opció és protegir tot el suport instal·lant en el mateix un disc virtual que s'encarrega d'acollir tot el que es copiï en aquest, així com controlar l'accés a aquest.
310. Una altra opció és emprar suports amb xifratge incorporat per maquinari que s'encarrega d'acollir tot el que es copiï en el suport, així com controlar l'accés a aquest.
311. Productes. Hi ha molts on triar. Al mercat existeixen moltes solucions de criptografia, que poden ser adaptades i configurades a les necessitats de cada entitat i a la infraestructura o aplicacions on es vulgui integrar.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.10 – Suports d'emmagatzematge<br>- A.8.12 – Prevenció de fuita de dades<br>- A.8.24 – Ús de criptografia |
| NIST SP 800-53 rev. 4 | - [SC-28] Protection of Information at Rest |
| Altres referències | - NIST SP 800-111 - Guide to Storage Encryption Technologies for End User Devices |

### 7.13.4 [MP.SI.3] CUSTÒDIA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

312. S'ha d'aplicar la deguda diligència i control als suports d'informació (tant en suport electrònic com no electrònic) que romanen sota la responsabilitat de l'entitat:
    - Garantint el control d'accés amb mesures físiques ([mp.if.1] i [mp.if.7) o lògiques ([mp.si.2]) o ambdues
    - Garantint que es respecten les exigències de manteniment del fabricador, especialment referent a temperatura, humitat i altres agressors mediambientals

313. Es recomana conservar la història de cada dispositiu, des del seu primer ús fins a la terminació de la seva vida útil i verificar regularment que els suports compleixen les regles concordes al seu etiquetatge.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.10 – Ús acceptable de la informació i actius associats<br>- A.7.10 – Suports d'emmagatzematge |
| NIST SP 800-53 rev. 4 | - [MP-4] Media Storage |
| Altres referències | - NIST SP 800-111 – Guide to Storage Encryption Technologies for End User Devices |

### 7.13.5 [MP.SI.4] TRANSPORT

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

314. S'ha de garantir que els dispositius romanen sota control i se satisfan els seus requisits de seguretat mentre són desplaçats d'un lloc a un altre. S'ha de:

- Disposar d'un registre de sortida que identifica almenys l'etiqueta i al transportista que rep el suport per al seu trasllat (tant electrònic com no electrònic)
- Disposar d'un registre d'entrada que identifica almenys l'etiqueta i al transportista que el lliura
- Disposar d'un procediment rutinari que acara les sortides amb les arribades i aixeca les alarmes pertinents quan es detecta algun incident
- Utilitzar els mitjans de protecció criptogràfica ([mp.si.2]) corresponents al nivell de classificació de la informació continguda de major nivell
- Gestionar les claus segons [op.exp.11]

315. Es recomana disposar d'un procediment sobre aquest tema i es verifica regularment que els procediments establerts se segueixen, aplicant mesures correctives en defecte d'això.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.10 – Suports d'emmagatzematge |
| NIST SP 800-53 rev. 4 | - [MP-5] Media Transport |

### 7.13.6 [MP.SI.5] BORRAT I DESTRUCCIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

316. S'ha d'aplicar un mecanisme d'esborrament segur als suports extraïbles (electrònics i no electrònics) que vagin a ser reutilitzats per a una altra informació o alliberats a una altra entitat. El mecanisme d'esborrament serà proporcionat a la classificació de la informació que ha estat present en el suport.

317. S'han de destruir els suports, de manera segura:

- Quan la naturalesa del suport no permeti un esborrament segur
- Quan el procediment associat al nivell de classificació de la informació continguda així ho requereix

318. El mecanisme de destrucció serà proporcionat a la classificació de la informació continguda.

319. Els mecanismes d'esborrament i destrucció han de tenir en la normativa de protecció mediambiental i els certificats de qualitat mediambiental de l'entitat.

320. R1: Productes certificats. S'han de triar productes certificats conforme al que s'estableix en [op.pl.5].

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.7.10 – Suports d'emmagatzematge<br>- A.7.14 – Eliminació o reutilització segura dels equips<br>- A.8.10 – Eliminació d'informació |
| NIST SP 800-53 rev. 4 | - [MP-6] Media Sanitization<br>- [MP-8] Media Downgrading |
| Altres referències | - NIST SP 800-88 - Guidelines for Media Sanitization<br>- DoD 5220 Block Erase |

Recomanacions (preses de NIST SP 800-88):

| Medi | Procediment | |
|---|---|---|
| Paper<br>Microfilm | Destruir | Trituradora a tires o quadres: 2mm |
| Mòbils<br>PDAs | Esborrar manualment | Agenda<br>Missatges<br>Trucades<br>Reiniciar a la configuració de fàbrica<br>Copies al núvol |
| Routers | Esborrar manualment | Taules d'encaminament<br>Registres d'activitat<br>Comptes d'administració<br>Reiniciar a la configuració de fàbrica |
| Impressores<br>Fax | Esborrar manualment | Reiniciar a la configuració de fàbrica |
| Discs regravables | Reescriure | Reescriure 3 vegades: amb zeros, amb uns, amb dades aleatòries |
| Discs de només lectura | Destruir | Trituradora: 5mm |
| Discs virtuals xifrats | A més de l'anterior | Destruir les claus |

Taula 4: Recomanacions NIST SP 800-88 per eliminar i destrucció

## 7.14 [MP.SW] PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES

### 7.14.2 [MP.SW.1] DESENVOLUPAMENT D'APLICACIONS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits + R1+R2+R3+R4 |

321. El desenvolupament d'aplicacions es realitzarà sobre un sistema diferent i separat del de producció, no havent d'existir eines o dades de desenvolupament a al voltant de producció. Veure [op.acc.3] sobre segregació de funcions. Perquè la segregació sigui creïble, s'han de separar els entorns i controlar els mecanismes d'identificació, autenticació i control d'accés dels usuaris diferenciant rigorosament els privilegis de cadascun.

322. La metodologia de desenvolupament convé que sigui un estàndard reconegut que inclogui la seguretat com a part integral del desenvolupament (per exemple, METRICA, Security Development Lifecycle, Correctness by Construction, Building Security In Maturity Model, OWASP, etc.). És a dir, des de la concepció arquitectònica cal plantejar els requisits de seguretat del sistema final i anar optant per solucions que introdueixin els controls necessaris en el programari desenvolupat.

323. Cal evitar que es desenvolupi pensant únicament en la funcionalitat i que els requisits de seguretat s'afegeixin posteriorment posant pegats.

324. Desenvolupament integral significa que les funcions de seguretat són part de la interfície d'usuari, que els registres d'activitat i incidències són part de l'arquitectura de registre i que existeixen mecanismes de validació, protecció de la informació i verificació que es respecta la política de seguretat desitjada.

325. Durant les proves de desenvolupament i d'acceptació no s'usaran dades de prova reals, sinó dades específiques per a proves. Quan les dades de prova procedeixin de dades reals, es manipularan perquè no es puguin reconèixer dades reals en les proves. Si no hi ha altre remei, si fos inevitable usar dades reals, es protegiran com si estiguessin en producció. Finalment, les dades de prova han de retirar-se quan el sistema passa a producció.

326. La inspecció del codi font ha de ser possible tant durant el desenvolupament com durant la vida útil del programari. Inspeccionar tot el codi és costós i probablement injustificat en els sistemes de suport a l'ENS-AD; però és necessari accedir al codi font per a analitzar incidents i per a planificar proves de penetració. Per això ha d'estar disponible amb les degudes garanties de control d'accés.

327. En tot cas cal revisar fallades típiques de programació que puguin derivar en problemes de seguretat:

    - desbordament de buffers,
    - informació residual en emmagatzematge temporal (RAM, fitxers en disc, dades en la xarxa, dades en el núvol…),
    - emmagatzematge de claus i material criptogràfic,
    - validació de les dades d'entrada, d'usuaris i entre processos,
    - validació de la configuració,
    - possibilitats d'injecció de codi,
    - possibles *race conditions* (carreres de concurrència),
    - escalat de privilegis,
    - comunicacions sense autenticar i/o sense xifrar,
    - etc.

328. S'inclouen normes de programació segura. Es recomana adoptar solucions automatitzades d'anàlisis de codi estàtic que permetin verificar davant cada nova versió que no és publicada amb errors de programació coneguts.

329. R1: Mínim privilegi. Les aplicacions es desenvoluparan respectant el principi de mínim privilegi, accedint únicament als recursos imprescindibles per a la seva funció.

330. R2: Metodologia de desenvolupament segur. S'aplicarà una metodologia que tindrà en consideració els aspectes de seguretat al llarg del cicle de vida. Inclourà normes de programació segura. Tractarà específicament les dades utilitzades en proves i permetrà la inspecció del codi font.

331. R3: Seguretat des del disseny. El disseny ha de comptar amb els següents elements. Mecanismes d'identificació i autenticació. Els mecanismes de protecció de la informació tractada i la generació i tractament de pistes d'auditoria.

332. R4: Dades de proves. Preferiblement, les proves prèvies a la implantació o modificació dels sistemes d'informació no es realitzaran amb dades reals.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.4 – Accés al codi font<br>- A.8.25 – Seguretat en el cicle de vida del desenvolupament<br>- A.8.26 – Requisits de seguretat en les aplicacions<br>- A.8.27 – Arquitectura segura de sistemes i principis d'enginyeria<br>- A.8.28 – Codificació segura<br>- A.8.30 – Externalització del desenvolupament<br>- A.8.33 – Dades de prova |
| NIST SP 800-53 rev. 4 | - [CM-4] (1) Security Impact Analysis - Separate Test Environments<br>- [SA-3] System Development Life Cycle<br>- [SA-4] Acquisition Process<br>- [SA-8] Security Engineering Principles<br>- [SA-10] Developer Configuration Management<br>- [SA-11] Developer Security Testing and Evaluation<br>- [SA-12] Supply Chain Protections<br>- [SA-15] Development Process, Standards, and Tools<br>- [SA-17] Developer Security Architecture and Design |
| Altres referències | - SANS<br>- http://www.sans.org/curricula/secure-software-development<br>- Mètrica v3 - Metodologia de Planificació, Desenvolupament i Manteniment de sistemes d'informació, Ministeri d'Administracions Públiques, Consell Superior d'Administració Electrònica<br>- NIST SP 800-64 - Security Considerations in the System Development Life Cycle |

### 7.14.3 [MP.SW.2] ACCEPTACIÓ I POSADA EN SERVEI

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

333. Es duen a terme proves estàndard d'acceptació perquè un nou programari s'integri en un procés, ja sigui un programari desenvolupat en la mateixa entitat o adquirit. Això inclou verificar que se satisfan els requisits de seguretat, que hi ha mecanismes que detecten i registren les fallades reals o sospites de violació de la seguretat i que estan preparats els procediments de gestió d'incidents.

334. Les proves han de fer-se en un entorn separat per a no causar problemes a la producció, ni alterant dades, ni obrint bretxes de seguretat per defectes de convivència. És convenient utilitzar un entorn de preproducció (encara que podrà fer-se servir excepcionalment per a les proves, un equip de l'entorn de producció que estigui degudament aïllat) i asseguri el nivell de seguretat adequat a les dades utilitzades.

335. Les proves d'acceptació es realitzaran amb dades fictícies o dissociades, evitant l'ús de dades reals sempre que sigui possible, tret que s'asseguri el nivell de seguretat adequat a les dades utilitzades.

336. L'anàlisi de vulnerabilitats constarà de 3 fases:

- Revisió exhaustiva dels components del programari, centrant-se en la seva superfície d'interacció amb els usuaris amb serveis de suport i amb altres programes.
- Hauria de verificar-se que el sistema no inclou versions de llibreries amb vulnerabilitats conegudes.
- Anàlisi de possibles vulnerabilitats en els elements identificats en el primer pas i estimació de l'impacte potencial que suposaria un incident.
- Proves de penetració per a cerciorar-se de si la vulnerabilitat és utilitzable, prioritzant aquells punts de més impacte potencial

337. Han de fer-se proves simulant usuaris externs i usuaris interns, en funció dels qui sigui accessible el programari.

338. R1: Proves. Les proves s'han de realitzar en un entorn aïllat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.19 – Instal·lació del software en sistemes de producció<br>- A.8.26 – Requisits de seguretat en les aplicacions<br>- A.8.29 – Proves de seguretat en desenvolupament i acceptació |

| | |
|---|---|
| | - A.8.30 – Externalització del desenvolupament<br>- A.8.31 – Separació dels entorns de desenvolupament, prova i producció<br>- A.8.33 – Dades de prova |

## 7.15 [MP.INFO] PROTECCIÓ DE LA INFORMACIÓ

### 7.15.2 [MP.INFO.1] DADES DE CARÀCTER PERSONAL

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

339. És obligatori el compliment de la regulació de protecció d'informació personal que estigui vigent, ja siguin les mesures de protecció determinades per a cada nivell o les especificacions del Reglament General de Protecció de Dades.

340. En aquest context, s'entén que la proposta presentada pretén que el tractament de dades es pugui fer sota la condició de l'article 6.1.c. i 6.1.e de la LQPD: c) El tractament és necessari per a complir una obligació legal aplicable al responsable del tractament; e) El tractament és necessari per a complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.

341. Les dades d'objecte de tractament seran l'adreça IP assignada en el moment del fet o durant un període temporal determinat; la identitat del titular del servei associat persona física o jurídica a l'adreça IP; les dades de contacte del titular del servei o de l'administrador del sistema afectat, en cas d'entitats corporatives o organitzacions; les dades tècniques necessàries per determinar l'origen de l'incident i la seva afectació, sempre respectant el principi de proporcionalitat.

342. La finalitat serà únicament i exclusivament la de detectar, notificar i donar resposta a incidents de ciberseguretat.

343. Des de l'Agència es considera que la finalitat descrita és massa genèrica i hauria de definir de forma més precisa i concreta què es farà amb les dades recollides.

344. Recordem que l'article 6.2 de la LQPD estipula el següent:

"2. La base del tractament esmentat a les lletres c) i e) de l'apartat anterior ha de ser establerta per la normativa que resulti d'aplicació al responsable del tractament. La finalitat del tractament s'ha de determinar en aquesta base jurídica o bé, pel que fa al tractament a què es refereix la lletra e) de l'apartat 1, ha de ser necessària per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.

345. La base jurídica pot contenir disposicions específiques per adaptar l'aplicació de les normes d'aquesta Llei, entre les quals: les condicions generals que regeixen la licitud del tractament efectuat pel responsable; els tipus de dades objecte de tractament; les persones interessades afectades; les entitats a les quals es poden comunicar dades

personals i les finalitats d'aquesta comunicació; la limitació de la finalitat; els terminis de conservació de les dades, així com les operacions i els procediments del tractament, incloses les mesures per garantir un tractament lícit i equitatiu, com les relatives a altres situacions específiques de tractament. La base jurídica ha de complir un objectiu d'interès públic i ha de ser proporcional a la finalitat legítima perseguida."

346. Igualment, cal recordar la definició establerta a l'article 4.1 de la LQPD:

«Dades personals o de caràcter personal: tota informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus relativa a una persona física identificada o identificable ("persona interessada"); s'entén per persona física identificable qualsevol persona amb una identitat que es pugui determinar, directament o indirectament, en particular mitjançant un identificador, o un o diversos elements específics, característics de la seva identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social.»

347. En aquest sentit, es considera que, per exemple, una adreça IP s'ha de considerar com una dada personal.

348. Així mateix, la base jurídica ha de:

- Contenir disposicions específiques relatives a les condicions generals que regeixen la licitud del tractament.
- Especificar els tipus de dades objecte de tractament, les persones interessades afectades i les entitats a les quals es poden comunicar dades personals.
- Determinar clarament la limitació de la finalitat, els terminis de conservació de les dades i les mesures de seguretat aplicables.
- Complir un objectiu d'interès públic i ser proporcional a la finalitat legítima perseguida.

349. En conseqüència, s'aconsella que es concreti i detalli amb més precisió la finalitat exacta del tractament (per exemple, establint si les dades només es conservaran durant el temps necessari per a la gestió i resolució de l'incident, si es procedeix a la seva anonimització posterior, quin serà el cicle de vida de les dades, etc.). Les dades s'analitzaran? Es recolliran estadístiques? Només es notificarà als afectats? Es comunicaran a les autoritats? A quines? Es farà un registre intern? Cadascuna de les finalitats hauria d'estar determinada en la norma, i el seu tractament s'hauria d'encabir en l'article 6.1.c i 6.1.e de la LQPD. També caldria definir quin serà el tractament posterior d'aquestes dades, es conservaran? Durant quant de temps? Seran anonimitzades?

350. Amb tot, es recomana descriure de manera detallada les operacions específiques que es duran a terme amb les dades recollides (anàlisi, notificació, comunicació a tercers autoritzats, etc.), així com establir clarament el període de conservació i el destí final de les dades (eliminació o anonimització un cop assolit l'objectiu).

351. Caldria establir un termini concret de conservació de les dades personals recollides o definir criteris clars que en permetin determinar la supressió, en compliment del principi de limitació de la conservació.

352. Que es reguli, mitjançant normativa específica o convenis, el procediment d'accés, ús, conservació i, si escau, comunicació de les dades obtingudes.

353. Que es garanteixin mesures adequades de protecció de les dades personals i es respecti el principi de minimització de dades, limitant el tractament només a aquelles dades estrictament necessàries per a la finalitat prevista.

354. També seria recomanable incloure una menció explícita a les mesures de seguretat que es preveuen per garantir la confidencialitat, integritat i disponibilitat de les dades personals tractades, així com el registre d'accessos i d'actuacions sobre aquestes dades.

355. Així mateix, es vol assenyalar que no es considera recomanable que en la redacció d'aquesta norma es facin referències directes a articles concrets de la LQPD, atès que la legislació pot ser modificada en el futur. Una referència tan específica podria deixar desfasada automàticament la norma interna o crear incoherències jurídiques en cas de modificació, derogació o enumeració dels articles citats. Per aquest motiu, es recomana fer una referència genèrica a "la legislació vigent en matèria de protecció de dades" o, si s'escau, al "compliment de les bases legals aplicables" en termes generals, evitant citar articles numèrics concrets.

356. Pel que fa a l'objecte i àmbit d'aplicació, caldria afegir les definicions per tal de trobar un terreny comú, en especial pels termes «integritat digital», «seguretat nacional», «seguretat de les entitats» i «seguretat i estabilitat de la xarxa de telecomunicacions».

357. En relació amb les facultats del CSIRT-AD per a la identificació d'afectats, per tal que les dades personals estiguin protegides de la millor manera possible, es considera que s'haurien de respectar tots els principis de protecció de dades regulats a l'article 5 de la LQPD, i no només el «principi de proporcionalitat».

358. Finalment, cal recordar que tot i que la informació es trobarà recollida a la normativa, l'ANC-AND ha de disposar del Registre d'Activitats de Tractament relatiu a aquest tractament de dades, així com de la informació mínima establerta als articles 16 i 17 de la LQPD.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.34 – Privacitat i protecció de dades de caràcter personal (DCP)<br>- A.7.4 – Monitorització de la seguretat física<br>- A.8.11 – Emmascarament de dades |
| Referències | - Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades |

| | |
|---|---|
| | - Llei qualificada de protecció de dades d'Andorra (LQPD)29/2021 de 28 d'octubre<br>- ENS-AD |

### 7.15.3 [MP.INFO.2] QUALIFICACIÓ DE LA INFORMACIÓ

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

359. S'ha d'establir un esquema per a assignar un nivell de qualificació a la informació, en funció de les seves necessitats de confidencialitat.

360. El sistema de qualificació:

- ha de ser conforme amb altres sistemes de qualificació propis de l'entorn en el qual desenvolupa la seva activitat l'entitat;
- ha de ser conforme amb l'indicat en l'ENS-AD sobre qualificació de la informació i categorització dels sistemes d'informació;
- i ha d'establir les responsabilitats per a adscriure inicialment una certa informació a una certa qualificació i per a possibles requalificacions posteriors (nivells de seguretat) i determinar el responsable de la documentació i aprovació formal.

361. S'han de desenvolupar procediments d'ús de la informació per a cada nivell (etiquetatge i tractament), cobrint almenys els següents aspectes:

- Com es controla l'accés, és a dir, normativa, i procediments d'autorització i mecanismes de control [op.acc]
- Com es realitza l'emmagatzematge (local, en el núvol, xifratge, etc.) [mp.si.2] i [mp.si.3]
- Normativa relativa a la realització de còpies en diferents mitjans: procés d'autorització i mecanismes de control [mp.info.9]
- Com es marquen els documents (etiquetatge de suports) [mp.si.1]
- Condicions d'adquisició, inventari, marcat, ús, esborrat i destrucció dels suports d'informació
- Com es gestiona el paper imprès i qui i on pot imprimir
- Transport físic: condicions sobre el mitjà de transport, del missatger, autoritzacions de sortida i controls de recepció
- Condicions de seguretat sobre el canal de comunicacions (especialment, autenticació i xifratge) i autoritzacions necessàries per a poder transmetre per xarxes de comunicacions [mp.com]

362. Cal esperar que les entitats organitzin la informació. Seguint aquest esquema, es poden desenvolupar taules com la següent:

| Nivell exigit ENS-AD | |
|---|---|
| Autoritzar d'accés [org.4] | • accessible a tot el personal propi |

| | |
|---|---|
| | • accessible als que el necessiten conèixer per les seves funcions |
| Copies impreses [mp.si] | • marcades<br>• cada persona s'encarrega de la seva destrucció quan ja no fa falta<br>• marcades<br>• destrucció fent servir destructora |
| Suports electrònics d'informació [mp.si] | • etiquetats<br>• és borra el contingut o s'inhabilita<br>• etiquetats<br>• es xifra el contingut<br>• es fa servir software d'esborrat segur o es destrueix |
| Ús en equips portàtils i PDAs [mp.info.3] [mp.eq.3] | • con control d'accés<br>• con control d'accés |
| Transmissió telemàtica [mp.com.2] [mp.com.3] | • canals autenticats<br>• canals autenticats i xifrats |

Taula 5: Exemple de criteris d'ús d'acord amb la qualificació de la informació segons categoria del sistema

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| Referències | - 5.12 – Classificació de la informació |

### 7.15.4 [MP.INFO.3] SIGNATURA ELECTRÒNICA

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 + R2+ R3 |

363. Totes les activitats relacionades amb la signatura electrònica i el segellament de temps han de regir-se per un marc tècnic i procedimental aprovat formalment. Se sol denominar Política de Signatura.

364. En el cas que s'utilitzin altres mecanismes de signatura electrònica subjectes a dret, el sistema ha d'incorporar mesures compensatòries suficients que ofereixin garanties equivalents o superiors quant a prevenció del repudi.

**Política de signatura electrònica**

365. En tots els casos ha de cobrir els següents punts tècnics i procedimentals:

- Delimitació de l'àmbit d'aplicació; és a dir, quina informació anirà signada i en quins processos o procediments se signarà i es verificarà cada signatura
- Els rols i funcions del personal involucrat en la generació i verificació de signatures

- Els rols i funcions del personal involucrat en la generació, renovació, revocació, custòdia i distribució de claus i certificats
- Directrius i normes tècniques aplicables a la utilització de certificats i signatures electròniques

**Codi segur de verificació**

366. Es tracta d'una forma alternativa d'assegurar l'autenticitat i integritat de la informació proporcionada per l'entitat.
367. En lloc de protegir la informació per mitjà d'una signatura inviolable, el que es proporciona és una forma còmoda de verificar que la informació és autèntica i no s'ha modificat (és íntegra).
368. S'utilitzen els formats establerts per la normativa per a assegurar la validesa de la signatura (sense perjudici que es pugui ampliar el període): verificació de la validesa del certificat i aportació de proves addicionals de validesa (com ara consultes OCSP, CRL, etc.).
369. S'adjunta a la signatura, o es referència, tota la informació pertinent per a la seva verificació i validació: certificats i dades de verificació i validació.
370. Es protegeixen la signatura, el certificat i les dades de verificació i validació amb un segell de temps.
371. R1: Certificats qualificats: Quan s'utilitzin sistemes de firma electrònica avançada basats en certificats, aquests han d'estar qualificats.
372. R2: Algoritmes i paràmetres autoritzats. Es faran servir algoritmes i paràmetres autoritzats degudament.
373. R3: Verificació i validació de firma. Es garantirà quan sigui necessari la verificació i validació de la firma electrònica durant el temps requerit per l'activitat administrativa que suporti.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.31 – Identificació de requisits legals, reglamentaris i contractuals<br>- A.8.24 – Ús de la criptografia |
| NIST 800-53 rev. 4 | - [SC-13] Cryptographic Protection<br>- [SC-28] Protection of Information at Rest |
| Altres referències | - NIST SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications |

### 7.15.5 [MP.INFO.4] SEGELLS DE TEMPS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

374. Els segells de temps prevenen la possibilitat d'un repudi posterior de la informació que sigui susceptible de ser utilitzada com a evidència en el futur, o que requereixi capacitat probatòria segons la llei de procediment administratiu. Per això, totes les activitats relacionades amb la signatura electrònica i el segell de temps han de regir-se per un marc tècnic i procedimental aprovat formalment. Se sol denominar Política de Signatura.

375. Ha d'identificar-se i establir-se el temps de retenció de la informació.

376. Es daten electrònicament els documents la data i l'hora d'entrada dels quals ha d'acreditar-se fefaentment.

377. Es daten electrònicament els documents la data i l'hora de sortida dels quals ha d'acreditar-se fefaentment.

378. Es daten electrònicament les signatures la validesa de les quals hagi d'estendre's per llargs períodes o així ho exigeixi la normativa aplicable, fins que la informació protegida ja no sigui requerida pel procés administratiu al qual dona suport; alternativament es poden utilitzar formats de signatura avançada que incloguin datat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27001:2022 | - A.8.26 – Requisits de seguretat en les aplicacions |
| NIST SP 800-53 rev. 4 | - [AU-10] Non-repudiation |
| Altres referències | - ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 1: Framework<br>- ISO/IEC 18014-2:2009 Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens<br>- ISO/IEC 18014-3:2009 Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens<br>- ISO/IEC TR 29149:2012 Information technology – Security techniques – Best practices for the provision and use of time-stamping services |

| | |
|---|---|
| | - RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) |

### 7.15.6 [MP.INFO.5] NETEJA DE DOCUMENTS

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

379. S'ha de retirar dels documents que seran transferits a un àmbit fora del domini de seguretat de l'entitat, tota la informació addicional continguda en camps ocults, meta-dades, comentaris, revisions anteriors, etc. excepte quan aquesta informació sigui pertinent per al receptor del document.

380. Aquesta mesura és especialment rellevant quan el document es difon àmpliament, com succeeix quan s'ofereix al públic en un servidor web o un altre tipus de repositoris interns / externs d'informació.

381. L'incompliment d'aquesta mesura pot perjudicar:

- al manteniment de la confidencialitat d'informació que no hauria d'haver-se revelat al receptor del document;
- al manteniment de la confidencialitat de les fonts o orígens de la informació, que no ha de conèixer el receptor del document;
- i a la bona imatge de l'entitat que difon el document, ja que demostra un descuit en el seu bon fer.

### 7.15.7 [MP.INFO.6] CÒPIES DE SEGURETAT (BACKUP)

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits + R1 |

382. S'han de realitzar còpies de seguretat que permetin recuperar dades perdudes accidentalment o intencionadament amb una antiguitat a determinar per l'entitat.

383. Les còpies de seguretat posseiran el mateix nivell de seguretat que les dades originals pel que fa a integritat, confidencialitat, autenticitat i traçabilitat. En particular, ha de considerar-se la conveniència o necessitat que les còpies de seguretat estiguin xifrades per a garantir la confidencialitat (i en aquest cas s'estarà al que es disposa en [op.exp.11]).

384. Es recomana establir un procés d'autorització per a la recuperació d'informació de les còpies de seguretat.

385. Es recomana conservar les còpies de seguretat en lloc(s) prou independent(s) de la ubicació normal de la informació en explotació com perquè els incidents previstos en l'anàlisi de riscos no es donin simultàniament en tots dos llocs, per exemple, si es conserven en la mateixa sala utilitzar un armari ignífug.

386. El transport de còpies de seguretat des del lloc on es produeixen fins al seu lloc d'emmagatzematge garanteix les mateixes seguretats que els controls d'accés a la informació original.

387. Les còpies de seguretat han d'abastar:

- informació de treball de l'entitat
- aplicacions en explotació, incloent-hi els sistemes operatius
- dades de configuració, serveis, aplicacions, equips, etc.
- claus utilitzades per a preservar la confidencialitat de la informació

388. Per als punts anteriors veure [op.exp] i [mp.info.3].

389. El responsable de la informació ha de determinar la freqüència amb la qual han de realitzar-se les còpies i el període de retenció durant el qual mantenir-les.

390. En cas de disposar d'un Pla de Continuïtat, les còpies de seguretat hauran de realitzar-se amb una freqüència que permeti complir amb el RPO i amb un objectiu de temps de restauració que permeti complir el RTO.

391. R1: proves de recuperació. Els procediments de còpia de seguretat i restauració han de provar-se regularment. La seva freqüència dependrà de la criticitat de les dades i de l'impacte que causi la falta de disponibilitat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.13 – Còpies de seguretat de la informació |
| NIST 800-53 rev. 4 | - [CP-6] Alternate Storage Site<br>- [CP-9] Information System Backup<br>- [CP-10] Information System Recovery and Reconstitution |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>o CSC.10 - Data Recovery Capability |

## 7.16 [MP.S] PROTECCIÓ DELS SERVEIS

### 7.16.2 [MP.S.1] PROTECCIÓ DEL CORREU ELECTRÒNIC (E-MAIL)

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

392. Quan s'ofereixi correu electrònic com a part del sistema, haurà de protegir-se enfront de les amenaces que li són pròpies mitjançant:

- Protecció del cos dels missatges i documents adjunts que pugui contenir el correu electrònic

- Protecció de l'encaminament de missatges (per exemple, protegint el servidor DNS i la seva configuració) i de l'establiment de les connexions (impedint que l'usuari final pugui connectar-se a un servidor de correu que no sigui el corporatiu)
- Protecció de l'entitat enfront de correus no sol·licitats (spam), virus, cucs, troians, programes espies (spyware) i codi mòbil tipus miniaplicació (per exemple, amb la instal·lació d'un antivirus, sigui en el servidor de correu oen el lloc d'usuari)
- Limitació de l'ús del correu electrònic a l'estrictament professional i conscienciació i formació relatives a l'ús adequat del mateix

393. També s'han de contemplar els següents elements:

- Filtrat i motor de regles configurables de manera independent per al correu entrant i sortint.
- Haurà d'incloure una solució antispam, antimalware/antivirus, etc., i comptar amb múltiples motors antivirus
- Els motors antivirus hauran de ser reconeguts i amb bona reputació, i estar sempre actualitzats amb les darreres firmes
- Capacitat per analitzar URLs dins dels correus, tant directes com escurçades, i poder configurar que no siguin clicables per l'usuari final en rebre el correu.
- Integració possible amb sistemes de correu al núvol, com Office 365.
- Funcionalitat de quarantena separada per a cada entitat, on es pugui conservar el correu sospitós de spam durant un mínim de 3 mesos.
- Possibilitat d'enviar notificacions als usuaris finals informant-los sobre correus retinguts a la quarantena, tant de forma individual com mitjançant informes resumits.
- L'administrador de cada domini podrà definir els criteris de notificació, decidint si s'informa o no els destinataris sobre correus maliciosos.
- Opció de personalitzar, per entitat, el contingut dels avisos que es fan arribar als usuaris.
- Possibilitat de definir polítiques d'excepcions específiques per entitat, com desactivar o activar el filtre antivirus per a dominis concrets, amb un alt nivell de detall en la configuració.
- El sistema haurà d'utilitzar diverses llistes de reputació (RBLs), com a mínim una d'elles de tipus comercial o de pagament, i compatibilitat amb protocols de seguretat de correu com SPF, greylisting, DMARC, DKIM, entre d'altres, inclòs el filtratge antispoofing.
- Funcionalitat d'anàlisi de fitxers adjunts en sandbox, amb capacitat d'integració amb sandboxes independents.
- Possibilitat d'emmagatzematge xifrat dels correus.
- S'inclouran prou llicències per permetre el xifratge dels correus de tots els usuaris de les entitats.
- Possibilitat de definir llistes blanques i negres per domini o grups de dominis.
- Es podrà utilitzar expressions regulars en els filtres.
- Capacitat d'implementar algoritmes d'aprenentatge automàtic en el procés de filtratge.

- Garantia d'eliminació del 99% del correu brossa.
- Haurà de protegir tots els dominis de les entitats participants de manera independent i sense límit en el nombre de polítiques o dominis per entitat.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.14 – Transferència de la informació |
| NIST 800-53 rev. 4 | - [SI-8] Spam Protection |
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>○ CSC.7 - Email and Web Browser Protections<br>- NIST SP 800-45 – Guidelines on Electronic Mail Security |

### 7.16.3 [MP.S.2] PROTECCIÓ DE SERVEIS I APLICACIONS WEB

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits + [R1 o R2] | Requisits + [R1 o R2] |

394. S'ha de protegir els subsistemes dedicats a la publicació d'informació enfront dels atacs o amenaces que els són pròpies.

395. Una sèrie de mesures són preventives, posant l'èmfasi en els processos de:

- Desenvolupament d'aplicacions i serveis (mp.sw),
- Configuració de seguretat (op.exp.2 i op.exp.3),
- En els controls de manteniment (op.exp.4) i
- En les proteccions de separació de tasques (op.acc.3)

396. Les tasques preventives no excusen d'un sistema de monitoratge i reacció enfront d'atacs exitosos.

397. Poden presentar-se atacs a nivell de xarxa, a nivell del sistema operatiu del servidor i a nivell de l'aplicació que atén peticions web. De les dues primeres maneres d'atac ens defensarem protegint l'equip de frontera.

398. Bàsicament, hi ha 2 maneres de protegir el servidor frontal: protegint l'equip i el programari que proporciona la interfície per a accés al servei web, o disposant una protecció prèvia en forma de tallafocs d'aplicació (appliance) entre el servidor i els usuaris.

399. Els atacs a nivell d'aplicació poden detectar-se en el servidor frontal o en algun servidor de suport en la rereguarda; és a dir, pot haver-hi atacs que apareixen com a correctes (sintàcticament correctes) però que causen problemes pel tipus de petició o per la seqüència de peticions (semàntica incorrecta). Per als atacs que entren en el nivell intern serà necessari desenvolupar regles específiques per a detectar i reaccionar. Regles de tipus:

- límit en el nombre de sessions, total o per usuari anònim o identificat
- tancament de sessions al cap d'un temps
- límit en el volum de dades (individual i agregat)

400. Per a verificar que en el procés de desenvolupament de l'aplicació s'han establert els controls enfront d'atacs potencials s'han d'identificar possibles vulnerabilitats a corregir. Per a això es poden realitzar auditories de seguretat periòdiques o proves de penetració (hacking ètic) dels serveis i aplicacions web per a posteriorment modificar l'aplicatiu o establir elements que el protegeixin almenys enfront de:

- Atacs que evitin el control d'accés obviant l'autenticació, si n'hi hagués, mitjançant accessos per vies alternatives al protocol predefinit (per exemple, HTTP i HTTPS, manipulacions d'URL o cookies o atacs d'injecció de codi (com introduir caràcters no autoritzats per l'aplicació).
- Atacs d'escalat de privilegis (com executar accions fent-se passar per un altre usuari).
- Atacs de Cross Site Scripting (XSS) que permeten robar informació delicada, segrestar sessions d'usuari o comprometre la integritat del sistema (introduint informació en la pàgina web que es mostri així posteriorment a l'usuari, per exemple)
- Atacs de manipulació de proxies i caché, en cas d'utilitzar aquestes tecnologies.

401. R1: Auditories de seguretat.
    - Es realitzaran auditories contínues de seguretat de «caixa negra» sobre les aplicacions web durant la fase de desenvolupament i abans de la fase de producció.
    - La freqüència d'aquestes auditories de seguretat quedarà definida en el procediment d'auditoria.

402. R2: Auditories de seguretat avançada.
    - Es realitzaran auditories de seguretat de «caixa blanca» sobre les aplicacions web durant la fase de desenvolupament.
    - S'empraran metodologies definides i eines automàtiques de detecció de vulnerabilitats en la realització de les auditories de seguretat sobre les aplicacions web.
    - Una vegada finalitzada una auditoria de seguretat, s'analitzaran els resultats i se solucionaran les vulnerabilitats trobades mitjançant els procediments definits [op.exp.5].

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.5.35 – Revisió independent de la seguretat de la informació<br>- A.8.26 – Requisits de seguretat de les aplicacions<br>- A.8.34 – Protecció dels sistemes d'informació durant les proves d'auditoria |

| | |
|---|---|
| Altres referències | - SANS - CIS Critical Security Controls - Version 6.1<br>  ○ CSC.7 - Email and Web Browser Protections<br>- NIST SP 800-44 - Guidelines on Securing Public Web Servers<br>- PCI-DSS v3.0<br>  ○ Requisit 6: Desenvolupi i mantingui sistemes i aplicacions segures |

### 7.16.4 [MP.S.3] PROTECCIÓ DE LA NAVEGACIÓ DE WEB

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | Requisits | Requisits |

403. L'accés dels usuaris interns a la navegació per internet es protegirà enfront de les amenaces que li són pròpies, actuant del següent mode:
404. S'establirà una normativa d'utilització, definint l'ús que s'autoritza i les limitacions d'ús personal. En particular, es concretarà l'ús permès de connexions xifrades.
405. Es duran a terme regularment activitats de conscienciació sobre higiene en la navegació web, fomentant l'ús segur i alertant d'usos incorrectes.
406. Es formarà al personal encarregat de l'administració del sistema en monitoratge del servei i resposta a incidents.
407. Es protegirà la informació de resolució d'adreces web i d'establiment de connexions.
408. Es protegirà l'organització en general i al lloc de treball en particular enfront de problemes que es materialitzen via navegació web.
409. Es protegirà contra l'actuació de programes nocius com ara pàgines actives, descàrregues de codi executable, etc., prevenint l'exposició del sistema a vectors d'atac del tipus spyware, ransomware, etc.
410. S'establirà una política executiva de control de cookies, en particular, per a evitar la contaminació entre ús personal i ús organitzatiu.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.23 – Filtrat Web |

### 7.16.5 [MP.S.4] PROTECCIÓ ENFRONT DE LA DENEGACIÓ DE SERVEI

| Categoria | Bàsica | Mitjana |
|---|---|---|
| | N.A. | Requisits |

411. S'han d'establir mesures preventives i reactives enfront d'atacs de denegació de servei (DoS) i denegació de servei distribuït (DDoS).

412. Els atacs de denegació de servei poden prevenir-se dimensionant amb folgança els elements susceptibles de ser atacats des de l'exterior, encara que poc es pot fer front a un atac amb prou recursos per part de l'atacant.

413. Múltiples atacs de denegació de servei són a causa d'un programari deficient per part d'alguns serveis o deficiències de hardware, bé perquè no s'han actualitzat les versions, bé perquè la configuració no és la correcta. Tots dos aspectes hauran de ser analitzats i reparats (veure mesures de protecció [mp.exp] quant a configuració, manteniment i canvis), de manera que s'actualitzin i es fortifiquin les tecnologies utilitzades de cara a prevenir atacs coneguts.

414. Fins i tot estant preparats, podem ser víctimes d'un nou tipus d'atac imprevist, i en aquest cas cal detectar-ho ràpidament i gestionar la incidència.

415. Els atacs de denegació de servei poden ser detectats i afrontats en el perímetre ([mp.com.1]), encara que poden requerir la intervenció d'altres elements. En el perímetre es poden detectar patrons sospitosos de comportament: allaus de peticions, peticions trucades i, en general, un ús maliciós dels protocols de comunicacions. Algunes d'aquestes peticions poden ser denegades directament per l'equip perimetral, en altres ocasions cal reaccionar davant ells i aixecar una alarma per a actuar on correspongui (servidors web, servidors de bases de dades…, i contactant amb el proveïdor de comunicacions o els centres de resposta a incidents, CERT. Per tant, és important disposar d'un procediment documentat que indiqui el procediment de reacció davant els atacs.

416. És responsabilitat de l'organisme detectar i bloquejar l'ús deliberat o accidental del mateix sistema d'informació per a atacar a tercers des de les mateixes instal·lacions. Notis que l'organisme pot ser simplement víctima d'una infecció nociva d'elements agressius que són llançats contra uns altres o d'un atac deliberat per part d'un empleat intern i al proveïdor de comunicacions o al centre de resposta d'emergència (CERT) per a coordinar la resposta.

417. Com a possibles tecnologies a utilitzar per a prevenir atacs es troben els sistemes de detecció d'intrusos (IDS), monitors amb alarmes en aconseguir un consum determinat d'amplada de banda o de sol·licitud de peticions, mecanismes per a bloquejar un nombre elevat de connexions internes concurrents o per a bloquejar l'enviament de grans quantitats d'informació, etc.

| Marc de referència | Controls d'aplicabilitat |
|---|---|
| ISO/IEC 27002:2022 | - A.8.6 – Gestió de la capacitat<br>- A.8.16 – Seguiment d'activitats |
| NIST SP 800-53 rev. 4 | - [CP-2] (2) Contingency Plan - Capacity Planning |

| | |
|---|---|
| | - [SC-5] (2) Denial of Service Protection - Excess Capacity / Bandwidth / Redundancy |

# ANNEX A. MESURES DE SEGURETAT

A continuació, es presenta la taula que mostra les diferents mesures que s'han d'aplicar o no segons categoria bàsica o mitja. També s'afegeix els reforços corresponents a la categoria mitjana.

| ID | Mesura | Per Categoria o Dimensions | Bàsica | Mitjana |
|---|---|---|---|---|
| **org** | **Marc organitzatiu** | | | |
| org.1 | Política de seguretat | Categoria | aplica | aplica |
| org.2 | Normativa de seguretat | Categoria | aplica | aplica |
| org.3 | Procediments de seguretat | Categoria | aplica | aplica |
| org.4 | Procés d'autorització | Categoria | aplica | aplica |
| **op** | **Marc operacional** | | | |
| op.pl. | Planificació | | | |
| op.pl.1 | Anàlisi de riscs | Categoria | aplica | + R1 |
| op.pl.2 | Arquitectura de Seguretat | Categoria | aplica | + R1 |
| op.pl.3 | Adquisició de nous components | Categoria | aplica | aplica |
| op.pl.4 | Dimensionament/ gestió de la capacitat | D | aplica | + R1 |
| op.pl.5 | Components certificats | Categoria | n.a. | aplica |
| op.pl.6 | Pla de seguretat | Categoria | aplica | aplica |
| op.pl.7 | Declaració d'aplicabilitat | Categoria | aplica | aplica |
| op.acc. | Control d'accés | | | |
| op.acc.1 | Identificació | TA | aplica | + R1 |
| op.acc.2 | Requisits d'accés | CITA | aplica | aplica |
| op.acc.3 | Segregació de funcions i tasques | CITA | n.a. | aplica |
| op.acc.4 | Procés de gestió de drets d'accés | CITA | aplica | aplica |
| op.acc.5 | Mecanisme d'autenticació (usuaris externs) | CITA | + [R1 o R2 o R3 o R4] | + [R2 o R3 o R4] + R5 |
| op.acc.6 | Mecanisme d'autenticació (usuaris de l'organització) | CITA | + [R1 o R2 o R3 o R4] + R8 + R9 | [R1 o R2 o R3 o R4] + R5 + R8 + R9 |

| ID | Mesura | Per Categoria o Dimensions | Bàsica | Mitjana |
|---|---|---|---|---|
| op.exp. | Explotació | | | |
| op.exp.1 | Inventari d'actius | Categoria | aplica | aplica |
| op.exp.2 | Configuració de seguretat | Categoria | aplica | aplica |
| op.exp.3 | Gestió de la configuració de seguretat | Categoria | aplica | + R1 |
| op.exp.4 | Manteniment i actualitzacions de seguretat | Categoria | aplica | + R1 |
| op.exp.5 | Gestió de canvis | Categoria | n.a. | aplica |
| op.exp.6 | Protecció enfront de codi nociu | Categoria | aplica | + R1 + R2 |
| op.exp.7 | Gestió d'incidents | Categoria | aplica | + R1 + R2 |
| op.exp.8 | Registre de l'activitat | T | aplica | + R1 + R2 + R3 + R4 |
| op.exp.9 | Registre de la gestió d'incidents | Categoria | aplica | aplica |
| op.exp.10 | Protecció de claus criptogràfiques | Categoria | aplica | + R1 |
| op.ext. | Recursos externs | | | |
| op.ext.1 | Contractació i acords de nivell de servei | Categoria | n.a. | aplica |
| op.ext.2 | Gestió diària | Categoria | n.a. | aplica |
| op.ext.3 | Interconnexió de sistemes | Categoria | n.a. | aplica |
| op.nub. | Serveis en el núvol | | | |
| op.nub.1 | Protecció de serveis en el núvol | Categoria | aplica | + R1 |
| op.cont. | Continuïtat del servei | | | |
| op.cont.1 | Anàlisi d'impacte | D | n.a. | aplica |
| op.cont.2 | Pla de continuïtat | D | n.a. | aplica |
| op.cont.3 | Proves periòdiques | D | n.a. | Aplica |
| op.cont.4 | Mitjans alternatius | D | n.a. | aplica |
| op.mon. | Monitoratge del sistema | | | |
| op.mon.1 | Detecció d'intrusió | Categoria | aplica | + R1 |
| op.mon.2 | Sistema de mètriques | Categoria | aplica | + R1 + R2 |

| ID | Mesura | Per Categoria o Dimensions | Bàsica | Mitjana |
|---|---|---|---|---|
| op.mon.3 | Vigilància | Categoria | aplica | + R1 + R2 |
| op.mon.4 | Registre d'esdeveniments | Categoria | aplica | aplica |
| **mp** | **Mesures de protecció** | | | |
| mp.if. | Protecció de les instal·lacions e infraestructures | | | |
| mp.if.1 | Àrees separades i amb control d'accés | Categoria | aplica | aplica |
| mp.if.2 | Identificació de les persones | Categoria | aplica | aplica |
| mp.if.3 | Condicionament dels locals | Categoria | aplica | aplica |
| mp.if.4 | Energia elèctrica | D | aplica | + R1 |
| mp.if.5 | Protecció enfront d'incendis | D | aplica | aplica |
| mp.if.6 | Protecció enfront d'inundacions | D | n.a. | aplica |
| mp.if.7 | Registre d'entrada i sortida d'equipament | Categoria | aplica | aplica |
| mp.per. | Gestió del personal | | | |
| mp.per.1 | Caracterització del lloc de treball | Categoria | n.a. | aplica |
| mp.per.2 | Deures i obligacions | Categoria | aplica | + R1 |
| mp.per.3 | Conscienciació | Categoria | aplica | aplica |
| mp.per.4 | Formació | Categoria | aplica | aplica |
| mp.eq. | Protecció de los equips | | | |
| mp.eq.1 | Lloc de treball buidat | Categoria | aplica | + R1 |
| mp.eq.2 | Bloqueig de lloc de treball | A | n.a. | aplica |
| mp.eq.3 | Protecció de dispositius portàtils | Categoria | aplica | aplica |
| mp.eq.4 | Altres dispositius connectats a la xarxa | C | aplica | + R1 |
| mp.com. | Protecció de les comunicacions | | | |
| mp.com.1 | Perímetre segur | Categoria | aplica | aplica |

| ID | Mesura | Per Categoria o Dimensions | Bàsica | Mitjana |
|---|---|---|---|---|
| mp.com.2 | Protecció de la confidencialitat | C | aplica | + R1 |
| mp.com.3 | Protecció de la integritat i de l'autenticitat | IA | aplica | + R1 + R2 |
| mp.com.4 | Separació de fluxos d'informació en la xarxa | Categoria | n.a. | + [R1 o R2 o R3] |
| mp.si. | Protecció dels suports d'informació | | | |
| mp.si.1 | Marcat de suports | C | n.a. | aplica |
| mp.si.2 | Criptografia | CI | n.a. | aplica |
| mp.si.3 | Custòdia | Categoria | aplica | aplica |
| mp.si.4 | Transport | Categoria | aplica | aplica |
| mp.si.5 | Esborrament i destrucció | C | aplica | + R1 |
| mp.sw. | Protecció de les aplicacions informàtiques | | | |
| mp.sw.1 | Desenvolupament d'aplicacions | Categoria | n.a. | + R1 + R2 + R3 + R4 |
| mp.sw.2 | Acceptació i posada en servei | Categoria | aplica | + R1 |
| mp.info. | Protecció de la informació | | | |
| mp.info.1 | Dades personals | Categoria | aplica | aplica |
| mp.info.2 | Qualificació de la informació | C | n.a. | aplica |
| mp.info.3 | Firma electrònica | IA | aplica | + R1 + R2 + R3 |
| mp.info.4 | Segells de temps | T | n.a. | aplica |
| mp.info.5 | Neteja de documents | C | aplica | aplica |
| mp.info.6 | Còpies de seguretat | D | aplica | + R1 |
| mp.s. | Protecció dels serveis | | | |
| mp.s.1 | Protecció del correu electrònic | Categoria | aplica | aplica |
| mp.s.2 | Protecció de serveis i aplicacions web | Categoria | + [R1 o R2] | + [R1 o R2] |
| mp.s.3 | Protecció de la navegació web | Categoria | aplica | aplica |
| mp.s.4 | Protecció contra denegació de servei | D | n.a. | aplica |

Taula 6. Mesures de seguretat segons la seva aplicabilitat

## ANNEX B. ESPECIFICACIONS TÈCNIQUES

En aquesta secció s'inclouen les especificacions tècniques relatives als controls de seguretat aplicables als usuaris, en el marc del desplegament de les mesures requerides per l'Esquema Nacional de Seguretat (ENS).
A continuació, es detalla una taula amb els **controls de seguretat d'usuaris** externs que cal implementar, incloent-hi una descripció general de cada control i els detalls específics d'aplicació. Aquests controls afecten directament la gestió d'identitats, accés, dispositius i pràctiques de conscienciació, essent claus per garantir la seguretat de l'entorn.

| CONTROLS DE SEGURETAT D'USUARIS | | |
|---|---|---|
| Nom del control | Descripció del control | Detalls |
| MFA | L'autenticació multifactor ha d'estar habilitada per a tots els usuaris. | MFA s'administra mitjançant normes d'accés condicional d'una eina de monitoratge. |
| Nomenclatura | Els noms dels comptes d'usuari han de seguir la convenció de nomenclatura de l'organització. | Utilitzeu la documentació oficial per als noms correctes |
| VPN | Els usuaris interns s'han de connectar a l'intern de l'organització mitjançant una eina segura. | |
| Formació de conscienciació en seguretat | Proporcionar als empleats formació de conscienciació sobre seguretat per ajudar-los a entendre millor el risc associat. | Bones pràctiques per a la gestió de contrasenyes, campanyes de phising, etc |
| No BYOD | Portar un dispositiu propi no està permès per als usuaris externs. | Els usuaris haurien d'utilitzar els dispositius proporcionats per l'organització. |
| Logging | Els registres dels usuaris sincronitzats a una eina de serveis al núvol i emmagatzemats. | Registres d'inici de sessió i registres d'auditoria |
| Accés | Els usuaris privilegiats s'han de revisar mitjançant revisions d'accés. | Eliminant els permisos de l'usuari, s'implementaran diferents revisions d'accés |
| Assignar responsable | S'ha d'assignar a l'usuari un responsable | El responsable ha de ser gerent, líder d'equip, etc |
| Accés VPN extern | Els usuaris externs s'han de connectar mitjançant VPN mitjançant la configuració VPN específica | Una eina per protecció de dades s'utilitza per a la connectivitat VPN |
| Grup extern | Els usuaris han de formar part d'un grup específic d'"Usuaris externs" | Creació d'un grup central per a la gestió de tots els usuaris externs |

| CONTROLS DE SEGURETAT SAAS |
|---|

| Nom del control | Descripció del control | Detalls |
|---|---|---|
| MFA | L'MFA hauria d'estar habilitada per accedir als serveis SaaS | MFA es gestiona mitjançant normes d'accés condicional |
| SSO | Habilitar l'inici de sessió únic per a SaaS | Habilitar l'inici de sessió únic per a SaaS |
| Permisos de recursos | Els empleats només haurien de tenir accés als recursos rellevants per a la seva feina | Els permisos d'usuari per accedir a determinats recursos s'han de revisar periòdicament |
| Logging | Els registres de seguretat rellevants són revisats per l'Oficina de Seguretat | Els registres estan presents en serveis com ara Defender for Cloud Apps, el Centre d'administració de l'Exchange, etc. |
| WAF | S'ha d'implementar un tallafoc d'aplicacions web (WAF) per al servei web | El producte actual del grup coordinat és DataDome (Antibot). |
| Exploracions de vulnerabilitats | Les exploracions de vulnerabilitats es realitzaran als serveis web mitjançant Tenable | Afegiu dominis web públics a les exploracions de seguretat periòdiques. |
| Acords de nivell de servei (SLA) | Acord d'SLA del proveïdor | Assegureu-vos que els SLA s'alineen amb els requisits de la vostra organització i inclouen disposicions per a incidents de seguretat i violacions de dades. |
| Accés | Els usuaris privilegiats s'han de revisar mitjançant revisions d'accés. | Eliminant els permisos de l'usuari, s'implementaran diferents revisions d'accés |
| Comptes d'administrador | Els comptes d'administrador han de complir la política de contrasenyes | Els comptes d'administrador han de complir la política de contrasenyes |
| Encriptació | Compleix els estàndards de xifratge de l'organització. | 1. Utilitzar algorismes de xifratge forts (per exemple: AES256) per protegir les dades sensibles en trànsit i en repòs (bases de dades, sistemes de fitxers, etc.)<br>2. Configureu TLS v1.2 o superior per xifrar la comunicació entre l'aplicació web i els navegadors dels usuaris. |
| Privacitat de dades | Verifiqueu si el proveïdor de SaaS obté el consentiment de l'usuari per a les activitats de recollida i processament de dades. | Verifiqueu si el proveïdor de SaaS obté el consentiment de l'usuari per a les activitats de recollida i processament de dades. |
| DR i còpies de seguretat | Garantir l'alta disponibilitat dels serveis | Verifiqueu si el proveïdor de SaaS té un pla complet de recuperació de desastres, incloses proves periòdiques i còpies de seguretat de dades fora del lloc. |

| CONTROLS DE SEGURETAT PAAS | | |
|---|---|---|
| Nom del control | Descripció del control | Detalls |

| | | |
|---|---|---|
| MFA | L'MFA hauria d'estar habilitada per accedir als serveis SaaS | MFA is managed via Conditional Access policies |
| SSO | Habilitar l'inici de sessió únic per a SaaS | Enable single sign-on for SaaS |
| Permisos de recursos | Els empleats només haurien de tenir accés als recursos rellevants per a la seva feina | User permissions to access certain resources should be reviewed periodically |
| Logging | Els registres de seguretat rellevants són revisats per l'Oficina de Seguretat | Els registres estan presents en serveis com ara Defender for Cloud Apps, el Centre d'administració de l'Exchange, etc. |
| WAF | S'ha d'implementar un tallafoc d'aplicacions web (WAF) per al servei web | El producte actual del grup coordinat és DataDome (Antibot). |
| Xarxa | Creació de regles de xarxa d'entrada i sortida. | Creació de regles de xarxa d'entrada i sortida. |
| Exploracions de vulnerabilitats | Les exploracions de vulnerabilitats es realitzaran als serveis web mitjançant Tenable | Afegir dominis web públics a les exploracions de seguretat periòdiques. |
| Acords de nivell de servei (SLA) | Acord d'SLA del proveïdor | Assegurar que els SLA s'alineen amb els requisits de la organització i inclouen disposicions per a incidents de seguretat i violacions de dades. |
| Accés | Els usuaris privilegiats s'han de revisar mitjançant revisions d'accés. | Eliminant els permisos de l'usuari, s'implementaran diferents revisions d'accés |
| Admin Accounts | Els comptes d'administrador han de complir la política de contrasenyes | Els comptes d'administrador han de complir la política de contrasenyes |
| Encriptació | Compleix els estàndards de xifratge de l'organització. | 1. Utilitzar algorismes de xifratge forts (per exemple: AES256) per protegir les dades sensibles en trànsit i en repòs (bases de dades, sistemes de fitxers, etc.)<br>2. Configurar TLS v1.2 o superior per xifrar la comunicació entre l'aplicació web i els navegadors dels usuaris. |
| Privacitat de dades | Verificar si el proveïdor de SaaS obté el consentiment de l'usuari per a les activitats de recollida i processament de dades. | Verifiqueu si el proveïdor de SaaS obté el consentiment de l'usuari per a les activitats de recollida i processament de dades. |
| DR i còpies de seguretat | Garantir l'alta disponibilitat dels serveis | Verifiqueu si el proveïdor de SaaS té un pla complet de recuperació de desastres, incloses proves periòdiques i còpies de seguretat de dades fora del lloc. |

| | | |
|---|---|---|
| Anàlisi de codi | Dur a terme anàlisis de codi per detectar possibles vulnerabilitats | Dur a terme anàlisis de codi aplicant el perfil de Sonarqube. |

| | | |
|---|---|---|
| **Estrictament prohibit:** | Està estrictament prohibit habilitar connexions RDP des d'Internet. | La política actual dicta que totes les connexions RDP s'han de dur a terme internament dins de la nostra xarxa. |

## ANNEX C. GLOSSARI

**Advanced Persistent Threats**

Amenaces Persistents Avançades.

**Bring your own device**

Porta el teu propi aparell (en anglès bring your own device (BYOD)) es refereix al mètode que permet que els empleats puguin portar els seus dispositius mòbils (portàtils, tauletes tàctils i telèfons intel·ligents) als seus llocs de treball, per tal d'utilitzar-los per accedir a la informació de l'empresa i als seus programes.

**Cookies**

Petita quantitat d'informació que se li envia al navegador del client i que permet que aquest quedi identificat en connexions successives.

**Computer Emergency Response Team**

És un centre de resposta per a incidents de seguretat en tecnologies de la informació.

**Data Loss Prevention (DLP)**

La Prevenció de la pèrdua de dades (DLP) és la pràctica de detectar i prevenir violacions de dades, exfiltració o destrucció no desitjada de dades sensibles. Les organitzacions utilitzen el DLP per protegir i assegurar les seves dades i complir amb les regulacions.

**Denial of Servicec (DoS)**

Un atac de denegació de servei, també conegut com a Atac DoS (de l'anglès denial-of-service attack) és una incursió contra la seguretat informàtica.

**Evaluaton Assurance Level (EAL)**

Nivells de confiança en l'avaluació.

**International Organization for Standardization**

Organització internacional de normalització.

**Intrusion Detection System (IDS)**

Un Sistema de Detecció d'Intrusos és un programa de detecció d'accessos no autoritzats a un computador o a una xarxa.

**Personal Digital Assistant**

Assistent digital personal o agenda electrònica de butxaca.

**Personal Identification Number**

És un número d'identificació personal utilitzat en certs sistemes, com el telèfon mòbil o el caixer automàtic, per identificar-se i obtenir accessos al sistema. És un tipus de contrasenya.

Targeta o dispositiu electrònic que fa servir un usuari autoritzat per accedir a un sistema informàtic.

**Recovery Point Objective**

Marca la freqüència de còpies de recolzament. Es refereix al volum de dades en risc de pèrdua que l'organització considera tolerable.

**Recovery Time and Point Objective**

Punt de recuperació objectiu i temps de recuperació objectiu.

**Security Information and Event Mangement (SIEM)**

Són productes i serveis de programari que combinen la gestió de la informació de seguretat. Aquests productes i serveis proporcionen anàlisis en temps real de les alertes de seguretat generades per aplicacions i maquinari de xarxa.

**Service Level Agreement**

Acord de Nivell de Servei.

**Target of Evaluation (TOE)**

Objectiu d'avaluació.

**Uniform Resource Locator (URL)**

Col·loquialment anomenat adreça web, és una referència a un recurs web que especifica la seva ubicació en una xarxa d'ordinadors i un mecanisme per recuperar-lo.

**Uninterruptible Power Supply**

Sistema d'Alimentació Ininterrompuda (SAI).

### Universal Serial Bus (USB)

És un estàndard industrial que defineix el cablejat, els connectors i el protocol de comunicacions emprat en un bus de dades per a connectar, comunicar i alimentar perifèrics des dels ordinadors.

### Wireless Fidelity (WiFi)

És una tecnologia de xarxa local sense fils que permet a un dispositiu electrònic intercanviar dades o connectar amb internet.

## ANNEX D. REFERÈNCIES

1. DSD - Australian Defence Signals Directorate (DSD)
   Top 35 Mitigation Strategies
   http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
2. ENS-AD
   Decret pel qual es regula l'ENS-AD en l'àmbit de l'Administració Electrònica.
3. ISO/IEC 27000
   Information technology – Security techniques – Information security management systems – Overview and vocabulary
4. ISO/IEC 27001
   Information technology – Security techniques – Information security management systems – Requirements
5. ISO/IEC 27002
   Information technology – Security techniques – Code of practice for information security management
6. ISO/IEC 27003
   Information technology – Security techniques – Information security management system implementation guidance
7. ISO/IEC 27005
   Information technology – Security techniques – Information security risk management
8. Manageable Network Plan
   NSA, version 2.2, April 2012
9. NIST SP 800-37 Rev.1
   Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
10. NIST SP 800-39
    Managing Information Security Risk: Organization, Mission, and Information System View
11. NIST SP 800-53 rev. 4
    Recommended Security Controls for Federal Information Systems,
    http://web.nvd.nist.gov/view/800-53/home
    http://csrc.nist.gov/
12. SANS
    20 Critical Security Controls
    http://www.sans.org/critical-security-controls/

# ANNEX E. HISTÒRIC DE VERSIONS I REGISTRE AMPLIAT DE CANVIS

Aquest annex recull, de manera sintètica, l'evolució del document i els principals canvis incorporats entre versions. Té caràcter informatiu i complementa el "Registre de canvis" inclòs a la fitxa del document.

| Versió | Data de publicació | Canvis incorporats |
|---|---|---|
| 1.0 | 20/12/2022 | Creació de la guia d'implementació.<br>Estructuració inicial del contingut i del marc de controls. |
| 1.1 | 20/03/2023 | Incorporació de l'ANNEX A.<br>Ajustos editorials associats (referències internes i estructura d'annexos). |
| 1.2 | 08/01/2025 | Incorporació d'un nou nivell de maduresa (L4) per caracteritzar la implementació.<br>Actualització amb impacte normatiu: ampliació de l'abast per incloure requeriments associats a categoria mitjana.<br>Inclusió de nous controls i reforços aplicables (controls addicionals en planificació, accés, explotació, monitorització, protecció i mesures complementàries). |
| 2.21 | 22/12/2025 | Actualització amb impacte normatiu (canvi legislatiu) i adequació del contingut.<br>Afegit l'apartat "3. MARC COMÚ" (abast, SGSI, planificació de revisions, DSI, rol de direcció, auditoria i PAC)<br>Remuneració de seccions (desplaçament de "Diferenciació de categories").<br>Actualització de l'índex amb incorporació de [OP.PL.6] Pla de seguretat i [OP.PL.7] Declaració d'aplicabilitat.<br>Reorganització d'annexos amb incorporació d'un annex d'especificacions tècniques i reubicació del glossari i de les referències.<br>Incorporació d'una taula d'equivalència de maduresa amb CMMI.<br>Ajust del pròleg per eliminar referències externes no aplicables al context andorrà. |