VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE HACIENDA

SEGIPSA

ENS

Política de Seguridad de la Información. V 2.0.

Tabla de contenido.

1. Introducción

SEGIPSA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad de la Información y la prestación continuada de los Servicios, actuando preventivamente, supervisando la actividad y reaccionando con presteza ante incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la Confidencialidad, Integridad, Disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que SEGIPSA debe aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

2. Aprobación y Entrada en Vigor

Texto aprobado el día 30 de abril de 2025 por parte del Consejo de Administración de la SOCIEDAD MERCANTIL ESTATAL DE GESTIÓN INMOBILIARIA DEL PATRIMONIO, M.P.S.A. (en adelante SEGIPSA).

Es aprobada por la Presidenta el 30 de abril de 2025.

Esta Política, debe ser conocida y asumida por todas las partes interesadas, como son las personas trabajadoras de SEGIPSA, subcontratistas y clientes de servicios de SEGIPSA que serán objeto del alcance de la certificación ENS, Nivel MEDIO. Deben establecerse los procedimientos necesarios para ello, a través de los canales corporativos de comunicación.

Esta Política de Seguridad de la Información, en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

3. Control de versiones.

Versión	Fecha	Autor	Cambios
1.0	22/03/2023	Comité de Seguridad	Versión inicial del documento
2.0	25/04/2025	Comité de Seguridad	Actualización de plantilla documental y cambios derivados de la adecuación a ENS nivel MEDIO

4. Misión y Alcance

La misión de SEGIPSA es proporcionar a la Administración General del Estado, a los poderes adjudicadores y no adjudicadores dependientes de ella, así como a las personas jurídicas de derecho público o privado del sector público estatal, controladas por la Administración General del Estado, un servicio eficiente en el ámbito inmobiliario, catastral y de gestión de la documentación administrativa, incluida la documentación digital, aplicando la experiencia y conocimiento de un modo sostenible, seguro y coordinado.

El alcance de la Política de Seguridad son los sistemas de información que soportan los servicios relacionados a continuación:

- Servicios CADA (Centro de Almacenamiento de Documentación Administrativa)
- Servicios de Catastro
- Gestión inmobiliaria
- Servicios de Comercialización
- Arquitectura y sostenibilidad

5. Objeto

El presente documento tiene por objeto establecer la Política de Seguridad de la información para la SOCIEDAD MERCANTIL ESTATAL DE GESTIÓN INMOBILIARIA DE PATRIMONIO, M.P.S.A. (SEGIPSA) regulado por Real Decreto 311/2022, de 3 de mayo, por el que se articula el Esquema Nacional de Seguridad, asegurando así la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los sistemas de información de SOCIEDAD MERCANTIL ESTATAL DE GESTIÓN INMOBILIARIA DE PATRIMONIO, M.P.S.A. (SEGIPSA) y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

6. Ámbito de Aplicación

Esta Política se aplicará a los sistemas de información de SEGIPSA, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

La Política de Seguridad de la Información será de obligado conocimiento y cumplimiento para todos los usuarios, tanto empleados como colaboradores externos, de sistemas de información de SEGIPSA y aplicable a los activos utilizados para prestar los servicios identificados en el catálogo, afectando a la información tratada por medios electrónicos.

Será de obligado cumplimiento para toda persona que acceda tanto a los sistemas de información como a la propia información que sea gestionada por la Empresa, con independencia de cuál sea su destino, adscripción o relación con el mismo.

7. Marco Normativo

En el desarrollo del presente documento se ha tenido en consideración la legislación y normativa aplicable relacionada en el documento Legislación Aplicable SEGIPSA.

El mantenimiento del marco normativo será responsabilidad de SEGIPSA.

SEGIPSA será responsable de identificar las guías de seguridad del CCN que sean de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

8. Principios de la Seguridad de la Información

SEGIPSA para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Compromiso de los órganos superiores.
La seguridad de la información cuenta 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 la Empresa para conformar un todo coherente y eficaz. Estos órganos superiores velarán por el cumplimiento del presente documento, manteniéndolo actualizado y aprobado en la Empresa, proporcionando todos los medios económicos y logísticos para el mantenimiento, evolución, adecuación al nivel MEDIO del ENS e implantación de nuevas medidas de seguridad.

La seguridad como un proceso integral y mínimo privilegio.
La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en SEGIPSA estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

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

Los sistemas de información de SEGIPSA se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño.

Vigilancia continua, reevaluación periódica, actualización del sistema y mejora continua del proceso de seguridad.
La vigilancia continua por parte de SEGIPSA permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.
La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Las medidas de seguridad se reevaluarán y actualizarán 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.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Gestión de personal y profesionalidad.
Todo el personal, propio o ajeno relacionado con los sistemas de información de SEGIPSA, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su interacción con los sistemas de información y las redes de comunicaciones podrá ser supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en el documento Normativa de Uso de Medios Electrónicos SEGIPSA, que será aprobado por el Comité de Seguridad de la Información de SEGIPSA. De igual modo, se determinarán los requisitos de formación y experiencia, en materia de seguridad de la información, necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción,

despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las empresas o profesionales que proporcionen servicios a SEGIPSA, que cuenten con profesionales cualificados y con unos niveles idóneos de seguridad, gestión y madurez de los servicios prestados.

Gestión de la seguridad basada en 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 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. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad, prevención, detección, reacción y recuperación.
SEGIPSA dispone de procedimientos de gestión de incidentes de seguridad, mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como vías de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un incidente de seguridad.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados.
SEGIPSA ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que si una capa ha sido comprometida permita desarrollar una reacción adecuada frente al incidente, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizando el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de la empresa se conecta a redes públicas, tal y como se definen en la legislación aplicable en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad.
SEGIPSA 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 el apartado de “Modelo de Gobernanza” del presente documento.

Autorización y control de los accesos.
SEGIPSA ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones.
SEGIPSA ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la

información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad.
Para la adquisición de productos o contratación de servicios tecnológicos incluidos o que afecten al alcance de la presente Política de Seguridad, SEGIPSA tendrá en cuenta, 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.

SEGIPSA valora positivamente la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones cuya funcionalidad esté certificada. Esta certificación deberá estar de acuerdo con las normas y estándares reconocidas internacionalmente, en el ámbito de la Seguridad de la Información.

Protección de la información almacenada y en tránsito y continuidad de la actividad.
SEGIPSA prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el alcance de esta Política, cuando ello sea exigible por la normativa aplicable.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica tratada por SEGIPSA, según la legislación aplicable, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las disposiciones que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código dañino.
SEGIPSA registrará la actividad en todas las redes de comunicación, los sistemas de información y los dispositivos propiedad de SEGIPSA, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación; reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo garantizar la Trazabilidad en todo momento.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las empresas de capital público, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, la empresa podrá, en la medida estrictamente necesaria y proporcionada, analizar y bloquear las comunicaciones entrantes o salientes, únicamente para los fines de seguridad de la información, de forma que se pueda impedir el acceso no autorizado a redes y sistemas de información, detener ataques contra el correo electrónico, detener ataques de denegación de servicio, evitar la distribución de código dañino, así como otros daños a las antedichas redes y sistemas de información.

Se prohíbe expresamente compartir o facilitar el identificador de usuario y la contraseña para acceder a los sistemas de información a otra persona física. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física que utilice de forma no autorizada el identificador del usuario.

Con la finalidad de proteger a la empresa de código dañino, se cuenta con soluciones de seguridad en todos los activos tecnológicos que lo permiten. De igual manera se tiene implementado soluciones proporcionadas por el CCN para el despliegue y ejecución de vacunas contra código dañino.

Seguridad por defecto.
Los sistemas de SEGIPSA se configuran de tal forma que:

- Proporcionen la mínima funcionalidad requerida para que la organización alcance sus objetivos y ninguna función adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos autorizados, poniendo si fuera necesario restricciones de horarios y puntos de accesos facultados.

- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funcionalidades innecesarias o que no sean de interés.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- Se hace al usuario partícipe de la seguridad inculcándole la necesidad de ello y realizando tareas como: cambio de contraseña, actualización de sistema operativo, recibiendo formación en seguridad, etc.

Todos estos aspectos se desarrollan en el documento **"Normativa de Uso de medios electrónicos SEGIPSA"**.

Infraestructuras y servicios comunes.
SEGIPSA tendrá en cuenta la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales para facilitar el cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.
SEGIPSA tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para empresas de capital público que sean aplicables.

Estructura documental.
La estructura documental de SEGIPSA se basa en la tipología relacionada a continuación, estructurada su dependencia en el orden mostrado, como se indica en el Documento de Seguridad de SEGIPSA:

- *Política de Seguridad de la Información*: declaración de alto nivel, en la que la organización, adquiere compromisos en materia de seguridad de la información.
- *Normativa*: documento de carácter general, que regula la aplicación de una medida o el uso de los recursos, puesto a disposición del personal.
- *Procedimiento*: documento que describe la forma en la cual lleva a cabo una tarea, actividad o proceso.
- *Instrucción Técnica*: documento que describe de forma detallada como se llevan a cabo las tareas, actividades o procesos definidos en los procedimientos.
- *Plan*: documento de planificación, tareas, actividades o procesos.
- *Registro*: evidencias de la implantación.

Calificación de la Información.
La información responsabilidad de SEGIPSA, será calificada en relación con su sensibilidad, estableciendo directrices para su gestión con relación a su generación, almacenamiento, transmisión y eliminación.

Cambio Climático.
En base a la certificación vigente ISO14001 de Gestión Ambiental y los análisis realizados, SEGIPSA determina que no causa perjuicio significativo al medio ambiente en el desarrollo de sus actividades en materia de Seguridad de la Información.

9. Modelo de Gobernanza

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información adaptada a las necesidades y particularidad de SEGIPSA, se realiza una designación de roles por bloques de responsabilidad: Gobierno, Supervisión y Operación.

De acuerdo con esta estructura, basados en la normativa CCN-STIC 801, se han asignado las siguientes responsabilidades y funciones de seguridad:

- Gobierno, **Responsable de la Información**, cuyas funciones implican la determinación de los requisitos de la información tratada. Este rol recae sobre el Director de Recursos Humanos, Tecnología y Servicios Generales.

- Gobierno, **Responsable del Servicio,** cuyas funciones implican la determinación de los requisitos del servicio y niveles en materia de seguridad. Este rol recae sobre el Jefe de Área de Seguridad Institucional y Servicios Generales.

- Supervisión, **Responsable de Seguridad**, cuyas funciones implican la supervisión y propuesta de los requisitos de seguridad de la información y de los servicios, promover la formación y concienciación en materia de seguridad de la información para todas las personas empleadas de SEGIPSA. Este rol recae sobre el Técnico Superior del Área de Seguridad Institucional y Servicios Generales.

- Operación, **Responsable del Sistema**, quien se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo. Este rol recae sobre el Jefe del Área de Tecnología y del cual depende el administrador de seguridad.

- **Administrador de Seguridad**, dependiente del Responsable del Sistema es quien se encarga de la ejecución y administración de los sistemas y medidas de seguridad aprobadas, Este rol recae sobre el Técnico Superior del Área de Tecnología.

9.1 Responsabilidades asociadas al Esquema Nacional de Seguridad.

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Bloque de Gobierno

Responsable de la Información, cuyas funciones son:

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el Anexo I del Real Decreto del Esquema Nacional de Seguridad.
- Es el responsable del uso que se haga de cierta información y, por tanto, de su protección.

Responsable del Servicio, cuyas funciones son:

- Establecer los requisitos del servicio en materia de seguridad.
- Establecer los niveles de seguridad de los servicios.
- Determinar los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Real Decreto del Esquema Nacional de Seguridad.

Bloque de Supervisión

Responsable de Seguridad, cuyas funciones son:

- Verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información, así como elaborar un Plan de Concienciación y Formación para toda la empresa.
- Definir, desarrollar y mantener procedimientos y normativas que permitan una gestión eficiente de la seguridad de la información.
- Conservar y revisar todos los documentos relativos a la Seguridad de la Información.

- Designar responsables de la ejecución del análisis de riesgos, declaración de aplicabilidad y plan de tratamiento de riesgos, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema.
- Participar en la elaboración e implantación de planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las auditorias de seguridad de la información que se realicen en SEGIPSA.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.
- Coordinar con el Responsable del Delegado de Protección de Datos de SEGIPSA, en su materia.

Bloque de Operación

Responsable del Sistema, cuyas funciones son:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto mantenimiento.
- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información 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.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

Administrador de la seguridad del sistema, cuyas funciones son:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La aplicación de los procedimientos operativos de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular, de los privilegios concedidos, incluyendo la monitorización de las actividades en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable del Sistema y al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad identificada.
- Investigar y resolver cualquier incidente de seguridad, desde su detección hasta su resolución.

9.2 Funciones del Comité de Seguridad de la Información.

El Comité de Seguridad de la Información está constituido por los siguientes responsables:

- Responsable de la Información: Director de Recursos Humanos, Tecnología, Seguridad y Servicios Generales.
- Responsable del Servicio: Jefe del Área de Seguridad Institucional y Servicios Generales.
- Responsable de Seguridad: Técnico Superior del Área de Seguridad Institucional y Servicios Generales.
- Responsable de Sistema: Jefe del Área de Tecnología.

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

- Asesorar en materia de Seguridad de la Información.

- 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - 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 cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la Normativa de Seguridad de la Información.
    - Verificar los Procedimientos de Seguridad de la Información y demás documentación para su aprobación.
    - Elaborar programas de formación y concienciación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y también Protección de Datos de carácter personal, si se realizan de manera conjunta.
    - 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 de Seguridad que permitan verificar el cumplimiento de las obligaciones de la organización en materia de Seguridad de la Información.

9.3 Procedimientos de designación.

La designación de los Responsables identificados en esta Política se realiza y aprueba por el Consejo de Administración de SEGIPSA.

La designación se basa en la estructura de la Dirección de RRHH, Tecnología, Seguridad y SSGG, y observa el principio recogido en el artículo 11 del Esquema Nacional de Seguridad que exige que el Responsable de Seguridad sea independiente del Responsable del Sistema.

9.4 Resolución de conflictos.

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

10. Normativa de Seguridad

10.1 Consideraciones Generales.

Todos los recursos que son puestos a disposición de los Usuarios de SEGIPSA (personal, directivos, etc.) para el desarrollo y cumplimiento de sus funciones laborales, incluyendo conexión a Internet, ordenadores, dispositivos móviles o portátiles y el correo electrónico, son propiedad de SEGIPSA.

SEGIPSA ha optado por un régimen de uso restringido de los Sistemas de Información, ello significa que los Usuarios sólo podrán realizar gestiones y comunicaciones que no entren dentro de lo personal y dentro de la esfera de su intimidad, puesto que toda actividad desarrollada usando activos y sistemas de información de SEGIPSA, así como en la red corporativa cableada e inalámbrica de SEGIPSA, podría ser monitorizada.

El documento ***Normativa de uso de medios electrónicos SEGIPSA***, tiene por objeto establecer la normativa de uso de medios electrónicos en SEGIPSA en base a los requisitos dispuestos en el Esquema Nacional de Seguridad.

10.2 Manejo de Documentación.

En relación a cualquier documento o información, perteneciente a SEGIPSA, al que tenga acceso el Usuario:

- Custodiará los documentos para impedir su visualización o manipulación por otras personas.
- Los documentos se guardarán bajo llave.
- El desecho de los documentos requerirá su destrucción o triturado de forma que se impida recuperar la información a posteriori.
- Se deberá llevar el control y hacer un seguimiento de aquella documentación que, por motivos laborales, deba compartirse con terceros. En todo caso, la información digital deberá compartirse con externos mediante el uso de las herramientas corporativas de SEGIPSA. Se estudiará, además, la necesidad de cifrar los archivos con información sensible que salga del sistema de SEGIPSA.

El Usuario, en cumplimiento de las obligaciones de confidencialidad establecidas tanto por el Estatuto de los Trabajadores, por la Ley de la Función Pública y por la normativa de Protección de Datos aplicable, en el desempeño de sus funciones laborales dentro de SEGIPSA, podrá tener acceso a información y documentación, tanto en formato informático como en soporte papel, de SEGIPSA o de terceros, informaciones y documentos respecto a la totalidad de las cuales el Usuario asume una obligación laboral de guardar secreto y mantener la confidencialidad.

El usuario deberá devolver dichos materiales a SEGIPSA, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación que le une con SEGIPSA (sea laboral, mercantil, o por traslado a cualquier otra Administración/entidad/órgano/empresa).

Se prohíben expresamente las siguientes actividades:

- Utilizar la información de ninguna otra forma o para cualquier otra finalidad que no haya sido previamente autorizada por los responsables departamentales de SEGIPSA.
- Utilizar la información en beneficio propio/privativo, o en beneficio de terceras personas, físicas o jurídicas, ajenas a SEGIPSA.

10.3 Cumplimiento legal.

SEGIPSA está comprometida con el cumplimiento de las leyes u obligaciones legales, reglamentarias o contractuales, y de los requisitos y medidas de seguridad que sean de aplicación a los Sistemas de Información de SEGIPSA.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

Todos los Usuarios implicados en el alcance, al firmar el Modelo de Aceptación y Compromiso, se obligan a conocer y asumir la presente Política de Seguridad y la Normativa de Uso de Medios Electrónicos SEGIPSA. En caso de detectarse una violación de seguridad por parte de un Usuario, se aplicarán las sanciones pertinentes según indique la ley o reglamento aplicable.

11. Datos de Carácter Personal.

SEGIPSA en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa aplicable, entre otra el Reglamento 679/2016, 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 (en adelante, Reglamento General de Protección de Datos o RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante, LOPDGDD), respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales, como en la Constitución.

Todo tratamiento de datos de carácter personal que pueda ser realizado por SEGIPSA, tanto para actividades de tratamiento dentro de los diferentes procesos de negocio, para la administración y gestión de personal, la gestión económica contable y fiscal, auditoria, prevención de blanqueo de capitales, proyectos de gestión inmobiliaria, contratación, acciones de comunicación y eventos, transparencia, entre otras actividades de tratamiento de datos, se realizará por parte de SEGIPSA respetando en todo momento los principios recogidos en la Política de Protección de Datos aprobada por la Entidad.

Igualmente, SEGIPSA llevará un registro actualizado de actividades en el que se describan los tratamientos de datos personales (RAT), que se lleven a cabo en el marco de su actividad.

De acuerdo con la LOPDGDD, SEGIPSA adoptará las medidas técnicas y organizativas apropiadas, de las establecidas en el Esquema Nacional de

Seguridad, para garantizar la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de sus datos personales.

12. Desarrollo de la Política de Seguridad de la Información

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad.

La revisión de la presente Política corresponde al Comité de Seguridad, proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del Consejo de Administración.

13. Terceras Partes

Cuando SEGIPSA realice encargos según lo dispuesto en la Disposición Adicional Décima de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. SEGIPSA definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de actuaciones que se lleven a cabo en materia de Seguridad en relación con otros organismos.

Cuando SEGIPSA utilice suministros o servicios de terceros, o ceda información a terceros, les hará partícipe de esta Política de Seguridad de la Información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la misma, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, siempre que se garantice el cumplimiento de las obligaciones y medidas de seguridad exigidas por SEGIPSA. Así mismo, se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Las terceras partes deberán garantizar que su personal esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

14. Cuadro de firmas

Este apartado, así como el resto de metadatos identificables presentes en el documento original, se retira en virtud de lo establecido en la medida de seguridad <<Limpieza de documentos [mp.info.5]>>, incluidas en el Anexo II, Medidas de Seguridad, del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.