SOCIEDAD ESTATAL DE PROMOCIÓN INDUSTRIAL Y DESARROLLO EMPRESARIAL, E.P.E.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad de la Información
Esquema Nacional de Seguridad

Código: 2018.001.SPD.PRE.NOR
Versión: 1.4
Fecha: 11/04/2025
Nivel: PÚBLICO

Revisión y aprobación

Elaboración	Revisión	Aprobación
Cristina Coto del Valle Para Comité de Seguridad	Cristina Coto del Valle Para Comité de Dirección	Cristina Coto del Valle Para Consejo Rector
Comité de Seguridad a celebrar el 11 de abril de 2025	Comité de Dirección a celebrar el 14 de abril de 2025	Consejo rector a celebrar el 29 de abril de 2025

Control de versiones

Versión	Fecha	Páginas	Descripción
1.4	11/04/2025	4-7, 11, 12, 14	Actualización de la denominación de la empresa, composición del Comité de Seguridad y de la misión y marco normativo
1.3	14/10/2022	todas	Adecuación al RD311/2022 del ENS
1.2	11/01/2021	4, 6, 11, 15	Recodificación del documento y actualización de la composición y frecuencia del Comité de Seguridad, procedimiento designación e incluido art. 26 mejora continua del proceso de seguridad. Derogado documento ENS.NOR.001
1.1	24/01/2019	4, 6, 11, 15	Modificación composición Comité de Seguridad e inclusión nueva legislación aplicable
1.0	01/10/2018	todas	Versión Inicial

Propiedad del documento

Tabla de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR

La Política de Seguridad debe ser aprobada por el Consejo Rector de la Sociedad Estatal de Promoción Industrial y Desarrollo Empresarial Entidad Pública Empresarial (en adelante "**SEPIDES**").

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

2. INTRODUCCIÓN

SEPIDES 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 o los servicios prestados.

Dicha información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad ("**ENS**"), persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Por tanto, para SEPIDES, el objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes lo antes posible, de acuerdo con lo establecido en el Artículo 8 del ENS.

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 los departamentos 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 servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades y Direcciones que componen SEPIDES, son conscientes de que la seguridad de la información 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. En ese sentido, la organización identificará e incluirá los requisitos de seguridad y las necesidades de financiación, en las fases de planificación, solicitud de oferta y pliegos de licitación de los proyectos de Tecnologías de la Información y Comunicaciones.

3. ALCANCE

Esta Política aplica a todo personal propio o de terceros colaboradores de SEPIDES y a todos los sistemas de información que soportan los servicios, así como los procesos que son necesarios para desarrollar y cumplir con los objetivos de negocio.

Esta Política será de difusión a toda la organización que tenga acceso a la información de SEPIDES y que tienen la obligación de conocer y cumplir con esta "***Política de Seguridad de la Información***" y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

4. MISIÓN DE SEPIDES

SEPIDES es una Entidad Pública Empresarial ("**SEPIDES E.P.E.**") () y está adscrita a la entidad pública Sociedad Estatal de Participaciones Industriales (en adelante, "**SEPI"**) conforme a lo dispuesto en el artículo 10.4 de la Ley 5/1996, de 10 de enero, de creación de determinadas entidades de derecho público, ejerciendo SEPI las funciones previstas en la citada ley. Sin perjuicio de las funciones que la Ley 5/1996, de 10 de enero, atribuye a SEPI, corresponderá al Ministerio de Industria y Turismo la tutela funcional de SEPIDES E.P.E. respecto a los fines de política industrial previstos en el artículo 6 de los Estatutos de SEPIDES E.P.E. , conforme a lo dispuesto por el Real Decreto 1247/2024, de 10 de diciembre, por el que se aprueba la transformación de la sociedad mercantil estatal SEPI Desarrollo Empresarial S.A. S.M.E. en la Sociedad Estatal de Promoción Industrial y Desarrollo Empresarial Entidad Pública Empresarial, y se aprueba su Estatuto (en adelante, "**Real Decreto"**)

Constituyen los fines de SEPIDES E.P.E.:

a) En el marco de la política industrial, la ejecución de las directrices y actuaciones que determine el Ministerio de Industria y Turismo, a través de la Secretaría de Estado de Industria, pudiendo a tal efecto desarrollar actuaciones de promoción industrial, económica, de la innovación y del diseño en relación con la industria, así como con el emprendimiento y las pequeñas y medianas empresas.

b) La canalización de los fondos nacionales y europeos hacia sectores industriales clave, el emprendimiento y las pequeñas y medianas empresas. A tal fin, también podrá movilizar fondos privados hacia proyectos innovadores, de fomento de la utilización de nueva tecnología relacionada con la digitalización o la sostenibilidad y de promoción económica que supongan una transformación de las cadenas de valor.

c) La gestión de fondos de titularidad pública carentes de personalidad jurídica que le sean encomendados.

El artículo 7 del Real Decreto detalla las funciones y competencias de SEPIDES E.P.E.

La misión de SEPIDES es poner a disposición de nuestros clientes soluciones inmobiliarias y financieras adaptadas a sus necesidades mediante equipos altamente especializados y comprometidos con la sostenibilidad, la innovación y el respeto al medioambiente.

Para el desarrollo y dinamización de la actividad empresarial, su actuación se concreta mediante actuaciones en tres áreas específicas:

- **Área Inmobiliaria**: la promoción, construcción, gestión, explotación y comercialización de terrenos para la ubicación en los mismos de proyectos industriales, comerciales o de servicios, así como su urbanización, acondicionamiento, planeamiento, parcelación y reparcelación.
- **Área Empresarial**: la promoción y desarrollo de estudios y proyectos industriales, comerciales y de servicios orientados a la creación de nuevas empresas, ampliación o reestructuración de unidades de negocio o de empresas ya existentes, generación de empleo y capacitación profesional de trabajadores por cuenta propia o ajena, pudiendo incluso, en su caso, para tales fines participar en el Capital Social de sociedades de nueva creación o ya existentes que ejecuten proyectos empresariales, garantizar sus operaciones y otorgar préstamos así como otras formas de financiación. Gestionar fondos públicos que a tal efecto se le encomienden.
- **Área de Programas Estratégicos Industriales**: la concesión de subvenciones, préstamos, avales, garantías o cualesquiera instrumentos de financiación o de ayuda que se establezcan al servicio de sus fines de política industrial. La aprobación de la concesión de subvenciones podrán serlo en ejecución del Plan de Recuperación Transformación y Resilencia de conformidad con la Decisión de Ejecución del Consejo (CID), relativa a la aprobación de la evaluación del Plan de Recuperación y Resilencia de España de 22 de abril de 2024, tal como establece la Disposición Adicional Cuarta del Real Decreto.

SEPIDES, trabaja para ser un referente de entidad pública eficiente y competitiva, con capacidad para fomentar la inversión, la creación de empleo y el desarrollo de la pequeña y mediana empresa española. Apoyar las directrices del Gobierno en política económica y social, contribuyendo por todo el territorio nacional y de manera especial en las zonas más desfavorecidas, promoviendo la cohesión social y territorial de España.

5. MARCO NORMATIVO

SEPIDES respeta la legislación vigente y exige a los destinatarios igual cumplimiento escrupuloso de la normativa en vigor en cada momento. El marco normativo en que se desarrollan las actividades de SEPIDES está integrado por las siguientes normas principales:

- Ley 5/1996, de 19 de enero, de creación de determinadas entidades de derecho público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones Públicas y en el resto de las normas de derecho administrativo general y especial que le sean de aplicación.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 2/2011, de 4 de marzo, de Economía Sostenible.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Real Decreto Legislativo 1/2010, de 2 de julio, que aprueba el Texto Refundido de la Ley de Sociedades de Capital para el ámbito de las filiales.
- Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.
- Ley 12/2003, de 21 de mayo, de bloqueo de la financiación del terrorismo.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley Orgánica 5/2010 de Reforma del Código Penal.
- Ley 44/2002 de 22 de noviembre, de medidas de reforma del sistema financiero.
- Toda aquella normativa en vigor nacional, comunitario e internacional que regule el desarrollo de las actividades empresariales e inmobiliarias de la entidad.

Asimismo, SEPIDES tiene el firme compromiso de velar por el cumplimiento de la legislación y normativa vigente en materia de protección y seguridad de la información. En ese sentido, SEPIDES ha establecido como requerimiento de seguridad el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información y a los servicios. La legislación y requisitos aplicables serán identificados y organizados para su correcta gestión en un documento adicional a esta Política denominado "***Legislación y requisitos aplicables SGSI***".

La normativa principal dentro del ámbito de la seguridad de la información y de la protección de datos:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resoluciones que se aprueban diferentes Instrucciones Técnicas de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales (LOPDGDD).
- Reglamento (UE) 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 (Reglamento general de protección de datos).

El mantenimiento del marco normativo aplicable será responsabilidad del Comité de Seguridad de la Información, teniendo en cuenta lo establecido en la "Disposición adicional

segunda. Desarrollo del Esquema Nacional de Seguridad" del RD 311/2022 por el que se regula el Esquema Nacional de Seguridad.

Así mismo, el Comité también será responsable de identificar las guías de seguridad del Centro Criptológico Nacional (CCN), referenciadas en la mencionada disposición, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. CUMPLIMIENTO DE ARTÍCULOS

SEPIDES establece los siguientes principios básicos para dar cumplimiento a los artículos del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad.

- **Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20)**

  La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, técnicos, jurídicos y organizativos, relacionados con el sistema de información. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos.

  Los sistemas se diseñarán y configurarán de forma que garanticen el mínimo privilegio necesario para su correcto desempeño, del siguiente modo:

  - El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
  - Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
  - Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. 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 aplicarán las guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema.

- **Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)**

  Como parte esencial del proceso de seguridad, todos los sistemas están sujetos a un análisis de riesgos continuo y permanentemente actualizado, con la finalidad de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se realizará:

  - Al menos una vez al año.
  - Cuando cambien los servicios prestados y/o información manejada.

- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

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

El Responsable de la Seguridad de la Información (ENS) será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

SEPIDES dispondrá de un proceso de gestión del riesgo, el cual se realizará según lo dispuesto en los anexos I y II del Real Decreto 311/2022 y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

- **Vigilancia y reevaluación periódica (artículo 10) e integridad y actualización del sistema (Artículo 21)**

  Se ha implementado controles de vigilancia continua y evaluaciones permanentes de la seguridad, para conocer en todo momento el estado de seguridad de los sistemas en relación con 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. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

  Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

- **Gestión de personal (artículo 15) y profesionalidad (artículo 16)**

  Todo el personal de SEPIDES atenderá a una sesión de concienciación en materia de seguridad de la información al menos una vez al año con el objetivo de estar formado e informado de los deberes, obligaciones y responsabilidades en materia de seguridad. Se establecerá un programa de concienciación continua para atender a todos los miembros de SEPIDES, 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.

- **Incidentes de seguridad (artículo 25), prevención, detección. respuesta y conservación (artículo 8)**

Se dispone de procedimientos de gestión de incidentes de seguridad que disponen de 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. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, se implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis, respuesta, reporte y conservación necesarios para que lleguen a los responsables regularmente.

SEPIDES establecerá las siguientes medidas de reacción ante incidentes de seguridad:

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

Para garantizar la disponibilidad de los servicios, SEPIDES dispone de los medios y técnicas necesarias que permiten garantizar la recuperación y conservación de los servicios más críticos.

- **Existencia de Líneas de defensa (artículo 9) y prevención ante otros sistemas interconectados (artículo 23)**

  Se establece una estrategia de protección basada en múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

  - 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.

  Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

- **Diferenciación de responsabilidades (artículo 11) y organización e implantación del proceso de seguridad (artículo 13)**

  SEPIDES ha organizado su seguridad comprometiendo a todos los miembros de la corporación, mediante la designación de diferentes roles de la seguridad con responsabilidades claramente diferenciadas, mecanismos de coordinación y resolución de conflictos, tal y como se recoge en el apartado de "Organización de la Seguridad" de la presente Política. Así mismo, en el caso de servicios externalizados, la organización prestataria designará un punto o persona de contacto para la seguridad de la información tratada y el servicio prestado.

- **Autorización y control de los accesos (artículo 17)**

  Se dispone de mecanismos de control de acceso a los sistemas de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

- **Protección de las instalaciones (artículo 18)**

  Se dispone de 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 las áreas controladas.

- **Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 19)**

  SEPIDES tendrá en cuenta, para la adquisición de productos de seguridad o la contratación de servicios de seguridad de las Tecnologías de la Información y la Comunicación (TIC), aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. Así mismo, se tendrá en cuenta los aspectos establecidos por el Organismo de Certificación del Centro Criptológico Nacional en relación con la certificación de los productos/servicios de seguridad de las TIC.

- **Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26)**

  Se establece mecanismos para proteger la información almacenada o en tránsito especialmente cuando esta se encuentra en entornos inseguros (dispositivos portátiles o móviles, dispositivos periféricos, soportes de información, redes abiertas, etc.).

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

  También ha desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias. De igual modo, se han implementado mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

- **Registros de actividad y detección de código dañino (artículo 24)**

  Se ha habilitado 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. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del Real Decreto311/2022, 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.

  Adicionalmente, se analizará las comunicaciones entrantes o salientes, y únicamente para los fines de la seguridad e la información, con el fin de impedir

acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino.

- **Mejora continua del proceso de seguridad (artículo 27)**

  El Sistema de Seguridad de la Información (SGSI) implementado velará por la mejora continua del proceso integral de seguridad establecido, aplicando criterios y métodos de reconocido prestigio nacional o internacional para la gestión de las tecnologías de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD

SEPIDES aporta los recursos necesarios para garantizar la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los sistemas de información para el desarrollo normal de las actividades de los empleados y los servicios prestados a nuestros clientes. La estructura establecida para la organización de la seguridad se indica a continuación:

7.1. Comité de Seguridad de la Información

SEPIDES ha constituido un Comité de Seguridad de la Información, como órgano colegiado y está formado por los siguientes miembros:

- Presidente/a de SEPIDES.
- Secretario/a General, Dirección de Asesoría Jurídica y Secretario/a del Consejo.
- Director/a de Auditoría.
- Director/a Comercial del Negocio Inmobiliario, Comunicación y Relaciones Institucionales.
- Director/a de Financiación e Inversión Empresarial.
- Director/a Corporativo y de Estrategia.
- Director/a Técnico del Negocio Inmobiliario.
- Director/a de Sistemas de Información.
- Director/a de Programas Estratégicos Industriales.
- Responsable de la Seguridad de la Información (ENS).
- Responsable del Sistema (ENS).
- Delegado/a de Protección de Datos.

El Comité estará presidido por el Presidente de la compañía como responsable máximo de las actividades, procesos y servicios de la organización. Su composición deberá tener representadas a todas las áreas de negocio significativas. El Secretario/a del Comité será desempeñado por el responsable de la Secretaría General, Dirección de Asesoría Jurídica y Secretario/a del Consejo.

El Comité celebrará sus sesiones con una periodicidad anual, previa convocatoria y con una agenda de temas a tratar previamente definida y enviada a todos sus miembros. La periodicidad de reunión de este Comité podrá alterarse en el caso de darse las circunstancias que así lo justifiquen.

Con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Las principales funciones y responsabilidades asociadas a la seguridad de la información serán:

- Definir, coordinar y supervisar (en cuanto a su ejecución y gestión) los planes estratégicos de seguridad de la información, asesorando a la organización y resolviendo los conflictos de responsabilidad en dicha materia.
- Difundir y revisar el cumplimiento eficaz y eficiente de la política y normativa de seguridad de la información. Fomentar una cultura de seguridad en la organización, promoviendo la concienciación y formación continua de los empleados (internos y/o externos), proveyendo de los recursos necesarios.
- Evaluar la eficacia y eficiencia de los procesos de gestión de la seguridad de la información corporativa y cumplimiento normativo a través de métricas y/o cuadros de mando.
- Realizar el control y seguimiento de las acciones y tomas de decisión determinadas en anteriores Comités, así como analizar las posibles desviaciones.
- Promover y aprobar la mejora continua del Sistema de Gestión de Seguridad, encargándose de:
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración 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 para su aprobación en coordinación con la Presidencia de SEPIDES.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Promover la realización de las auditorías periódicas ENS y LOPD que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.
    - Revisar y refrendar (si es necesario) las decisiones adoptadas por el Grupo de Trabajo en cuanto a criterios, hitos, revisiones, alcances del Sistema de Gestión y/o documentaciones formales asociadas a la seguridad de la información.

- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.

7.2. Roles de Seguridad asociados al ENS

La seguridad de la información se conforma principalmente en tres figuras organizativas diferenciadas según recoge el Esquema Nacional de Seguridad. Las funciones y responsabilidades de cada una de estas figuras se recogen a continuación.

1. Responsable de la Información y de los Servicios

Desempeñados por los Directores responsables de un servicio en particular. Este rol tiene las siguientes funciones:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro de su ámbito funcional de responsabilidad y del marco establecido en el anexo I del Real Decreto 311/2022, previa propuesta al Responsable de la Seguridad de la Información (ENS), y/o Comité de Seguridad de la Información.
- Definir los distintos niveles de seguridad, participando activamente en el Análisis de Riesgos y realizando la valoración de los activos de su responsabilidad en las dimensiones de seguridad contempladas.
- Informar sobre los derechos de acceso al Servicio y a la Información.
- Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- Poner en comunicación del Responsable de la Seguridad de la Información (ENS), cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.

2. Responsable de la Seguridad de la Información (ENS)

Desempeñado por la Secretaria General, Dirección de Asesoría Jurídica y Secretario/a del Consejo. Este rol tiene las siguientes funciones:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover campañas de formación y concienciación en materia de seguridad de la información.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema (ENS) y/o Comité de Seguridad de la Información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias.
- Elaborar y mantener actualizada la documentación en materia de seguridad, gestionando las revisiones externas o internas del sistema.

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Coordinar y administrar el Sistema de Gestión, gestionando los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

3. Responsable del Sistema (ENS)

Desempeñado por el Director de Sistemas de Información. Este rol tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Garantizar que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Establecer la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Elaborar y mantener los procedimientos operativos e instrucciones técnicas necesarias.
- Participar en la determinación de la Categoría del Sistema, en colaboración con el Responsable de la Seguridad de la Información (ENS) y/o Comité de Seguridad de la Información.
- Colaborar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - Aprobar los cambios en la configuración vigente de los sistemas y asegurar que los controles de seguridad establecidos sean cumplidos.
    - 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.
    - Garantizar la aplicación de los procedimientos aprobados.
    - Gestionar las autorizaciones de los privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

7.3. Delegado/a de Protección de Datos

El Delegado/a de Protección de Datos (DPD) tiene como funciones principales las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos, 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 que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del Reglamento
- 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 del Reglamento, y realizar consultas, en su caso, sobre cualquier otro asunto.

7.4. Procedimiento de Designación y Renovación

SEPIDES, a través de su Comité de Dirección, procederá a la designación y renovación de los roles o perfiles de seguridad y a la constitución del Comité de Seguridad de la Información. Todos los nombramientos se revisarán cada cuatro años o cuando el puesto quede vacante.

8. DATOS DE CARÁCTER PERSONAL

SEPIDES realiza el tratamiento de los datos de carácter personal, para lo cual dispone de un Manual de Tratamiento de Datos Personales conforme al Reglamento (UE) 2016/679. Este Protocolo, incluido el análisis de riesgo del tratamiento de datos personales, recoge todos los elementos iniciales requeridos para dar cumplimiento a la normativa de protección de datos, definiendo y estableciendo aspectos esenciales, para mantener la diligencia debida del responsable.

A todos los efectos este documento da cumplimiento 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. En adelante, Reglamento o Reglamento General de Protección de Datos o RGPD. Así mismo, también da cumplimiento a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales (LOPDGDD).

Todos los sistemas de información de SEPIDES se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Manual. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de SEPIDES 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este SGSI se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad. Así mismo, el SGSI estará documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Todos los documentos que conformarán el SGSI estarán accesibles para todos los empleados de la organización, tanto propios como externos, en la medida que sea necesario basándose en su "necesidad de conocer" para el correcto desempeño de sus funciones en la empresa.

El SGSI, de manera total o parcial, se someterá periódicamente a auditorías internas y externas con la finalidad de verificar su correcto funcionamiento, determinando grados de cumplimiento y recomendando medidas correctoras para una mejora continua.

Corresponde al Comité de Seguridad de la Información la revisión de esta Política con periodicidad anual o siempre que se produzcan cambios significativos, a fin de mantener su idoneidad, adecuación y eficacia. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad como a la adecuación a los cambios organizativos, legales y de infraestructura tecnológica.

Esta Política será aprobada por el Consejo Rector y difundida para que la conozcan todas las partes afectadas.

11. TERCERAS PARTES

Cuando SEPIDES preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad

de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SEPIDES 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. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de la Seguridad de la Información (ENS) 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 de seguir adelante.