ENS-STIC-804
Guia d'implementació

(DOCUMENT SUBJECTE A MODIFICACIONS)

Desembre 2022

Fitxa del document

Títol	Guia d'implementació ENS-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		20/3	Afegit annex A

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 (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 Secretari d'Estat de Transició Digital i Projectes Estratègics la responsabilitat de dirigir l´ANC-AD.

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

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

César Marquina Pérez de la Cruz
Secretari d´Estat de Transició Digital i Projectes Estratègics

ÍNDEX

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'ENS-AD d´Andorra(d'aquí en endavant "ENS-AD") estableix una sèrie de mesures de seguretat en el que 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 als responsables dels sistemes perquè puguin implantar ràpida 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 amplia que la proporcionada a l'ENS-AD,
   - referencies externes que ajuden a la seva comprensió i realització,
   - relació amb mesures o controls en altres esquemes de seguretat,
   - 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
L0	Inexistent. Aquesta mesura no està sent aplicada en aquest moment.
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.
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. Existeix 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. 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.

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	Bàsica	L3

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

3. [ORG] MARC ORGANIZATIU

9. Tota entitat necessita poder assegurar l'abast dels seus objectius, definint funcions i establint responsabilitats i canals de coordinació. Aquesta estructura permet la gestió dia a dia de les activitats rutinàries i la resolució ordenada dels incidents que puguin sobrevenir.
10. 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.
11. 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.
12. 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.

3.1 [ORG.1] POLÍTICA DE SEGURETAT

13. 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.
14. Estableix les autoritats dins de l'entitat: rols i funcions. La política té caràcter d'obligat compliment.
    - Guia ENS-402 – (CCNCERT)Entitat i Gestió par la Seguretat dels Sistemes TIC
15. Son de especial rellevància els següents principis bàsics:
    - La seguretat com a procés integral.
    - Revaluació periòdica.

16. ISO/IEC 27000
    - 27001:2022
        - 4 – Context de l'Entitat
        - 5.2 – Política de Seguretat
        - 5.3 – Rols, responsabilitats i autoritat
    - 27002:2022
        - 6.1.1 - Rols i responsabilitats relatives a la seguretat de la informació
        - 18.1.1 - Identificació de legislació aplicable i requisits contractuals

17. NIST SP 800-53 rev.4
    - [PM-2] Senior Information Security Officer

- [PM-11] Mission/Business Process Definition

18. Altres referencies:
    - NIST SP 800-12 - An Introduction to Computer Security.

3.2 [ORG.2] NORMATIVA DE SEGURETAT

19. 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.
20. A vegades es denominen "policies" (en anglès).
21. A vegades es denominen "standards" (en anglès).
22. 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.
23. Les normes han de descriure el que es considera ús correcte, així com el que es considera ús incorrecte.
24. La normativa té caràcter d'obligat compliment. Això ha de destacar-se, així com les conseqüències derivades del seu incompliment (mesures disciplinàries).
25. 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.
26. Les normes han d'escriure-les 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.
27. 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.
28. Normativa típica:
    - 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, etc.

- 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
- copies de seguretat (back ups)
- 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

29. Són d'especial rellevància els següents principis bàsics:
    - Prevenció, reacció i recuperació.
    - Revaluació periòdica.
30. ISO/IEC 27000
    - 27002:2022
        - 5.1 – Directrius de gestió de la seguretat de la informació
        - 6.1.3 - Contacte amb les autoritats
        - 6.1.4 – Contacte amb grups d'interès especial
        - 18.1.2 – Drets de propietat intel·lectual (IPR)
        - 18.2.3 - Comprovació del compliment tècnic
31. NIST SP 800-53 rev.4
    - Tots els apartats, primer control (XX-1).Per exmple, AC-1 "Access Control Policy and Procedures".
    - PM-15 - Contacts with Security Groups and Associations
32. Altres referències:

- The SANS Security Policy Project
  http://www.sans.org/resources/policies/
- NIST SP800-12 - An Introduction to Computer Security
- NSA - Manageable Network Plan

3.3 [ORG.3] PROCEDIMIENTS OPERATIUS DE SEGURETAT

33. Conjunt de documents que descriuen pas a pas com realitzar una certa activitat. Faciliten les tasques rutinàries evitant que s'oblidin passos importants. El que mai ha d'ocórrer és que una certa activitat només sàpiga fer-la una determinada persona; ha d'estar escrit com es fa perquè la persona pugui ser reemplaçada.
34. 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.
35. A vegades es denominen "guies" o "instruccions".
36. 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 el registre de l'activitat realitzada
    - com es reporten deficiències en els procediments
37. 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.
38. Mai es pot dir que hi ha massa procediments. Quants més, millor.
39. No obstant això, és millor no tenir un procediment que tenir un procediment erroni o antiquat.
40. 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.
41. 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.
42. Són d'especial rellevància los següents principis bàsics:
    - Revaluació periòdica.
43. ISO/IEC 27000

- 27002:2022
  - 12.1.1 - Documentació dels procediments d'operació
  - 18.2.3 - Comprovació del compliment tècnic

44. NIST SP 800-53 rev.4
    - Tots els apartats, primer control (XX-1). Per exemple, AC-1 "Access Control Policy and Procedures".
    - PM-15 - Contacts with Security Groups and Associations

3.4 [ORG.4] PROCÉS D'AUTORITZACIÓ

45. 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.

46. L'ENS-AD singularitza una sèrie d'elements, sense perjudici que s'apliqui sempre la regla de 'es requereix autorització prèvia' amb caràcter general a tots els components durant tot el seu cicle de vida:
    a. Utilització d'instal·lacions, habituals i alternatives.
    b. Entrada d'equips en producció, en particular, equips que involucren criptografia.
    c. Entrada d'aplicacions en producció.
    d. Establiment d'enllaços de comunicacions amb altres sistemes.
    e. Utilització de mitjans de comunicació, habituals i alternatius.
    f. Utilització de suports d'informació.
    g. Utilització d'equips mòbils. S'entendrà per equips mòbils: ordinadors portàtils, PDA, i altres de naturalesa anàloga.
    h. Utilització de serveis de tercers, sota contracte o conveni.
    i. Utilització d'equips propietat de l'usuari (BYOD – *Bring Your Own Device*).

47. 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,
      - o descripció precisa de les activitats per a les quals es requereix el nou component,

- o justificació que nou component no afecta a 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,
- informació dels procediments de seguretat que són aplicables al cas o, si fos necessari, 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

48. 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.
49. L'autorització només cobrirà la utilització dels nous recursos per als objectius explícitament aprovats.
50. Són d'especial rellevància els següents principis bàsics:
    - Revaluació periòdica.
51. ISO/IEC 27000
    - 27002:2022
        - 6.1.1 - Rols i responsabilitats relatives a la seguretat de la informació
52. NIST SP 800-53 rev.4
    - [PM-10] Security Authorization Process
53. Altres referències:
    - NIST SP800-12 - An Introduction to Computer Security
    - Manageable Network Plan

4. MARC OPERACIONAL

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

4.1 [OP.PL] PLANIFICACIÓ

55. Activitats prèvies a la posada en explotació.
56. Són d'especial rellevància els següents principis bàsics:
    - La seguretat com un procés integral.
    - Gestió de la seguretat basada en els riscos

4.1.1 [OP.PL.1] ANÀLISI DE RISCOS

57. Emprem l'expressió "anàlisi de riscs" en el sentit de "risk assessment" en la terminologia d'ISO.
58. 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
59. Tot 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.
60. L'anàlisi de riscos ha de ser una activitat recurrent; és a dir, s'ha de mantenir actualitzat.
61. L'aspecte formal exigeix que l'anàlisi estigui documentada i aprovat. La documentació ha d'incloure els criteris utilitzats per a seleccionar i valorar actius, amenaces i salvaguardes.
62. Una anàlisi de riscos ha de ser realitzat:
    - 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,
    - durant l'operació del sistema, per a ajustar a nous actius, noves amenaces, noves vulnerabilitats i noves salvaguardes
63. 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).
64. Son de especial rellevància els següents principis bàsics:
    - La seguretat com a procés integral.
    - Gestió de la seguretat basada en els riscos.

65. ISO/IEC 27000
    - 27001:2022
        - 6.1 – Accions per abordar riscos i oportunitats
        - 6.1.1 - General
        - 6.1.2 – Avaluació de riscos
        - 6.1.3 – Tractament dels riscos
        - 8.2 – Avaluació de riscos
        - 8.3 – Tractament dels riscos
66. NIST SP 800-53 rev.4
    - [RA] Risk Assessment
    - [PM-9] Risk Management Strategy
67. Altres referències:
    - NIST SP 800-30 - Risk Management Guide for Information Technology Systems
    - NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - NIST SP 800-39 - Managing Risk from Information Systems: An Organizational Perspective
    - ISO/IEC 27005 - Information security risk management
    - ISO/IEC 31000 – Gestió del risc – Principis i directrius

4.1.2 [OP.PL.2] ARQUITECTURA DE SEGURETAT

68. 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.
69. L'arquitectura de seguretat és elaborada sota la direcció del Responsable del Sistema, i és aprovada pel Responsable de la Seguretat.
70. Són d'especial rellevància els següents principis bàsics:
    - Prevenció, reacció i recuperació.
    - Línies de defensa.
71. ISO 27000
    - 27002:2022
        - 8.1.1 - Inventari d'actius
        - 8.1.2 - Propietat dels actius
        - 13.1.1 - Controls de xarxa
        - 14.2.5 - Principis per a la enginyeria de sistemes segurs
72. NIST 800-53 rev.4
    - [CM-8] Information system Component Inventory
    - [PM-5] Information Systems Inventory

- [PM-7] Enterprise Architecture
- [PM-8] Critical Infrastucture Plan
- [SA-5] Information System Documentation
- [SA-8] Security Engineering Principles
- [PL-8] Information Security Architecture

73. Altres referències:

- Manageable Network Plan

4.1.3 [OP.PL.3] ADQUISICIÓ DE NOUS COMPONENTS

74. 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.
- en tot moment s'atendrà tant les necessitats tècniques com a la necessària conscienciació i formació de les persones que treballaran amb els components.

75. Són de especial rellevància los següents principis bàsics:

- Revaluació periòdica.

76. ISO/IEC 27000

- 27002:2022
  - 14.1.1 - Anàlisi de requisits i especificacions de seguretat de la informació

77. NIST 800-53 rev.4

- [PL-1] Security Planning Policy and Procedures
- [PL-2] System Security Plan
- [PL-7] Security Concept of Operations
- [PL-8] Information Security Architecture
- [SA-1] System and Services Acquisition Policy and Procedures
- [SA-3] System Development Life Cycle
- [SA-4] Acquisition Process
- [SA-8] Security Engineering Principles
- [SA-12] Supply Chain Protection

78. Altres referències:

- NIST SP 800-18 - Guide for Developing Security Plans for Federal Information Systems

- NIST SP 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process

4.1.4 [OP.PL.4] DIMENSIONAMENT / GESTIÓ DE CAPACITATS

79. 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 major raó.
80. 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.
81. ISO/IEC 27000
    - 27002:2022
        - 12.1.3 - Gestió de capacitats
82. NIST SP 800-53 rev.4
    - [SA-2] Allocation of Resources
    - [AU-4] Audit Storage Capacity

4.1.5 [OP.PL.5] COMPONENTS CERTIFICATS

83. Totes les paraules es queden curtes per tal d'insistir en la necessitat de recórrer a components provats, avaluats i certificats. Desenvolupar els propis 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 es 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.
84. 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
85. 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. Es 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 que 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 major cost. L'aplicació pràctica d'EAL7 es limita actualment a TOEs amb una funcionalitat estrictament dirigida a la seguretat que permet una extensa anàlisi formal.

86. 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
87. Guies ajuda ENS-AD:
    - Guia CCN-STIC-105 "Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación" (es tracta d'una guia amb constants modificacions i actualitzacions, cal mirar sempre l'última versió).
88. ISO/IEC 27000
89. NIST SP 800-53 rev. 4
90. Altres referències:
    - NIST SP 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
    - NIST SP 800-36 – Guide to Selecting Information Technology Security Products
    - ISO/IEC 15408-1:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

- ISO/IEC 15408-2:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- ISO/IEC 15408-3:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- ISO/IEC 18045:2005 - Information technology – Security techniques – Methodology for IT security evaluation
- ISO/IEC TR 19791:2006 - Information technology – Security techniques – Security assessment of operational systems

4.2 [OP.ACC] CONTROL D'ACCÉS

91. 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.

92. 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.

93. 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.

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

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

4.2.1 [OP.ACC.1] IDENTIFICACIÓ

95. 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.).

96. D'aquesta manera:

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

97. 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.

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

    - Els comptes han de ser inhabilitats quan:
        - l'usuari deixa l'entitat

- o cessa en la funció per a la qual es requeria el compte d'usuari
- o 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

99. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 9.2.1 - Registre i baixa d'usuari
100. NIST SP 800-53 rev. 4
    - [AC-2] Account Management
    - [AC-14] Permitted Actions without Identification or Authentication
    - [IA-2] Identification and Authentication (Organizational Users)
    - [IA-3] Device Identification and Authentication
    - [IA-4] Identifier Management
    - [IA-5] Authenticator Management
    - [IA-8] Identification and Authentication (Non-Organizational Users)

4.2.2 [OP.ACC.2] REQUISITS D'ACCÉS

101. 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.
102. 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.
103. 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.
104. Guies ajuda ENS-AD:
    - Guia CCN-STIC-105 "Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación" (es tracta d'una guia amb constants modificacions i actualitzacions, cal mirar sempre l'última versió).
105. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 9.1.1 - Política de control d'accés
        - 9.1.2 - Accés a xarxes i serveis en xarxa
        - 9.4.1 - Restricció del accés a la informació

- 9.4.4 - Ús dels recursos del sistema amb privilegis especials
- 9.4.5 - Control d'accés al codi font dels programes

106. NIST SP 800-53 rev. 4

- [AC-3] Access Enforcement
- [AC-4] Information Flow Enforcement
- [AC-6] Least Privilege
- [AC-24] Access Control Decisions
- [CM-5] Access Restrictions for Change
- [MP-2] Media Access

107. Altres referències:

- Manageable Network Plan
  - Milestone 5: Control Your Network (User Access)

4.2.3 [OP.ACC.3] SEGREGACIÓ DE FUNCIONS I TASQUES

108. La segregació de funcions té dos objectius:

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

109. 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.

110. 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.

111. 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

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

113. 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.

114. ISO/IEC 27000
    - 27002:2022:
        - 6.1.2 – Segregació de tasques

115. NIST SP 800-53 rev4:
    - [AC-5] Separation of Duties

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

116. 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.

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

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

119. 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.

120. ISO/IEC 27000
    - 27002:2022:
        - 9.2.2 - Provisió d'accés d'usuari
        - 9.2.3 - Gestió de privilegis d'accés
        - 9.2.5 - Revisió dels drets d'accés d'usuari
        - 9.2.6 - Retirada o reassignació dels drets d'accés
        - 9.4.1 - Restricció de l'accés a la informació

121. NIST SP 800-53 rev4:
    - [AC-3] Access Enforcement
    - [AC-24] Access Control Decisions
    - [CM-5] Access Restrictions for Change

122. Altres referències:
    - Manageable Network Plan
        - Milestone 5: Control Your Network (User Access)

4.2.5 [OP.ACC.5] MECANISME D'AUTENTICACIÓ

123. 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.

124. 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)

125. 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

126. 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 claus concertades PIN	amb cautela	amb cautela
Alguna cosa que es té	*tokens* targeta	ok	criptogràfics
Alguna cosa que s'és	biometria	ok	ok

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

127. 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.

128. 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.

129. 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

130. 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)

131. 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
132. S'ha de conscienciar als usuaris dels riscos de l'ús de contrasenyes i instruir-los en com generar-les i custodiar-les.
133. 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 les nn(nombre de contrasenyes) últimes).
    - 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.

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

Claus concertades

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

136. 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 pròpia 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 suficient 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
- 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.

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

138. És responsabilitat del usuari custodiar aquestes claus de manera segura.

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

140. 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

141. Han de generar-se de manera aleatòria per a:
    - resistir atacs aleatoris
    - resistir atacs de diccionari

Claus o targetes

142. Característiques:
    - es poden perdre, accidental o deliberadament
    - es poden robar
    - es poden fer còpies

143. Ús habitual:
    - autenticació enfront de terminals (logon)
    - accés remot i establiment de canals segurs
    - activació de dispositius criptogràfics
    - ús de dos o més targetes d'activació
    - accés a instal·lacions

144. 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.

145. Biometria

146. 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

147. Ús habitual:
    - En la autenticació enfront de terminals:
        - reconeixement d'empremta digital
        - o reconeixement facial
        - o com a doble factor es pot utilitzar una contrasenya o un PIN
    - En el accés a locals o àrees:
        - reconeixement de la mà
        - o reconeixement de l'iris o del fons de l'ull
        - o com a doble factor es pot utilitzar una targeta o un PIN

148. ISO/IEC 27000

- 27002:2022:
  - 9.2.4 - Gestió de la informació secreta d'autenticació d'usuaris
  - 9.3.1 - Ús de la informació secreta d'autenticació
  - 9.4.3 - Sistema de gestió de contrasenyes

149. NIST SP 800-53 rev4:
    - [IA-2] Identification and Authentication (Organizational Users)
    - [IA-3] Device Identification and Authentication
    - [IA-5] Authenticator Management
    - [IA-7] Cryptographic Module Authentication
    - [IA-8] Identification and Authentication (Non-Organizational Users)
150. Altres referències:
    - SANS - CIS Critical Security Controls - Version 6.1
      - CSC.5 - Controlled Use of Administrative Privileges
      - CSC.14 - Controlled Access Based on the Need to Know
    - Password Policy, SANS Institute https://www.sans.org/

4.2.6 [OP.ACC.6] ACCÉS LOCAL (LOCAL LOGON)

151. 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 a 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, ja 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).

152. El sistema ha d'informar i detectar si el seu compte d'usuari ha estat compromes 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.

153. 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.

154. 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.

155. 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.

156. 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.

157. ISO/IEC 27000

- 27002:2022:
  - 9.4.2 - Procediments segurs d'inici de sessió

158. NIST SP 800-53 rev4:

- [AC-7] Unsuccessful Login Attempts
- [AC-8] System Use Notification
- [AC-9] Previous Login Notification
- [IA-5] Authenticator Management
- [IA-6] Authenticator Feedback
- [SI-11] Error Handling

4.2.7 [OP.ACC.7] ACCÉS REMOT (REMOTE LOGIN)

159. L'accés remot és font de nombrosos problemes perquè no pot suposar el mateix nivell de controls de seguretat física que en les instal·lacions corporatives. Per això convé tenir regles específiques respecte a què es pot fer i què no es pot fer des d'un accés remot. I fins i tot dins del que està autoritzat, cal tenir cura en el procés

d'identificació i autenticació per a prevenir la suplantació de la identitat d'un usuari autoritzat.

160. S'exigeix establir un mecanisme robust d'identificació i autenticació segons [op.acc.6]
161. S'exigeix establir una xarxa privada virtual (VPN), segons [mp.com.2] i [mp.com.3].
162. S'ha de redactar una política que regeixi el que es pot fer remotament: quines aplicacions es poden usar, quines dades són accessibles i en quines condicions aquestes dades poden emmagatzemar-se en el dispositiu extern d'accés.
163. La política també ha d'establir límits al mateix temps que pot estar oberta una sessió i imposar un temps màxim per a tancar sessions inactives.
164. A més de redactar la política, cal imposar-la. Això és gairebé impossible si el dispositiu és de l'usuari (BYOD) i en general si l'usuari té drets d'administrador de l'equip. És per això que es procurarà que l'equip remot sigui propietat de l'organisme, estigui configurat per l'organisme i l'usuari no tingui drets d'administrador.
165. A fi de limitar el que es pot fer en remot, s'ha d'establir un filtre, bé als sistemes IT de l´entitat o , bé en el propi client.
166. Si les limitacions s'imposen a l´entitat , farem que l'usuari accedeixi a un segment de xarxa separat del nucli corporatiu i entre el segment d'accés remot i el nucli establirem un tallafocs intern que només permeti les aplicacions i protocols autoritzats.
167. Si les limitacions s'imposen en l'equip client, instal·larem un tallafocs personal, configurat per l'organisme, que estableixi les limitacions corresponents.
168. En tots dos escenaris s'ha de considerar l'oportunitat d'instal·lar una funció de prevenció de fugida de dades (DLP) que monitori les dades que viatgen per la xarxa.
169. En tots els casos s'han d'activar els registres d'activitat i analitzar regularment que es compleix la política autoritzada. Considerar l'oportunitat d'un sistema d'informació de seguretat i administració d'esdeveniments (SIEM) que aixequi alarmes i centralitzi el seu reporti.

170. ISO/IEC 27000
    - 27002:2022:
        - 9.4.2 - Procediments segurs d'inici de sessió
        - 10.1.1 - Política d'ús dels controls criptogràfics
        - 13.1.1 - Controls de xarxa
        - 13.1.2 - Seguretat dels serveis de xarxa
        - 18.1.5 - Regulació dels controls criptogràfics
171. NIST SP 800-53 rev4:

- [AC-10] Concurrent Session Control
- [AC-17] Remote Access
- [AC-18] Wireless Access
- [AC-20] Use of External Information Systems
- [MA-4] Nonlocal Maintenance
- [SA-9] External Information System Services
- [SC-10] Network Disconnect

172. Altres referències:

- http://www.sans.org/reading_room/whitepapers/vpns/remote-access-vpn-security-concerns-policy-enforcement_881

4.3 [OP.EXP] EXPLOTACIÓ

4.3.1 [OP.EXP.1] INVENTARI D'ACTIUS

173. L'inventari 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 reporti d'incidents i per a fer un seguiment, tant 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

174. ISO/IEC 27000

- 27002:2022:
  - 8.1.1 - Inventari d'actius.
  - 8.1.2 – Propietat dels actius.

175. NIST SP 800-53 rev4:

- [CM-8] Information System Component Inventory
- [PM-5] Information System Inventory

176. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.1 - Inventory of Authorized and Unauthorized Devices
  - CSC.2 - Inventory of Authorized and Unauthorized Software

4.3.2 [OP.EXP.2] CONFIGURACIÓ DE SEGURETAT

177. 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
178. 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.
179. 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).
180. La configuració de seguretat ha d'incloure un perfil bàsic d'auditoria d'ús de l'equip.
181. ISO/IEC 27000
182. NIST SP 800-53 rev4:
    - [CM-2] Baseline Configuration
    - [CM-6] Configuration Settings
    - [CM-7] Least Functionality
    - [SI-5] Security Alerts, Advisories, and Directives
183. Altres referències:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.3 - Secure Configurations for Hardware and Software
        - CSC.9 - Limitation and Control of Network Ports
        - CSC.18 - Application Software Security
    - FDCC - Federal Desktop Core Configuration http://nvd.nist.gov/fdcc/index.cfm
    - USGCB - The United States Government Configuration Baseline https://csrc.nist.gov/h
    - Manageable Network Plan
        - Milestone 7: Manage Your Network, Part II (Baseline Management)

4.3.3 [OP.EXP.3] GESTIÓ DE LA CONFIGURACIÓ

184. 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.

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

186. NIST SP 800-53 rev4:

- [CM-3] Configuration Change Control
- [CM-9] Configuration Management Plan

187. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.3 - Secure Configurations for Hardware and Software
- NIST 800-128 Guide for Security-Focused Configuration Management of Information Systems

4.3.4 [OP.EXP.4] MANTENIMENT

188. 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 de el site de l´ANC-AD mitjançant la subscripció al servei de defectes.

189. ISO/IEC 27000

- 27002:2022:
  - 11.2.4 - Manteniment dels equips
  - 12.6.1 - Gestió de les vulnerabilitats tècniques

190. NIST SP 800-53 rev4:

- [CA-2] Security Assessments
- [CA-7] Continuous Monitoring
- [CA-8] Penetration Testing
- [MA-2] Controlled Maintenance
- [MA-3] Maintenance Tools
- [MA-4] Nonlocal Maintenance
- [MA-5] Maintenance Personnel
- [MA-6] Timely Maintenance
- [RA-5] Vulnerability Scanning
- [SI-2] Flaw Remediation
- [SI-4] Information System Monitoring
- [SI-5] Security Alerts, Advisories, and Directives

191. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.4 - Continuous Vulnerability Assessment and Remediation
  - CSC.20 - Penetration Tests and Red Team Exercises

- NIST SP 800-40 - Creating a Patch and Vulnerability Management Program
- Manageable Network Plan
    - Milestone 6: Manage Your Network, Part I (Patch Management)

4.3.5 [OP.EXP.5] GESTIÓ DE CANVIS

192. Ha d'existir un procediment per a canviar components del sistema que requereix:
    - l'aprovació del responsable,
    - la documentació del canvi,
    - proves de la seguretat del sistema després del canvi, en un entorn equivalent que no estigui en producció (o es trobi aïllat del mateix)
    - la retenció d'una còpia del component previ per un temps preestablert
    - còpies de seguretat del component programari, cobrint almenys la versió actual i la immediata anterior
    - s'actualitza l'inventari d'actius
    - s'actualitzen els procediments operatius relacionats amb el component actualitzat
    - s'actualitza el pla de continuïtat de negoci (si existeix tal pla; veure [op.cont])
193. ISO/IEC 27000
    - 27002:2022:
        - 12.1.2 - Gestió de canvis
        - 14.2.2 - Procediments de control de canvis al sistema
        - 14.2.3 – Revisió tècnica de les aplicacions un cop efectuats canvis al sistema operatiu
194. NIST SP 800-53 rev4:
    - [CA-5] Plan of Action and Milestones
    - [CM-4] Security Impact Analysis
    - [CM-5] Access Restrictions for Change
    - [MA-2] Controlled Maintenance
    - [SI-2] Flaw Remediation
    - [SI-7] Software, Firmware, and Information Integrity
195. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.4 - Continuous Vulnerability Assessment and Remediation

4.3.6 [OP.EXP.6] PROTECCIÓ ENFRONT A CODI NOCIU

196. 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.
197. Ha de conscienciar-se al personal per a detectar comportament sospitós i establir canals per a reportar-lo.

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

199. ISO/IEC 27000

- 27002:2022:
  - 12.2.1 Controls contra el codi nociu

200. NIST SP 800-53 rev4:

- [SC-18] Mobile Code
- [SI-3] Malicious Code Protection

201. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.8 - Malware Defenses
- NIST SP 800-28 - Guidelines on Active Content and Mobile Code
- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling

4.3.7 [OP.EXP.7] GESTIÓ D'INCIDENTS

202. 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

203. 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)

204. Procediment que estableix identificar si l'incident afecta a 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.

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

206. 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.

207. ISO/IEC 27000

- 27002:2022:
  - 6.1.3 – Contacte amb les autoritats
  - 6.1.4 – Contacte amb grups d'interès especial
  - 16.1 - Gestió d'incidents de seguretat de la informació i millores

208. NIST SP 800-53 rev4:

- [IR] Incident Response
- [PM-15] Contacts with Security Groups and Associations
- [SI-5] Security Alerts, Advisories, and Directives

209. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.19 - Incident Response and Management
- NIST SP 800-61 – Computer Security Incident Handling Guide
- ISO/IEC TR 18044:2004 - Information technology – Security techniques – Information security incident management

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

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

211. 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).

212. ISO/IEC 27000

- 27002:2022:
  - 12.4.1 – Registre d'esdeveniments
  - 12.4.3 - Registres d'administració i operació

213. NIST SP 800-53 rev4:

- [AU] Audit and Accountability

214. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.16 - Account Monitoring and Control

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

215. 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.

216. ISO/IEC 27000

- 27002:2022:
  - 16.1.5 - Resposta a incidents de seguretat de la informació
  - 16.1.7 - Recopilació d'evidències

217. NIST SP 800-53 rev4:

218. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.19 - Incident Response and Management

4.3.10 [OP.EXP.10] PROTECCIÓ DELS REGISTRES D'ACTIVITAT

219. S'hauran de retenir els registres de manera adequada:

- existeix una declaració formal dels períodes de retenció habituals
- existeix un pla per a garantir la capacitat d'emmagatzematge de registres atenent el seu volum i política de retenció
- existeix un procediment formal per a la retenció d'evidències després d'un incident

220. Existeixen mecanismes que garanteixin la correcció de l'hora a la qual es realitza el registre, en prevenció de manipulacions dels rellotges

221. Únicament el personal autoritzat podrà modificar o eliminar els registres:

- existeixen mecanismes per a prevenir l'accés als registres de persones no autoritzades
- existeixen mecanismes per a prevenir l'accés de persones no autoritzades a la configuració del sistema per al registre automàtic d'activitats
- existeix un procediment per a l'eliminació dels registres després del període estipulat de retenció, incloent-hi les còpies de seguretat

222. Els registres estan contemplats en els processos de còpies de seguretat, garantint les seguretats abans esmentades.

223. ISO/IEC 27000

- 27002:2022:
  - 12.4.2 - Protecció de la informació de registre
  - 12.4.4 - Sincronització del rellotge

224. NIST SP 800-53 rev4:

- [AU-8] Time Stamps
- [AU-9] Protection of Audit Information

225. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.6 - Maintenance, Monitoring, and Analysis of Audit Logs
- NIST SP 800-92 - Guide to Computer Security Log Management

4.3.11 [OP.EXP.11] PROTECCIÓ DE LES CLAUS CRIPTOGRÀFIQUES

226. 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.

227. 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.

228. 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.

229. 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
  - o amb programes avaluats o dispositius criptogràfics certificats conforme a [op.pl.5]
  - o 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

230. ISO/IEC 27000
  - 27002:2022:
    - 10.1.2 - Gestió de claus

231. NIST SP 800-53 rev4:
  - [SC-12] Cryptographic Key Establishment and Management
  - [SC-17] Public Key Infrastructure Certificates

232. Altres referències:
  - NIST SP 800-57 Recommendation for Key Management

4.4 [OP.EXT] SERVEIS EXTERNS

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

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

235. 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.

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

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

237. Ha d'establir-se un contracte formal, 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

238. 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]).

239. ISO/IEC 27000

- 27002:2022
  - 13.2.2 - Acords d'intercanvi d'informació
  - 13.2.4 - Acords de confidencialitat o no revelació
  - 15.1 - Seguretat en la relació amb proveïdors

240. NIST SP 800-53 rev4:

- [SA-9] External Information System Services

241. Altres referències:

- NIST SP 800-35 – Guide to Information Technology Security Services

4.4.2 [OP.EXT.2] GESTIÓ DIÀRIA

242. 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.

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

244. ISO/IEC 27000

- 27002:2022:
  - 15.2 – Gestió de la provisió de serveis del proveïdor

245. NIST SP 800-53 rev4:

- [SA-9] External Information System Services

246. Altres referències:

- NIST SP 800-35 – Guide to Information Technology Security Services

4.4.3 [OP.EXT.3] MITJANS ALTERNATIUS

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

248. S'ha establert un protocol de comunicació amb el proveïdor per a avisar de desastres i escalar el problema.
249. S'ha definit un procediment de reacció i recuperació (RTO) davant fallades prolongades del servei per part del proveïdor.
250. S'ha definit un procediment per a recuperar la informació amb l'antiguitat (RTPO) determinada per la política de l'Entitat.
251. Els processos d'actuació en cas de desastre es proven dins del pla de proves periòdiques ([op.cont.3]) de l'Entitat.

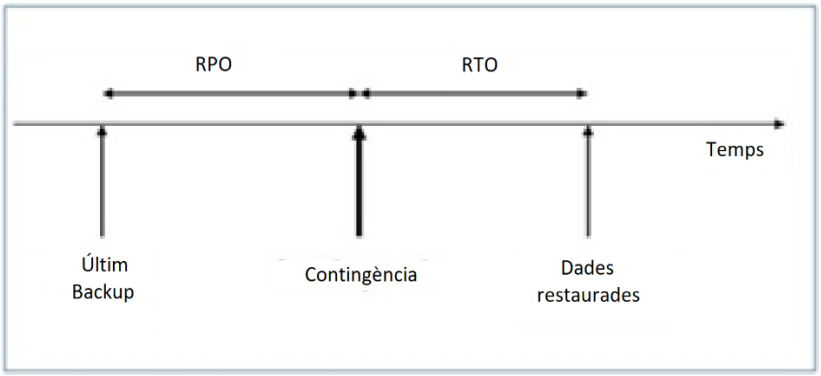

fig.1: Punt de recuperació objectiu (RPO) i temps de recuperació objectiu (RTO).

252. Hi ha una àmplia varietat d'opcions alternatives a un servei prestat per un tercer:
    - El propi proveïdor proporciona els mitjans alternatius, en estar inclosos uns nivells mínims de SLAs 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
    - L'entitat pot recórrer a mitjans, havent de preveure els procediments citats en els punts anteriors
253. NIST SP 800-53 rev. 4

4.5 [OP.CONT] CONTINUÏTAT DEL SERVEI

254. Aquestes activitats permeten instrumentar els principis de seguretat:
    - Prevenció, reacció i recuperació.
255. 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.

256. S'entén per desastre qualsevol esdeveniment accidental, natural o malintencionat que interromp les operacions o serveis habituals d'una entitat durant el temps suficient com per a veure la mateixa afectada de manera significativa.

257. 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.

258. ISO/IEC 27000

- 27002:2022:
  - 17 - Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci

259. NIST SP 800-53 rev4:

- [CP] Contingency Planning

260. Altres referències:

- NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems
- BSI 25999 - BS 25999 Business continuity
- BS 25999-1:2006 Business continuity management. Code of practice.
- BS 25999-2:2007 Business continuity management. Specification.
- ISO 22301
  Societal security – Business continuity management systems – Requirements
- ISO/IEC 24762
  Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
- ISO/IEC 27031
  Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

4.5.1 [OP.CONT.1] ANÀLISI D'IMPACTE

261. 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.

262. Un 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.

263. 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.

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

265. ISO/IEC 27000

- 27002:2022:
  - 17.1.1 - Planificar la continuïtat de la seguretat de la informació

266. NIST SP 800-53 rev4:

- [CP-2] Contingency Plan

4.5.2 [OP.CONT.2] PLA DE CONTINUITAT

267. 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.

268. 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

269. 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])

270. 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.

271. Les persones afectades pel pla han de rebre formació específica relativa al seu paper en aquest pla.

272. El pla de continuïtat ha de ser part integra i harmònica amb els plans de continuïtat de l'entitat en altres matèries alienes a la seguretat.

273. 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.

274. ISO/IEC 27000

- 27002:2022:
  - 17.1.2 Implementar la continuïtat de la seguretat de la informació

275. NIST SP 800-53 rev4:

- [CP] Contingency Planning

4.5.3 [OP.CONT.3] PROVES PERIÒDIQUES

276. S'han de realitzar 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.

277. 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.

278. Després de cada exercici ha de realitzar-se un informe d'anàlisi de les proves realitzades, destacant les incidències pròpies o en subcontractes i derivant un pla de millores tant en els mitjans com en els procediments i en la conscienciació i formació de les persones implicades.

279. Es recomana que l'informe de les proves realitzades contingui informació relativa a la seva eficiència per a poder establir si es compleix amb les necessitats de temps d'execució del Pla de Continuïtat i per a identificar, en comparar-lo amb anteriors proves, si s'està empitjorant en temps per algun factor que hagi de millorar-se.

280. ISO/IEC 27000

- 27002:2022:
  - 17.1.3 - Verificar, revisar i avaluar la continuïtat de la seguretat de la informació

281. NIST SP 800-53 rev4:

- [CP-4] Contingency Plan Testing

4.6 [OP.MON] MONITORITZACIÓ DEL SISTEMA

4.6.1 [OP.MON.1] DETECCIÓ D'INTRUSIÓ

282. Aquestes activitats permeten instrumentar els principis de seguretat:

- Prevenció, reacció i recuperació.
- Línies de defensa.

283. El monitoratge del sistema permet detectar atacs i incidents en general habilitant les mesures de reacció i recopilant informació per a analitzar l'incident.

284. 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.

285. 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.

286. Es monitoraran aquells punts on l'anàlisi de riscos ha identificat un risc elevat.

287. 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.

288. Cal detectar activitats d'atacants interns i externs, així com l'existència de troians o APTs que poguessin haver-se introduït en el sistema.

289. ISO/IEC 27000

290. NIST SP 800-53 rev4:

    - [SI-4] Information System Monitoring

291. Altres referències:

    - NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)

4.6.2 [OP.MON.2] SISTEMA DE MÈTRIQUES

292. Aquestes activitats permeten instrumentar els principis de seguretat

    - Prevenció, reacció i recuperació.
    - Revaluació periòdica.

293. 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.

294. 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.

295. És recomanable formalitzar el procés de generació d'indicadors, havent d'estar aprovat un conjunt d'indicadors, indicant per a cadascun d'ells:

    - 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

296. 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

297. 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.

298. 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

299. 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.

300. ISO/IEC 27000

301. NIST SP 800-53 rev. 4

- [PM-6] Information Security Measures of Performance

302. Altres referències:

- NIST SP 800-55 - Performance Measurement Guide for Information Security
- NIST SP 800-80 - Guide for Developing Performance Metrics for Information Security
- ISO/IEC 27004 - Information technology – Security techniques – Information security management – Measurement

5. [MP] MESURES DE PROTECCIÓ

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

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

303. 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.

304. 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.

305. Es disposarà de mitjans que evitin l'accés per punts diferents al 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.).

306. ISO/IEC 27000

- 27002:2022
  - 11.1 – Àrees segures
  - 11.2.1 - Emplaçament i protecció d'equips

307. NIST SP 800-53 rev. 4

- [PE-18] Location of Information System Components
- [PE-3] Physical Access Control
- [PE-4] Access Control for Transmission Medium
- [PE-5] Access Control for Output Devices

5.1.2 [MP.IF.2] IDENTIFICACIÓ DE LES PERSONES

308. 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).

309. 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.

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

311. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 11.1.2 - Controls físics d'entrada

312. NIST SP 800-53 rev.4

- [PE-2] Physical Access Authorizations
- [PE-6] Monitoring Physical Access
- [PE-8] Visitor Access Records

5.1.3 [MP.IF.3] ACONDICIONAMIENT DELS LOCALS

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

314. 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

315. ISO/IEC 27000

- 27002:2022
  - 11.2.2 - Instal·lacions de subministrament
  - 11.2.3 – Seguretat del cablejat

316. NIST SP 800-53 rev. 4

- [PE-14] Temperature and Humidity Controls

5.1.4 [MP.IF.4] ENERGIA ELÈCTRICA

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

318. Prevenció de problemes d'origen intern:

- dimensionament i protecció del cablejat de potència
- dimensionat i protecció dels quadres i armaris de potència

319. Reacció a problemes d'origen extern:

- subministrament alternatiu: UPS, generadors, proveïdor alternatiu

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

321. 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.

322. ISO/IEC 27000

- 27002:2022
  - 11.2.2 - Instal·lacions de subministrament

323. NIST SP 800-53 rev.4

- [PE-9] Power Equipment and Cabling
- [PE-10] Emergency Shutoff
- [PE-11] Emergency Power
- [PE-12] Emergency Lighting

5.1.5 [MP.IF.5] PROTECCIÓ ENFRONT D'INCENDIS

324. 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

325. 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

326. ISO/IEC 27000

- 27002:2022
  - 11.1.4 - Protecció contra les amenaces externes i d'origen ambiental

327. NIST SP 800-53 rev.4

- [PE-13] Fire Protection

5.1.6 [MP.IF.6] PROTECCIÓ ENFRONT A INUNDACIONS

328. S'ha de realitzar un estudi del risc d'inundacions, tant d'origen natural com industria:
    - proximitat a rius o corrents d'aigua
    - canalitzacions d'aigua (canonades) especialment damunt dels equips
329. 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
330. ISO/IEC 27000
    - 27002:2022
        - 11.1.4 - Protecció contra les amenaces externes i d'origen ambiental
331. NIST SP 800-53 rev.4
    - [PE-15] Water Damage Protection

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

332. 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
333. 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.
334. ISO/IEC 27000
    - 27002:2022
        - 11.2.5 - Retirada de materials propietat de l'empresa
        - 11.2.6 - Seguretat dels equips fora de les instal·lacions
335. NIST SP 800-53 rev. 4
    - [PE-16] Delivery and Removal

5.1.8 [MP.IF.8] INSTAL·LACIONS ALTERNATIVES

336. S'ha de disposar de plans per a poder prestar els serveis en un lloc alternatiu en cas d'indisponiblitat de les instal·lacions actuals.

337. Les instal·lacions alternatives han de garantir les mateixes mesures de protecció que les habituals. En particular, pel que fa a control d'accés de persones i entrada i sortida d'equips.

338. Les instal·lacions alternatives poden estar disposades per a entrar en servei immediatament (hot site) o requerir un temps de personalització (cold site). En tot cas el temps d'entrada en servei ha d'estar recolzat per una anàlisi d'impacte (veure [op.cont.1]), ser part del pla de continuïtat provat (veure [op.cont.2]) i ser objecte de proves regulars per a validar la viabilitat del pla (veure [op.cont.3]).

339. ISO/IEC 27000

- 27002:2022
  - 17.2.1 - Disponibilitat dels mitjans de processament d'informació

340. NIST SP 800-53 rev. 4

- [CP-2] Contingency Plan
- [CP-6] Alternate Storage Site
- [CP-7] Alternate Processing Site
- [PE-17] Alternate Work Site

5.2 [MP.PER] GESTIÓ DEL PERSONAL

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

5.2.1 [MP.PER.1] CARACTERITZACIÓ DEL LLOC DE TREBALL

342. 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.

343. 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.

344. 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.

345. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 7.1.1 - Investigació d'antecedents

346. NIST SP 800-53 rev. 4

- [PS-2] Position Risk Designation
- [PS-3] Personnel Screening
- [SA-21] Developer Screening

5.2.2 [MP.PER.2] DEURES I OBLIGACIONS

347. 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.

348. 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.

349. 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.

350. 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

351. ISO/IEC 27000

- 27002:2022
  - 7.1.2 - Termes i condicions de contractació
  - 7.2.1 - Responsabilitats de la Direcció
  - 7.2.3 - Procés disciplinari
  - 7.3.1 - Terminació o canvi de responsabilitats laborals
  - 8.1.4 - Devolució d'actius
  - 13.2.4 - Acords de confidencialitat o no divulgació

352. NIST 800-53 rev. 4

- [PL-4] Rules of Behavior
- [PS-6] Access Agreements
- [PS-7] Third-Party Personnel Security
- [PS-4] Personnel Termination
- [PS-5] Personnel Transfer
- [PS-8] Personnel Sanctions

5.2.3 [MP.PER.3] CONCIENCIACIÓ

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

354. En particular cal refrescar regularment:
    - la normativa de seguretat relativa al bon ús dels sistemes
    - 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
355. Tot el personal ha de rebre inicial i regularment informació sobre els punts a dalt descrits.
356. ISO/IEC 27000
    - 27001:2022
        - 7.3 - Conscienciació
    - 27002:2022
        - 7.2.2 - Conscienciació, formació i capacitació a seguretat de la informació
357. NIST SP 800-53 rev. 4
    - [AT-2] Security Awareness Training
    - [AT-3] Role-Based Security Training
    - [CP-3] Contingency Training
    - [IR-2] Incident Response Training
    - [PM-13] Information Security Resources
358. Altres referències:
    - NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

5.2.4 [MP.PER.4] FORMACIÓ

359. S'ha de formar regularment a les persones en aquelles tècniques que requereixin per a l'acompliment de les seves funcions.
360. 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)
361. 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.
362. ISO/IEC 27000
    - 27001:2022
        - 7.2 - Competències

- 27002:2022
    - 7.2.2 - Conscienciació, formació i capacitació a seguretat de la informació

363. NIST SP 800-53 rev. 4
    - [AT-2] Security Awareness Training
    - [AT-3] Role-Based Security Training
    - [AT-4] Security Training Records
    - [CP-3] Contingency Training
    - [IR-2] Incident Response Training
    - [PM-13] Information Security Resources
364. Altres referències:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.17 - Security Skills Assessment and Appropriate Training to Fill Gaps
    - NIST SP 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
    - NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

5.2.5 [MP.PER.5] PERSONAL ALTERNATIU

365. S'ha de preveure l'existència d'altres persones que es puguin fer càrrec de les funcions en cas d'indisponiblitat del personal habitual. El personal alternatiu haurà d'oferir les mateixes garanties de seguretat que el personal habitual.
366. Aquest personal alternatiu pot ser, per exemple:
    - Personal del mateix equip sobredimensionat amb capacitat d'assumir el treball
    - Personal d'altres torns 24x7 que puguin cobrir baixes eventuals
    - Personal d'altres departaments amb els coneixements necessaris (respectant la segregació)
    - Personal d'un tercer contractat previst en el Pla de Continuïtat
367. El pla d'utilització de personal alternatiu es descriu dins del pla de continuïtat de l'entitat, incloent-se en les proves periòdiques.
368. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 17.2.1 - Disponibilitat dels recursos de tractament de la informació
369. NIST SP 800-53 rev. 4
    - [CP-2] Contingency Plan
    - [CP-6] Alternate Storage Site
    - [CP-7] Alternate Processing Site

5.3 [MP.EQ] PROTECCIÓ DELS EQUIPS

5.3.1 [MP.EQ.1] LLOC DE TREBALL ORDENAT

370. 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.
371. El material de treball es guardarà en lloc tancat. Poden ser calaixos o armaris amb clau, o una habitació separada tancada amb clau almenys fora de l'horari de treball.
372. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 11.2.9 - Política de lloc de treball ordenat i pantalla neta
373. NIST SP 800-53 rev. 4

5.3.2 [MP.EQ.2] BLOQUEIG DE LLOC DE TREBALL

374. 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.
375. S'ha de requerir a l'usuari autenticar-se de nou per a reprendre l'activitat en curs.
376. El temps esmentat serà part de la configuració de l'equip i no podrà ser alterat per l'usuari.
377. 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).
378. El temps esmentat serà part de la configuració de l'equip i no podrà ser alterat per l'usuari.
379. ISO/IEC 27000
    - 27002:2022:
        - 11.2.8 - Equip d'usuari desatès
380. NIST SP 800-53 rev. 4
    - [AC-11] Session Lock
    - [AC-12] Session Termination

5.3.3 [MP.EQ.3] PROTECCIÓ D'EQUIPS PORTÀTILS

381. 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.

382. 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]).
383. 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.
384. El mecanisme de control de l'equip formarà part de la configuració de l'equip i no podrà ser modificat per l'usuari.
385. 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.
386. 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.
387. 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
388. 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.).
389. S'ha de protegir la informació continguda de nivell alt per mitjans criptogràfics: [mp.si.2].
390. Les claus criptogràfiques han de protegir-se segons [op.exp.11].
391. Quan l'equip és desmantellat, s'ha d'aplicar el que es preveu en [mp.si.5].
392. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 6.2.1 - Política de dispositius mòbils
        - 11.2.6 – Seguretat dels equips fora de les instal·lacions
393. NIST SP 800-53 rev4:
    - [AC-19] Access Control for Mobile Devices

5.3.4 [MP.EQ.4] MITJANS ALTERNATIUS

394. 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.
395. S'ha d'establir un temps màxim perquè els equips alternatius entrin en funcionament.
396. 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 recolzat per una anàlisi d'impacte (veure [op.cont.1]).
397. ISP/IEC 27000
    - 27002:2022
        - 17.2.1 - Disponibilitat d'instal·lacions de tractament de la informació
398. NIST SP 800-53 rev. 4

5.4 [MP.COM] PROTECCIÓ DE LES COMUNICACIONS

5.4.1 [MP.COM.1] PERÍMETRE SEGUR

399. 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).
400. 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.
401. Quan es requereixi nivells de seguretat crítics, el sistema de tallafocs constarà de dos o més equips de diferent fabricant disposats en cascada. Aquests tallafocs podran ser equips físics o instal·lacions o aplicacions tallafocs virtuals.
402. Quan la disponibilitat de les transmissions a través del tallafocs sigui de nivell crític, es disposaran sistemes redundants.
403. 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).
404. ISO/IEC 27000

- 27002:2022:
  - 13.1.2 – Seguretat dels serveis de xarxa

405. NIST SP 800-53 rev. 4
   - [AC-4] Information Flow Enforcement
   - [CA-3] System Interconnections
   - [SC-7] Boundary Protection

406. Altres referències:
   - SANS - CIS Critical Security Controls - Version 6.1
     - CSC.8 - Malware Defenses
     - CSC.9 – Limitation and Control of Network Ports
     - CSC.11 – Secure Configurations for Network Devices
     - CSC.12 – Boundary Defense
     - CSC.13 – Data Protection
     - CSC.15 - Wireless Access Control
   - NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy

5.4.2 [MP.COM.2] PROTECCIÓ DE LA CONFIDENCIALITAT

407. 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.3].

408. S'han d'emprar algorismes acreditats que garanteixin el secret de les dades transmeses.

409. En connexions establertes fora del domini de seguretat de l'entitat, es recorrerà a xarxes privades virtuals que, amb mètodes criptogràfics i després d'una autenticació fiable (veure [mp.com.3]), estableixen una clau de xifratge per a la sessió.

410. 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.

411. Cal atendre el secret de les claus de xifratge segons l'indicat 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 de les claus de xifratge durant el seu cicle de vida: generació, distribució, ocupació, retirada del servei i retenció si n'hi hagués.

412. Cal seleccionar algorismes avaluats o acreditats. Sovint n'hi ha prou amb seleccionar els algorismes i els paràmetres adequats dins de les opcions possibles.

413. 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.

414. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 10.1.1 - Política d'ús dels controls criptogràfics
  - 13.1.1 - Controls de xarxes
  - 13.1.2 - Seguretat dels serveis de xarxa
  - 14.1.2 - Assegurar els serveis d'aplicacions a xarxes públiques
  - 18.1.5 - Regulació dels controls criptogràfics

415. NIST 800-53 rev. 4

- [AC-4] Information Flow Enforcement
- [AC-18] Wireless Access
- [SC-8] Transmission Confidentiality and Integrity
- [SC-12] Cryptographic Key Establishment and Management
- [SC-13] Cryptographic Protection
- [SC-40] Wireless Link Protection

416. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.15 - Wireless Access Control
- NIST SP 800-48 - Wireless Network Security for IEEE 802.11a/b/g and Bluetooth
- NIST SP 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-77 - Guide to IPsec VPNs
- NIST SP 800-113 - Guide to SSL VPNs
- NIST SP 800-121 - Guide to Bluetooth Security
- NIST SP 800-127 - Guide to Securing WiMAX Wireless Communications
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- SSL – Secure Sockets Layer
  - [RFC 6101] The Secure Sockets Layer (SSL) Protocol Version 3.0
- TLS – Transport Layer Security
  - [RFC 5246] The Transport Layer Security (TLS) Protocol – Version 1.2
  - [RFC 6176] Prohibiting Secure Sockets Layer (SSL) Version 2.0
- SSH – Secure Shell
- SCP – Secure copy
- SFTP – SSH File Transfer Protocol

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

417. 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].

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

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

420. 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.

421. 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

422. 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.

423. 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 d'utilitzar-se amb cautela aplicant exigències mitjanes de qualitat.

424. 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.

425. 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.

426. Cal atendre el secret de les claus de xifratge segons l'indicat 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 de les claus de xifratge durant el seu cicle de vida: generació, distribució, ocupació, retirada del servei i retenció si n'hi hagués.

427. 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.

428. 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 d'utilitzar-se amb cautela aplicant exigències altes de qualitat.

429. ISO/IEC 27000

    - ISO/IEC 27002:2022:
        - 10.1.1 - Política d'ús dels controls criptogràfics
        - 13.1.1 - Controls de xarxa
        - 13.1.2 - Seguretat dels serveis de xarxa
        - 14.1.2 - Assegurar els serveis d'aplicacions en xarxes públiques

430. NIST SP 800-53 rev. 4

    - [AC-18] Wireless Access
    - [SC-8] Transmission Confidentiality and Integrity
    - [SC-13] Cryptographic Protection
    - [SC-23] Session Authenticity
    - [SC-40] Wireless Link Protection

431. Altres referències:

    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.15 - Wireless Access Control

5.4.4 [MP.COM.4] SEGREGACIÓ DE XARXES

432. 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].

433. 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

434. 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 què cal vigilar els protocols de comunicacions que s'estableixen i les dades que es transmeten.

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

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

437. 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 propi sistema per a evitar que es capturin credencials amb privilegis d'administració o es pugui suplantar la identitat dels administradors.

438. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 13.1.3 – Segregació a xarxes

439. NIST SP 800-53 rev. 4

- [SC-32] Information System Partitioning

5.4.5 [MP.COM.5] MITJANS ALTERNATIUS

440. S'ha de preveure mitjans alternatius de comunicació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius han de proporcionar les mateixes garanties de seguretat que els mitjans habituals i haurà d'establir-se un temps màxim d'entrada en funcionament que estigui aprovat pel seu responsable.

441. En tot cas, el temps d'entrada en servei ha d'estar recolzat per una anàlisi d'impacte (veure [op.cont.1]), ser part del pla de continuïtat provat (veure [op.cont.2]) i ser objecte de proves regulars per a validar la viabilitat del pla (veure [op.cont.3]).

442. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 17.2.1 - Disponibilitat dels recursos de tractament de la informació

443. NIST SP 800-53 rev. 4

- [CP-8] Telecommunications Services
- [CP-11] Alternate Communications Protocol

5.5 [MP.SI] PROTECCIÓ DELS SOPORTS D'INFORMACIÓ

444. 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

5.5.1 [MP.SI.1] ETIQUETAT

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

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

447. 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.

448. 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

449. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 8.2.2 - Etiquetat de la informació
  - 8.3.1 - Gestió de suports extraïbles

450. NIST SP 800-53 rev. 4

- [MP-3] Media Marking

5.5.2 [MP.SI.2] CRIPTOGRAFIA

451. Aquest requisit s'aplica, en particular, a tots els dispositius removibles (com CD, DVD, discos USB, etc.).

452. Referent a claus criptogràfiques, s'ha d'aplicar [op.exp.11].

453. 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.

454. 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.

455. 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.

456. ISO/IEC 27000

- 27002:2022:
  - 8.3.1 - Gestió de suports extraïbles
  - 10.1.1 - Política d'ús dels controls criptogràfics

457. NIST SP 800-53 rev4:
   - [SC-28] Protection of Information at Rest
458. Altres referències:
   - NIST SP 800-111 - Guide to Storage Encryption Technologies for End User Devices
459. 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.

5.5.3 [MP.SI.3] CUSTÒDIA

460. 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
461. 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.
462. ISO/IEC 27000
   - ISO/IEC 27002:2022:
     - 8.3.1 - Gestió de suports extraïbles
463. NIST SP 800-53 rev. 4
   - [MP-4] Media Storage
464. Altres referències:
   - NIST SP 800-111 – Guide to Storage Encryption Technologies for End User Devices

5.5.4 [MP.SI.4] TRANSPORT

465. S'ha de garantir que els dispositius romanen sota control i se satisfan els seus requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre.
466. 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]

467. 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.

468. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 8.3.3 – Suports físics en trànsit
  - 11.2.5 - Retirada de materials propietat de l'empresa

469. NIST SP 800-53 rev4:

- [MP-5] Media Transport

5.5.5 [MP.SI.5] BORRAT I DESTRUCCIÓ

470. S'ha d'aplicar un mecanisme d'esborrat 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'esborrat serà proporcionat a la classificació de la informació que ha estat present en el suport.

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

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

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

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

474. S'han de triar productes certificats conforme al que s'estableix en [op.pl.5]

475. Recomanacions (preses de NIST SP 800-88):

Medi	Procediment	
Paper Microfilm	Destruir	trituradora a tires o quadres: 2mm
Mòbils PDAs	Esborrar manualment	agenda missatges trucades resetejar a la configuració de fàbrica Copies al núvol
Routers	Esborrar manualment	taules d'encaminament registres d'activitat comptes d'administració resetejar a la configuració de fàbrica
Impresores Fax	Esborrar manualment	resetejar a la configuració de fàbrica
Discs reescribibles	Reescriure	reescriure 3 vegades: amb zeros, amb uns, amb dades aleatòries
discs de només lectura	Destruir	trituradora: 5mm
discs virtuals xifrats	A més del anterior	destruir les claus

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

476. ISO/IEC 27000

- 27002:2022:
  - 8.3.2 - Eliminació de suports
  - 11.2.7 - Reutilització o eliminació segura d'equips

477. NIST SP 800-53 rev4:

- [MP-6] Media Sanitization
- [MP-8] Media Downgrading

478. Altres referències:

- NIST SP 800-88 - Guidelines for Media Sanitization
- DoD 5220 Block Erase

5.6 [MP.SW] PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES

5.6.1 [MP.SW.1] DESENVOLUPAMENT

479. 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 l'entorn 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.

480. 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.

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

482. 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.

483. 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.

484. 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.

485. 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.

486. 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.

487. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 9.4.5 - Control de Control d'accés al codi font dels programes
  - 12.1.4 - Separació dels recursos de desenvolupament, prova i operació
  - 14.2.1 - Política de desenvolupament segur
  - 14.2.5 - Principis d'enginyeria de sistemes segurs
  - 14.2.6 - Entorn de desenvolupament segur
  - 14.2.7 - Externalització del desenvolupament de programari
  - 14.3.1 - Protecció de les dades de prova

488. NIST SP 800-53 rev. 4

- [CM-4] (1) Security Impact Analysis - Separate Test Environments
- [SA-3] System Development Life Cycle
- [SA-4] Acquisition Process
- [SA-8] Security Engineering Principles
- [SA-10] Developer Configuration Management
- [SA-11] Developer Security Testing and Evaluation
- [SA-12] Supply Chain Protections
- [SA-15] Development Process, Standards, and Tools
- [SA-17] Developer Security Architecture and Design

489. Altres referències:

- SANS http://www.sans.org/curricula/secure-software-development
- Mètrica v3 - Metodologia de Planificació, Desenvolupament i Manteniment de sistemes d'informació, Ministeri d'Administracions Públiques, Consell Superior d'Administració Electrònica
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle

5.6.2 [MP.SW.2] ACEPTACIÓ I POSADA EN SERVEI

490. Es realitzen proves estàndard d'acceptació perquè un nou programari s'integri en un procés, ja sigui un programari desenvolupat en la pròpia 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.

491. 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 pre-producció (encara que podrà utilitzar-se 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.

492. 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.

493. 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 major impacte potencial

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

495. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 12.1.4 - Separació dels recursos de desenvolupament, prova i operació
  - 12.5.1 - Instal·lació del programari en explotació
  - 14.2.8 - Proves funcionals de seguretat de sistemes
  - 14.2.9 - Proves d'acceptació de sistemes
  - 14.2.7 - Externalització del desenvolupament de programari
  - 14.3.1 - Protecció de les dades de prova

496. NIST SP 800-53 rev. 4

5.7 [MP.INFO] PROTECCIÓ DE LA INFORMACIÓ

5.7.1 [MP.INFO.1] DADES DE CARÀCTER PERSONAL

497. 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.

498. 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
- ENS-AD

5.7.2 [MP.INFO.2] QUALIFICACIÓ DE LA INFORMACIÓ

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

500. 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
- ha d'establir les responsabilitats per a adscriure inicialment una certa informació a una certa qualificació i per a possibles re-qualificacions posteriors (nivells de seguretat) i determinar el responsable de la documentació i aprovació formal

501. 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]

502. 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 • cada persona s'encarrega de la seva destrucció quan ja no fa falta • marcades • destrucció fent servir destructora
Suports electrònics d'informació [mp.si]	• etiquetats • es borra el contingut o s'inhabilita • etiquetats • es xifra el contingut • es fa servir software d'esborrat segur o es destrueix
Ús en equips portàtils i PDAs [mp.info.3] [mp.eq.3]	• con control de accés • con control de accés
Transmissió telemàtica [mp.com.2] [mp.com.3]	• canals autenticats • canals autenticats i xifrats

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

503. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 8.1.2 – Propietat dels actius
        - 8.2.1 - Classificació de la informació
504. NIST SP 800-53 rev.

5.7.3 [MP.INFO.3] XIFRAT

505. S'ha de xifrar la informació de nivell alt, tant durant el seu emmagatzematge (mp.si.2) com durant la seva transmissió (mp.com.2). Només estarà en clar mentre s'està fent ús d'ella. Això inclou:
    - xifratge de fitxers
    - xifrat de directoris
    - discos virtuals xifratges
    - xifrat de dades en bases de dades
506. S'ha de xifrar la informació en funció de la seva qualificació i el mitjà en el qual s'emmagatzema.
507. ISO/IEC 27000
    - 27002:2022:

- 10.1.1 - Política d'ús dels controls criptogràfics
- 14.1.3 - Protecció de les transaccions de serveis d'aplicacions
- 18.1.5 - Regulació dels controls criptogràfics

508. NIST SP 800-53 rev4:
    - [SC-13] Cryptographic Protection
    - [SC-28] Protection of Information at Rest
509. Altres referències:
    - GNUPG – The GNU Privacy Guard
    - PGP – Pretty Good Privacy
    - Veracrypt

5.7.4 [MP.INFO.4] SIGNATURA ELECTRÒNICA

510. Totes les activitats relacionades amb la signatura electrònica i el segellat de temps han de regir-se per un marc tècnic i procedimental aprovat formalment. Se sol denominar Política de Signatura.
511. 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

512. 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

Ús de claus concertades per a signar

Codi segur de verificació

513. Es tracta d'una forma alternativa d'assegurar l'autenticitat i integritat de la informació proporcionada per l´entitat..
514. 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).
515. 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.).

516. S'adjunta a la signatura, o es referencia, tota la informació pertinent per a la seva verificació i validació: certificats i dades de verificació i validació.

517. Es protegeixen la signatura, el certificat i les dades de verificació i validació amb un segell de temps.

518. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 10.1.1 - Política d'ús dels controls criptogràfics
        - 14.1.3 - Protecció de les transaccions de serveis d'aplicacions
        - 18.1.5 - Regulació dels controls criptogràfics

519. NIST SP 800-53 rev. 4
    - [SC-13] Cryptographic Protection
    - [SC-28] Protection of Information at Rest

520. Altres referències:
    - NIST SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications

5.7.5 [MP.INFO.5] SEGELLS DE TEMPS

521. 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.

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

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

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

525. 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.

526. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 14.1.3 - Protecció de les transaccions de serveis d'aplicacions

527. NIST SP 800-53 rev. 4

- [AU-10] Non-repudiation
- ISO/IEC 18014-1:2008
  Information technology – Security techniques – Time-stamping services – Part 1: Framework
- ISO/IEC 18014-2:2009
  Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens
- ISO/IEC 18014-3:2009
  Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens
- 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)

5.7.6 [MP.INFO.6] NETEJA DE DOCUMENTS

528. 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.

529. 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.

530. 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
- a la bona imatge de l'entitat que difon el document ja que demostra un descuit en el seu bon fer

531. NIST SP 800-53 rev. 4

5.7.7 [MP.INFO.7] COPIES DE SEGURETAT (BACKUP)

532. S'han de realitzar còpies de seguretat que permetin recuperar dades perdudes accidental o intencionadament amb una antiguitat a determinar per l'entitat.

533. 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]).

534. Es recomana establir un procés d'autorització per a la recuperació d'informació de les còpies de seguretat.

535. 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.

536. 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.

537. 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

538. Per als punts anteriors veure [op.exp] i [mp.info.3].

539. 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.

540. 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.

541. Es recomana realitzar periòdicament proves de restauració de còpies de seguretat.

542. ISO/IEC 27000

- 27002:2022:
  - 12.3.1 - Copies de seguretat de la informació

543. NIST SP 800-53 rev4:

- [CP-6] Alternate Storage Site
- [CP-9] Information System Backup
- [CP-10] Information System Recovery and Reconstitution

544. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.10 - Data Recovery Capability

5.8 [MP.S] PROTECCIÓ DELS SERVEIS

5.8.1 [MP.S.1] PROTECCIÓ DEL CORREU ELECTRÒNIC (E-MAIL)

545. 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, ja sigui en el servidor de correu o en 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
546. ISO/IEC 27000
    - ISO/IEC 27002:2022:
        - 13.2.3 - Missatgeria electrònica
547. NIST 800-53 rev. 4
    - [SI-8] Spam Protection
548. Altres referències:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.7 - Email and Web Browser Protections
    - NIST SP 800-45 – Guidelines on Electronic Mail Security

5.8.2 [MP.S.2] PROTECCIÓ DE SERVEIS I APLICACIONS WEB

549. S'ha de protegir els subsistemes dedicats a la publicació d'informació enfront dels atacs o amenaces que els són pròpies.
550. 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)
551. Les tasques preventives no excusen d'un sistema de monitoratge i reacció enfront d'atacs exitosos.

552. 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.

553. 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.

554. 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)

555. 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.

556. ISO/IEC 27000

- 27002:2022:
  - 14.1.2 - Assegurar els serveis d'aplicacions en xarxes públiques

557. NIST SP 800-53 rev. 4

558. Altres referències:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.7 - Email and Web Browser Protections

- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- PCI-DSS v3.0
    - Requisit 6: Desenvolupi i mantingui sistemes i aplicacions segures

5.8.3 [MP.S.3] PROTECCIÓ ENFRONT LA DENEGACIÓ DE SERVEI

559. S'han d'establir mesures preventives i reactives enfront d'atacs de denegació de servei (DoS).

560. 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 suficients recursos per part de l'atacant.

561. 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.

562. 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.

563. 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.

564. És responsabilitat de l'organisme detectar i bloquejar l'ús deliberat o accidental del propi sistema d'informació per a atacar a tercers des de les pròpies 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.

565. 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.

566. ISO/IEC 27000

- ISO/IEC 27002:2022:
  - 12.1.3 - Gestió de capacitats

567. NIST SP 800-53 rev. 4
    - [CP-2] (2) Contingency Plan - Capacity Planning
    - [SC-5] (2) Denial of Service Protection - Excess Capacity / Bandwidth / Redundancy

5.8.4 [MP.S.4] MITJANS ALTERNATIUS

568. S'ha de preveure mitjans alternatius per a oferir els serveis en el cas que fallin els mitjans habituals, mentre es recupera la disponibilitat d'aquests (com per exemple una instància alternativa a un portal). Aquests mitjans alternatius estaran subjectes a les mateixes garanties de protecció.
569. S'ha d'establir un temps màxim perquè els serveis alternatius entrin en funcionament.
570. Els serveis alternatius poden estar disposats per a entrar en servei immediatament o requerir un temps de personalització. En tot cas, el temps d'entrada en servei ha d'estar recolzat per una anàlisi d'impacte (veure [op.cont.1]).
571. El pla d'utilització de serveis alternatius es vertebrarà dins del pla de continuïtat aprovat (veure [op.cont.2]) i ser objecte de proves regulars per a validar la viabilitat del pla (veure [op.cont.3]).
572. ISO/IEC 27000
    - ISO/IEC 27002:2022:
      - 17.2.1 - Disponibilitat dels recursos de tractament de la informació
573. NIST SP 800-53 rev. 4
    - [CP] Contingency Planning

ANNEX A. MESURES DE SEGURETAT

574. La correspondència entre les mesures de seguretat exigides per al nivell basic s'indiquen en a següent taula:

Mesures de Seguretat		Nivell Basic
org	Marc organitzatiu	
org.1	Política de seguretat	aplica
org.2	Normativa de seguretat	aplica
org.3	Procediments de seguretat	aplica
org.4	Procés d'autorització	aplica
op	Marc operacional	
op.pl	Planificació	
op.pl.1	Anàlisi de riscos	aplica
op.pl.2	Arquitectura de seguretat	aplica
op.pl.3	Adquisició de nous components	aplica
op.pl.4	Dimensionament/gestió de la capacitat	aplica
op.pl.5	Components certificats	n.a.
op.acc	Control d'accés	
op.acc.1	Identificació	aplica
op.acc.2	Requisits d'accés	aplica
op.acc.3	Segregació de funciones i tasques	n.a.
op.acc.4	Procés de gestió de drets d'accés	aplica
op.acc.5	Mecanisme d'autenticació (usuaris externs)	aplica
op.acc.6	Mecanisme d'autenticació (usuaris de l'organització)	aplica
op.exp	Explotació	
op.exp.1	Inventari d'actius	aplica
op.exp.2	Configuració de seguretat	aplica
op.exp.3	Gestió de la configuració de seguretat	aplica
op.exp.4	Manteniment i actualitzacions de seguretat	aplica
op.exp.5	Gestió de canvis	n.a.
op.exp.6	Protecció enfront a codi maliciós	aplica
op.exp.7	Gestió d'incidents	aplica
op.exp.8	Registre de l'activitat	aplica
op.exp.9	Registre. de la gestió d'incidents	aplica
op.exp.10	Protecció de Claus criptogràfiques	aplica
op.ext	Recursos externs	
op.ext.1	Contractació i acords de nivell de servei	n.a.

op.ext.2	Gestió diària	n.a.
op.ext.3	Protecció de la cadena de subministrament	n.a.
op.ext.4	Interconnexió de sistemes	n.a.
op.nub	Serveis al núvol	
op.nub.1	Protecció de serveis al núvol	aplica
op.cont	Continuïtat del servei	
op.cont.1	Anàlisi d'impacte	n.a.
op.cont.2	Pla de continuïtat	n.a.
op.cont.3	Proves periòdiques	n.a.
op.cont.4	Mitjans alternatius	n.a.
op.mon	Monitorització del sistema	
op.mon.1	Detecció d'intrusió	aplica
op.mon.2	Sistema de mètriques	aplica
op.mon.3	Vigilància	aplica
mp	Mesures de protecció	
mp.if	Protecció de les instal·lacions i infraestructures	
mp.if.1	Àrees separades i amb control d'accés	aplica
mp.if.2	Identificació de les persones	aplica
mp.if.3	Condicionament dels locals	aplica
mp.if.4	Energia elèctrica	aplica
mp.if.5	Protecció enfront incendis	aplica
mp.if.6	Protecció enfront inundacions	n.a
mp.if.7	Registre d'entrada i sortida d'equipament	aplica
mp.per	Gestió del personal	
mp.per.1	Caracterització del lloc de treball	n.a.
mp.per.2	Deures i obligacions	aplica
mp.per.3	Conscienciació	aplica
mp.per.4	Formació	aplica
mp.eq	Protecció dels equips	
mp.eq.1	Lloc de treball ordenat	aplica
mp.eq.2	Bloqueig del lloc de treball	n.a.
mp.eq.3	Protecció de dispositius portàtils	aplica
mp.eq.4	Altres dispositius connectats a la xarxa	aplica
mp.com	Protecció de les comunicacions	
mp.com.1	Perímetre segur	aplica
mp.com.2	Protecció de la confidencialitat	aplica
mp.com.3	Protecció de la integritat i de la autenticitat	aplica

mp.com.4	Separació de fluxos de informació en la xarxa	n.a.
mp.si	Protecció dels suports de informació	
mp.si.1	Marcat de suports	n.a.
mp.si.2	Criptografia	n.a.
mp.si.3	Custodia	aplica
mp.si.4	Transport	aplica
mp.si.5	Eliminació i destrucció	aplica
mp.sw	Protecció de les aplicacions informàtiques	
mp.sw.1	Desenvolupament d'aplicacions	n.a
mp.sw.2	Acceptació i posada en servei	aplica
mp.info	Protecció de la informació	
mp.info.1	Dades personals	aplica
mp.info.2	Qualificació de la informació	n.a.
mp.info.3	Firma electrònica	aplica
mp.info.4	Segells de temps	n.a.
mp.info.5	Neteja de documents	aplica
mp.info.6	Copies de seguretat	aplica
mp.s	Protecció dels serveis	
mp.s.1	Protecció del correu electrònic	aplica
mp.s.2	Protecció de serveis i aplicacions web	aplica
mp.s.3	Protecció de la navegació web	aplica
mp.s.4	Protecció enfront a denegació de servei	n.a.

Taula 6. Mesures de seguretat segons la seva aplicabilitat

ANNEX B. 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 de identificació personal utilitzat en certs sistemes, com el telèfon mòbil o el caixer automàtic, per identificar-se i obtenir accessos al sistema. Es un tipus de contrasenya.
Targeta o dispositiu electrònic que utilitza un usuari autoritzat per accedir a un sistema informàtic.

Recovery Point Objective

Marca la freqüència de copies de recolzament. Es refereix al volum de dades en risc de pèrdua que la 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 C. 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/