PLA D’ACTUACIO D’ADEQUACIÓ A L’ESQUEMA NACIONAL DE SEGURETAT (ENS)

INDEX

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

PLA D'ACTUACIO D'ADEQUACIÓ A L'ESQUEMA NACIONAL DE SEGURETAT (ENS)

1 Introducció i antecedents

El present **Pla d'actuació d'adequació a l'Esquema Nacional de Seguretat (ENS)** neix de la necessitat de transformar el diagnòstic d'estat actual en un full de ruta operatiu i executable. El CCM, com a institució pública, gestiona actius d'informació crítics per a la ciutadania que requereixen un nivell de protecció homogeni i robust.

Aquest document s'ha elaborat prenent com a base el resultat de l'**Anàlisi de Riscos**, la **Declaració d'Aplicabilitat (SoA) 2025 i** l'**Informe d'estat d'adequació a l'ENS.**

S'ha identificat que, per assolir la conformitat amb la **categoria mitjana**, el sistema d'informació del CCM ha de donar resposta a 67 controls

L'**Informe d'estat de l'adequació a l'ENS** revela un sòlid punt de partida en el procés d'adequació. El sistema ja compta amb **37 controls completats** i **7 de forma parcial**, d'un total de 67. Això indica que més de la meitat de les mesures necessàries per a la categoria mitjana ja estan definides i procedimentades. En l'annex 1 es detallen les mesures executades completament o de manera parcial.

Pel que fa als 33 controls restants, requereixen una intervenció directa per a la seva implantació o millora.

2 Fonaments tècnico-jurídics

L'adequació a l'ENS no és només un exercici de seguretat informàtica, sinó un imperatiu legal vinculat al funcionament de l'Administració Digital. El marc normatiu que sustenta aquest pla es divideix en tres nivells:

Marc Legal Estatal i Europeu

- **Real Decreto 311/2022 (ENS):** És la norma matriu que regula els principis bàsics i els requisits mínims de seguretat per a la protecció de la informació i els serveis del sector públic.
- **Lleis 39/2015 i 40/2015:** Estableixen l'obligatorietat de l'ús dels mitjans electrònics i la responsabilitat de les administracions sobre els serveis digitals.
- **Reglament (UE) 2016/679 (RGPD):** La seguretat de l'ENS és la base tècnica que garanteix la confidencialitat i integritat de les dades de caràcter personal.

Marc Autonòmic i Local

- **Llei 29/2010 i Decret 76/2020 de Catalunya:** Normativa específica sobre l'administració digital al territori català que reforça el model de governança TIC.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- **Normativa Interna del CCM:** El pla es complementa amb els procediments, manuals operatius i instruccions de treball propis de l'organització.

Fonament Tècnic

El pla es basa en la **traçabilitat documental**. Això vol dir que cada acció tècnica executada (com el xifratge o el monitoratge) ha de correspondre directament a un control de seguretat definit a l'Annex II del RD 311/2022, garantint que el sistema sigui auditable en qualsevol moment.

3 Relació entre el Pla d'Actuació ENS i el Pla d'Acció en matèria de Protecció de Dades (LOPDGDD i RGPD)

3.1 Marc de complementarietat normativa

El Pla d'Actuació d'Adequació a l'Esquema Nacional de Seguretat (ENS) i el Pla d'Acció en matèria de Protecció de Dades de Caràcter Personal (LOPDGDD i Reglament (UE) 2016/679) constitueixen **dos instruments normatius diferenciats però intrínsecament complementaris** dins del model de governança de la informació del Consell Comarcal del Maresme.

Mentre que l'ENS estableix els **principis, requisits i mesures tècniques i organitzatives** necessàries per garantir la seguretat dels sistemes d'informació, la normativa de protecció de dades regula el **tractament lícit, lleial i segur de les dades personals**, amb especial atenció als drets de les persones interessades.

En aquest sentit, l'ENS actua com a **base tècnica i operativa** que permet donar compliment efectiu a les obligacions establertes a l'article 32 del RGPD, relatiu a la seguretat del tractament.

3.2 Alineació d'objectius entre ENS i LOPDGDD

Els objectius del Pla d'Actuació ENS es troben plenament alineats amb els del Pla d'Acció LOPDGDD, especialment en relació amb:

- La **confidencialitat** de la informació i de les dades personals.
- La **integritat** dels sistemes i dels conjunts de dades.
- La **disponibilitat** dels serveis i la capacitat de recuperació davant incidències.
- La **traçabilitat** de les actuacions i responsabilitats.
- La **gestió dels riscos** associats al tractament de dades personals.

Aquesta alineació garanteix que les mesures implantades en el marc de l'ENS **no siguin redundants**, sinó que reforcin i operativitzin les obligacions derivades del RGPD i la LOPDGDD.

3.3 Correspondència entre mesures ENS i mesures del Pla d'Acció LOPDGDD

El Pla d'Actuació ENS dona suport directe a diverses línies del Pla d'Acció LOPDGDD, especialment a les relatives a les **mesures comunes de seguretat** i a les **mesures específiques per àmbits funcionals**.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Consell Comarcal del **Maresme**

A títol exemplificatiu:

- **Gestió d'accessos i identitats (ENS – op.acc.*)**
  Dona suport a les mesures LOPDGDD relatives al control d'accés del personal, el principi de necessitat de conèixer i la limitació de l'accés a dades personals.

- **Gestió d'incidents i violacions de seguretat (ENS – op.exp.7, op.exp.9)**
  Constitueix la base operativa per a la detecció, anàlisi i notificació de violacions de seguretat de dades personals, d'acord amb els articles 33 i 34 del RGPD.

- **Còpies de seguretat i continuïtat del servei (ENS – mp.info.6, mp.if.*)**
  Assegura la disponibilitat i resiliència dels sistemes que tracten dades personals, tal com exigeix l'article 32 del RGPD.

- **Xifratge i protecció de la informació (ENS – mp.si.*)**
  Dona compliment a les mesures tècniques de protecció de dades personals en repòs i en trànsit.

- **Registre i traçabilitat (ENS – op.exp.8)**
  Facilita la responsabilitat proactiva (*accountability*) exigida per la normativa de protecció de dades.

3.4 Governança conjunta i rols de responsabilitat

El desplegament del Pla d'Actuació ENS es realitza en coordinació amb els òrgans i figures previstes al Pla d'Acció LOPDGDD, en particular:

- El **Comitè de Seguretat de la Informació**, com a òrgan de seguiment i decisió.
- El **Delegat/da de Protecció de Dades (DPD)**, com a figura clau d'assessorament, supervisió i garantia dels drets de la ciutadania.
- Les unitats gestores, com a responsables de l'aplicació efectiva de les mesures en els seus respectius àmbits.

Aquesta governança compartida evita duplicitats, reforça la coherència de les decisions i consolida una visió integrada de la seguretat de la informació i la protecció de dades.

3.5 Valor afegit institucional

La integració entre el Pla d'Actuació ENS i el Pla d'Acció LOPDGDD permet al Consell Comarcal del Maresme disposar d'un **model de governança de la informació coherent i sostenible**, alineat amb les exigències legals i amb les expectatives de la ciutadania en matèria de seguretat, transparència i protecció dels seus drets.

4 Objectius del Pla d'Actuació

L'objectiu principal és establir un conjunt d'actuacions **ordenades, traçables i verificables** per mantenir el compliment de l'ENS. En detall, es persegueixen les fites següents:

- **Planificació Operativa:** Programar l'execució de les mesures de seguretat segons la seva criticitat i l'impacte en el servei.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- **Definicó d'Accions:** Documentar què es fa, com es fa i quins elements (programari o maquinari) es necessiten per a cada control.
- **Governança i Seguiment:** Habilitar un mecanisme de control intern que permeti al Comitè de Seguretat conèixer l'estat d'adequació en temps real.
- **Preparació per a l'Auditoria:** Assegurar que existeixen evidències suficients per superar amb èxit les auditories externes de certificació.

5 Actuacions a dur a terme

A continuació, es detalla la proposta d'execució dels controls identificats com a necessaris per a l'adequació del sistema d'informació del Consell Comarcal del Maresme (CCM) a la categoria mitjana de l'ENS.

Aquesta anàlisi organitza els 33 controls pendents segons la seva naturalesa tècnica i operativa.

a) Bloc de mesures crítiques (Prioritat immediata)

Aquestes accions s'han d'abordar de forma urgent per mitigar els riscos de major impacte en la continuïtat del servei i la integritat de les dades.

Codi	Nom del control	Accions previstes i justificació
mp.info.6	**Còpies de seguretat**	Documentar la política de còpies i, sobretot, establir un calendari de proves de restauració per garantir que les dades són recuperables en cas de desastre[4].
op.mon.3	**Vigilància**	Implantar un sistema de correlació d'esdeveniments (SIEM) com Wazuh i renovar el conveni amb l'Agència de Ciberseguretat de Catalunya per a la vigilància activa[5].
mp.com.4	**Separació de fluxos**	Dissenyar i implementar una estructura de xarxa basada en VLANs per evitar moviments laterals d'amenaces dins de la xarxa del CCM[6].
op.exp.4	**Manteniment i actualitzacions**	Actualitzar el parc informàtic a Windows 11 o versions suportades i desplegar un sistema de gestió centralitzada de parches de seguretat[7].
mp.com.1	**Perímetre segur**	Actualitzar i llicenciar el tallafoc (firewall), activant els sistemes de detecció d'intrusions (IDS) i enviant els registres al SIEM[8].
op.exp.8	**Registre de l'activitat**	Establir alertes automàtiques per accessos anòmals o reiterats i garantir la retenció de logs durant un mínim de 6 mesos amb seguretat de temps (timestamp)[9].

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Codi	Nom del control	Accions previstes i justificació
mp.if.4	**Energia elèctrica**	Manteniment del SAI (Sistema d'Alimentació Ininterrompuda) i integració en el sistema de monitoratge per evitar caigudes brusques del sistema[10].

b) Bloc d'accés i protecció física (curt termini)

Mesures centrades en qui pot accedir a la informació i com es protegeixen els equips físics.

Codi	Nom del control	Accions previstes i justificació
op.acc.1, 5, 6	**Identificació i Autenticació**	Implementació obligatòria del doble factor d'autenticació (2FA) per a l'accés extern i Google Workspace, a més de restringir l'accés a través de VPN per a personal extern
mp.if.1, 2, 3	**Seguretat Física del CPD**	Tancament físic del centre de dades, instal·lació de sensors de temperatura/humitat amb alertes i creació d'un protocol de control d'accés a les claus.
op.exp.2, 3	**Gestió de la Configuració**	Elaborar guies de configuració segura ("hardening") per a cada tipus d'equip (PCs i servidors) per evitar vulnerabilitats per defecte.
Esborrat Segur	**mp.si.5**	Implantar l'eina "Olvido" o similar per garantir que la informació dels dispositius retirats s'elimina de forma irrecuperable

c) Bloc de Governança i organització (mitjà termini)

Actuacions destinades a la maduresa del sistema i la seva traçabilitat a llarg termini.

Codi	Nom del control	Accions previstes i justificació
op.exp.1	**Inventari Automatitzat**	Desplegar eines que detectin en temps real quins equips hi ha connectats a la xarxa, integrant-ho amb la seguretat centralitzada (com Gravity Zone).
op.nub.1	**Protecció al Núvol**	Establir revisions periòdiques per verificar que els proveïdors de serveis al núvol (SaaS) compleixen amb les mesures de seguretat exigides.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Codi	Nom del control	Accions previstes i justificació
mp.si.2, 3, 4	**Criptografia i Transport**	Sistematitzar el xifratge de portàtils i definir clarament qui és el responsable de la custòdia d'un dispositiu quan surt de la seu del CCM.
mp.si.1, mp.info.5	**Marcatge i Neteja d'Informació**	Establir com es classifica la documentació (púbica, interna, confidencial) i assegurar que els documents web no contenen metadades ocultes.

5.1 Fitxa tècnica d'actuacions ENS

A continuació, es presenta una **fitxa tècnica detallada** que agrupa els controls pendents segons la seva naturalesa operativa. Aquesta estructura permet conèixer exactament què s'ha de fer en cadascuna de les àrees (sistemes, xarxes, gestió), la prioritat i els recursos necessaris segons el pla definit.

Àrea 1: Infraestructura crítica i continuïtat

Aquestes accions garanteixen que el "cor" informàtic estigui protegit contra fallades físiques o pèrdues de dades.

Codi Control	Acció Detallada	Criticitat	Recursos
mp.info.6	**Política de Backup**: Documentar la política de còpies i establir una sistemàtica de proves de restauració periòdica. 4	Crític	Llicència + Inversió + Personal
mp.if.4	**Energia (SAI)**: Contractar manteniment del SAI, revisar bateries i integrar-lo al sistema de monitoratge. 5	Crític	Inversió
mp.if.1, 2, 3	**CPD Segur**: Tancar físicament el CPD, moure la central d'alarmes, etiquetar cablejat i instal·lar sensors de temp/humitat. 6	Curt termini	Inversió + Procediment

Àrea 2: Control d'accés i gestió d'identitats

L'objectiu és assegurar que només les persones autoritzades accedeixin a la informació i des d'entorns segurs.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Codi Control	Acció Detallada	Criticitat	Recursos
op.acc. 1	**Doble Factor** (2FA): Activar 2FA a Google Workspace i accessos externs. Forçar VPN per a usuaris externs i implantar GPO per a missatges d'obligacions d'ús.	Curt termini	Llicència + Personal
op.acc. 5, 6	**Mecanismes d'Autenticació**: Definir i implementar els mètodes segurs per a usuaris interns i externs.	Curt termini	Llicències + Personal
op.exp. 2, 3	**Hardening**: Crear documents de "plataformat" (configuració segura) per a equips i servidors, i fer mostrejos periòdics de compliment.	Curt termini	Personal

Àrea 3: Vigilància, operació i xarxa

Controls destinats a detectar atacs en temps real i mantenir els sistemes actualitzats contra vulnerabilitats.

Codi Control	Acció Detallada	Criticitat	Recursos
op.mon.3	**SIEM/SOC:** Desplegar Netskope (CataloniaSOC) i el sistema de correlació d'esdeveniments Wazuh (OpenSource). 14	Crític	Conveni + Llicència + Personal
mp.com.4	**Segregació de Xarxa**: Dissenyar i implementar VLANs segures per separar els fluxos d'informació. 15	Crític	Personal (Configuraci ó)
op.exp.4	**Actualitzacions**: Passar a versions suportades (Windows 11) i desplegar gestió centralitzada de parches. 16	Crític	Inversió + Personal
mp.com.1	**Firewall**: Contractar llicència de suport, activar IDS (Detecció d'Intrusions) i enviar logs al SIEM. 17	Crític	Inversió + Llicència
op.exp.8	**Logs**: Retenció mínima de 6 mesos, sincronització de rellotge (NTP) i sistema d'alarmes per accessos reiterats. 18	Crític	Llicències + Personal

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Àrea 4: Governança i gestió de la Informació

Documentació i polítiques que donen suport legal i organitzatiu a la seguretat del CCM.

Codi Control	Acció Detallada	Criticitat	Recursos
org.3	Procediments: Actualitzar documentació de hardening i gestió de firewall/servidors amb revisions semestrals. 21	Crític	Personal (Documentació)
op.exp.1	Inventari Actius: Automatitzar l'inventari en temps real (endpoints, xarxa, servidors) integrat amb eines SIEM. 22	Mitjà termini	Llicència + Personal
mp.si.5	Esborrat Segur: Implantar eines d'esborrat certificat (eina Olvido) per a dispositius en desús. 23	Curt termini	Llicència + Personal
mp.info.2, 5	Classificació: Establir criteris de classificació de la informació i neteja automàtica de metadades en fitxers web. 24	Curt termini / Mitjà	Personal (Documentació)

Resum de les accions crítiques

Segons el pla, hi ha 10 controls crítics que formen la base del compliment. L'ordre d'execució recomanat és prioritzar aquells que combinen la criticitat amb la prevenció d'atacs externs (Firewall, SIEM, 2FA) i la recuperació de dades (Backup, SAI).

6 Cronograma d'adequació a l'ENS

A continuació, es presenta la proposta de calendari mensualitzat per a l'any 2026. Aquest cronograma està dissenyat per prioritzar els **10 controls crítics** durant el primer trimestre, assegurant que els riscos més alts quedin coberts al més aviat possible.

Fase 1: Implementació crítica (Gener - Març)

L'objectiu és mitigar els riscos més alts i establir els controls de supervisió base.

- **Mes 1:**
  - **Acció:** Formalització de la política de **Còpies de Seguretat** i proves restauració (mp.info.6).
  - **Supervisió:** Primera prova real de restauració de dades crítiques.
  - **Manteniment:** Revisió física i tècnica del **SAI** (mp.if.4).

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- **Mes 2:**
    - **Acció:** Implementació del **SIEM** (Wazuh) i renovació del conveni amb **l'Agència de Ciberseguretat**. (op.mon.3).
    - **Acció**: Definició de Mètriques Base de Vigilància. Establir els llindars d'alerta inicials (intents de login, accessos fora d'hores, canvis de privilegis) per evitar el soroll excessiu des del primer dia. (op.mon.2).
    - **Acció:** Actualització de llicències i activació de l'IDS al **Firewall** (mp.com.1).
    - **Supervisió:** Configuració d'alertes automàtiques per intents d'accés fallits.
- **Mes 3:**
    - **Acció:** Segmentació de xarxa mitjançant **VLANs** (mp.com.4).
    - **Acció:** Redacció de guies de **Hardening** i **de Servidors i Equips Crítics**. (configuració segura) (op.exp.2-3).
    - **Supervisió:** Auditoria de l'inventari per identificar equips obsolets restants.

Fase 2: Control d'Accés i Seguretat Física (Abril - Juny)

Focalitzat en la protecció de la identitat i l'entorn físic del CPD.

- **Mes 4:**
    - **Acció:** Implantació del **Doble Factor** d'Autenticació **(2FA)** i configuració de VPN obligatòria. (op.acc.1,5,6).
    - **Acció:** Inici del pla de renovació del **parc informàtic** a Windows 11 (op.exp.4).
    - **Acció**: Configuració de la retenció de registres (logs) i sincronització horària ENS (op.exp.8)
    - Supervisió: Revisió semestral d'autoritzacions d'accés (perfils d'usuari vs funcions).
- **Mes 5:**
    - **Acció:** Adequació física del **CPD**: tancament, sensors i alarmes (mp.if.1-3).
    - **Acció:** Adquisició i posada en marxa de l'eina d'esborrat segur (Olvido) (mp.si.5)
    - **Supervisió:** Inspecció del llibre de registre d'entrada a la sala de servidors.
- **Mes 6:**
    - **Acció:** Documentació dels procediments de posada en producció de programari (mp.sw.2)
    - **Supervisió:** Verificació tècnica d'una mostra d'equips per comprovar el compliment del hardening.

Fase 3: Gestió de la informació i tercers (Juliol - Setembre)

Consolidació de la governança i el control sobre proveïdors externs.

- **Mes 7:**
    - **Acció:** Definició dels criteris de **Classificació de la Informació** (mp.info.2).

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- o **Acció:** Actualització de tota la documentació de seguretat segons la nova operativa (org.3)
- o **Supervisió:** Revisió del registre de canvis (Jira) del primer semestre.

- **Mes 8:**
  - **Acció:** Implementació del sistema de **marcatge de documents** segons nivell seguretat (mp.si.1).
  - **Acció:** Automatització de l'**Inventari d'Actius** (op.exp.1).
  - **Acció:** Creació del registre formal d'entrada i sortida d'equipament. (mp.if.7)
  - **Supervisió: Avaluació de proveïdors externs**: verificació de certificats ENS i compliment de SLA.

Fase 4: Auditoria, xifratge i tancament (Octubre - Desembre)

Garantia de la traçabilitat final i preparació per a l'auditoria externa.

- **Mes 9:**
  - **Acció:** Optimització i Automatització del Sistema de Mètriques Refinament dels indicadors basat en l'històric de dades recollides des del febrer i generació de quadres de comandament (dashboards) per a la Comissió de Seguretat. (op.mon.2).
  - **Acció:** Implementació de polítiques de **Xifratge i Custòdia** de portàtils (mp.si.2-4).
  - **Acció:** Revisió de seguretat de tots els serveis contractats al núvol (SaaS). (op.nub.1)
- **Mes 10:**
  - **Acció:** Neteja de metadades en documents web (mp.info.5).
  - **Supervisió:** Verificació de la retenció de logs (6 mesos) i sincronització NTP (op.exp.8).
- **Mes: 11**
  - **Acció: Informe Anual de Seguretat**: Recopilació de mètriques i verificació de la traçabilitat entre l'Anàlisi de Riscos, la SoA i les evidències generades per a la Comissió de Seguretat
  - **Supervisió:** Revisió final de la Declaració d'Aplicabilitat (SoA) per a l'auditoria 2027 i preparació de la memòria anual per a la Comissió de Seguretat

6.1 Calendari de supervisió i control (Periodicitat)

A partir de l'anàlisi dels documents de gestió del Consell Comarcal del Maresme (CCM), s'ha dissenyat un calendari tècnic que sistematitza les **mesures de control i supervisió**.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

L'objectiu d'aquest calendari és passar d'una gestió puntual a una **vigilància contínua**, tal com exigeix l'ENS en categoria mitjana.

Aquest calendari organitza les tasques segons la seva recurrència per garantir que cap control quedi desatès.

a) Controls diaris / automatitzats (Monitoratge en temps real)

Aquests controls es basen en sistemes que generen alertes si detecten una anomalia.

- **Vigilància de vulnerabilitats:** Revisió diària de fonts oficials de ciberseguretat per detectar pegats d'urgència que afectin la infraestructura del CCM. (op.exp.4)
- **Vigilància d'incidents (SIEM/SOC):** Monitoratge d'alertes de seguretat i intents d'intrusió (op.mon.3).
- **Estat de les còpies de seguretat:** Verificació diària del log d'execució dels backups (mp.info.6).
- **Disponibilitat de serveis:** Monitoratge de caigudes de servidors o de la climatització del CPD (mp.if.3).

b) Controls quinzenals (Revisió incidències)

Aquest control té per objecte garantir la continuïtat operativa dels serveis, així com la supervisió i gestió de les incidències

- **Gestió de Canvis i seguiment d'incidències i peticions (op.exp.5):** Revisió dels tiquets a JIRA per assegurar que tot canvi a producció ha estat degudament autoritzat, control i registre de canvis no autoritzats.

c) Controls mensuals (Revisió Operativa)

Tasques per assegurar el compliment del dia a dia de l'equip tècnic.

- **Registre d'equips (mp.if.7):** Conciliació de les entrades i sortides d'equipament físic de les instal·lacions. *La supervisió mensual s'iniciarà un cop implementat el registre (desembre o gener del següent any*).
- **Afinament del SIEM (op.mon.2/3):** Revisió dels falsos positius generats pel SIEM durant el mes i ajust dels llindars de les mètriques per mantenir el soroll sota control.
- **Actualitzacions (op.exp.4):** Verificació de l'estat *global* del parc informàtic i validació del cicle mensual de pegats.

  Nota: Amb independència de la revisió mensual, els pegats qualificats com a crítics per l'Agència de Ciberseguretat de Catalunya s'aplicaran en un termini màxim de 72 hores"

d) Controls Trimestrals (Validació Tècnica)

Controls que requereixen una acció proactiva de verificació.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- **Proves de Restauració (mp.info.6):** Prova real de recuperació de dades d'una de les còpies per garantir que són llegibles.
- **Mostreig de Hardening (op.exp.2):** Revisió aleatòria d'equips per comprovar que la configuració de seguretat no ha estat alterada.
- **Control de claus i sensors:** Prova física dels sistemes d'alarma i verificació de la custòdia de claus del CPD.

e) Controls Semestrals (Supervisió d'Accessos)

Revisions centrades en la governança de la identitat.

- **Auditoria de Drets d'Accés (op.acc.2):** Revisió de les altes, baixes i canvis de permisos. Eliminació de comptes d'usuaris que ja no formen part de l'organització.
- **Revisió de Privilegis Especials:** Verificació de l'ús de comptes d'administrador.

f) Controls Anuals (Governança i Tercers)

Accions de tancament i planificació estratègica.

- **Avaluació de Proveïdors:** Revisió dels contractes de tercers i verificació que mantenen les seves certificacions ENS (mp.s.4).
- **Anàlisi de Riscos i Impacte (op.pl.1):** Actualització formal del document de riscos davant de nous actius o amenaces.
- **Informe Anual de Seguretat:** Elaboració del resum de mètriques per a la Comissió de Seguretat.

7 Estimació pressupostària d'adequació ENS

A partir de les accions definides en el Pla d'actuació i els tipus de costos identificats per a cada control, s'ha elaborat una estimació pressupostària detallada.

S'han dividit les partides en Inversions (CAPEX), que són despeses puntuals per posar al dia la infraestructura, i Despeses Operatives (OPEX), que són llicències o serveis anuals.

Partida Presupostària	Descripció de la despesa	Controls ENS vinculats	Estimació Econòmica (€)
Infraestructura Física	Tancament CPD, sensors de temperatura, renovació de bateries SAI i millora de cablejat	mp.if.1, mp.if.3, mp.if.4	4.500€ - 7.000€

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Partida Presupostària	Descripció de la despesa	Controls ENS vinculats	Estimació Econòmica (€)
Renovació de Maquinari	Actualització del parc informàtic (PCs/Servidors) per suportar versions amb manteniment (1)	op.exp.4, op.pl.5	Condicionat a l'inventari i avaluació dels equips actuals
Seguretat Perimetral	Llicència de suport Firewall, activació IDS i llicències de VPN segura.	mp.com.1, mp.com.3	3.000€ - 5.500€
Vigilància i SIEM	Implementació de Wazuh (OpenSource, cost d'implantació) i quota SOC Catalunya	op.mon.3, op.exp.1	4.000€ - 8.000€
Identitat i Accés	Llicències per al Doble Factor d'Autenticació (2FA) i gestió centralitzada	op.acc.1, op.acc.5	2.500€ - 4.500€
Eines Específiques	Llicència d'esborrat segur (Olvido) i sistemes de mètriques	mp.si.5, op.mon.2	1.000€ - 2.500€
Costos recurrents (anuals)	Serveis al núvol, anualitats llicències, etc.	Depenent de les solucions adoptades	

(1) El cost de renovació del parc dependrà del volum d'equips que no admetin Windows 11 o versions equivalents segons el pla d'homogeneïtzació

7.1 Detall dels tipus de recursos

El pla preveu que moltes accions no tinguin un cost econòmic directe en factures de proveïdors, sinó en **hores de personal intern**:

1. Inversió i llicenciament (Cost econòmic directe)

- **Adquisició de components certificats pel CCN:** Obligatori per a tallafocs i antivirus en categoria mitjana.
- **Serveis al núvol:** Revisió de les mesures de protecció i llicenciament SaaS amb certificats eIDAS.

CSV: [redacted]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

2. Recursos Interns (Cost d'oportunitat/hores)

- **Elaboració documental:** Es requereix personal per redactar els procediments de seguretat, classificació d'informació i polítiques de neteja de documents.
- **Configuració tècnica:** Tasques de "hardening" (configuració segura), definició de VLANs i automatització de l'inventari.

7.2 Resum de criticitat pressupostària

Hi ha un total de **33 controls que requereixen actuacions**. Segons la taula de criticitat del document:

- **10 controls són crítics:** Requereixen la major part de la inversió inicial (SAI, Firewall, SIEM, Backups).
- **13 controls a curt termini:** Centrats en llicències de programari (2FA, esborrat segur).
- **10 controls a mitjà termini:** Principalment hores de personal per a procediments i marcatge.

8 Mesures de control i supervisió

A partir de l'anàlisi del **Manual de procediments del marc operacional** i del document de **Mesures de protecció de les TIC**, s'han identificat les accions i mesures de control de supervisió dissenyades per garantir el compliment dels protocols de l'ENS al Consell Comarcal del Maresme.

Aquestes mesures s'han tipificat segons la seva funció (preventiva, de monitoratge o d'auditoria i es relacionen amb el seu procediment d'origen:

Àmbit: Gestió de la infraestructura i accessos

Procediment: *Procediment d'autorització i gestió de la infraestructura tecnològica*

- **Acció: Revisió periòdica d'autoritzacions d'accés**
  - **Tipus:** Supervisió de compliment (Auditoria interna).
  - **Què s'ha de fer:** Verificar semestralment que els permisos d'accés als sistemes i carpetes de xarxa coincideixen amb les funcions actuals de cada treballador.
  - **Objectiu:** Garantir el principi de "mínim privilegi", assegurant que ningú tingui accés a informació que no li correspon per la seva feina.

- **Acció: Control de lliurament i devolució d'equips mòbils**
  - **Tipus:** Control operatiu (Preventiu).

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- **Què s'ha de fer:** Supervisar que cada dispositiu lliurat estigui vinculat a un document d'acceptació signat que inclogui les obligacions de seguretat.
- **Objectiu:** Mantenir l'inventari actualitzat i assegurar que l'usuari és conscient de la seva responsabilitat sobre l'actiu.

Àmbit: Configuració i manteniment

Procediment: *Procediment per a la gestió de la configuració i manteniment*

- **Acció: Verificació de la configuració de seguretat (Hardening)**
  - **Tipus:** Supervisió tècnica (Monitoratge).
  - **Què s'ha de fer:** Realitzar comprovacions periòdiques sobre una mostra d'equips per confirmar que mantenen els paràmetres de seguretat establerts (antivirus actiu, xifratge, sense programari prohibit).
  - **Objectiu:** Evitar la "degradació" de la seguretat dels equips amb el pas del temps o per manipulacions de l'usuari.

- **Acció: Supervisió del registre de canvis**
  - **Tipus:** Control de traçabilitat (Auditoria).
  - **Què s'ha de fer:** Revisar que tots els canvis significatius en la infraestructura estiguin documentats a l'eina de tiquets (Jira) i hagin estat validats.
  - **Objectiu:** Garantir que no es realitzen modificacions no autoritzades que puguin comprometre l'estabilitat o la seguretat del sistema.

Àmbit: Protecció física i d'instal·lacions

Procediment: Mesures de protecció de les TIC (Instal·lacions)

- **Acció: Revisió del registre d'accés a la sala de servidors**
  - **Tipus:** Supervisió física (Detectiva).
  - **Què s'ha de fer:** Inspeccionar el llibre de registre o els logs del sistema de control d'accessos al CPD per identificar entrades no habituals o de personal no autoritzat.
  - **Objectiu:** Prevenir i detectar manipulacions físiques sobre el maquinari crític de l'organització.

- **Acció: Verificació de sistemes de suport (SAI i Climatització)**
  - **Tipus:** Manteniment preventiu (Operatiu).
  - **Què s'ha de fer:** Comprovar l'estat de les bateries del SAI i el funcionament dels sensors de temperatura de forma programada.
  - **Objectiu:** Garantir la continuïtat del servei davant d'incidències elèctriques o ambientals.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

Àmbit: Gestió de serveis externs

Procediment: Procediment per gestionar els serveis externs

- **Acció: Supervisió del compliment de l'SLA i seguretat de proveïdors**
    - **Tipus:** Supervisió contractual (Auditoria de tercers).
    - **Què s'ha de fer:** Avaluar anualment si els proveïdors externs compleixen amb els nivells de servei signats i si mantenen les seves certificacions de seguretat (com l'ENS).
    - **Objectiu:** Assegurar que la subcontractació de serveis no esdevingui una baula feble en la cadena de seguretat del CCM.

Àmbit: Governança i millora contínua

Procediment: *Procediment de revisió del sistema per la direcció*

- **Acció: Elaboració de l'informe anual de seguretat**
    - **Tipus:** Supervisió estratègica (Governança).
    - **Què s'ha de fer:** Recopilar mètriques d'incidents, resultats d'auditories i estat dels riscos per presentar-los a la Comissió de Seguretat.
    - **Objectiu:** Permetre que la direcció prengui decisions informades sobre inversions i canvis en la política de seguretat basant-se en dades reals.

9 Sistema d'indicadors de compliment i seguiment (KPIs ENS)

9.1 Finalitat dels indicadors ENS

Amb l'objectiu de garantir l'aplicació efectiva, continuada i verificable de les mesures de seguretat establertes a l'Esquema Nacional de Seguretat (ENS), el Consell Comarcal del Maresme estableix un **sistema d'indicadors clau de rendiment (KPIs)**.

Aquest sistema permet:

- Mesurar de manera objectiva el **grau real de compliment** dels controls ENS.
- Facilitar el **seguiment periòdic** per part del Comitè de Seguretat.
- Disposar d'**evidències mesurables** per a auditories internes i externes.
- Detectar desviacions, riscos emergents o relaxacions en l'aplicació dels controls.
- Donar suport al **cicle de millora contínua** del Sistema de Gestió de Seguretat de la Informació (SGSI).

Els indicadors no substitueixen els controls, sinó que **en validen l'eficàcia operativa**.

9.2 Principis del sistema d'indicadors

El sistema de KPIs ENS es regeix pels principis següents:

- **Traçabilitat ENS**: cada indicador està vinculat a un o diversos controls de l'Annex II del RD 311/2022.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça
https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

- **Simplicitat i utilitat**: es prioritzen indicadors comprensibles, mesurables i accionables.
- **Periodicitat definida**: cada indicador té associada una freqüència de revisió.
- **Responsabilitat assignada**: cada KPI té un responsable funcional del seu seguiment.
- **Evolució temporal**: els indicadors permeten analitzar tendències, no només fotografies puntuals.

9.3 Conjunt inicial d'indicadors (KPIs mínims ENS)

El CCM estableix com a **conjunt mínim inicial** els indicadors següents, sense perjudici de la seva ampliació futura:

a) Indicadors de protecció i operació tècnica

Indicador	Control ENS vinculat	Descripció
% d'equips amb actualitzacions de seguretat al dia	op.exp.4	Percentatge d'equips amb sistema operatiu i parches actualitzats
Temps mitjà d'aplicació de parches crítics	op.exp.4	Dies entre publicació del parche i desplegament
% d'equips amb xifratge actiu	mp.si.2, mp.si.3	Especialment portàtils i dispositius mòbils
Estat de salut del SAI	mp.if.4	Disponibilitat, bateries i alertes

b) 3.2. Indicadors de vigilància i detecció

Indicador	Control ENS vinculat	Descripció
Nombre d'incidents de seguretat detectats	op.mon.3	Incidents registrats pel SIEM
Temps mitjà de detecció d'incidents	op.mon.3	Interval entre esdeveniment i detecció
% de logs centralitzats al SIEM	op.exp.8	Sistemes amb enviament correcte de registres
Compliment de la retenció mínima de logs	op.exp.8	≥ 6 mesos segons ENS

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

c) Indicadors d’identitat i control d’accés

Indicador	Control ENS vinculat	Descripció
% d’usuaris amb doble factor d’autenticació	op.acc.1	Especialment accessos externs i serveis crítics
Nombre d’intents d’accés no autoritzats	op.acc.5, op.acc.6	Detectats i bloquejats
Temps de baixa d’accessos en cessaments	op.acc.4	Temps entre baixa administrativa i tècnica

d) Indicadors de continuïtat i recuperació

Indicador	Control ENS vinculat	Descripció
% de còpies de seguretat correctes	mp.info.6	Resultat dels backups programats
Nombre de proves de restauració realitzades	mp.info.6	Proves documentades anuals
Temps mitjà de restauració (RTO)	mp.info.6	En proves o incidents reals

e) Indicadors de governança i organització

Indicador	Control ENS vinculat	Descripció
% de controls ENS amb evidències actualitzades	org.3	Evidències disponibles i vigents
Grau de compliment del cronograma ENS	Pla d’Actuació	Accions executades vs planificades
Nombre de revisions documentals realitzades	org.3	Polítiques i procediments
% d’incidències i peticions relacionades amb els sistemes d’informació que són resoltes dins dels terminis definits.	op.exp.7, op.exp.9, op.mon.2	Registre i traçabilitat d’incidents Mètriques i monitoratge

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

4. Periodicitat i mecanisme de seguiment

- Els indicadors es revisaran amb **periodicitat trimestral**, sense perjudici d'indicadors crítics amb seguiment mensual.
- Els resultats es presentaran al **Comitè de Seguretat** mitjançant un quadre de comandament sintètic.
- Les desviacions significatives generaran **accions correctores** o preventives, degudament documentades

10 Governança coordinada del Pla d'Actuació ENS i del Pla d'Acció LOPDGDD

10.1 Enfocament de governança integrada

El desplegament del Pla d'Actuació d'Adequació a l'Esquema Nacional de Seguretat (ENS) i del Pla d'Acció en matèria de Protecció de Dades (LOPDGDD i RGPD) es fonamenta en un **model de governança integrada**, orientat a garantir una aplicació coherent, eficient i verificable de les mesures de seguretat i protecció de dades del Consell Comarcal del Maresme.

Aquest model parteix del principi que la seguretat de la informació i la protecció de dades personals són **dimensions complementàries d'un mateix sistema**, amb riscos, processos i responsabilitats compartides.

10.2 Òrgans i rols clau

Comitè de Seguretat de la Informació
És l'òrgan col·legiat de supervisió i seguiment del sistema. Li correspon:

- Fer el seguiment del Pla d'Actuació ENS i de la seva coherència amb el Pla d'Acció LOPDGDD.
- Analitzar els indicadors de compliment i les desviacions.
- Impulsar accions correctores i de millora.
- Elevar informació periòdica als òrgans directius.

Responsable del servei

Vetllar pel compliment de les polítiques i normes de seguretat determinades pel Consell i garantir la disponibilitat dels recursos necessaris per al compliment del Pla d'Actuació.

Delegat/da de Protecció de Dades (DPD)
Exerceix funcions d'assessorament i supervisió en matèria de protecció de dades, vetllant perquè les mesures ENS siguin coherents amb el RGPD i la LOPDGDD, especialment en la gestió de riscos i de violacions de seguretat de dades personals.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

10.3 Responsables tècnics, funcionals i responsable de privadesa

El responsable del sistema, els serveis tècnics informàtics, i la responsable de privadesa, en el marc del Pla d'Acció LOPDGDD, són els encarregats de l'aplicació operativa de les mesures previstes als dos plans.

De manera coordinada, els correspon:

- Aplicar les mesures ENS als sistemes, serveis i processos sota la seva responsabilitat.
- Garantir que els tractaments de dades personals compleixin les mesures de seguretat definides.
- Coordinar-se amb la responsable de privadesa per a la correcta implementació de les mesures comunes i específiques de protecció de dades.
- Facilitar la recollida d'evidències, indicadors de compliment i documentació associada.
- Comunicar incidències o riscos que puguin afectar la seguretat de la informació o la protecció de dades personals.

La figura de la **responsable de privadesa** actua com a element de coordinació operativa, reforçant la responsabilitat proactiva i assegurant una visió integrada entre seguretat de la informació i protecció de dades, sense substituir les funcions pròpies del DPD.

11 ANNEX 1. Mesures d'adequació ENS ja executades

Aquest apartat detalla els controls que han assolit l'estat de **"executat o fet"** segons l'informe d'estat actual, agrupats per la seva naturalesa.

a) Marc organitzatiu i planificació

- **Política de seguretat (org.1):** Aprovada pel ple el 18/03/25, publicada i comunicada a tot el personal.

- **Normativa de seguretat (org.2):** Normativa d'ús de les TIC aprovada per decret de gerència i disponible a la wiki corporativa.

- **Procés d'autorització (org.4):** Processos definits per a l'ús de dispositius portàtils i autoritzacions d'accés a la infraestructura.

- **Anàlisi de riscos (op.pl.1):** Realitzada de forma formal i integrada en la documentació de la Comissió de Seguretat.

- **Arquitectura de seguretat (op.pl.2):** Diagrames de xarxa i plànols d'instal·lacions documentats a Confluence.

- **Adquisició de nous components (op.pl.3):** Procediment establert al Manual de Procediments del Marc Operacional.

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

b) Control d'accés i gestió de drets

- **Requisits d'accés (op.acc.2):** Procediment aprovat per a l'autorització i assignació d'accessos tant per a personal intern com extern.
- **Segregació de funcions i tasques (op.acc.3):** Implantació de missatges informatius sobre el darrer accés a l'AD i Google Workspace.
- **Procés de gestió de drets d'accés (op.acc.4):** Procediment establert per al control d'accés.

c) Operació i protecció tècnica

- **Gestió de canvis (op.exp.5):** Implementació de la metodologia i ús de l'eina Jira per al seguiment de tots els canvis del sistema.
- **Gestió d'incidents i el seu registre (op.exp.7, op.exp.9):** Controls marcats com a completats en la infraestructura actual.
- **Protecció de claus criptogràfiques (op.exp.10):** Mesura implementada segons l'inventari de controls.
- **Criptografia (mp.si.2):** Aplicació de mesures criptogràfiques segons la SoA.
- **Protecció de serveis i aplicacions web (mp.s.2):** Contractats a proveïdors certificats en ENS categoria Alta i amb escanejos de vulnerabilitats periòdics.
- **Protecció davant de denegació de servei (mp.s.4):** Sistemes correctament dimensionats i firewall habilitat per a la prevenció d'atacs DoS.

d) Seguretat Física i del Personal

- **Protecció davant d'incendis i inundacions (mp.if.5, mp.if.6):** Mesures físiques de protecció de les instal·lacions ja operatives.
- **Deures, obligacions i conscienciació del personal (mp.per.2, mp.per.3):** Accions formatives i deures definits i comunicats.
- **Bloqueig de lloc de treball (mp.eq.2):** Implementat en els equips d'usuari.

11.1 Valoració de l'estat actual i compromís de seguretat

És fonamental **posar en valor** l'esforç realitzat pel Consell Comarcal del Maresme en haver consolidat ja 37 controls de l'ENS. Haver assolit parcialment un **estat L3 (Procés definit)** en una bona part dels controls aplicables demostra una maduresa organitzativa destacable, ja que significa que la seguretat no és una acció aïllada, sinó que està procedimentada i documentada.

No obstant això, cal subratllar que la seguretat de la informació és un **procés dinàmic**. El fet que una mesura estigui "executada o feta" no implica la finalització del treball, sinó

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx

l'inici d'una fase de vigilància constant. La **necessitat de garantir el seu compliment i aplicació** diària és imperativa per:

1. **Mantenir la validesa de l'Anàlisi de Riscos:** Qualsevol relaxació en l'aplicació dels controls ja establerts podria invalidar les previsions de risc actuals.
2. **Preparar l'organització per a l'auditoria:** La certificació ENS no només requereix que la mesura existeixi, sinó que es puguin presentar **evidències verificables** del seu funcionament continuat.
3. **Millora contínua:** L'adequació ha d'estar alineada amb el cicle de millora contínua, assegurant que els procediments aprovats s'actualitzen davant de qualsevol canvi en la infraestructura o en l'amenaça cibernètica.

Aquest annex, juntament amb el pla d'actuació de mesures pendents, conforma la **visió completa del procés d'adequació**, assegurant la traçabilitat documental necessària per a la governança del sistema d'informació del CCM

CSV: [illegible]
Aquest és un document públic administratiu emès pel Consell Comarcal del Maresme de conformitat amb l'article 26 de la Llei 39/2015, d'1 d'octubre. La seva autenticitat pot ser comprovada a l'adreça https://tramits.ccmaresme.cat/Ciutadania/ValidarDocuments.aspx