grupo elecnor

# Política de Seguridad de la información y Ciberseguridad

# ÍNDICE

## 1. INTRODUCCIÓN

El Consejo de Administración de Elecnor, S.A. (**"Elecnor Holding"** o la **"Sociedad"**) en su condición de sociedad cotizada, tiene legalmente atribuida como facultad indelegable la determinación de las políticas y estrategias generales de la Sociedad y del Grupo del que es entidad dominante (**"Grupo Elecnor"** o **"Grupo"**), facultad recogida asimismo en la Política de Gobierno Corporativo y en el Reglamento del Consejo de Administración.

La presente *Política de Seguridad de la Información y Ciberseguridad* (la **"Política"**) asume el compromiso de Elecnor Holding y de las sociedades que forman parte del Grupo, de garantizar la seguridad de las redes y los sistemas de información en los que se apoyen los diferentes procesos de negocio, de manera que refuerce su Resiliencia Operativa Digital, alineando sus prácticas con la normativa vigente que resulte de aplicación, así como con sus valores corporativos.

En este sentido, Elecnor Holding se compromete a desarrollar en su Grupo las máximas capacidades en materia de Ciberseguridad, reduciendo así las amenazas para los sistemas de red y de información utilizados para prestar servicios esenciales en sectores fundamentales, de modo que sus productos y servicios generen beneficios sostenibles y se alineen con los más altos estándares éticos y legales.

La presente Política forma parte de la estrategia de seguridad de Elecnor Holding como sociedad cabecera del Grupo, con la finalidad de que el uso de las redes y sistemas de información responda al respeto del derecho de todas las partes interesadas a la salvaguarda de los más altos estándares de Ciberseguridad y privacidad, teniendo en cuenta al respecto las actividades y estructura del Grupo y, en particular, su presencia en sectores críticos como el desarrollo de infraestructuras y energías renovables.

De conformidad con los objetivos referidos, el Consejo de Administración de la Sociedad ha aprobado la presente Política que se proyecta sobre el Grupo y se integra en el Sistema de Gobierno Corporativo de la Sociedad.

## 2. DEFINICIONES

A los efectos de la presente Política, se deberán tener en consideración las siguientes definiciones:

- **Análisis de Riesgos:** proceso sistemático cuyo fin es la identificación, análisis y evaluación de riesgos que puedan afectar a la información en alguna de sus dimensiones de seguridad.
- **Comité de Seguridad de la información e Inteligencia Artificial:** comité de composición interdisciplinar con responsabilidades de supervisión y regulación para adoptar cualquier resolución, con relevancia en materia de Ciberseguridad e Inteligencia Artificial en Elecnor Holding y su Grupo, con el objetivo de garantizar que las medidas para la gestión de riesgos en seguridad de la información sean idóneas y que cualquier actividad de la organización que tenga especial relevancia esté alineada con los valores y políticas que se proyectan sobre el Grupo Elecnor (el "Comité").
- **Ciberseguridad:** todas las actividades necesarias para garantizar la seguridad de la información, la protección de las redes y de los sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas.
- **Datos personales:** toda información sobre una persona física identificada o identificable. Esto incluye cualquier dato que, directa o indirectamente, pueda ser utilizado para identificar a una persona como nombres, fotografías, direcciones de correo electrónico, datos bancarios, información sobre redes sociales, ubicación, información médica o dirección IP de un ordenador, entre otros. Los Datos Personales están protegidos por diversas legislaciones y se deben seguir prácticas adecuadas para su recogida, tratamiento y almacenamiento de cara a respetar los derechos de privacidad de las personas involucradas.
- **Gestión de riesgos:** actividades coordinadas para dirigir y controlar en el Grupo Elecnor los riesgos identificados en materia de Ciberseguridad.
- **Gestión de incidentes:** conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un Incidente de Ciberseguridad, así como a resolverlo e incorporar medidas de evaluación del desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en problemas relevantes.

- **Incidente de Ciberseguridad (o Ciberincidente):** suceso inesperado o no deseado que pueda comprometer la disponibilidad, autenticidad, trazabilidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos.
- **Profesional:** los miembros de los órganos de administración, directivos, trabajadores, colaboradores, estudiantes en prácticas y becarios del Grupo Elecnor con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios, su nivel jerárquico, su ubicación geográfica o funcional y de la sociedad del Grupo para la que presten sus servicios.
- **Responsable:** directores, mandos intermedios o cualquier otra persona con responsabilidad para tomar decisiones en materia de Ciberseguridad.
- **Resiliencia operativa digital:** la capacidad de la entidad para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente, el uso de servicios prestados por proveedores terceros de servicios de tecnologías de la información y comunicaciones (**"TIC"**), toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza el Grupo Elecnor y que sustentan la prestación continuada de servicios y su calidad, incluso en caso de perturbaciones.
- **Tratamiento de datos:** cualquier operación o conjunto de operaciones realizadas sobre Datos Personales, o conjuntos de éstos, ya sea por procesos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, almacenamiento, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Vulnerabilidad:** cualquier debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado.

Salvo que se disponga expresamente lo contrario en cualquier apartado de la presente Política, las definiciones en singular incluyen el plural y viceversa.

## 3. OBJETO

La presente Política y los principios básicos establecidos en ella tienen como objetivo permitir al Grupo desplegar las estrategias, procedimientos, tecnologías y estándares de Ciberseguridad necesarios para desarrollar un marco operativo y de control adecuado, en cuanto alineados con los objetivos de negocio y de la seguridad de los datos, de las redes y sistemas de información del Grupo Elecnor.

Y ello de conformidad con la regulación aplicable y teniendo en cuenta a las distintas partes interesadas.

## 4. ÁMBITO DE APLICACIÓN

Esta Política es aplicable a todas las divisiones y filiales que integran el Grupo Elecnor, así como a los proveedores y socios que presenten servicios para o se relacionen con el Grupo.

Sin perjuicio de lo dispuesto en el párrafo anterior, en aquellas sociedades participadas en las que esta Política no sea de aplicación, la Sociedad promoverá en lo posible, a través de sus representantes en sus órganos de administración, el alineamiento de sus políticas propias con las de la Sociedad, en el marco en todo caso del respeto a la autonomía de decisión de las sociedades participadas.

Además, esta Política resultará también aplicable, en lo que proceda, a las uniones temporales de empresas, *joint ventures* y otras asociaciones equivalentes, ya sean estas nacionales o extranjeras, cuando cualesquiera de las sociedades que integran el Grupo Elecnor tengan el control de su gestión y siempre dentro de los límites legalmente establecidos.

Es responsabilidad de todos los Profesionales y sujetos obligados por la Política, leer y comprender el contenido de la misma, así como observar y cumplir sus directrices, principios y procesos en el desarrollo de su trabajo, en la medida en que la comprensión y adherencia a las definiciones y principios establecidos en ella es fundamental para garantizar que se alcancen los objetivos de Ciberseguridad en todo el Grupo Elecnor.

## 5. PRINCIPIOS GENERALES

El Grupo Elecnor entiende la Ciberseguridad como un elemento fundamental para proteger los activos de negocio, considerándola como un proceso integral basado en la gestión y el control de riesgos con el fin de lograr sus objetivos y cumplir con su misión.

En este sentido, Elecnor Holding se compromete a dotar a las diferentes áreas del Grupo de los recursos técnicos, humanos, materiales y organizativos necesarios para garantizar una adecuada gestión de la seguridad de las redes y sistemas de información del Grupo Elecnor.

Para ello, el Grupo Elecnor guiará su actuación de acuerdo con los siguientes principios:

I. **Definir, desarrollar y mantener un marco integrado de controles:** el Grupo Elecnor impulsará el desarrollo de un marco integrado de controles técnicos, legales y de gestión de la Ciberseguridad acordes con sus objetivos y estrategias, y que permitan garantizar en todo momento el cumplimiento de los requisitos legales, reglamentarios y contractuales que le sean de aplicación.

II. **Promocionar una cultura de Ciberseguridad:** el Grupo Elecnor se compromete a promocionar de forma activa una "cultura de Ciberseguridad" entre todos sus Profesionales y demás sujetos obligados por esta Política, y por tanto internamente y entre sus clientes y proveedores. En especial, promoverá la integración de dicha cultura de Ciberseguridad en todos los ámbitos del Grupo como base de sus actividades y en relación con los productos y servicios que el Grupo Elecnor ofrece a sus clientes.

III. **Gestionar permanentemente la seguridad:** el Grupo Elecnor asume el compromiso de proteger la seguridad de las redes y sistemas de información, diseñando medidas de seguridad robustas, alineadas con las necesidades de las diferentes partes interesadas, así como con la normativa vigente aplicable en la materia, para lo cual el Grupo Elecnor aprobará las políticas y/o procedimientos específicos que desarrollarán los principios y requisitos básicos de seguridad establecidos en la presente Política. Todo ello con el objetivo de identificar los riesgos y corregir todas las Vulnerabilidades detectadas a fin de evitar la materialización de Incidentes que comprometan la continuidad de negocio del Grupo Elecnor.

IV. **Proteger proactivamente los activos de información y asegurar la resiliencia:** el Grupo Elecnor asumirá activamente el compromiso de lograr la salvaguarda de los niveles establecidos de confidencialidad, disponibilidad, autenticidad, trazabilidad e integridad de los activos de información del Grupo, así como para asegurar la Resiliencia Operativa Digital del Grupo Elecnor.

V. **Mejorar de forma continua la gestión de riesgos:** el Grupo Elecnor persigue el progreso constante de todos los procesos vinculados a la gestión de riesgos en materia de Ciberseguridad, así como de los controles para la seguridad de las redes y de los sistemas de información, analizando las Vulnerabilidades, ciberamenazas e Incidentes de Ciberseguridad para identificar sus causas y las mejoras necesarias en las operaciones y la continuidad de negocio del Grupo Elecnor.

## 6. REQUISITOS BÁSICOS DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

Toda la documentación de Ciberseguridad que se desarrolle en ejecución de los requisitos establecidos en este apartado se gestiona, estructura y conserva conforme a las políticas y los procedimientos documentados que el Grupo Elecnor ha desarrollado teniendo en cuenta la normativa y los estándares nacionales e internacionales que apliquen en cada caso.

Para llevar a cabo la gestión diaria de la Ciberseguridad, todos los Profesionales del Grupo Elecnor y demás sujetos obligados por esta Política, deben conocer, comprender y, en su caso actuar siempre, conforme a los siguientes requisitos básicos de seguridad de las redes y sistemas de información:

### > Prevención, detección, respuesta y conservación

Se establecerán, documentarán y aplicarán procesos, políticas y/o procedimientos para la prevención y Gestión de Incidentes de Ciberseguridad que garanticen que estos son conocidos por todos los Profesionales del Grupo Elecnor y demás sujetos obligados por esta Política, para detectar, analizar, contener o responder a Incidentes, recuperarse de ellos, documentarlos y notificarlos oportunamente.

### > Análisis y gestión de los riesgos

Se realizarán y documentarán evaluaciones de riesgos sobre la base de una vigilancia continuada y reevaluación periódica de los riesgos y, basándose en los resultados, se establecerá, aplicará y supervisará un plan de tratamiento de riesgos.

### > Diferenciación de responsabilidades

Se establecerán de forma clara las funciones y responsabilidades en materia de Ciberseguridad, de manera que todos los Profesionales del Grupo Elecnor y demás sujetos obligados por esta Política, las conozcan y comprendan.

### > Organización e implantación del proceso de Ciberseguridad

Se establecerá y mantendrá un marco adecuado de gestión de riesgos para identificar y tratar los riesgos que se plantean para la seguridad de las redes y los sistemas de información.

### > Gestión y formación

Se tendrá como objetivo que todos los Profesionales y, cuando proceda, los demás sujetos obligados por esta Política comprendan y se comprometan con sus responsabilidades en materia de Ciberseguridad, realizando las verificaciones de antecedentes y requisitos necesarias para su función, responsabilidades y autorizaciones.

A su vez, se llevarán a cabo programas de sensibilización y formación, de manera que todos los Profesionales, incluidos los miembros de los órganos de dirección, así como los proveedores directos y los prestadores de servicios, y otros sujetos obligados por esta Política, sean conscientes de los riesgos, estén informados de la importancia de la Ciberseguridad y apliquen prácticas de ciberhigiene.

### > Autorización y control de accesos

Se establecerán, documentarán y aplicarán procedimientos y/o políticas de control de acceso lógico y físico para el acceso a su red y a sus sistemas de información, basadas en los requisitos empresariales y en los requisitos de seguridad de la red y de los sistemas de información, gestionando los derechos de acceso a estos, así como a las cuentas privilegiadas y de administración del sistema que se habiliten, sobre la base del principio de mínimo privilegio.

### > Protección de las instalaciones

Se adoptarán controles y medidas para evitar la pérdida, el daño o el compromiso de las instalaciones donde se encuentran situados los sistemas de red y de información y demás activos, así como la interrupción de sus operaciones debido al fallo y la interrupción de los servicios de apoyo.

### > Integridad y actualización del sistema de información

Se establecerán y aplicarán procesos para gestionar y actualizar tanto los riesgos, como el contenido del Sistema de Gestión asociado. En particular, se establecerán requisitos relativos a las actualizaciones de seguridad aplicables al Sistema de Gestión durante su vida útil.

### > Protección de la información almacenada y en tránsito

Se establecerán, implantarán y aplicarán los controles oportunos, con vistas a garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información, tanto almacenada como en tránsito, en consonancia con la clasificación de activos y los resultados de la evaluación de riesgos realizada.

### > Prevención ante otros sistemas de información interconectados

Se adoptarán medidas para segmentar los sistemas en redes o zonas (tantos propios, como los provistos por terceros) de acuerdo con los resultados de la evaluación de riesgos.

### > Registro de la actividad y detección de código dañino

Se establecerán procedimientos y se utilizarán herramientas para supervisar y registrar las actividades en las redes y sistemas de información del Grupo Elecnor a fin de detectar sucesos que puedan considerarse Incidentes

y responder en consecuencia para mitigar el impacto de estos, garantizando que los resultados de estas evaluaciones sean tomados en consideración en los procesos de aprendizaje y mejora.

**> Continuidad de la actividad**

Se establecerá y mantendrá un plan de continuidad de la actividad y de recuperación en caso de catástrofe que se aplicará en caso de Incidentes, que establezca, entre otras cuestiones, condiciones de activación, contactos clave, funciones y responsabilidades y recursos necesarios, con el fin de garantizar que las operaciones se reestablezcan con arreglo a dicho plan, así como la continuidad del negocio en el Grupo Elecnor.

**> Seguridad en la cadena de suministro**

Se establecerán, implantarán y aplicarán procedimientos y/o políticas de seguridad de la cadena de suministro que rijan las relaciones con los proveedores directos y prestadores de servicios y establezca las medidas y controles oportunos con el fin de mitigar los riesgos detectados derivados de estos terceros para la seguridad de las redes y los sistemas de información del Grupo Elecnor.

# 7. GOBERNANZA

La gobernanza de la Ciberseguridad en el Grupo Elecnor es esencial tanto para garantizar la toma de decisiones en función del riesgo real de la materialización de las amenazas de Ciberseguridad en el Grupo, como para la continuidad de las operaciones de negocio, siendo la presente Política una herramienta fundamental para el establecimiento de unas bases adecuadas de gobernanza de la Ciberseguridad.

## 7.1. El Consejo de Administración y sus Comisiones

Corresponde al Consejo de Administración de Elecnor Holding el establecimiento de la estrategia y las directrices de gestión del Grupo Elecnor en materia de Ciberseguridad, a través de la presente Política y, en su caso, de otras normas corporativas que se aprueben en desarrollo de la misma.

A su vez, es competencia de la Comisión de Nombramientos, Retribuciones y Sostenibilidad, de acuerdo con sus funciones de supervisión y control, velar por la implementación y desarrollo de la presente Política y de las medidas adoptadas en aplicación de la misma, así como revisar y, en su caso, proponer al Consejo de Administración la actualización de la presente Política.

De otro lado, corresponde a la Comisión de Auditoría la supervisión de la eficacia de los sistemas de control y gestión de riesgos en materia de Ciberseguridad de la Sociedad y su Grupo, así como la supervisión del proceso de reporte de dichos riesgos.

Para el ejercicio de sus funciones de supervisión, tanto la Comisión de Nombramientos, Retribuciones y Sostenibilidad como la Comisión de Auditoría recibirán periódicamente del Comité de Seguridad de la Información e Inteligencia Artificial, a través del Responsable de Seguridad de la Información, información sobre las actuaciones y gestión desarrollada por el Comité y el propio Responsable, en el ámbito de sus respectivas competencias.

## 7.2. Comité de Seguridad de la Información e Inteligencia Artificial

### 7.2.1. Principios de actuación

Elecnor Holding, a través del Comité, observará y promoverá en el Grupo Elecnor los siguientes principios en relación con la gobernanza de la Ciberseguridad:

**a) Principio de alineamiento estratégico y visión de futuro**

La Ciberseguridad es entendida como una parte más del negocio, constituyéndose como una herramienta que ayuda al Grupo Elecnor a alcanzar sus objetivos, alineada con la misión y visión del Grupo.

En este sentido, el Comité impulsará en el Grupo Elecnor un enfoque holístico de modo que la Ciberseguridad no sea vista como un obstáculo sino como parte de un conjunto más amplio apto para el desarrollo de su negocio.

### b) Principio de ética y cumplimiento

El gobierno de la Ciberseguridad incluye no sólo el cumplimiento de la normativa aplicable, sino también las buenas prácticas de seguridad y el uso ético de los recursos del Grupo.

En aras de favorecer una actuación ética y responsable, el Comité fomentará la alineación con las mejores prácticas en la materia, entre otras, en la gestión de los riesgos de Ciberseguridad, tanto dentro del Grupo Elecnor como en cada uno de los mercados en los que opera y en su relación con los distintos grupos de interés.

### c) Principio de confiabilidad

Las redes y sistemas de información utilizados en el Grupo Elecnor deberán ser robustos y funcionar de manera confiable, de manera que sean capaces de dar soporte a las operaciones comerciales de manera continua y efectiva.

El Comité asegurará la implementación del principio de confiabilidad en los sistemas de información y redes, así como la continuidad del negocio en el Grupo Elecnor, en aras de fomentar la confianza de los clientes y demás grupos de interés.

### d) Principio de responsabilidad y rendición de cuentas

La Ciberseguridad es una disciplina compleja y transversal que afecta a todas las actividades de una organización. Es por esto por lo que requiere de un adecuado liderazgo y una estructura que, para ser implantada y gestionada adecuadamente, debe estar integrada por profesionales con formación y experiencia adecuados.

El Comité asume la función de definición, impulso y control de la Ciberseguridad y participa en la toma de decisiones y estrategias en este ámbito. Asimismo, el Comité deberá velar por el reporte adecuado y a los niveles oportunos, de los riesgos relacionados con la Ciberseguridad, así como de los mecanismos de mitigación y control de estos que sean necesarios.

### e) Principio de seguridad y resiliencia

Las redes y sistemas de información deben funcionar de manera segura y digitalmente resiliente.

Una de las finalidades perseguidas por la Ciberseguridad es asegurar la continuidad de la capacidad operativa del Grupo Elecnor en interés de este y de los grupos de interés que puedan verse afectados por sus actividades (Resiliencia Operativa Digital) y por ello se deben desarrollar capacidades para contener o recuperarse de los Ciberincidentes.

A estos efectos, el Comité impulsará la aprobación de los procedimientos y/o políticas que aseguren la gestión efectiva de los Ciberincidentes, identificando los grupos operativos encargados de su gestión (tanto a nivel técnico y táctico, como estratégico) para minimizar el impacto en el negocio y para asegurar el cumplimiento regulatorio y la adecuada comunicación interna o externa, así como disponiendo de capacidades que permitan al Grupo ser resiliente para asegurar la continuidad de las operaciones y la recuperación completa de los servicios en un plazo adecuado de tiempo que se determinará en el plan de continuidad de negocio.

## 7.2.2. Composición y funciones del Comité

Los miembros del Comité, así como el Responsable de Seguridad de la Información serán designados por el Consejo de Administración a propuesta de la Comisión de Nombramientos, Retribuciones y Sostenibilidad. El Comité actuará como instancia interna de apoyo al Responsable de Seguridad de la Información.

Con carácter adicional a cualesquiera otras funciones que tenga atribuidas, o se le atribuyan en virtud de la normativa interna en cada momento, corresponderá al Comité:

- Informar regularmente a la Dirección y diferentes áreas en relación con las medidas de seguridad y control adaptadas en materia de Ciberseguridad.

- Atender las cuestiones sobre Ciberseguridad planteadas por la Dirección y los diferentes departamentos de Elecnor Holding y su Grupo.
- Elaborar y actualizar la estrategia de Elecnor Holding y su Grupo en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas y filiales en materia de Ciberseguridad, para asegurar que los esfuerzos son consistentes, están alineados con la estrategia acordada en la materia y evitar duplicidades.
- Elaborar, aprobar e impulsar los cursos y requisitos de formación y calificación de los operadores desde la perspectiva de la seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por el Grupo 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 implicadas en la Gestión de Incidentes de Ciberseguridad.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la Ciberseguridad, así como velar por la coordinación de los diferentes planes que puedan realizarse en diferentes áreas y filiales del Grupo.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar por que la Ciberseguridad 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 transversales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad referentes a la seguridad de la información y ciberseguridad que puedan aparecer entre los diferentes Responsables y/o entre diferentes áreas de Elecnor Holding y su Grupo.
- Proponer a la Comisión de Nombramientos, Retribuciones y Sostenibilidad las actualizaciones que considere necesarios o convenientes respecto de la presente Política.
- Aprobar procedimientos, normas o protocolos internos dirigidos al desarrollo e implementación de la presente Política en Elecnor Holding y a nivel de Grupo.
- Asegurar de que se disponen de los medios humanos y materiales necesarios para la realización de las funciones que le han sido encomendadas.

# 8. SEGUIMIENTO, INTERPRETACIÓN Y REVISIÓN

## 8.1. Seguimiento

El cumplimiento de esta Política será supervisado por el Comité de Seguridad de la Información e Inteligencia Artificial. Se establecerán mecanismos de auditoría y revisión periódica para asegurar que todas las medidas de Ciberseguridad establecidas en el Grupo cumplan con los requisitos establecidos en esta Política y en la normativa aplicable.

En caso de tener algún problema, o detectar un Incidente que pueda afectar al funcionamiento o seguridad de los sistemas de información, este se deberá comunicar inmediatamente al Comité, a través de los cauces habilitados a tales efectos y que se determinarán en los procedimientos internos.

A modo de métrica, se documentarán los resultados del proceso de gestión de vulnerabilidades.

El incumplimiento de la presente Política puede conllevar responsabilidades legales de diversa naturaleza según dispone la legislación vigente, dando derecho a Elecnor Holding, si así se estimara necesario, a iniciar las acciones legales que procedan.

### 8.2. Interpretación

El órgano de contacto para cualquier duda y/o consulta en relación con la interpretación y ejecución de la presente Política será el Comité de Seguridad de la Información e Inteligencia Artificial, que podrá ser contactado por los cauces habilitados al efecto.

### 8.3. Revisión y actualización

Esta Política será revisada y, en su caso, actualizada al menos una vez al año, y siempre que se produzcan Incidentes significativos o cambios importantes en las operaciones o los riesgos. Se dejará constancia documental del resultado de estas revisiones.

La modificación y/o actualización de la presente Política será aprobada por el Consejo de Administración de Elecnor Holding, previo informe de la Comisión de Nombramientos, Retribuciones y Sostenibilidad, y se difundirá a los Profesionales a través de los canales habituales.

## 9. DIFUSIÓN

Esta Política y sus modificaciones se publicarán en la página web corporativa de la Sociedad y se mantendrá permanentemente actualizada, con el consiguiente conocimiento y asunción de su contenido íntegro por parte de los Profesionales del Grupo Elecnor y demás sujetos obligados por esta Política.

Sin perjuicio de ello, Elecnor Holding llevará a cabo acciones de comunicación, formación y sensibilización para la comprensión y puesta en práctica de esta Política, así como de sus actualizaciones.

En todo caso, se recomienda acceder de forma periódica al contenido de esta Política a través de los canales disponibles para una mejor comprensión de la misma, debiendo tenerse en cuenta que el desconocimiento de todo o parte de su contenido no exime de su cumplimiento.

## 10. ENTRADA EN VIGOR

La presente Política fue aprobada por el Consejo de Administración de Elecnor Holding en su reunión de fecha 27 de noviembre de 2024, entrando en vigor el 1 de enero de 2025.

grupo elecnor

www.grupoelecnor.com