1. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información (en adelante Política), ha sido aprobada por resolución de la Presidencia del Instituto Mallorquín de Asuntos Sociales, en adelante IMAS.

Esta Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

El IMAS es un organismo autónomo, adscrito al Departamento de Bienestar Social del Consejo de Mallorca, que ejerce las competencias atribuidas por cualquier título al Consell de Mallorca en materia de servicios sociales y protección de menores, así como cualquier finalidad determinada en sus Estatutos (BOIB Núm. 67 de 18 de mayo de 2019)

El IMAS, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para la correcta prestación de los servicios, ejecución y ejercicio de sus competencias. Estos sistemas deben garantizar la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. El IMAS aplicará las medidas mínimas de seguridad exigidas por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelanta ENS) y, realizará un seguimiento continuo de los niveles de prestación de servicios, análisis de las vulnerabilidades reportadas, y preparará una respuesta efectiva ante los incidentes, para garantizar la continuidad de los servicios prestados.

3. MISIÓN DE IMAS

El IMAS desea potenciar el uso de las nuevas tecnologías, en el desarrollo de sus competencias e interacción con la propia ciudadanía. Estas competencias pueden encontrarse en el artículo 2 de los Estatutos del IMAS

4. OBJETO

La presente política de seguridad de la información y protección de datos personales tiene por objeto:

1) Establecer el marco normativo que recoja los principios básicos y requisitos mínimos que permitan una protección adecuada de la información que se

gestiona en el ámbito de las competencias del IMAS, y que será de aplicación, a todos los servicios y sistemas de información y a todas las actividades de tratamiento de datos personales de las que sea responsable el IMAS. En particular, la Política establece las directrices que rigen la forma en la que el IMAS gestiona y protege la información que trata y los servicios que presta.

2) Definir el modelo organizativo y técnico apropiado para garantizar el cumplimiento de la normativa aplicable al tratamiento de los datos personales y el acceso y utilización de los sistemas de información.

5. ALCANCE

Lo dispuesto en esta política será de obligado cumplimiento para todas las unidades que conforman la estructura orgánica del IMAS y para todo el personal con acceso a la información de las que son responsables aquellas, con independencia de su destino, condición laboral o relación contractual que autorice el acceso a la información.

En particular, quedarán comprendidas en el ámbito subjetivo de aplicación:

1) El IMAS, respecto de la información tratada por cualquier medio con independencia del soporte en el que se encuentre.
2) Otras personas o entidades con acceso a información: cuando se utilicen servicios externos o permitan el acceso legítimo o cedan información a terceras personas, en particular cuando éstas participen, utilicen, operen o administren datos personales y/o sistemas de información y comunicaciones, se les hará partícipes de esta Política, quedando sujetas a las obligaciones establecidas en las mismas.

6. MARCO NORMATIVO

El marco legal y regulatorio que afecta al desarrollo de las actividades y competencias del IMAS en el ámbito del ENS, está constituido por normas jurídicas estatales, autonómicas y sectoriales orientadas a la administración electrónica, a la ciberseguridad y seguridad de la información en general, así como a la protección de datos personales.

En concreto, la legislación y las principales normativas aplicables serían las siguientes:

a) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

c) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
d) Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas.
e) Ley 40/2015, de 1 de octubre, de régimen jurídico del Sector Público.
f) Ley 12/1993, de 20 de diciembre, de atribución de competencias en materia de Servicios Sociales y Asistencia Social.
g) Ley 8/1997, de 18 de diciembre, de atribución de competencias a los Consejos Insulares en materia de Tutela, Acogida y Adopción de menores.
h) Ley 14/2001, de 29 de octubre, de transferencia de competencias a los Consejos Insulares en materia de Servicios Sociales y Seguridad Social.
i) Ley 4/2009, de 11 de junio, de servicios sociales de las Illes Balears.
j) Acuerdo del pleno del consejo insular de Mallorca, de día 11 de abril de 2019, por el que se aprueban los Estatutos del IMAS.
k) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
l) Real Decreto 1372/1986, de 13 de junio, por el que se aprueba el Reglamento de Bienes de las Entidades Locales.
m) Ley 57/2003, de 16 de diciembre, de Medidas para la Modernización del Gobierno Local.
n) Resto de normativa que resulte de aplicación.
o) Guías serie 800 CCN-CERT.
p) Instrucciones técnicas referentes al ENS.

También forman parte del marco legal y regulatorio las restantes normas aplicables a la Administración Electrónica del IMAS, que sean desarrollo de las anteriores o estén relacionadas con ellas, comprendidas dentro del ámbito de aplicación de la presente Política.

7. PRINCIPIOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

El IMAS será responsable del cumplimiento de la presente política de seguridad de la información y protección de datos personales, y deberá ser capaz de demostrar dicho cumplimiento, asumiendo una responsabilidad proactiva. Para ello, tratará la información y los datos personales conforme a los siguientes principios estructurales:

a) **Alcance estratégico**: La protección de datos personales y la seguridad de la información deben contar con el compromiso y apoyo de todos los niveles directivos del IMAS, asegurando que se integren con el resto de las iniciativas estratégicas de la entidad para conformar un complejo coherente y eficaz.

b) **Responsabilidad proactiva**: El IMAS será responsable de cumplir con los principios establecidos en este artículo, adoptando las medidas organizativas, operacionales y técnicas necesarias para demostrar dicho cumplimiento.

c) **Diferenciación de responsabilidades**: Las responsabilidades sobre los datos personales, la información, los servicios y la seguridad estarán claramente diferenciadas en diversos roles, los cuales deberán estar capacitados para desempeñar sus funciones. Se establecerán mecanismos de coordinación y resolución de conflictos para garantizar una gestión eficaz de la seguridad de los sistemas de información.

d) **Cumplimiento**: El IMAS adoptará las medidas técnicas, organizativas y procedimentales necesarias para asegurar el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos personales.

e) **Licitud, lealtad y transparencia**: Los datos personales se tratarán de forma lícita, leal y transparente, respetando los derechos de los titulares de los datos y sus representantes.

f) **Limitación de la finalidad**: Los datos personales se recogerán con fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines, salvo en casos de interés público, investigación científica o fines estadísticos.

g) **Minimización de datos**: Solo se recogerán y tratarán los datos personales que sean estrictamente necesarios, adecuados y pertinentes para los fines correspondientes.

h) **Exactitud**: Se garantizará que los datos personales sean exactos y se actualizarán cuando sea necesario. Se adoptarán medidas para suprimir o rectificar cualquier dato inexacto de manera oportuna.

i) **Limitación del plazo de conservación**: Los datos personales se conservarán únicamente durante el tiempo necesario para cumplir con los fines del tratamiento y las obligaciones legales relacionadas.

j) **Integridad y confidencialidad**: Los datos se tratarán de forma que se garantice una seguridad adecuada, protegiéndolos contra el tratamiento no autorizado, pérdida, destrucción o daño accidental mediante medidas técnicas y organizativas apropiadas.

k) **Atención a los derechos de las personas interesadas**: Se garantizará el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad por parte de las personas interesadas.

l) **Actualización y adecuación**: La protección de los datos de los sistemas de información del IMAS será adaptada y actualizada en función de los cambios en el entorno, manteniendo siempre su eficacia y eficiencia.

m) **Seguridad como proceso integral**: La seguridad de la información será entendida como un proceso integral que engloba todos los aspectos técnicos, humanos, organizativos y jurídicos relacionados con los sistemas de información del IMAS.

n) **Gestión de la seguridad basada en los riesgos**: El IMAS gestionará la seguridad de sus sistemas e información mediante una evaluación continua de riesgos, asegurando que se implementen medidas de control proporcionadas a la naturaleza de los datos y los servicios.

ñ) **Prevención, detección, respuesta y conservación**: Se establecerán medidas preventivas, de detección, de respuesta ante incidentes y de conservación de la información, con el fin de minimizar las vulnerabilidades y proteger los datos y servicios del IMAS.

o) **Proporcionalidad**: Las medidas de protección de la seguridad de la información serán proporcionales a los riesgos y a la criticidad de los datos personales y los servicios.

q) **Reducción de probabilidad e impacto:** Se implementarán múltiples capas de seguridad para reducir los tiempos de respuesta ante incidentes, disminuir la probabilidad de que ocurran, y minimizar su impacto tanto en las personas afectadas como en los activos del IMAS.

r) **Líneas de defensa:** La estrategia de protección incluirá varias capas de seguridad que permitirán:

1. Reaccionar de manera oportuna ante incidentes inevitables.
2. Reducir la probabilidad de comprometer todo el sistema de información.
3. Minimizar el impacto final. Estas capas incluirán medidas organizativas, físicas y lógicas.

s) **Seguridad de los activos de información:** Se aplicarán medidas técnicas y organizativas para que el personal con acceso a los activos de información y datos personales conozcan sus responsabilidades, reduciendo el riesgo de uso indebido.

t) **Seguridad en la gestión de comunicaciones:** Se establecerán procedimientos para gestionar la seguridad de las tecnologías de la información y comunicaciones. La información transmitida por redes será protegida de acuerdo a su nivel de sensibilidad y criticidad, utilizando mecanismos adecuados.

u) **Gestión de incidentes de seguridad:** El IMAS destinará los recursos económicos, humanos y tecnológicos necesarios para fortalecer la ciberseguridad, conforme al principio de proporcionalidad y el nivel de seguridad requerido. Se

planificarán y documentarán procedimientos en un marco de mejora continua con participación de los actores involucrados.

v) **Seguridad del entorno tecnológico:** Con el objetivo de garantizar un entorno tecnológico seguro el IMAS implementará las medidas necesarias para cumplir con la política de seguridad de la información y protección de datos personales, evitando la expansión de incidentes derivados de vulnerabilidades entre los sistemas.

w) **Vigilancia continua y reevaluación periódica:** Se establecerán mecanismos de vigilancia continua para detectar actividades anómalas, y se evaluará constantemente el estado de seguridad de los activos para identificar vulnerabilidades. Las medidas de seguridad se actualizarán periódicamente para responder a la evolución de los riesgos.

x) **Infraestructura y recursos informáticos:** El IMAS cuenta con una infraestructura tecnológica que garantiza la eficiencia y eficacia en la prestación de servicios, incluyendo equipos, programas, servidores, redes, y servicios corporativos (como el correo electrónico) y el acceso a aplicaciones.

y) **Adquisición e instalación de productos de seguridad:** El uso de la infraestructura informática se ajustará a las directrices internas y a las normativas y procedimientos de seguridad vigentes.

z) **Seguridad desde el diseño y por defecto:** El IMAS promoverá la inclusión de la protección de datos y seguridad desde el diseño y por defecto en todos los sistemas de información y tratamientos de datos personales, siguiendo la normativa aplicable. Se adoptará un enfoque que respete la privacidad, la transparencia y los principios de seguridad, disponibilidad, autenticidad, trazabilidad, integridad y confidencialidad en los procesos futuros.

8. MODELO DE GOBERNANZA

Para garantizar el cumplimiento del ENS y las obligaciones derivadas de la seguridad de la información, el IMAS designará roles de seguridad y constituirá un Comité de Seguridad de la información.

8.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable/s de Información: Persona que ocupe la Vicepresidencia.

- Responsable de los Servicios: Personas que ocupen las Direcciones Insulares y la Gerencia del IMAS
- Responsable de la Seguridad: Persona que ocupe la Jefatura de la Sección de Seguridad, adscrita al Departamento de Informática.
- Responsable del Sistema: Persona que ocupe la Jefatura del Departamento de Informática
- Delegado de Protección de Datos: Empresa externa

A fin de dotar de estabilidad a la estructura de la seguridad de la información y de protección de datos personales, los roles descritos se asignan a puestos o cargos de la estructura orgánica del IMAS. Por lo tanto, el nombramiento para el puesto o cargo que corresponda conllevará la asunción del rol, así como la consiguiente aceptación de responsabilidades y funciones en el ejercicio del puesto o cargo correspondiente.

A continuación, se procede a describir las funciones y responsabilidades de los roles de seguridad de manera pormenorizada:

8.1.1. Responsable de la información

Le corresponden las siguientes responsabilidades y funciones:

a) Responsabilidad última del uso que se haga de la información, y de su protección.
b) Responsabilidad última de cualquier error o negligencia que conlleve un incidente de seguridad, en el ámbito de protección de datos personales en las dimensiones de confidencialidad o de integridad y en el ámbito de seguridad de la información en la dimensión de disponibilidad.
c) Valora la información y los servicios pertenecientes a su sistema de información, según el impacto que tendría un incidente que afectara a la seguridad de la información con perjuicio para las dimensiones de seguridad, siguiendo el procedimiento y dentro del marco establecido en el Anexo I del ENS.
d) Determina los requisitos de seguridad y los niveles de seguridad de la información y de los servicios pertenecientes a su sistema de información. La aprobación formal de los requisitos de seguridad, niveles de seguridad y valoraciones se realizará por el responsable de la información a propuesta conjunta de los responsables del servicio de su sistema de información (éstos proponen y determinan previamente los requisitos, niveles y valoraciones de seguridad de la información y del servicio) con la asistencia del responsable de seguridad y con el soporte del responsable del sistema.
e) Propone la categoría de su información y/o de su sistema/s de información, dentro de su ámbito competencial, al responsable de seguridad.

f) Con carácter general, debe tener en cuenta las indicaciones del responsable del sistema y del responsable de seguridad.

8.1.2. Responsable del servicio

Le corresponden las siguientes responsabilidades y funciones:

a) Propone al responsable de información para su aprobación definitiva: la valoración de su servicio y de la información tratada en el mismo, y la determinación de los requisitos de seguridad y los niveles de seguridad del mismo.
   Para la valoración tendrá en cuenta el impacto que supondría un incidente que afectará a la seguridad con perjuicio para las dimensiones de seguridad, siguiendo el procedimiento y dentro del marco establecido en el Anexo I del ENS, con la asistencia del responsable de seguridad y con el soporte del responsable del sistema.
b) Informar de todas aquellas necesidades, afecciones e incidentes que estén directamente relacionadas con sus servicios.
c) Con carácter general, debe tener en cuenta las indicaciones del responsable del sistema y del responsable de seguridad. Responsabilidad última del uso que se haga de la información, y de su protección.

8.1.3. Responsable de seguridad.

Le corresponden las siguientes responsabilidades y funciones:

a) Mantiene la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la presente política y en el resto de normativa aplicable.
b) Promueve la formación y concienciación en materia de seguridad, definiendo e impulsando iniciativas de formación y sensibilización para el desarrollo y promoción de buenas prácticas en materia de seguridad de la información.
c) Elabora y propone para su aprobación la política de seguridad, que incluye las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los incidentes de seguridad que afecten al IMAS.
d) Desarrolla las normas, procedimientos, guías e instrucciones de seguridad y supervisa su efectividad, impulsando la realización de las auditorías periódica de seguridad que sean necesarias.
e) Recibe, interpreta y aplica las instrucciones y guías emanadas de las autoridades competentes, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

f) Recopila, prepara y suministra información o documentación a las autoridades competentes, a su solicitud o por propia iniciativa.
g) Firma la declaración de aplicabilidad, documento que formaliza la relación de medidas de seguridad seleccionadas, que se realizará con la asistencia del responsable del sistema.
h) Actúa como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
i) Constituye el punto de contacto con la autoridad competente en materia de seguridad de la información.
j) Es interlocutor de los roles de responsable de la información, responsables del servicio y responsable del sistema.
k) Asiste a los responsables de información y responsable de servicio, sobre el correcto ejercicio de sus funciones en materia del ENS.
l) Notifica a la autoridad competente los incidentes de seguridad que tengan efectos perturbadores en la prestación de los servicios.
m) Participa en la gestión adecuada de los incidentes de seguridad y de las acciones de tratamiento que se sigan, con la asistencia del Responsable del sistema.
n) Analiza y propone salvaguardas que prevengan incidentes similares en el futuro, con la asistencia del Responsable del sistema.
o) Reporta al responsable de la información y al responsable del servicio, respectivamente, de las decisiones e incidentes en materia de seguridad que afecten a la información y al servicio que les compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados, con la asistencia del responsable del sistema.
p) Determina la categoría del sistema de información conforme a las valoraciones propuestas por responsables de información y de servicios, y con la asistencia del responsable del sistema. Impulsa y realiza el análisis de riesgos periódico, y el informe de resultados del proceso de análisis de riesgos y su Plan de Tratamiento de riesgos, y, además, asume la responsabilidad de gestión de las tareas del Plan de Tratamiento de Riesgos. En todo el proceso, cuenta con la asistencia del responsable del sistema para la infraestructura TIC.
q) Gestiona la realización de auditorías de los sistemas de información en los plazos que establece el ENS.
r) Analiza los resultados de los análisis de riesgos y auditorías realizadas y propone acciones de mejora y correctoras para el adecuado cumplimiento y alineamiento con el ENS.
s) Analiza y propone mejoras organizativas, de procedimientos y funcionales en el marco del plan de alineamiento del ENS. Para ello, se encarga de identificar los niveles de cumplimiento de las medidas de seguridad aplicables y determinar las recomendaciones correspondientes, y

promueve la implantación coordinada de las mismas y de los sistemas de información afectos al ENS.

t) Adopta o en su caso, valida las propuestas de las medidas urgentes que se estimen necesarias para prevenir, mantener y restablecer la seguridad de la información en todas aquellas situaciones que constituyan amenazas y generen riesgos para la seguridad de la información en cuanto a disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad, con especial incidencia en la gestión inminente de ciber incidentes asociados a los sistemas y tecnologías de Información y comunicaciones (TIC).
u) Garantiza el adecuado reporte al Centro Criptológico Nacional de los indicadores necesarios para obtener el Informe Nacional del Estado de la Seguridad (INES) según lo establecido en el artículo 32 del ENS.
v) Con carácter general para la ejecución de las responsabilidades y funciones descritas, debe disponer del soporte del responsable del sistema.

8.1.4. Responsable del sistema

Le corresponden las siguientes responsabilidades y funciones:

a) Desarrolla, opera y mantiene el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Define la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Debe cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d) Define la organización y el despliegue de los procesos tecnológicos.
e) Reporta al responsable de la información de las incidencias funcionales relativas a la información que le compete; reporta al responsable del servicio de las incidencias funcionales relativas al servicio que le compete; y reporta al responsable de seguridad de las actuaciones en materia de seguridad, en particular, en lo relativo a decisiones de arquitectura del sistema.
f) Planifica la implantación de las salvaguardas en el sistema.
g) Ejecuta el plan de mejora de la seguridad que se apruebe de ser necesario, para atender a los riesgos que no son aceptables.
h) Implementa, gestiona y mantiene las medidas de seguridad aplicables a los sistemas de tecnologías de información.
i) Gestiona los servicios de seguridad.
j) Propone medidas de gestión y control de acceso a los sistemas de información y su gestión. Implementa, gestiona y mantiene las medidas de seguridad aplicables a la gestión de acceso a los sistemas de información.

k) Reporta al responsable del sistema y al responsable de seguridad de los incidentes de seguridad y de las acciones de configuración, actualización o corrección.
l) Gestiona, configura y actualiza el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de tecnología de la Información.
m) Gestiona las autorizaciones y privilegios concedidos a personas usuarias del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado y el aseguramiento de la aplicación de los procedimientos que se aprueben para el manejo del sistema de información.
n) Aplica los procedimientos operativos de seguridad.
o) Supervisa que todo el equipamiento se ajusta a lo autorizado, supervisa las actuaciones y la aplicación de los procedimientos de seguridad, supervisa que las actividades de las personas usuarias del sistema son conformes a lo autorizado para cada una de ellas, y también supervisa las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
p) Monitoriza el estado de la seguridad y el cumplimiento de los controles en su ámbito competencial de las tecnologías de la información y las comunicaciones.
q) Informa al responsable de seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
r) Asiste al responsable de seguridad para la determinación por este de la categoría del sistema de información.
s) Asiste al responsable de seguridad para la firma por este de la Declaración de Aplicabilidad.
t) Asiste al responsable de seguridad durante el proceso de análisis de riesgos y en particular, en la elaboración del informe de resultados y de su Plan de Tratamiento de riesgos. Gestiona el desarrollo y ejecución de las tareas del Plan de Tratamiento de Riesgos dentro del proceso de Análisis y Gestión de Riesgos y de acuerdo con las instrucciones y colaboración inmediata del responsable de seguridad correspondiente, dentro de su ámbito competencial de tecnologías de la información y las comunicaciones.
u) Gestiona de manera adecuada los incidentes de seguridad, en particular las tareas que se le asignen para la prevención, detección, respuesta y conservación de los incidentes y de las acciones de tratamiento que se sigan, de acuerdo con las funciones que se establezcan en el procedimiento que regule la gestión de incidentes.
v) Asiste en la notificación de las violaciones de seguridad de los datos personales.

w) Asiste al responsable de seguridad en las consultas técnicas que surjan durante el desarrollo de las auditorías y resto de procesos para el cumplimiento del ENS, dentro de su ámbito competencial de tecnologías de la información y las comunicaciones.
x) Cualesquiera otras actuaciones del ámbito de la seguridad relacionadas con su ámbito funcional y competencial que le sean encomendadas por el responsable de seguridad, por el responsable del sistema o por el Comité de Seguridad.

8.1.5. Delegado de Protección de Datos

Le corresponden las siguientes responsabilidades y funciones:

a) Informa y asesora al responsable o al encargado del tratamiento y al personal empleado que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras normas o disposiciones de protección de datos.
b) Supervisa el cumplimiento por el responsable o el encargado del tratamiento de lo dispuesto en el RGPD, en otras normas o disposiciones de protección de datos personales y en la presente política, en particular respecto a la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
c) Ofrece el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
d) Coopera con la autoridad de control competente.
e) Actúa como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 RGPD y realizar consultas, en su caso, sobre cualquier otro asunto.
f) Cualquier otra función o responsabilidad que la normativa de protección de datos le atribuya y, especialmente, las detalladas en el apartado 9.1.3. de la presente Política.

8.2. Comité de Seguridad de la Información

El Comité de Seguridad de la Información (en adelante CSI), es el órgano colegiado superior competente para la toma de decisiones y ejercicio de funciones de dirección y coordinación en materia de seguridad de la información y protección de datos con plenos efectos en todo el IMAS, y que da cumplimiento a la medida 3.1 política de seguridad del marco organizativo del Anexo II del ENS y resto de normativa de protección de datos.

El Comité deberá reunirse de forma semestral, con carácter ordinario.

8.2.1. Funciones del Comité de Seguridad de la Información

El CSI ostentará a las siguientes funciones:

a) Coordina todas las funciones de seguridad del IMAS.
b) Aprueba la normativa de seguridad de la información y vela, impulsa, supervisa el cumplimiento de esta.
c) Atiende las inquietudes manifestadas en el ámbito de seguridad de la información en las sesiones del comité y se las transmite a los responsables respectivos para recabar respuestas y soluciones.
d) Recaba, de los responsables los informes sobre el estado de la seguridad.
e) En su caso, propone y designa roles en el ámbito de seguridad de la información.
f) Recibe las comunicaciones del responsable de seguridad relacionadas con los cambios de normativa de seguridad de la información.
g) Promueve la mejora continua de la seguridad de la información.
h) Vela porque la seguridad de la información se tenga en cuenta en todos los proyectos desde su diseño inicial hasta su puesta en ejecución.
i) Recibe dación en cuenta de la normativa y procedimientos de seguridad derivados de la presente política.
j) Recibe dación en cuenta de las medidas técnicas y organizativas de seguridad de la información.
k) Recibe dación en cuenta del estado de los procesos de análisis de riesgos, auditorías, medidas de seguridad y resto de actuaciones que den cumplimiento al ENS.
l) Aprueba el informe de resultados del proceso de análisis de riesgos y su correspondiente plan de tratamiento de riesgos.
m) Aprueba el plan de mejora de la seguridad que se apruebe de ser necesario, para atender a los riesgos que no son aceptables, a propuesta del responsable de seguridad.
n) Recibe dación en cuenta de los niveles de seguridad de la información y de la categorización de los Sistemas de información y los servicios.
o) Recibe dación en cuenta de la Declaración de aplicabilidad.
p) Recibe dación en cuenta de los incidentes de seguridad acontecidos.
q) Recibe dación en cuenta del estado de la seguridad y de las posibles incidencias en la ejecución de las medidas de seguridad.
r) Elaborar y revisar regularmente la Política de Seguridad de la Información para su ulterior aprobación por el órgano competente.
s) Aprobar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
t) Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

8.2.2. Composición del Comité de Seguridad de la Información

EL CSI, como órgano colegiado, está formado por los siguientes miembros:

a) **Presidente/a:** Será ejercido por la persona que ostente el cargo de Responsable de la Información y atenderá a las siguientes funciones:
b) Ostentar la representación del órgano.
c) Acordar la convocatoria de las sesiones ordinarias y extraordinarias y la fijación del orden del día, teniendo en cuenta, en su caso, las peticiones de los demás miembros formuladas con la suficiente antelación.
d) Presidir las sesiones del Comité, moderar el desarrollo de los debates y suspenderlos por causas justificadas.
e) Dirigir las deliberaciones y, en general, ejercitar las facultades precisas para el adecuado desarrollo de las sesiones.
f) Dirimir con su voto los empates, a efectos de adoptar acuerdos.
g) Asegurar el cumplimiento de la normativa aplicable.
h) Revisar las actas y certificaciones de los acuerdos del Comité.
i) Ejercer cuantas otras funciones sean inherentes a su condición de presidente del órgano.

- **Secretario/a:** Recaerá en la persona que ostente la jefatura del Servicio Juridicoadministrativo o persona que le sustituya y atenderá a las siguientes funciones:

a) Asistir a las sesiones con voz, pero sin voto.
b) Preparar las sesiones.
c) Levantar las actas de las sesiones del Comité.
d) Expedir certificaciones de los Acuerdos del Comité.
e) Archivar y custodiar los documentos en que consten las actuaciones desarrolladas por el Comité.

- **Vocales:**
  - Responsables de Servicios[1].
  - Responsable de la Seguridad.
  - Responsable del Sistema.

Las y los vocales del Comité tienen las siguientes funciones:

a) Asistir a las sesiones y participar en los debates.
b) Presentar al Comité las propuestas que estimen oportunas.
c) Emitir su voto, expresando el sentido del mismo, así como formular voto particular discrepante con el parecer de la mayoría. Posibilidad de delegación

[1] Los Responsables Servicios serán convocados cuando se traten cuestiones en las que estén implicados sus servicios, no obstante, podrán acudir voluntariamente cuando lo estimen oportuno.

de voto: en caso de imposibilidad de asistencia del vocal titular o suplente, se podrá delegar el voto en otro miembro del comité.

- **Delegado de Protección de datos (DPD):** con funciones de asesoramiento y supervisión en materia de protección de datos y sin derecho a voto.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del CSI, grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Los miembros del Comité serán designados por resolución de la Presidencia del IMAS.

8.2.3. Normas de Funcionamiento

El funcionamiento del Comité en todo lo no previsto en esta convocatoria se tiene que ajustar, de conformidad a las Disposición Adicional Segunda del Reglamento Orgánico del Consell de Mallorca, a la a lo que prevé la Ley 40/2015, de Régimen Jurídico del Sector Público.

8.2.4 Resolución de conflictos

Si hubiera conflicto entre los responsables, será resuelto por el Comité de Seguridad de la Información.

9. PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

El IMAS, en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, siendo esta el RGPD y la LOPDGDD, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

A este respecto, en el marco de la normativa europea y española, el IMAS asume el compromiso de garantizar la protección de los datos personales que maneja, conforme a los principios y obligaciones establecidas en las citadas normativas, siendo la protección de datos no solo un deber legal, sino también una herramienta clave para salvaguardar los derechos fundamentales de las personas físicas en lo que respecta al tratamiento de su información personal.

Por ello, el IMAS ha desarrollado una política integral que contempla todas las medidas necesarias para garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos personales que trata en el curso de sus actividades.

A continuación, se procederá a detallar los aspectos fundamentales relacionados con la protección de datos personales, abordando las figuras clave implicadas en su gestión, los

principios que rigen su tratamiento, los derechos de las personas interesadas, la evaluación de impacto en la protección de datos y la gestión de incidentes de seguridad.

9.1. Figuras vinculadas a protección de datos personales

En el ámbito de la protección de datos, el IMAS contará con diversas figuras que asumirán roles y responsabilidades específicas para garantizar el cumplimiento de la normativa vigente. Estos roles estarán alineados con el RGPD, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), y el ENS.

A continuación, se describen las principales figuras involucradas:

9.1.1. Responsable del Tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de los datos personales. En concreto, el IMAS ostentará el rol de Responsable del tratamiento en todos aquellos tratamientos en los cuales determine los fines y los medios, los cuales serán definidos y detallados en el Registro de Actividades del Tratamiento (en adelante RAT) de la organización.

Las funciones del Responsable del Tratamiento son, principalmente:

a) Decide y aplica las medidas técnicas y organizativas de seguridad adecuadas a los tratamientos de datos que se encuentren bajo su responsabilidad.
b) Realiza los correspondientes análisis de riesgos y evaluaciones de impacto cuando sean necesarios de acuerdo con el RGPD.
c) Notifica a la autoridad de control competente las violaciones de la seguridad de los datos personales, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de una indicación en la cual se aleguen los motivos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento lo comunicará a la persona interesada sin dilación indebida. Para realizar estas notificaciones contará con la asistencia técnica del responsable del sistema y, en su caso, se valorará la delegación de la tarea en éste, según complejidad técnica la violación.
d) Resuelve las solicitudes de ejercicio de derechos en materia de protección de datos personales con arreglo a los artículos 15 a 22 del RGPD.
e) Con carácter general, desempeña el resto de las funciones que le asigne la normativa de protección de datos personales.

9.1.2. Encargado del Tratamiento

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En concreto, desempeña las siguientes responsabilidades y funciones:

a) Asiste a la persona responsable del tratamiento, teniendo en cuenta la naturaleza del tratamiento, para el cumplimiento de las medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de las personas interesadas.
b) Ayuda a la persona responsable del tratamiento a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición de la persona encargada del tratamiento.
c) A elección de la persona responsable del tratamiento, suprime o devuelve todos los datos personales una vez finalizada la prestación de los servicios de tratamiento, y suprime las copias existentes, a menos que se requiera la conservación de los datos personales.
d) Pone a disposición de la persona responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones.
e) Informa inmediatamente a la persona responsable del tratamiento si, de acuerdo con su criterio, una instrucción o actividad infringe cualquier disposición en materia de protección de datos personales.
f) Notifica sin dilación indebida al responsable del tratamiento de las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
g) Cuando una persona encargada de tratamiento recurra a otra persona encargada (subencargada) para llevar a cabo determinadas actividades de tratamiento por cuenta de la persona responsable, se impondrá a esta otra persona encargada, mediante contrato u otro acto jurídico, las mismas obligaciones de protección de datos personales que las estipuladas en el contrato u acto jurídico entre responsable y encargado principal, en particular la prestación de las garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del RGPD. Si el subencargado incumple sus obligaciones de protección de datos personales, la persona encargada inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones.
h) Con carácter general, desempeña el resto de las funciones que le asigne la normativa de protección de datos personales.

En relación a esta figura, el IMAS, en calidad de Responsable del tratamiento, se compromete a firmar con cada encargado del tratamiento un encargo de tratamiento. En concreto, los encargos de tratamiento en el IMAS son actos jurídicos que establecen la relación entre el responsable del tratamiento y los encargados del tratamiento (entidades

o personas que tratan datos personales en su nombre). Estos acuerdos contendrán los elementos esenciales indicados en el artículo 28 del RGPD, tales como:

- Objeto del tratamiento: La finalidad para la cual se lleva a cabo el tratamiento de los datos personales.
- Duración del tratamiento: El periodo durante el cual se realizará el tratamiento de los datos.
- Naturaleza y finalidad del tratamiento: Descripción clara del tipo de tratamiento que se llevará a cabo y su propósito.
- Tipo de datos personales: Los tipos de datos que se manejarán, tales como datos de salud, datos identificativos o datos económicos.
- Categorías de personas interesadas: Definir a quién pertenecen los datos, como usuarios de servicios sociales, empleados, etc.
- Obligaciones y derechos de ambas partes: Las responsabilidades que deben cumplir tanto el responsable como el encargado en el manejo de los datos personales.

Con el fin de monitorizar el estado de los contratos de encargo, el IMAS se compromete a generar y mantener un registro actualizado de los Encargados de Tratamiento que estén prestando servicio a la entidad y los cuales tengan acceso a datos personales.

9.1.3. Delegado de Protección de Datos

El Delegado de Protección de Datos podrá ser interno o externo, velando siempre por evitar conflictos de interés entre cualquiera de sus miembros.

El Delegado de Protección de la entidad, se ajustará en cada momento a las necesidades según sus funciones, tendrá que ser designado formalmente y comunicado a la Autoridad competente. Estará disponible para la contestación de consultas y atender los ejercicios de derecho a través del correo electrónico o los medios habilitados para tal fin.

Las funciones asociadas a esta figura son:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, así como de las obligaciones derivadas, en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
b) Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
d) Cooperar con la autoridad de control.
e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa citada en el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. Para eso deberá ser capaz de:
    - Solicitar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
    - Solicitar información para supervisar el registro de las operaciones de tratamiento.
    - Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
f) Asesorar sobre:
    - Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos.
    - Que metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
    - Si se debe llevar a cabo a evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
    - Que salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.
    - Si se llevó a cabo correctamente o no la evaluación de impacto de la protección de datos.
    - Si sus conclusiones (se seguir adelante o no con el tratamiento y que salvaguardas aplicar) son conformes al Reglamento.
g) Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
h) Asesorar al responsable del tratamiento sobre:
    - Que metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos.
    - Que áreas deben someterse la auditoría de protección de datos interna o externa.
    - Que actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y determinar a qué operaciones de tratamiento dedicar más tiempo y recursos.

El DPD deberá reunir conocimientos especializados en Derecho y en la práctica de protección de datos. En consecuencia, es necesario identificar aquellos conocimientos, habilidades y destrezas necesarias que tiene que saber el DPD para llevar a cabo de forma satisfactoria las funciones propias de su puesto.

Estas funciones genéricas del DPD se concretan en tareas de asesoramiento y supervisión, entre otras:

a) Supervisión del cumplimiento de los principios relativos al tratamiento, como pueden ser la limitación de la finalidad, minimización o exactitud de los datos.
b) Identificar las bases jurídicas de los tratamientos.
c) Valorar la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
d) Determinar la existencia de normativas sectoriales que pueden determinar condiciones especiales de tratamiento de datos.
e) Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
f) Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
g) Contratación de encargados de tratamiento, incluido los contratos y actos jurídicos que regulen la relación responsable/encargado.
h) Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
i) Diseño e implementación de políticas de protección de datos.
j) Será el encargado de auditar en materia de protección de datos.
k) Analizará los riesgos asociados a los tratamientos que se realicen.
l) Implantación de medidas de protección de datos desde el diseño y por defecto, siempre adecuados a los riesgos y la naturaleza de los tratamientos.
m) Establecer el procedimiento de gestión de incidentes de seguridad de los datos, incluida la evaluación de los riesgos derivados del incidente, para los derechos y libertades de los ciudadanos, así como la notificación a la autoridad competente.
n) Determinación de necesidad de realizar Evaluaciones de Impacto en protección de datos.
o) Implantación de programas de formación y de concienciación para el personal en materia de protección de datos.

9.2. Registro de actividades de tratamiento de datos personales

El RAT es un elemento esencial en la gestión de la protección de datos personales, según lo establecido en el artículo 30 del RGPD. En el contexto del IMAS, este registro permitirá documentar y demostrar el cumplimiento de la normativa de protección de datos, además de facilitar la gestión y supervisión de las actividades relacionadas con el tratamiento de datos personales.

El IMAS, en su calidad de responsable del tratamiento, deberá llevar y mantener actualizado el registro, debiendo estar disponible para su consulta por la Autoridad de Control competente. En este sentido, el IMAS deberá revisar y actualizar el registro periódicamente, especialmente cuando:

- Se incorporen nuevas actividades de tratamiento.
- Se modifiquen los fines del tratamiento o las categorías de datos personales tratados.
- Se introduzcan nuevos encargados del tratamiento o destinatarios de los datos.
- Existan cambios en las medidas de seguridad aplicadas.

9.2.1. Contenido del Registro de Actividades de Tratamiento

El RAT deberá contener, al menos, la siguiente información sobre las actividades de tratamiento de datos personales que se realizan en el IMAS:

1. Nombre y datos de contacto del responsable del tratamiento y, en su caso, del encargado del tratamiento y del Delegado de Protección de Datos.
2. Fines del tratamiento.
3. Categorías de interesados.
4. Categorías de datos personales tratados.
5. Destinatarios de los datos personales.
6. Transferencias internacionales de datos.
7. Plazos previstos para la supresión de los datos.
8. Descripción general de las medidas de seguridad.

9.3. Transparencia de la información y comunicaciones

En cumplimiento del deber de transparencia, cuando el IMAS actúe en calidad de responsables del tratamiento, tomarán las medidas adecuadas para facilitar, a las personas físicas titulares de los datos toda la información indicada en los artículos 13 y 14 del RGPD, que distinguen, respectivamente:

- Cuando los datos personales se obtengan directamente de la persona interesada, la información se facilitará en el momento en que se obtengan los datos.
- Cuando los datos personales no se hayan obtenido de la persona interesada, la información se facilitará en el momento de la primera comunicación con las mismas o cuando los datos se comuniquen por primera vez a otra persona destinataria. En este caso, la persona responsable del tratamiento tiene obligación de informar en el plazo razonable de un mes.

Las comunicaciones se realizarán de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a menores de edad.

La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando la persona interesada lo solicite, la información podrá facilitarse verbalmente siempre que se demuestre la identidad de la persona por otros medios.

9.4. Ejercicio de derechos personales

En cumplimiento de los artículos 15 a 22 del RGPD, el IMAS garantizará el ejercicio de los siguientes derechos de la ciudadanía, respecto de los datos personales que trate:

a) Derecho de acceso. Faculta para conocer si se tratan los datos personales y toda la información completa de ese tratamiento.
b) Derecho de rectificación. Faculta para corregir los datos personales inexactos y completar los datos incompletos.
c) Derecho de supresión. Faculta para eliminar los datos personales en los supuestos tasados por la propia normativa.
d) Derecho de oposición. Cuando el responsable del tratamiento realice tratamiento de datos personales legitimado en una misión de interés público o ejercicio de poderes públicos, la persona interesada puede ejercitar el derecho de oposición, en cualquier momento, por motivos relacionados con su situación particular.
    En este supuesto, se realizará un juicio de ponderación de los intereses del responsable y de la persona interesada, valorando y considerando:
    1. Los motivos legítimos imperiosos para el tratamiento del responsable.
    2. Los intereses, derechos y libertades de la persona interesada.
e) Derecho de limitación. Faculta para la limitación del tratamiento de datos personales, que implica la suspensión del tratamiento y en su caso, conservación de los datos, cuando se cumpla alguna de las condiciones siguientes:
    1. Cuando se impugna la exactitud de datos personales durante el plazo para verificar la exactitud.
    2. Cuando se presenta oposición al tratamiento manifestando motivos personales, mientras se verifica que el responsable trata sus datos legitimado en misión de interés público o ejercicio de poderes públicos, y se determina que este tratamiento del responsable prevalece.
    3. Cuando el tratamiento es ilícito y se solicita la limitación de uso y no la supresión.
    4. Cuando las personas necesitan los datos para el ejercicio o defensa de reclamaciones, pero simultáneamente el responsable ya no necesita esos datos para los fines del tratamiento.
f) Derecho a no ser objeto de decisiones individuales automatizadas. Se garantizará no ser sometido a una decisión basada únicamente en el tratamiento de datos personales, incluida la elaboración de perfiles, y que produce efectos jurídicos sobre la persona. No obstante, este derecho no se aplicará:
    1. Si fuera necesario para la celebración o ejecución de un contrato entre persona interesada y responsable del tratamiento.

2. Si el tratamiento se encuentra autorizado por el Derecho de la Unión o de los Estados miembros.
3. Si el tratamiento estuviera legitimado por el consentimiento.

g) Derecho a la portabilidad de los datos. Faculta para recibir los datos personales en un formato estructurado, de uso común y lectura mecánica y poder transmitir estos datos a otro responsable del tratamiento siempre que se den dos condiciones:
   1. Que el tratamiento esté basado en el consentimiento o en un contrato.
   2. Y que el tratamiento se efectúe por medios automatizados.

   El derecho a la portabilidad no se aplica al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable de tratamiento, tal y como dispone el artículo 20 del RGPD.

9.4.1. Procedimiento para el ejercicio de derechos personales

Las personas físicas podrán ejercer ante la persona responsable del tratamiento, directamente o por medio de representante, los derechos arriba indicados en relación con los datos tratados por el IMAS, a través del trámite previsto a tal efecto en la Sede Electrónica del Consell de Mallorca. A su vez, podrán presentar una reclamación ante las autoridades de control pertinentes.

En relación al procedimiento, estará dividido en tres fases, las cuales se detallan a continuación:

a) **Presentación.** Las solicitudes referidas al ejercicio de derechos personales que se correspondan o hagan referencia en cuanto a su contenido al ámbito competencial que deba resolver algún responsable de tratamiento del IMAS podrán presentarse mediante modelo de solicitud habilitado, que se pondrá a disposición de la ciudadanía de la siguiente forma:
   a. Telemáticamente: en la sede electrónica del Consell de Mallorca.
   b. Presencialmente: en las oficinas del IMAS.

b) **Tramitación y resolución.** De la solicitud presentada se dará traslado al responsable del tratamiento y éste dispondrá de un plazo de un mes para responder a partir de la recepción de la solicitud, de acuerdo con el artículo 12.3 RGPD. Este plazo será prorrogable por un plazo máximo de dos meses, atendiendo a la complejidad y número de solicitudes. Los motivos de la prórroga serán debidamente informados a la persona interesada.

c) **Impugnación.** En caso de desestimación expresa o presunta de la solicitud del ejercicio de derechos en materia de protección de datos personales correspondiente, las personas interesadas podrán recabar la tutela del derecho ante la Autoridad de Control competente mediante la presentación de reclamación ante la misma o, en su caso, de conformidad con el artículo 37 LOPDGDD, dirigiendo una reclamación previa ante el DPD del IMAS.

10. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN Y SALVAGUARDAS

En el IMAS, para garantizar la protección adecuada de los datos y la información, se establecen una serie de estándares mínimos y salvaguardas que deben regir todos los procesos relacionados con la seguridad de los sistemas de información. Estos estándares no solo aseguran el cumplimiento de la normativa vigente, sino que también fortalecen la capacidad de la organización para proteger la confidencialidad, integridad y disponibilidad de los datos.

A continuación, se describen los principios y medidas fundamentales:

a) Organización e implantación del proceso de seguridad

La seguridad deberá comprometer a todas las personas pertenecientes al IMAS tal y como se ha expuesto en de la presente política, asignando expresamente responsabilidades diferenciadas entre los siguientes roles: responsable de la información, responsable del servicio, responsable de seguridad y responsable del sistema.

b) Gestión del personal y profesionalidad

Todo el personal relacionado con la información y los sistemas del IMAS, será informado y formado respecto de sus responsabilidades de seguridad, y su actuación será supervisada para asegurar el cumplimiento de las normas. Los roles definidos en esta política actuarán con profesionalidad, y se exigirá que las organizaciones que presten servicios de seguridad cuenten con profesionales cualificados y niveles adecuados de gestión.

La seguridad de los sistemas será gestionada y auditada por personal cualificado en todas las fases de su ciclo de vida. Además, las empresas que presten servicios a el IMAS, en protección de datos y seguridad de la información, deberán contar con profesionales cualificados y niveles adecuados de gestión y madurez.

c) Análisis y gestión de los riesgos

El IMAS como organización que desarrolla e implantan sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema, sin perjuicio de lo dispuesto en el anexo II del ENS, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre estas y los riesgos.

d) Autorización y control de accesos

Se establecerán los mecanismos necesarios de protección que controlen el acceso a los sistemas de información, a través de la mejora continua. Estos accesos estarán limitados exclusivamente a las personas usuarias, procesos, dispositivos u otros sistemas de información, debidamente autorizados exclusivamente para el desempeño de las funciones atribuidas, de acuerdo con el artículo 17 del ENS.

En caso de existir indicios de actividades delictivas o que comprometan la seguridad de la información tratada, deberán ser gestionados de acuerdo con el procedimiento y normativa que, en su caso, aplique.

e) Protección de las instalaciones

Se procurará que los sistemas de información y su infraestructura de comunicaciones asociada se ubiquen en áreas controladas que sean emplazamientos seguros, y que estén protegidos, bien por controles de acceso físicos adecuados a su nivel de criticidad o mediante medidas apropiadas a los mismos. Las medidas implantadas deberán garantizar su protección en función de los requisitos legales y normativos existentes, su valor para la organización, y el riesgo al que pueden estar sometidos en cada momento, de acuerdo con el artículo 18 del ENS. Como mínimo, las salas deben estar cerradas y disponer de un control de accesos.

f) Integridad y actualización del sistema

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema o su modificación requerirá autorización formal previa del responsable del sistema. La evaluación y monitorización permanente permitirá adecuar el estado de seguridad de los sistemas atendiendo las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos, tal y como consta en el artículo 21 del ENS. Los detalles sobre la auditoría de registros de monitorización para la correcta adecuación del sistema se desarrollarán en una normativa específica.

g) Protección de la información almacenada y en tránsito

Se prestará especial atención a la protección de la información almacenada o en tránsito en equipos o dispositivos portátiles o móviles, periféricos y redes abiertas. Se aplicarán procedimientos para garantizar la recuperación y conservación a largo plazo de los documentos electrónicos. La información en soporte no electrónico, relacionada con la información electrónica, que se encuentre en el ámbito de aplicación del ENS, deberá estar protegida con el mismo grado de seguridad.

Toda la información, ya sea en papel o en formato digital, se etiquetará adecuadamente según su clasificación para facilitar su uso, manipulación y protección. Los documentos y sus soportes llevarán un etiquetado que permita reconocer su nivel de clasificación de

acuerdo con los criterios de seguridad del ENS, cumpliendo con lo dispuesto en su Anexo II sobre la política de seguridad y el estándar de clasificación y etiquetado de la información.

h) Registro de actividades y detección de código dañino

Para garantizar la seguridad de los sistemas de información y cumplir con el ENS se implementarán mecanismos de registro y monitorización de actividades de los usuarios, así como la detección de código dañino. Estas medidas buscan asegurar el cumplimiento de la política de seguridad de la información y la protección de datos personales, respetando los derechos fundamentales al honor, la intimidad y la propia imagen.

El IMAS registrará las actividades de los usuarios que accedan a los sistemas de información, incluyendo solo la información necesaria para monitorizar el uso adecuado de los recursos, investigar actividades indebidas y documentarlas y asegurar la trazabilidad de las acciones realizadas. Además, se analizarán las comunicaciones para impedir accesos no autorizados, detectar y prevenir ataques, y bloquear la distribución de códigos dañinos, siempre respetando los principios de limitación de la finalidad y minimización de datos.

Cada usuario deberá estar identificado de forma única para conocer sus derechos de acceso y actividades realizadas, permitiendo corregir situaciones indebidas y, si es necesario, exigirle responsabilidades.

i) Incidentes de seguridad

El IMAS dispondrá de un procedimiento específico para la gestión de incidentes de seguridad, en cumplimiento del artículo 25 del ENS.

Este procedimiento será accesible y conocido por las personas que desempeñen roles clave en su implementación, garantizando que todos los responsables comprendan sus obligaciones y responsabilidades.

El procedimiento abarcará los siguientes aspectos:

a) Mecanismos de detección.
b) Criterios de clasificación.
c) Procedimientos de análisis y resolución.
d) Cauces de comunicación interna y externa.
e) Notificación a autoridades.
f) Registro de actuaciones.

j) Continuidad de la actividad

Los sistemas del IMAS dispondrán de copias de seguridad y de mecanismos que garanticen la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo o afección grave de los activos empleados, tal y como indica el artículo 26 del ENS.

k) Mejora continua del proceso de seguridad

El proceso integral para la gestión de la protección de datos personales y seguridad de la información será mejorado de manera continua en base a los indicadores que se consideren en función de los requisitos establecidos, el nivel de madurez en cada momento y las necesidades estratégicas del IMAS, tal y como indica el artículo 27 del ENS.

11. GARANTÍAS DE LA SEGURIDAD DE LOS SISTEMAS

Para garantizar la seguridad de los sistemas de información del IMAS y cumplir con los estándares del ENS, se implementarán una serie de medidas y procedimientos que aseguren la protección de los activos digitales y de los datos personales tratados por la entidad.

Estas medidas se ajustarán a los requisitos mínimos establecidos en el ENS considerando los riesgos asociados a los sistemas de información y su criticidad. Este apartado detalla las garantías que se aplicarán en el IMAS para asegurar el cumplimiento de la normativa vigente, además de ofrecer un marco claro para la gestión de la seguridad de los sistemas, tanto para los servicios internos como para aquellos prestados por terceros.

A continuación, se describen las principales medidas y procedimientos a seguir para garantizar la seguridad de los sistemas de información en el IMAS.

a) Declaración de Aplicabilidad

El IMAS adoptará las medidas de seguridad establecidas en el Anexo II del ENS. Estas medidas se implementarán considerando los siguientes aspectos clave:

- Los activos que constituyen los sistemas de información del IMAS, asegurando su protección según su valor y criticidad.
- La categoría del sistema: Basada en la clasificación de los sistemas de información según su nivel de riesgo (alto, medio o bajo), tal como lo define el ENS.
- Gestión de riesgos: Se tomarán decisiones específicas para gestionar los riesgos identificados, aplicando controles y salvaguardas que protejan los activos y aseguren el cumplimiento de los principios de seguridad.

Las medidas de seguridad adoptadas serán las mínimas exigibles y podrán ser ampliadas o reforzadas a criterio del Responsable de Seguridad del IMAS, mediante la

implementación de medidas adicionales o compensatorias. Estas medidas compensatorias se utilizarán siempre que se justifique que ofrecen un nivel de protección equivalente o superior al de las medidas descritas en el Anexo II del ENS. Este conjunto de medidas quedará reflejado en un documento denominado Declaración de Aplicabilidad, que será firmado por el Responsable de Seguridad.

La declaración detallará la correspondencia entre las medidas compensatorias implantadas y las medidas originales del Anexo II, garantizando que los riesgos asociados a los activos quedan debidamente gestionados.

b) Catálogo de Servicios Electrónicos

El IMAS elaborará un Catálogo de Servicios Electrónicos que recogerá el inventario de los servicios gestionados electrónicamente y la información asociada a ellos. Este catálogo se empleará como referencia para evaluar los requisitos de seguridad de los datos almacenados y tratados en dichos servicios, tal como se establece en el artículo 40 del ENS.

El catálogo también servirá para analizar el impacto de posibles amenazas sobre los servicios electrónicos y ayudará en la realización de análisis de riesgos y continuidad del negocio, siguiendo las medidas de seguridad establecidas en el ENS. Este catálogo abarcará todos los servicios electrónicos que el IMAS gestione para llevar a cabo sus competencias y estará alineado con la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

c) Directrices para la Estructuración de la Documentación de Seguridad

El IMAS adoptará una normativa específica para la estructuración de la documentación de seguridad, en cumplimiento del artículo 12.1.e) del ENS.

Esta normativa incluirá la creación de procedimientos y documentos que aborden los siguientes aspectos:

- Auditorías de registros de monitorización.
- Clasificación y tratamiento de la información.
- Control de accesos lógicos.
- Gestión de incidentes de seguridad

La normativa de seguridad será concisa y contendrá referencias claras para facilitar su interpretación y aplicación. Además, incluirá métricas para evaluar el cumplimiento de los procedimientos y ofrecerá la posibilidad de proponer mejoras. Todos los empleados de la entidad están sujetos a diversas funciones y obligaciones según su perfil profesional.

12. OBLIGACIONES Y FORMACIÓN DEL PERSONAL

Todo el personal debe conocer y cumplir esta política, así como las normativas, procedimientos e instrucciones que conforman el Sistema de Gestión de Seguridad de la Información (en adelante SGSI). El IMAS garantizará que esta información sea accesible a todo el personal y a terceros que presten servicios. Cada empleado es responsable del uso y administración segura de los sistemas e información. Estas obligaciones se detallarán en la normativa accesoria.

El IMAS promoverá planes de formación y concienciación que incluirán:

- Sesiones formativas recurrentes sobre protección de datos y seguridad de la información para nuevas incorporaciones y personal activo.
- Formación continua para el personal con responsabilidades en sistemas.
- Programas de formación obligatorios para empleados con responsabilidades especializadas en seguridad de la información y protección de datos.

Las formaciones se diseñarán según las necesidades específicas de cada grupo, priorizando áreas clave para la seguridad y el cumplimiento normativo.

13. RELACIONES CON TERCEROS

Cuando el IMAS gestione información de otros organismos o preste servicios a estos, dichos organismos serán partícipes de la presente Política. El IMAS establecerá canales claros de coordinación para la gestión de información y la resolución de incidentes de seguridad. Esto incluirá la definición de procedimientos operativos, garantizando que la cooperación con terceros se lleve a cabo conforme a las directrices de seguridad establecidas.

Asimismo, cuando el IMAS utilice servicios de terceros o comparta información con ellos, estos terceros serán igualmente partícipes de esta Política, así como de la Normativa de Seguridad aplicable a los servicios o la información implicada. Las terceras partes estarán sujetas a las obligaciones de dicha normativa.

a) Requisitos de Conformidad con el ENS para Terceras Partes

Las entidades del sector privado que presten servicios al IMAS, ya sea mediante soluciones tecnológicas o servicios externos, deberán cumplir con los requisitos establecidos en el ENS.

Los pliegos de prescripciones administrativas y técnicas del IMAS recogerán todos los requisitos necesarios para asegurar que los sistemas de información gestionados por los contratistas cumplen con los estándares de seguridad exigidos por el ENS.

b) Designación de un Punto de Contacto (POC)

En el caso de servicios externalizados, las entidades prestadoras de servicios deberán designar un punto o persona de contacto (POC) responsable de la seguridad de la información gestionada.

Este POC será el encargado de supervisar el cumplimiento de los requisitos de seguridad asociados al servicio, así como de gestionar las comunicaciones y los incidentes de seguridad.

El POC coordinará todas las actuaciones necesarias para garantizar la seguridad de la información tratada en el marco del servicio prestado, en cumplimiento de las obligaciones del artículo 13.5 del ENS.

c) Concienciación en Seguridad de Terceras Partes

El IMAS se asegurará de que el personal de las terceras partes que intervienen en la gestión de servicios o información esté adecuadamente formado y concienciado en materia de seguridad de la información. Este personal deberá recibir una formación equivalente al nivel de concienciación y cumplimiento establecido en la Política de Seguridad del IMAS.

En caso de que alguna tercera parte no pueda cumplir con algún aspecto de la presente Política de Seguridad, será necesario presentar un informe elaborado por el Responsable de Seguridad del IMAS, el cual deberá detallar los riesgos asociados al incumplimiento y las medidas que se tomarán para tratarlos. Este informe deberá ser aprobado por los responsables de la información y los servicios implicados, antes del inicio de cualquier relación contractual con la tercera parte en cuestión.

d) Procedimientos de Comunicación y Resolución de Incidencias

Se establecerán procedimientos específicos para la comunicación y resolución de incidencias de seguridad que involucren a terceras partes. Estos procedimientos asegurarán una respuesta ágil y efectiva ante incidentes de seguridad, permitiendo la rápida detección, análisis y resolución de problemas que puedan surgir en el manejo de la información o la prestación de servicios.

e) Adquisición de Productos y Servicios de Seguridad

En el proceso de adquisición de productos de seguridad o contratación de servicios de seguridad en el ámbito de las tecnologías de la información y la comunicación, el IMAS

se compromete a utilizar soluciones que sean proporcionales a la categoría del sistema y al nivel de seguridad requerido.

Para garantizar la eficacia de estas adquisiciones, se tendrán en cuenta los siguientes aspectos:

- **Certificación de funcionalidad de seguridad**

  Los productos de seguridad adquiridos deberán contar con certificaciones que respalden su funcionalidad en relación con los objetivos de seguridad establecidos. Esta certificación es esencial para asegurar que las soluciones seleccionadas cumplen con los requisitos mínimos de seguridad definidos por el ENS y otras normativas aplicables.

- **Proceso formal de adquisición**

  El IMAS establecerá un proceso formal para la planificación de la adquisición de nuevos componentes del sistema, el cual incluirá las siguientes etapas:

  - Ajuste a la arquitectura de seguridad: Las adquisiciones se realizarán en consonancia con la arquitectura de seguridad elegida por el IMAS. Esto asegurará que cualquier nuevo componente se integre adecuadamente en el entorno de seguridad existente y no comprometa la integridad del sistema.
  - Consideración de realizar un Análisis de Riesgos en función de la criticidad del componente como parte de la arquitectura.
  - Consideración de necesidades técnicas, formativas y financieras: El proceso de adquisición contemplará de manera conjunta las necesidades técnicas de los nuevos componentes, los requerimientos de formación para el personal que los manejará, así como la financiación necesaria para su adquisición e implementación.

- **Evaluación continua de proveedores**

  Además, el IMAS llevará a cabo una evaluación continua de los proveedores de productos y servicios de seguridad. Esta evaluación incluirá la revisión de su capacidad para proporcionar soluciones que cumplan con los estándares de seguridad y la normativa vigente, así como su historial en la gestión de incidentes de seguridad.

14. DESARROLLO DE LA POLÍTICA

El cumplimiento de los objetivos marcados en esta Política se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del ENS. Para su organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al CSI proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.