Política de Seguridad de la Información

1. Aprobación y Entrada en Vigor

La presente Política de Seguridad de la Información ha sido aprobada por el Comité de seguridad de Esment, adquiriendo plena vigencia a partir de la fecha de su aprobación: 20 de Marzo de 2026 .

La responsabilidad de su revisión y actualización recae en el Comité de Seguridad de la Información, que llevará a cabo una evaluación periódica, al menos con carácter anual, para asegurar su adecuación a la realidad operativa, tecnológica y normativa de la organización.

Asimismo, se podrán realizar revisiones extraordinarias cuando concurran circunstancias que así lo aconsejen, tales como:

- Cambios relevantes en la estructura organizativa o funcional de la organización.
- Modificaciones significativas en el marco normativo aplicable.
- Lecciones aprendidas derivadas de auditorías, incidentes o análisis de riesgos.

Esment garantizará una difusión eficaz de esta Política entre todo el personal afectado, asegurando que esté disponible en los medios adecuados y que se proporcionen los recursos necesarios para su conocimiento, comprensión y cumplimiento.

Además, se establecerán mecanismos de supervisión, seguimiento y control, que permitan:

- Verificar la correcta implantación de la Política.
- Evaluar su eficacia y grado de cumplimiento.
- Identificar necesidades de mejora o actualización.

Esta Política constituye el marco de referencia para todas las actuaciones en materia de seguridad de la información y deberá ser observada en todos los niveles organizativos, garantizando una protección eficaz de los activos y servicios gestionados por la entidad.

2. Introducción

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

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto 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.

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

3. Misión de Esment

La Organización es de iniciativa social y tiene como misión apoyar y acompañar a las personas con diversidad intelectual y a sus familias a lo largo de toda su vida, promoviendo su dignidad, autonomía y bienestar. Para ello, desarrolla actividades y presta servicios centrados en la persona, desde un enfoque inclusivo, ético y sostenible.

Su modelo de actuación se basa en la creación de oportunidades reales para que cada persona pueda desarrollar su proyecto de vida en igualdad de condiciones, mediante el acceso a servicios de apoyo, empleo, formación, vivienda, relaciones significativas y participación activa en la comunidad.

La Organización articula redes de colaboración con familias, profesionales, administraciones públicas, entidades del tercer sector y empresas, con el objetivo de favorecer entornos inclusivos y accesibles, donde la diversidad sea valorada y respetada. Asimismo, promueve iniciativas productivas socialmente responsables, como actividades agrícolas, de restauración, imprenta y servicios, que generan empleo y aportan valor social, económico y medioambiental.

Su actuación se rige por principios de transparencia, ética, responsabilidad y mejora continua, integrando la sostenibilidad en todas sus áreas de gestión.

4. Marco Normativo

Las actividades y competencias de la Organización, se desarrollan en el marco de un conjunto normativo compuesto por legislación estatal y autonómica. Este cuerpo legal abarca ámbitos como la administración electrónica, la seguridad de la información, la protección de datos personales y los servicios tecnológicos que dan soporte a dichas funciones, garantizando así el cumplimiento de las obligaciones legales aplicables.

La relación de normas que conforman este marco se recoge en el documento ESM STIC-REG-1, un registro específico que se mantiene actualizado de forma continua conforme a lo establecido en la normativa interna de gestión de requisitos legales y cumplimiento normativo. Este instrumento permite una gestión centralizada de la legislación aplicable y asegurando que la organización se adapte eficazmente a los cambios regulatorios.

5. Alcance

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

6. La Seguridad de la Información

El propósito de esta Política es establecer la postura de la Organización en relación con la seguridad de la información que se maneja en el desarrollo de sus funciones. Este compromiso incluye de forma prioritaria los procesos vinculados a la administración electrónica, tanto en lo que respecta a los servicios ofrecidos a los ciudadanos como en las actividades internas de gestión y operación.

La Organización basa la prestación de sus servicios en el uso de las Tecnologías de la Información y las Comunicaciones, siendo plenamente consciente de los riesgos inherentes a su uso, como los incidentes de seguridad -fortuitos o malintencionados- y del impacto que estos pueden generar en la consecución de sus objetivos, en la confianza de los usuarios y en la continuidad operativa. Se reconoce, además, que estos incidentes pueden originarse tanto en el entorno interno como a través de accesos remotos mediante redes de comunicación, especialmente desde internet, a través de ciberataques.

Frente a este contexto de amenazas, se adopta un enfoque proactivo, orientado a mitigar los riesgos dentro de sus capacidades operativas y presupuestarias. Para ello, establece una estructura de

seguridad apoyada por mecanismos de gestión, medidas técnicas y procedimientos organizativos que permitan:

- Garantizar el cumplimiento de sus objetivos institucionales y la prestación de los servicios.
- Asegurar la conformidad con el marco normativo vigente.
- Proteger sus infraestructuras frente a amenazas deliberadas.

Para alcanzar estos fines, la Organización desplegará medidas preventivas orientadas a reducir la probabilidad de que se materialicen incidentes de seguridad que puedan comprometer servicios, datos o infraestructuras. Del mismo modo, se establecerán procedimientos de respuesta, que permitan gestionar y contener de forma adecuada los incidentes, minimizando sus consecuencias y restaurando cuanto antes la normalidad operativa.

Como principio rector, la gestión de la seguridad estará guiada por un enfoque basado en el riesgo, priorizando la identificación y mitigación de aquellas amenazas que supongan mayor impacto para la organización.

Las unidades responsables de los servicios deberán incorporar la seguridad como un factor desde la fase de diseño de cualquier nuevo sistema o servicio. Esta integración desde el inicio permitirá aplicar de forma efectiva las medidas exigidas por el Esquema Nacional de Seguridad (ENS), tanto en sistemas de nueva implantación como en los ya existentes, garantizando la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de la información y los servicios gestionados.

7. Modelo de Gobernanza

La gestión de la seguridad de la información en la Organización se articula mediante una estructura organizativa basada en tres niveles funcionales, que permiten una gestión integral y eficaz de los aspectos relacionados con la protección de la información y los servicios:

7.1. Estructura de especificación

Este primer nivel es responsable de definir los requisitos y criterios de seguridad aplicables a los servicios y sistemas gestionados por la Organización. Su función principal es garantizar que dichos requisitos estén alineados tanto con el marco establecido por el Esquema Nacional de Seguridad como con los objetivos estratégicos y operativos de la entidad. Esta estructura proporciona las directrices que servirán de base para el diseño, planificación y contratación de soluciones tecnológicas seguras.

7.2. Estructura de supervisión

Encargada de verificar el cumplimiento de los requisitos de seguridad definidos en la fase de especificación y de asegurar que las medidas implementadas sean coherentes con las necesidades reales y los principios estratégicos. Esta capa de supervisión incluye figuras clave como el Responsable de Seguridad de la Información, quien lidera la implantación de la política de seguridad, coordina la actuación de los distintos responsables implicados y actúa como enlace con los órganos de dirección. También participa en la evaluación de riesgos, revisión de incidentes y seguimiento de auditorías.

7.3. Estructura de operación

Compuesta por los perfiles y unidades encargadas de aplicar y mantener en funcionamiento las medidas de seguridad definidas. Esta estructura incluye roles como el Responsable del Sistema, así como los administradores de sistemas y los operadores de seguridad, quienes ejecutan los controles técnicos, gestionan los accesos, monitorizan la actividad y atienden los eventos de seguridad del sistema. Su función es clave para garantizar la protección continua de los activos de información en la operativa diaria.

Esta estructura en tres niveles permite distribuir funciones y responsabilidades de forma clara, evitando solapamientos y asegurando una coordinación efectiva entre los diferentes actores implicados. Además, refuerza el principio de diferenciación de responsabilidades establecido en el ENS y promueve una gestión continua y adaptada a los riesgos reales que enfrenta la organización.

7.4. Estructura de Especificación

La estructura de especificación es responsable de definir los requisitos de seguridad aplicables a los servicios que presta la Organización en las infraestructuras que gestiona. Su principal misión es garantizar el cumplimiento de la normativa vigente, en particular:

El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.

A continuación, se describen las funciones y responsabilidades de los roles clave asociados a la estructura de especificación:

Responsable de la Información

El Responsable de la Información es la figura encargada de velar por la protección de los datos e información gestionados por la Organización asegurando que su disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad estén debidamente garantizadas en todos los procesos en los que se traten.

Esta figura asume, de forma unificada, las funciones del Responsable del Tratamiento de Datos Personales, conforme al Reglamento General de Protección de Datos y a la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. Esta integración evita duplicidades, refuerza la coherencia en la gestión de la seguridad de la información y optimiza la toma de decisiones en materia de cumplimiento normativo.

Entre sus funciones principales se encuentran:

- Establecer los requisitos de seguridad asociados a la información bajo su responsabilidad, asignándole una valoración que permita determinar el nivel de protección necesario.
- Coordinarse con el Responsable de Seguridad de la Información y el Responsable del Sistema para definir, ajustar y validar las medidas de protección aplicables a la información tratada.
- Asegurar que las medidas de seguridad se adecuen a las necesidades específicas de los distintos tipos de información gestionados por la Organización.
- Determinar los fines y medios del tratamiento de datos personales, conforme al artículo 24 del RGPD.
- Supervisar el cumplimiento de los principios fundamentales del tratamiento de datos personales, como la licitud, lealtad, transparencia, minimización, exactitud y limitación de la conservación.

- Garantizar la existencia, mantenimiento y actualización del Registro de Actividades de Tratamiento.
- Supervisar el cumplimiento del deber de información a los interesados y la correcta implementación de mecanismos que permitan el ejercicio de sus derechos.
- Evaluar los riesgos para los derechos y libertades de los interesados ante posibles brechas de seguridad, adoptando las medidas necesarias y, en su caso, gestionando las notificaciones ante la autoridad de control y los propios afectados.
- Establecer e implementar medidas técnicas y organizativas apropiadas que garanticen un tratamiento conforme con el RGPD.
- Actuar como punto de contacto con la Agencia Española de Protección de Datos u otras autoridades competentes, en coordinación con el Delegado de Protección de Datos.
- Promover programas de formación y concienciación sobre protección de datos personales dirigidos al personal de la Organización, adaptados a los distintos perfiles de responsabilidad.

Este rol podrá ser desempeñado por una persona física, un grupo de personas o un órgano colegiado, en función de la estructura organizativa de la entidad. En determinadas circunstancias, y siempre que no se produzca conflicto de funciones, este rol podrá coincidir con el del Responsable del Servicio correspondiente.

Responsable del Servicio

El Responsable del Servicio es la figura encargada de definir y garantizar los niveles de seguridad necesarios para los servicios prestados por la Organización. Su función principal es asegurar que los servicios bajo su ámbito de responsabilidad cuenten con medidas de protección proporcionales a su criticidad, a los riesgos identificados y al valor de la información que gestionan.

Este rol tiene un papel clave en la gestión de la seguridad desde la perspectiva funcional y operativa de los servicios TIC, velando por que estos se diseñen, implanten y mantengan con garantías adecuadas de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Entre sus principales funciones se encuentran:

- Establecer los requisitos de seguridad específicos de los servicios, en coordinación con el Responsable de Seguridad de la Información y el Responsable del Sistema, garantizando la coherencia entre la protección del servicio y la de la información que lo sustenta.
- Asegurar que las medidas de seguridad implementadas respondan tanto a las necesidades operativas del servicio como a los requisitos normativos y de gestión del riesgo.
- Considerar las características de la información tratada en el marco de los servicios bajo su responsabilidad, alineando los requisitos de seguridad del servicio con los establecidos para la información correspondiente.
- Participar en la definición de niveles de servicio, incluyendo objetivos de continuidad, disponibilidad, recuperación ante incidentes y respuesta a catástrofes.

Este rol podrá ser desempeñado por una persona individual, por varias personas o por un órgano colegiado, en función de la organización interna. Cuando no exista conflicto de intereses, esta responsabilidad podrá coincidir con la del Responsable de la Información.

7.5. Estructura de Supervisión

La estructura de supervisión de la seguridad tiene como finalidad principal garantizar que la implantación y operación de los requisitos de seguridad se lleven a cabo de forma adecuada, en consonancia con los objetivos estratégicos de la organización y en cumplimiento de la normativa vigente, incluyendo el Esquema Nacional de Seguridad y la legislación sectorial o específica que resulte de aplicación.

Esta función de supervisión se materializa mediante un modelo organizativo que permite evaluar de manera continua la eficacia de las medidas implantadas, identificar desviaciones y proponer acciones de mejora.

Dentro de esta estructura, la supervisión de la seguridad de la información y de los servicios recae principalmente en el Responsable de Seguridad de la Información, figura encargada de coordinar y dinamizar la implementación de las políticas, procedimientos y controles de seguridad en toda la organización.

La coordinación global y el seguimiento estratégico de la seguridad se canalizan a través del Comité de Seguridad de la Información, órgano colegiado que asegura una visión transversal e integradora de la seguridad, fomentando la colaboración entre las distintas áreas implicadas y facilitando la toma de decisiones informada en esta materia.

Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información es la figura encargada de liderar, coordinar y supervisar la implementación de las políticas, estrategias y medidas de seguridad de la información. Su papel es clave para asegurar que la protección de la información y los servicios se realice conforme a los requisitos establecidos por la organización, por el Esquema Nacional de Seguridad y por el resto de la normativa aplicable.

El Responsable de Seguridad de la información participa activamente en el Comité de Seguridad de la Información, actuando como figura técnica de referencia y como catalizador de las decisiones estratégicas en materia de cibeResponsable de Seguridad de la Informaciónuridad.

Entre sus principales funciones se encuentran:

- Coordinar y supervisar la implantación de las medidas de seguridad de la información y de protección de datos, en colaboración con los distintos responsables implicados.
- Impulsar la elaboración del presupuesto anual destinado a la seguridad de las tecnologías de la información, asegurando su adecuación a las necesidades reales.
- Definir y mantener actualizado un modelo de gestión de la seguridad alineado con la estrategia institucional de la Organización.
- Supervisar la ejecución de las estrategias de seguridad y gestionar la respuesta ante incidentes de cibeResponsable de Seguridad de la Informaciónuridad, incluyendo su contención, análisis, mitigación y reporte.
- Promover y supervisar la realización periódica de análisis de riesgos, elevando los planes de tratamiento y mejora correspondientes al Comité de Seguridad.
- Establecer indicadores clave (KPIs) para evaluar la eficacia de las medidas de seguridad implantadas, proponiendo ajustes cuando sea necesario.
- Elaborar normativa interna en materia de seguridad de la información, asegurando su coherencia con esta Política y su aplicación efectiva en toda la organización.

- Asegurar la inclusión de cláusulas de seguridad de la información en los contratos con proveedores, especialmente en aquellos que impliquen tratamiento de información o prestación de servicios TIC.
- Impulsar auditorías regulares de seguridad y colaborar activamente en los procesos de auditoría interna o externa que afecten al ámbito de la seguridad de la información.
- Redactar y mantener la Declaración de Aplicabilidad de medidas de seguridad, conforme al ENS y a los resultados del análisis de riesgos.
- Coordinar las acciones de formación, concienciación del personal en materia de seguridad de la información, adaptándolas a los perfiles de riesgo y responsabilidades.

El Responsable de Seguridad de la Información debe contar con independencia operativa, conocimientos técnicos acreditados y capacidad de interlocución con todos los niveles organizativos.

Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el órgano colegiado responsable de coordinar, supervisar y dinamizar todas las actuaciones relacionadas con la seguridad de la información en la Organización. Su misión es asegurar un enfoque transversal de la seguridad, promover la mejora continua y garantizar la alineación con los objetivos estratégicos de la organización.

Este Comité actúa como punto de encuentro entre las distintas áreas funcionales y técnicas implicadas, facilitando la toma de decisiones informadas y la gestión eficaz de la seguridad en todos los niveles.

Entre sus funciones principales se encuentran:

- Establecer los objetivos corporativos en materia de seguridad de la información, en coherencia con la estrategia institucional de la Organización.
- Informar periódicamente a la Gerencia sobre el estado de la seguridad, los riesgos emergentes y las acciones en curso.
- Revisar la Política de Seguridad y la normativa interna asociada, proponiendo actualizaciones cuando existan cambios normativos, tecnológicos u organizativos relevantes.
- Evaluar y aprobar los planes de tratamiento de riesgos presentados por las áreas responsables, así como supervisar su ejecución.
- Coordinar la implementación de medidas de seguridad entre las distintas áreas y servicios de la organización, garantizando una actuación coherente.
- Supervisar la gestión de los incidentes de seguridad, definir estrategias de respuesta y evaluar las lecciones aprendidas.
- Analizar los indicadores clave de seguridad y proponer medidas correctoras ante desviaciones significativas.
- Impulsar la realización de auditorías de seguridad, tanto internas como externas, y garantizar la implantación de las acciones correctivas derivadas de sus resultados.

El Comité estará integrado por miembros permanentes designados por la Gerencia, representando a las áreas clave (tic, legal, protección de datos, recursos humanos, etc.), así como por miembros invitados según la naturaleza de los asuntos a tratar. La participación del Responsable de Seguridad de la Información es permanente, actuando además como coordinador técnico del Comité.

Miembros:

- Responsable de la Información (RI) – Luis Gil de Sola

- Responsable de Seguridad (RSeg) – Gregorio Cobacho Navarro
- Responsable del Servicio (RSer) – Gregorio Cobacho Navarro
- Responsable del Sistema (RSis) – Francisco Cuello Principal
- Delegado/a de Protección de Datos (DPD) – Iuristec
- Secretaría del Comité – Lucia Enseñat Bilbao
- Responsable Nuevos Proyectos – Javier de Juan Martín

Este órgano se reunirá con una periodicidad mínima semestral, y de forma extraordinaria cuando la situación lo requiera, especialmente ante la ocurrencia de incidentes graves, auditorías o modificaciones normativas sustanciales.

7.6. Estructura de Operación

La estructura de operación de la seguridad tiene como finalidad garantizar la aplicación de las medidas de protección definidas por los niveles superiores de gobierno de la seguridad en la Organización. Esta estructura actúa directamente sobre los sistemas de información y comunicaciones, asegurando que los controles de seguridad estén correctamente integrados.

Su papel es esencial para mantener la seguridad en la operativa diaria, gestionar los recursos tecnológicos de forma segura y responder de manera eficiente ante cualquier evento o incidente que pueda comprometer la integridad, autenticidad, disponibilidad, confidencialidad o trazabilidad de los activos de información.

La estructura de operación ejecuta las medidas de seguridad, monitoriza su funcionamiento y colabora en la mejora continua del entorno de seguridad de la información.

A continuación, se describen las funciones y responsabilidades de los perfiles clave que conforman esta estructura.

Responsable de los Sistemas de Información

El Responsable del Sistema es la figura clave en la estructura de operación de la seguridad de la Organización, encargada de garantizar que los sistemas tecnológicos y las infraestructuras de comunicaciones operen de manera segura, conforme a los requisitos definidos por la organización.

Su función se centra en la implementación técnica de las medidas de seguridad y en la gestión segura del ciclo de vida de los sistemas, desde su diseño y configuración hasta su mantenimiento y supervisión continua.

Entre sus principales funciones y responsabilidades se encuentran:

- Definir especificaciones funcionales de seguridad en colaboración con el Responsable de Seguridad de la Información, asegurando que los sistemas de información cumplan los requisitos establecidos.
- Garantizar la seguridad desde el diseño, incorporando mecanismos de protección fundamentales -como la disponibilidad, integridad, confidencialidad, autenticación, control de acceso, trazabilidad y registro- en todas las fases del ciclo de vida del sistema.

- Supervisar la configuración segura de los sistemas (bastionado), tanto en su fase inicial como tras cualquier modificación significativa, asegurando la aplicación de configuraciones acordes a los estándares definidos por la Organización.
- Controlar los accesos a los sistemas y recursos, verificando que los mecanismos de autenticación y autorización funcionen adecuadamente y que no puedan ser desactivados o eludidos por los usuarios.
- Gestionar vulnerabilidades, realizando un seguimiento proactivo de las fuentes oficiales de alertas y planificando la aplicación de parches en función del impacto y criticidad, en coordinación con los administradores de sistemas.
- Implantar medidas de seguridad derivadas de los planes de tratamiento de riesgos, así como ejecutar las acciones correctivas recomendadas por auditorías técnicas o de cumplimiento.
- Aportar información relevante para la elaboración y seguimiento de los indicadores de seguridad, facilitando una visión objetiva del estado de los sistemas.
- Supervisar los procedimientos de copia de seguridad, asegurando su ejecución regular, su eficacia y la posibilidad de recuperación ante fallos o incidentes.
- Realizar auditorías técnicas periódicas sobre la infraestructura, sistemas y aplicaciones, con el objetivo de verificar su alineación con las políticas, estándares y normativa interna de seguridad de la información.

El Responsable del Sistema debe actuar con un alto nivel de coordinación con el Responsable de Seguridad de la Información, el Responsable del Servicio y el Responsable de la Información, formando parte activa de la estructura operativa que garantiza la seguridad del entorno tecnológico de la Organización.

Además del Responsable del Sistema, la estructura operativa de la seguridad de la información se apoya en otros perfiles técnicos especializados que desempeñan funciones clave en el mantenimiento seguro de los sistemas.

Entre ellos se encuentran los administradores de sistemas, responsables de aplicar configuraciones, gestionar accesos y ejecutar tareas técnicas bajo las directrices establecidas; los operadores de seguridad, encargados de la monitorización, registro y respuesta operativa ante eventos e incidentes; y el personal técnico de soporte, que colabora en la ejecución diaria de los procedimientos de seguridad y en la atención de incidencias.

Todos estos perfiles actúan bajo la coordinación del Responsable del Sistema y en estrecha colaboración con el Responsable de Seguridad de la Información, asegurando la correcta implementación de las medidas de protección y el cumplimiento de los principios establecidos en esta Política.

8. Designación de Roles en las Estructuras de Seguridad

La designación y modificación de los roles clave en el modelo de gobierno de la seguridad de la información es competencia de la Gerencia de la entidad.

Las designaciones se formalizarán mediante acta o resolución, que actuará como documento justificativo de los nombramientos. Estos registros deberán mantenerse actualizados, reflejando

cualquier cambio organizativo, funcional o de responsabilidades que afecte a las estructuras de seguridad, con el fin de garantizar una asignación clara, trazable y efectiva de funciones.

8.1. Procedimiento de Designación y Renovación

- El Responsable de la Información será, por defecto, la Gerencia de la Organización, en coherencia con su rol funcional dentro de la estructura organizativa de la entidad.
- El Responsable del Servicio será el Responsable de la Unidad TIC, por ostentar la responsabilidad directa sobre la gestión operativa y la continuidad de los servicios tecnológicos. Esta designación será automática, salvo que la Gerencia disponga lo contrario mediante resolución, con informe del Comité de Seguridad de la Información.
- El Responsable de Seguridad de la Información será designado por la Gerencia, a propuesta del Comité de Seguridad de la Información, en función de sus competencias técnicas y capacidad de coordinación.
- El Responsable del Sistema de Información será también designado por la Gerencia, a propuesta del Comité, atendiendo a su conocimiento técnico de la infraestructura y su rol operativo.
- El Delegado de Protección de Datos será nombrado por la Gerencia, conforme a los criterios establecidos en el Reglamento General de Protección de Datos (RGPD), garantizando independencia, formación especializada y ausencia de conflicto de intereses.
- El Responsable del Tratamiento, cuando corresponda identificarlo de forma expresa, será igualmente designado por la Gerencia, de acuerdo con lo dispuesto en la normativa vigente en materia de protección de datos.

Los demás miembros del Comité de Seguridad de la Información serán nombrados por la Gerencia en función de su responsabilidad jerárquica y funcional dentro de la organización.

8.2. Renovación y Sustituciones

Las designaciones se revisarán, con carácter general, cada dos años, pudiendo ser modificadas antes en caso de vacante, reorganización, ausencia prolongada o incumplimiento grave de funciones.

La Gerencia deberá asegurar la existencia de personas sustitutas designadas temporalmente para cubrir ausencias prolongadas de cualquier responsable clave, con el fin de mantener la continuidad del modelo de gobierno de la seguridad.

Este procedimiento garantiza que la estructura de roles y responsabilidades en materia de seguridad se mantenga operativa, actualizada y conforme con lo exigido por el Esquema Nacional de Seguridad.

De acuerdo con esta estructura, se han asignado las siguientes responsabilidades y funciones de seguridad:

Bloque de Gobierno:

Responsable de Gobierno, cuyas funciones ejercita la GERENCIA de la organización, que integra los siguientes roles y funciones ENS:

- Comité de Seguridad de la Información.
- Responsable de la Información.

- Responsable del Servicio.

Bloque Ejecutivo/Supervisión:

Responsable de Supervisión, cuyas funciones ejercita la Secretaría de la organización y que integra el siguiente rol ENS:

- Responsable de la Seguridad.

Delegado Protección de Datos (DPD), Secretario. apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

Bloque de Operación:

Responsable de Operación, cuyas competencias ejercita un empleado que ocupa el puesto Administrativo, y que integra el siguiente rol ENS:

- Responsable del Sistema.

9. Gestión del Personal

Todo el personal de la Organización que interviene directa o indirectamente en el uso, administración, mantenimiento o explotación de la información y de los servicios prestados -incluidos los considerados esenciales- está obligado a conocer y cumplir la presente Política de Seguridad, así como la normativa, procedimientos y directrices que la desarrollan.

La seguridad de la información, conforme al principio de proceso integral recogido en el Esquema Nacional de Seguridad, debe ser considerada una responsabilidad compartida por todas las personas que forman parte de la organización, sin importar su nivel jerárquico o funcional.

Con el fin de garantizar el cumplimiento de esta obligación, el Comité de Seguridad de la Información será el encargado de establecer los mecanismos necesarios para asegurar la difusión efectiva de esta Política y su correcta comprensión por parte de todo el personal afectado. Esto incluirá, entre otros medios, la publicación en entornos accesibles, la comunicación formal en procesos de incorporación, así como la incorporación de contenidos de seguridad en programas de formación y concienciación continua.

De acuerdo con el principio de diferenciación de responsabilidades, el personal con funciones específicas relacionadas con la seguridad (como responsables de sistemas, información, servicios o tratamiento de datos) deberá tener claramente asignadas sus atribuciones y recibir formación adecuada para su desempeño, en coherencia con el marco normativo interno y externo vigente.

Esta implicación activa del personal en la gestión de la seguridad contribuye a fortalecer la cultura organizativa en esta materia, y resulta imprescindible para garantizar la resiliencia operativa, la protección de los activos de información y el cumplimiento del marco legal y regulatorio aplicable.

10. Formación y Concienciación en Seguridad de la Información

El programa de formación y concienciación en seguridad de la información de la Organización tiene como finalidad reforzar la capacidad del personal para actuar de forma segura, en todas aquellas

actividades que impliquen el uso o tratamiento de información, especialmente en entornos y servicios soportados por tecnologías de la información y las comunicaciones.

Este programa se estructura en dos líneas complementarias:

- Formación: orientada al personal que desempeña funciones directamente relacionadas con la administración, mantenimiento o explotación de sistemas y servicios TIC, con el objetivo de proporcionar conocimientos específicos sobre procedimientos de seguridad, configuración segura de equipos, desarrollo seguro, gestión de incidentes, análisis de riesgos y otras buenas prácticas relevantes.
- Concienciación: dirigida a la totalidad del personal, con el propósito de sensibilizar sobre la importancia de la seguridad de la información y fomentar hábitos seguros en el manejo, almacenamiento e intercambio de datos. Se promoverá el cumplimiento de buenas prácticas mediante pautas claras, mensajes accesibles y recursos formativos adaptados al perfil del destinatario.

En aplicación del principio de seguridad como proceso integral, todas las personas que prestan servicios en la Organización deberán participar en sesiones de concienciación con la periodicidad establecida por el Comité de Seguridad de la Información. Estas sesiones tendrán como finalidad reforzar el entendimiento de los riesgos más comunes, los procedimientos básicos de protección de la información, y los canales para la notificación de incidentes.

Asimismo, las personas que asuman responsabilidades específicas en el uso, gestión o mantenimiento de servicios TIC deberán recibir formación especializada antes de iniciar dichas funciones, ya sea por asignación inicial, cambio de puesto o ampliación de competencias. Esta formación será obligatoria y estará adaptada al nivel técnico requerido por el puesto.

Los contenidos formativos incluirán tanto aspectos normativos como técnicos y operativos, y se estructurarán conforme al principio de profesionalidad recogido en el Esquema Nacional de Seguridad.

Las unidades responsables de la seguridad de la información, en coordinación con el área de Recursos Humanos, serán las encargadas de definir el formato, los contenidos y los criterios de evaluación de estas acciones formativas, asegurando que respondan a las necesidades reales de la organización y que sean accesibles y actualizadas.

El compromiso institucional con la formación continua y la concienciación del personal constituye una medida fundamental para minimizar los riesgos humanos, reforzar la cultura de la seguridad de la información y mantener un entorno de trabajo resiliente frente a amenazas y vulnerabilidades.

11. Terceras partes

Las entidades externas que colaboren con la Organización en la gestión, mantenimiento o explotación de sus servicios estarán sujetas al cumplimiento de los requisitos establecidos en esta Política de Seguridad de la Información, debiendo garantizar la protección adecuada de los sistemas y los servicios involucrados. Esta obligación incluye tanto a proveedores de servicios como a terceros con acceso a información o infraestructuras.

Los procedimientos, controles y medidas adoptadas por terceros deberán alinearse con los principios y estándares definidos por la Organización. Se permitirá la utilización de procedimientos operativos

propios por parte de dichas entidades, siempre que sean equivalentes en eficacia a los definidos por la Organización y estén validados por el Responsable de Seguridad de la Información.

Para garantizar una colaboración segura, se establecerán mecanismos específicos para la comunicación de incidencias, permitiendo que las entidades externas informen de manera eficiente sobre cualquier evento que pueda comprometer la seguridad de la información o los servicios.

El personal de estas entidades deberá participar en acciones de concienciación en seguridad de la información, en condiciones equiparables a las exigidas al personal interno, a fin de asegurar un conocimiento adecuado de la normativa, los procedimientos y las responsabilidades en materia de seguridad de la información.

En caso de que una entidad externa no pueda cumplir con alguno de los requisitos establecidos, el Responsable de Seguridad de la Información elaborará un informe de riesgo, detallando la situación y las posibles medidas de mitigación. Este informe será evaluado por el Comité de Seguridad de la Información, que decidirá si se acepta el riesgo y bajo qué condiciones puede continuar la relación contractual. La decisión deberá ser aprobada por la Gerencia.

La contratación de servicios o adquisición de productos tecnológicos deberá considerar expresamente los requisitos de seguridad del ENS, incluyendo la obligación del adjudicatario de cumplir con las medidas recogidas en el Anexo II del Real Decreto 311/2022. En el caso de servicios en la nube, se tendrán en cuenta las guías de seguridad publicadas por el CCN, especialmente las que rigen la contratación, evaluación y uso seguro de servicios cloud.

La Organización podrá requerir que las entidades externas aporten evidencias de cumplimiento, incluidas auditorías de segunda o tercera parte, así como la documentación necesaria para verificar la aplicación efectiva de las medidas exigidas.

Se establecerán procedimientos específicos de reporte y resolución de incidencias, que deberán ser canalizados a través del Punto de Contacto (POC) designado por el proveedor o entidad externa, y, cuando se vean afectados datos personales, también mediante el Delegado de Protección de Datos.

Cuando la Organización actúe como proveedor de servicios o encargado del tratamiento para otras entidades, se garantizará el cumplimiento de las obligaciones legales correspondientes, así como la difusión de esta Política a las entidades afectadas. Se establecerán mecanismos de coordinación entre los respectivos Comités de Seguridad y procedimientos para la gestión conjunta de incidentes.

En todos los casos, los terceros deberán garantizar que su personal está suficientemente formado y sensibilizado en materia de seguridad, cumpliendo al menos con el nivel exigido por esta Política o el establecido contractualmente.

En caso de que algún aspecto de la Política no pueda ser satisfecho por un tercero, el Responsable de Seguridad de la Información elaborará un informe de riesgos que será evaluado por los Responsables de la Información y del Servicio afectados. La aprobación de este informe será requisito previo para la adjudicación o formalización del contrato, y deberá contar con la conformidad expresa de la Gerencia de la Organización, quien asumirá formalmente los riesgos identificados.

12. Gestión de Riesgos

Todos los sistemas de información y servicios tecnológicos sujetos a esta Política de Seguridad de la Información deberán someterse a un proceso sistemático de análisis y gestión de riesgos, con el objetivo de identificar, evaluar y tratar aquellas amenazas que puedan comprometer los principios fundamentales de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Este proceso se fundamenta en el principio de gestión basada en riesgos, establecido en el Esquema Nacional de Seguridad, y constituye la base para la adopción de medidas proporcionales en materia de seguridad de la información.

El análisis de riesgos deberá realizarse:

- De forma periódica, con una frecuencia mínima anual.
- Cuando se produzcan cambios sustanciales en la información tratada o en los servicios prestados.
- Tras la ocurrencia de incidentes de seguridad relevantes.
- Cuando se identifiquen vulnerabilidades significativas que puedan afectar a los activos de información.
- Ante la generación o modificación de evaluaciones de impacto en protección de datos (EIPD) o cambios en los análisis de riesgos relacionados con datos personales.

Con el fin de armonizar y normalizar los análisis de riesgos, el Comité de Seguridad de la Información establecerá valoraciones de referencia para los diferentes tipos de información y servicios que gestiona la Organización. Estas referencias facilitarán la comparación entre sistemas, la agregación de resultados y la priorización de medidas correctivas o preventivas.

Este Comité también será responsable de:

- Establecer los niveles de riesgo aceptables para la organización.
- Aprobar los planes de tratamiento de riesgos, asegurando su alineación con la estrategia de seguridad institucional.
- Impulsar la disponibilidad de recursos, especialmente para iniciativas transversales que refuercen la seguridad de forma horizontal en toda la organización.

Como complemento al análisis de riesgos, la Organización desarrollará un documento de continuidad de negocio o Business Impact Analysis (BIA). Este documento identificará los procesos críticos, los tiempos máximos de recuperación aceptables (RTO y RPO), y establecerá las medidas necesarias para garantizar la continuidad operativa frente a interrupciones, incidentes graves o fallos tecnológicos.

En lo relativo a los riesgos vinculados al tratamiento de datos personales, se prestará especial atención a su evaluación conforme al Reglamento General de Protección de Datos. El Delegado de Protección de Datos (DPD) participará activamente en la identificación y valoración de estos riesgos, así como en la validación de las EIPD, en aquellos casos en que sean exigibles.

La coordinación entre los planes de tratamiento del ENS y los derivados del RGPD será clave para garantizar un enfoque integral y coherente de la gestión de riesgos, evitando duplicidades y asegurando una protección eficaz.

Todos los resultados obtenidos del análisis y tratamiento de riesgos deberán quedar documentados de forma trazable, y constituirán el soporte principal para:

- La toma de decisiones en materia de inversiones en seguridad.
- La planificación y ejecución de medidas correctoras o preventivas.
- El seguimiento del nivel de protección alcanzado por los sistemas y servicios afectados.

13. Gestión de Incidentes de Seguridad

La Organización contará con un procedimiento formal para la gestión de incidentes de seguridad de la información, orientado a identificar, comunicar, analizar y resolver de forma eficiente cualquier evento que pueda comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de los servicios y los datos gestionados.

Este procedimiento se articulará conforme al principio de prevención, detección y respuesta, recogido en el Esquema Nacional de Seguridad, e integrará mecanismos específicos en cada una de las fases del ciclo de vida de un incidente:

13.1. Prevención

Se adoptarán medidas técnicas y organizativas preventivas para proteger los servicios y la información frente a amenazas potenciales. Estas medidas incluirán tanto las previstas en el Anexo II del ENS como aquellas derivadas de los resultados del análisis de riesgos. Se priorizarán las acciones que reduzcan la superficie de exposición, refuercen los controles de acceso y fortalezcan la continuidad de los sistemas.

13.2. Detección y reacción

Se dispondrá de sistemas de monitorización continua, herramientas de detección de anomalías y mecanismos automáticos para identificar, en tiempo real, eventos o comportamientos inusuales que puedan derivar en incidentes de seguridad.

El procedimiento incluirá:

- Canales de notificación accesibles para que tanto el personal interno como usuarios externos puedan reportar posibles incidentes de manera estructurada.
- Protocolos de respuesta rápida, con responsabilidades claramente definidas, para garantizar la contención y análisis inmediato del incidente.
- Activación coordinada de los equipos responsables (Responsable del Sistema, Responsable de Seguridad de la Información, responsables del servicio/información y Comité de Seguridad), según el tipo y alcance del incidente.

13.3. Recuperación

Para los servicios identificados como críticos, se desarrollarán y mantendrán actualizados planes de continuidad y recuperación, que contemplen:

- Tiempos máximos de recuperación aceptables (RTO y RPO).
- Procedimientos de restauración de sistemas.
- Medidas de mitigación de impacto.
- Pruebas periódicas de eficacia de los planes.

El procedimiento de gestión de incidentes será compatible y coordinado con otros marcos normativos aplicables, como el Reglamento General de Protección de Datos (RGPD) o normativas sectoriales específicas. Esta coordinación garantizará una respuesta eficaz, multidisciplinar y sin dilaciones indebidas, incluyendo:

- La notificación a autoridades de control competentes, como la Agencia Española de Protección de Datos.
- La comunicación, cuando proceda, con Fuerzas y Cuerpos de Seguridad del Estado, organismos judiciales o autoridades del ámbito de la cibeResponsable de Seguridad de la Informaciónuridad.

El Comité de Seguridad de la Información supervisará la eficacia del procedimiento, propondrá medidas de mejora y garantizará la adecuada documentación y trazabilidad de cada incidente y su resolución.

14. Datos personales

La Organización trata datos de carácter personal en el ejercicio de sus competencias y funciones, conforme a lo descrito en su Registro de Actividades de Tratamiento, de acuerdo con el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

En cumplimiento de lo dispuesto por la normativa de protección de datos, se evaluará de forma sistemática los riesgos que puedan afectar a los derechos y libertades de las personas titulares de los datos, proponiendo un plan de actuación que contemple medidas correctoras cuando dichos riesgos superen los umbrales definidos como aceptables.

El análisis de riesgos relativos al tratamiento de datos personales será:

- Revisado periódicamente.
- Actualizado siempre que se detecte un cambio sustancial en los tratamientos, tecnologías empleadas o contexto normativo.
- Acompañado, en su caso, de una Evaluación de Impacto en Protección de Datos (EIPD) cuando se trate de tratamientos de alto riesgo.

Este proceso contará con el asesoramiento, supervisión y validación del Delegado de Protección de Datos, en cumplimiento del principio de *responsabilidad proactiva*.

El plan de tratamiento de riesgos derivados del RGPD se coordinará de forma integrada con el plan de riesgos definido en el marco del Esquema Nacional de Seguridad. Esta coordinación será especialmente relevante en ámbitos como:

- El control de prestadores de servicios con acceso a datos personales.
- La respuesta a incidentes de seguridad que puedan suponer brechas de datos personales.
- La implementación de medidas técnicas y organizativas comunes, evitando duplicidades y asegurando coherencia entre los marcos normativos.

La Organización garantizará que las obligaciones y principios de protección de datos se integren en el diseño de sus sistemas, procesos y servicios, conforme al principio de privacidad desde el diseño y por defecto.

15. Gestión de Información

La información tratada por la Organización deberá ser gestionada conforme a los principios de seguridad establecidos en esta Política, garantizando su protección en todo momento, independientemente del formato, soporte o entorno en el que se encuentre.

Con base en los principios de seguridad integral, seguridad por defecto y proporcionalidad, se adoptarán las medidas necesarias para asegurar la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de los datos, en coherencia con la normativa vigente en materia de seguridad de la información, protección de datos y administración electrónica.

Para ello, se tendrán en cuenta los siguientes aspectos clave:

- Protección de la información en reposo y en tránsito: se aplicarán mecanismos de cifrado y otros controles de seguridad que garanticen la protección de los datos tanto en su

almacenamiento como durante su transmisión a través de redes, especialmente cuando se trate de información sensible o sujeta a protección legal.

- Seguridad física y lógica de las instalaciones: se establecerán medidas de protección adecuadas para los entornos donde residen los sistemas de información, incluyendo controles de acceso físicos, videovigilancia, gestión de credenciales y medidas frente a amenazas ambientales o eléctricas.
- Gestión de accesos y autorizaciones: se implementarán mecanismos que aseguren que únicamente el personal autorizado pueda acceder a la información, en función de su rol y responsabilidades. Se aplicará el principio de mínimo privilegio, limitando los accesos exclusivamente a lo necesario para el desempeño de las funciones asignadas.
- Mantenimiento de la integridad de los sistemas: se garantizará la aplicación oportuna de parches y actualizaciones que corrijan vulnerabilidades, asegurando que los sistemas mantengan su funcionamiento dentro de parámetros seguros.
- Supervisión y registro de actividad: se habilitarán sistemas de registro, auditoría y monitorización que permitan documentar los accesos, modificaciones y eventos relevantes relacionados con la información. Asimismo, se implementarán medidas de detección de software malicioso o código dañino, incluyendo mecanismos de análisis y respuesta temprana.

Estas medidas se enmarcan en un modelo de seguridad basado en riesgos, y su correcta aplicación contribuirá a reforzar la confianza en los servicios y sistemas gestionados por la Organización, garantizando un tratamiento seguro y conforme a los estándares exigidos por el ENS.

16. Mecanismos de coordinación y Resolución de Conflictos

La coordinación entre los distintos roles y niveles organizativos implicados en la seguridad de la información se articulará a través del Comité de Seguridad de la Información, que actúa como órgano colegiado de consulta, supervisión y toma de decisiones estratégicas en esta materia.

Este comité será el espacio de referencia para garantizar una gestión integrada, coherente y colaborativa de la seguridad, permitiendo alinear las actuaciones técnicas, organizativas, estratégicas y normativas de las diferentes unidades y responsables.

En caso de que se produzcan discrepancias o conflictos de criterio entre los distintos roles de gobierno de la seguridad de la información -como pueden ser el Responsable de Seguridad de la Información, el Responsable del Sistema, el Responsable del Servicio o el Responsable de la Información-, corresponderá a la Gerencia de la Organización ejercer las funciones de mediación y resolución, garantizando que las decisiones adoptadas sean consistentes con:

- Los objetivos estratégicos de la organización.
- Los principios definidos en esta Política de Seguridad.
- El marco normativo aplicable, incluyendo el Esquema Nacional de Seguridad y la legislación en materia de protección de datos.

La decisión final de la Gerencia, cuando medie en la resolución de conflictos, deberá quedar registrada por escrito, pudiendo contar con el asesoramiento del Comité de Seguridad de la Información u otros órganos técnicos, en función de la complejidad o impacto de la cuestión tratada.

Cuando la Organización utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segúnda del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que 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.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

17. Gestión y Desarrollo de la Política de Seguridad de la Información

La Política de Seguridad de la Información de la Organización se desarrollará mediante la elaboración de normativas complementarias que aborden aspectos específicos de la seguridad, así como de procedimientos operativos que detallen su aplicación práctica en los distintos entornos tecnológicos y organizativos.

17.1. Aprobación y Revisión de la Documentación de Seguridad

La gestión de los documentos vinculados a la seguridad de la información seguirá las siguientes directrices:

- Política de Seguridad de la Información: será aprobada por el Consejo de Administración. Su revisión será responsabilidad del Comité de Seguridad de la Información, que, a través de Gerencia, propondrá las actualizaciones que se consideren necesarias.
- Normativa interna de seguridad de la información: será elaborada y actualizada por el Responsable de Seguridad de la Información, revisada por el Comité de Seguridad, y aprobada por la Gerencia, a propuesta del propio Comité.
- Procedimientos operativos de seguridad de la información: serán aprobados por Gerencia, a propuesta de los responsables de las unidades organizativas o del Responsable de Seguriad de la Información, previo informe favorable del Comité de Seguridad de la Información.

17.2. Clasificación Documental

Toda la documentación de seguridad se organizará atendiendo a su naturaleza y propósito:

- Documentos normativos: políticas, normas e instrucciones de obligado cumplimiento.
- Documentos operativos: procedimientos, planes y guías que describen la implementación práctica de las normas.
- Documentación de evidencia y registro: informes de auditoría, actas, resultados de revisiones, controles y evidencias de cumplimiento.

17.3. Control, Acceso y Trazabilidad

El acceso a la documentación de seguridad estará restringido y controlado según el rol del usuario, conforme al principio de mínimo privilegio. Su almacenamiento y gestión se llevará a cabo mediante plataformas seguras de gestión documental o herramientas del Sistema de Gestión de Seguridad de la Información (SGSI), que permitirán:

- Control de versiones.
- Registro de cambios.
- Disponibilidad controlada solo para perfiles autorizados.

El Responsable de Seguridad de la Información será el encargado de coordinar la gestión, actualización y trazabilidad de esta documentación, con la colaboración de los responsables implicados y bajo la supervisión del Comité de Seguridad de la Información.

Esta documentación estará disponible para todo el personal de la organización que, por razón de sus funciones, deba consultarla, especialmente para quienes utilicen, gestionen u operen sistemas de información incluidos en el alcance del ENS.

17.4. Mejora Continua

La Política de Seguridad, así como sus normativas y procedimientos asociados, estarán sometidos a un proceso de mejora continua, en cumplimiento de los principios del ENS. Este proceso garantizará su permanente actualización, teniendo en cuenta:

- Cambios en el panorama de riesgos.
- Modificaciones normativas o regulatorias.
- Avances tecnológicos.
- Lecciones aprendidas a partir de auditorías, revisiones, análisis de riesgos o incidentes de seguridad.

Este enfoque proactivo permitirá mantener la eficacia del modelo de seguridad y su adaptación a los desafíos emergentes.