Política de Seguridad de la Información y Protección de Datos Personales

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
STIC-01-Politica_Seguridad	0.0	Borrador inicial de trabajo	01/02/2021
STIC-01-Politica_Seguridad	1.0	Primera versión. Texto final aprobado	27/05/2021
Política de Seguridad de la Información y Protección de Datos Personales	2.0	Segunda versión. Adaptación a la nueva normativa del ENS, a la Política de Seguridad del Ayuntamiento de Sevilla y a la nueva estructura organizativa de LIPASAM.	17/12/2024

CLASIFICACIÓN

INFORMACIÓN PÚBLICA
Nota de confidencialidad: la información contenida en este documento es INFORMACIÓN PÚBLICA. Es responsabilidad del Área o Departamento receptor de este documento su distribución interna con base en la necesidad de conocer la información aquí contenida.

CONTROL DE DIFUSIÓN

AUTOR: Limpieza Pública y Protección Ambiental, S.A.M. (LIPASAM).
DISTRIBUCIÓN: LIPASAM.

Índice

1 Introducción

Limpieza Pública y Protección Ambiental, S.A.M. (en adelante, LIPASAM), como muestra de compromiso con la seguridad de sus sistemas de información, los administrará adoptando las medidas adecuadas para protegerlos frente a cualquier amenaza que pueda afectar a la disponibilidad, integridad o confidencialidad de la información tratada y para proteger el honor y la intimidad de las personas por el uso inapropiado de la información , ha desarrollado la presente Política de Seguridad de la Información y Protección de Datos (en adelante, también "Política de Seguridad"), de conformidad con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, teniendo en cuenta, asimismo, el cumplimiento de la legislación en materia de protección de datos vigente, acorde con el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (en adelante, RGPD) así como con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales (en adelante, LOPDgdd).

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento normativo de LIPASAM, la cual es desplegada a través de las diferentes normativas y procedimientos internos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y los servicios.

2 Objetivo y ámbito de aplicación

Este documento constituye el establecimiento de una estructura organizativa para definirla, implantarla y gestionarla.

El ámbito de aplicación del presente documento aplica a todos los sistemas de información gestionados por LIPASAM.

Afectará a la información tratada por medios electrónicos y a la información en soporte papel que LIPASAM gestiona en el ámbito de sus competencias.

Debe ser conocida y cumplida por todas las personas que forman parte de LIPASAM, independientemente de cuál sea el vínculo contractual, posición, puesto, cargo y responsabilidad que desempeñen dentro de la organización.

3 Normativa de referencia

El marco legal de referencia de las actividades de LIPASAM en el ámbito de esta Política de Seguridad de la Información y Protección de Datos Personales está integrado, entre otros, principalmente por los siguientes cuerpos normativos y sus respectivos desarrollos:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 y por el que se deroga la Directiva 95/46/CE.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- DIRECTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n. o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Política de seguridad de la información de los organismos que conforman la red corporativa del Ayuntamiento de Sevilla, denominada RED HISPALNET, aprobada por la Junta de Gobierno de la ciudad de Sevilla en sesión ordinaria celebrada el día 16/07/2024.

Política de Seguridad de la Información de los organismos que conforman la red corporativa del Ayuntamiento de Sevilla, denominada red HISPALNET. El marco ético viene determinado por el Código Ético de LIPASAM, aprobado por la Comisión Ejecutiva del Consejo de

Administración el día 30 de noviembre de 2016, donde se recogen los principios, valores, compromisos estándares de conducta que tanto LIPASAM como las personas que la integran han de observar.

4 Principios y directrices

Los principios que deben contemplarse en la gestión a la hora de garantizar la seguridad de la información son: prevención, detección, respuesta y recuperación.

Con la observancia de estos principios de actuación se pretende que las amenazas existentes no se materialicen o, en caso de materializarse, no afecten gravemente a la información que maneja o los servicios que presta LIPASAM.

4.1 Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estas medidas y controles, así como los roles y responsabilidades de seguridad de todo el personal de la empresa, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política de Seguridad, el Departamento o Área encargada de gestionar los sistemas de información de LIPASAM debe realizar las siguientes medidas:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y, en cualquier caso, cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.3 Respuesta

Se deben llevar a efecto las siguientes actuaciones:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

4.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

4.5 Otros principios generales

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La seguridad de la información es responsabilidad de todos. Todas las personas que tienen acceso a la información de LIPASAM deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas. En particular, la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de LIPASAM.
- Todas las personas que de una forma u otra participen en la utilización, operación, administración o gestión de un sistema de información serán responsables de observar las normas de seguridad establecidas. Para ello las correspondientes responsabilidades deberán quedar determinadas de forma explícita y ser comunicadas a cada una de ellas.
- La seguridad de la información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en

ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el ENS, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.

- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes:

    - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

    - 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

5 Organización de la seguridad de la información

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

- El Comité de Seguridad de la Información (en adelante, también, Comité de Seguridad).
- El Responsable de Seguridad TIC (en adelante, también Responsable de Seguridad).
- El Delegado de Protección de Datos (en adelante, también DPD).
- El Responsable de la Información y de los Servicios (en adelante, también, Responsable de la Información).
- El Responsable de Sistemas de Información (en adelante, también, Responsable de Sistemas).

5.1 Comité de Seguridad de la Información

El Comité de Seguridad es un equipo multidisciplinar nombrado para llevar a cabo la gestión y coordinación de la seguridad de la información, debiendo supervisar las actividades y controles de seguridad establecidos en LIPASAM y velar por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad de la información y protección de datos de carácter personal.

Las funciones del Comité de Seguridad tendrán las características de estratégicas, regulatorias y de supervisión que abordan aspectos concretos de la seguridad de la información y protección de datos personales. Estas funciones son:

a) Alinear e identificar los objetivos en el ámbito de la seguridad de la información y protección de datos personales con la estrategia de LIPASAM.
b) Establecer los criterios de revisión de la Política de Seguridad, así como, en su caso, proponer sus actualizaciones y modificaciones, ya sea a iniciativa propia o a propuesta de cualquiera de los integrantes de la estructura organizativa de la gestión de la seguridad de la seguridad de la información y protección de datos personales de LIPASAM, debiendo elevar sus propuestas al Consejo de Administración de la empresa para su aprobación, así como distribuirla y velar por su cumplimiento.
c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en LIPASAM.
d) Garantizar que la seguridad y protección de datos personales forman parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.
e) Proponer y aprobar, según los casos, las políticas, las normativas y los procedimientos internos que se generen en materia de seguridad de la información y protección de datos personales, así como impulsar el desarrollo normativo que se defina en LIPASAM para dar cumplimiento a la Política de Seguridad, según ésta dispone en su apartado 10 (Estructura de la normativa interna), debiendo mantener la documentación organizada y actualizada y gestionar los mecanismos de publicidad y acceso a la misma.

f) Elaborar y actualizar el Registro de Actividades de Tratamiento.
g) Aceptar los riesgos calculados en el análisis de riesgos y realizar su seguimiento y control.
h) Verificar que todas las acciones llevadas a cabo en materia de seguridad de la información y protección de datos personales sean compatibles o se encuentren respaldadas por la Política de Seguridad.
i) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de LIPASAM en materia de seguridad y protección de datos personales.
j) Promover la formación y concienciación en materia de seguridad de la información y protección de datos personales a todo el personal.
k) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad y protección de datos personales de LIPASAM.
l) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad ~~de~~ la información y protección de datos personales.
m) Evaluar de forma periódica el grado de exposición a riesgos que afecten a los sistemas de información, así como evaluar el impacto sobre la protección de datos.
n) Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información y protección de datos personales.
o) Diseñar y ejecutar los programas de actuación propios de LIPASAM, incluyendo, entre otros, el Plan de Mejora de la Seguridad, los proyectos de desarrollo normativo y las auditorías de cumplimiento y planes de adecuación legal.
p) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnico y de control, los sistemas y servicios de LIPASAM.
q) Definir, implantar y mantener los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como realizar y mantener los análisis de riesgos.
r) Supervisar de forma sistemática los controles de carácter procedimental, operacional y las medidas técnicas de protección de los datos, aplicaciones y sistemas de LIPASAM.
s) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la seguridad de la información y protección de datos personales, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de LIPASAM.

El Comité de Seguridad estará compuesto por los siguientes miembros permanentes:

- El Responsable de Seguridad.
- El DPD.
- El Responsable de Sistemas.
- El Responsable de la Información.

Adicionalmente, podrán ser invitados a asistir al Comité de Seguridad, la persona que, de acuerdo con el documento que establezca la estructura organizativa de la empresa vigente en cada momento, detente la máxima responsabilidad y autoridad ejecutiva dentro de la misma y otros responsables de las materias específicas que se vayan a tratar en las reuniones, los cuales tendrán voz, pero no tendrán voto.

Se considerará válidamente constituido el Comité de Seguridad cuando asistan al menos tres de sus miembros, entre ellos el Responsable de Seguridad y el DPD.

El Comité de Seguridad celebrará cuantas reuniones sean necesarias para cumplir sus funciones y, al menos, una vez cada año natural. Estas reuniones tendrán lugar, con carácter general, en la sede social de LIPASAM, pudiendo designarse otro lugar si así se estima oportuno en cada convocatoria.

La convocatoria de reunión corresponde al Responsable de Seguridad o al DPD, tanto por iniciativa propia como a instancia de cualquiera de los miembros del Comité.

El Comité de Seguridad adoptará sus acuerdos por mayoría simple de votos.

Se levantará acta de cada una de las sesiones del Comité de Seguridad.

El Comité de Seguridad reportará al Consejo de Administración información sobre su actividad, debiendo hacerlo al menos una vez al año tras el cierre de cada ejercicio anual.

5.2 Responsable de Seguridad TIC

Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por el responsable de la información y de los servicios. Es el responsable de que los servicios y sistemas de información de LIPASAM se mantengan con el mayor grado de seguridad atendiendo a los principios de:

- Confidencialidad: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.
- Integridad: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.
- Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios proporcionados por LIPASAM permanecerán disponibles.

Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, normativas y procedimientos derivados de la misma, haciendo controles periódicos.
b) Asesorar en materia de seguridad a los integrantes de LIPASAM que así lo requieran.
c) Coordinar la interacción con otros organismos especializados.
d) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
e) Establecer las medidas de seguridad, adecuadas y eficaces, para cumplir los requisitos de seguridad establecidos por el Responsable de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.

f) Asesorar, en colaboración con el Responsable de Sistemas y el Responsable de la Información, en la realización de los análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.
g) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
h) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones y, en su caso, realizar las convocatorias para las reuniones de este.
i) Proponer la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con el Responsable de la Información y el Responsable de Sistemas antes de ser ejecutada.
j) Elevar al Comité de Seguridad las actuaciones para tratar y mitigar el riesgo derivadas del análisis de riesgos previsto en el apartado 9 de esta Política.
k) Proponer y aprobar, según los casos, las normativas y procedimientos internos que se generen en materia de seguridad de la información, así como impulsar el desarrollo normativo que se defina en LIPASAM para dar cumplimiento a la Política de Seguridad, según ésta dispone en su apartado 10 (Estructura de la normativa interna), debiendo mantener la documentación organizada y actualizada y gestionar los mecanismos de publicidad y acceso a la misma.
l) Investigar y monitorizar los incidentes de seguridad.
m) Colaborar con el DPD para procurar una coherente gestión de seguridad de la información.
n) Formar parte del grupo Técnico de Seguridad TIC de la RED HISPALNET, al que prestará asesoramiento y soporte.
o) Poner en conocimiento de la Persona Responsable de seguridad TIC de la RED HISPALNET los incidentes de seguridad que ocurran en LIPASAM.
p) Preparar los temas relacionados con LIPASAM, a tratar en las reuniones del Grupo Técnico de Seguridad TIC de la RED HISPALNET, aportando información puntual para la toma de decisiones.
q) Responsabilizarse de la ejecución en el ámbito de LIPASAM de las decisiones del Grupo Técnico de Seguridad TIC de la RED HISPALNET.
r) Elaborar Planes con medidas para gestionar los riesgos detectados.
s) Supervisar y desarrollar las políticas de seguridad, normativas y procedimientos, y evaluar su efectividad.
t) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad.
u) Promover y formar sobre “buenas prácticas” de la organización en materia de ciberseguridad.
v) Remitir a la autoridad competente las notificaciones de incidencias con efectos adversos.
w) Recibir, interpretar y supervisar la aplicación de instrucciones y guías de la autoridad competente.
x) Recopilar y suministrar información o documentación a la autoridad competente.

Corresponde al Consejo de Administración llevar a cabo la identificación de forma inequívoca de la persona Responsable de Seguridad.

5.3 Delegado de Protección de Datos (DPD)

LIPASAM, como responsable y, en su caso, encargada del tratamiento de los datos personales, es la responsable del cumplimiento de la normativa sobre protección de datos personales de la empresa. El DPD es la persona física que ocupa la posición sobre la que recaen las siguientes funciones:

a) Informar y asesorar al Consejo de Administración y a los empleados/as que se ocupen del tratamiento de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
b) Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos y de la presente Política, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
c) Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al 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 del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto. Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones y, en su caso, realizar las convocatorias para las reuniones de este.
f) Elevar al Comité de Seguridad las actuaciones para tratar y mitigar el riesgo derivadas del análisis de riesgos previsto en el apartado 9 de esta Política.
g) Proponer y aprobar, según los casos, las normativas y procedimientos internos que se generen en materia de seguridad de la información, así como impulsar el desarrollo normativo que se defina en LIPASAM para dar cumplimiento a la Política de Seguridad, según ésta dispone en su apartado 10 (Estructura de la normativa interna), debiendo mantener la documentación organizada y actualizada y gestionar los mecanismos de publicidad y acceso a la misma.
h) Cuando detecte la existencia de una vulneración relevante en materia de protección de datos, documentarla y comunicarla inmediatamente al Consejo de Administración.
i) Formar parte del Grupo Técnico de Protección de Datos Personales de la RED HISPALNET.
j) Poner en conocimiento del Delegado/a de Protección de Datos Personales de la RED HISPALNET las cuestiones relacionadas con la protección de datos que aplican a LIPASAM para que este pueda ejercer las funciones de coordinación que se le atribuyen en la Política de Seguridad del ayuntamiento de Sevilla TIC.
k) Poner en conocimiento del Delegado/a de Protección de Datos Personales de la RED HISPALNET los incidentes sobre protección de datos personales que detecte en LIPASAM.
l) Elaborar los informes que demande el Grupo Técnico de Protección de Datos Personales de la RED HISPALNET.
m) Colaborar con el Delegado/a de Protección de Datos Personales de la RED HISPALNET en el diseño e implantación de las normas que desarrollen el presente documento en cuanto a la protección de datos personales.

El DPD será designado y cesado por el Consejo de Administración de LIPASAM.

El DPD ostentará la posición regulada en el RGPD y en la LOPDgdd, por lo que no podrá ser removido ni sancionado por el normal desempeño de sus funciones, debiendo garantizarse su independencia dentro de la organización y el acceso sin excepción a los datos personales y procesos de tratamiento gestionados en LIPASAM.

5.4 Responsable de la Información y de los Servicios

El Responsable de la Información y de los Servicios será quien en primera instancia determine la finalidad, contenido y uso de la información que se genera y gestiona dentro de su marco de competencias, siendo su responsabilidad determinar los requisitos de seguridad según los parámetros del ENS, tanto de la información tratada como de los servicios prestados.

Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información, clasificando la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.
b) Proporcionar la información necesaria al Responsable de Seguridad y el DPD para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda del Responsable de Sistemas.
c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de estos.
d) Colaborar en la evaluación de los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control.
e) Colaborar con el DPD proporcionando la información necesaria acerca del tratamiento de datos personales que se lleve a cabo en el servicio.
f) Velar por el cumplimiento de la normativa de seguridad y protección de datos personales definida por la organización en el servicio.
g) Proponer la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con el Responsable de Seguridad y el Responsable de Sistemas antes de ser ejecutada.
h) Ejecutar los requisitos de seguridad organizativos, técnicos y de control que deben cumplir los sistemas y servicios de LIPASAM.
i) Informar y asesorar al Comité de Seguridad y asistir a las reuniones de este cuando sea convocado.
j) Realizar, junto con el Responsable de Sistemas, análisis de riesgos de acuerdo con lo previsto en el apartado 9 de esta Política, cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo y serán elevadas al Responsable de Seguridad y al DPD.

Podrá identificarse un único Responsable de la Información y de los Servicios o diferenciarse ambos roles, en cuyo caso, también se podrá identificar un único Responsable de la

Información y un único Responsable de los Servicios o identificar a ambos para cada actividad de tratamiento.

Corresponde al Consejo de Administración llevar a cabo la identificación de forma inequívoca de la persona/s Responsable/s de la Información y de la/s persona/s Responsable/s de los Servicios de LIPASAM.

5.5 Responsable de Sistemas de Información

Es la persona designada a los efectos de dar cumplimiento a esta Política. Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad. Sus responsabilidades sobre todos los sistemas de información existentes en la empresa son las siguientes:

a) Realizar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la seguridad de la información.
c) Informar sobre toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos de seguridad de los sistemas de información.
e) Elaborar Planes de Continuidad de los sistemas de información.
f) Informar y asesorar al Comité de Seguridad y asistir a las reuniones del mismo cuando sea convocado.
g) Proponer la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con el Responsable de la Información y el Responsable de Seguridad antes de ser ejecutada.
h) Promover las medidas que el apartado 4.1 de esta Política establece para garantizar el cumplimiento de la Política de Seguridad con relación al principio de prevención.
i) Realizar, junto con el Responsable de la Información, análisis de riesgos de acuerdo con lo previsto en el apartado 9 de esta Política, cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo y serán elevadas al Responsable de Seguridad y al DPD.

Corresponde al Consejo de Administración llevar a cabo la identificación de forma inequívoca de la persona Responsable de Sistemas de Información de LIPASAM.

5.6 Resolución de conflictos

En caso de conflicto entre los diferentes responsables definidos en la Política, éste será resuelto por el Comité de Seguridad.

5.7 Obligaciones del personal

Todo el personal, interno o externo, de LIPASAM tiene la obligación de conocer y cumplir la presente Política de Seguridad, 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 disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

Asimismo, deberá cumplir además con las instrucciones y normas que regulen el comportamiento del personal en el uso de los sistemas informáticos y redes de comunicaciones de LIPASAM.

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

6 Asesoramiento especializado en materia de seguridad

6.1 Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en LIPASAM con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos y asesores externos especializados.

6.2 Cooperación entre organismos y otras Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, LIPASAM mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad y protección de datos personales tales como:

- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- Agencia Española de Protección de Datos (AEPD), velando por el cumplimiento de la legislación sobre protección de datos de carácter personal y controlando su aplicación.
- Instituto Nacional de Ciberseguridad (INCIBE) – CERT Centro de Respuesta a Incidentes de Seguridad: ofreciendo soluciones reactivas a incidentes informáticos, servicios de prevención frente a posibles amenazas y servicios de información, concienciación y formación en materia de seguridad (www.incibe.es).
- Grupo de Delitos Informativos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, investigando acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones que le encomienden las Autoridades Judiciales o que conozca por comunicaciones y denuncias de los ciudadanos y que por su importancia o relevancia social, dificultad técnica o número de afectados, aconseje la dedicación de este grupo.
- Consejo de Transparencia y Protección de Datos de Andalucía, velando por el cumplimiento de la legislación sobre protección de datos de carácter personal y controlando su aplicación.
- Ayuntamiento de Sevilla, determinando la Política de Seguridad a implantar en nuestra entidad y estableciendo los mecanismos de colaboración y actuación conjunta de la RED HISPALNET.

6.3 Revisión independiente de la seguridad de la información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas de LIPASAM reflejan adecuadamente sus disposiciones.

7 Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se cumplirá en todo momento lo exigido en el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD), así como lo establecido en la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDgdd) y la normativa de desarrollo de ambos cuerpos normativos y de la presente Política.

El Responsable de Seguridad, contando con el asesoramiento del DPD, determinará los requisitos de protección de datos personales que sean necesarios implementar en los sistemas teniendo en cuenta la naturaleza, alcance, contexto y fines de los tratamientos, así como los riesgos para los derechos y libertades de las personas físicas de acuerdo con lo establecido en los artículos 24 y 32 del RGPD y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo, la evaluación de riesgos penales vinculados a la protección de datos.

El DPD será el encargado de coordinar los conocimientos y las experiencias disponibles en LIPASAM con el fin de proporcionar ayuda en la toma de decisiones en esta materia, pudiendo obtener asesoramiento de otros organismos o asesores externos.

Igualmente, el DPD mantendrá contactos periódicos con organismos, entidades y asesores externos especializados en temas de protección de datos de carácter personal a los efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de LIPASAM.

8 Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información y la protección de datos personales que afecta a todo el personal de LIPASAM y a todas las actividades de acuerdo al principio de seguridad integral recogido en el ENS. A estos efectos, LIPASAM propondrá y organizará sesiones informativas, formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren y puedan acceder a dicha información.

9 Análisis y gestión de riesgos

LIPASAM 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.

El Responsable de la Información y de los Servicios es el propietario de los riesgos sobre la información y sobre los servicios, así como de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

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, el Responsable de la Información, junto con el Responsable de Sistemas, realizarán, con periodicidad al menos bienal, un análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario. El Responsable de Seguridad asesorará de la realización de los análisis y gestión de riesgos.

Se realizará un análisis de riesgos:

- Regularmente, y al menos una vez cada dos años.
- 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.
- Cuando haya cambios esenciales de la estructura organizativa definida en esta Política.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de los datos personales, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de esta forma, así como la comunicación o acceso no autorizado a dichos datos.

Las conclusiones de los análisis de riesgos serán trasladadas al DPD y elevadas al Comité de Seguridad.

10 Estructura de la normativa interna

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, al cual no puede contradecir:

Niveles	Documentos	Responsables
Primero	Política de Seguridad de la Información y Protección de Datos	Consejo de Administración
Segundo	Normativas de Seguridad y de Protección de Datos	Comité de Seguridad
Tercero	Procedimientos de Seguridad y de Protección de Datos	Responsable de Seguridad y DPD
Cuarto	Informes, registros y evidencias electrónicas	Responsable de Sistemas

10.1 Primer nivel: Política de Seguridad de la Información y Protección de Datos

Política de obligado cumplimiento por todo el personal, interno o externo, de LIPASAM que se recoge en el presente documento, siendo aprobada por acuerdo del Consejo de Administración

10.2 Segundo Nivel: Normativas de Seguridad y Protección de Datos

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal, correspondiente.

Se trata de normas generales dictadas en desarrollo de la Política de Seguridad que establecen el marco normativo aplicable a LIPASAM en materia de Seguridad y Protección de Datos.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité de Seguridad, a propuesta del Responsable de Seguridad en materia de Seguridad y del Delegado de Protección de Datos en materia de Protección de Datos.

10.3 Tercer Nivel: Procedimientos de Seguridad y Protección de Datos

Documentos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

En definitiva, describen las acciones a realizar, de una manera más detallada y concreta, dentro de un proceso relacionado con la seguridad o con la protección de datos personales. La responsabilidad de aprobación de estos procedimientos es del Responsable de Seguridad en materia de seguridad o del DPD en materia de protección de datos personales, ya sea a iniciativa propia o ya sea a propuesta del Responsable de Sistemas o del Responsable de la Información.

10.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Se incluyen en este nivel los documentos de carácter técnico mediante los que el Responsable de Sistemas recoge el resultado y las conclusiones de un estudio o una valoración y los documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también las evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que exista este tipo de documentos es del Responsable de la Información y de los Servicios.

10.5 Otra documentación

Se podrán seguir en todo momento los procedimientos, normas e instrucciones técnicas internos, así como las guías CCN y de la Agencia de Protección de Datos.

10.6 Sistema de gestión de información documentada

La Política de Seguridad y Protección de Datos será aplicable a partir del día siguiente de la fecha de su aprobación por el Consejo de Administración.

La Política de Seguridad y Protección de Datos formará parte del sistema de gestión integrado de la empresa, debiendo incorporarse a la información documentada del mismo y ser publicada para su general conocimiento y cumplimiento.

La presente Política será publicada en la intranet de LIPASAM y en las sedes electrónicas que resulten de aplicación.