Política de seguridad corporativa

C

20 de febrero de 2024

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 en las sociedades del Grupo en materia de seguridad, para garantizar la efectiva protección de las personas, de los activos físicos (incluyendo infraestructuras críticas), de la información y del conocimiento y de los sistemas de control y 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 ley y cumplan escrupulosamente lo previsto en la *Política de respeto de los derechos humanos*.

A través de esta *Política*, la Sociedad manifiesta su compromiso con la excelencia en materia de seguridad, la cual ostenta un papel protagonista en el día a día de las sociedades del Grupo, para que permanezcan seguras, resilientes y confiables en una comunidad digital en continua transformación, donde surgen nuevas amenazas cada vez más sofisticadas, tanto físicas como de ciberseguridad o híbridas, lo que provoca un aumento del grado de exigencia de los reguladores, de los clientes y de los demás Grupos de interés con los que las sociedades del Grupo se relacionan, respecto del cumplimiento de los cada vez más altos estándares de seguridad que permitan construir y consolidar relaciones duraderas de confianza.

2. Ámbito de aplicación

Esta *Política* es de aplicación en la Sociedad y en las demás compañías del 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 y con las directrices 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.

Adicionalmente, 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.

Esta *Política* se desarrolla y complementa a través de las siguientes políticas específicas, también aprobadas por el Consejo de Administración de la Sociedad: la *Política de protección de datos personales* y la *Política de riesgos de ciberseguridad*, por lo que respecta a las citadas materias.

3. Principios básicos de actuación

Para materializar el compromiso indicado en el apartado 1 anterior, se establecen los siguientes principios básicos de actuación que deben presidir las actividades de las sociedades del Grupo en materia de seguridad corporativa:

a. Definir una estrategia de seguridad integral con un enfoque tanto preventivo como proactivo para garantizar un nivel razonable de riesgo.

b. Asegurar la adecuada protección de los activos (incluyendo infraestructuras críticas), para gestionar proactivamente los riesgos.

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, así como la protección de las personas cuando se encuentren en las instalaciones o en cualquier evento institucional de las sociedades del Grupo.

d. 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.

e. Asegurar la adecuada protección de la información y del conocimiento, así como de los sistemas de control, información y comunicaciones, para gestionar proactivamente los riesgos, de conformidad con lo dispuesto en la *Política de Riesgos de Ciberseguridad* (o norma que la sustituya en cada momento).

f. Promover la identificación de la información no pública clasificada (o susceptible de ser clasificada) como confidencial o secreta, así como la información considerada (o susceptible de ser considerada) como secreto empresarial y definir los criterios para su adecuada protección, asegurando su implementación.

g. Impulsar la lucha activa contra el fraude y contra ataques a la marca, a la imagen y a la reputación de las sociedades del Grupo y de sus profesionales.

h. Garantizar el derecho a la protección de los datos personales de todas las personas físicas que se relacionan con las sociedades pertenecientes al Grupo, de conformidad con lo dispuesto en la *Política de protección de datos personales* (o norma que la sustituya en el futuro).

i. 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.

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

k. Fomentar una cultura inclusiva y una concienciación en materia de seguridad dentro del Grupo, mediante la realización de acciones de divulgación, concienciación y formación adecuadas, adaptadas a cada destinatario y con la suficiente periodicidad para garantizar la actualización de los conocimientos en este ámbito.

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

m. 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.

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

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

p. Prestar toda la asistencia y cooperación que puedan requerir las instituciones y los organismos competentes en materia de seguridad, incluyendo entre otros reguladores, fuerzas y cuerpos de seguridad y agencias gubernamentales, nacionales e internacionales, en aquellos países en los que el Grupo desarrolle su actividad.

q. Velar por el efectivo cumplimiento de las obligaciones impuestas por el Sistema de gobernanza y sostenibilidad y por la regulación aplicable en cada momento en materia de seguridad, actuando siempre conforme a la legislación vigente y a lo establecido en el *Código ético* y en las demás normas del Sistema de gobernanza y sostenibilidad.

4. Programa Estratégico de Seguridad

La Dirección de Seguridad Corporativa (o la dirección que en el futuro asuma sus funciones) identificará, implantará y evaluará las acciones necesarias para la elaboración de un Programa Estratégico de Seguridad (el "**Programa**"), conforme a los principios y directrices definidos en esta *Política* y desarrollará las normas, metodologías y procedimientos internos para asegurar la adecuada implementación del Programa por la Sociedad y por las demás sociedades del Grupo, las cuales lo adaptarán a las particularidades de los territorios y de los negocios de cada una de ellas.

Las direcciones de seguridad corporativa (o las direcciones, áreas o funciones que en cada momento asuman sus competencias) de cada una de las sociedades del Grupo velarán, respecto de su correspondiente sociedad, por que en todo momento se garantice un nivel de madurez de la organización en materia de seguridad acorde a los más altos estándares existentes en cada momento, atendiendo al territorio y a los negocios desarrollados por la correspondiente compañía.

Por su parte, la Dirección de Seguridad Corporativa (o la dirección que en cada momento asuma sus funciones) velará, además, por la adecuada coordinación de las prácticas y la gestión de los riesgos en el ámbito de la seguridad entre las distintas sociedades del Grupo, así como por el mantenimiento de un nivel adecuado de madurez en materia de seguridad a nivel de Grupo.

5. Supervisión y control

Corresponde a la Dirección de Seguridad Corporativa (o a la dirección que, en cada momento, asuma sus funciones) supervisar el cumplimiento de lo dispuesto en esta *Política*.

Lo anterior se entenderá, en todo caso, sin perjuicio de las responsabilidades que correspondan a otros órganos, áreas, funciones y direcciones de la Sociedad y, en su caso, a los órganos de administración y de dirección de las sociedades del Grupo.

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

***

Esta *Política* fue aprobada inicialmente por el Consejo de Administración el 23 de septiembre de 2013 y modificada por última vez el 20 de febrero de 2024.