



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código	SGSI-04
Documento	Política de Seguridad de la Información
Versión	2.1
Fecha de la versión	09/10/2026
Nivel de confidencialidad	Uso Interno
Aprobado por	Román Mesa Martínez (CEO)
Firma y fecha de la aprobación	09/10/2026 

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

Información del documento	
Entidad	Meta-Data Digital S.L.
Objeto	Exponer la Política de Seguridad de la Información de la Entidad, entendida como conjunto de principios básicos y líneas de actuación a los que la organización se compromete.
Ámbito de aplicación	Todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen información que se encuentre dentro del alcance del Sistema de Gestión de la Seguridad de la Información.
Usuarios	Todas las personas con acceso a la información dentro del alcance, independientemente de si el individuo es empleado o no de la Entidad (aplica también a contratistas, clientes o cualquier tercero que tenga acceso a la información).
Documentos relacionados	Alcance y Categorización.
Propietario del documento	Responsable de la Seguridad de la Información.
Validez y actualización	El propietario del documento es el responsable de verificar, y si es necesario, actualizar, el documento por lo menos una vez al año. Asimismo, el propietario del documento es competente para interpretar las dudas que puedan surgir en su aplicación y verificar su efectividad. Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios: - La cantidad de personal, interno y externo, que cumplen una función en el SGSI pero que no están familiarizados con esta política. - La existencia de responsabilidades ambiguas o ineficacia en la implementación y mantenimiento del SGSI. - El incumplimiento del SGSI en relación a la normativa, obligaciones contractuales y demás documentos internos de la organización.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

Anexos	
Código	Descripción
SGSI-04.01	Roles y responsabilidades en seguridad de la información
SGSI-04.02	Designación de responsables en la seguridad de la información
SGSI-04.03	Aceptación Responsable de la Seguridad
SGSI-04.04	Aceptación Responsable de la Información y del Servicio (Órgano Colegiado)
SGSI-04.05	Aceptación Responsable del Sistema
CON-ICT-2025-01 - TRUST IDENTITY SECURITY SOFTWARE.pdf	Contrato externalización Delegado de Protección de Datos
CON-ICT-2025-03 - INFORMATICA Y CONTROL DE NAVARRA TUDELA.pdf	Contrato externalización Administrador del sistema/de la seguridad del sistema

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

ÍNDICE

2. Alcance	6
3. Términos y definiciones	6
4. Principios fundamentales de esta Política	6
5. Capacidades del Sistema de Gestión de Seguridad de la Información	9
5.1 Prevención	9
5.2 Detección	9
5.3 Respuesta	9
5.4 Recuperación	10
6. Objetivos y medición	10
7. Misión de la Organización	10
8. Marco Normativo	10
9. Organización de la seguridad de la información	11
9.1 Comité de Seguridad de la Información	11
9.2 Roles, funciones y responsabilidades	12
9.2.1 Responsable de la Información	12
9.2.2 Responsable del Servicio	12
9.2.3 Responsable de la Seguridad de la Información	13
9.2.4 Responsable del Sistema	14
9.2.5 Administrador del Sistema/de la seguridad del Sistema	14
9.2.6 Delegado de Protección de Datos	15
9.3 Procedimiento de designación	15
9.4 Coordinación y resolución de conflictos	15
9.5 Usuarios	15
10. Datos personales	16
11. Evaluación de riesgos y controles	17
12. Seguridad de la información en nuevos proyectos	17
13. Desarrollo de la Política de Seguridad de la Información	18
14. Obligaciones del personal	19
15. Terceras partes	19

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

1. Introducción

La información es un activo que, al igual que otros activos importantes, es esencial para las actividades de la organización y, por consiguiente, necesita ser debidamente protegida. La información puede ser almacenada de muchas formas, incluyendo: formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato material (por ejemplo, papel), así como la información intangible que forma parte del conocimiento del personal.

Toda la información guardada y procesada por la organización está expuesta a ataques, errores, riesgos naturales (por ejemplo, inundaciones o incendios), etc. y está expuesta a vulnerabilidades inherentes en su uso.

Por tanto, este activo debe ser adecuadamente protegido, mediante controles y medidas de seguridad, frente a las distintas amenazas que puedan afectarle, independientemente de los soportes en la que se encuentre (papel o soporte digital), medios de transmisión, sistemas, equipos o personas que intervengan en su recogida, registro, tratamiento o supresión.

La Seguridad de la Información es la protección de este activo con la finalidad de asegurar que la información no está accesible a aquellas personas o entidades no autorizadas, que dicha información es veraz y no ha sido objeto de manipulaciones no autorizadas y que está disponible cuando se necesita.

Para ello, los sistemas de información 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 (ENS) y la vigente normativa de protección de datos personales, 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 de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en la realización de los proyectos.

La Seguridad de la Información es un proceso que requiere de medios técnicos y humanos, en la que es fundamental la máxima implicación y colaboración de todo el personal de la organización.

La Dirección es consciente del valor de la información y está profundamente comprometida con la política descrita en el presente documento.

El propósito de esta Política es establecer las directrices de alto nivel para definir, desarrollar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI).

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

Determina objetivos, principios y reglas básicas para la gestión de la seguridad de la información en la organización.

Consideración de factores medioambientales y cambio climático. La Dirección reconoce que los factores medioambientales, incluyendo los derivados del cambio climático (p. ej., disponibilidad energética, condiciones extremas, impacto en infraestructuras TIC o proveedores), pueden influir en la continuidad y resiliencia de los servicios y, por tanto, en la seguridad de la información. El SGSI incorporará la consideración de estos factores en su análisis del contexto y en la planificación de objetivos y recursos.

2. Alcance

Esta política se aplica a todos los sistemas de información y a todos los miembros de la organización, sin excepciones, así como a las empresas externas que accedan, gestionen o traten información de la organización.

3. Términos y definiciones

- **Confidencialidad:** es la propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** es la propiedad de la información por la cual solo es modificada por personas o entidades autorizadas y de una forma permitida, de manera que dicha información sea veraz y completa.
- **Disponibilidad:** es la propiedad de la información de ser accesible y estar lista para su uso a demanda de una entidad autorizada.
- **Trazabilidad:** es la propiedad o característica de la información consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- **Autenticidad:** es la propiedad o característica de la información consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Sistema de información:** es el conjunto de aplicaciones, servicios, activos de tecnologías de la información y otros componentes que se utilizan para manejar la información.
- **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de la Seguridad de la Información (SGSI):** conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar sus objetivos de negocio.
- **Riesgo:** estimación del nivel de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

4. Principios fundamentales de esta Política

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, en su transmisión, transporte, almacenamiento y hasta su borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

- **Principio de confidencialidad:** la información y los sistemas de información deberán ser accesibles únicamente para aquellas personas, órganos, entidades y/o procesos expresamente autorizados para ello. A esto se suma la obligación de secreto profesional de todo el personal que tenga acceso a la información.
- **Principio de integridad:** se deberá garantizar el mantenimiento de la integridad de la información, así como de los procesos de tratamiento de la misma, estableciéndose mecanismos para asegurar que los procesos de creación, recepción, tratamiento, almacenamiento y distribución de la información contribuyan a preservar que sea veraz y completa.
- **Principio de disponibilidad y continuidad:** se deberá garantizar un nivel de disponibilidad en los sistemas de información y se dotará de medidas necesarias para asegurar la continuidad de los servicios y su recuperación ante posibles contingencias graves.
- **Principio de trazabilidad:** se deberá mantener, en la medida de lo posible, una trazabilidad de la información y las entidades que la tratan, de forma que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- **Principio de autenticidad:** se deberá garantizar que las entidades que tratan la información son quien dicen ser, así como la fuente de la que proceden los datos.
- **Principio de gestión del riesgo:** se deberá habilitar un proceso metódico, sistemático y continuo de análisis, evaluación y tratamiento de los riesgos para la seguridad de la información como mecanismo básico sobre el que debe girar la gestión de la seguridad de la información.
- **Principio de proporcionalidad en costes:** la implantación de los controles y medidas de seguridad que mitiguen los riesgos de seguridad de la información deberá realizarse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará de que los recursos para el SGSI estén disponibles.
- **Principio de concienciación y formación:** se desarrollarán iniciativas que permitan al personal involucrado en el SGSI conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De la misma forma, se fomentará la formación específica en seguridad TIC de todas aquellas personas que gestionan y administran los sistemas de información y los dispositivos de red y telecomunicaciones.
- **Principio de mínimo privilegio:** los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- **Principio de prevención:** se desarrollarán planes y actuaciones específicas orientadas a prevenir la ocurrencia de incidentes relacionados con la seguridad de la información.
- **Principio de detección y respuesta:** se debe monitorizar la operación del sistema continuamente para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, respondiendo eficazmente, a través de los mecanismos establecidos, a los incidentes de seguridad que ocurran.
- **Principio de mejora continua:** se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad de la información planificados anualmente y el grado de eficacia de los controles y medidas de seguridad implantadas, con el fin de adecuarlos a la evolución de los riesgos y el entorno tecnológico cambiante.
- **Principio de la seguridad de la información en el ciclo de vida de los sistemas:** las especificaciones de seguridad de la información se incluirán en todas las fases del ciclo de vida de los sistemas y servicios, a través de los correspondientes procedimientos de control.
- **Principio de autorización y control de accesos:** el acceso controlado a los sistemas de información comprendidos en el alcance deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.
- **Principio de protección de las instalaciones:** los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.
- **Principios para la adquisición de productos de seguridad y contratación de servicios de seguridad:** en la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información dentro del alcance, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.
- **Principio de integridad y actualización de sistemas:** la inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.
- **Principio de protección de la información almacenada y en tránsito:** se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.
- **Principio de prevención ante otros sistemas de información interconectados:** se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- **Principio de registro de la actividad y detección de código dañino:** se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Se analizarán las comunicaciones entrantes y salientes, únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños relacionados.
- **Gestión segura de credenciales:** la organización utilizará un **gestor de contraseñas corporativo** para la generación, almacenamiento y compartición de credenciales; los detalles operativos se regulan en **POS-03** e **ITS-04.03**.
- **Principio de resiliencia y sostenibilidad del SGSI:** la gestión de la seguridad considerará, cuando proceda, los factores medioambientales y los efectos del cambio climático que puedan impactar en la confidencialidad, integridad y disponibilidad de la información o en la continuidad de los servicios, promoviendo prácticas eficientes (p. ej., uso de servicios cloud sostenibles, virtualización, teletrabajo) de forma proporcionada.

5. Capacidades del Sistema de Gestión de Seguridad de la Información

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

5.1 Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detección, los servicios deben monitorizar la operación de

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar con consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.3 Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

5.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

6. Objetivos y medición

El marco para establecer los objetivos anuales del SGSI es el siguiente:

- Gestionar los riesgos que existen para la seguridad de la información de una forma sistemática, completa y contrastada a nivel mundial.
- Aumentar la confianza de los clientes y otras partes interesadas, en cuanto a la seguridad de la información que nos depositan, y a la que tenemos (o podríamos) tener acceso.
- Cumplir con las obligaciones contractuales contraídas con los clientes, tanto externos como internos.
- Cumplir con las disposiciones y requisitos marcados por la normativa de protección de datos personales y el resto de leyes aplicables a la organización.
- Asegurar la mejora continua del SGSI para responder a los cambios futuros.
- Considerar, cuando sea relevante, **objetivos de eficiencia operativa del SGSI** (p. ej., consolidación/virtualización de recursos, uso de servicios con garantías de eficiencia

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

energética) siempre que contribuyan a la seguridad y resiliencia.

- **Revisar anualmente** si existen **factores medioambientales con impacto en la seguridad** (disponibilidad energética, continuidad de proveedores críticos, climatología extrema) e incorporar, en su caso, métricas y seguimiento en la Revisión por la Dirección.

La Dirección es la responsable de revisar este marco de objetivos y establecer un nuevo marco.

7. Misión de la Organización

Proporcionar soluciones integrales y avanzadas en ciberseguridad para proteger los datos, infraestructuras y sistemas críticos de nuestros clientes, fomentando la confianza y garantizando el cumplimiento de normativas internacionales.

8. Marco Normativo

Las leyes, reglamentos, y otra normativa, nacional o internacional, a la que la entidad está sujeta es la siguiente:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 32/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Sin carácter certificativo ni de conformidad normativa adicional, la organización **tiene en cuenta** las orientaciones relevantes de **ISO/IEC 27001:2022 enmienda 2024** respecto de la **consideración del cambio climático** en el contexto organizacional y la planificación del SGSI.

9. Organización de la seguridad de la información

9.1 Comité de Seguridad de la Información

Se constituye el **Comité de Seguridad de la Información** como el máximo órgano colegiado de decisión, supervisión y control del SGSI y del cumplimiento del **Esquema Nacional de Seguridad (ENS)**.

Su función principal es garantizar un proceso de toma de decisiones objetivo, basado en riesgos

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

y documentado, actuando como el principal mecanismo de coordinación entre los diferentes roles definidos en el marco del ENS.

Composición

- **Presidente:** El Director General (CEO).
- **Miembros internos:**
 - El **Responsable de la Seguridad**.
 - El **Responsable del Sistema**.
 - El **Órgano Colegiado Responsable de la Información y del Servicio** (compuesto por los anteriores).

Funciones

- Atender las inquietudes de la Dirección y de las diferentes áreas de la organización.
- Informar periódicamente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del SGSI y del cumplimiento del ENS.
- Elaborar y revisar la **Política de Seguridad de la Información**, para su aprobación por la Dirección.
- Aprobar la normativa, procedimientos e instrucciones técnicas relacionadas con la seguridad.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.
- Velar por la integración de los **requisitos de seguridad** en todos los proyectos y servicios desde su diseño.
- Supervisar los principales **riesgos residuales** y recomendar medidas de mitigación.
- Monitorizar el **proceso de gestión de incidentes**, auditorías y revisiones de seguridad.
- Aprobar planes de mejora y priorizar actuaciones en materia de seguridad.
- Resolver conflictos de responsabilidad entre diferentes roles o áreas.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- **Revisar anualmente** los posibles **efectos del cambio climático** y otros factores medioambientales en el **contexto de la organización y las partes interesadas**, y su repercusión en la continuidad y resiliencia de los servicios del alcance.

El **Responsable de la Seguridad** coordinará las reuniones del Comité, levantará acta de cada sesión y propondrá la incorporación o revocación de miembros, con la aprobación final de la Dirección.

9.2 Roles, funciones y responsabilidades

A continuación, se describen los roles establecidos conforme al **ENS** y su equivalencia con el modelo del SGSI:

9.2.1 Órgano Colegiado Responsable de la Información y del Servicio

Función: Determinar los requisitos de seguridad aplicables a la información y a los servicios, garantizando su protección, disponibilidad e integridad, y coordinando las decisiones entre los responsables técnicos y organizativos.

Responsabilidades:

- Establecer los requisitos de seguridad de la información y de los servicios prestados.
- Validar la clasificación de la información y las medidas de protección asociadas.
- Evaluar los impactos sobre la información y los servicios ante cambios o incidentes.
- Garantizar la coordinación entre el Responsable del Sistema y el Responsable de la Seguridad.
- Actuar como punto de contacto interno ante auditorías o revisiones ENS.

El órgano está integrado por:

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

9.2.2 Responsable de la Seguridad

Función: Coordinar e impulsar las medidas necesarias para garantizar la protección de la información y los servicios, así como supervisar la correcta implantación del ENS.

Responsabilidades:

- Coordinar las actividades de seguridad en toda la organización.
- Supervisar la gestión de incidentes, vulnerabilidades y revisiones periódicas.
- Promover la concienciación y formación en seguridad.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- Convocar y dirigir el Comité de Seguridad.
- Informar a la Dirección del estado de la seguridad.
- Garantizar el cumplimiento de las políticas y procedimientos del SGSI.

9.2.3 Responsable del Sistema

Función: Asegurar la operación, mantenimiento y disponibilidad de los sistemas bajo su responsabilidad, aplicando las medidas de seguridad aprobadas.

Responsabilidades:

- Implementar y mantener las medidas de seguridad técnicas.
- Controlar los accesos y configuraciones de los sistemas.
- Colaborar en la gestión de incidentes y auditorías técnicas.
- Validar los cambios de configuración antes de su implantación.

9.2.4 Administrador del Sistema / Seguridad del Sistema

Función: Ejecutar las tareas operativas y técnicas necesarias para mantener las medidas de seguridad, bajo la supervisión del Responsable del Sistema.

Responsabilidades:

- Implementar y monitorizar los mecanismos de seguridad (EDR, RMM, backups, etc.).
- Gestionar usuarios, permisos y privilegios.
- Supervisar las alertas y logs de seguridad.
- Colaborar en la investigación y resolución de incidentes.

9.2.5 Delegado de Protección de Datos (DPD)

Función: Asesorar y supervisar el cumplimiento de la normativa de protección de datos personales en la organización.

Responsabilidades:

- Velar por el cumplimiento del RGPD y la LOPDGDD.
- Promover la concienciación y formación en materia de privacidad.
- Atender y coordinar las solicitudes de ejercicio de derechos.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

En el documento **Roles y responsabilidades en la seguridad de la información** se encuentran más detalladas las funciones, responsabilidades y tareas de los diferentes roles relacionados con la seguridad de la información.

9.3 Procedimiento de designación

Los distintos roles ENS son designados formalmente por la Dirección mediante el documento SGSI-04.02 Designación de Responsables en la Seguridad de la Información y las correspondientes aceptaciones de responsabilidad (SGSI-04.03 a SGSI-04.05).

Los roles externalizados (Administrador del Sistema, DPD, Auditor Interno, etc.) se formalizan mediante contrato de prestación de servicios aprobado por la Dirección.

9.4 Coordinación y resolución de conflictos

Cualquier conflicto o falta de alineación entre roles será comunicado al **Responsable de la Seguridad**, quien convocará al **Comité de Seguridad de la Información** para analizarlo y resolverlo colegiadamente, dejando constancia mediante acta.

9.5 Usuarios

Cualquier persona que acceda a la información gestionada por la organización será considerada un usuario.

Los usuarios son responsables de su conducta cuando accedan a información o utilicen los sistemas de información de la organización. El usuario es responsable de todas las acciones realizadas con sus identificadores o credenciales personales.

Por tanto, los usuarios tienen la obligación de:

- Conocer y cumplir la Política de Seguridad de la Información, las normas, procedimientos e instrucciones correspondientes.
- Proteger y custodiar la información de la organización, evitando la revelación, transmisión o comunicación al exterior, borrado, mal uso o destrucción (accidental o no autorizada) de la misma, independientemente del soporte en el que se encuentre o los medios por los que ha sido accedida o conocida.

10. Datos personales

La organización trata datos personales y se preocupa por la adecuada protección de los mismos. El tratamiento de datos personales involucra una serie de riesgos relacionados con la pérdida de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de estos datos.

La gestión de riesgos de privacidad se alinearán con el análisis de riesgos de la seguridad. El DPD podrá, a petición del responsable del tratamiento, proporcionar asesoramiento y herramientas específicas tanto para esta gestión de riesgos, como para la realización de evaluaciones de impacto en la privacidad para los tratamientos, cuando sea requerido por un elevado nivel de riesgo.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

Los datos personales a proteger incluyen todos aquellos que son objeto de tratamiento por nuestra parte (ya sean datos de clientes, potenciales clientes, proveedores, trabajadores, contactos, colaboradores externos, etcétera).

Por ello, tanto la organización, como todo su personal, ya sea interno o externo, que esté involucrado de alguna forma en el tratamiento de datos personales, debe:

- Guardar secreto y confidencialidad de la información personal que trata.
- Proteger los datos personales que esté tratando y custodiarlos para que el personal no autorizado no tenga acceso a ellos.
- Cumplir con los principios de protección de datos (licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva).
- Garantizar que los interesados puedan ejercer sus derechos (información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y decisiones individuales automatizadas).
- Cumplir, y en su caso, hacer cumplir, los controles y las medidas de seguridad que la organización ha implantado para proteger la seguridad de los datos personales, evitando que pueda resultar comprometida la confidencialidad, integridad o disponibilidad de dichos datos.
- Comunicar inmediatamente, según los procedimientos habilitados para ello, las incidencias que puedan afectar a la seguridad de los datos personales y que puedan comprometer su confidencialidad, integridad o disponibilidad, así como el incumplimiento de los requisitos dispuestos por la normativa de protección de datos personales.
- Cumplir con todos los requisitos y obligaciones legales impuestas por la normativa de protección de datos personales.

Todos los sistemas de información se ajustarán a las medidas de seguridad que sean requeridas por la normativa según la naturaleza y finalidad de los datos personales que se traten y de acuerdo con el análisis de riesgos relativo a la protección de datos personales que se ha realizado.

La documentación relativa a la normativa de protección de datos personales, a la que tendrá acceso el Delegado de Protección de Datos, incluye el Registro de Actividades de Tratamiento y toda la documentación requerida por dicha normativa.

11. Evaluación de riesgos y controles

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- cuando cambien los servicios prestados o los activos que los soportan
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia de los distintos tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

12. Seguridad de la información en nuevos proyectos

Todo proyecto, iniciativa o implantación tecnológica dentro del alcance del SGSI deberá integrar la seguridad de la información desde su fase inicial y a lo largo de todo su ciclo de vida.

El gerente de proyecto, en coordinación con el Responsable de la Seguridad, deberá garantizar que los riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos sean identificados, evaluados y tratados de manera adecuada.

En particular:

- Los objetivos de seguridad deberán incluirse entre los objetivos del proyecto.
- Se realizará una evaluación de riesgos de seguridad de la información en una fase temprana del proyecto para identificar los controles necesarios, aplicando la metodología definida en el SGSI.
- Los requisitos de seguridad deberán definirse, documentarse y aprobarse antes de cualquier desarrollo o implantación, incluyendo aspectos como:
 - autenticación y control de acceso,
 - cifrado de la información en tránsito y en reposo,
 - protección frente a código dañino,
 - gestión de copias de seguridad y recuperación,
 - intercambio seguro de información y uso de medios cifrados.
- Los requisitos deberán revisarse y consensuarse con las partes interesadas relevantes, asegurando su trazabilidad y cumplimiento.
- El Responsable de Seguridad participará en las revisiones de seguridad del proyecto y en la validación final de cumplimiento antes de su cierre.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

- Toda la documentación generada (evaluaciones de riesgo, requisitos, aprobaciones y revisiones) se conservará como registro de proyecto seguro dentro del marco documental del SGSI.

El cumplimiento de estos principios se desarrolla operativamente en la POS-03 Norma de Uso de los Sistemas e Información, que establece el procedimiento para la gestión segura de proyectos y nuevas implantaciones, incluyendo la evaluación temprana de riesgos, la definición de requisitos de seguridad, las revisiones del Responsable de Seguridad y el registro de evidencias asociadas.

13. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información se desarrollará por medio de otras políticas de seguridad que afronten aspectos específicos (también denominada normativa de seguridad). Dichas políticas de seguridad estarán a disposición de todos los miembros de la organización que necesiten conocerlas, en particular para aquellos que administren los sistemas de información y comunicaciones.

La documentación relativa a la seguridad de la información estará disponible en el apartado relativo al SGSI, compartido en Google Cloud, con accesos restringidos y compartimentados por usuarios teniendo en cuenta el principio de privilegio mínimo. El acceso a la documentación se realiza a través de Google Workspace con verificación de usuario y doble factor de autenticación (2FA). La documentación será gestionada por el Responsable de Seguridad según los procedimientos internos de elaboración y control documental.

14. Obligaciones del personal

Todos los miembros de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y el resto de políticas de seguridad (normativa de seguridad), siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la entidad atenderán actividades de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la entidad, en particular a los de nueva incorporación.

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

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

15. Terceras partes

Cuando la organización preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán los canales de reporte y coordinación y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la organización utilice los servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de las políticas de seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dichas políticas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerlas. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

 Meta-Data	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	SGSI-04
		Uso Interno

Gestión de registros guardados en base a este documento					
Código	Nombre	Ubicación	Responsable del archivo	Controles para la protección del registro	Tiempo de retención
N.A.					3 años

Control de versiones			
Versión	Fecha	Autor	Descripción de la modificación
1.0	27/12/2024	Román Mesa Martínez	Versión inicial del documento
2.0	23/10/2025	Román Mesa Martínez	Mejoras en la sección 12 Seguridad de la información en nuevos proyectos y Se incorpora la consideración del cambio climático y de factores medioambientales en la política del SGSI (enmienda 2024 ISO/IEC 27001): introducción, principio de resiliencia y sostenibilidad, objetivos y medición, referencia en marco normativo y función del Comité de Seguridad.
2.1	09/10/2026	Adriana Arias Chaves	Corrección de la referencia a las aceptaciones de responsabilidad (SGSI-04.03 a 04.05).