1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Dirección de SOGESEL**.** Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hora hasta que sea reemplazada por una nueva versión.

2. INTRODUCCIÓN

SOGESEL depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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 a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuidad de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los 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 implican que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

SOGESEL debe 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 las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en las condiciones de contratación para para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

SOGESEL debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del Real Decreto 311/2022, de 4 de mayo, por el que se regula el Esquema Nacional de Seguridad en adelante (ENS)

3. ALCANCE

Sistema de la información que da soporte a las actividades de:

- Tratamiento y gestión de residuos
- Mantenimiento y gestión de zonas verdes
- Gestión integral del ciclo del agua, Sistemas inteligentes de gestión del agua
- Limpieza viaria y de interiores
- Mantenimiento integral de infraestructuras
- Movilidad, gestión del aparcamiento
- Mantenimiento de instalaciones y eficiencia energética
- Regulación de estacionamiento en la vía pública.

4. MISIÓN

La misión de SOGESEL es prestar servicios integrales a entidades públicas y privadas en los ámbitos del medioambiente, las infraestructuras y la gestión urbana, garantizando soluciones

eficientes, innovadoras y sostenibles, basadas en la calidad, la mejora continua y la confianza de sus clientes.

En el marco de la seguridad de la información, SOGESEL orienta su actividad a proteger la información y los sistemas que soportan sus servicios, asegurando su confidencialidad, integridad y disponibilidad, como elemento clave para ofrecer un servicio fiable y de calidad.

5. MARCO NORMATIVO

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 23/2006, de 7 de julio, 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.
- 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
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones. (Derogada parcialmente)
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de 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.
- 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 (NIS2).

6. PRINCIPIOS BÁSICOS

6.1. Alcance estratégico

La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.

6.2. Seguridad como proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

6.3. Gestión de la seguridad basada en riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

6.4. Prevención, detección, respuesta y conservación

6.4.1. Prevención

SOGESEL debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos. Estos controles, van a estar claramente definidos y documentados.
Para garantizar el cumplimiento de la política, los departamentos deben:

- 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.

6.4.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación 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 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

6.4.3. Respuesta

SOGESEL:

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

6.4.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, las distintas áreas de SOGESEL deben desarrollar, cuando sea necesario, planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio de actividades de recuperación.

6.4.5. Conservación

La información gestionada debe mantenerse accesible y utilizable durante el tiempo que sea necesario para cumplir con las obligaciones legales, administrativas o contractuales. Este principio garantiza que la información no se pierda ni se degrade, y que pueda ser recuperada en condiciones adecuadas de calidad, integridad y autenticidad.

Se debe asegurar la continuidad operativa y la trazabilidad de las actuaciones de la organización, permitiendo responder ante auditorías, reclamaciones o revisiones.

6.5. Existencia de líneas de defensa

El sistema de información dispondrá de una estrategia de protección constituida por diferentes capas, de forma que cuando una de las capas sea comprometida, permita desarrollar una acción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad del que el sistema sea comprometido en su conjunto, minimizando el impacto final sobre el mismo.
Existirán líneas de defensa constituidas tanto por medidas organizativas, físicas y lógicas.

6.6. Vigilancia continua y reevaluación periódica

SOGESEL llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.
La evaluación permanente del estado de la seguridad de los activos permite a SOGESEL medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
SOGESEL reevaluará y actualizará periódicamente las medidas de seguridad, 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.

6.1. Seguridad por defecto y desde el diseño

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

6.2. Diferenciación de responsabilidades

SOGESEL tendrá en cuenta la diferenciación de responsabilidades en su sistema de información siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

7. Organización de la seguridad

La implantación de la Política de Seguridad en SOGESEL requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsables del Servicio

c) Responsables de la Información

d) Responsable de Seguridad de la Información

e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

7.1. Comité de seguridad de la información

La seguridad de la Información es una responsabilidad organizativa que es compartida con la Dirección. En consecuencia, la Dirección de SOGESEL promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vida definida y el palpable apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por el Responsable del Servicio, el Responsable de la Información, el Responsable de Seguridad de la Información y el Responsable del Sistema, y actuando el Responsable de Seguridad como Secretario.

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

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información;
    - Elaboración y actualización de planes de continuidad
    - Cumplimiento y difusión de las Políticas de Seguridad

7.2. Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

- Determina los niveles de seguridad de la información, efectuando las valoraciones del impacto que tendría un incidente que afectase a la seguridad de la información, así como posteriores modificaciones que fuesen necesarias.

7.3. Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.

- Determina los niveles de seguridad del servicio, efectuando las valoraciones del impacto que tendría un incidente que afectase este, así como posteriores modificaciones que fuesen necesarias.

7.4. Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos de la Dirección.

El Responsable de Seguridad será el Punto de Contacto (PoC) en materia de seguridad de la información y tendrá las siguientes funciones:

- La determinación de la categoría de seguridad del sistema, con base en las valoraciones de los Responsables de la Información y del Servicio.

- Formalizar y aprobar la Declaración de Aplicabilidad, que incluirá las medidas seleccionadas del Anexo II del ENS, incluyendo las medidas compensatorias o complementarias de vigilancia.

- Analizar los informes de Auditoria que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información.

- Aprobar explícitamente los cambios que impliquen un riesgo alto, con carácter previo a su implantación.

- Actuará como Punto o Persona de Contacto (POC), canalizando las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio con los destinatarios de los servicios.

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de SOGESEL.

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de SOGESEL y normativa de desarrollo.
- Supervisar (como responsable último) los incidentes de seguridad informática producidas en SOGESEL.
- Difundir en SOGESEL las normas y procedimientos contenidos en la Política de Seguridad de la Información de SOGESEL y normativa de desarrollo, así como las funciones y obligaciones de toda SOGESEL en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de SOGESEL.

7.5. Responsable del Sistema

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad de SOGESEL, de acuerdo a los objetivos estratégicos de SOGESEL.

Las funciones del Responsable del Sistema de la Información son las siguientes:

- 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.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de SOGESEL, conforme a la estrategia de seguridad definida.
- Adoptar las medidas correctoras adecuadas derivadas de los informes de Auditoría. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.
- Garantizar la actualización del inventario de activos de Sistemas de Información de SOGESEL.
- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.

- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en SOGESEL.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

7.6. Procedimientos de designación

Mediante un acta formal se designan las siguientes responsabilidades:

- **Responsable del Servicio**
- **Responsable de la Información**
- **Responsable de Seguridad**
- **Responsable del Sistema**

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad.

7.7. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad, elevándose para su resolución a la Dirección en caso de no llegar a un acuerdo.
En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

8. Revisión de la política de seguridad de la información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

9. Datos de carácter personal

SOGESEL trata datos de carácter personal.

Todos los sistemas de información de SOGESEL se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado **5. Marco Normativo**, de la presente Política de Seguridad de la Información.

10. Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada

- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad, de acuerdo al marco organizativo definido en el **apartado 7 de esta Política.**
- Análisis y gestión de los riesgos, de acuerdo a lo previsto en el procedimiento **PS02 Planificacion.**
- Gestión de personal, de acuerdo a lo previsto en el procedimiento **PS09 Gestion de personal.**
- Profesionalidad, de acuerdo a lo previsto en el procedimiento **PS09 Gestion de personal.**
- Autorización y control de los accesos, de acuerdo a lo previsto en el procedimiento **PS03 Control de acceso.**
- Protección de las instalaciones, de acuerdo a lo previsto en el procedimiento **PS08 Proteccion de instalaciones**
- Adquisición de productos, de acuerdo a lo previsto en el procedimiento **PS02 Planificacion**.
- Mínimo privilegio, de acuerdo a lo previsto en el procedimiento **PS03 Control de acceso y PS04 Explotacion.**
- Integridad y actualización del sistema, de acuerdo a lo previsto en el procedimiento **PS10 Protección de equipos.**
- Protección de la información almacenada y en tránsito, de acuerdo a lo previsto en el procedimiento **PS14 Protección de la información**
- Prevención ante otros sistemas de información interconectados, de acuerdo a lo previsto en el procedimiento **PS11 Proteccion de comunicaciones.**
- Registro de actividad, de acuerdo a lo previsto en el procedimiento **PS04 Explotacion.**
- Incidentes de seguridad, de acuerdo a lo previsto en el procedimiento **PS04 Explotacion**.
- Continuidad de la actividad, de acuerdo a lo previsto en el procedimiento **PS06**

Continuidad del servicio.

- Mejora continua del proceso de seguridad, de acuerdo a lo previsto en el procedimiento **PS06 Continuidad del servicio.**

12. Estructuración de la documentación

Las directrices para la estructuración, gestión y acceso a la documentación de seguridad del sistema de Gestión Seguridad de la Información de SOGESEL, se definen en el procedimiento "**PS00 Gestión del sistema**".
Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por la Dirección de SOGESEL a propuesta del Comité de Seguridad.

- Segundo nivel: la normativa de seguridad de la información aprobada por la Dirección de SOGESEL. En ella se establecerán unas normas de uso aceptable de los sistemas de información.

- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad.

- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Estos documentos han de ser aprobados por el Comité de Seguridad.

Los documentos que integran el SGSI se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

13. Calificación de la información

Para calificar la información SOGESEL atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.
Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **PS14 Proteccion de informacion**

14. Obligaciones del personal

Todos los miembros de SOGESEL tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de SOGESEL recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de SOGESEL, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

15. Terceras partes, prestadores de servicios y proveedores de soluciones

Cuando SOGESEL preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando SOGESEL utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

Dichas terceras partes quedarán sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que SOGESEL pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Responsable de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y

del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Responsable de Protección de Datos emitir su parecer.

16. Gestión de incidentes de seguridad

SOGESEL dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

17. Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

Fecha: 28/05/2026	
Firma Dirección: **Javier Nuevo García**