EMASESA

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

HISTÓRICO DE MODIFICACIONES

Revisión nº	Fecha	Causas del cambio
1	10/07/2025	Publicación web

ÍNDICE

1 INTRODUCCIÓN 5
2 OBJETO Y ÁMBITO DE APLICACIÓN 5
3 MISIÓN Y VALORES 5
3.1 MISIÓN 6
3.2 VISIÓN 6
3.3 VALORES 6
4 LEGISLACIÓN Y NORMATIVA DE REFERENCIA 8
5 PRINCIPIOS Y DIRECTRICES 8
6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 9
6.1 COMITÉ DE DIRECCIÓN 10
6.2 COMITÉ DE SEGURIDAD INTEGRADA 10
6.3 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 11
6.4 COMITÉ TÉCNICO DE SEGURIDAD TIC 13
6.5 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI) 14
6.6 OFICINA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN (OTSI) 15
6.7 RESPONSABLE DE SEGURIDAD FÍSICA 15
6.8 RESPONSABLE DE LA INFORMACIÓN 16
6.9 RESPONSABLE DEL SERVICIO 17
6.10 RESPONSABLE DEL SISTEMA 17
6.11 ADMINISTRADOR DE SEGURIDAD 18
6.12 ADMINISTRADOR DE SISTEMAS 19
6.13 DESARROLLADOR DE SISTEMAS 20
6.14 USUARIOS 21
6.15 DELEGADO DE PROTECCIÓN DE DATOS (DPD) 22
6.16 RESPONSABLE DEL TRATAMIENTO 25
6.17 ENCARGADO DEL TRATAMIENTO 26
7 RESOLUCIÓN DE CONFLICTOS 27
8 OBLIGACIONES DEL PERSONAL 27
9 ASESORAMIENTO ESPECIALIZADO EN MATERIA DE SEGURIDAD 27
9.1 ASESORAMIENTO ESPECIALIZADO 27
9.2 COOPERACIÓN ENTRE ORGANISMOS Y ADMINISTRACIONES PÚBLICAS 28
9.3 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN 28

10 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 28
11 FORMACIÓN Y CONCIENCIACIÓN 28
12 ANÁLISIS Y GESTIÓN DE RIESGOS 28
13 ESTRUCTURA NORMATIVA 29
14 CALIFICACIÓN DE LA INFORMACIÓN. 29
14.1 APROBACIÓN 29
14.2 REVISIÓN DE LA DOCUMENTACIÓN 30
14.3 CATEGORÍAS DE SEGURIDAD. 30
14.4 OTRA DOCUMENTACIÓN 31
15 PUBLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 31
16 ENTRADA EN VIGOR 31

1 INTRODUCCIÓN

EMASESA, la Empresa de Abastecimiento y Saneamiento de Aguas de Sevilla, ha desarrollado esta Política de Seguridad de la Información (PSI) conforme al Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad.

La PSI es una declaración ética y obligatoria que se despliega a través de diversas normativas y procedimientos para tratar adecuadamente los riesgos. El uso de los activos de información debe seguir las buenas prácticas profesionales y cumplir con los requisitos legales, reglamentarios y contractuales para garantizar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y los servicios.

EMASESA define esta PSI compatible con el Artículo 1 de la PSI de los organismos que conforman la Red Corporativa del Ayuntamiento de Sevilla, llamada RED HISPALNET. En dicho documento se establecen las directrices básicas y transversales en materia de seguridad de la información para el conjunto de entidades que la conforman.

2 OBJETO Y ÁMBITO DE APLICACIÓN

La Política de Seguridad de la Información de EMASESA tiene como objetivos:

- Proteger las redes y sistemas de información de EMASESA, asegurando su nivel adecuado de seguridad, disponibilidad y resiliencia frente a cualquier amenaza.

- Garantizar a la ciudadanía, personal propio y colaboradores, que sus datos personales serán tratados conforme a los estándares y buenas prácticas de seguridad de la información y protección de datos.

- Salvaguardar la información generada en el ejercicio de las actividades propias.

- Fomentar la concienciación en seguridad y protección de datos entre todo el personal, asegurando el conocimiento de sus obligaciones y responsabilidades.

- Establecer un modelo integral de gestión de la seguridad de la información, basado en un ciclo continuo de mejora técnica, organizativa y procedimental.

- Garantizar el cumplimiento de la legislación vigente, en especial en materia de seguridad de la información y protección de datos personales.

Este documento define un marco organizativo y tecnológico en EMASESA y debe ser conocido y cumplido por todo el personal, propio o externo, sin importar el cargo.

3 MISIÓN Y VALORES

EMASESA gestiona el ciclo integral del agua en Sevilla y su área metropolitana bajo un enfoque sostenible. Comenzó su actividad el 23 de octubre de 1974, cuando el Ayuntamiento de Sevilla la constituyó como empresa municipal. El 8 de mayo de 2007, cambia su denominación a metropolitana al incorporar al accionariado los ayuntamientos de las principales poblaciones abastecidas (Camas, Dos Hermanas, Alcalá de Guadaíra, Mairena de Alcor, San Juan de Aznalfarache, Coria del Río, La Puebla del Río, Alcalá del Río, La Rinconada, El Garrobo y El

Ronquillo). En todas ellas, ofrece servicios de abastecimiento, vertido y depuración, salvo en El Garrobo, donde solo abastece de agua a la población.

3.1 MISIÓN

Garantizamos la continuidad y calidad en la prestación del servicio del ciclo integral del agua de uso urbano, con la concepción del agua como derecho humano, situando al usuario y a la sociedad en su conjunto como principal beneficiario de su actividad, proporcionando agua potable y un servicio de saneamiento y depuración respetuoso con la naturaleza de manera sostenible, suficiente, saludable, aceptable, accesible y asequible.

3.2 VISIÓN

Queremos ser una empresa pública, sostenible y eficiente, contando con la sociedad, el territorio y los agentes implicados en la prestación de nuestro servicio y convirtiéndonos así en un referente en innovación, conocimiento, gestión y competitividad.

3.3 VALORES

En nuestra condición de empresa pública nos caracterizamos por una cultura organizacional claramente comprometida con nuestros sus usuarios y la sociedad en general, con los grupos de interés y el territorio en el que prestamos el servicio, así como con nuestro personal y, por supuesto, con el agua como derecho humano y recurso imprescindible para la vida y con fiel respeto al entorno ambiental en el que desarrollamos nuestras actividades.

De este compromiso emanan los siguientes valores, que rigen toda la actividad de la empresa y, especialmente, su Plan Estratégico:

- Vocación de servicio público

  Trabajamos por y para los usuarios del servicio y la sociedad en general.

  Actuamos de acuerdo con los intereses generales de los usuarios y de la sociedad de la que formamos parte, haciendo uso de sus recursos naturales y públicos que son de todos, con criterios de eficiencia y sostenibilidad.

- Ética

  Somos íntegros y honestos.

  Aplicamos un código deontológico propio de nuestra actividad pública, generando confianza con la ciudadanía y grupos de interés y credibilidad y reconocimiento social de la empresa. Nuestra ética la aplicamos para la sostenibilidad, adaptando de una forma continuada nuestra organización a cambios permanentes en el ámbito social, económico y político, en el que impactamos con nuestras decisiones y en el que la naturaleza es un factor primordial, como valor de cuidado, protección y preservación.

  Internamente, conducimos nuestra actividad con criterio y responsabilidad, siendo sostenibles y eficientes, creando y fomentando entornos de confianza, promoviendo el trabajo en equipo y transversal dentro de la organización, generando talento y culturas de colaboración e innovación que aporten sentido a las personas y valor a nuestra actividad.

- Compromiso

Nuestro compromiso con el entorno natural y urbano es consustancial a nuestra propia actividad. Además de proteger el medio y preservar la salud, tratamos de generar un impacto positivo en el mismo manteniendo una actitud proactiva en todo lo que se refiere a la acción preventiva de la salud derivada de nuestra actividad. De igual forma, es clave nuestro compromiso social, como prestadores de un servicio público básico que inspira toda nuestra gestión y se basa en la participación y en la cohesión de un territorio metropolitano, haciendo que nuestra gobernanza genere un vínculo de confianza con nuestros grupos de interés, dando cabida a sus diferentes perspectivas en el establecimiento de nuestras políticas como el Observatorio del Agua o el Defensor del Usuario.

- Responsabilidad social, técnica, económica y ambiental

  Prestamos un servicio público esencial para la ciudadanía situando al usuario en el centro de nuestra estrategia, por lo que es nuestra responsabilidad realizar una gestión eficaz y eficiente de los recursos económicos, materiales y humanos con los que contamos para el desarrollo de nuestra actividad, como servicio público de carácter básico y esencial, garantizando el Derecho Humano al Agua, cumpliendo con todos los estándares y normas de aplicación, promoviendo usos diversos del agua y colaborando en la generación de entornos saludables y llenos de biodiversidad.

  Minimizando pérdidas de agua, el consumo de energía y otros consumibles, con políticas de circularidad de nuestros residuos, aplicando, en un entorno exigente y competitivo, la mejora continua y la eficiencia, principios que garantizarán la estabilidad y el futuro de esta organización pública.

- Innovación

  Si el Plan Estratégico de la organización es el faro que nos guía, la innovación es el vehículo que nos guiará para el cumplimiento de nuestros objetivos como organización, con la constante mejora de la eficiencia de nuestras operaciones, impulsando y desarrollando conocimiento, promoción del talento y generando valor a medio y largo plazo. La innovación es pieza clave para hacer realidad nuestra visión de empresa, es el motor que va a dinamizar la transformación, permitiendo una rápida y efectiva adaptación a las circunstancias cambiantes de nuestro entorno, y la herramienta que viene a dar respuesta a los retos a los que nos enfrentamos.

- Cohesión territorial

  EMASESA, es una empresa netamente Metropolitana.

  Tenemos muy clara la importancia de la colaboración leal y solidaria entre las distintas organizaciones públicas de nuestro ámbito territorial, destinada a unificar esfuerzos y trabajar en la mejora del servicio en todo el territorio, poniendo al usuario en el centro, en términos de igualdad, como principal receptor de los servicios que prestamos,

  La prestación del servicio de agua pone en valor las características particulares de cada espacio y, de manera especial, de aquellos territorios donde la activación de los recursos ligados a la planificación pueda suponer una oportunidad de desarrollo cultural, social y económico, promoviendo la sostenibilidad, la salud y la biodiversidad. Una articulación capaz de conectar y cohesionar el territorio a través del agua, como un todo donde mejorar la calidad de vida de la ciudadanía.

- Personas y empresa

  Cada persona de EMASESA debe ser consciente de su papel en la organización, reforzando su lealtad tanto con las personas que integran la plantilla como con la organización e

incrementando su compromiso para lograr los objetivos comunes. También se refuerza la idea de pertenencia en la organización, trabajando en equipo, anteponiendo los intereses generales a los propios, con el fin de llevar a cabo los programas y proyectos que se realizan en esta empresa, que es pública y es de todos.

El nuevo marco de relaciones laborales, con el instrumento del convenio colectivo, la Transformación Cultural y el Plan de Gestión del Talento, transformarnos para transformar, basado en el Liderazgo Humano, Ético y Creativo, se constituye en uno de los pilares esenciales de la Transformación integral de EMASESA, y debe facilitar el relevo generacional. Fomentaremos el desarrollo de un sistema de gestión de competencias, técnicas y transversales, que garanticen capacidades de aprendizaje continuo, de una actitud innovadora y colaborativa y que, junto a una comunicación integradora, permitan un funcionamiento más transversal, ágil y dinámico, orientado al crecimiento personal y de la organización, afianzando el trabajo en equipo, desarrollando talento y aplicando inteligencia emocional.

4 LEGISLACIÓN Y NORMATIVA DE REFERENCIA

El marco normativo de prestación de servicios a los ciudadanos de EMASESA, en el ámbito de esta PSI, está integrado por una serie de requisitos legales a nivel local, autonómico, estatal y europeo. Estos requisitos se identifican, analizan, revisan y actualizan en base a lo establecido en el Procedimiento Control de la Información Documentada (GE 027.03), así como en el Manual Operativo SGSI (GE010.02), manteniendo en consecuencia un Listado de Normativa y Legislación en vigor.

5 PRINCIPIOS Y DIRECTRICES

La Seguridad es entendida como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. se establecen los siguientes principios básicos:

a) La seguridad como un proceso integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

b) Gestión de la seguridad basada en los riesgos: el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de

los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

c) Prevención, reacción y recuperación: las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente y estarán acompañadas de medidas de respuesta, de forma que los incidentes de seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios. El sistema de información garantizará la conservación de los datos e información en soporte electrónico y su recuperación.

d) Líneas de defensa: la monitorización es especialmente relevante cuando se establecen líneas de defensa. De este modo, se establecen mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

e) Reevaluación periódica: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

f) La seguridad como función diferenciada: en los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de Seguridad de la Información (RSI), que determina las decisiones para satisfacer los requisitos de seguridad de la información y los servicios.

6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

La PSI, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 del Esquema Nacional de Seguridad (ENS) y según se detalla en la sección 3.1 del anexo II del ENS, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información de EMASESA está compuesta por los siguientes agentes:

1. Comité de Dirección.
2. Comité de Seguridad Integrada.
3. Comité de Seguridad de la Información.
4. Comité Técnico de Seguridad TIC.
5. Responsable de Seguridad de la Información (RSI).
6. Oficina Técnica de Seguridad de la Información (OTSI).
7. Responsable de Seguridad Física.
8. Responsable de la Información.
9. Responsable del Servicio.
10. Responsable del Sistema.
11. Administrador de Seguridad.

12. Administrador de Sistemas.
13. Desarrollador de Sistemas.
14. Usuarios.

Los perfiles específicos en materia de Protección de Datos de Carácter Personal son los siguientes:

15. Delegado de Protección de Datos (DPD).
16. Responsable del Tratamiento.
17. Encargado del Tratamiento.

6.1 COMITÉ DE DIRECCIÓN

Este órgano lo integran el Consejero Delegado, los Directores, Subdirectores y el Jefe de División responsable de las Áreas Territoriales.

Es el responsable de:

a) Aprobar la PSI.

b) Designar al Responsable de Seguridad de la Información (RSI) y al Delegado de Protección de Datos (DPD).

c) Coordinar, a través del Consejero Delegado o la persona en quien este delegue, la estrategia de seguridad corporativa con el Comité Director de Seguridad de la RED HISPALNET.

6.2 COMITÉ DE SEGURIDAD INTEGRADA

Este órgano es el encargado de coordinar la seguridad en EMASESA en todas sus modalidades, incorporando la representación:

- Presidente: Consejero Delegado.
- Coordinador: Director de Seguridad
- Seguridad Física: Responsable de Seguridad y Enlace (RSE)
- Seguridad Lógica: Responsable de Seguridad de la Información (RSI)
- Responsables de los siguientes Servicios Esenciales:
  - Presas y Conservación de Infraestructuras de Producción.
  - Agua Potable.
  - Aguas Residuales.
  - Centro de Control de Operaciones y Planificación.
  - Aseguramiento del Riesgo.
  - Seguridad, salud y bienestar de las Personas.
  - Planes de Seguridad del Agua.
  - Seguridad Reputacional.
  - Medio Ambiente.
  - Recursos Humanos.
  - Cumplimiento Legal.

Son funciones del Comité de Seguridad Integrada:

g) Revisar y aprobar la Política General de Seguridad de EMASESA

h) Coordinar los esfuerzos de Seguridad y Protección de los activos de EMASESA, de cualquier tipología, desde un punto de vista integral (físico, lógico, legal, operacional, etc.), y su alineamiento con los intereses generales y estratégicos de la compañía.

i) Promover la gestión integral de la seguridad.

j) Coordinar y gestionar la respuesta ante emergencias críticas de seguridad que tengan especial impacto o que pongan en riesgo la continuidad de las actividades esenciales de EMASESA.

6.3 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Este órgano coordina todas las actividades de seguridad de los sistemas de información, especialmente desde el punto de vista legal. Se enfoca en proteger los activos de información de EMASESA, sin importar el soporte (informático, papel, conocimiento, etc.), como parte esencial de la seguridad integral.

Lo constituyen los siguientes perfiles:

- Responsable de Seguridad de la Información (RSI).

- Responsable de Asesoría Jurídica.

- Delegado de Protección de Datos (DPD).

El RSI actúa como portavoz del Comité frente a otros órganos internos. En caso de falta de acuerdo sobre alguna materia objeto de análisis, se elevará la cuestión al Comité de Dirección para que adopte la decisión final.

Las funciones del Comité de Seguridad de la Información son las siguientes:

a) Asegurar el alineamiento de la estrategia en Seguridad de la Información en EMASESA con los objetivos generales de la compañía.

b) Revisar la PSI y establecer los criterios de revisión de esta.

c) Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento a los requisitos legales vigentes.

d) Promover y respaldar los planes de acción e iniciativas para la implantación de la PSI en EMASESA.

e) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la PSI y la legislación vigente.

f) Promover la difusión y apoyo a la seguridad de la información dentro de las unidades organizativas de EMASESA.

g) Supervisar el cumplimiento de las obligaciones legales de EMASESA, así como la aplicación de las mejores prácticas reconocidas internacionalmente en materia de Seguridad de la Información.

h) Identificar oportunidades de mejora en materia de Seguridad de la Información.

i) Favorecer los esfuerzos de todas las áreas con responsabilidad en la seguridad de la información.

j) Delimitar responsabilidades de todo el personal involucrado, interno o externo (proveedores, colaboradores y terceros), y resolver conflictos de responsabilidad, o elevarlos al Comité de Dirección para su revisión.

k) Decidir sobre los casos de incumplimiento de la normativa interna de seguridad de la información y reportar en su caso al órgano interno encargado de iniciar el procedimiento disciplinario correspondiente.

l) Reportar al Comité de Seguridad Integrada en materia de Seguridad de la Información.

En relación con la protección de datos de carácter personal:

a) Apoyar al DPD en el ámbito de la protección de datos de carácter personal.

b) Revisar y validar el Análisis de riesgos de los tratamientos de datos de carácter personal y las evaluaciones de impacto sobre la privacidad.

c) Establecer un Plan de auditorías a realizar por EMASESA, tanto para los ficheros automatizados como los no automatizados, que contengan datos de carácter personal, y promover la realización de las auditorías, bien con personal interno de la organización o con personal externo.

d) Recibir y analizar el informe de auditoría y promover y supervisar la adoptación de medidas para solventar las anomalías y deficiencias detectadas.

e) Analizar los informes de incidentes que tengan afección sobre datos de carácter personal y promover y requerir la adopción de medidas para solventar las anomalías y deficiencias detectadas.

Las obligaciones de los integrantes de este Comité son las siguientes:

Responsable de Asesoría Jurídica:

a) Asesorar al Comité sobre los aspectos legales que puedan afectar a la seguridad de la información en EMASESA.

Responsable de Seguridad de la Información:

a) Asesorar al Comité sobre los cuestiones técnicas, organizativas, legales y normativas propias de su área, así como proponer las medidas necesarias para proteger la información.

b) Identificar y comunicar cambios legales y normativos que puedan afectar a la Seguridad de la Información en EMASESA.

c) Informar al Comité sobre la marcha de las actuaciones promovidas por el Comité Técnico de Seguridad TIC para la adecuación y mejora de la seguridad de los sistemas de información de corporativos.

d) Aquellas otras recogidas en el apartado “Responsable de Seguridad de la Información (RSI)”.

Delegado de Protección de Datos:

a) Informar sobre el estado general de situación en relación con el tratamiento de datos de carácter personal, en particular, sobre las actividades de tratamiento existentes o nuevas, el

ejercicio de derechos realizado por los usuarios y el estado de cumplimiento de las obligaciones legales por parte de EMASESA.

b) Aquellas otras recogidas en el apartado “Delegado de Protección de Datos”.

El Comité de Seguridad se reunirá con carácter ordinario al menos una vez al año, pudiendo reunirse de manera extraordinaria por razones de urgencia y causa justificada en periodos inferiores.

6.4 COMITÉ TÉCNICO DE SEGURIDAD TIC

Este órgano tiene un carácter eminentemente técnico, especializado en soluciones de seguridad y protección de los sistemas de información y telecomunicaciones (TIC).

Lo constituyen los siguientes miembros:

- Responsable global del área de Transformación Digital.
- Responsable de Seguridad de la Información (RSI).
- Responsable del área de Infraestructuras TI.
- Responsable del área de Sistemas de Información.
- Responsable del Centro de Atención al Usuario (CAU)

En cuestiones que afecten a las Tecnologías de la Operación (TO) se podrá requerir, según se precise, la asistencia de:

- Responsable del área de Automatización y Control

En función del asunto a tratar por el Comité, se puede requerir igualmente la incorporación de expertos o personal interesado de otras áreas de la organización.

El Responsable general del área de Transformación Digital actúa como coordinador del Comité. En caso de falta de acuerdo sobre alguna materia objeto de análisis será, así mismo, quien adopte la decisión final.

Son funciones del Comité Técnico de Seguridad TIC las siguientes:

a) Analizar y valorar las medidas técnicas de ciberseguridad necesarias para mitigar los riesgos sobre los recursos TIC de EMASESA, planificando su implementación e identificando los recursos humanos, técnicos y económicos requeridos para garantizar su ejecución de forma eficiente y en los plazos establecidos.

b) Gestionar los incidentes de seguridad de la información, cuando así lo establezca el procedimiento correspondiente.

Las obligaciones de los integrantes de este Comité son las siguientes:

a) Asegurar la implantación, en calidad y plazo, de las soluciones aprobadas.

6.5 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI)

El Responsable de Seguridad de la Información (RSI) tiene como misión garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información gestionada por la organización. Asimismo, es responsable de diseñar, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI), asegurando el cumplimiento de la normativa vigente, incluyendo la ISO/IEC 27001, el Esquema Nacional de Seguridad (ENS), la normativa sobre protección de las redes y sistemas información para la prestación de servicios esenciales, la normativa de protección de datos y los estándares internacionales aplicables.

Sus principales funciones son las siguientes:

a) Elaborar la PSI, distribuirla y velar por su cumplimiento y el de sus normas y procedimientos derivados.

b) Determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios.

c) Definir, desarrollar y mantener la normativa interna en materia de seguridad de la información y protección de datos, en coordinación con las áreas competentes.

d) Supervisar y aprobar la documentación del SGSI, incluidos los análisis y la gestión de riesgos.

e) Asegurar el cumplimiento de los requisitos normativos aplicables, supervisando el ciclo de mejora continua (PDCA) del SGSI y gestionando los planes de tratamiento de riesgos y de mejora.

f) Aprobar la categorización de los sistemas de información conforme a lo dispuesto en el ENS, en base a las valoraciones realizadas por los Responsables de los Servicios y de la Información.

g) Proponer las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales, conforme al estado de la técnica, la naturaleza de los datos y los riesgos identificados, y verificar su implantación efectiva.

h) Coordinar la interacción, y actuar como punto de contacto, con las autoridades nacionales de ciberseguridad y otros organismos especializados.

i) Asesorar a los Responsables de Servicios y de la Información en materia de seguridad y gestión de riesgos, elevando los resultados al Comité de Seguridad.

j) Gestionar el cuadro de mandos de seguridad de la información, elaborando informes periódicos de situación para la Dirección y el Comité de Seguridad.

k) Supervisar la gestión de incidentes de seguridad desde su notificación hasta su resolución, estableciendo medidas de seguridad adecuadas y eficaces.

l) Promover y coordinar, junto con el área de Formación de EMASESA, las actividades de formación, concienciación y capacitación del personal en materia de seguridad de la información y protección de datos.

m) Preparar los temas a tratar en las reuniones del Comité de Seguridad, proporcionando información para la toma de decisiones.

n) Formar parte del Grupo Técnico de Seguridad de la Información de la RED HISPALNET y actuar conforme a la normativa específica que regula su funcionamiento.

o) Asumir las funciones atribuidas explícitamente a la figura del Responsable de Seguridad de la Información en el Real Decreto que regula el Esquema Nacional de Seguridad y la legislación en el ámbito de la seguridad en las redes y sistemas de información para servicios esenciales.

Obligaciones:

a) Mantenerse actualizado en normativa de seguridad de la información y ciberseguridad, tanto técnica como organizativamente.

b) Conocer la legislación aplicable, en especial la relacionada con protección de datos, ciberseguridad en servicios esenciales, ENS e ISO/IEC 27001.

c) Cumplir las responsabilidades asociadas como usuario de los sistemas de información de la organización.

Las funciones de Responsable del Seguridad de la Información recaerán en el Jefe del Departamento responsable de la Seguridad de la Información.

Cuando las características de los sistemas lo requieran, el RSI podrá designar Responsables de Seguridad de la Información Delegados, quienes dependerán funcionalmente de él.

El RSI será nombrado y cesado por el Comité de Dirección.

6.6 OFICINA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN (OTSI)

La Oficina Técnica de Seguridad de la Información (OTSI) es un grupo de apoyo al RSI para el cumplimiento de sus funciones, que aglutinará los esfuerzos de prevención de incidentes de seguridad, detección de anomalías, mecanismos de respuesta eficaz ante los mismos y actividades de recuperación mediante el desarrollo de planes de continuidad de los sistemas de información para garantizar la disponibilidad de los servicios críticos.

A estos efectos, la OTSI realizará las auditorías periódicas de seguridad, como parte del Plan Director de Auditorías de EMASESA, el seguimiento y control del estado de seguridad de los sistemas y servicios, la respuesta eficaz a los incidentes de seguridad desde su notificación hasta su resolución y el desarrollo de los planes de continuidad de los sistemas de información.

6.7 RESPONSABLE DE SEGURIDAD FÍSICA

El Responsable de Seguridad Física tiene como objetivo planificar, implementar y supervisar las políticas y medidas de seguridad física destinadas a proteger personas, instalaciones e infraestructuras críticas de EMASESA. Es además el responsable de garantizar el cumplimiento normativo, la continuidad del servicio y la colaboración efectiva con organismos de seguridad.

Sus principales funciones son las siguientes:

a) Diseñar y mantener los planes de seguridad física de todas las instalaciones.

b) Supervisar la instalación, mantenimiento y operación de sistemas de videovigilancia, alarmas, controles de acceso y dispositivos perimetrales.

c) Coordinar al personal de seguridad externa (vigilantes) y planificar rondas y dispositivos de vigilancia.

d) Aprobar la elaboración de protocolos de actuación ante incidentes físicos (intrusiones, vandalismo, sabotajes, amenazas, etc.) y coordinar respuestas.

e) Colaborar con el con el área de Prevención de Riesgos Laborales en el mantenimiento y actualización de los planes de emergencia y evacuación de las instalaciones.

f) Velar por el cumplimiento normativo en materia de seguridad física, especialmente en lo relativo a infraestructuras críticas.

g) Ejercer como punto de contacto (Responsable de Seguridad y Enlace o RSE) con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

h) Formar y concienciar al personal sobre buenas prácticas de seguridad, accesos restringidos y actuación ante emergencias.

i) Participar en proyectos técnicos y de infraestructuras para incluir desde el diseño medidas preventivas de seguridad.

j) Elaborar informes periódicos, analizar indicadores de seguridad física y proponer mejoras continuas en base a datos y evolución de amenazas.

6.8 RESPONSABLE DE LA INFORMACIÓN

Al Responsable de la Información le corresponden las siguientes funciones:

a) Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información. Si esta información incluye datos de carácter personal, además deberá tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento.

b) Establecer los niveles de seguridad de la información, conforme al Anexo I del ENS, evaluando el impacto sobre la confidencialidad, integridad y disponibilidad.

c) Determinar la categoría del sistema, junto con el Responsable del Servicio y el Responsable de Seguridad de la Información, en función de los requisitos de seguridad de la información.

d) Revisar y validar el análisis de riesgos de la información, fijando el nivel de riesgo aceptable y aprobando el plan de tratamiento.

e) Aceptar formalmente el riesgo residual, asegurando que se encuentra dentro de los márgenes definidos por la política de seguridad.

f) Asumir la responsabilidad última sobre el uso que se haga de una cierta información y garantizar su protección, así como de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Las funciones de Responsable de la Información recaerán en los Jefes de División, o el Subdirector en caso de que no exista división.

6.9 RESPONSABLE DEL SERVICIO

Sus funciones podrán ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información.

Las funciones del Responsable del Servicio son las siguientes:

a) Determinar los niveles de seguridad de los servicios, considerando la confidencialidad, disponibilidad, accesibilidad, interoperabilidad y criticidad operativa, prestando especial atención al marco establecido en el Anexo I del Esquema Nacional de Seguridad.

b) Participar en la categorización del sistema, aportando los requisitos de seguridad desde el punto de vista del servicio.

c) Aprobar el riesgo residual sobre los servicios, tras el análisis realizado por el RSI, si se encuentra dentro de los márgenes aceptables.

d) Colaborar en la planificación de medidas de seguridad, asegurando que los servicios heredan los requisitos derivados de la información tratada.

e) Asistir a la definición de la política de seguridad y normativa, desde la perspectiva de los procesos de negocio y la continuidad de los servicios.

f) Asumir la responsabilidad última de cualquier error o negligencia, imputable a sus funciones, que lleve a un incidente de disponibilidad de los servicios, así como sobre el uso que se haga de los mismos.

g) Asumir la responsabilidad sobre la gestión de los ficheros y tratamientos de datos personales que se realizan en su área en concreto y, por tanto, sobre su protección.

Las funciones de Responsable del Servicio recaerán en los Jefes de Departamento.

6.10 RESPONSABLE DEL SISTEMA

Al Responsable del Sistema le corresponden las siguientes funciones:

a) Implantar las medidas de seguridad indicadas por el RSI, asegurando su correcta integración en la arquitectura del sistema.

b) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

c) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

d) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

e) Ejecutar la suspensión cautelar del servicio, si identifica deficiencias graves de seguridad, informando a los responsables correspondientes.

f) Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el RSI.

g) Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al RSI.

h) Elaborar los Planes de Continuidad del Sistema para que sean validados por el RSI, y aprobados por el Comité de Dirección.

i) Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

j) Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al RSI de la Información para su aprobación.

En sistemas que, por su complejidad, distribución, separación física o número de usuarios, requieran apoyo adicional, el Responsable del Sistema podrá designar Responsables de Sistemas Delegados. Estos asumirán, en su ámbito, las funciones que les delegue en materia de operación, mantenimiento, instalación y verificación del sistema. La responsabilidad última seguirá recayendo en el Responsable del Sistema, a quien los delegados reportarán directamente.

No podrá existir dependencia jerárquica entre el Responsable de la Seguridad de la Información (RSI) y el Responsable del Sistema.

Las funciones de Responsable del Sistema recaerán en los Jefes de Departamento o Sección de cada especialidad tecnológica (Desarrollo de Sistemas de Información, Infraestructuras de las tecnologías de la información o de la operación y parque microinformático).

6.11 ADMINISTRADOR DE SEGURIDAD

Al Administrador de Seguridad le corresponden las siguientes funciones:

a) Aplicar las medidas técnicas de seguridad acordadas, ejecutando su implantación y validando su funcionamiento.

b) Monitorizar el estado de seguridad del sistema (tanto en el ámbito TI como TO, según corresponda), reportando al RSI cualquier anomalía detectada.

c) Gestionar la configuración segura de los componentes, incluyendo sistemas operativos, redes, dispositivos y aplicaciones.

d) Responder a los incidentes de seguridad según el procedimiento y protocolos establecidos.

e) Realizar el análisis forense tras la ocurrencia del incidente y generar el informe correspondiente.

f) Realizar periódicamente y como parte del Plan Director de Auditorías de EMASESA, auditorías técnicas de seguridad o supervisar su realización por parte de terceros.

g) Proponer al RSI mejoras en los mecanismos de seguridad.

h) Asesorar técnicamente a administradores de sistemas, respecto a configuraciones y decisiones de seguridad.

En lo que respecta a sus obligaciones:

a) No abusar de sus privilegios de acceso especiales, ni intentar saltar los mecanismos y dispositivos de seguridad sin autorización (por ejemplo, sólo en pruebas de hacking).

b) Evitar cualquier intento de acceso no autorizado a datos o recursos de EMASESA, e informar de posibles debilidades en los controles o fallos de seguridad detectados.

c) Utilizar los controles y medios que se hayan establecido para proteger tanto la información como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos.

d) Mantener la confidencialidad sobre mecanismos de seguridad y posibles debilidades, que conozca en el desempeño de sus funciones, aun cuando haya cesado en el puesto o su relación con EMASESA.

e) No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los administradores de seguridad serán responsables ante EMASESA de todos los accesos y actividades que se puedan haber realizado utilizando su identificador de usuario y contraseña.

f) Cumplir y aplicar la normativa interna en cuanto a gestión de soportes informáticos que contengan información, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia. En el caso de averías que requieran su transporte fuera de las instalaciones se intentará borrar previamente su contenido o se exigirán garantías escritas de que se hará así.

g) Las que le correspondan como usuario de los sistemas de información de EMASESA.

6.12 ADMINISTRADOR DE SISTEMAS

Las funciones del Administrador de Sistemas son:

a) Administrar y monitorizar el funcionamiento correcto de los sistemas informáticos e infraestructura de soporte de EMASESA (tanto en el ámbito TI como TO según corresponda).

b) Realizar las copias de seguridad de los sistemas, aplicaciones y datos, así como almacenar y proteger las copias obtenidas, según el procedimiento establecido.

c) Realizar las recuperaciones de información desde copias de seguridad siguiendo el procedimiento establecido.

d) Deshabilitar servicios y puertos abiertos innecesarios en los equipos, desactivar cuentas por defecto que no sean necesarias o modificar las credenciales en caso contrario y apagar servidores sin uso. En general, inhabilitar cualquier activo o recurso informático cuyo uso no esté justificado.

e) Instalar los parches y actualizaciones de seguridad de las aplicaciones y sistemas de información.

f) Habilitar los registros de accesos y de funcionamiento en los sistemas de información y salvaguardar estos ficheros.

g) Aplicar los procedimientos de enmascaramiento, disociación, seudonimización u otro tipo establecidos para asegurar que en las fases de desarrollo y/o test de los sistemas de información no se utilicen datos personales reales.

h) Realizar las pruebas del Plan de Recuperación ante Desastres con la periodicidad y criterios establecidos.

En cuanto a sus obligaciones, son las siguientes:

a) No abusar de sus privilegios de acceso especiales, ni intentar saltar los mecanismos y dispositivos de seguridad.

b) Administrar las herramientas de seguridad de EMASESA de acuerdo con los requisitos de seguridad establecidos.

c) Cumplir la normativa en cuanto a gestión de soportes informáticos que contengan datos, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia.

d) Las que le correspondan como usuario de los sistemas de información de EMASESA.

6.13 DESARROLLADOR DE SISTEMAS

Su principal función es desarrollar y probar los sistemas de información y aplicaciones conforme a los requerimientos y necesidades de EMASESA, teniendo en cuenta los principios fundamentales de Desarrollo Seguro de Software.

En lo que respecta a sus obligaciones, son las siguientes:

a) No abusar de sus privilegios de acceso especiales, ni intentar saltar los mecanismos y dispositivos de seguridad.

b) Mantener la confidencialidad sobre mecanismos de seguridad y posibles debilidades, que conozca en el desempeño de sus funciones, aun cuando haya cesado en el puesto o su relación con EMASESA.

c) Impedir accesos al código fuente de los desarrollos por parte de personas no autorizadas por EMASESA, ni durante ni después de finalizar su relación laboral con la compañía.

d) No usar para fines personales, ceder, ni lucrarse del código fuente de los desarrollos al que tenga o haya tenido acceso durante su relación laboral con EMASESA o en caso de que esta haya finalizado.

e) No alterar el código fuente de los desarrollos con fines de pérdida de confidencialidad, integridad y/o disponibilidad.

f) Cumplir la normativa interna en cuanto a gestión de soportes informáticos que contengan datos, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia.

g) Asegurarse de que, en las fases de desarrollo y/o test de los sistemas de información de cada una de las aplicaciones, así como en los Manuales de Usuario, no se utilicen datos personales reales, o bien que, en caso contrario, se haya asegurado el nivel de seguridad correspondiente al tipo de dato tratado.

h) Las que le correspondan como usuario de los sistemas de información de EMASESA.

6.14 USUARIOS

Se considera como usuario a cualquier persona empleada, contratista o tercero autorizado a acceder y hacer uso de los sistemas y recursos de información de EMASESA.

Las funciones y obligaciones establecidas afectarán a todas las personas usuarias sin excepción, en función en su puesto de trabajo y de las actividades que realicen

Sus funciones son las siguientes:

a) Realizar las funciones propias de su cargo de acuerdo con la ficha de valoración del puesto de trabajo, en el caso de personal interno.

b) Realizar las actividades asignadas para la realización de un trabajo o actividad concretos contratado por EMASESA, en el caso de personal externo.

Las obligaciones de los usuarios son las siguientes:

Con carácter general:

a) Conocer y cumplir la normativa y directrices de EMASESA en materia de Seguridad de la Información, así como las consecuencias y responsabilidades que se pudieran derivar de su incumplimiento. En particular, conocer, cumplir y aceptar las “Normas de Usos de los Recursos Tecnológicos y de Información” (NURTI).

b) Cuidar los elementos de trabajo y herramientas que EMASESA ponga a su disposición, y utilizarlos prioritariamente con fines laborales compatibles con el puesto de trabajo desempeñado.

c) Mantener la confidencialidad de la información de EMASESA que conozca en el desempeño de su función, aun después de haber cesado en su puesto o en su relación con EMASESA.

d) No intentar evitar los mecanismos y dispositivos de seguridad para el control de acceso y uso de los recursos de información de EMASESA.

e) Informar con la mayor diligencia, de cualquier sospecha de debilidades en los controles o mecanismos de seguridad, así como de cualquier incidente de seguridad que se sospeche o detecte.

f) No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables ante EMASESA de todos los accesos y actividades que se puedan haber realizado utilizando su identificador de usuario y contraseña.

g) Usar de forma adecuada y cumpliendo la normativa interna de EMASESA, los mecanismos de identificación y autenticación ante los sistemas de información bien sean contraseñas u otros sistemas más avanzados (biométricos u otros). En el caso de contraseñas cumplir especialmente con lo previsto en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de estas, así como el cambio con la periodicidad que se determine.

h) Utilizar los controles y medios que se hayan establecido para proteger tanto la información como los propios sistemas de información y sus componentes: los ficheros automatizados,

los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos.

i) No sacar equipos, soportes de información o documentación de las instalaciones de EMASESA sin la autorización necesaria, y en todo caso, con los controles que se hayan establecido.

j) Devolver todos los activos de información de EMASESA que obren en su poder en caso de que le sean requeridos o al finalizar su relación laboral con la compañía.

k) Colaborar con el personal encargado de la investigación de un incidente en todo cuanto le sea solicitado.

l) Participar de las acciones formativas y de concienciación en materia de Seguridad de la Información que se lleven a cabo en EMASESA.

m) En relación con el cumplimiento en materia de Protección de Datos de Carácter Personal:

n) No acceder ni hacer uso de datos de carácter personal si no ha sido expresamente autorizado para ello y, de ser así, sólo para la finalidad concreta que le haya sido encomendada, cumpliendo cualquier limitación que se haya establecido y utilizando los medios técnicos establecidos en la autorización al tratamiento de los datos.

o) Notificar cualquier fallo de seguridad que le posibilite el acceso de cualquier tipo de dato de carácter personal, incluso el simple visionado en pantalla de un ordenador, para los cuales no haya sido expresamente autorizado a acceder.

p) Proteger los datos personales de EMASESA que excepcionalmente, y habiéndole sido autorizado su uso, tuvieran que almacenarse o usarse fuera del lugar de trabajo: en equipos de proveedores, en el propio domicilio o en otras instalaciones alternativas, tanto en sistemas fijos como en portátiles.

En el caso de usuarios con acceso remoto (teletrabajo), además de las anteriores:

a) Comunicar cualquier incidente o sospecha de incidente de seguridad que ocurra en el equipamiento que está siendo utilizado para el acceso remoto que, aun cuando no haya sido suministrado por EMASESA, pueda poner en riesgo la seguridad de la información y sistemas de la compañía (detección de malware, accesos o sospecha de accesos no autorizados, etc.).

b) Facilitar el acceso al lugar y recursos técnicos utilizados para el trabajo remoto durante el incidente al personal designado por EMASESA para la investigación del mismo, si fuera necesario.

Perfiles específicos en materia de Protección de Datos de Carácter Personal:

6.15 DELEGADO DE PROTECCIÓN DE DATOS (DPD)

El Delegado de Protección de Datos será único en EMASESA y se informará de su nombramiento y cese a la Agencia Española de Protección de Datos.

Son funciones del Delegado de Protección de Datos:

a) Coordinar las distintas estrategias en materia de protección de datos con el Grupo Técnico de Protección de Datos Personales de la RED HISPALNET, así como formar parte del mismo, tal y como se establece en el Artículo 10 de la PSI de los Organismos de la RED HISPALNET.

b) Las atribuciones establecidas en el Artículo 18 de la PSI de los Organismos de la RED HISPALNET

c) Informar y asesorar al Responsable de Tratamiento y al personal que presta sus servicios en EMASESA (propio o externo), de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones vigentes en materia de protección de datos de carácter personal.

d) Supervisar el cumplimiento de lo recogido en el RGPD y otras disposiciones de protección de datos personales.

e) Asesorar, en cuanto le sea requerido, acerca de la evaluación de impacto relativa a la protección de datos

f) Cooperar con la autoridad de control, actuando como punto de contacto para cuestiones relativas al tratamiento, incluida la realización de consultas.

En relación con el Registro de Actividades de Tratamiento:

a) Identificar las bases jurídicas de los tratamientos.

b) Establecer y gestionar los registros de actividades de tratamiento.

En relación con la aplicación de los derechos de los afectados por el tratamiento:

a) Supervisar las formalidades que la regulación en materia de protección de datos de carácter personal exige en el ejercicio de los derechos de los afectados.

b) Verificar el cumplimiento del derecho a la información y consentimiento del afectado, así como la legalidad de las cesiones datos y transferencias internacionales si las hubiera, todo ello relacionado con los datos de carácter personal.

c) Valorar las solicitudes de ejercicio de derechos por parte de los interesados (acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad) y elaborar la respuesta en nombre de EMASESA, verificando su cumplimiento.

En relación con el tratamiento de ficheros temporales:

a) Concienciar a los usuarios para que eliminen periódicamente los ficheros temporales de los ordenadores personales y de sus carpetas en los servidores.

En relación con la gestión de soportes y documentos

a) Revisar las autorizaciones de la salida, fuera de EMASESA, de soportes informáticos o de otro tipo con datos de carácter personal.

b) Dictar normas específicas y supervisar las relaciones de EMASESA con empresas externas que vayan a efectuar el mantenimiento de los sistemas informáticos.

c) Verificar que las empresas externas aplican las medidas necesarias para garantizar la seguridad de los ficheros de datos de carácter personal, cualquiera que sea el soporte utilizado.

En relación con la Inspección de la Agencia de Protección de Datos:

a) Asumir la representación de EMASESA (en delegación del Responsable del Tratamiento).

b) Seleccionar a las personas por parte de EMASESA que participarán en la inspección.

c) Colaborar en todo lo posible con los inspectores de la Agencia de Protección de Datos.

d) Presentar el Informe de Inspección al Responsable del Tratamiento.

e) Además de las anteriores, asesorar al Responsable del Tratamiento u otros órganos internos en cuestiones relativas a:

f) Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

g) Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

h) Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

i) Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

j) Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

k) Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

l) 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.

m) Diseño e implantación de políticas específicas para la protección de datos de carácter personal.

n) Implantación de las medidas de protección de datos de carácter personal desde el diseño y por defecto, adecuadas a los riesgos y naturaleza de los tratamientos.

o) Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

p) Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

q) Relaciones con las autoridades de supervisión.

r) Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

6.16 RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona jurídica que, solo o junto con otros, determina los fines y medios del tratamiento, es decir, EMASESA a través de su representante legal.

Las funciones del Responsable del Tratamiento son las siguientes:

a) Decidir sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal.

b) Designar las responsabilidades en materia de seguridad y establecer su funcionamiento administrativo.

c) Llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

d) Adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pueden incurrir en caso de incumplimiento.

e) Adoptar las medidas de índole técnica, procedimentales y organizativas para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

f) Adoptar medidas y establecer criterios para la selección de encargados de tratamiento que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del RGPD y la protección de los datos de carácter personal.

g) Formular las alegaciones que considere pertinentes cuando la autoridad de control le dé traslado de la reclamación de un afectado.

Las obligaciones son las siguientes:

a) Garantizar el cumplimiento de los deberes de secreto y seguridad y cumplir con el deber de custodia de los datos de carácter personal.

b) Evaluar los riesgos que sus actividades de tratamiento suponen para los derechos y libertades de las personas físicas (artículo 24 y 32 del RGPD) y determinar qué medidas técnicas y organizativas son adecuadas (principio de responsabilidad proactiva).

c) Realizar una Evaluación de Impacto en la Privacidad cuando el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas.

d) Proporcionar a los titulares de los datos personales, en la recogida de éstos, toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

e) Obtener el consentimiento libre, informado, específico e inequívoco por parte del interesado, para el tratamiento de los datos personales.

f) Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

g) Implantar y poner a disposición de los interesados titulares de los datos, o en su caso sus representantes, medios, accesibles y sencillos para el ejercicio de sus derechos sobre los datos de carácter personal (acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad), así como resolver sobre las peticiones recibidas.

h) Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en el RGPD y la LOPDGDD. En particular, incluir en los contratos de prestación de servicios que impliquen acceso a datos de carácter personal las cláusulas que establezcan las obligaciones de las empresas de servicios en la seguridad de los datos.

i) Notificar los incidentes con afección a datos personales a la autoridad de control, siempre que entrañe un riesgo para los derechos y las libertades de las personas físicas, así como a los interesados en caso de que dicho riesgo pueda ser alto.

j) Informar a los afectados en el caso de cesión de datos.

k) Autorizar el tratamiento de datos de carácter personal fuera de los locales cuando sea estrictamente necesario.

l) Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que sea de aplicación.

6.17 ENCARGADO DEL TRATAMIENTO

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable, en este caso a EMASESA, que conlleva el tratamiento de datos personales por cuenta de éste.

Sus funciones son las siguientes:

a) Realizar todos los tratamientos, automatizados o no, que le hayan sido encomendados formalmente, aplicando medidas técnicas y organizativas apropiadas para el cumplimiento de los requisitos del RGPD y de la finalidad del tratamiento, y que garantice la protección de la información y los derechos del interesado.

b) Llevar un registro de todas las actividades de tratamiento efectuadas por cuenta de EMASESA.

En cuanto a sus obligaciones, serían las siguientes:

a) Preservar que solo tengan acceso y a los ficheros correspondientes, las personas autorizadas para ello, actuando únicamente con el alcance que le haya sido fijado: solo lectura, lectura y copia, modificación, etc.

b) Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad.

c) Aplicar las medidas técnicas y organizativas apropiadas para asistir y colaborar con EMASESA en el cumplimiento de su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

d) Notificar, sin dilación indebida, a EMASESA las violaciones de la seguridad de los datos personales de las que tenga conocimiento, así como a la autoridad de control y/o a los interesados si le hubiera sido encomendada dicha actividad.

e) Comunicar a EMASESA, cualquier mal funcionamiento de los medios técnicos y materiales puestos para regular el control de acceso a ficheros automatizados o no automatizados.

f) No recurrir a otro encargado sin la autorización previa por escrito del EMASESA y, en este último caso, informar a EMASESA y solicitar autorización para cualquier cambio previsto en la incorporación o sustitución de otros encargados.

g) Suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios encomendados, incluso las copias existentes, a menos que se requiera la conservación de los datos personales en virtud de alguna regulación y así quede recogido en el contrato de encargado.

h) Poner a disposición de EMASESA, cuando así le sea solicitado, toda la información necesaria para demostrar el cumplimiento de sus obligaciones contractuales y legales.

i) Cooperar con la autoridad de control, si le fuera requerido.

j) Cumplir todas las funciones, obligaciones y recomendaciones asignadas a los usuarios de los Sistemas de Información automatizados o no automatizados de EMASESA.

7 RESOLUCIÓN DE CONFLICTOS

De acuerdo con el Principio de Jerarquía que rige en las Administraciones Públicas, en caso de conflicto entre los diferentes responsables y/o diferentes servicios, éste será resuelto por el superior jerárquico de los mismos.

En defecto de lo anterior, prevalecerá en primer lugar la decisión del Comité de Seguridad de la Información y en segundo lugar la del Comité de Dirección.

8 OBLIGACIONES DEL PERSONAL

Todo el personal de EMASESA y colaboradores externos, tienen la obligación de conocer y cumplir la presente PSI, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad de la Información disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la PSI o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

9 ASESORAMIENTO ESPECIALIZADO EN MATERIA DE SEGURIDAD

9.1 ASESORAMIENTO ESPECIALIZADO

El RSI será el encargado de coordinar los conocimientos y las experiencias disponibles en EMASESA con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

9.2 COOPERACIÓN ENTRE ORGANISMOS Y ADMINISTRACIONES PÚBLICAS

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, EMASESA mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

9.3 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

El RSI propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la PSI con el fin de garantizar que las prácticas en EMASESA reflejan adecuadamente sus disposiciones.

10 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Reglamento UE del Parlamento Europeo y del Consejo en vigor, 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.

11 FORMACIÓN Y CONCIENCIACIÓN

EMASESA, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso, y sus responsables jerárquicos, tengan una especial sensibilidad hacia los riesgos de seguridad de la información. El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de EMASESA y a todas las actividades, de acuerdo con el principio de seguridad integral recogido en el art. 5 del ENS.

12 ANÁLISIS Y GESTIÓN DE RIESGOS

EMASESA asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas).

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad se realizará un análisis de riesgo cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.

- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas por el RSI al Comité de Seguridad de la Información y al Comité de Dirección.

Estas conclusiones, entre las que se incluirán los riesgos residuales y el riesgo objetivo, deberán ser aceptados y aprobados por el Comité de Dirección, o bien solicitar medidas adicionales de mitigación de tal riesgo residual.

13 ESTRUCTURA NORMATIVA

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: constituido por la PSI, establece los principios generales y objetivos en materia de seguridad. Lo aprueba, en última instancia, el Consejero Delegado.
- Segundo nivel: constituido por los Manuales y Procedimientos de Seguridad de la Información. Se aprueban según lo recogido en el Procedimiento del SIG: Control de la Información Documentada (GE 027.03).
- Tercer nivel: Instrucciones Técnicas de Seguridad, que son documentos técnicos orientados a resolver las tareas críticas. Los aprueba el Responsable del Sistema de Información correspondiente, bajo la supervisión del RSI.
- Cuarto nivel: Informes, registros y evidencias electrónicas. La responsabilidad de que existan este tipo de documentos es de cada Responsable del Sistema de Información.

14 CALIFICACIÓN DE LA INFORMACIÓN.

Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Se establecen mecanismos para calificar la información en función de su naturaleza, estableciendo requisitos de acceso y control para el acceso a la misma, tal y como se desarrolla en el Procedimiento de Clasificación y Manejo de la Información (GE.010.12).

14.1 APROBACIÓN

La documentación que es susceptible de necesidad de aprobación contará con una sección dentro del documento definida a tal fin donde quede contenida la firma del aprobador.

La versión aprobada será almacenada en el repositorio dispuesto a tal fin y el Responsable del Sistema de Información velará por la seguridad de sus metadatos a fin de prevenir modificaciones no autorizadas.

14.2 REVISIÓN DE LA DOCUMENTACIÓN

La documentación que es susceptible de necesidad de aprobación tendrá definidos los plazos y métodos de revisión y actualización de documentos.

Las versiones siguientes a la documentación inicial identificarán los cambios y el estado de la versión vigente de los documentos.

Los documentos se mantendrán accesibles, identificables y legibles de acuerdo con su calificación para los miembros autorizados que así lo requieran.

Para la documentación de origen externo, como resultados de auditorías externas, se llevará a cabo el control de su distribución.

Prevenir el uso de documentos obsoletos y aplicarles una identificación adecuada en el caso de que se mantengan por razones de utilidad para la Organización.

La documentación informal de los sistemas cuando vaya a servir de evidencia documental del cumplimiento de los controles se restructurará de conformidad con lo descrito en la PSI, de este modo la documentación contará con la aprobación del responsable del sistema y será sometida al mismo trato que el resto de documentación del ENS.

El RSI, junto con los Responsables de la Información y de los Servicios velarán por el cumplimiento de la Política de Seguridad.

14.3 CATEGORÍAS DE SEGURIDAD.

La categoría de seguridad del sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I del ENS.

- Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

- Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

- Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

El responsable de cada información seguirá los criterios determinados anteriormente para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo con lo descrito anteriormente.

14.4 OTRA DOCUMENTACIÓN

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC.

15 PUBLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El presente documento se incluirá dentro del Sistema de Gestión Integrado de EMASESA y se difundirá mediante cualquier medio que EMASESA estime oportuno, en particular, a través de la web corporativa de la entidad.

16 ENTRADA EN VIGOR

La PSI que se aprueba en este documento será aplicable a partir del día de su firma.