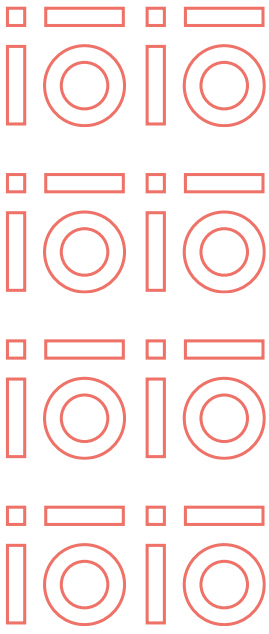
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



Contenido

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado en 16/02/2026 por el Comité de Seguridad de **REDFLEXION CONSULTORES S.L., & REDFLEXIA S.L.**

Esta política de seguridad de la información está vigente desde la fecha de aprobación hasta que sea reemplazada por una nueva versión.

2. INTRODUCCIÓN

2.1 Justificación de la política de seguridad de la información

REDFLEXION CONSULTORES, S.L. & REDFLEXIA S.L. depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

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. Es por ello que, el Esquema Nacional de Seguridad (Real Decreto 311/2022 de 3 de mayo, ENS en adelante), en su artículo 11 establece que "*Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente*".

Esto implica que las diferentes áreas de la organización 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.

Todas las áreas 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 las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

2.2 Objetivos y alcance de los servicios prestados

La presente Política de Seguridad aplica a los diferentes servicios prestados en su actividad diaria, en concreto:

Los sistemas de información que dan soporte a:

- Los servicios de consultoría de comercio exterior (solo REDFLEXION).
- Los servicios profesionales en el ámbito de la consultoría y asesoría empresarial, de protección de datos y cumplimiento normativo.
- Los servicios en materia de ciberseguridad, análisis de riesgos y protección de sistemas informáticos.
- Los servicios de consultoría estratégica y tecnológica.

Esta política se aplica a todos los sistemas de información de **REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L.** a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de **REDFLEXION CONSULTORES, S.L. & REDFLEXIA S.L.**

Asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de la misma, con el fin de ofrecer a todos sus grupos de interés las mayores garantías, con los siguientes objetivos:

- Garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con celeridad a los incidentes.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Proteger la información de posibles amenazas, de forma que se asegure la continuidad de las líneas de negocio
- Minimizar los posibles daños causados
- Maximizar el retorno de las inversiones y las oportunidades de negocio.

2.3 Principios rectores de la política

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, dando una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios para la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

3. MARCO NORMATIVO

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
- 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 (en adelante RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad de la Información complementa/se integra junto con otras políticas de la **REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L.** en diferentes materias:

- Anexo 1 (MS-01) Política de calidad y seguridad de la información, basada en la norma ISO 9001 e ISO 27001.

La Política, junto con el documento de referencia, estarán a disposición de todos los miembros de **REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L.** y se ubicará para su consulta en www.redflexion.com

5. ORGANIZACIÓN DE LA SEGURIDAD

Tal como indica el artículo 12 del ENS, La seguridad deberá comprometer a todos los miembros de la organización.

La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. Se establecen los siguientes roles en la organización relacionados con la Seguridad de la Información: responsable de la información, responsable del servicio, responsable de la seguridad de la información, responsable del sistema, administrador de la seguridad del sistema, responsable de la seguridad física y responsable de la gestión del personal.

5.1 Roles en seguridad de la información:

5.1.1 Responsable de la información:

La figura del **Responsable de la Información** tiene las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los tratamientos de datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

5.1.2 Responsable del servicio:

Se ha designado **responsables del Servicio** a cada uno de los responsables de unidades funcionales, a quienes les corresponde las siguientes funciones:

- En cuanto al RGPD, por delegación del Responsable del tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto.
- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

5.1.3 Responsable de la seguridad de la información:

Se ha designado un responsable de Seguridad de la Información, a quien le corresponderá llevar a cabo las siguientes funciones:

- Coordinará y controlará las medidas definidas en el Registro de actividades del tratamiento y en general se encargará del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.

- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

5.1.4 Responsable del sistema:

Se ha designado un responsable del Sistema, al que le corresponden las siguientes funciones:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los

Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.

- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

5.1.5 Administrador de la seguridad del sistema:

Se ha designado un Administrador de la Seguridad del Sistema, al que, como tal, le corresponden las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

En caso de ocurrencia de incidentes de seguridad de la información:

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.

- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

5.1.6 Responsable de la seguridad física:

Se ha designado un responsable de Seguridad Física, al que le corresponderá implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

5.1.7 Responsable de la gestión del personal:

Se ha designado un responsable de Gestión de Personal, al que le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

5.2 Comité de seguridad de la información

Se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

Podrán acudir a requerimiento del Comité cualquier otro usuario y/o responsables cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por el RGPD.

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

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de la organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
- Se asesorará de los temas que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:
    - Grupos de trabajo especializados internos, externos o mixtos.
    - Asesoría interna y/o externa.
    - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

En caso de ocurrencia de incidentes de seguridad de la información:

- Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente.

5.3 Jerarquía en el proceso de decisiones y mecanismos de coordinación

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

El Administrador de la Seguridad del Sistema reporta al Responsable del Sistema:

- Incidentes relativos a la seguridad del sistema.
- Acciones de configuración, actualización o corrección.

El Responsable del Sistema informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.

El Responsable del Sistema informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.

El Responsable del Sistema reporta al Responsable de la Seguridad:

- Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
- Resumen consolidado de los incidentes de seguridad
- Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

El Responsable de la Seguridad informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

Cuando exista un Comité de Seguridad de la Información, el Responsable de la Seguridad reporta a dicho *comité* como secretario:

- Resumen consolidado de actuaciones en materia de seguridad.
- Resumen consolidado de incidentes relativos a la seguridad de la información.
- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

El Responsable de la Seguridad informa a la Dirección de la Organización, según lo acordado en el Comité de Seguridad de la Información.

5.4 Procedimiento de designación de personas

La **Dirección de la Organización** nombrará formalmente y designará en esta política:

- Al Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
- A los Responsables del Servicio; puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
- Al Responsable de la Seguridad, que debe reportar directamente a la Dirección o, cuando exista, al Comité de Seguridad de la Información.
- Al Responsable del Sistema, que debe reportar directamente a la Dirección o, cuando exista, al Comité de Seguridad de la Información.

La **Dirección de la Organización** designa a la persona Responsable del Sistema:

- A propuesta del Responsable de la Información tratada, cuando el Sistema de información trate una única información.
- A propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.
- Directamente cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.

La **Dirección de la Organización** designa al Administrador de Seguridad del Sistema a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

5.5 Datos de carácter personal

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes, así

como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades del Tratamiento.

6. FIGURAS VINCULADAS A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

6.1 Funciones y obligaciones del responsable de tratamiento

El Responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

REDFLEXION CONSULTORES, S.L. & REDFLEXIA como responsable de tratamiento, trata sus datos de carácter personal contenidos en sus sistemas de información, y que derivan de la prestación de los servicios públicos atribuidos a nivel de competencias.

Las funciones del Responsable del tratamiento son:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- Deberá informar a los titulares de los datos los derechos que les asisten y en los términos en los que pueden ejercerlos.
- Deberá excluir del tratamiento los datos relativos al afectado que se oponga al tratamiento de los mismos.
- Deberá cesar en la utilización o cesión ilícita de los datos cuando así lo requiera el interesado.
- Obligación de hacer efectivo el derecho de rectificación o supresión del interesado en el plazo máximo de 1 mes.
- Notificar las rectificaciones o cancelaciones efectuadas en los datos personales a quien se haya comunicado dichos datos, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

6.2 Funciones y obligaciones del delegado de protección de datos

El DPO puede ser una persona física o un órgano colegiado, cuyas funciones se señalan en el artículo 39 del Reglamento (UE) 679/2016, así como los artículos 36 y 37 de la Ley Orgánica 3/2018, y se ocupa de la aplicación de la legislación sobre privacidad y protección de datos en la entidad en la que desarrolla sus funciones.

REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L. ha designado un Delegado de Protección de Datos, Blanca Muñoz Galdeano, perteneciente a REDFLEXION CONSULTORES, S.L. - B73182925 & REDFLEXIA S.L. - B12912028

El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
d) cooperar con la autoridad de control;
e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá ser capaz de:

a) Recabar información para determinar las actividades de tratamiento,
b) analizar y comprobar la conformidad de las actividades de tratamiento, e
c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
d) Recabar información para supervisar el registro de las operaciones de tratamiento.
e) Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
f) Asesorar sobre:
    - Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos
    - Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
    - Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
    - Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.
    - Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
    - Si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes al Reglamento.
g) Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
h) Asesorar al responsable del tratamiento sobre:
    - Qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos,
    - qué áreas deben someterse a auditoría de protección de datos interna o externa,
    - qué actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

El DPO deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos conocimientos, habilidades o destrezas necesarias que tiene que saber o poseer el Delegado de Protección de Datos para llevar a cabo una de las funciones propias de su puesto.

Estas funciones genéricas del DPO se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
2. Identificación de las bases jurídicas de los tratamientos.
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
4. Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
9. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
10. Diseño e implantación de políticas de protección de datos.
11. Auditoría de protección de datos.
12. Establecimiento y gestión de los registros de actividades de tratamiento.
13. Análisis de riesgos de los tratamientos realizados.
14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
18. Realización de evaluaciones de impacto sobre la protección de datos
19. Relaciones con las autoridades de supervisión
20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

6.3 Funciones y obligaciones de usuarios con acceso a datos

Todos los empleados de la entidad están sujetos a funciones y obligaciones. Todo el personal de la organización que disponga de acceso a los datos de carácter personal debe cumplir con las siguientes obligaciones:

- No se permite la difusión de datos de carácter personal ni confidencial perteneciente a la entidad. Estando obligado a guardar secreto de la información incluso terminada la relación laboral.
- El usuario se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias, no notificar una incidencia será considerada una omisión del deber del trabajador.
- El usuario se responsabilizará de todos los accesos que se realicen bajo su identificador y contraseña, por tanto, no deberá revelar la contraseña.
- El usuario se responsabilizará siempre que abandone el puesto de trabajo de cerrar su sesión o bloquear el equipo con contraseña.
- No se podrán instalar aplicaciones en los sistemas de la entidad sin el consentimiento del delegado de protección de datos.
- No se permite la copia de datos de carácter personal, en soportes, sin la autorización expresa del delegado de protección de datos.
- El usuario se responsabilizará de guardar la información de los correos electrónicos en las carpetas del servidor correspondiente, no manteniéndolos en el gestor de correo electrónico de forma indefinida.

6.4 Funciones y obligaciones de encargado de tratamiento

Los encargados del tratamiento tienen como misión realizar las tareas ordinarias para el desarrollo efectivo de las funciones para las que ha sido creado el tratamiento por cuenta del Responsable del tratamiento.

En este sentido, el apartado 8 del artículo 4 del RGPD define al Encargado de Tratamiento como *la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*.

El Encargado del Tratamiento deberá aplicar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado

Igualmente deberá implementar las medidas de seguridad a que se refiere el párrafo anterior y que aparecerán estipuladas en el contrato con el Responsable del Tratamiento.

En concreto, sus funciones son las de:

- Tratar los datos del tratamiento.
- Realizar el control de tratamiento, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a las adiciones y cancelaciones.
- Controlar los soportes de seguridad.
- Control y acceso de contraseñas.
- Mantenimiento del registro de incidencias.
- Crear una lista para las situaciones en la que un afectado no desee que sus datos personales se almacenen en el tratamiento.
- Dar traslado al responsable del tratamiento de aquellas solicitudes de ejercicio de derecho que se reciban por parte de los interesados.

REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L. deberá llevar a cabo un documento actualizado donde se identificarán los encargados de tratamiento que están prestando servicios, así como la indicación de la formalización del pertinente contrato con estos prestadores de servicios con acceso a datos.

7. GESTIÓN DE RIESGOS

7.1 Justificación

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

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

7.2 Criterios de evaluación de riesgos

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

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

7.3 Directrices del tratamiento

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

7.4 Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.
Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de ese Servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

7.5 Necesidad de realizar o actualizar las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

8.1 Prevención de incidentes

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.
El ENS a través de su artículo 19 establece que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 17 del citado ENS define que los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

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:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- 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.

8.2 Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 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.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

8.3 Respuesta ante incidentes

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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).

8.4 Recuperación ante incidentes y planes de continuidad

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.

9. CONCIENCIACIÓN Y FORMACIÓN

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de **REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L.** y a todas las actividades, de acuerdo con el principio de Seguridad como proceso integral recogido en el Artículo 6 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

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

Todos los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

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

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

10. TERCERAS PARTES

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.
Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la **REDFLEXION CONSULTORES S.L. & REDFLEXIA S.L.** pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

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

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

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

11. REVISIÓN Y APROBACIÓN DE CAMBIOS EN POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 12 del ENS.
Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

12. DOCUMENTACIÓN COMPLEMENTARIA

La Política de Seguridad de la Información se cumplimentará con documentos más precisos que ayudan a llevar a cabo lo propuesto. Para ello se utilizarán:

- Normas de seguridad.
- Guías de seguridad
- Procedimientos de seguridad

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Anexo. glosario de términos

Análisis de riesgos
Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
Datos de carácter personal
Cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes
Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos
Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad
Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Información
Caso concreto de un cierto tipo de información.

Política de seguridad
Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad
Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información
Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad
El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio
Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema
Persona que se encarga de la explotación del sistema de información.

Servicio
Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información
Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.