

## **1. APROVACIÓ I ENTRADA EN VIGOR**

La present Política de Seguretat de la Informació (en endavant Política), ha estat aprovada per Resolució de la Presidència de l'Institut Mallorquí d'Afers Socials, en endavant IMAS.

Aquesta Política, serà efectiva des d'aquesta data i fins que sigui reemplaçada per una nova Política.

## **2. INTRODUCCIÓ**

L'IMAS és un organisme autònom, adscrit al Departament de Benestar Social del Consell de Mallorca, que exerceix les competències atribuïdes per qualsevol títol al Consell de Mallorca en matèria de serveis socials i protecció de menors, així com qualsevol finalitat determinada en els seus Estatuts (BOIB Núm. 67 de 18 de maig de 2019)

L'IMAS, depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per a la correcta prestació dels serveis, execució i exercici de les seves competències. Aquests sistemes han de garantir la disponibilitat, integritat o confidencialitat de la informació tractada o dels serveis prestats.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. L'IMAS aplicarà les mesures mínimes de seguretat exigides pel Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (en avança ENS) i, realitzarà un seguiment continu dels nivells de prestació de serveis, anàlisi de les vulnerabilitats reportades, i prepararà una resposta efectiva davant els incidents, per garantir la continuïtat dels serveis prestats.

## **3. MISSIÓ D'IMAS**

L'IMAS vol potenciar l'ús de les noves tecnologies, en el desenvolupament de les seves competències i interacció amb la pròpia ciutadania. Aquestes competències es poden trobar a l'article 2 dels Estatuts de l'IMAS

## **4. OBJECTE**

La present política de seguretat de la informació i protecció de dades personals té per objecte:

- 1) Establir el marc normatiu que reculli els principis bàsics i requisits mínims que permetin una protecció adequada de la informació que es gestiona en l'àmbit de les competències de l'IMAS, i que serà d'aplicació, a tots els serveis i sistemes d'informació i a totes les activitats de tractament de dades personals de les quals sigui responsable l'IMAS. En particular, la Política estableix les directrius que regeixen la forma en què l'IMAS gestiona i protegeix la informació que tracta i els serveis que presta.

- 2) Definir el model organitzatiu i tècnic apropiat per garantir el compliment de la normativa aplicable al tractament de les dades personals i l' accés i utilització dels sistemes d' informació.

## 5. ABAST

El disposat en aquesta política serà d' obligat compliment per a totes les unitats que conformen l' estructura orgànica de l' IMAS i per a tot el personal amb accés a la informació de les quals són responsables aquelles, amb independència de la seva destinació, condició laboral o relació contractual que autoritzi l' accés a la informació.

En particular, quedaran compreses en l' àmbit subjectiu d' aplicació:

- 1) L' IMAS, respecte de la informació tractada per qualsevol mitjà amb independència del suport en el qual es trobi.
- 2) Altres persones o entitats amb accés a informació: quan s'utilitzin serveis externs o permetin l'accés legítim o cedeixin informació a terceres persones, en particular quan aquestes participin, utilitzin, operin o administrin dades personals i/o sistemes d'informació i comunicacions, se'ls farà partícips d'aquesta Política, quedant subjectes a les obligacions establertes en les mateixes.

## 6. MARC NORMATIU

El marc legal i regulatori que afecta el desenvolupament de les activitats i competències de l' IMAS en l' àmbit de l' ENS, està constituït per normes jurídiques estatals, autonòmiques i sectorials orientades a l' administració electrònica, a la ciberseguretat i seguretat de la informació en general, així com a la protecció de dades personals.

En concret, la legislació i les principals normatives aplicables serien les següents:

- a) 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 (en endavant RGPD).
- b) Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (en endavant LOPDGDD).
- c) Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- d) Llei 39/2015, de l'1 d'octubre, del procediment administratiu comú de les Administracions Públiques.
- e) Llei 40/2015, de l'1 d'octubre, de règim jurídic del Sector Públic.
- f) Llei 12/1993, de 20 de desembre, d'atribució de competències en matèria de Serveis Socials i Assistència Social.
- g) Llei 8/1997, de 18 de desembre, d'atribució de competències als Consells Insulars en matèria de Tutela, Acolliment i Adopció de menors.

- h) Llei 14/2001, de 29 d'octubre, de transferència de competències als Consells Insulars en matèria de Serveis Socials i Seguretat Social.
- i) Llei 4/2009, d'11 de juny, de serveis socials de les Illes Balears.
- j) Acord del ple del consell insular de Mallorca, de dia 11 d'abril de 2019, pel qual s'aproven els Estatuts de l'IMAS.
- k) Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local.
- l) Reial Decret 1372/1986, de 13 de juny, pel qual s'aprova el Reglament de Béns de les Entitats Locals.
- m) Llei 57/2003, de 16 de desembre, de Mesures per a la Modernització del Govern Local.
- n) Resta de normativa que resulti d'aplicació.
- o) Guies sèrie 800 CCN-CERT.
- p) Instruccions tècniques referents a l'ENS.

També formen part del marc legal i regulatori les restants normes aplicables a l'Administració Electrònica de l'IMAS, que siguin desenvolupament de les anteriors o hi estiguin relacionades, compreses dins l'àmbit d'aplicació de la present Política.

## 7. PRINCIPIS BÀSICS DE LA SEGURETAT DE LA INFORMACIÓ I PROTECCIÓ DE DADES PERSONALS

L'IMAS serà responsable del compliment de la present política de seguretat de la informació i protecció de dades personals, i haurà de ser capaç de demostrar aquest compliment, assumint una responsabilitat proactiva. Per a això, tractarà la informació i les dades personals conforme als següents principis estructurals:

- a) **Abast estratègic:** La protecció de dades personals i la seguretat de la informació han de comptar amb el compromís i suport de tots els nivells directius de l'IMAS, assegurant que s'integrin amb la resta de les iniciatives estratègiques de l'entitat per conformar un complex coherent i eficaç.
- b) **Responsabilitat proactiva:** L'IMAS serà responsable de complir amb els principis establerts en aquest article, adoptant les mesures organitzatives, operacionals i tècniques necessàries per demostrar aquest compliment.
- c) **Diferenciació de responsabilitats:** Les responsabilitats sobre les dades personals, la informació, els serveis i la seguretat estaran clarament diferenciades en diversos rols, els quals hauran d'estar capacitats per exercir les seves funcions. S'establiran mecanismes de coordinació i resolució de conflictes per garantir una gestió eficaç de la seguretat dels sistemes d'informació.
- d) **Compliment:** L'IMAS adoptarà les mesures tècniques, organitzatives i procedimentals necessàries per assegurar el compliment de la normativa legal vigent en matèria de seguretat de la informació i protecció de dades personals.

- e) **Licitud, lleialtat i transparència:** Les dades personals es tractaran de forma lícita, lleial i transparent, respectant els drets dels titulars de les dades i els seus representants.
- f) **Limitació de la finalitat:** Les dades personals es recolliran amb finalitats determinades, explícites i legítimes, i no seran tractades de manera incompatible amb aquestes finalitats, llevat de casos d'interès públic, investigació científica o fins estadístics.
- g) **Minimització de dades:** Només es recolliran i tractaran les dades personals que siguin estrictament necessàries, adequades i pertinents per a les finalitats corresponents.
- h) **Exactitud:** Es garantirà que les dades personals siguin exactes i s'actualitzaran quan sigui necessari. S'adoptaran mesures per suprimir o rectificar qualsevol dada inexacte de manera oportuna.
- i) **Limitació del termini de conservació:** Les dades personals es conservaran únicament durant el temps necessari per complir amb les finalitats del tractament i les obligacions legals relacionades.
- j) **Integritat i confidencialitat:** Les dades es tractaran de manera que es garanteixi una seguretat adequada, protegint-les contra el tractament no autoritzat, pèrdua, destrucció o dany accidental mitjançant mesures tècniques i organitzatives apropiades.
- k) **Atenció als drets de les persones interessades:** Es garantirà l'exercici dels drets d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat per part de les persones interessades.
- l) **Actualització i adequació:** La protecció de les dades dels sistemes d'informació de l'IMAS serà adaptada i actualitzada en funció dels canvis en l'entorn, mantenint sempre la seva eficàcia i eficiència.
- m) **Seguretat com a procés integral:** La seguretat de la informació serà entesa com un procés integral que engloba tots els aspectes tècnics, humans, organitzatius i jurídics relacionats amb els sistemes d'informació de l'IMAS.
- n) **Gestió de la seguretat basada en els riscos:** L'IMAS gestionarà la seguretat dels seus sistemes i informació mitjançant una avaluació contínua de riscos, assegurant que s'implementin mesures de control proporcionades a la naturalesa de les dades i els serveis.
- ñ) **Prevenció, detecció, resposta i conservació:** S'establiran mesures preventives, de detecció, de resposta davant d'incidents i de conservació de la informació, per tal de minimitzar les vulnerabilitats i protegir les dades i serveis de l'IMAS.
- o) **Proporcionalitat:** Les mesures de protecció de la seguretat de la informació seran proporcionals als riscos i a la criticitat de les dades personals i els serveis.

q) **Reducció de probabilitat i impacte:** S' implementaran múltiples capes de seguretat per reduir els temps de resposta davant d' incidents, disminuir la probabilitat que s' esdevinguessin, i minimitzar el seu impacte tant en les persones afectades com en els actius de l' IMAS.

r) **Línies de defensa:** L' estratègia de protecció inclourà diverses capes de seguretat que permetran:

1. Reaccionar de manera oportuna davant incidents inevitables.
2. Reduir la probabilitat de comprometre tot el sistema d' informació.
3. Minimitzar l' impacte final. Aquestes capes inclouran mesures organitzatives, físiques i lògiques.

s) **Seguretat dels actius d' informació:** S' aplicaran mesures tècniques i organitzatives perquè el personal amb accés als actius d' informació i dades personals coneguin les seves responsabilitats, reduint el risc d' ús indegut.

t) **Seguretat en la gestió de comunicacions:** S' establiran procediments per gestionar la seguretat de les tecnologies de la informació i comunicacions. La informació transmesa per xarxes serà protegida d' acord al seu nivell de sensibilitat i criticitat, utilitzant mecanismes adequats.

u) **Gestió d' incidents de seguretat:** L' IMAS destinarà els recursos econòmics, humans i tecnològics necessaris per enfortir la ciberseguretat, conforme al principi de proporcionalitat i el nivell de seguretat requerit. Es planificaran i documentaran procediments en un marc de millora contínua amb participació dels actors involucrats.

v) **Seguretat de l' entorn tecnològic:** Amb l' objectiu de garantir un entorn tecnològic segur l' IMAS implementarà les mesures necessàries per complir amb la política de seguretat de la informació i protecció de dades personals, evitant l' expansió d' incidents derivats de vulnerabilitats entre els sistemes.

w) **Vigilància contínua i re avaluació periòdica:** S' establiran mecanismes de vigilància contínua per detectar activitats anòmales, i s' avaluarà constantment l' estat de seguretat dels actius per identificar vulnerabilitats. Les mesures de seguretat s' actualitzaran periòdicament per respondre a l' evolució dels riscos.

x) **Infraestructura i recursos informàtics:** L'IMAS compta amb una infraestructura tecnològica que garanteix l'eficiència i eficàcia en la prestació de serveis, incloent equips, programes, servidors, xarxes, i serveis corporatius (com el correu electrònic) i l'accés a aplicacions.

y) **Adquisició i instal·lació de productes de seguretat:** L'ús de la infraestructura informàtica s'ajustarà a les directrius internes i a les normatives i procediments de seguretat vigents.

z) **Seguretat des del disseny i per defecte:** L' IMAS promourà la inclusió de la protecció de dades i seguretat des del disseny i per defecte en tots els sistemes d' informació i tractaments de dades personals, seguint la normativa aplicable. S' adoptarà un enfocament que respecti la privacitat, la transparència i els principis de seguretat, disponibilitat, autenticitat, traçabilitat, integritat i confidencialitat en els processos futurs.

## 8. MODEL DE GOVERNANÇA

Per garantir el compliment de l' ENS i les obligacions derivades de la seguretat de la informació, l' IMAS designarà rols de seguretat i constituirà un Comitè de Seguretat de la informació.

### 8.1. Rols o perfils de seguretat

Per garantir el compliment i l' adaptació de les mesures exigides reglamentàriament, s' han creat rols o perfils de seguretat i s' han designat els càrrecs o òrgans que els ocuparan, de la manera següent:

- Responsable/s d'Informació: Persona que ocupi la Vicepresidència.
- Responsable dels Serveis: Persones que ocupin les Direccions Insulars i la Gerència de l'IMAS
- Responsable de la Seguretat: Persona que ocupi la Prefectura de la Secció de Seguretat, adscrita al Departament d' Informàtica.
- Responsable del Sistema: Persona que ocupi la Prefectura del Departament d' Informàtica
- Delegat de Protecció de Dades: Empresa externa

Per tal de dotar d' estabilitat l' estructura de la seguretat de la informació i de protecció de dades personals, els rols descrits s' assignen a llocs o càrrecs de l' estructura orgànica de l' IMAS. Per tant, el nomenament per al lloc o càrrec que correspongui comportarà l' assumptió del rol, així com la consegüent acceptació de responsabilitats i funcions en l' exercici del lloc o càrrec corresponent.

A continuació, es procedeix a descriure les funcions i responsabilitats dels rols de seguretat de manera detallada:

#### *8.1.1. Responsable de la informació*

Li corresponen les responsabilitats i funcions següents:

- a) Responsabilitat última de l' ús que es faci de la informació, i de la seva protecció.
- b) Responsabilitat última de qualsevol error o negligència que comporti un incident de seguretat, en l' àmbit de protecció de dades personals en les dimensions de confidencialitat o d' integritat i en l' àmbit de seguretat de la informació en la dimensió de disponibilitat.

- c) Valora la informació i els serveis pertanyents al seu sistema d'informació, segons l'impacte que tindria un incident que afectés la seguretat de la informació amb perjudici per a les dimensions de seguretat, seguint el procediment i dins del marc establert a l'Annex I de l'ENS.
- d) Determina els requisits de seguretat i els nivells de seguretat de la informació i dels serveis pertanyents al seu sistema d'informació. L'aprovació formal dels requisits de seguretat, nivells de seguretat i valoracions es realitzarà pel responsable de la informació a proposta conjunta dels responsables del servei del seu sistema d'informació (aquests proposen i determinen prèviament els requisits, nivells i valoracions de seguretat de la informació i del servei) amb l'assistència del responsable de seguretat i amb el suport del responsable del sistema.
- e) Proposa la categoria de la seva informació i/o del seu sistema/s d'informació, dins del seu àmbit competencial, al responsable de seguretat.
- f) Amb caràcter general, ha de tenir en compte les indicacions del responsable del sistema i del responsable de seguretat.

#### *8.1.2. Responsable del servei*

Li corresponen les responsabilitats i funcions següents:

- a) Proposa al responsable d'informació per a la seva aprovació definitiva: la valoració del seu servei i de la informació tractada en el mateix, i la determinació dels requisits de seguretat i els nivells de seguretat del mateix.  
Per a la valoració tindrà en compte l'impacte que suposaria un incident que afectarà la seguretat amb perjudici per a les dimensions de seguretat, seguint el procediment i dins del marc establert a l'Annex I de l'ENS, amb l'assistència del responsable de seguretat i amb el suport del responsable del sistema.
- b) Informar de totes aquelles necessitats, afeccions i incidents que estiguin directament relacionades amb els seus serveis.
- c) Amb caràcter general, ha de tenir en compte les indicacions del responsable del sistema i del responsable de seguretat. Responsabilitat última de l'ús que es faci de la informació, i de la seva protecció.

#### *8.1.3. Responsable de seguretat*

Li corresponen les responsabilitats i funcions següents:

- a) Manté la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que estableix aquesta política i la resta de normativa aplicable.
- b) Promou la formació i conscienciació en matèria de seguretat, definint i impulsant iniciatives de formació i sensibilització per al desenvolupament i promoció de bones pràctiques en matèria de seguretat de la informació.

- c) Elabora i proposa per a la seva aprovació la política de seguretat, que inclou les mesures tècniques i organitzatives, adequades i proporcionades, per gestionar els riscos que es plantegin per a la seguretat de les xarxes i sistemes d' informació utilitzats i per prevenir i reduir al mínim els efectes dels incidents de seguretat que afectin l' IMAS.
- d) Desenvolupa les normes, procediments, guies i instruccions de seguretat i supervisa la seva efectivitat, impulsant la realització de les auditories periòdica de seguretat que siguin necessàries.
- e) Rep, interpreta i aplica les instruccions i guies emanades de les autoritats competents, tant per a l' operativa habitual com per a l' esmena de les deficiències observades.
- f) Recopila, prepara i subministra informació o documentació a les autoritats competents, a la seva sol·licitud o per pròpia iniciativa.
- g) Signa la declaració d' aplicabilitat, document que formalitza la relació de mesures de seguretat seleccionades, que es realitzarà amb l' assistència del responsable del sistema.
- h) Actua com a capacitat de bones pràctiques en seguretat de les xarxes i sistemes d' informació, tant en aspectes físics com lògics.
- i) Constitueix el punt de contacte amb l' autoritat competent en matèria de seguretat de la informació.
- j) És interlocutor dels rols de responsable de la informació, responsables del servei i responsable del sistema.
- k) Assisteix els responsables d' informació i responsable de servei, sobre el correcte exercici de les seves funcions en matèria de l' ENS.
- l) Notifica a l' autoritat competent els incidents de seguretat que tinguin efectes perturbadors en la prestació dels serveis.
- m) Participa en la gestió adequada dels incidents de seguretat i de les accions de tractament que se segueixin, amb l' assistència del responsable del sistema.
- n) Analitza i proposa salvaguardes que previnguin incidents similars en el futur, amb l' assistència del Responsable del sistema.
- o) Reporta al responsable de la informació i al responsable del servei, respectivament, de les decisions i incidents en matèria de seguretat que afectin la informació i el servei que els competeix, en particular de l' estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats, amb l' assistència del responsable del sistema.
- p) Determina la categoria del sistema d' informació conforme a les valoracions proposades per responsables d' informació i de serveis, i amb l' assistència del responsable del sistema. Impulsa i realitza l' anàlisi de riscos periòdic, i l' informe de resultats del procés d' anàlisi de riscos i el seu Pla de Tractament de riscos, i, a més, assumeix la responsabilitat de gestió de les tasques del Pla de Tractament de Riscos. En tot el procés, compta amb l' assistència del responsable del sistema per a la infraestructura TIC.

- q) Gestiona la realització d' auditories dels sistemes d' informació en els terminis que estableix l' ENS.
- r) Analitza els resultats de les anàlisis de riscos i auditories realitzades i proposa accions de millora i correctores per a l' adequat compliment i alineament amb l' ENS.
- s) Analitza i proposa millores organitzatives, de procediments i funcionals en el marc del pla d' alineament de l' ENS. Per a això, s' encarrega d' identificar els nivells de compliment de les mesures de seguretat aplicables i determinar les recomanacions corresponents, i promou la implantació coordinada de les mateixes i dels sistemes d' informació afectes a l' ENS.
- t) Adopta o en el seu cas, valida les propostes de les mesures urgents que s' estimin necessàries per prevenir, mantenir i restablir la seguretat de la informació en totes aquelles situacions que constitueixin amenaces i generin riscos per a la seguretat de la informació quant a disponibilitat, autenticitat, integritat, confidencialitat i traçabilitat, amb especial incidència en la gestió imminent de ciber incidents associats als sistemes i tecnologies d' Informació i comunicacions (TIC).
- u) Garanteix l'adequat report al Centre Criptològic Nacional dels indicadors necessaris per obtenir l'Informe Nacional de l'Estat de la Seguretat (INES) segons el que estableix l'article 32 de l'ENS.
- v) Amb caràcter general per a l' execució de les responsabilitats i funcions descrites, ha de disposar del suport del responsable del sistema.

#### *8.1.4. Responsable del sistema*

Li corresponen les responsabilitats i funcions següents:

- a) Desenvolupa, opera i manté el sistema d' informació durant tot el seu cicle de vida, incloent-hi les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- b) Defineix la topologia i la gestió del sistema d' informació, establint els criteris d' ús i els serveis disponibles en el mateix.
- c) S' ha de cerciorar que les mesures específiques de seguretat s' integren adequadament dins el marc general de seguretat.
- d) Defineix l' organització i el desplegament dels processos tecnològics.
- e) Reporta al responsable de la informació de les incidències funcionals relatives a la informació que li competeix; reporta al responsable del servei de les incidències funcionals relatives al servei que li competeix; i reporta al responsable de seguretat de les actuacions en matèria de seguretat, en particular, pel que fa a decisions d' arquitectura del sistema.
- f) Planifica la implantació de les salvaguardes en el sistema.
- g) Executa el pla de millora de la seguretat que s' aprovi de ser necessari, per atendre els riscos que no són acceptables.
- h) Implementa, gestiona i manté les mesures de seguretat aplicables als sistemes de tecnologies d' informació.

- i) Gestiona els serveis de seguretat.
- j) Proposa mesures de gestió i control d' accés als sistemes d' informació i la seva gestió. Implementa, gestiona i manté les mesures de seguretat aplicables a la gestió d' accés als sistemes d' informació.
- k) Reporta al responsable del sistema i al responsable de seguretat dels incidents de seguretat i de les accions de configuració, actualització o correcció.
- l) Gestiona, configura i actualitza el maquinari i programari en els quals es basen els mecanismes i serveis de seguretat del sistema de tecnologia de la Informació.
- m) Gestiona les autoritzacions i privilegis concedits a persones usuàries del sistema, incloent-hi el monitoratge que l' activitat desenvolupada en el sistema s' ajusta a l' autoritzat i l' assegurem de l' aplicació dels procediments que s' aprovin per al maneig del sistema d' informació.
- n) Aplica els procediments operatius de seguretat.
- o) Supervisa que tot l' equipament s' ajusta a l' autoritzat, supervisa les actuacions i l' aplicació dels procediments de seguretat, supervisa que les activitats de les persones usuàries del sistema són conformes a l' autoritzat per a cadascuna d' elles, i també supervisa les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s' ajusten a les autoritzacions pertinents.
- p) Monitoritza l' estat de la seguretat i el compliment dels controls en el seu àmbit competencial de les tecnologies de la informació i les comunicacions.
- q) Informa el responsable de seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- r) Assisteix el responsable de seguretat per a la determinació per aquest de la categoria del sistema d' informació.
- s) Assisteix el responsable de seguretat per a la signatura per aquest de la Declaració d' Aplicabilitat.
- t) Assisteix el responsable de seguretat durant el procés d' anàlisi de riscos i en particular, en l' elaboració de l' informe de resultats i del seu Pla de Tractament de riscos. Gestiona el desenvolupament i execució de les tasques del Pla de Tractament de Riscos dins del procés d' Anàlisi i Gestió de Riscos i d' acord amb les instruccions i col·laboració immediata del responsable de seguretat corresponent, dins del seu àmbit competencial de tecnologies de la informació i les comunicacions.
- u) Gestiona de manera adequada els incidents de seguretat, en particular les tasques que se li assignin per a la prevenció, detecció, resposta i conservació dels incidents i de les accions de tractament que se segueixin, d' acord amb les funcions que s' estableixin en el procediment que reguli la gestió d' incidents.
- v) Assisteix en la notificació de les violacions de seguretat de les dades personals.
- w) Assisteix el responsable de seguretat en les consultes tècniques que sorgeixin durant el desenvolupament de les auditories i resta de processos per al compliment de l' ENS, dins del seu àmbit competencial de tecnologies de la informació i les comunicacions.

- x) Qualsevol altres actuacions de l'àmbit de la seguretat relacionades amb el seu àmbit funcional i competencial que li siguin encomanades pel responsable de seguretat, pel responsable del sistema o pel Comitè de Seguretat.

#### *8.1.5. Delegat de Protecció de Dades*

Li corresponen les responsabilitats i funcions següents:

- a) Informa i assessora el responsable o l'encarregat del tractament i el personal empleat que s'ocupin del tractament de les obligacions que els incumbeixen en virtut del RGPD i d'altres normes o disposicions de protecció de dades.
- b) Supervisa el compliment pel responsable o l'encarregat del tractament del que disposa el RGPD, en altres normes o disposicions de protecció de dades personals i en la present política, en particular respecte a l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- c) Ofereix l'assessorament que se li demani sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seva aplicació de conformitat amb l'article 35 del RGPD.
- d) Coopera amb l'autoritat de control competent.
- e) Actua com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36 RGPD i realitzar consultes, si s'escau, sobre qualsevol altre assumpte.
- f) Qualsevol altra funció o responsabilitat que la normativa de protecció de dades li atribueixi i, especialment, les detallades a l'apartat 9.1.3. de la present Política.

### **8.2. Comitè de Seguretat de la Informació**

El Comitè de Seguretat de la Informació (en endavant CSI), és l'òrgan col·legiat superior competent per a la presa de decisions i exercici de funcions de direcció i coordinació en matèria de seguretat de la informació i protecció de dades amb plens efectes en tot l'IMAS, i que dona compliment a la mesura 3.1 política de seguretat del marc organitzatiu de l'Annex II de l'ENS i resta de normativa de protecció de dades.

El Comitè s'ha de reunir de forma semestral, amb caràcter ordinari.

#### *8.2.1. Funcions del Comitè de Seguretat de la Informació*

El CSI ostentarà a les següents funcions:

- a) Coordina totes les funcions de seguretat de l'IMAS.
- b) Aprova la normativa de seguretat de la informació i vela, impulsa, supervisa el compliment d'aquesta.

- c) Atén les inquietuds manifestades en l' àmbit de seguretat de la informació en les sessions del comitè i se les transmet als responsables respectius per recaptar respostes i solucions.
- d) Recava, dels responsables els informes sobre l'estat de la seguretat.
- e) Si s' escau, proposa i designa rols en l' àmbit de seguretat de la informació.
- f) Rep les comunicacions del responsable de seguretat relacionades amb els canvis de normativa de seguretat de la informació.
- g) Promou la millora contínua de la seguretat de la informació.
- h) Vetlla perquè la seguretat de la informació es tingui en compte en tots els projectes des del seu disseny inicial fins a la seva posada en execució.
- i) Rep dació en compte de la normativa i procediments de seguretat derivats de la present política.
- j) Rep dació en compte de les mesures tècniques i organitzatives de seguretat de la informació.
- k) Rep dació en compte de l' estat dels processos d' anàlisi de riscos, auditories, mesures de seguretat i resta d' actuacions que donin compliment a l' ENS.
- l) Aprova l' informe de resultats del procés d' anàlisi de riscos i el seu corresponent pla de tractament de riscos.
- m) Aprova el pla de millora de la seguretat que s' aprovi de ser necessari, per atendre els riscos que no són acceptables, a proposta del responsable de seguretat.
- n) Rep dació en compte dels nivells de seguretat de la informació i de la categorització dels Sistemes d' informació i els serveis.
- o) Rep dació en compte de la Declaració d' aplicabilitat.
- p) Rep dació en compte dels incidents de seguretat esdevinguts.
- q) Rep dació en compte de l' estat de la seguretat i de les possibles incidències en l' execució de les mesures de seguretat.
- r) Elaborar i revisar regularment la Política de Seguretat de la Informació per a la seva ulterior aprovació per l' òrgan competent.
- s) Aprovar programes de formació destinats a formar i sensibilitzar el personal en matèria de Seguretat de la Informació i en particular en matèria de protecció de dades de caràcter personal.
- t) Promoure la realització de les auditories periòdiques ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l' Administració en matèria de seguretat de la Informació.

### *8.2.2. Composició del Comitè de Seguretat de la Informació*

EL CSI, com a òrgan col·legiat, està format pels membres següents:

- a) **President/a:** Serà exercit per la persona que ostenti el càrrec de Responsable de la Informació i atendrà les següents funcions:
- b) Tenir la representació de l' òrgan.

- c) Acordar la convocatòria de les sessions ordinàries i extraordinàries i la fixació de l'ordre del dia, tenint en compte, si s'escau, les peticions dels altres membres formulades amb la suficient antelació.
  - d) Presidir les sessions del Comitè, moderar el desenvolupament dels debats i suspendre'ls per causes justificades.
  - e) Dirigir les deliberacions i, en general, exercitar les facultats precises per a l'adequat desenvolupament de les sessions.
  - f) Dirimir amb el seu vot els empats, a l'efecte d'adoptar acords.
  - g) Assegurar el compliment de la normativa aplicable.
  - h) Revisar les actes i certificacions dels acords del Comitè.
  - i) Exercir totes les altres funcions que siguin inherents a la seva condició de president de l'òrgan.
- **Secretari/a:** Recaurà en la persona que ostenti la prefectura del Servei Juridicoadministratiu o persona que el substitueixi i atindrà les següents funcions:
    - a) Assistir a les sessions amb veu, però sense vot.
    - b) Preparar les sessions.
    - c) Aixecar les actes de les sessions del Comitè.
    - d) Expedir certificacions dels Acords del Comitè.
    - e) Arxivar i custodiar els documents en què constin les actuacions desenvolupades pel Comitè.
  - **Vocals:**
    - Responsables de Serveis<sup>1</sup>.
    - Responsable de la Seguretat.
    - Responsable del Sistema.

Les i els vocals del Comitè tenen les funcions següents:

- a) Assistir a les sessions i participar en els debats.
- b) Presentar al Comitè les propostes que estimin oportunes.
- c) Emetre el seu vot, expressant el sentit del mateix, així com formular vot particular discrepant amb el parer de la majoria. Possibilitat de delegació de vot: en cas d'impossibilitat d'assistència del vocal titular o suplent, es podrà delegar el vot en un altre membre del comitè.
- **Delegat de Protecció de dades (DPD):** amb funcions d'assessorament i supervisió en matèria de protecció de dades i sense dret a vot.

Així mateix, i amb caràcter opcional, podran incorporar-se a les tasques del CSI, grups de treball especialitzats, ja siguin de caràcter intern, extern o mixt.

Els membres del Comitè seran designats per resolució de la Presidència de l'IMAS.

---

<sup>1</sup> Els Responsables Serveis seran convocats quan es tractin qüestions en les quals estiguin implicats els seus serveis, no obstant això, podran acudir voluntàriament quan ho estimin oportú.

### *8.2.3. Normes de Funcionament*

El funcionament del Comitè en tot allò no previst en aquesta Política, s'ha d'ajustar, de conformitat a les Disposició Addicional Segona del Reglament Orgànic del Consell de Mallorca, a la al que preveu la Llei 40/2015, de Règim Jurídic del Sector Públic.

### *8.2.4 Resolució de conflictes*

Si hi hagués conflicte entre els responsables, serà resolt pel Comitè de Seguretat de la Informació.

## **9. PROTECCIÓ DE DADES PERSONALS I PRIVACITAT**

L'IMAS, en el tractament de les dades personals, compleix amb els principis i obligacions de la normativa vigent, essent aquesta el RGPD i la LOPDGDD, respectant, en tot cas, el dret fonamental a la protecció de dades personals, la intimitat i la resta dels drets fonamentals reconeguts tant en la legislació i tractats internacionals com en la Constitució vigent.

Referent a això, en el marc de la normativa europea i espanyola, l'IMAS assumeix el compromís de garantir la protecció de les dades personals que maneja, conforme als principis i obligacions establertes en les esmentades normatives, essent la protecció de dades no només un deure legal, sinó també una eina clau per salvaguardar els drets fonamentals de les persones físiques pel que fa al tractament de la seva informació personal.

Per això, l'IMAS ha desenvolupat una política integral que contempla totes les mesures necessàries per garantir la seguretat, confidencialitat, integritat i disponibilitat de les dades personals que tracta en el curs de les seves activitats.

A continuació, es procedirà a detallar els aspectes fonamentals relacionats amb la protecció de dades personals, abordant les figures clau implicades en la seva gestió, els principis que regeixen el seu tractament, els drets de les persones interessades, l'avaluació d'impacte en la protecció de dades i la gestió d'incidents de seguretat.

### **9.1. Figures vinculades a protecció de dades personals**

En l'àmbit de la protecció de dades, l'IMAS comptarà amb diverses figures que assumiran rols i responsabilitats específiques per garantir el compliment de la normativa vigent. Aquests rols estaran alineats amb el RGPD, la Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia dels Drets Digitals (LOPDGDD), i l'ENS.

A continuació, es descriuen les principals figures involucrades:

#### *9.1.1. Responsable del Tractament*

El responsable del tractament és la persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, determina els fins i mitjans del

tractament de les dades personals. En concret, l'IMAS ostentarà el rol de Responsable del tractament en tots aquells tractaments en els quals determini els fins i els mitjans, els quals seran definits i detallats en el Registre d'Activitats del Tractament (en endavant RAT) de l'organització.

Les funcions del Responsable del Tractament són, principalment:

- a) Decideix i aplica les mesures tècniques i organitzatives de seguretat adequades als tractaments de dades que es trobin sota la seva responsabilitat.
- b) Realitza les corresponents anàlisis de riscos i avaluacions d'impacte quan siguin necessàries d'acord amb el RGPD.
- c) Notifica a l'autoritat de control competent les violacions de la seguretat de les dades personals, sense dilació indeguda i, si és possible, com a molt tard 72 hores després que n'hagi tingut constància, llevat que sigui improbable que aquesta violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques. Si la notificació a l'autoritat de control no té lloc en el termini de 72 hores, haurà d'anar acompanyada d'una indicació en la qual s'al·legui els motius de la dilació. Quan sigui probable que la violació de la seguretat de les dades personals comporti un alt risc per als drets i llibertats de les persones físiques, el responsable del tractament ho comunicarà a la persona interessada sense dilació indeguda. Per realitzar aquestes notificacions comptarà amb l'assistència tècnica del responsable del sistema i, en el seu cas, es valorarà la delegació de la tasca en aquest, segons complexitat tècnica la violació.
- d) Resol les sol·licituds d'exercici de drets en matèria de protecció de dades personals d'acord amb els articles 15 a 22 del RGPD.
- e) Amb caràcter general, exerceix la resta de les funcions que li assigni la normativa de protecció de dades personals.

#### *9.1.2. Encarregat del Tractament*

És la persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades personals per compte del responsable del tractament. En concret, exerceix les següents responsabilitats i funcions:

- a) Assisteix la persona responsable del tractament, tenint en compte la naturalesa del tractament, per al compliment de les mesures tècniques i organitzatives apropiades, sempre que sigui possible, perquè aquest pugui complir amb la seva obligació de respondre a les sol·licituds que tinguin per objecte l'exercici dels drets de les persones interessades.
- b) Ajuda la persona responsable del tractament a garantir el compliment de les obligacions establertes als articles 32 a 36 del RGPD, tenint en compte la naturalesa del tractament i la informació a disposició de la persona encarregada del tractament.
- c) A elecció de la persona responsable del tractament, suprimeix o retorna totes les dades personals un cop finalitzada la prestació dels serveis de tractament, i

suprimeix les còpies existents, llevat que es requereixi la conservació de les dades personals.

- d) Posa a disposició de la persona responsable del tractament tota la informació necessària per demostrar el compliment de les obligacions, així com per permetre i contribuir a la realització d' auditories, incloses inspeccions.
- e) Informa immediatament la persona responsable del tractament si, d' acord amb el seu criteri, una instrucció o activitat infringeix qualsevol disposició en matèria de protecció de dades personals.
- f) Notifica sense dilació indeguda al responsable del tractament de les violacions de la seguretat de les dades personals de les quals tingui coneixement.
- g) Quan una persona encarregada de tractament recorri a una altra persona encarregada (subencarregada) per dur a terme determinades activitats de tractament per compte de la persona responsable, s'imposarà a aquesta altra persona encarregada, mitjançant contracte o un altre acte jurídic, les mateixes obligacions de protecció de dades personals que les estipulades en el contracte o acte jurídic entre responsable i encarregat principal, en particular la prestació de les garanties suficients d' aplicació de mesures tècniques i organitzatives apropiades de manera que el tractament sigui conforme amb les disposicions del RGPD. Si el subencarregat incompleix les seves obligacions de protecció de dades personals, la persona encarregada inicial seguirà sent plenament responsable davant el responsable del tractament pel que fa al compliment de les obligacions.
- h) Amb caràcter general, exerceix la resta de les funcions que li assigni la normativa de protecció de dades personals.

En relació a aquesta figura, l' IMAS, en qualitat de Responsable del tractament, es compromet a signar amb cada encarregat del tractament un encàrrec de tractament. En concret, els encàrrecs de tractament a l'IMAS són actes jurídics que estableixen la relació entre el responsable del tractament i els encarregats del tractament (entitats o persones que tracten dades personals en el seu nom). Aquests acords contindran els elements essencials indicats a l' article 28 del RGPD, tals com:

- Objecte del tractament: La finalitat per a la qual es duu a terme el tractament de les dades personals.
- Durada del tractament: El període durant el qual es realitzarà el tractament de les dades.
- Naturalesa i finalitat del tractament: Descripció clara del tipus de tractament que es durà a terme i el seu propòsit.
- Tipus de dades personals: Els tipus de dades que es manejaran, com ara dades de salut, dades identificatives o dades econòmiques.
- Categories de persones interessades: Definir a qui pertanyen les dades, com usuaris de serveis socials, empleats, etc.
- Obligacions i drets d' ambdues parts: Les responsabilitats que han de complir tant el responsable com l' encarregat en el maneig de les dades personals.

Per tal de monitoritzar l' estat dels contractes d' encàrrec, l' IMAS es compromet a generar i mantenir un registre actualitzat dels Encarregats de Tractament que estiguin prestant servei a l' entitat i els quals tinguin accés a dades personals.

#### *9.1.3. Delegat de Protecció de Dades*

El delegat de Protecció de Dades podrà ser intern o extern, vetllant sempre per evitar conflictes d' interès entre qualsevol dels seus membres.

El delegat de Protecció de l' entitat, s' ajustarà en cada moment a les necessitats segons les seves funcions, haurà de ser designat formalment i comunicat a l' Autoritat competent. Estarà disponible per a la contestació de consultes i atendre els exercicis de dret a través del correu electrònic o els mitjans habilitats per a tal fi.

Les funcions associades a aquesta figura són:

- a) Informar i assessorar el responsable o l' encarregat del tractament i els empleats que s' ocupin del tractament, així com de les obligacions derivades, en virtut del present Reglament i d' altres disposicions de protecció de dades de la Unió o dels Estats membres.
- b) Supervisar el compliment del que disposa el present Reglament, d' altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l' encarregat del tractament en matèria de protecció de dades personals, inclosa l' assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- c) Oferir l' assessorament que se li demani sobre l' avaluació d' impacte relativa a la protecció de dades i supervisar la seva aplicació de conformitat amb l' article 35 del RGPD.
- d) Cooperar amb l' autoritat de control.
- e) Actuar com a punt de contacte de l' autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia esmentada a l' article 36 del RGPD, i realitzar consultes, si s' escau, sobre qualsevol altre assumpte. El delegat de protecció de dades exercirà les seves funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l' abast, el context i fins del tractament. Per això haurà de ser capaç de:
  - Sol·licitar informació per determinar les activitats de tractament.
  - Analitzar i comprovar la conformitat de les activitats de tractament.
  - Informar, assessorar i emetre recomanacions al responsable o l' encarregat del tractament.
  - Demanar informació per supervisar el registre de les operacions de tractament.

- Assessorar en l'aplicació del principi de la protecció de dades per disseny i per defecte.
- f) Assessorar sobre:
- Si s'ha de dur a terme o no una avaluació d'impacte de la protecció de dades.
  - Que metodologia s'ha de seguir en efectuar una avaluació d'impacte de la protecció de dades.
  - Si s'ha de dur a terme avaluació d'impacte de la protecció de dades amb recursos propis o amb contractació externa.
  - Que salvaguardes (incloses mesures tècniques i organitzatives) aplicar per mitigar qualsevol risc per als drets d'interessos dels afectats.
  - Si es va dur a terme correctament o no l'avaluació d'impacte de la protecció de dades.
  - Si les seves conclusions (se seguir endavant o no amb el tractament i que salvaguardes aplicar) són conformes al Reglament.
- g) Prioritzar les seves activitats i centrar els seus esforços en aquelles qüestions que presentin majors riscos relacionats amb la protecció de dades.
- h) Assessorar el responsable del tractament sobre:
- Que metodologia emprar en dur a terme una avaluació d'impacte de la protecció de dades.
  - Que àrees s'han de sotmetre l'auditoria de protecció de dades interna o externa.
  - Que activitats de formació internes proporcionar al personal o als directors responsables de les activitats de tractament de dades i determinar a quines operacions de tractament dedicar més temps i recursos.

El DPD haurà de reunir coneixements especialitzats en Dret i en la pràctica de protecció de dades. En conseqüència, cal identificar aquells coneixements, habilitats i destreses necessàries que ha de saber el DPD per dur a terme de forma satisfactòria les funcions pròpies del seu lloc.

Aquestes funcions genèriques del DPD es concreten en tasques d'assessorament i supervisió, entre d'altres:

- a) Supervisió del compliment dels principis relatius al tractament, com poden ser la limitació de la finalitat, minimització o exactitud de les dades.
- b) Identificar les bases jurídiques dels tractaments.
- c) Valorar la compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.
- d) Determinar l'existència de normatives sectorials que poden determinar condicions especials de tractament de dades.
- e) Establiment de mecanismes de recepció i gestió de sol·licituds d'exercici de drets per part dels interessats.
- f) Valoració de les sol·licituds d'exercici de drets per part dels interessats.

- g) Contractació d'encarregats de tractament, inclòs els contractes i actes jurídics que regulin la relació responsable/encarregat.
- h) Identificació dels instruments de transferència internacional de dades adequats a les necessitats i característiques de l'organització i de les raons que justifiquin la transferència.
- i) Disseny i implementació de polítiques de protecció de dades.
- j) Serà l'encarregat d'auditar en matèria de protecció de dades.
- k) Analitzarà els riscos associats als tractaments que es realitzin.
- l) Implantació de mesures de protecció de dades des del disseny i per defecte, sempre adequats als riscos i la naturalesa dels tractaments.
- m) Establir el procediment de gestió d'incidents de seguretat de les dades, inclosa l'avaluació dels riscos derivats de l'incident, per als drets i llibertats dels ciutadans, així com la notificació a l'autoritat competent.
- n) Determinació de necessitat de realitzar Avaluacions d'Impacte en protecció de dades.
- o) Implantació de programes de formació i de conscienciació per al personal en matèria de protecció de dades.

## **9.2. Registre d'activitats de tractament de dades personals**

El RAT és un element essencial en la gestió de la protecció de dades personals, segons el que estableix l'article 30 del RGPD. En el context de l'IMAS, aquest registre permetrà documentar i demostrar el compliment de la normativa de protecció de dades, a més de facilitar la gestió i supervisió de les activitats relacionades amb el tractament de dades personals.

L'IMAS, en la seva qualitat de responsable del tractament, haurà de portar i mantenir actualitzat el registre, havent d'estar disponible per a la seva consulta per l'Autoritat de Control competent. En aquest sentit, l'IMAS haurà de revisar i actualitzar el registre periòdicament, especialment quan:

- S'incorporin noves activitats de tractament.
- Es modifiquin els fins del tractament o les categories de dades personals tractades.
- S'introdueixin nous encarregats del tractament o destinataris de les dades.
- Existeixin canvis en les mesures de seguretat aplicades.

### *9.2.1. Contingut del Registre d'Activitats de Tractament*

El RAT haurà de contenir, almenys, la següent informació sobre les activitats de tractament de dades personals que es realitzen a l'IMAS:

1. Nom i dades de contacte del responsable del tractament i, si s'escau, de l'encarregat del tractament i del Delegat de Protecció de Dades.

2. Fins del tractament.
3. Categories d'interessats.
4. Categories de dades personals tractades.
5. Destinataris de les dades personals.
6. Transferències internacionals de dades.
7. Terminis previstos per a la supressió de les dades.
8. Descripció general de les mesures de seguretat.

### **9.3. Transparència de la informació i comunicacions**

En compliment del deure de transparència, quan l' IMAS actuï en qualitat de responsables del tractament, prendran les mesures adequades per facilitar, a les persones físiques titulars de les dades tota la informació indicada als articles 13 i 14 del RGPD, que distingeixen, respectivament:

- Quan les dades personals s' obtinguin directament de la persona interessada, la informació es facilitarà en el moment en què s' obtinguin les dades.
- Quan les dades personals no s' hagin obtingut de la persona interessada, la informació es facilitarà en el moment de la primera comunicació amb les mateixes o quan les dades es comuniquin per primera vegada a una altra persona destinatària. En aquest cas, la persona responsable del tractament té obligació d' informar en el termini raonable d' un mes.

Les comunicacions es realitzaran de forma concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, en particular qualsevol informació dirigida específicament a menors d'edat.

La informació serà facilitada per escrit o per altres mitjans, inclusivament, si escau, per mitjans electrònics. Quan la persona interessada ho demani, la informació podrà facilitar-se verbalment sempre que es demostrï la identitat de la persona per altres mitjans.

### **9.4. Exercici de drets personals**

En compliment dels articles 15 a 22 del RGPD, l' IMAS garantirà l' exercici dels següents drets de la ciutadania, respecte de les dades personals que tracti:

- a) Dret d' accés. Faculta per conèixer si es tracten les dades personals i tota la informació completa d' aquest tractament.
- b) Dret de rectificació. Faculta per corregir les dades personals inexactes i completar les dades incompletes.
- c) Dret de supressió. Faculta per eliminar les dades personals en els supòsits taxats per la pròpia normativa.

- d) Dret d'oposició. Quan el responsable del tractament realitzi tractament de dades personals legitimat en una missió d'interès públic o exercici de poders públics, la persona interessada pot exercitar el dret d'oposició, en qualsevol moment, per motius relacionats amb la seva situació particular.

En aquest supòsit, es realitzarà un judici de ponderació dels interessos del responsable i de la persona interessada, valorant i considerant:

1. Els motius legítims imperiosos per al tractament del responsable.
2. Els interessos, drets i llibertats de la persona interessada.

- e) Dret de limitació. Faculta per a la limitació del tractament de dades personals, que implica la suspensió del tractament i si s'escau, conservació de les dades, quan es compleixi alguna de les condicions següents:

1. Quan s'impugna l'exactitud de dades personals durant el termini per verificar l'exactitud.
2. Quan es presenta oposició al tractament manifestant motius personals, mentre es verifica que el responsable tracta les seves dades legitimat en missió d'interès públic o exercici de poders públics, i es determina que aquest tractament del responsable preval.
3. Quan el tractament és il·lícit i es demana la limitació d'ús i no la supressió.
4. Quan les persones necessiten les dades per a l'exercici o defensa de reclamacions, però simultàniament el responsable ja no necessita aquestes dades per a les finalitats del tractament.

- f) Dret a no ser objecte de decisions individuals automatitzades. Es garantirà no ser sotmès a una decisió basada únicament en el tractament de dades personals, inclosa l'elaboració de perfils, i que produeix efectes jurídics sobre la persona. No obstant això, aquest dret no s'aplicarà:

1. Si fos necessari per a la celebració o execució d'un contracte entre persona interessada i responsable del tractament.
2. Si el tractament es troba autoritzat pel Dret de la Unió o dels Estats membres.
3. Si el tractament estigués legitimat pel consentiment.

- g) Dret a la portabilitat de les dades. Faculta per rebre les dades personals en un format estructurat, d'ús comú i lectura mecànica i poder transmetre aquestes dades a un altre responsable del tractament sempre que es donin dues condicions:

1. Que el tractament estigui basat en el consentiment o en un contracte.
2. I que el tractament s'efectuï per mitjans automatitzats.

El dret a la portabilitat no s'aplica al tractament que sigui necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable de tractament, tal com disposa l'article 20 del RGPD.

#### *9.4.1. Procediment per a l'exercici de drets personals*

Les persones físiques podran exercir davant la persona responsable del tractament, directament o per mitjà de representant, els drets a dalt indicats en relació amb les dades tractades per l' IMAS, a través del tràmit previst a tal efecte a la Seu Electrònica del Consell de Mallorca. Al seu torn, podran presentar una reclamació davant les autoritats de control pertinents.

En relació al procediment, estarà dividit en tres fases, les quals es detallen a continuació:

- a) **Presentació.** Les sol·licituds referides a l'exercici de drets personals que es corresponguin o facin referència quant al seu contingut a l'àmbit competencial que hagi de resoldre algun responsable de tractament de l'IMAS podran presentar-se mitjançant model de sol·licitud habilitat, que es posarà a disposició de la ciutadania de la manera següent:
  - a. Telemàticament: a la seu electrònica del Consell de Mallorca.
  - b. Presencialment: a les oficines de l' IMAS.
- b) **Tramitació i resolució.** De la sol·licitud presentada es donarà trasllat al responsable del tractament i aquest disposarà d'un termini d'un mes per respondre a partir de la recepció de la sol·licitud, d'acord amb l'article 12.3 RGPD. Aquest termini serà prorrogable per un termini màxim de dos mesos, atenent la complexitat i nombre de sol·licituds. Els motius de la pròrroga seran degudament informats a la persona interessada.
- c) **Impugnació.** En cas de desestimació expressa o presumpta de la sol·licitud de l'exercici de drets en matèria de protecció de dades personals corresponent, les persones interessades podran recaptar la tutela del dret davant l'Autoritat de Control competent mitjançant la presentació de reclamació davant la mateixa o, si escau, de conformitat amb l'article 37 LOPDGDD, dirigint una reclamació prèvia davant el DPD de l' IMAS.

## **10. ESTÀNDARDS DE SEGURETAT DE LA INFORMACIÓ I SALVAGUARDES**

A l' IMAS, per garantir la protecció adequada de les dades i la informació, s' estableixen una sèrie d' estàndards mínims i salvaguardes que han de regir tots els processos relacionats amb la seguretat dels sistemes d' informació. Aquests estàndards no només assegurin el compliment de la normativa vigent, sinó que també enforteixen la capacitat de l' organització per protegir la confidencialitat, integritat i disponibilitat de les dades.

A continuació, es descriuen els principis i mesures fonamentals:

### **a) Organització i implantació del procés de seguretat**

La seguretat haurà de comprometre totes les persones pertanyents a l' IMAS tal com s' ha exposat en la present política, assignant expressament responsabilitats diferenciades

entre els següents rols: responsable de la informació, responsable del servei, responsable de seguretat i responsable del sistema.

### **b) Gestió del personal i professionalitat**

Tot el personal relacionat amb la informació i els sistemes de l' IMAS, serà informat i format respecte de les seves responsabilitats de seguretat, i la seva actuació serà supervisada per assegurar el compliment de les normes. Els rols definits en aquesta política actuaran amb professionalitat, i s' exigirà que les organitzacions que prestin serveis de seguretat comptin amb professionals qualificats i nivells adequats de gestió.

La seguretat dels sistemes serà gestionada i auditada per personal qualificat en totes les fases del seu cicle de vida. A més, les empreses que prestin serveis a l' IMAS, en protecció de dades i seguretat de la informació, hauran de comptar amb professionals qualificats i nivells adequats de gestió i maduresa.

### **c) Anàlisi i gestió dels riscos**

L' IMAS com a organització que desenvolupa i implanten sistemes per al tractament de la informació o la prestació de serveis realitzarà la seva pròpia gestió de riscos. Aquesta gestió es realitzarà per mitjà de l' anàlisi i tractament dels riscos als quals està exposat el sistema, sens perjudici del que disposa l' annex II de l' ENS, s' emprarà alguna metodologia reconeguda internacionalment. Les mesures adoptades per mitigar o suprimir els riscos hauran d' estar justificades i, en tot cas, existirà una proporcionalitat entre aquestes i els riscos.

### **d) Autorització i control d' accessos**

S' establiran els mecanismes necessaris de protecció que controlin l' accés als sistemes d' informació, a través de la millora contínua. Aquests accessos estaran limitats exclusivament a les persones usuàries, processos, dispositius o altres sistemes d' informació, degudament autoritzats exclusivament per a l' acompliment de les funcions atribuïdes, d' acord amb l' article 17 de l' ENS.

En cas d' existir indicis d' activitats delictives o que comprometin la seguretat de la informació tractada, hauran de ser gestionats d' acord amb el procediment i normativa que, si s' escau, apliqui.

### **e) Protecció de les instal·lacions**

Es procurarà que els sistemes d' informació i la seva infraestructura de comunicacions associada s' ubiquin en àrees controlades que siguin emplaçaments segurs, i que estiguin protegits, bé per controls d' accés físics adequats al seu nivell de criticitat o mitjançant mesures apropiades als mateixos. Les mesures implantades hauran de garantir la seva protecció en funció dels requisits legals i normatius existents, el seu valor per a l'

organització, i el risc al qual poden estar sotmesos en cada moment, d' acord amb l' article 18 de l' ENS. Com a mínim, les sales han d' estar tancades i disposar d' un control d' accessos.

#### **f) Integritat i actualització del sistema**

La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d' actius del sistema o la seva modificació requerirà autorització formal prèvia del responsable del sistema. L' avaluació i monitoratge permanent permetrà adequar l' estat de seguretat dels sistemes atenent les deficiències de configuració, les vulnerabilitats identificades i les actualitzacions que els afectin, així com la detecció primerenca de qualsevol incident que tingui lloc sobre els mateixos, tal com consta a l' article 21 de l' ENS. Els detalls sobre l' auditoria de registres de monitoratge per a la correcta adequació del sistema es desenvoluparan en una normativa específica.

#### **g) Protecció de la informació emmagatzemada i en trànsit**

Es prestarà especial atenció a la protecció de la informació emmagatzemada o en trànsit en equips o dispositius portàtils o mòbils, perifèrics i xarxes obertes. S' aplicaran procediments per garantir la recuperació i conservació a llarg termini dels documents electrònics. La informació en suport no electrònic, relacionada amb la informació electrònica, que es trobi en l' àmbit d' aplicació de l' ENS, haurà d' estar protegida amb el mateix grau de seguretat.

Tota la informació, ja sigui en paper o en format digital, s' etiquetarà adequadament segons la seva classificació per facilitar-ne l' ús, la manipulació i la protecció. Els documents i els seus suports portaran un etiquetatge que permeti reconèixer el seu nivell de classificació d' acord amb els criteris de seguretat de l' ENS, complint amb el disposat en el seu Annex II sobre la política de seguretat i l' estàndard de classificació i etiquetatge de la informació.

#### **h) Registre d' activitats i detecció de codi danyós**

Per garantir la seguretat dels sistemes d' informació i complir amb l' ENS s' implementaran mecanismes de registre i monitoratge d' activitats dels usuaris, així com la detecció de codi danyós. Aquestes mesures busquen assegurar el compliment de la política de seguretat de la informació i la protecció de dades personals, respectant els drets fonamentals a l' honor, la intimitat i la pròpia imatge.

L' IMAS registrarà les activitats dels usuaris que accedeixin als sistemes d' informació, incloent només la informació necessària per monitoritzar l' ús adequat dels recursos,

investigar activitats indegudes i documentar-les i assegurar la traçabilitat de les accions realitzades. A més, s'analitzaran les comunicacions per impedir accessos no autoritzats, detectar i prevenir atacs, i bloquejar la distribució de codis danyosos, sempre respectant els principis de limitació de la finalitat i minimització de dades.

Cada usuari haurà d'estar identificat de forma única per conèixer els seus drets d'accés i activitats realitzades, permetent corregir situacions indegudes i, si cal, exigir-li responsabilitats.

#### **i) Incidents de seguretat**

L'IMAS disposarà d'un procediment específic per a la gestió d'incidents de seguretat, en compliment de l'article 25 de l'ENS.

Aquest procediment serà accessible i conegut per les persones que exerceixin rols clau en la seva implementació, garantint que tots els responsables compreguin les seves obligacions i responsabilitats.

El procediment abastarà els aspectes següents:

- a) Mecanismes de detecció.
- b) Criteris de classificació.
- c) Procediments d'anàlisi i resolució.
- d) Lleres de comunicació interna i externa.
- e) Notificació a autoritats.
- f) Registre d'actuacions.

#### **j) Continuitat de l'activitat**

Els sistemes de l'IMAS disposaran de còpies de seguretat i de mecanismes que garanteixin la continuïtat de les operacions en cas de pèrdua dels mitjans habituals de treball o afecció greu dels actius emprats, tal com indica l'article 26 de l'ENS.

#### **k) Millora contínua del procés de seguretat**

El procés integral per a la gestió de la protecció de dades personals i seguretat de la informació serà millorat de manera contínua en base als indicadors que es considerin en funció dels requisits establerts, el nivell de maduresa en cada moment i les necessitats estratègiques de l'IMAS, tal com indica l'article 27 de l'ENS.

## 11. GARANTIES DE LA SEGURETAT DELS SISTEMES

Per garantir la seguretat dels sistemes d'informació de l'IMAS i complir amb els estàndards de l'ENS, s'implementaran una sèrie de mesures i procediments que assegurin la protecció dels actius digitals i de les dades personals tractades per l'entitat.

Aquestes mesures s'ajustaran als requisits mínims establerts a l'ENS considerant els riscos associats als sistemes d'informació i la seva criticitat. Aquest apartat detalla les garanties que s'aplicaran a l'IMAS per assegurar el compliment de la normativa vigent, a més d'oferir un marc clar per a la gestió de la seguretat dels sistemes, tant per als serveis interns com per a aquells prestats per tercers.

A continuació, es descriuen les principals mesures i procediments a seguir per garantir la seguretat dels sistemes d'informació a l'IMAS.

### **a) Declaració d'Aplicabilitat**

L'IMAS adoptarà les mesures de seguretat establertes en l'Annex II de l'ENS. Aquestes mesures s'implementaran considerant els aspectes clau següents:

- Els actius que constitueixen els sistemes d'informació de l'IMAS, assegurant la seva protecció segons el seu valor i criticitat.
- La categoria del sistema: Basada en la classificació dels sistemes d'informació segons el seu nivell de risc (alt, mitjà o baix), tal com el defineix l'ENS.
- Gestió de riscos: Es prendran decisions específiques per gestionar els riscos identificats, aplicant controls i salvaguardes que protegeixin els actius i assegurin el compliment dels principis de seguretat.

Les mesures de seguretat adoptades seran les mínimes exigibles i podran ser ampliades o reforçades a criteri del Responsable de Seguretat de l'IMAS, mitjançant la implementació de mesures addicionals o compensatòries. Aquestes mesures compensatòries s'utilitzaran sempre que es justifiqui que ofereixen un nivell de protecció equivalent o superior al de les mesures descrites a l'Annex II de l'ENS. Aquest conjunt de mesures quedarà reflectit en un document denominat Declaració d'Aplicabilitat, que serà signat pel Responsable de Seguretat.

La declaració detallarà la correspondència entre les mesures compensatòries implantades i les mesures originals de l'Annex II, garantint que els riscos associats als actius queden degudament gestionats.

### **b) Catàleg de Serveis Electrònics**

L'IMAS elaborarà un Catàleg de Serveis Electrònics que recollirà l'inventari dels serveis gestionats electrònicament i la informació associada a ells. Aquest catàleg s'emprarà com a referència per avaluar els requisits de seguretat de les dades

emmagatzemades i tractades en aquests serveis, tal com s' estableix a l' article 40 de l' ENS.

El catàleg també servirà per analitzar l'impacte de possibles amenaces sobre els serveis electrònics i ajudarà en la realització d'anàlisis de riscos i continuïtat del negoci, seguint les mesures de seguretat establertes a l'ENS. Aquest catàleg abastarà tots els serveis electrònics que l'IMAS gestioni per dur a terme les seves competències i estarà alineat amb la Llei 39/2015 de Procediment Administratiu Comú de les Administracions Públiques.

### **c) Directrius per a l' Estructuració de la Documentació de Seguretat**

L' IMAS adoptarà una normativa específica per a l' estructuració de la documentació de seguretat, en compliment de l' article 12.1.e) de l' ENS.

Aquesta normativa inclourà la creació de procediments i documents que abordin els aspectes següents:

- Auditories de registres de monitoratge.
- Classificació i tractament de la informació.
- Control d' accessos lògics.
- Gestió d' incidents de seguretat

La normativa de seguretat serà concisa i contindrà referències clares per facilitar la seva interpretació i aplicació. A més, inclourà mètriques per avaluar el compliment dels procediments i oferirà la possibilitat de proposar millores. Tots els empleats de l' entitat estan subjectes a diverses funcions i obligacions segons el seu perfil professional.

## **12. OBLIGACIONS I FORMACIÓ DEL PERSONAL**

Tot el personal ha de conèixer i complir aquesta política, així com les normatives, procediments i instruccions que conformen el Sistema de Gestió de Seguretat de la Informació (en endavant SGSI). L' IMAS garantirà que aquesta informació sigui accessible a tot el personal i a tercers que prestin serveis. Cada empleat és responsable de l' ús i administració segura dels sistemes i informació. Aquestes obligacions es detallaran en la normativa accessòria.

L' IMAS promourà plans de formació i conscienciació que inclouran:

- Sessions formatives recurrents sobre protecció de dades i seguretat de la informació per a noves incorporacions i personal actiu.
- Formació contínua per al personal amb responsabilitats en sistemes.
- Programes de formació obligatoris per a empleats amb responsabilitats especialitzades en seguretat de la informació i protecció de dades.

Les formacions es dissenyaran segons les necessitats específiques de cada grup, prioritzant àrees clau per a la seguretat i el compliment normatiu.

### **13. RELACIONS AMB TERCERS**

Quan l' IMAS gestioni informació d' altres organismes o presti serveis a aquests, aquests organismes seran partícips de la present Política. L' IMAS establirà canals clars de coordinació per a la gestió d' informació i la resolució d' incidents de seguretat. Això inclourà la definició de procediments operatius, garantint que la cooperació amb tercers es dugui a terme conforme a les directrius de seguretat establertes.

Així mateix, quan l' IMAS utilitzi serveis de tercers o comparteixi informació amb ells, aquests tercers seran igualment partícips d' aquesta Política, així com de la Normativa de Seguretat aplicable als serveis o la informació implicada. Les terceres parts estaran subjectes a les obligacions de l' esmentada normativa.

#### **a) Requisits de Conformitat amb l' ENS per a Terceres Parts**

Les entitats del sector privat que prestin serveis a l' IMAS, ja sigui mitjançant solucions tecnològiques o serveis externs, hauran de complir amb els requisits establerts a l' ENS.

Els plecs de prescripcions administratives i tècniques de l' IMAS recolliran tots els requisits necessaris per assegurar que els sistemes d' informació gestionats pels contractistes compleixen amb els estàndards de seguretat exigits per l' ENS.

#### **b) Designació d'un Punt de Contacte (POC)**

En el cas de serveis externalitzats, les entitats prestadores de serveis hauran de designar un punt o persona de contacte (POC) responsable de la seguretat de la informació gestionada.

Aquest POC serà l' encarregat de supervisar el compliment dels requisits de seguretat associats al servei, així com de gestionar les comunicacions i els incidents de seguretat.

El POC coordinarà totes les actuacions necessàries per garantir la seguretat de la informació tractada en el marc del servei prestat, en compliment de les obligacions de l' article 13.5 de l' ENS.

#### **c) Conscienciació en Seguretat de Terceres Parts**

L' IMAS s' assegurarà que el personal de les terceres parts que intervenen en la gestió de serveis o informació estigui adequadament format i conscienciat en matèria de seguretat de la informació. Aquest personal haurà de rebre una formació equivalent al nivell de conscienciació i compliment establert en la Política de Seguretat de l' IMAS.

En cas que alguna tercera part no pugui complir amb algun aspecte de la present Política de Seguretat, caldrà presentar un informe elaborat pel Responsable de Seguretat de l' IMAS, el qual haurà de detallar els riscos associats a l' incompliment i les mesures que es prendran per tractar-los. Aquest informe haurà de ser aprovat pels responsables de la informació i els serveis implicats, abans de l' inici de qualsevol relació contractual amb la tercera part en qüestió.

#### **d) Procediments de Comunicació i Resolució d' Incidències**

S' establiran procediments específics per a la comunicació i resolució d' incidències de seguretat que involucrin terceres parts. Aquests procediments asseguraran una resposta àgil i efectiva davant incidents de seguretat, permetent la ràpida detecció, anàlisi i resolució de problemes que puguin sorgir en el maneig de la informació o la prestació de serveis.

#### **e) Adquisició de Productes i Serveis de Seguretat**

En el procés d' adquisició de productes de seguretat o contractació de serveis de seguretat en l' àmbit de les tecnologies de la informació i la comunicació, l' IMAS es compromet a utilitzar solucions que siguin proporcionals a la categoria del sistema i al nivell de seguretat requerit.

Per garantir l' eficàcia d' aquestes adquisicions, es tindran en compte els aspectes següents:

- **Certificació de funcionalitat de seguretat**

Els productes de seguretat adquirits hauran de comptar amb certificacions que donin suport a la seva funcionalitat en relació amb els objectius de seguretat establerts. Aquesta certificació és essencial per assegurar que les solucions seleccionades compleixen amb els requisits mínims de seguretat definits per l' ENS i altres normatives aplicables.

- **Procés formal d' adquisició**

L' IMAS establirà un procés formal per a la planificació de l' adquisició de nous components del sistema, el qual inclourà les següents etapes:

- Ajust a l' arquitectura de seguretat: Les adquisicions es realitzaran en consonància amb l' arquitectura de seguretat escollida per l' IMAS. Això assegurarà que qualsevol nou component s' integri adequadament en l' entorn de seguretat existent i no comprometi la integritat del sistema.

- Consideració de realitzar una Anàlisi de Riscos en funció de la criticitat del component com a part de l'arquitectura.
- Consideració de necessitats tècniques, formatives i financeres: El procés d'adquisició contemplarà de manera conjunta les necessitats tècniques dels nous components, els requeriments de formació per al personal que els manejarà, així com el finançament necessari per a la seva adquisició i implementació.

- **Avaluació contínua de proveïdors**

A més, l' IMAS durà a terme una avaluació contínua dels proveïdors de productes i serveis de seguretat. Aquesta avaluació inclourà la revisió de la seva capacitat per proporcionar solucions que compleixin amb els estàndards de seguretat i la normativa vigent, així com el seu historial en la gestió d' incidents de seguretat.

## **14. DESENVOLUPAMENT DE LA POLÍTICA**

El compliment dels objectius marcats en aquesta Política es duu a terme mitjançant el desenvolupament de documentació que componen les normes i procediments de seguretat associats al compliment de l' ENS. Per a la seva organització s' ha definit una Norma per a la Gestió de la Documentació, que estableix les directrius per a l' organització, gestió i accés.

La revisió anual de la present Política correspon al CSI proposant en cas que sigui necessari millores de la mateixa, per a la seva aprovació per part del mateix òrgan que la va aprovar inicialment.