Control de versiones

Versión	Motivo	Realizado por	Fecha
1.0	Versión preliminar	Responsable de Seguridad	11/06/2024

Índice

1 Introducción

Este documento presenta la Política de Seguridad de la Información (en adelante, PSI) de Sociedad Municipal de Aparcamientos de Las Palmas de Gran Canaria, SA (en adelante, SAGULPA), la cual se fundamenta en el Esquema Nacional de Seguridad (ENS). La información es un activo crítico y de un gran valor para las operaciones de la empresa, por lo que debe ser protegida adecuadamente contra cualquier amenaza, sin importar el formato, soporte, medio de transmisión, sistemas, o persona involucrada en su manejo.

La protección de la información asegura su calidad, garantiza la continuidad del negocio, minimiza riesgos y maximiza el retorno de las inversiones y las oportunidades de negocio. Este proceso requiere tanto de medios técnicos como humanos, así como una adecuada gestión y definición de los procedimientos. La colaboración e implicación de todo el personal son esenciales para el éxito de esta política.

La Dirección es consciente del valor de la información, está firmemente comprometida con los principios y directrices establecidos en este documento, y se asegurará de que todas las medidas necesarias se implementen y mantengan de manera efectiva.

2 Misión y servicios prestados de la empresa

El Excmo. Ayuntamiento de Las Palmas de Gran Canaria constituyó, como único accionista, la SOCIEDAD MUNICIPAL DE APARCAMIENTOS DE LAS PALMAS DE GRAN CANARIA, S.A. (SAGULPA), inscrita inicialmente en el Registro Mercantil de la provincia de Las Palmas el día 14 de diciembre de 1.993, como instrumento para el estudio, ordenación, regulación, construcción y explotación de aparcamientos que palíen la escasez de plazas de aparcamiento, reduciendo la intensidad del tráfico en las calles y que coadyuve a su solución.

SAGULPA desarrolla su actividad actualmente en la gestión directa e indirecta de aparcamientos, en la construcción y promoción de aparcamientos para residentes, en la gestión del servicio de retirada de vehículos de la vía pública y en la custodia de vehículos por cesión del Excmo. Ayuntamiento de Las

Palmas de Gran Canaria y en la gestión del servicio de estacionamiento regulado de vehículos de tracción mecánica en las vías públicas de la ciudad por acuerdo de dicho Ayuntamiento.

3 Propósito

El propósito de esta PSI es establecer un marco de principios y directrices que garanticen la protección adecuada de los activos de información de SAGULPA, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente. Además, promueve una cultura de seguridad dentro de la organización, involucrando a todo el personal en la implementación y mantenimiento de seguridad efectivas.

4 Alcance

Esta PSI se aplica a todos los activos de información de SAGULPA, incluyendo datos, sistemas, redes y aplicaciones, así como a las instalaciones física y virtuales donde se procesan, gestionan, transmiten y almacenan estos activos. Este alcance incluye:

1. **Personal**: Todos los empleados contratistas, proveedores y cualquier otra parte externa que tenga acceso a los activos de información de SAGULPA.
2. **Activos de Información**: Toda la información, independientemente de su formato (digital, físico, oral, etc.), que sea propiedad de SAGULPA o que esté bajo su custodia.
3. **Sistemas y Redes**: Todos los sistemas informáticos, aplicaciones, redes y dispositivos utilizados para procesar, almacenar y transmitir información.
4. **Instalaciones**: Todas las ubicaciones físicas donde se encuentren activos de información, incluyendo oficinas, centros de datos, almacenes y cualquier otra instalación.
5. **Procesos**: Todos los procesos y procedimientos relacionados con la gestión de la información, incluyendo su creación, recepción, uso, almacenamiento, transmisión y eliminación.

5 Definiciones

- **Sistema de Información:** Conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización. Incluye hardware, software, datos, procedimientos y personas.
- **Riesgo:** La posibilidad de que ocurra un evento que pueda afectar negativamente los objetivos de la organización. En el contexto de la seguridad de la información, se refiere a la probabilidad de que una amenaza explote una vulnerabilidad para causar un impacto.
- **Gestión de riesgos:** El proceso de identificar, evaluar y controlar los riesgos que podrían afectar los activos de información de la organización. Incluye la implementación de medidas para minimizar el impacto de los riesgos identificados.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Un enfoque sistemático para gestionar la información sensible de la empresa, asegurando que permanezca segura. Incluye políticas, procedimientos, directrices y recursos para gestionar y proteger la información.
- **Disponibilidad:** La propiedad de que la información esté accesible y utilizable por los usuarios autorizados cuando lo requieran.
- **Integridad:** La propiedad de que la información sea exacta y completa, y que no haya sido alterada de manera no autorizada.
- **Confidencialidad:** La propiedad de que la información no sea divulgada a personas, entidades o procesos no autorizados.
- **Autenticidad**: La propiedad que asegura que las partes involucradas en una comunicación o la fuente de la información son quienes dicen ser.
- **Trazabilidad**: La capacidad de rastrear las acciones realizadas sobre un activo de información a lo largo de su ciclo de vida, incluyendo la identificación de quién realizó las acciones y cuándo.

6 Fundamentos de esta política

El objetivo de la seguridad de la información es garantizar que SAGULPA pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Para esto, en materia de seguridad de la información deben tenerse en cuenta los siguientes principios básicos:

6.1 Seguridad como proceso integral

La seguridad debe entenderse como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Por lo tanto, debe promover la concienciación de las personas que intervienen en el proceso y de sus responsables jerárquicos para mitigar las posibles fuentes de riesgos o amenazas.

6.2 Gestión de la seguridad basada en los riesgos

El análisis de los riesgos es parte esencial y continua del proceso de seguridad. La gestión de esos riesgos permite el mantenimiento de un entorno controlado con niveles aceptables. Este análisis se realiza aplicando medidas de seguridad proporcionadas a la naturaleza de la información tratada y de los servicios prestados.

6.3 Prevención, detección, respuesta y conservación

La seguridad del sistema contempla medidas que implementen aspectos de prevención, detección y respuesta ante incidentes de seguridad, y de conservación de la información y servicios si ocurre un incidente.

6.4 Existencia de líneas de defensa

SAGULPA implementa una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permite:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa están constituidas por medidas de naturaleza organizativa, física y lógica.

6.5 Vigilancia continua y reevaluación periódica

La vigilancia continua permite la detección de actividades o comportamientos anómalos y su oportuna respuesta. Por eso, SAGULPA implementa controles y evaluaciones regulares de la seguridad (incluyendo evaluaciones de los cambios de configuración rutinaria), para conocer siempre la seguridad de los sistemas en relación con las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, se requiere una autorización formal y se debe solicitar la revisión periódica por terceros para obtener una evaluación independiente.

Las medidas de seguridad se evalúan y actualizan periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

6.6 Diferenciación de responsabilidades

SAGULPA ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en este documento.

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**, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales, además, se identifica el responsable de tratamiento y, en su caso, el encargado de tratamiento.

6.7 Organización e implantación del proceso de seguridad

La seguridad de la información compromete a todos los miembros de SAGULPA, por lo que, se identifica a los responsables y se establecen sus responsabilidades al efecto en los apartados de "Roles, responsabilidades y deberes" y "Terceras Partes" de este documento. Esta PSI y la normativa deben ser conocidas por todas las personas comprendidas en el ámbito de aplicación de este documento.

6.8 Análisis y gestión de los riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

6.9 Gestión de personal

Todo el personal de SAGULPA relacionado con la información y los sistemas es formado e informado de sus deberes y obligaciones en materia de seguridad, esencialmente mediante los procedimientos de seguridad que en cada caso procedan y mediante la normativa de uso de los activos. Sus actuaciones son supervisadas según los roles establecidos para verificar que se siguen los procedimientos definidos.

Los accesos de los usuarios son únicos y se verifican de forma periódica sus derechos y las actividades que tienen que ver con la Seguridad de la información para corregir o exigir responsabilidades en su caso.

6.10 Profesionalidad, Concienciación y Formación

La seguridad de los sistemas es gestionada y revisada por personal cualificado de SAGULPA y por personal externo especializado, que recibe y actualiza la formación necesaria para garantizar la seguridad de la información en todo el ciclo de vida de los sistemas de información: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento. Los requisitos de cualificación (formación y experiencia) son establecidos por SAGULPA.

La presente PSI debe ser conocida por todos los usuarios internos y externos y por las empresas que accedan, gestionen o traten datos de SAGULPA. El conjunto de Políticas, normas y procedimientos complementarios a esta PSI también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso. Por tanto, debe promover la formación técnica en seguridad de la información, especialmente para los RSIS. Es por esto que periodicamente, se definen programas de comunicación, concienciación y formación que se ponen a disposición de los usuarios, así como, la normativa de uso de los activos de información.

6.11 Autorización y control de los accesos

El acceso a los sistemas de información es controlado, monitorizado y limitado a los usuarios, procesos, dispositivos y sistemas de información con las mínimas funcionalidades permitidas y/o autorizadas. Por otro lado, las autorizaciones necesarias para las tareas críticas están establecidas y gestionadas.

6.12 Protección de las instalaciones

Los sistemas de SAGULPA y su infraestructura de comunicaciones están situados en áreas protegidas dotadas de medidas de seguridad físicas, de redundancia, continuidad y ambientales, y con un procedimiento de control de acceso físico.

6.13 Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad en SAGULPA tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad. Para la contratación de servicios de seguridad se acata lo señalado en los apartados anteriores y lo dispuesto en el apartado de “Terceras partes”.

6.14 Mínimo privilegio y seguridad desde el diseño

Los sistemas están diseñados y configurados con la seguridad predeterminada, proporcionando la mínima funcionalidad requerida para las operaciones, administración y registro de actividad para asegurarse que sólo acceden los usuarios y/o equipos autorizados. Se aplican las guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema para eliminar o desactivar las funciones que no sean necesarias. Todos los proyectos relacionados o que afecten a los sistemas de información en su proceso de análisis incluye una evaluación de los requisitos de seguridad para definir un modelo de seguridad consensuado con el RSI.

6.15 Integridad y actualización del sistema

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se conocerá en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

6.16 Protección de la información almacenada y en tránsito

La información se clasifica de acuerdo con la sensibilidad requerida en su tratamiento y según los niveles de seguridad y protección exigibles. SAGULPA presta especial atención a la información almacenada o en tránsito a través de entornos inseguros. Esto incluye a la información almacenada o tratada en equipos y dispositivos portátiles y periféricos, soportes de información, así como a las comunicaciones sobre redes abiertas o con cifrado débil, donde se aplican las medidas de seguridad que garanticen que la información se trata acorde a su clasificación. Se aplican procedimientos que garantizan la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información. Toda información en soporte no electrónico está protegida con el mismo grado de seguridad que si se tratara de soporte electrónico.

6.17 Prevención ante otros sistemas de información interconectados

Se protege el perímetro de acceso al sistema, en particular en las conexiones a través de Internet, analizando siempre los riesgos derivados de la interconexión con otros sistemas, y estableciendo las medidas que garanticen el nivel de seguridad necesario.

6.18 Registro de actividad y detección de código dañino

Están habilitados los registros de la actividad de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Además, se implementa un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

Al objeto de preservar la seguridad de los sistemas de información se puede analizar las comunicaciones entrantes o salientes para impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino.

6.19 Incidentes de seguridad

Se implementan medidas de seguridad, y en caso necesario, controles adicionales para prevenir incidentes. No obstante, cuando se produce una desviación significativa de los parámetros preestablecidos, se activan los mecanismos de detección, análisis y reportes necesarios y se remiten a los RSIS.

Ante un incidente de seguridad se establecen las siguientes medidas de reacción:

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

- Disponibilidad de los servicios a través de los medios y técnicas necesarias que permiten garantizar la recuperación de los más críticos.

Los usuarios disponen de canales establecidos para informar inmediatamente de cualquier incidente o anomalía detectada.

6.20 Continuidad de la actividad

Se realizan copias de seguridad que garantizan la recuperación de la información, y se establecen los mecanismos adecuados para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales. En este sentido se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos y datos electrónicos generados en el ámbito de sus competencias.

6.21 Mejora continua del proceso de seguridad

El SGSI de seguridad implantado se actualiza y mejora periódicamente.

7 Requisitos legales y marco normativo

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de AAPP, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el ENS.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de AAPP, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

Además, el RS es responsable de identificar las guías de seguridad del CCN que son de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

8 Roles y Responsabilidades

8.1 Dirección

El equipo directivo se compromete a cumplir y hacer cumplir esta Política, siendo consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad. Por lo tanto, asume las responsabilidades siguientes:

- Demostrar liderazgo y compromiso con respecto al SGSI.
- Asegurarse de que se establece la política y los objetivos de seguridad de la información y que estos son compatibles con la Dirección estratégica de la organización.
- Aprobar y comunicar la PSI y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

- Asegurarse de que estén disponibles los recursos necesarios para el cumplimiento de la PSI, de las normas de uso de los sistemas y para el funcionamiento del SGSI.
- Definir y controlar el presupuesto para seguridad de la información.
- Reunirse de manera extraordinaria bajo demanda, para ser informados sobre el SGSI y actualizar la estrategia en materia de Seguridad de la Información.

8.2 Delegado de Protección de Datos (DPD)

A tenor, del RGPD y la LOPDGDD, el DPD debe cumplir con las funciones siguientes:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación con el RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento solicitado sobre la evaluación de impacto sobre la protección de datos y supervisar su aplicación según el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

8.3 Comité de Seguridad de la Información (CSI)

Compuesto por el RS, el RSIS y la Dirección, que se reúnen semestralmente para coordinar la seguridad de la información a nivel de la organización. Sus funciones son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.

- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del SGSI, asumiendo las responsabilidades siguientes:
  - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
  - Velar por la Seguridad de la Información para considerar en todos los proyectos desde su especificación inicial hasta su puesta en operación, la creación y uso de servicios horizontales que reducen duplicidades y apoyan un funcionamiento homogéneo de los sistemas TIC.
  - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones al respecto.
  - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
  - Revisar regularmente la presente PSI para su aprobación por el órgano competente.
  - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y protección de datos de carácter personal.
  - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
  - Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la organización en materia de seguridad de la Información.
  - Reunirse al menos una vez al año o más veces de manera extraordinaria, bajo demanda, para revisión del SGSI y actualizar la estrategia en materia de Seguridad de la Información.
  - Fomentar una cultura corporativa de seguridad de la información.
  - Apoyar la mejora continua de los procesos de seguridad de la información.
  - Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de estos al menos con una periodicidad anual.

- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la Seguridad de la Información.
- Aprobar la documentación hasta su segundo nivel de normas y procedimientos.

8.4 Responsable de la Información (RSI)

El RSI es quien determina los requisitos de la información tratada. Sus responsabilidades son:

- Velar por el buen uso de la información y su protección.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información tratada mediante el análisis de su impacto.

8.5 Responsable del Servicio (RSER)

El RSER tiene las siguientes responsabilidades generales:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad del servicio, de acuerdo con el RS y el RSIS.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

8.6 Responsable de Seguridad (RS)

El RS determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reporta estas cuestiones. Sus funciones son:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el SGSI cumple con los requisitos del ENS.

- Supervisar el cumplimiento de esta PSI, normas, procedimientos derivados y la configuración de seguridad de los sistemas.
- Establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos establecidos por los RSER y RSI, según el Anexo II del ENS para declarar la aplicabilidad de las medidas.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas en colaboración con el RSIS.
- En compañía del RSIS, realiza el análisis de riesgos, seleccionar las salvaguardas a implantar, revisa el proceso de gestión del riesgo y acepta los riesgos residuales.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al RSIS para que adopte las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Seguridad, en colaboración con el RSIS.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el RSIS.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Preparar los temas a tratar en las reuniones del CSI, en coordinación con el RSIS, aportando información puntual para la toma de decisiones.
- Mediante reuniones se responsabiliza de la ejecución directa o delegada de las decisiones de la Dirección con el RSIS para asegurar la estrategia.

Además, respecto a la documentación, y apoyándose en el RSIS, también tiene las funciones siguientes:

- Proponer a la Dirección y al RSIS la documentación de seguridad de segundo nivel, procedimientos generales del SGSI y firmar esta documentación para su aprobación.
- Aprobar la documentación de seguridad de tercer nivel, es decir, los Procedimientos Operativos STIC e Instrucciones Técnicas STIC (POS e ITS).

- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.
- Para servicios externalizados, el RS se designó como POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.

Para el desarrollo de cualquiera de sus funciones el RS podrá recabar la colaboración del RSIS.

8.7 Responsable del Sistema (RSIS)

Se encarga de desarrollar e implementar la seguridad en el sistema, además, de la supervisión de la operación diaria, pudiendo delegar en administradores u operadores bajo su responsabilidad. Sus funciones son:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y SGSI, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el RS.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el RS y la Dirección.
- Realizar con la colaboración del RS, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al RS, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el RS, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).

8.8 El Administrador de la Seguridad del Sistema

Las funciones que desempeñará son las siguientes:

- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- Gestión, configuración y actualización del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- Gestión de autorizaciones concedidas a usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los procedimientos operativos de seguridad.
- Aplicar los cambios de configuración del sistema de información.
- Asegurarse que se cumplen estrictamente los controles de seguridad establecidos y que se aplican los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras, para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los respectivos Responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

8.9 Usuarios

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de SAGULPA se considerará un usuario. Los usuarios son responsables de todas las acciones realizadas utilizando sus identificadores o credenciales personales. Sus obligaciones son:

- Cumplir la PSI y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información, evitando la revelación, emisión, modificación, borrado o destrucción accidental o no autorizadas o por su mal, independientemente del soporte o medios por el que se obtenga.

- Conocer y aplicar la PSI, las normas de uso de los sistemas de información y el resto de las políticas, normas, procedimientos y medidas de seguridad aplicables.

Se sancionará a los usuarios que incumplan la PSI o las normas y procedimientos complementarios, según lo establecido en los contratos, que amparen su relación con SAGULPA, y con la legislación vigente y aplicable.

9 Datos de Carácter Personal

La organización solo recoge datos personales cuando sea necesario y guardan relación con el ámbito y las finalidades para los que se recogieron. De igual modo, se adoptan medidas técnicas y organizativas para el cumplimiento de la normativa de Protección de Datos vigente. De este modo, con la LOPDGDD se adaptan las medidas oportunas, como el análisis de legitimidad jurídica de cada uno de los tratamientos de datos, análisis de riesgos, evaluación de impacto, registro de actividades y nombramiento de los responsables que desempeñan las funciones de Delegado de Protección de Datos.

10 Procedimiento de designación y resolución de conflictos

El CSI asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información, y determinando en cada caso los motivos y el plazo de vigencia. También se asegura que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen en relación con cada responsabilidad en Seguridad de la Información.

11 Terceras partes

Cuando se presten servicios a otros organismos, o maneje información de otros organismos, se les debe hacer partícipes de esta PSI. Por tanto, está definidos y aprobados los canales para la coordinación de la información y los procedimientos de actuación ante incidentes de seguridad, así como el resto de las actuaciones que se lleven a cabo en materia de Seguridad en relación con otros organismos.

En cuanto a la utilización de servicios de terceros o cesión de información a terceros, se les debe hacer partícipes de esta PSI y de la Normativa de Seguridad existente que atañe a dichos servicios o información, quedando sujeta a las obligaciones establecidas en la esta normativa. Estos servicios, también pueden desarrollar sus propios procedimientos operativos para satisfacerla. Por lo tanto, existen procedimientos específicos de comunicación y resolución de incidencias, y se garantiza que este personal está concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta PSI.

12 Desarrollo del SGSI, Revisión y Auditorías

El CSI aprueba el desarrollo de un SGSI que es establecido, implementado, mantenido y mejorado conforme a los estándares de seguridad. Este sistema se adecua y sirve como gestión de los controles del ENS. El sistema es documentado y permite generar evidencias de los controles y del cumplimiento de los objetivos marcados. En consonancia, existe un procedimiento de gestión documental que establece las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La Política y las Normas de Seguridad de la Información se adaptan a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinean con la legislación vigente y las mejores prácticas del ENS, especialmente las guías publicadas por el CCN.

Las medidas de seguridad, los controles físicos, administrativos y técnicos aplicables se detallan en el Documento de Aplicabilidad, y son proporcionales a la criticidad de la información a proteger y a su clasificación.

El CSI revisa esta política anualmente o cuando se manifiestan cambios significativos, en donde, es sometida a una nueva aprobación por la Dirección. Mediante las revisiones se comprueba la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

La Dirección es responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en este documento.

El SGSI se debe auditar cada dos años, según el plan de auditorías desarrollado por el RS.