ENS-STIC-804_S
Guia simplificada d'implementació

(DOCUMENT SUBJECTE A MODIFICACIONS)

Gener 2023

Fitxa del document

Títol	Guia simplificada d'implementació ENS-STIC-804_S

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	25/1/23	26/1/23

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document: ANC-AD

PRÒLEG

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

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
Ministre de Finances i portaveu del Govern

ÍNDEX

1. INTRODUCCIÓ

1. Aquesta guia simplificada estableix unes pautes de caràcter general que són aplicables a entitats de diferent naturalesa, dimensió i sensibilitat sense entrar en casuístiques particulars. Per a la versió completa veure document ENS-STIC-804.

2. NIVELLS DE MADURESA

2. 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

3. 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. MESURES

3.1 [ORG] MARC ORGANITZATIU

[ORG] MARC ORGANIZATIU		
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.		
[ORG.1]	POLÍTICA DE SEGURETAT	És un document d'alt nivell que defineix el significat de "seguretat de la informació" 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.
[ORG.2]	NORMATIVA DE SEGURETAT	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.
[ORG.3]	PROCEDIMIENTS OPERATIUS DE SEGURETAT	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.

[ORG] MARC ORGANIZATIU		
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.		
[ORG.4]	PROCÉS D'AUTORITZACIÓ	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.

Taula 3. Mesures Marc Organitzatiu

3.2 [OP] MARC OPERACIONAL

[OP] MARC OPERACIONAL		
Mesures a prendre per a protegir l'operació del sistema com a conjunt integral de components per a un fi.		
[OP.PL] PLANIFICACIÓ		
Activitats prèvies a la posada en explotació.		
[OP.PL.1]	ANÀLISI DE RISCOS	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.
[OP.PL.2]	ARQUITECTURA DE SEGURETAT	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.
[OP.PL.3]	ADQUISICIÓ DE NOUS COMPONENTS	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 o la implantació inicial. o el manteniment al llarg de la seva vida útil. o atendre a l'evolució de la tecnologia.
[OP.PL.4]	DIMENSIONAMENT / GESTIÓ DE CAPACITATS	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.

[OP.PL.5]	COMPONENTS CERTIFICATS	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 alt 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.
[OP.ACC] CONTROL D'ACCÉS		
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.		
[OP.ACC.1]	IDENTIFICACIÓ	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.).
[OP.ACC.2]	REQUISITS D'ACCÉS	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.
[OP.ACC.3]	SEGREGACIÓ DE FUNCIONS I TASQUES	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.
[OP.ACC.4]	PROCÉS DE GESTIÓ DE DRETS D'ACCÉS	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.
[OP.ACC.5]	MECANISME D'AUTENTICACIÓ	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.

[OP.ACC.6]	ACCÉS LOCAL (LOCAL LOGON)	La major part de les mesures requerides es poden aconseguir simplement configurant els llocs d'usuari segons s'indica.
[OP.ACC.7]	ACCÉS REMOT (REMOTE LOGIN)	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.
[OP.EXP] EXPLOTACIÓ		
[OP.EXP.1]	INVENTARI D'ACTIUS	L'inventari ha de cobrir tot el domini de 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.
[OP.EXP.2]	CONFIGURACIÓ DE SEGURETAT	Tots els sistemes han de ser configurats de manera sistemàtica abans d'entrar en producció.
[OP.EXP.3]	GESTIÓ DE LA CONFIGURACIÓ	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.
[OP.EXP.4]	MANTENIMENT	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.
[OP.EXP.5]	GESTIÓ DE CANVIS	Ha d'existir un procediment per a canviar components del sistema.
[OP.EXP.6]	PROTECCIÓ ENFRONT A CODI NOCIU	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.

[OP.EXP.7]	GESTIÓ D'INCIDENTS	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
[OP.EXP.8]	REGISTRE DE L'ACTIVITAT DELS USUARIS	Es realitza una inspecció regular dels registres per identificar anomalies en l'ús dels sistemes (ús irregular o no previst).
[OP.EXP.9]	REGISTRE DE LA GESTIÓ D'INCIDENTS	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.
[OP.EXP.10]	PROTECCIÓ DELS REGISTRES D'ACTIVITAT	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
[OP.EXP.11]	PROTECCIÓ DE LES CLAUS CRIPTOGRÀFIQUES	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.
[OP.EXT] SERVEIS EXTERNS		

Mesures per a protegir el sistema de possibles perjudicis derivats de la contractació de determinats serveis a proveïdors externs.		
[OP.EXT.1]	CONTRACTACIÓ I ACORDS DE NIVELL DE SERVEI	Ha de realitzar-se una anàlisi de riscos que identifiqui els riscos associats al proveïdor extern.
[OP.EXT.2]	GESTIÓ DIÀRIA	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.
[OP.EXT.3]	MITJANS ALTERNATIUS	La provisió de serveis externs serà part dels plans de continuïtat de l'entitat ([op.cont]).
[OP.CONT] CONTINUÏTAT DEL SERVEI		
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.		
[OP.CONT.1]	ANÀLISI D'IMPACTE	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.
[OP.CONT.2]	PLA DE CONTINUITAT	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.
[OP.CONT.3]	PROVES PERIÒDIQUES	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.
[OP.MON] MONITORITZACIÓ DEL SISTEMA		
El monitoratge del sistema permet detectar atacs i incidents en general habilitant les mesures de reacció i recopilant informació per a analitzar l'incident.		
[OP.MON.1]	DETECCIÓ D'INTRUSIÓ	Cal detectar activitats d'atacants interns i externs, així com l'existència de troians o APTs que poguessin haver-se introduït en el sistema.

[OP.MON.2]	SISTEMA DE MÈTRIQUES	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.

Taula 4. Mesures Marc Operacional

3.3 [MP] MESURES DE PROTECCIÓ

[MP] MESURES DE PROTECCIÓ		
[MP.IF] PROTECCIÓ DE LES INSTAL·LACIONS I INFRAESTRUCTURES		
[MP.IF.1]	ÀREES SEPARADES I AMB CONTROL D'ACCÉS	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.
[MP.IF.2]	IDENTIFICACIÓ DE LES PERSONES	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).
[MP.IF.3]	ACONDICIONAMIENT DELS LOCALS	S'ha de disposar d'unes instal·lacions adequades per a l'eficaç acompliment de l'equipament que s'instal·la en elles.
[MP.IF.4]	ENERGIA ELÈCTRICA	S'han de preveure mesures per a cobrir un possible tall de subministrament elèctric i un correcte funcionament de les llums d'emergència.
[MP.IF.5]	PROTECCIÓ ENFRONT D'INCENDIS	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
[MP.IF.6]	PROTECCIÓ ENFRONT A INUNDACIONS	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

[MP.IF.7]	REGISTRE D'ENTRADA I SORTIDA D'EQUIPAMENT	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
[MP.IF.8]	INSTAL·LACIONS ALTERNATIVES	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.
[MP.PER] GESTIÓ DEL PERSONAL		
Mesures per a protegir el sistema de problemes que poguessin ser causats per les persones que gaudeixen d'accés a aquest.		
[MP.PER.1]	CARACTERITZACIÓ DEL LLOC DE TREBALL	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.
[MP.PER.2]	DEURES I OBLIGACIONS	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.
[MP.PER.3]	CONCIENCIACIÓ	S'ha de conscienciar regularment al personal sobre el seu paper i responsabilitat perquè la seguretat del sistema aconsegueixi els nivells exigits.
[MP.PER.4]	FORMACIÓ	S'ha de formar regularment a les persones en aquelles tècniques que requereixin per a l'acompliment de les seves funcions.
[MP.PER.5]	PERSONAL ALTERNATIU	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.
[MP.EQ] PROTECCIÓ DELS EQUIPS		

[MP.EQ.1]	LLOC DE TREBALL ORDENAT	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.
[MP.EQ.2]	BLOQUEIG DE LLOC DE TREBALL	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.
[MP.EQ.3]	PROTECCIÓ D'EQUIPS PORTÀTILS	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.
[MP.EQ.4]	MITJANS ALTERNATIUS	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.
[MP.COM] PROTECCIÓ DE LES COMUNICACIONS		
[MP.COM.1]	PERÍMETRE SEGUR	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).
[MP.COM.2]	PROTECCIÓ DE LA CONFIDENCIALITAT	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].
[MP.COM.3]	PROTECCIÓ DE L'AUTENTICITAT I DE LA INTEGRITAT	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].

[MP.COM.4]	SEGREGACIÓ DE XARXES	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].
[MP.COM.5]	MITJANS ALTERNATIUS	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.
[MP.SI] PROTECCIÓ DELS SOPORTS D'INFORMACIÓ		
[MP.SI.1]	ETIQUETAT	S'ha d'etiquetar de manera que, sense revelar el seu contingut, s'indiqui el nivell de qualificació més alt de la informació continguda.
[MP.SI.2]	CRIPTOGRAFIA	Aquest requisit s'aplica, en particular, a tots els dispositius extraïbles (com CD, DVD, discos USB, etc.).
[MP.SI.3]	CUSTÒDIA	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.
[MP.SI.4]	TRANSPORT	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.
[MP.SI.5]	BORRAT I DESTRUCCIÓ	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.
[MP.SW] PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES		

[MP.SW.1]	DESENVOLUPAMENT	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.
[MP.SW.2]	ACEPTACIÓ I POSADA EN SERVEI	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.
[MP.INFO] PROTECCIÓ DE LA INFORMACIÓ		
[MP.INFO.1]	DADES DE CARÀCTER PERSONAL	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 de la LQPD (llei qualificada de la protecció de dades)
[MP.INFO.2]	QUALIFICACIÓ DE LA INFORMACIÓ	S'ha d'establir un esquema per a assignar un nivell de qualificació a la informació, en funció de les seves necessitats de confidencialitat.
[MP.INFO.3]	XIFRAT	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.
[MP.INFO.4]	SIGNATURA ELECTRÒNICA	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.

[MP.INFO.5]	SEGELLS DE TEMPS	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.
[MP.INFO.6]	NETEJA DE DOCUMENTS	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 (metadades)
[MP.INFO.7]	COPIES DE SEGURETAT (BACKUP)	S'han de realitzar còpies de seguretat que permetin recuperar dades perdudes accidental o intencionadament amb una antiguitat a determinar per l'entitat.
[MP.S] PROTECCIÓ DELS SERVEIS		
[MP.S.1]	PROTECCIÓ DEL CORREU ELECTRÒNIC (E-MAIL)	Quan s'ofereixi correu electrònic com a part del sistema, haurà de protegir-se enfront de les amenaces que li són pròpies.
[MP.S.2]	PROTECCIÓ DE SERVEIS I APLICACIONS WEB	S'ha de protegir els subsistemes dedicats a la publicació d'informació enfront dels atacs o amenaces que els són pròpies.
[MP.S.3]	PROTECCIÓ ENFRONT LA DENEGACIÓ DE SERVEI	S'han d'establir mesures preventives i reactives enfront d'atacs de denegació de servei (DoS).
[MP.S.4]	MITJANS ALTERNATIUS	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.

Taula 5. Mesures de Protecció

ANNEX A. MESURES DE SEGURETAT

4. 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.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