

Manual de seguridad de la información

07 de abril de 2026

Contenido

1.	Introducción	4
1.1.	Finalidad	4
1.2.	Ámbito de aplicación	4
1.3.	Definiciones	5
1.4.	Documentación y contactos de referencia	5
2.	Seguridad de la información	5
2.1.	Misión, Visión y Contexto de la Organización	9
2.2.	Objetivos	10
2.3.	Organización de la ciberseguridad	10
2.3.1.	Triple línea de defensa Ciberseguridad Global Iberdrola	10
2.3.2.	El Comité de Seguridad de la Información de NCE (1er línea de defensa)	11
2.3.3.	Roles y Responsabilidades de ciberseguridad de la 1º línea de Defensa	13
2.4.	Marco normativo	18
2.5.	Concienciación y formación	19
2.6.	Gestión de riesgos	19
2.7.	Revisión, aprobación del documento y gestión documental	19

Historial de versiones:

Versión	Autor	Aprobador	Estado	Motivo del problema/cambio	Fecha
v1	Negocio Clientes España	CEO Negocio Clientes	Anulado	<ul style="list-style-type: none"> Primera versión 	20/06/2025
v2	Negocio Clientes España	CEO Negocio Clientes	Anulado	<ul style="list-style-type: none"> Cambios menores 	12/01/2026
V3	Negocio Clientes España	CEO Negocio Clientes	Anulado	<ul style="list-style-type: none"> Cambios menores. Inclusión de un matiz en el alcance para clarificar el papel del certificado de ISO transversal. 	14/01/2026
V4	Negocio Clientes España	CEO Negocio Clientes	Aprobado	<ul style="list-style-type: none"> Cambios menores e inclusión de mayor detalle en los requisitos mínimos y principios básicos del ENS y en el gobierno del cuerpo normativo. 	07/04/2026

1. Introducción

1.1. Finalidad

En el presente **Manual de seguridad de la información** (también llamado la Política de Seguridad de la Información de Negocio Clientes España) se **establecen directrices generales de seguridad de la información que Negocio Clientes España** (en adelante, NCE) debe aplicar para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida a la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, ocasionando pérdida o mal uso de los activos, daño en su imagen y reputación y/o interrupción de los procesos que soportan el negocio. A su vez, se definen los objetivos de seguridad de la información.

Mediante la aprobación de este Manual, NCE manifiesta su **determinación y compromiso en alcanzar un nivel de seguridad de la información adecuado a sus necesidades** que **garantice la protección de los activos** de forma homogénea y la **gestión adecuada de los riesgos** asociados. Así mismo, se **compromete** a la **mejora continua** del Sistema de Gestión Seguridad de la Información y al **cumplimiento** de los **objetivos** marcados y de toda la **regulación** que le es de aplicación, tanto interna como externa.

1.2. Ámbito de aplicación

Este documento es de aplicación, con carácter obligatorio, a todo el personal de NCE, así como a las entidades colaboradoras que intervienen en la utilización y protección de la información propiedad de NCE y los sistemas que la soportan. Los incumplimientos de ciberseguridad, así como las posibles sanciones están recogidas en el convenio colectivo de Iberdrola.

El presente Manual (o Política de Seguridad de la Información) debe ser accesible para todos los miembros de NCE y disponible para las partes interesadas.

El alcance que viene definido en el certificado para la ISO 27001 es el siguiente: “El sistema de información que da soporte al proceso de contratación por canales digitales y el proceso de Recarga Pública en negocio Clientes España según declaración de aplicabilidad vigente a fecha de emisión del certificado.” Queda excluida de este alcance la gestión de seguridad de la información que realizan las áreas transversales (Ciberseguridad Global y España, IT España, Servicios Generales España, Seguridad y Resiliencia España) ya que está incluida en el certificado de AENOR SI-0167. El detalle de las actividades en el alcance de cada SGSI se establece en las declaraciones de aplicabilidad de cada SGSI.

El alcance que viene definido en el certificado para el Esquema Nacional de Seguridad (ENS) nivel medio es el siguiente: “El sistema de información que da soporte al proceso de contratación a través de los sistemas operacionales y al proceso de Recarga Pública en Negocio Clientes España de acuerdo al documento de categorización vigente.”

Hay que destacar que el proceso de contratación a través de sistemas operacionales se encuentra contenido dentro del proceso de contratación a través de canales digitales.

Es importante destacar que una parte relevante de los requisitos exigidos por los controles del ENS vienen cubiertos por los controles de la ISO 27001 (siguiendo lo definido en la guía 825 del CCN-CERT), por lo que se puede usar el certificado de AENOR SI-0167 para el cumplimiento de dichos requisitos.

1.3. Definiciones

Se proporcionan las siguientes definiciones para permitir un entendimiento común de los conceptos de ciberseguridad relevantes incluidos en este documento:

- **CoE:** Center of Excellence. Departamento cuyo propósito es obtener productos digitales que aporten valor al negocio y al cliente final.
- **NCE:** Negocio Clientes España. Es uno de los 3 principales negocios de Iberdrola.
- **BISO:** Business Information Security Officer. Ostenta un rol de CISO pero de la primera línea de defensa, encontrándose en el negocio del que es BISO.
- **RGPD:** El Reglamento General de Protección de Datos (RGPD), o GDPR en inglés, es un reglamento de la Unión Europea que regula el tratamiento de datos personales de las personas físicas dentro de la UE.
- **SGSI:** El sistema de gestión de la seguridad de la información es un marco estructurado usado para gestionar, controlar y mejorar la seguridad de su información de manera integral.

1.4. Documentación y contactos de referencia

- Política de Seguridad Corporativa.
- Política de Riesgos de Ciberseguridad.
- Política de Protección de Datos Personales.
- Política de Resiliencia Operativa.
- Series CCN-STIC: Se ha tomado como referencia las normas, instrucciones, guías y recomendaciones que son de aplicabilidad desarrolladas por el Centro Criptológico Nacional (CCN) para el cumplimiento de los estándares de seguridad exigidos por el Esquema Nacional de Seguridad.
- ISO/IEC 27014.
- ISO/IEC 27001.
- Código del buen gobierno de la ciberseguridad – CNMV.
- Marco de Ciberseguridad del Grupo Iberdrola.
- ciberseguridad_negocio_clientes_es@iberdrola.es

2. Seguridad de la información

Las medidas implementadas en NCE para salvaguardar la seguridad de la información tienen como piedra angular asegurar lo siguiente:

- **Confidencialidad:** propiedad de la información, por la que se garantiza que es accesible únicamente a personal autorizado a acceder a dicha información.
- **Integridad:** propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

- **Disponibilidad:** propiedad de la información, por la que se garantiza que es accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.
- **Autenticidad:** propiedad de la información, por la que se garantiza que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad de la información, por la que se garantiza que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Así mismo, se tienen en cuenta los siguientes **principios básicos**:

- **Alcance estratégico:** La seguridad de la información cuenta con el compromiso y apoyo de todos los niveles de la entidad y se coordina e integra con el resto de las iniciativas estratégicas de forma coherente.
- **Seguridad como proceso integral:** la seguridad se entiende en Iberdrola Negocio Clientes 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 se considera como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de la seguridad basada en los riesgos:** La gestión de la seguridad basada en los riesgos identificados permite el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecen en función de los riesgos a que está sujeta la información y sus sistemas y son proporcionales al riesgo que tratan, debiendo estar justificadas. Se tiene también en cuenta los riesgos identificados en el tratamiento de datos personales.
- **Prevención, detección, respuesta y conservación:** Este principio se aplica a 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:** Tal como se define en el modelo de gobierno definido en el presente documento, Iberdrola cuenta con un modelo de 3 líneas de defensa. El sistema de información dispone de una estrategia de protección constituida por múltiples capas de seguridad, de forma que, cuando una de las capas sea comprometida, se minimiza el impacto y se desarrolla una reacción adecuada.
- **Vigilancia continua:** Iberdrola implementa medios de detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos.
- **Reevaluación periódica:** Existe, 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 están diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionan la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- **Diferenciación de responsabilidades:** Las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas. También están diferenciados el responsable de la información, del servicio, de seguridad y del sistema. El presente

documento detalla las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos

Por último, el actual Manual de Seguridad (la Política de Seguridad) se establece de acuerdo con los principios básicos señalados en el capítulo II del Esquema Nacional de Seguridad y se desarrolla aplicando los siguientes requisitos mínimos (los cuales son ampliados en los distintos documentos que componen el cuerpo normativo, y en los controles definidos en el Anexo II del Esquema Nacional de Seguridad):

- **Organización e implantación del proceso de seguridad:** Iberdrola Clientes España establece y mantiene un proceso de seguridad estructurado que asegura la correcta definición, implantación y supervisión de todas las medidas necesarias. La seguridad compromete a todos los miembros de la organización. Tanto a nivel documental como a nivel operativo, dicho proceso de seguridad se encuentra estructurado en los distintos dominios de ciberseguridad (gobierno, riesgos, gestión de activos, protección de la información, gestión de la identidad y accesos, cifrado, seguridad física, bastionado, gestión de vulnerabilidades, gestión del cambio, *antimalware*, seguridad en red, S-SDCL, riesgos en terceros, monitorización, gestión de incidentes, continuidad, cumplimiento). La política de seguridad (el presente manual) define en el apartado 2.3.4 el modelo de gobierno de la ciberseguridad. Para aquellos servicios externalizados, se cuenta con un POC (o persona de contacto) para la seguridad de la información.
- **Análisis y gestión de los riesgos:** Se realiza un análisis de riesgos anual sobre los diferentes activos dentro del alcance de la certificación con el fin de identificar amenazas, evaluar su impacto y aplicar controles adecuados para su mitigación, siguiendo con la metodología interna definida (basada en una metodología de reconocido prestigio internacional). Todos aquellos riesgos cuyo nivel supera el apetito definido, deben ser tratados con un plan de acción para disminuir el riesgo por debajo del apetito.
- **Gestión de personal:** El personal de Negocio Clientes España cumple con las responsabilidades asignadas en materia de seguridad (definidas en la norma de Uso Aceptable y en la Normativa de Utilización de Medios Informáticos, la cual es aceptada por todos los empleados al comenzar a trabajar en Iberdrola) y recibe la formación necesaria y periódica para desempeñar sus funciones de manera segura.
- **Profesionalidad:** Todo el personal implicado en actividades relacionadas con la seguridad actúa con diligencia, competencia y respeto a las normas internas de la compañía. Se cuentan con diversos planes de formación y concienciación para continuar mejorando las capacidades de los empleados de forma anual. La seguridad de los sistemas de información está atendida y es revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Para todo el personal que presta servicios de seguridad a Iberdrola Negocio Clientes España se les exige de manera objetiva y no discriminatoria, que sean profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

- **Autorización y control de los accesos:** El acceso a los sistemas y recursos se limita únicamente a usuarios autorizados y se aplicarán mecanismos de control para garantizar su uso adecuado. Se llevan a cabo de forma periódica revisión de accesos de los permisos, para asegurar que los mismos siguen siendo los correctos.
- **Protección de las instalaciones:** Las instalaciones físicas cuentan con medidas de protección que aseguran la integridad y protección física de los recursos frente a las amenazas físicas y medioambientales y evitar accesos no autorizados. Se cuenta con diversas normas y procedimientos de seguridad física que regulan este apartado.
- **Adquisición de productos de seguridad y contratación de servicios de seguridad:** La selección de productos y servicios de seguridad se realiza conforme la metodología interna definida en Iberdrola, basada en la gestión de riesgos que garantiza que estos son evaluados y tratados de forma adecuada de forma previa y posterior a la contratación. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación del Esquema Nacional de Seguridad, se utilizarán aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.
- **Mínimo privilegio:** Los usuarios disponen únicamente de los privilegios necesarios para el desempeño de sus funciones, minimizando riesgos asociados al uso indebido. Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y se asegura que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados. Se eliminan o desactivan, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema se intenta buscar siempre que sea sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario. Por último, se aplican guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas. Dichas guías de configuración de seguridad se basan en estándares de reconocido prestigio.
- **Integridad y actualización del sistema:** Los sistemas se mantienen actualizados y protegidos para asegurar su integridad y para reducir vulnerabilidades. Se siguen los tiempos establecidos internamente para la solución de vulnerabilidades. La inclusión de cualquier elemento físico o lógico en el inventario, o su modificación, requiere autorización formal previa.
- **Protección de la información almacenada y en tránsito:** La información es tratada de forma segura de acuerdo con la categoría del sistema, aplicando medidas de protección tanto cuando se almacena como cuando se transmite (usando cifrado cuando se trasmite por redes ajenas a la compañía).

- **Prevención ante otros sistemas de información interconectados:** Se establecen y documentan los riesgos, procesos y controles que garantiza la seguridad en las interconexiones con otros sistemas, evitando propagación de riesgos o accesos no autorizados.
- **Registro de la actividad y detección de código dañino:** Se cuentan con diversos mecanismos de registro y monitorización que permitan identificar actividades anómalas y detectar posibles incidentes. Se cuenta con un SOC 24x7 y un equipo de respuesta ante incidentes propios.
- **Incidentes de seguridad:** Iberdrola Clientes España dispone de procedimientos para la gestión eficaz de incidentes de seguridad, asegurando una identificación, clasificación, escalado, análisis, respuesta y resolución rápida y coordinada. Los planes de respuesta ante incidentes se testean de forma periódica.
- **Continuidad de la actividad:** Se han documentado e implementado planes de continuidad que permiten mantener operativas las funciones críticas ante interrupciones o contingencias. Se cuenta con un proceso de gestión de copias de seguridad para asegurar la continuidad del dato.
- **Mejora continua del proceso de seguridad:** El proceso de seguridad es revisado de forma continua para identificar oportunidades de mejora y adaptar las medidas a nuevos riesgos o requisitos. Esto se realiza mediante las propias revisiones internas del sistema de gestión, así como las diferentes auditorías internas y externas que se realizan anualmente.

2.1. Misión, Visión y Contexto de la Organización

La **Misión del Grupo** se basa en la creación de valor de forma sostenible en el desarrollo de todas sus actividades, para sus accionistas, trabajadores, clientes y demás grupos de interés y, en general, para los ciudadanos y la sociedad en su conjunto. La Misión se complementa por la **Visión**, que refleja la aspiración a ser el grupo multinacional líder en el sector energético que protagonice un futuro mejor creando valor de forma sostenible con un servicio de calidad para las personas, de modo eficiente, seguro, sostenible y respetuoso con el medioambiente. La Misión y la Visión del Grupo se asientan en el firme compromiso con unos **Valores**, entre los que destacan el impulso dinamizador, la fuerza integradora y la Energía Sostenible. En este último valor, la **Seguridad** se posiciona como un pilar esencial para su consecución. Esto se traduce en la consolidación de la Seguridad Integral como un pilar fundamental en la toma de decisiones de Iberdrola, promoviendo continuamente prácticas de seguridad innovadoras y sostenibles en todas las operaciones, contribuyendo de esta manera a la resiliencia, confiabilidad y al éxito global del Grupo en un entorno híbrido en constante transformación.

Negocio Clientes España ocupa un lugar destacado dentro de la estrategia empresarial de Iberdrola S.A. (en adelante, Iberdrola o la Organización), como una de sus líneas de negocio principales. Esta línea se enfoca en la comercialización y suministro de energía, así como en la provisión de productos y servicios centrados en la descarbonización.

En el ámbito de **Negocio Clientes España**, Iberdrola se dedica a satisfacer las necesidades del usuario final, ofreciendo soluciones energéticas sostenibles. Su objetivo es proporcionar energía limpia y servicios innovadores que contribuyan a la transición hacia un modelo energético más respetuoso con el medio ambiente. Además, dentro de esta línea de negocio, Iberdrola también

desempeña un papel clave en la compraventa de energía en los mercados mayoristas, consolidando así su posición en el mercado energético.

Junto a Negocio Clientes España, Iberdrola desarrolla otras líneas de negocio igualmente relevantes. Entre ellas se encuentra el **Negocio de Redes Grupo**, que se dedica a la construcción, operación y mantenimiento de infraestructuras eléctricas, tales como líneas de transmisión, subestaciones y centros de transformación. Estas infraestructuras son fundamentales para garantizar el suministro eficiente de energía eléctrica desde los centros de producción hasta el usuario final.

Asimismo, Iberdrola se involucra activamente en el **Negocio Renovables Grupo**, donde se especializa en la generación de energía eléctrica a partir de fuentes renovables, como la energía eólica, termo solar, fotovoltaica, entre otras. Esta línea de negocio refleja el compromiso de Iberdrola con la generación de energía limpia y sostenible, contribuyendo así a la mitigación del cambio climático y la preservación del medio ambiente.

Para mayor detalle del propósito corporativo de la compañía, se puede consultar los recursos publicados [Hacia un propósito corporativo global - Iberdrola](#)

2.2. Objetivos

Asimismo, se identifican los 6 objetivos de seguridad de la información, teniendo en cuenta los principios básicos de actuación establecidos en la [Política de Seguridad Corporativa](#):

- **Gobierno:** Establecer y mantener un modelo de gobierno para gestionar, operar y mejorar la seguridad de la información a través de un enfoque orientado a la gestión del riesgo.
- **Identificación:** Comprender el entorno e identificar los riesgos para sus sistemas, activos, datos y capacidades.
- **Protección:** Diseñar e implementar salvaguardas para minimizar el nivel de riesgo en relación con la materialización de una posible ciberamenaza.
- **Detección:** Monitorizar los eventos de información de la Organización e identificar potenciales comportamientos anómalos que puedan derivar en la materialización de una posible ciberamenaza.
- **Respuesta:** Tomar todas las acciones pertinentes para gestionar, analizar, responder, escalar y mitigar los incidentes identificados.
- **Recuperación:** Restaurar los activos y operaciones afectados por un incidente de ciberseguridad.

2.3. Organización de la ciberseguridad

Iberdrola se organiza de forma que se controla y se garantiza la seguridad del Sistema de Gestión por medio de la asignación, comunicación y coordinación de los diferentes roles y responsabilidades en materia de seguridad de la información a fin de garantizar que el Sistema de Gestión cumple con los requisitos exigidos en materia de seguridad de la información.

2.3.1. Triple línea de defensa Ciberseguridad Global Iberdrola

El sistema de control interno de Iberdrola y las sociedades de grupo se configuran tomando como referencia las mejores prácticas internacionales. Por ello, este sistema de control está basado en un aseguramiento combinado en torno a tres líneas de defensa, proporcionando una visión integrada de cómo las diferentes partes de la Organización interactúan de una manera efectiva y coordinada, haciendo más eficaces los procesos de gestión y control interno de los riesgos relevantes de la Organización.

A continuación, se proporciona más detalle sobre cada una de las líneas de defensa:

- **Primera línea de defensa:** incluye todas las funciones propietarias de los riesgos, en este sentido, las primeras líneas designarán Business Information Security Officer (BISOs) que liderarán la definición y supervisarán la implantación de un plan de ciberseguridad específico por parte de sus organizaciones de negocio, alineado con la estrategia, las normas y los marcos generales de ciberseguridad y se asegurará de que estén soportados por recursos (personas y presupuesto) adecuados en materia de ciberseguridad. En esta línea se localiza TAS (IT), los Negocios y las Áreas Corporativas.
- **Segunda línea de defensa:** incluye aquellas funciones que definen el marco general de gobierno y control de la ciberseguridad, establecen normas, estándares y criterios globales y soportan y supervisan la implantación de los planes de ciberseguridad de la primera línea, así como la identificación de riesgos relevantes. En esta línea se localiza Riesgos Corporativos, Seguridad y Resiliencia Corporativa y Ciberseguridad.
- **Tercera línea de defensa:** proporciona el más alto nivel de independencia y objetividad en el aseguramiento de la eficacia del gobierno corporativo, la gestión de riesgos y los controles internos, incluyendo la forma en que la primera y la segunda línea de defensa logran los objetivos de gestión y control de riesgos. En esta línea se localiza el departamento de Auditoría Interna, las Auditorías Externas y las Auditorías regulatorias.

2.3.2. El Comité de Seguridad de la Información de NCE (1er línea de defensa)

El Comité de Seguridad de la Información de NCE es el máximo órgano de gobierno de la ciberseguridad al que asiste la Alta Dirección (y los Responsables de Servicio e Información), y liderado por el Responsable de Seguridad (BISO), que se encarga de establecer y supervisar la estrategia de gestión de los riesgos de ciberseguridad. Este se reúne al menos 2 veces al año.

Las funciones del Comité del SG están recogidas en el cuerpo normativo del Sistema de Gestión de la organización, aunque destacan entre otras:

- **Revisar y aprobar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.**
- **Atender las inquietudes de la Dirección de Negocio clientes y de los diferentes departamentos que sean invitados al comité.**
- Servir como **foro para informar regularmente del estado de la seguridad de la información a la Alta Dirección**
- **Realizar anualmente la reunión de revisión por dirección** exigida por la ISO 27001 y el ENS.
- **Revisar y ratificar el modelo de gobierno de ciberseguridad**, así como sus posibles cambios periódicos. Así mismo, **resolver los conflictos de responsabilidad en materia de ciberseguridad.**
- **Monitorizar y aprobar los resultados de los análisis de riesgos** periódicos de ciberseguridad de la organización.
- **Revisar y ratificar periódicamente la Política de Seguridad de la Información** (el presente documento) y los distintos documentos que componen el cuerpo normativo.
- **Velar por el cumplimiento de la normativa legal y sectorial de aplicación.**
- **Promover la realización de las auditorías periódicas.**
- **Promover la comunicación, coordinación de esfuerzos y concienciación de ciberseguridad.**
- **Velar por que la seguridad de la información se tenga en cuenta en los proyectos TIC.**
- **Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad.**

- **Aprobar planes de mejora de la seguridad de la información de la organización para conseguir la mejora continua.**
- **Priorizar las actuaciones** en materia de seguridad.
- **Promover la mejora continua** del sistema de gestión de la seguridad de la información.

2.3.3. Roles y Responsabilidades de ciberseguridad de la 1º línea de Defensa

Alta Dirección

- **Proveer y asegurar que los recursos necesarios** para la planificación, implantación, revisión y mejora del SGSI (Sistema de Gestión de la Seguridad de la Información) estén disponibles, aprobando los presupuestos de ciberseguridad.
- **Asegurar** que las **responsabilidades** para los roles pertinentes a la seguridad de la información **se asignen y comuniquen** dentro de NCE.
- **Asegurar** que el SGSI **alcanza los objetivos y resultados** de seguridad de la información y se cumple con la política de seguridad.
- **Aplicar las medidas para la gestión de riesgos de ciberseguridad y supervisar su implantación efectiva.** Para ello, deben estar informados de todos los criterios de aceptación de riesgos y sus correspondientes niveles y cumplir con todo lo definido en los procedimientos internos de gestión de riesgos y excepciones.
- **Asegurar** que se **organizan periódicamente formaciones en materia de ciberseguridad** para todos los empleados.
- **Participar y promover** la realización el comité de revisión por Dirección (**Comité de Ciberseguridad de Negocio Clientes España**).
- Responsable de velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- **Garantizar que se realizan las auditorías internas y externas** necesarias para la correcta revisión periódica del SGSI.
- Realizar todas las **funciones** que le **correspondan** como **participante** en el **comité de ciberseguridad** de Negocio Clientes España.
- **Promover la mejora continua** de ciberseguridad.

Responsable de la Información y del Servicio

- **Aprobar**, dentro de su ámbito de actuación y competencias, los **requisitos de la información y servicio**.
- **Determinar los niveles de seguridad de la información y servicio**, valorando los impactos de los incidentes que afecten a la seguridad de la información. Para ello, el Responsable de la Información y del Servicio solicitará informe del Responsable de la Seguridad. Los criterios seguidos para fijar los niveles de seguridad vendrán en la guía del CCN-CERT definida a tal efecto y en documentación interna de Iberdrola.
- **Colaborar** (contando con la participación del responsable de la Seguridad y el Responsable del Sistema) **en participar en la realización de los preceptivos análisis de riesgos** de los activos de los que es responsables y en la selección de las salvaguardas que requiere.
- Responsable de **aceptar los riesgos residuales respecto de la información y servicios** (o activos) de los que es responsable calculados en el análisis de riesgos.
- **Responsable del uso que se haga de la información** y, por tanto, de su protección. Para ello se apoyará en el Responsable de Seguridad, el Responsable del Sistema y el Responsable de Ciberseguridad del CoE.
- **Asegurar que se implementan las medidas necesarias sobre sus activos para tratar de minimizar los posibles elementos adversos que puedan conllevar un incidente** de seguridad sobre ellos. Para ello se apoyará en el Responsable de Seguridad, en el de Ciberseguridad del CoE y en el equipo de ciberseguridad.
- **Asegurar que se incluyen las especificaciones de seguridad en el ciclo de vida de su servicio** (y sistemas que lo componen), acompañadas de los correspondientes procedimientos de control. Para ello se apoyará en el Responsable de Seguridad, en el de Ciberseguridad del CoE y en el equipo de ciberseguridad
- **Cumplir con las tareas formativas de ciberseguridad** que le sean asignadas en el plan de formación y concienciación.

Responsable de Seguridad (BISO y Responsable del SGSI de NCE):

Máximo responsable de ciberseguridad de NCE, siendo el responsable de determinar las decisiones para satisfacer los requisitos de seguridad de la información y los servicios. Lidera el reporte a la Alta Dirección.

- Como Responsable del sistema de gestión de seguridad de la información (SGSI), es **responsable de liderar la planificación, implantación, operación, mantenimiento, supervisión y mejora continua del sistema de gestión de seguridad de la información.**
- **Mantener 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 Información de la organización.
- **Definir los objetivos** de seguridad de la información a nivel de NCE y los recursos necesarios para poder cumplirlos y someterlos a aprobación. Así mismo, se encargará de supervisar el cumplimiento de dichos objetivos.
- **Fomentar que la Dirección esté implicada en la implantación, mantenimiento y mejora continua del SGSI.** Así mismo, liderar el reporte periódico del estado y nivel de cumplimiento del SGSI a la Dirección.
- **Elaborar y someter a la aprobación de la Alta Dirección la estrategia** y políticas de seguridad, que deberán incluir las medidas de gestión de riesgos de ciberseguridad, técnicas y organizativas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciber incidentes que afecten a la organización y los servicios.
- **Diseñar e implementar el modelo de gobierno de ciberseguridad** de NCE.
- **Representar a NCE** (geografía concreta) **en los posibles grupos de trabajo** de ciberseguridad (riesgos, cultura, etc.) a nivel España y Global dentro de Iberdrola.
- **Liderar el departamento de ciberseguridad y a todos los recursos** humanos en él contenido.
- **Gestionar los recursos económicos designados** para el departamento de **ciberseguridad** de NCE, priorizando los planes en función de los recursos disponibles.
- **Supervisar la estrategia de gestión de riesgos.**
- **Reporte y comunicación del estado de la ciberseguridad en el área de NCE la Alta Dirección.**
- **Supervisar y desarrollar la aplicación del cuerpo normativo.** Así mismo, llevar a cabo la evaluación y coordinación en la implementación de controles periódicos de seguridad en los sistemas y servicios que le sean de aplicación.
- **Aprobar los documentos** que le correspondan según los flujos de aprobación marcados.
- **Supervisar el cumplimiento de la normativa** aplicable en materia de seguridad de las redes y sistemas de información, tomando todas las medidas necesarias para garantizar su cumplimiento.
- **Liderar** los procesos de **auditoría** del SGSI.
- Actuar como **capacitadora de buenas prácticas y estándares en seguridad** de las redes y sistemas de información.
- Elaborar y suscribir el **documento de aplicabilidad** de sistemas o activos.
- **Remitir a las autoridades de control**, a través de los CSIRT nacionales de referencia, sin dilación indebida, **las notificaciones de incidentes** que tengan efectos perturbadores en la prestación de los servicios y de las vulnerabilidades detectadas.
- **Recopilar, preparar y suministrar información o documentación a la autoridad de control y a los CSIRT nacionales nacional de referencia.**
- **Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad de control**, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

- **Velar por el cumplimiento de empresas externas y proveedores** de los criterios de seguridad de la información establecidos por la entidad.
- Definir y aprobar el plan de respuesta a incidentes de NCE. Así mismo, se encargará de **gestionar y liderar los incidentes** de ciberseguridad de acuerdo con las responsabilidades fijadas por los documentos que gobiernan la gestión de incidentes.

El Responsable de Seguridad **no dependerá jerárquicamente del Responsable del Sistema.**

Responsable Ciberseguridad CoE (Center of Excellence)

Encargado de gestionar la ciberseguridad de los activos de CoE, **colaborando** estrechamente con el **Responsable de Seguridad de la Información (BISO)** de NCE en materia de seguridad, y asegurando la mejora continua de la ciberseguridad del CoE. El detalle de sus funciones se encuentra recogido en el cuerpo normativo del Sistema de Gestión de la organización.

Responsable del Sistema

Entre las principales responsabilidades destacan:

- **Gestión y/o supervisión del desarrollo, operación y mantenimiento del sistema** de información durante todo su ciclo de vida. La operación es responsabilidad directa de Sistemas Corporativos para aquellos activos desplegados en su infraestructura.
- **Encargado de desarrollar la forma concreta de gestionar la implantación de la seguridad en el sistema definidas por el Responsable de Seguridad** (y el Responsable de ciberseguridad del CoE) y de la **supervisión de la operación diaria** del mismo, **pudiendo ser ejecutada por administradores, operadores o sistemas corporativos** (incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento).
- **Definir la topología y la gestión del sistema de información**, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- **Supervisar y asegurar la identificación de vulnerabilidades y amenazas sobre los activos de los que es responsable**. Para ello, se apoyará en el equipo de ciberseguridad.
- **Cerciorarse** (apoyándose en el departamento de ciberseguridad) **de que las medidas de seguridad se integren adecuadamente** en el marco general de seguridad.
- **Adoptar** las medidas correctoras adecuadas de acuerdo con las evaluaciones y auditorías de seguridad.
- **Proponer la suspensión de la operación de alguna información, de algún servicio o del sistema en su totalidad**, durante el tiempo que estime prudente y **hasta la satisfacción de las modificaciones prescritas en el caso de apreciar deficiencias graves de seguridad** que pudieran afectar a satisfacción de los requisitos establecidos. Para ello se puede apoyar en el equipo de ciberseguridad. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los Responsables de la información y los servicios afectados y la Responsable de la Seguridad.
- **Asistir a las tareas formativas de ciberseguridad** que le sean asignados en el plan de formación y concienciación.

Técnico de ciberseguridad

Las principales responsabilidades del técnico de ciberseguridad (que formará parte del equipo de ciberseguridad) son el **apoyar en todas las tareas de ciberseguridad que le sean asignadas por el Responsable de Seguridad (BISO) y/o su Responsable de ciberseguridad del CoE**.

Propietario del activo/riesgo asociado

- **Conocer** toda la **información relevante al activo**.
- **Asegurar** que el **activo** está correctamente **inventariado**, clasificado y protegido debidamente.
- **Definir y revisar periódicamente restricciones de acceso y clasificación de activos** importante, teniendo en cuenta las políticas aplicables de control de acceso.
- Supervisar el estado de los activos.

- **Conocer los riesgos de seguridad de la información asignados.**
- **Aprobar el plan de tratamiento de riesgos** de seguridad de la información.
- **Aceptar los riesgos residuales de seguridad** de la información.
- **Supervisar el estado** de los riesgos.
- **Mantenerse actualizado sobre las amenazas y riesgos emergentes**, pudiéndose apoyar para ello en el Responsable de Seguridad de la Información (BISO) y todo el departamento de ciberseguridad.

Empleados de Negocio Clientes España

Las funciones y responsabilidades en materia de ciberseguridad de los empleados están recogidas en el cuerpo normativo del Sistema de Gestión de la organización.

El resto de los elementos que componen el modelo de gobierno de ciberseguridad (organigrama, matriz RASCI, flujos de comunicación, designación y revocación de roles, etc.) de NCE se encuentran definidos en el cuerpo normativo del SGSI.

2.4. Marco normativo

- **Privacidad de datos**
 - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
 - 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.

- **Otra legislación nacional**
 - Ley de Coordinación y gobernanza de la ciberseguridad, de 2025.
 - Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión
 - Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
 - Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
 - Ley 59/2003, de 19 de diciembre, de firma electrónica.
 - Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.
 - Ley 10/2021, de 9 de julio, de trabajo a distancia.
 - Código civil y penal.

- **Otra legislación o regulación internacional**
 - Normativa PCI – DSS, de Junio 2024.
 - Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER).
 - IA Act.

- **Esquema Nacional de Seguridad**
 - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
 - Guías CCN-STIC.
 - Instrucciones Técnicas de Seguridad de conformidad con el Esquema Nacional de Seguridad (Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas) y de Auditoría de la Seguridad de los Sistemas de Información (Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública).

- **UNE-ISO/IEC 27001**
 - UNE-ISO/IEC 27001:2023 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
 - UNE-ISO/IEC 27002:2023 Código de buenas prácticas para la Gestión de la Seguridad de la información.

2.5. Concienciación y formación

Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información, para la implantación y seguimiento de la presente Política en materia de seguridad de la información.

Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de NCE, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación general y específica necesaria e imprescindible en todos los niveles de la organización de NCE.

2.6. Gestión de riesgos

NCE identifica y, cuando proceda, evalúa y categoriza los riesgos y oportunidades inherentes a las actividades, procesos y servicios, planificando las acciones necesarias para su tratamiento, previniendo los efectos no deseados y potenciando los efectos favorables de los mismos.

Los procesos de apreciación de riesgos de seguridad de la información y tratamiento de estos se encuentran documentados en documentos corporativos y propios de NCE.

En relación con los riesgos que se derivan del tratamiento de los datos personales, se seguirán todos los documentos que rigen el gobierno de la gestión de la protección de datos.

2.7. Revisión, aprobación del documento y gestión documental

El presente manual de seguridad de la información (que hace de Política de Seguridad de la Información para el alcance del ENS y la ISO 27001) es aprobado formalmente por el CEO de NCE y tiene carácter imperativo sobre toda la organización de NCE. Estará sujeta a un proceso de revisión regular que lo adapte a nuevas circunstancias, técnicas u organizativas, y evite que quede obsoleto. Se revisará al menos de forma anual, para asegurar su continua oportunidad, idoneidad, completitud y precisión de lo que la Política establezca y sea sometido a aprobación formal por la Alta Dirección.

Así mismo, NCE cuenta con el documento “Procedimiento de elaboración de documentación” en el que se definen las líneas maestras que rigen el gobierno del cuerpo normativo. Todos los empleados dentro del alcance tienen acceso al cuerpo normativo a través del SharePoint habilitado a tal efecto. Los tipos de documentos más relevantes del cuerpo normativo son los manuales (aprobados por el CEO del negocio), los procedimientos de ciberseguridad (aprobados por el BISO/Responsable de Seguridad de Negocio Clientes España) donde se define a nivel operativo los diferentes dominios de ciberseguridad y los registros. Estas tipologías de documentos deben ser revisadas y actualizadas de forma anual. El manual más importante y que se encuentra en la cúspide de la pirámide del cuerpo normativo de Negocio Clientes España, es el Manual de Seguridad de la información (el presente documento), que hace de Política de Seguridad para el alcance de la ISO y el ENS. La gestión del cuerpo normativo de ciberseguridad es responsabilidad del equipo de ciberseguridad de Negocio Clientes España (inventariado, actualización/revisión anual, archivado, etc.). A nivel de Corporación, Iberdrola cuenta también con el cuerpo normativo (normas, metodologías, procedimientos, etc.) de Seguridad y Resiliencia, Ciberseguridad España y Ciberseguridad Global, gestionado por dichos departamentos y de acceso a todos los empleados en la intranet.