GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Sociedad Española para la Transformación Tecnológica

Política de Seguridad de la Información de la Sociedad Española de Transformación Tecnológica, E.P.E. (SETT)

DICIEMBRE 2025

Ficha del Documento

AUTOR	**Responsable de Seguridad de la Información**
ÁREA	Seguridad de la Información
PROYECTO	SGSI / Adecuación al ENS
NOMBRE DOCUMENTO	Política de Seguridad de la Información SETT
REVISADO POR	Comité de Seguridad de la Información SETT
APROBADO POR	Dirección General de la SETT

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
1.0	Oficina de Seguridad de la Información	Abril 2025	Política de Seguridad de la Información
1.1	Oficina de Seguridad de la Información	30/07/2025	Modificaciones sugeridas por el Abogado del Estado en el Informe EREGES DIG 378/2025
1.2	Oficina de Seguridad de la Información	23/09/2025	Modificaciones sugeridas por el Abogado del Estado en el Informe 434/2025 EREGES DIG. Ampliación del epígrafe 8. ESTRUCTURA ORGANIZATIVA
1.3	Responsable de Seguridad de la Información	15/12/2025	Modificación supresión OSI

Firmas

Revisado:	**Aprobado por:**
Comité de Seguridad de la Información	**Comité de Dirección / Dirección General**
Fecha Sesión: 19/01/2026	Fecha Sesión: 19/01/2026
Firmado por:	Firmado por:

Índice:

1. OBJETO / MISIÓN

1.1 Objeto

La Sociedad Española de Transformación Tecnológica (en adelante, SETT) depende de los sistemas de Tecnologías de la Información y las Telecomunicaciones (en adelante, TIC) para alcanzar sus objetivos.

El uso de estos sistemas exige el establecimiento de un conjunto de actividades y procedimientos para el tratamiento y la gestión de los riesgos asociados a la seguridad de la información. La gestión de la seguridad de los sistemas de información es un proceso complejo que incluye a todas las personas de la organización, sus tecnologías y las normas y procedimientos establecidos.

La aprobación y publicación de esta política manifiesta el interés y compromiso de la SETT en cumplir con los requisitos aplicables y de mejora continua en la gestión de la seguridad de la información y en la prestación de sus servicios. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad, trazabilidad y autenticidad de la información tratada, o a la continuidad de los servicios prestados.

Este instrumento normativo, además viene a cumplir y ejecutar el art. 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS, o RD 311/2022), que define la presente política, así como el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta, y recoge los requisitos mínimos que debe tener.

Para la SETT, el objetivo de la seguridad de la información es también garantizar la calidad de la información y la prestación adecuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el ENS, para lo que establecerán las medidas técnicas, organizativas y de control necesarias que garanticen la consecución de estos objetivos.

Por tanto, el presente documento tiene por objeto establecer las directrices y principios que regirán el modo en que la SETT gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (en

adelante, SGSI) aplicando los requisitos legales y de sus partes interesadas, dentro del marco regulatorio legal y vigente y de los requisitos del Real Decreto 311/2022, de 3 de mayo, siendo su aplicación en el ámbito de la administración electrónica del sector público, que exige el establecimiento de los principios básicos y requisitos mínimos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información y los servicios.

1.2 Misión

La SETT, como Entidad Pública Empresarial, es un organismo público de los regulados en el artículo 103 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, Ley 40/2015 o LRJSP).

La SETT tiene personalidad jurídica pública diferenciada y plena capacidad jurídica y de obrar para el cumplimiento de sus fines, dispone de patrimonio y tesorería propios y autonomía de gestión y funcional dentro de los límites establecidos por la Ley 40/2015.

Así mismo, está adscrita al Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, el cual ejercerá la dirección estratégica, la evaluación de los resultados de su actividad y el control de eficacia.

El objetivo de la SETT es consolidarse como entidad de referencia para el fomento de la Transformación Tecnológica en España, para ello sus funciones, reflejadas en su estatuto son:

Impulsar y ejecutar la financiación y la inversión en sectores estratégicos vinculados a la transformación digital, las telecomunicaciones, la microelectrónica, los semiconductores, las nuevas tecnologías digitales o el sector audiovisual.

En particular:

- Apoyar a través de préstamos y/o subvenciones a empresas y entidades existentes, que promuevan o financien desarrollos en el ámbito de la transformación digital, las telecomunicaciones o el sector audiovisual e invertir directamente o a través de vehículos de inversión en pymes, empresas emergentes y de capitalización media en estos ámbitos de actuación y en este último caso la inversión habrá de ser temporal, salvo casos excepcionales en los que el carácter indefinido de la inversión quede justificado.

- Apoyar e invertir directamente o a través de vehículos de inversión en empresas y entidades de nueva creación destinadas al desarrollo de infraestructuras y capacidades digitales, en infraestructuras de investigación y líneas piloto asociadas a tecnologías digitales críticas y de la cadena de valor de la microelectrónica, los semiconductores y sus tecnologías vinculadas.
- Elaborar estudios, e informes, adquirir prototipos y desarrollar actividades de asistencia técnica, asesoramiento, formación y capacitación en todo lo relativo a la transformación digital, las telecomunicaciones, el sector audiovisual, la microelectrónica y/o semiconductores y sus tecnologías vinculadas.

De forma estrechamente relacionada con el cumplimiento de esta misión, la SETT es consciente de la necesidad de disponer y mantener una infraestructura TIC que prime y fomente servicios ciberseguros y de calidad para la consecución de sus objetivos estratégicos.

2. ALCANCE

2.1 Alcance subjetivo

Los sujetos obligados por esta Política son todo el personal de la SETT y todas aquellas personas, instituciones, entidades o unidades y servicios, sean internos o externos, que presten servicios a la Sociedad, sea en las instalaciones propias de la SETT o en remoto y que requieran para su prestación el soporte de servicios TIC.

2.2 Alcance objetivo

El alcance objetivo de esta Política comprende todos los sistemas de información de la SETT que den soporte a sus servicios y procesos, y afecta a todos los activos de información sustentados en ellos, así como a las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

Para ello, se toma en cuenta el contexto de la Entidad, en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, así como las interfaces y dependencias entre las actividades realizadas por la entidad y las que se llevan a cabo por otras organizaciones

en el cumplimiento de su misión como organismo público dentro del marco de las funciones encomendadas por la Secretaría de Estado de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio para la Transformación Digital y la Función Pública, además del cumplimiento de los requisitos establecidos en el Real Decreto 311/2022, de 3 de mayo.

La SETT ha establecido el alcance de su Sistema de Gestión de la Seguridad de la Información y por extensión de la implantación del Esquema Nacional de Seguridad en la prestación de los siguientes servicios, en la información que se maneja y en los sistemas de información que los soportan:

- Servicios de la Sede Electrónica.
- Gestión de Adquisiciones y Compras.
- Gestión del Personal.
- Gestión de Programas y Proyectos, así como el seguimiento de los mismos.

El detalle del Alcance se describe en la Documentación / Normativa del SGSI sobre la determinación del Alcance del Sistema de Gestión de la Seguridad de la Información de la Entidad y en la documentación desarrollada en el proceso de adecuación al Esquema Nacional de Seguridad.

Los objetivos en materia de seguridad que la pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de la respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea

transmita a través de redes de comunicaciones sea adecuadamente protegida.

- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

3. TÉRMINOS Y DEFINICIONES

- **Sistema de Gestión de la Seguridad de la Información o SGSI:** Es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Esquema Nacional de Seguridad o ENS**: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Parte interesada: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.
- **Autenticidad**: Propiedad de que una persona y o empresa que ha accedido y utilizado la información es lo que afirma ser.

- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser reveladas a personas y o empresas no autorizadas.
- **Integridad**: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a una persona y o empresa.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable en el momento que se requiera por la persona y o empresa autorizada.
- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, ...) que tenga valor para la organización.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Tratamiento de riesgos**: Proceso de modificar el riesgo, mediante la implementación de controles.
- **Datos personales**: Cualquier información relacionada con una persona que permita identificarla o pueda servir para identificarla.
- **Política de Seguridad** y Política de Seguridad de la Información se utilizará como términos equivalentes, excepto en aquellos lugares en donde se manifieste explícitamente alguna diferencia.

4. MARCO LEGAL Y NORMATIVO

El marco legal y normativo, sin carácter exhaustivo, en el que se desarrollan las actividades de la SETT, y, en particular, la prestación de sus servicios electrónicos a los usuarios está integrado por las siguientes leyes y normas:

4.1 Legislación

El marco legislativo de la SETT está basado en normas españolas y europeas relacionadas con la ciberseguridad y la protección de datos:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.
- Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G (ENS5G).
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley de Presupuestos Generales del Estado en vigor en cada momento.
- Real Decreto-ley 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información.
- 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 (RGPD).
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 36/2015, de 28 de septiembre de Seguridad Nacional.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 47/2003, de 26 de noviembre, General Presupuestaria.
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico (en adelante, LSSI).
- Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad.
- Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento general de la Ley de Contratos de las Administraciones Públicas.
- Ley 19/1988, de 12 de julio, de auditoría de Cuentas y Real Decreto 1156/2005, de 30 de septiembre, por el que se modifica el Reglamento que desarrolla la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas, aprobado por el Real Decreto 1636/1990, de 20 de diciembre.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de

26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales y Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la prevención de riesgos laborales.
- Real Decreto 676/2024, de 16 de julio, por el que se regulan las condiciones de la transformación de la Sociedad Estatal de Microelectrónica y Semiconductores, S.A., S.M.E., en la Entidad Pública Empresarial Sociedad Española para la Transformación Tecnológica, E.P.E., y se aprueba su estatuto.

Este listado no pretende incluir de forma exhaustiva en la Política una relación de normas jurídicas, sino definir el marco basado en normas españolas y europeas relacionadas con la ciberseguridad y la protección de datos. Para poder establecer este marco de forma específica, la SETT dispone de un procedimiento de identificación de la legislación aplicable y de actualización permanente de un registro donde se conservan referencias a dichas normas actualizadas.

4.2 Normativa

Estándares internacionales de referencia en la gestión de la seguridad de la información y los servicios TIC / Normativas ISO:

- UNE-EN ISO 9001:2015 Sistemas de Gestión de la Calidad.
- UNE-EN ISO/IEC 27001:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- UNE-EN ISO/IEC 27002:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información.
- UNE-ISO/IEC 20000-1:2018 Tecnologías de la información. Gestión de Servicios. Parte 1: Requisitos del Sistema de Gestión de Servicios (SGS).

Para aplicar los requisitos del propio Real Decreto 311/2022, de 3 de mayo, se deberán de conocer y utilizar las **Guías CCN-STIC** de Seguridad que lo desarrollan y que son las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de seguridad de las organizaciones, especialmente la Serie CCN-STIC-

800 que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS.

Para la protección de información de tipo datos personales se deberán de aplicar los requisitos establecidos en el RGPD / LOPDGDD y se aplicarán las guías e informes desarrollados por la Agencia Española de Protección de Datos (en adelante, AEPD).

5. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN

El Comité de Dirección de la SETT se comprometen a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la entidad que posibilita implementar y cumplir con los requisitos del Esquema Nacional de Seguridad, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del **Comité de Seguridad de la Información** que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de la SETT para la transformación tecnológica en España.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de la entidad.
- Asegurar que los recursos necesarios para la implantación de su SGSI y el cumplimiento del ENS estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
- Asegurar que el SGSI consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

El detalle de las funciones específicas del Comité de Seguridad de la Información se describe en la Documentación / Normativa del SGSI sobre la Organización de la Seguridad de la Información y el establecimiento de las Responsabilidades y Funciones necesarias.

6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, trazabilidad y autenticidad de la información y la disponibilidad de los servicios, así como la protección de los datos personales.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta los siguientes elementos:

- Lo que se va a hacer.
- Los recursos necesarios.
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

El detalle de los objetivos de seguridad de la información y las líneas estratégicas en este campo se establecen en el Plan Director de Seguridad de la Entidad.

7. PRINCIPIOS RECTORES DE LA POLÍTICA: PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS.

El despliegue del SGSI y la adecuación al ENS de la SETT se iniciará a partir de la categorización de los sistemas de información de la Entidad dentro del alcance partiendo de la valoración de sus dimensiones de seguridad (Confidencialidad, Integridad, Trazabilidad y Autenticidad para la información y Disponibilidad para los servicios).

El Análisis de Riesgos de Seguridad de los Sistemas de Información (incluyendo los derivados del tratamiento de datos personales), permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios y oportunidades de mejora para el tratamiento del riesgo y llevarlo a un nivel aceptable, tomando en cuenta el Contexto de la Organización.

Para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, que recoge los principios básicos y requisitos mínimos, se implementan 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.

En función de la Categoría de los Sistemas de Información y de los resultados del Análisis de Riesgos realizado se aplicaran en mayor o menor grado los controles de seguridad del Anexo II del ENS que deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada (Declaración de Aplicabilidad) que deberá ser revisada y aprobada, según se establezca en el procedimiento de correspondiente relativo a la creación, actualización y control de la información documentada del SGSI de la Entidad.

La aplicación de estos controles permitirá reducir los riesgos, mantenerlos dentro de los niveles aceptados y aprobados por la Entidad y de este modo asegurar la seguridad de la información y los servicios.

La Política de Seguridad de la Información de la SETT articula la gestión continua de la seguridad.

Esta Política se ha establecido de acuerdo con los siguientes **principios básicos** señalados en el ENS como directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información y la prestación de los servicios:

- **Alcance estratégico:** La seguridad de la información cuenta con el compromiso y apoyo de todos los niveles directivos, de forma que estará coordinada e integrada con el resto de las iniciativas estratégicas de la Entidad para conformar un todo coherente y eficaz.
- **Responsabilidad determinada:** Se establecen los perfiles, funciones y responsabilidades señaladas en el ENS para la gestión de la seguridad de la información. Se concreta así el principio de Diferenciación de responsabilidades del artículo 11 del RD 311/2022. En aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.
- **Seguridad integral:** La seguridad es entendida 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 es considerada como parte de la operativa habitual, estando presente y aplicándose desde la concepción y el diseño inicial de los sistemas TIC.

  El artículo 9 del RD 311/2022 establece la importancia de implementar múltiples capas de seguridad, conocidas como el **principio de líneas de defensa**, para garantizar una mayor protección de la información, de manera que, si una capa falla, otras puedan actuar como respaldo y mitigar el impacto.
- **Gestión de riesgos:** La gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación será proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Vigilancia continua y reevaluación periódica:** La SETT implementa medios la detección y respuesta a actividades o comportamientos anómalos, además de otros que permitan una evaluación continuada del estado de seguridad de los activos. Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de

seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

- **Prevención, detección, respuesta y conservación** con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- **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.

Se desarrolla teniendo en cuenta la aplicación de los siguientes **requisitos mínimos** de seguridad:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos de seguridad de los sistemas de información (incluyendo los derivados del tratamiento de datos personales).
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Para dar cumplimiento a estos requisitos mínimos, se aplicarán las medidas de seguridad indicadas en el Anexo II del ENS, teniendo en cuenta:

- Los activos que constituyen los sistemas de información, su valoración y relaciones.
- La categoría de seguridad del sistema.
- Las decisiones que se adopten para gestionar los riesgos identificados.

Para aplicar los requisitos del Esquema Nacional de Seguridad, se deberán utilizar las Guías CCN-STIC de Seguridad que lo desarrollan y que son las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de seguridad de las organizaciones, especialmente la Serie CCN-STIC-800 que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS.

Para la protección de información de tipo datos personales se deberán de aplicar los requisitos establecidos en el RGPD / LOPDGDD y se aplicarán las guías e informes desarrollados por la AEPD.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de este modo, al cumplimiento de los requisitos del ENS y de las directrices establecidas en el SGSI de la Entidad.

La información documentada será clasificada según se establece en el procedimiento correspondiente del SGSI relativo a la clasificación, etiquetado, uso y protección de la información, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en dicho Procedimiento.

Se realizarán auditorías que revisen y verifiquen el cumplimiento por parte del SGSI de los requisitos del Real Decreto 311/2022 por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de estas, así como en la aplicación de las acciones correctivas que se deriven para la Mejora Continua del SGSI.

8. ESTRUCTURA ORGANIZATIVA DE LA SEGURIDAD DE LA INFORMACIÓN.

Para garantizar que se lleva a cabo de manera adecuada la protección de la información y que las responsabilidades para su ejecución sean asignadas

adecuadamente, la SETT establece una estructura organizativa, responsabilidades y funciones que permiten promover la aplicación consistente de la presente Política y una gestión eficaz de la Seguridad de la Información.

La estructura organizativa que articula la SETT diferencia niveles de responsabilidad de acuerdo con el principio básico de "diferenciación de responsabilidades" que recoge el ENS.

La SETT, en su proceso de adecuación al cumplimiento del Esquema Nacional de Seguridad crea sus órganos específicos para la estructurar la gestión de la seguridad, tanto de la información como de la protección de datos personales.

Para cumplir las medidas de seguridad del ENS, en los marcos organizativo, operacional y de protección, debe ser la organización, a través de uno o varios órganos quien dirija y oriente a la dirección la forma de conseguirlo.

Estos órganos se estructuran en 3 niveles: Gobierno, Ejecutivo/Supervisión y Operativo.

Se describe a continuación los órganos planteados en el caso de la SETT:

8.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES

8.1.1 Comité de Dirección

El Comité de Dirección deberá proponer a la Dirección General la designación de los integrantes del Comité de Seguridad de la Información. Asimismo, deberá facilitar los recursos adecuados para alcanzar los objetivos de seguridad y resolver los conflictos que se planteen y que no puedan ser resueltos por el Comité de Seguridad de la Información. El Comité de Dirección asume las funciones relacionadas con la organización y estrategia de la seguridad de la información.

Facilitará los recursos adecuados para alcanzar los objetivos estratégicos de seguridad definidos en la política, así como para la implementación y mantenimiento del SGSI.

8.1.2 Comité de Seguridad de la Información

Dentro de la estructura de Seguridad de la Información de la SETT, y como elemento de Gobierno, se constituye el Comité de Seguridad de la Información (en adelante, CSI) que coordina la seguridad de la información en la Entidad.

Se constituye como un órgano colegiado, algunos de cuyos miembros ostentan roles especializados dentro de la organización de la seguridad.

Es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio.

El Comité de Seguridad de la Información contará con los siguientes perfiles:

Perfiles a nivel de Gobierno:

- ✓ Responsable de la Dirección.
- ✓ Responsabilidad de Tratamiento de Datos (RGPD - LOPDGDD).
- ✓ Responsable de la Información / Responsable del Servicio.

Perfiles a nivel de Supervisión:

- ✓ Responsable de Seguridad: Ejerce las funciones de Secretaria/o del Comité de Seguridad de la Información.
- ✓ Delegado de Protección de Datos (RGPD - LOPDGDD). Deberá de ser invitado expresamente al Comité de Seguridad de la Información.

Adicionalmente, y por necesidades del Comité, podrán asistir a sus reuniones otros perfiles, a Nivel Operativo, como el Responsable del Sistema, expertos en seguridad de la propia Entidad o consultores externos incluidos en el perfil Administradores de Seguridad.

Composición en SETT:

- **Dirección General / Representante de la Dirección.**
  Perfil ENS: Responsable de la Dirección del Organismo; Responsable del Tratamiento de Datos Personales (en representación de la Entidad que es la responsable como persona jurídica del tratamiento de los datos personales).

- **Secretaría General.**
  Perfil ENS: Responsable de Seguridad; Secretaria del Comité de Seguridad de la Información.
- **Dirección de Desarrollo de Negocio.**
  Perfil ENS: Responsable de la Información; Responsable del Servicio.

El Comité de Seguridad de la Información reportará de ordinario al Comité de Dirección, así como al Consejo Rector cuando así se solicite.

Funciones:

a. Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.

b. Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.

c. Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.

d. Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

e. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

f. Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión e incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.

g. Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección (o por el órgano competente) y aprobar la Normativa de Seguridad de la información.

h. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad.

i. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

j. Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento el Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.

k. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información no es un comité técnico, y, podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento, realizando formación especializada en la materia. También podrá contar con Grupos de Trabajo especializados, internos, externos o mixtos.

Habitualmente, el Responsable de la Seguridad actuará como Secretario del Comité de Seguridad, con las siguientes funciones derivadas:

a. Convocar las reuniones del Comité de Seguridad de la Información, atendiendo a las instrucciones del presidente del Comité.

b. Preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables.

c. Elaborar el acta de las reuniones.

d. Remitir el acta de las reuniones a los asistentes, recabando su firma.

e. Conservar las actas, de acuerdo con los criterios de conservación documental de la entidad.

8.2 ROLES: FUNCIONES Y RESPONSABILIDADES EN LA SETT

8.2.1 Responsable de la Dirección

La responsabilidad de la actividad de una entidad del sector público se sitúa, en última instancia, en su Titular.

Mientras que las competencias o funciones de una entidad deben estar recogidas en su norma de creación o en las sucesivas normas de desarrollo de su estructura, el titular de la Entidad es responsable de fijar los objetivos estratégicos, organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas, y dirigir su actividad, incluyendo la aprobación de la Política de Seguridad de la Información del organismo, así como, en su caso, la Política de Protección de Datos, facilitando los recursos adecuados para alcanzar los objetivos propuestos, velando por su cumplimiento.

Así pues, la figura de la Dirección de la Entidad (personificada en su Titular) cobra una importancia capital, ya que de la Dirección depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.

8.2.2 Responsable de la Información

La información es la materia prima de la que se nutre la actividad de las entidades y puede tener su origen en la propia entidad, las personas que se relacionan con ellas y en terceras entidades (públicas o privadas).

El ENS asigna al Responsable de la Información, como principal función, la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información, pudiendo ser una persona física concreta o un órgano colegiado.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema6 y la del Delegado de Protección de Datos de acuerdo con las funciones de asesoramiento que le asigna el RGPD.

8.2.3 Responsable del Servicio

El ENS asigna al Responsable del Servicio -que puede ser una persona física o un órgano colegiado de la entidad-, la función principal de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema y del Delegado de Protección de Datos.

La determinación de los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

En la valoración de un servicio siempre se debe atender a los requisitos de seguridad de la información que maneja a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad.

8.2.4 Responsable de la Seguridad de la información

El Responsable de la Seguridad de la Información es la persona designada por la Dirección de la Entidad, según el procedimiento definido. Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Las funciones esenciales del Responsable de la Seguridad son:

a. Determinar las medidas de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.

b. Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio

c. Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.

d. Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.

e. Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.

f. Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.

g. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

h. En la gestión de los ciberincidentes, contando con los responsables de la entidad, de la información y de los servicios actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política.

Por otro lado, el Responsable de la Seguridad colaborará con el Delegado de Protección de Datos de la Entidad en la gestión de los incidentes que afecten a datos personales y, en su caso, a la notificación a las autoridades de control y a las personas afectadas.

El Responsable de la Seguridad debe estar situado en una posición que le permita tener un acceso directo a los niveles directivos de la organización teniendo en cuenta las peculiaridades organizativas de cada entidad pública o privada.

En el supuesto de externalizaciones de servicios, la entidad tercera debe disponer de un Punto de Contacto (POC), sin perjuicio de otras figuras que puedan requerirse por normativa sectorial especifica como la de protección de datos personales.
El POC, que puede ser el Responsable de la Seguridad o una persona de su área o departamento o con quien esté en comunicación, tiene entre sus principales funciones se encuentran:

a. Canalización de las comunicaciones en materia de seguridad e incidentes a la entidad que contrata el servicio.
b. Supervisión del cumplimiento de los requisitos de seguridad del servicio que presta o solución suministrada.
c. Gestión de incidentes de seguridad.

8.2.5 Responsable del Sistema

El Responsable del Sistema será designado por la Dirección de la Entidad. Tiene las siguientes funciones:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.

b. Adopción de las medidas correctoras derivadas de las auditorías de seguridad.

El Responsable del Sistema, en los sistemas de categoría Alta, puede suspender el tratamiento de una cierta información o la prestación de un determinado servicio si, en una auditoría, se aprecian deficiencias graves de seguridad. Tras la suspensión, será informada la dirección de la entidad, y los responsables de la información y los servicios afectados y el Responsable de la Seguridad, pudiendo solicitar la opinión del Delegado de Protección de Datos. En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos y si afecta a la tramitación administrativa, a los servicios jurídicos de la entidad para, en su caso, proceder a la suspensión de los plazos.

En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada organización podrá designar cuantos Responsables del Sistema Delegados considere necesarios. La propuesta de designación corresponde al Responsable del Sistema, que delega funciones, no responsabilidad.

Los Responsables del Sistema Delegados se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Es habitual que estas figuras se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.

Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.

8.2.6 Administrador de Seguridad

Atendiendo a la estructura organizativa de la entidad, la entidad podrá contar con un Administrador que, según las funciones que realice, puede depender del Responsable del Sistema o del Responsable de la Seguridad.

Las funciones más significativas del Administrador del Sistema serían las siguientes:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
c. La aplicación de los Procedimientos Operativos de Seguridad (POS).
d. Informar al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
e. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Son funciones del Administrador dependiente del Responsable de la Seguridad:

a. Comprobar que los controles de seguridad establecidos son adecuadamente observados.
b. Comprobar que son aplicados los procedimientos aprobados para manejar el sistema de información.
c. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
d. Comprobar 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.
e. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

f. Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
g. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Puede depender del Responsable del Sistema o del Responsable de la Seguridad (pero no de ambos).

En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal
adicional para llevar a cabo las funciones del Administrador, se podrán designar administradores delegados.

Los administradores delegados serán responsables, en su ámbito competencial, de aquellas acciones que delegue el Administrador relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

El administrador delegado será designado a solicitud del Administrador, del que dependerá funcionalmente.

8.2.7 Delegado de Protección de Datos

El **Delegado de Protección de Datos** tendrá como mínimo las siguientes funciones

a. 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 presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
b. Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.c. 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 RGPD.

d. Cooperar con la autoridad de control.

e. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos 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.

8.2.8 Responsable del Tratamiento

El **Responsable del Tratamiento** (art. 4 RGPD). «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Aprueba y supervisa las medidas técnicas y organizativas aplicadas a los tratamientos.

Se correspondería con el Responsable de la Dirección.

8.2.9 Encargado del Tratamiento

Encargado del Tratamiento (art. 4 RGPD). «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento aplicando las medidas de seguridad acordadas contractualmente y en la política de seguridad de la organización. Colaborará con el responsable del tratamiento y con el Delegado de Protección de Toaos en la gestión de incidencias.

Se correspondería con el Responsable del Proyecto en la empresa proveedora.

8.3 PROCEDIMIENTOS DE DESIGNACIÓN

El Comité de Dirección de la SETT designará:

- Los miembros del Comité de Seguridad.
- El Responsable de la Seguridad.

Asimismo, el Comité de Dirección de la SETT designará a propuesta del Comité de Seguridad:

- El Responsable de la Información.
- El Responsable del Servicio.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento.

Si por circunstancias internas o cambios de estructura internos no se encuentra disponible alguno de los miembros del CSI, asumirá sus funciones, de forma temporal, aquella otra persona que la Dirección General designe. Deberá constar su designación formal y aceptación, incluyendo las funciones temporalmente asignadas y el periodo máximo de ejercicio de estas funciones, sin incumplir el principio de diferenciación de responsabilidades.

Por tanto, es función de la Dirección de la Entidad, es decir, el Comité de Dirección de la SETT, designar los siguientes perfiles que, adicionalmente, forman parte de los diferentes órganos para la gestión de la seguridad de la información que se establecen en la Entidad:

- ✓ Al **Responsable de la Información,** que puede ser un cargo unipersonal o un órgano colegiado (integrado en el Comité de Seguridad de la Información).
- ✓ Al **Responsable del Servicio,** que puede ser el mismo que el Responsable de la Información, también puede ser un cargo unipersonal o un órgano colegiado (integrado en el Comité de Seguridad de la Información).
- ✓ Al **Responsable de la Seguridad,** que debe reportar directamente a la Dirección o a los órganos de gobierno de la Entidad y, cuando existan, a los Comités de Seguridad Corporativa y de Seguridad de la Información.
- ✓ A los **Responsables del Sistema,** que, en materia de seguridad, reportarán al Responsable de la Seguridad. Esta designación podrá ser:
  - A propuesta del Responsable de la Información tratada, cuando el Sistema de información trate una única información.
  - A propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.

- Directamente, cuando el sistema de información trate diferentes informaciones o preste diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.

✓ Al **Administrador de Seguridad,** a propuesta del Responsable del Sistema o del Responsable de Seguridad.

Se comunicará a la persona empleada el cargo asignado, sus deberes y responsabilidades sin perjuicio de otras que puedan corresponderle.

9. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa definida en la Entidad y reflejada en esta Política de Seguridad de la Información de la SETT, este conflicto será planteado y tratado en el Comité de Seguridad de la Información.

En caso de no alcanzarse un acuerdo deberá ser finalmente resuelto por el superior jerárquico de los mismos, teniendo en cuenta que, en caso de conflicto en aspectos relativos a la seguridad de la información y la protección de datos de carácter personal, debe prevalecer la decisión que implique el nivel más alto de protección.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La SETT ha diseñado un SGSI, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad y calidad.

El SGSI será documentado y permitirá generar evidencias de las salvaguardas y del cumplimiento de los requisitos del Esquema Nacional de Seguridad y de los objetivos marcados.

En dicho SGSI existe un procedimiento de gestión documental que establece las directrices para la estructuración de la documentación de seguridad, su gestión y acceso.

La pirámide documental del SGSI se estructura, a nivel documental, en los siguientes niveles relacionados jerárquicamente:

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se podrá estructurar como máximo en los siguientes niveles relacionados jerárquicamente:

- **Primer nivel normativo:** Política de Seguridad de la Información (en adelante, PSI) y directrices.

Está constituido por la PSI y las directrices fundamentales de seguridad aplicables a los órganos superiores o directivos de la SETT. Se aprobarán por el Comité de Seguridad la normativa de seguridad de la información, el marco normativo y las medidas técnicas a implementar de acuerdo con el Plan de Implantación de la Seguridad de las TIC en la organización.

- **Segundo nivel normativo**: Normativa y recomendaciones de seguridad.

Está constituido por la normativa y recomendaciones de seguridad que se definan en cada ámbito organizativo de aplicación específico. Este marco regulador TIC, comprende los procedimientos, las normas y las instrucciones técnicas de seguridad, es de obligado cumplimiento y se formalizará mediante instrucciones o resoluciones de los titulares de los órganos correspondientes, , mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

Estas normas de seguridad deberán cumplir los siguientes requisitos:

1.º Limitarse única y exclusivamente al ámbito específico de las competencias de los roles adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo.

2.º Cumplir estrictamente con lo indicado en el Esquema Nacional de Seguridad y con el primer nivel normativo.

- **Tercer nivel normativo: Procedimientos técnicos.**

Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en Instrucciones previas, que establecen las configuraciones mínimas de

seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo. La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel normativo las guías CCN-STIC elaboradas por el Centro Criptológico Nacional.

Este tercer nivel normativo deberá cumplir los siguientes requisitos:

1.º Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u comités adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo.

2.º Cumplir estrictamente con lo indicado en el Esquema Nacional de Seguridad y con el primer y segundo nivel normativos enunciados en el presente artículo.

Además, de la normativa enunciada en el presente epígrafe, la estructura normativa podrá disponer, a criterio de cada uno de los órganos u organismos adscritos a la presente PSI, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como: informes técnicos, registros, evidencias, buenas prácticas, etc.

El personal de la SETT y de terceras empresas que vayan a prestar sus servicios para ella tendrán la obligación de conocer y cumplir, además de la política de seguridad de la información, todas las normativas, procedimientos e instrucciones técnicas operativas de seguridad de la información que puedan afectar a sus funciones en el desempeño de su trabajo y/o prestación de los servicios; en particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones se desarrollarán las Instrucciones Técnicas Operativas pertinentes y necesarias para su operativa, y cuyo conocimiento, uso obligado y difusión limitada aplicará a estos equipos de trabajo.

La SETT establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI. Existirá un procedimiento de gestión documental, donde se etiquetará la información conforme a su confidencialidad, y se establecerá el nivel de difusión del mismo.

Este marco normativo estará a disposición de todos los miembros de la SETT.

11. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información de la Sociedad Española de Transformación Tecnológica será revisada juntamente con la revisión del Sistema de Gestión de la Seguridad de la Información (SGSI) conforme al cumplimiento del ENS que llevará a cabo la Dirección General de la Entidad, a través del Comité de Seguridad de la Información.

De manera general esta revisión tendrá lugar, como mínimo, una vez al año.

La Política de Seguridad de la información se revisará y actualizará siempre que se produzcan cambios significativos en la organización y estructura de la Entidad, en su organización y responsabilidades de Seguridad de la Información o en su SGSI.

Las revisiones, modificaciones y actualizaciones de la Política de Seguridad de la Información serán revisadas y válidas por el Comité de Seguridad de la Información previamente a su aprobación y firma por la Dirección General de la Entidad / Comité de Dirección.

12. APROBACIÓN, DIFUSIÓN Y APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información de la Sociedad Española de Transformación Tecnológica será aprobada por la Dirección General de la Entidad y por su Comité de Dirección, como órganos que ostenta las máximas competencias ejecutivas, mediante su firma y será publicada para ser de este modo difundida a las partes interesadas.

Así mismo, la Dirección General de la SETT dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el SGSI posibilitando así la adecuada implantación y el proceso de adecuación a los requisitos del ENS.

La Política de Seguridad de la Información, revisada, aprobada y firmada será comunicada a las partes interesadas, específicamente a los miembros de la

organización internos o externos, especialmente a las nuevas incorporaciones, mediante su publicación en los medios disponibles que se determine.

13. TRATAMIENTO DE DATOS PERSONALES

La SETT trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento (en adelante, RAT).

La SETT deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice la persona que ostente el cargo de Delegado/a de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales. La SETT solo recogerá datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan recabado.

La SETT adoptará las medidas de índole técnica y organizativas, necesarias para el cumplimiento de la legislación y normativa de protección de datos vigente en cada caso.

La gestión corporativa para el cumplimiento de la normativa de protección de datos corresponde a la Secretaría General de la SETT. La Política de Protección de Datos Personales está publicada en el portal web de la SETT

La SETT mantendrá actualizado el RAT con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del RGPD.

Cuando la información contenga datos de carácter personal, se llevará a cabo, de forma periódica y al menos cada 2 años, un análisis de riesgos que

permita identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleve a cabo la SETT, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

Asimismo, se llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del RGPD.

Se adoptarán las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse a través del procedimiento establecido al efecto, de conformidad con lo dispuesto en el artículo 33 del RGPD.

Igualmente, se adoptarán las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, conforme a lo dispuesto en el artículo 34 del RGPD.

14. GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política de Seguridad y que están dentro del alcance están sujetos a una gestión de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos la información y los datos personales, los servicios, los activos de soporte y dichos sistemas de información.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en su artículo 7.

El análisis de riesgos se repetirá regularmente:

- Al menos una vez al año. De acuerdo con el apartado 1.1 d) del Anexo III del ENS se revisará y aprobará anualmente.

- Cuando se produzcan modificaciones notables en la información, los servicios, el tratamiento de datos personales, los sistemas de información u otros activos de soporte.
- Cuando se produzcan incorporaciones de nuevos servicios, activos o sistemas de información al alcance.
- Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave (entendiéndose como tal lo especificado en el Anexo I del RD 311/2022).
- Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, (entendiéndose como tal lo especificado en el Anexo I del RD 311/2022).
- Cuando se contemplen riesgos derivados de la normativa de protección de datos, contando con el asesoramiento del Delegado/a de Protección de Datos.

Las fases del proceso de gestión de riesgos se realizarán 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 CCN.

En particular, para realizar el análisis de riesgos se utilizará la Metodología de Análisis y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica (en adelante, MAGERIT).

La descripción detallada de la metodología, resultados y documentación de la gestión de los Riesgos de Seguridad de la Información y Tratamiento de Datos Personales en la SETT se ha reflejado en la documentación específica para la Gestión de Riesgos del SGSI de la Entidad.

Con este proceso, se determina el compromiso la SETT con la seguridad de la información y, para ello, establece la obligación de los responsables de los sistemas de realizar análisis de riesgos, atendiendo a sus conclusiones y gestionar los riesgos por encima de umbral asumible acordado por la entidad.

15. TERCERAS PARTES

En el caso de que la SETT preste servicios a otros organismos o maneje información sensible de los mismos, se les hará partícipe de esta Política, se establecerán canales de comunicación y colaboración entre los respectivos

órganos de coordinación de la seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

En el caso de que la SETT utilice soluciones y/o servicios de terceros, o ceda información a terceros, se les hará partícipes de esta Política y de la Normativa de Seguridad de la Información relacionada aprobada y vigente y se suscribirán los acuerdos de confidencialidad necesarios con la empresa prestadora de los servicios y sus trabajadores.

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.

La entidad prestataria de los servicios externalizados designará un Punto o Persona de Contacto (en adelante, POC).

De igual modo, los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

En caso de que la información a la que accede la tercera parte incluya datos personales se cumplirá la legislación vigente en materia de Protección de Datos Personales (RGPD / LOPDGDD).

Si la prestación de servicios por parte de proveedores externos implica el acceso a datos personales durante la prestación de esos servicios, de los que la SETT sea Responsable de Tratamiento se establecerán los correspondientes Acuerdos de Encargo de Tratamiento adicionales a los acuerdos de Confidencialidad.

16. MEJORA CONTINUA, AUDITORIA, CERTIFICACIÓN.

16.1 MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización.

Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo de situaciones en las que es necesaria una mejora continua de los sistemas.

Por ello, es necesario para la SETT implantar un proceso de mejora continua dentro de su SGSI, proceso permanente que comportará, entre otras acciones:

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realizar planes de acciones que corrijan los nuevos riesgos detectados.
- Realización de auditorías internas o, cuando proceda, externas.
- Implantación de Planes de Acciones Correctivas que soluciones la No-Conformidades y Observaciones detectadas en las auditorías.
- Revisión de las medidas de seguridad.
- Revisión y actualización de las normas y procedimientos.
- Establecer un sistema de Métricas de seguimiento y control que permitan detectar desviaciones y planificar acciones para corregir esas desviaciones.

Para la SETT, la gestión adecuada de la ciberseguridad constituye un reto continuo y colectivo al que necesariamente se ha de enfrentar y es necesario afrontar su mejora de manera continua.

16.2 AUDITORIA

Además de la realización de estas acciones de forma constante, se deberá implantar un proceso de auditoría de dichas actividades al menos una vez al año o cuando existan cambios significativos en el SGSI, tal y como se indica en el artículo 31 del Real Decreto 311/2022 que se refiere a la "Auditoría de la seguridad" dentro del contexto del Esquema Nacional de Seguridad. Este artículo establece la obligación de realizar auditorías regulares a los sistemas de información comprendidos en el ámbito de aplicación del mismo, con el

objetivo de verificar el cumplimiento de los requisitos y medidas de seguridad establecidas.

16.3 CERTIFICACIÓN

A tal efecto, cuando los servicios e información de la SETT se hayan definido de categoría MEDIA o ALTA, precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir, asimismo, para los fines de la certificación.

17. OBLIGACIONES DEL PERSONAL

Todos los miembros del personal tanto interno como externo que desarrollan su labor profesional para la SETT tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolla, siendo responsabilidad del Comité de Seguridad de la Información de la Entidad disponer los medios necesarios para que la información llegue a los implicados.

Todos los miembros de la Entidad atenderán a las sesiones de concienciación en materia de seguridad TIC con la periodicidad que se determine. Se establecerá para ello un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación técnica específica 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.

Para ello la SETT garantizará la definición y la ejecución de las acciones necesarias para concienciar y fomentar el cumplimiento de las obligaciones por parte del personal con relación a los riesgos y las amenazas relativos a la seguridad de la información.

La gestión y preservación de la seguridad de la información y el cumplimiento de los objetivos citados en esta Política deben ser el fin común de todas las personas que presten servicio directa o indirectamente en la organización, de tal manera que son responsables del uso correcto de los activos de

tecnologías de la información y de las comunicaciones puestos a su disposición.

De igual modo todo el personal, interno o externo, de la SETT tiene la responsabilidad de participar en la gestión preventiva de la seguridad de la información, así como en la detección temprana y comunicación de incidentes de seguridad a través de los medios que la organización habilite para ello.

El incumplimiento de esta Política de Seguridad de la Información y de la Normativa de Seguridad que la desarrolla podrá suponer el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales que correspondan.

Los usuarios de la SETT serán responsables de aquella información que manejen y/o a la que accedan, en función de los permisos que les sean asignados dentro de la gestión de permisos y control de accesos de la organización, en el desarrollo de sus actividades profesionales. Dicha información tendrá asignados los niveles de seguridad requeridos en función de los procedimientos definidos en el SGSI e implantados en la organización a tal efecto.

18. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información entrará en vigor el día de su aprobación por la Dirección General de la SETT y su Comité de Dirección.

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