



Política de seguridad corporativa

20 de junio de 2023

■ 1. Finalidad	2
■ 2. Ámbito de aplicación	2
■ 3. Principios básicos de actuación	2



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 y, específicamente, de aprobar y actualizar las políticas corporativas, las cuales contienen las pautas que rigen la actuación de la Sociedad y de 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 responsabilidades, con el objeto de establecer los principios generales que deben regir las actuaciones en materia de seguridad corporativa en todas sus vertientes, y en cumplimiento de lo dispuesto en el *Propósito y Valores del Grupo Iberdrola*, el Consejo de Administración aprueba esta *Política de seguridad corporativa* (la "**Política**").

1. Finalidad

La finalidad de esta *Política* es establecer los principios básicos de actuación que deben regir dentro del perímetro del Grupo para garantizar la efectiva protección de las personas, de los activos físicos y lógicos e infraestructuras críticas, de la información, así como de la privacidad de los datos tratados, garantizando un nivel razonable de seguridad, resiliencia y cumplimiento.

Además, esta *Política* constata el firme compromiso de la Sociedad con la excelencia en materia de seguridad de las personas, de los activos físicos y lógicos e infraestructuras críticas de las sociedades del Grupo y de la información, asegurando, en todo momento, que las actuaciones en materia de seguridad sean plenamente conformes con la ley y cumplan escrupulosamente lo previsto en la *Política de respeto de los derechos humanos*.

2. Ámbito de aplicación

Esta *Política* es de aplicación en todas las sociedades que integran el Grupo, así como en las sociedades participadas no integradas en el Grupo sobre las que la Sociedad tiene un control efectivo, dentro de los límites legalmente establecidos.

Sin perjuicio de lo dispuesto en el párrafo anterior, las sociedades *subholding* cotizadas y sus filiales, al amparo de su propio marco especial de autonomía reforzada, podrán establecer una política equivalente, que deberá ser conforme con los principios recogidos en esta *Política* y en las demás políticas medioambientales, sociales y de gobierno corporativo y cumplimiento normativo del Sistema de gobernanza y sostenibilidad.

En aquellas sociedades participadas en las que esta *Política* no sea de aplicación, la Sociedad promoverá, a través de sus representantes en sus órganos de administración, el alineamiento de sus políticas propias con las de la Sociedad.

Además, esta *Política* es también aplicable, en lo que proceda, a las *joint ventures*, uniones temporales de empresas y otras asociaciones equivalentes, cuando la Sociedad asuma su gestión.

3. Principios básicos de actuación

Para materializar el compromiso indicado en el apartado 1 anterior, se asumen y promueven dentro del perímetro del Grupo los siguientes principios básicos de actuación que deben presidir las actividades de las sociedades que lo integran en materia de seguridad corporativa:

- a. Diseñar una estrategia de seguridad preventiva, con una visión integral, cuyo objetivo sea minimizar los riesgos de seguridad física y lógica, incluidas las consecuencias resultantes de un acto terrorista, y destinar los recursos necesarios para su implementación.
- b. Desarrollar planes de defensa específicos para la protección de las infraestructuras críticas y para garantizar la continuidad de los servicios esenciales que prestan las sociedades del Grupo.
- c. Garantizar la protección de los profesionales de las sociedades del Grupo tanto en su puesto de trabajo como en sus desplazamientos por motivos profesionales.
- d. Asegurar la adecuada protección de la información y el conocimiento y su confidencialidad, así como de los sistemas de control, información y comunicaciones del Grupo y establecer controles y procedimientos a tal fin, en particular, para evitar cualquier obtención, utilización o revelación ilícitas de la información o conocimiento, de conformidad con lo dispuesto en la *Política de riesgos de ciberseguridad*.
- e. Identificar la información no pública que deba ser clasificada como confidencial o secreta, así como la información o conocimiento considerado (o susceptible de serlo) como secreto empresarial e implementar y desarrollar los procedimientos o protocolos de seguridad y privacidad adecuados y razonablemente suficientes, teniendo en cuenta el nivel de riesgo de que se produzca, velando asimismo por la salvaguarda de la integridad y disponibilidad de dicha información o conocimiento.
- f. Dotarse de procedimientos y herramientas que permitan luchar activamente contra el fraude y contra ataques a la marca y a la reputación del Grupo y de sus profesionales.
- g. Garantizar el derecho a la protección de los datos personales de todas las personas físicas que se relacionan con las sociedades pertenecientes al Grupo, asegurando el respeto del derecho al honor y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, de conformidad con lo dispuesto en la *Política de protección de datos personales*.
- h. Implementar medidas de seguridad basadas en criterios de eficiencia y que contribuyan al normal desarrollo de las actividades del Grupo.
- i. Evitar el uso de la fuerza en el ejercicio de la seguridad, empleándola única y exclusivamente en casos estrictamente necesarios, siempre de acuerdo con la ley y de forma proporcional a la amenaza recibida, en defensa de la vida.





- j. Promover una cultura de la seguridad en el seno del Grupo, mediante la realización de acciones de divulgación y formación en la materia.
- k. Asegurar la adecuada cualificación de todo el personal de seguridad, tanto interno como externo, estableciendo rigurosos planes de formación y definiendo requisitos y criterios en la contratación que tengan en cuenta este principio. En particular, formar a todo el personal de seguridad en materia de derechos humanos, o asegurarse de que ha recibido la adecuada formación en dicha materia.
- l. Trasladar los principios de esta *Política* a los proveedores de seguridad que se contraten, según corresponda, y evaluar periódicamente su cumplimiento.
- m. Colaborar con las autoridades públicas con responsabilidades en materia de seguridad pública y no interferir en el cumplimiento de sus funciones legítimas.
- n. Actuar, en todo momento, al amparo de la legislación vigente y dentro del marco establecido por el *Código ético* y las demás normas del Sistema de gobernanza y sostenibilidad.

Esta *Política* fue aprobada inicialmente por el Consejo de Administración el 23 de septiembre de 2013 y modificada por última vez el 20 de junio de 2023.