Política de Seguridad de la Información

CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 31/03/2026 por Comité de Seguridad.

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

EDENRED ESPAÑA depende de los sistemas TIC (Tecnologías de la Información y las 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 seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a 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), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades administrativas de EDENRED ESPAÑA tienen presente 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.

Por tanto, para EDENRED ESPAÑA, 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 para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 7 del ENS, con la aplicación de las medidas que se relacionan a continuación.

2.1 PREVENCIÓN

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

Para garantizar el cumplimiento de la política, EDENRED ESPAÑA:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

2.2 DETECCIÓN

EDENRED ESPAÑA establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS, Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3 RESPUESTA

EDENRED ESPAÑA establece las siguientes medidas:

- 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).

2.4 RECUPERACIÓN

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

3. ALCANCE DE EDENRED ESPAÑA

El sistema de información da soporte a los servicios de **diseño, desarrollo, comercialización y soporte de productos de retribución flexible y beneficios para empleados**, así como la administración operativa y técnica de dichos procesos, prestados por EDENRED ESPAÑA, será objeto de certificación al **Esquema Nacional de Seguridad (ENS)**, de acuerdo con la **Declaración de Aplicabilidad vigente.**

4. PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos del EDENRED ESPAÑA, de forma que pueda estar coordinada e

integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

- Responsabilidad determinada: En los sistemas TIC se determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

5. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

EDENRED ESPAÑA establece como objetivos de la seguridad de la información los siguientes:

1. Evidenciar el compromiso de EDENRED ESPAÑA con la seguridad de la información
2. Reducir el riesgo de potenciales ciberataques
3. Reducir el daño ocasionado por potenciales incidentes
4. Reducir el riesgo de robo o pérdida de información sensible
5. Alinear la estrategia de seguridad de la información con los objetivos comerciales, la estrategia y los planes de negocio de la organización

6. MARCO NORMATIVO

El marco normativo que afecta al desarrollo de las actividades y competencias de EDENRED ESPAÑA está constituido por normas jurídicas estatales orientadas a la administración electrónica, a la

seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

EDENRED ESPAÑA, para lograr el cumplimiento de los artículos del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y seguridad por defecto (artículo 19)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica (artículo 9) e integridad y actualización del sistema (Artículo 2)

EDENRED ESPAÑA ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

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

Gestión de personal (artículo 14) y profesionalidad (artículo 15)

Todos los miembros de EDENRED ESPAÑA, dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de

concienciación continua para atender a todos los miembros, 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.

Gestión de la seguridad basada en los riesgos (artículo 6) y análisis y gestión de riesgos (artículo 13)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

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

Incidentes de seguridad (artículo 24), prevención, reacción y recuperación (artículo 7)

EDENRED ESPAÑA ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

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

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

EDENRED ESPAÑA establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- 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, EDENRED ESPAÑA dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 8) y prevención ante otros sistemas interconectados (artículo 22)

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

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

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

Función diferenciada (artículo 10) y organización e implantación del proceso de seguridad (artículo 12)

EDENRED ESPAÑA ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos (artículo 16)

EDENRED ESPAÑA ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 17)

EDENRED ESPAÑA ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 18)

Para la adquisición de productos, EDENRED ESPAÑA tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito (artículo 21) y continuidad de la actividad (artículo 25)

EDENRED ESPAÑA ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tabletas, soportes de información, redes abiertas, etc.).

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

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

Registros de actividad (artículo 23)

EDENRED ESPAÑA ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1 CRITERIOS UTILIZADOS PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

EDENRED ESPAÑA, teniendo en cuenta lo establecido en el antedicho Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las pautas establecidas en la Guía *CCN-STIC-801 "Responsabilidades y Funciones en el ENS"*, para organizar la seguridad de la información emprenderá las siguientes acciones:

i. **Designará roles de seguridad**: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.
ii. **Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información**. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2 ROLES Y ÓRGANOS DE LA SEGURIDAD DE LA INFORMACIÓN

En EDENRED ESPAÑA, en el marco del ENS, los roles y órganos de la Seguridad de la Información, serán los siguientes.

Los nombres están recogidos en el Acta de Constitución de Comité de Seguridad, recogido en Referencias de este documento.

- Responsable de la Información y el Servicio
- Responsable de Seguridad.
- Responsable del Sistemas.

Asimismo, se ha compuesto un Comité de Seguridad de la Información, compuesto por:

- Director
- Secretario: Responsable de Seguridad, Información y Servicios
- Vocales:
  - Responsable del Sistema,
  - Delegado de protección de datos
  - Responsable de RRHH

Los Responsables de Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar.

El Comité de Seguridad de la Información se reunirá, con carácter ordinario, al menos una vez cada Seis (6) meses pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

El Secretario/a del Comité levantará actas de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

7.3 RESPONSABILIDADES DE LOS ROLES ASOCIADOS AL ESQUEMA NACIONAL DE SEGURIDAD

7.3.1 Responsable de la Información y de los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) ya los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo. Pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

7.3.2 Responsable de la Seguridad

Serán funciones del Responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.

- Participará en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema
- Gestionar los procesos de certificación
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

7.3.3 Responsable del Sistema

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
    - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
    - Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

7.3.4 Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a EDENRED ESPAÑA y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de EDENRED ESPAÑA en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.

El Delegado de Protección de datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:

- Recabar información para determinar las actividades de tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en el principio de la protección de datos por diseño y por defecto.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.
- Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

7.3.5 Responsable de RRHH (People)

Serán funciones del Responsable de Recursos Humanos:

- Gestionar el ciclo completo del personal con responsabilidades relacionadas con la seguridad de la información, incluyendo selección, contratación, cambios de puesto y bajas, velando porque se cumplan los principios establecidos en el Esquema Nacional de Seguridad (ENS).
- Definir y supervisar el cumplimiento de las obligaciones de confidencialidad del personal, asegurando la firma, actualización y custodia de los compromisos de confidencialidad, privacidad y uso aceptable de los sistemas.
- Promover y coordinar la formación y concienciación en materia de seguridad de la información, en colaboración con el Responsable de Seguridad y el Comité de Seguridad de la Información.
- Comunicar al Responsable de Seguridad y al Responsable del Sistema cualquier cambio organizativo que afecte a usuarios con accesos, privilegios o responsabilidades relevantes para la seguridad.
- Gestionar el alta, modificación y baja de personal, garantizando que:
    - Se asignen perfiles adecuados a las funciones del puesto.

  - Se retiren todos los accesos al finalizar la relación laboral o cambio de funciones.
  - Se sigan los procedimientos autorizados para la incorporación y salida segura del personal.
- Velar por el cumplimiento de la normativa interna de seguridad y protección de datos en todos los procesos vinculados al personal.
- Asegurar que el personal conoce y cumple las políticas, normas y procedimientos internos relacionados con la seguridad de la información, protección de datos y uso de sistemas.
- Colaborar en la gestión de incidentes de seguridad relacionados con el personal, facilitando información o medidas disciplinarias cuando sea necesario conforme a las políticas internas.

7.3.6 Director del comité de Seguridad de la Información

Serán funciones del Director del Comité de Seguridad de la Información:

- Presidir y coordinar las reuniones del Comité de Seguridad de la Información, asegurando su correcto funcionamiento y la participación de los distintos roles implicados en la seguridad.
- Dirigir y supervisar la definición, aprobación y actualización del marco de seguridad de la entidad, incluidos políticas, normas, procedimientos y roles del ENS.
- Asegurar la correcta evaluación y categorización de los sistemas de información, en colaboración con el Responsable de Seguridad y el Responsable del Sistema.
  - Revisar y validar las propuestas elevadas al Comité, incluyendo:
  - Requisitos de seguridad de información y servicios.
  - Resultados del análisis de riesgos.
  - Declaración de Aplicabilidad.
  - Planes de mejora de la seguridad.
  - Cambios relevantes en los sistemas de información.
- Impulsar la implantación del Plan Director de Seguridad, supervisando su cumplimiento y priorizando las acciones necesarias según el riesgo y las necesidades estratégicas de la organización.
- Velar por la adecuada coordinación entre los distintos responsables ENS (Información, Seguridad, Sistema, RRHH, Protección de Datos, etc.).
- Asegurar la disponibilidad de recursos y apoyo organizativo para el correcto funcionamiento del sistema de gestión de seguridad de la información.
- Revisar periódicamente el estado de la seguridad, incluyendo:
  - Informes de auditoría interna o externa.
  - Resultados de monitorización y explotación del sistema.
  - Situación de los incidentes de seguridad.
- Elevar a la Dirección General o Gerencia las decisiones estratégicas, riesgos significativos, necesidades de inversión y cualquier asunto relevante relacionado con la seguridad.
- Garantizar el cumplimiento del Esquema Nacional de Seguridad y la alineación con otras normativas aplicables (protección de datos, directrices sectoriales, etc.).

7.4 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Serán funciones del Comité de Seguridad de la Información:

- Aprobar y coordinar las propuestas de los Responsables de la Información y los Servicios sobre los niveles de seguridad de la información y de los servicios y asumir las funciones de los Responsables de la Información y los Servicios en las actuaciones en que se considere necesario.
- Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asumir temporalmente (hasta el nombramiento de Delegado de Protección de Datos) las funciones de éste.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos 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.
    - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por el Órgano de Administración.
    - Elaborar la normativa de Seguridad de la Información para su aprobación por el Órgano de Administración.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
    - Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones del EDENRED ESPAÑA en materia de seguridad de la Información y protección de datos.

7.5 PROCEDIMIENTOS DE DESIGNACIÓN

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por el comité de dirección de **EDENRED ESPAÑA.**

El nombramiento se revisará en Acta de Comité de Seguridad de la Información.

8. DATOS PERSONALES

EDENRED ESPAÑA solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

EDENRED ESPAÑA publicará en la web pública su política de seguridad.

9. OBLIGACIONES DEL PERSONAL

Todo el personal de EDENRED ESPAÑA comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al 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 o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

10. GESTIÓN DE RIESGOS

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

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

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

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.

- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

11. NOTIFICACIÓN DE INCIDENTES

De conformidad con lo dispuesto en el marco normativo vigente del Esquema Nacional de Seguridad (Real Decreto 311/2022), EDENRED ESPAÑA notificará al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables a los organismos o unidades de EDENRED ESPAÑA a los que sea de aplicación dichos documentos.

b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.

c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Comité de Dirección de EDENRED ESPAÑA la aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de EDENRED ESPAÑA, siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad de EDENRED ESPAÑA en materia de protección de datos.

La normativa de seguridad y, muy especialmente, la Política de seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos, será conocida y estará a disposición de todos los miembros de EDENRED ESPAÑA, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet, en soporte papel, esta documentación será custodiada por el Servicio de Informática.

13. TERCERAS PARTES

Cuando EDENRED ESPAÑA preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **EDENRED ESPAÑA** utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecen 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 de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información 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.

14. MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.

b) Revisión de los servicios e información y su categorización.

c) Ejecución con periodicidad anual del análisis de riesgos.

d) Realización de auditorías internas o, cuando procedan, externas.

e) Revisión de las medidas de seguridad.

f) Revisión y actualización de las normas y procedimientos.