Política de seguridad

25 de marzo de 2025

El Consejo de Administración de IBERDROLA, S.A. (la "**Sociedad**") tiene atribuida la competencia de diseñar, evaluar y revisar con carácter permanente el Sistema de gobernanza y sostenibilidad de la Sociedad y, específicamente, de aprobar y actualizar las políticas, las cuales contienen las pautas que rigen la actuación de la Sociedad y, además, en lo que sea de aplicación, informan las políticas que, en ejercicio de su autonomía de la voluntad, decidan aprobar las sociedades integradas en el grupo cuya entidad dominante es, en el sentido establecido por la ley, la Sociedad (el "**Grupo**").

En el ejercicio de estas competencias y en el marco de la normativa legal, de los Estatutos Sociales y del Propósito y Valores del Grupo Iberdrola, el Consejo de Administración aprueba esta Política de seguridad (la "**Política**") que respeta, desarrolla y adapta, en relación con la Sociedad, los Principios éticos y básicos de gobernanza y de sostenibilidad del Grupo Iberdrola.

En esta Política, la Sociedad manifiesta su compromiso con la excelencia en materia de seguridad, que tiene un papel protagonista en su día a día, para que permanezca segura, resiliente y confiable en un entorno en continua transformación, en el que surgen nuevas amenazas cada vez más sofisticadas, tanto físicas como de ciberseguridad o híbridas. Todo ello, conlleva a un aumento del grado de exigencia de los reguladores, de los clientes y de los demás Grupos de interés de la Sociedad respecto del cumplimiento de los cada vez más altos estándares de seguridad que permitan construir y consolidar relaciones duraderas de confianza.

1. Ámbito de aplicación

Esta Política es de aplicación a la Sociedad. Sin perjuicio de lo cual, incluye principios básicos que complementan, en materia de la cadena de valor sostenible y, en particular, de seguridad, los contenidos en los Principios éticos y básicos de gobernanza y de sostenibilidad del Grupo Iberdrola y, en esta medida, deben informar la actuación y los desarrollos normativos que, en el ejercicio de sus competencias y al amparo de su autonomía de la voluntad, lleven a cabo las demás sociedades del Grupo en esta materia.

En la medida en que formen parte del Grupo sociedades *subholding* cotizadas, ellas y sus filiales, al amparo de su propio marco especial de autonomía reforzada, podrán establecer principios y normas que deberán tener un contenido conforme a los principios de esta Política.

Estos principios deberán informar también, en lo que proceda, la actuación de las entidades de naturaleza fundacional vinculadas al Grupo.

La Sociedad promoverá, igualmente, en aquellas otras compañías en las que participe y que no formen parte del Grupo, así como en las *joint ventures*, uniones temporales de empresas y otras entidades en las que asuma la gestión, el alineamiento de su normativa con los principios básicos en materia de la cadena de valor sostenible y, en particular, de seguridad contenidos en esta Política.

2. Finalidad

La finalidad de esta Política es establecer los principios básicos de actuación que deben regir en la Sociedad en materia de seguridad, para velar por la efectiva protección de las personas, de los activos, tanto activos físicos como ciberactivos (incluyendo infraestructuras críticas), de la información y del conocimiento y de los sistemas de control y de las comunicaciones, así como de la privacidad de los datos tratados, velando en todo momento, por que las actuaciones en materia de seguridad sean plenamente conformes con la normativa legal y cumplan escrupulosamente lo previsto en la Política de respeto de los derechos humanos.

3. Principios básicos de actuación

La Sociedad asume y promueve los siguientes principios básicos de actuación que deben presidir sus actividades en materia de seguridad:

a. Velar por la protección de los profesionales de las sociedades del Grupo tanto en su puesto de trabajo como en sus desplazamientos por motivos profesionales, así como la protección de las personas cuando se encuentren en las instalaciones o en cualquier evento institucional de la Sociedad.

b. Asegurar la adecuada protección de los activos, tanto activos físicos como ciberactivos, para gestionar proactivamente los riesgos en todas las fases de su ciclo de vida, garantizando que poseen un nivel de seguridad, ciberseguridad y resiliencia adecuados, aplicando los estándares más avanzados para aquellos que soporten la operación de infraestructuras críticas de conformidad con las Bases generales de control y gestión de riesgos del Grupo Iberdrola y con las Directrices y límites de riesgo de ciberseguridad aprobadas por el Consejo de Administración.

c. Definir un modelo de gestión de la seguridad con una asignación clara de roles y responsabilidades y mecanismos de coordinación efectivos, que integre la seguridad y la gestión proactiva de los riesgos en los procesos decisorios.

d. Promover la identificación de la información no pública considerada (o susceptible de ser considerada) como secreto empresarial, así como aquella cuya divulgación o alteración no autorizada pudiera causar serios perjuicios a los intereses de la Sociedad.

e. Definir los criterios para la adecuada protección de la información y del conocimiento, así como de los sistemas de control, información y comunicaciones, supervisando y asegurando su implementación.

f. Impulsar la lucha activa contra el fraude y contra ataques a la marca, a la imagen y a la reputación de la Sociedad y de sus profesionales.

g. Garantizar el derecho a la protección de los datos personales de las personas físicas con las que se relaciona, de conformidad con lo dispuesto en la Política de protección de datos personales.

h. Adoptar las medidas necesarias para prevenir, neutralizar, minimizar o restaurar el daño causado por amenazas de seguridad, ya sean físicas, de ciberseguridad o híbridas, para el normal desarrollo de las actividades, con base en criterios de proporcionalidad a los potenciales riesgos y a la criticidad y al valor de los activos y servicios afectados.

i. Cumplir con los principios básicos de actuación establecidos en la Política de resiliencia operativa.

j. Fomentar una cultura inclusiva y una concienciación en materia de seguridad, tanto internamente como externamente, a terceros y colaboradores mediante la realización de acciones de divulgación, concienciación y formación adecuadas, adaptadas a cada destinatario y con la suficiente periodicidad para garantizar que disponen de los conocimientos, habilidades, experiencia y capacidades necesarias.

k. Impulsar la adecuada capacitación en materia de seguridad de todo su personal, tanto interno como externo, definiendo requisitos y criterios en la contratación que tengan en cuenta dicha capacitación.

l. Promover la integración de la seguridad en la gestión de los proyectos de la Sociedad, que puedan implicar algún potencial riesgo de seguridad, de forma que se procure una

adecuada identificación y tratamiento de este riesgo desde el diseño y las fases iniciales del proyecto y el establecimiento de los controles necesarios durante la vida de este.

m. Impulsar un uso seguro de los activos que fortalezca las capacidades de detección, prevención, defensa, respuesta y recuperación frente a ataques o incidentes de seguridad, velando por la eficacia de estas y prestando especial atención a las amenazas de ciberseguridad.

n. Vigilar el contexto actual de la organización y el entorno, así como de la evolución de eventos que permitan identificar las amenazas de seguridad más relevantes con el objetivo de anticipar su potencial impacto.

o. Promover las mejores prácticas y la innovación en el ámbito de la seguridad.

p. Colaborar con los Grupos de interés involucrados (entre otros, la cadena de suministro y los clientes) en riesgos de seguridad que afecten a la Sociedad para reforzar la respuesta coordinada ante potenciales riesgos y amenazas en materia de seguridad.

4. Coordinación a nivel del Grupo

La Dirección de Seguridad y Resiliencia (o la dirección que, en cada momento, asuma sus facultades), a través del Comité de Seguridad, Resiliencia y Tecnologías Digitales (o del comité que, en cada momento, asuma sus facultades) se coordinará con los comités de seguridad, resiliencia y tecnologías digitales que, en su caso, se constituyan en las sociedades *subholding* o, en su defecto, con las correspondientes direcciones de seguridad y resiliencia (o las direcciones, áreas o funciones que, en cada momento, asuman sus facultades) de cada una de las sociedades del Grupo, para velar por un adecuado nivel consolidado de madurez y riesgos en materia de seguridad a nivel del Grupo.

Además, la Dirección de Seguridad y Resiliencia (o la dirección que, en cada momento, asuma sus facultades), a través del Comité de Seguridad, Resiliencia y Tecnologías Digitales (o del comité que, en cada momento, asuma sus facultades), identificará, implantará y evaluará las acciones necesarias para la elaboración y la supervisión de un Programa estratégico de seguridad, conforme a los principios y directrices definidos en esta Política y desarrollará las normas, metodologías y procedimientos internos para asegurar la adecuada implementación de este.

5. Implementación y seguimiento

Para la implementación y seguimiento de lo previsto en esta Política, el Consejo de Administración cuenta con la Dirección de Seguridad y Resiliencia (o la dirección que, en cada momento, asuma sus facultades), que desarrollará los procedimientos necesarios para ello.

Además, se realizarán evaluaciones y auditorías periódicas con auditores internos o externos para verificar el cumplimiento de esta Política.

* * *

Esta Política fue aprobada inicialmente por el Consejo de Administración el 23 de septiembre de 2013 y modificada por última vez el 25 de marzo de 2025.