# POLÍTICA DE CIBERSEGURIDAD

## 1. OBJETO

ACCIONA considera la información, junto con los sistemas que la sustentan y procesan, uno de sus activos más importantes, por lo que establece como objetivo la gestión efectiva y eficiente de los riesgos a los que se ven sujetos.

Esta política establece los principios de ciberseguridad por los que se rige ACCIONA para garantizar la protección de su información y los sistemas que la soportan.

Los objetivos específicos de este documento son:

- Definir los principios que rigen la gestión de la ciberseguridad en ACCIONA, de forma que éstos protejan la información del grupo, mitiguen los riesgos de ciberseguridad a los que se ve expuesta y se encuentren alineados con los requerimientos normativos y regulatorios vigentes.
- Definir y asignar las responsabilidades asociadas a la implantación y mantenimiento de su modelo de gestión.
- Establecer un marco que facilite la toma de decisiones en lo referente a la implantación de medidas de ciberseguridad, tanto técnicas como procedimentales y organizativas, con el fin de prevenir los siguientes impactos:
    - Daño en la imagen y reputación de ACCIONA.
    - interrupción de los procesos críticos que soportan el negocio.
    - Pérdida o mal uso de los activos de información.

## 2. ALCANCE

Esta política aplica a todos los activos de información, las empresas y empleados del Grupo, así como a colaboradores y empresas externas que acceden a los sistemas de información de ACCIONA.

ACCIONA tiene la obligación de garantizar, en los mismos términos, la seguridad de la información que concierne a sus clientes, entidades colaboradoras y a los organismos oficiales competentes.

## 3. DESARROLLO DE LA POLÍTICA

La política se complementa con un Cuerpo Normativo para la gestión de la Ciberseguridad, adecuado para dar respuesta a las amenazas actuales y emergentes, así como a los requerimientos regulatorios. La estructura de este cuerpo normativo se divide en los siguientes niveles:

- **Primer nivel normativo**: constituido por la presente política.
- **Segundo nivel normativo**: constituido por las normas generales de ciberseguridad.
- **Tercer nivel normativo**: compuesto por procedimientos, manuales operativos y guías técnicas.

El Cuerpo Normativo de Ciberseguridad es revisado regularmente, al menos una vez al año, así como tras cambios significativos que afecten al entorno de la ciberseguridad de ACCIONA y/o a las circunstancias de su negocio.

## 4. PRINCIPIOS

Los principios que rigen la gestión de la ciberseguridad en ACCIONA son los siguientes:

- **Prevención y resiliencia:** Potenciar las capacidades para la protección y detección precoz frente a las ciberamenazas, para evitar que éstas lleguen a impactar a ACCIONA, o en caso de que lo hagan, se puedan minimizar sus efectos sobre el negocio.
- **Participación de la Alta Dirección:** se asume la ciberseguridad como una función cuya responsabilidad se ejerce a partir del máximo nivel jerárquico de la organización, de tal forma que el Comité de Dirección asume el compromiso de asegurar la implantación del sistema de gestión de la ciberseguridad que permita llevar a la práctica lo definido en el presente documento.
- **Responsabilidad compartida:** la ciberseguridad es una función a la que debe su plena colaboración todo el personal de ACCIONA, tanto en lo que se refiere al cumplimiento de aquellas normas y procedimientos establecidos que les conciernan expresamente, como a la colaboración que se le requiera ocasionalmente por parte de los responsables funcionales de ciberseguridad.
- **Formación**: se considera que uno de los pilares indispensables para la correcta gestión de la ciberseguridad es un adecuado nivel de formación y concienciación. Por ello ACCIONA promueve una cultura de ciberseguridad mediante acciones de formación dirigidas a todos los empleados y grupos de interés implicados. Así mismo, garantiza que los equipos de ciberseguridad disponen de los conocimientos, experiencia y capacidades tecnológicas para cumplir con los objetivos de ciberseguridad de ACCIONA.
- **Cumplimiento normativo:** es necesario garantizar el cumplimiento de las leyes y regulaciones aplicables en materia de ciberseguridad en todos aquellos países en los que opera ACCIONA. Así mismo ACCIONA colabora con las autoridades y organismos competentes para contribuir a la mejora de la ciberseguridad.

## 5. ORGANIZACIÓN DE CIBERSEGURIDAD

El Comité de Dirección de Ciberseguridad es el máximo responsable en materia de ciberseguridad en ACCIONA, delegando la ejecución de dicha función al Director de Ciberseguridad. Dicha figura depende jerárquicamente del Director de Sistemas de Información y del Director de Seguridad Corporativa. De esta forma, se asegura la coherencia y convergencia de los controles técnicos, responsabilidad de la Dirección de Tecnología y Procesos, con los controles físicos y personales responsabilidad del área de Seguridad Corporativa.

La misión de la Dirección de Ciberseguridad es proteger de manera eficaz y eficiente los activos de información del Grupo, tratando de velar por la viabilidad del negocio y encargándose de impulsar la organización de ciberseguridad definida en la presente política.

El Comité de Dirección de Ciberseguridad es responsable de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la integridad, disponibilidad y confidencialidad de la información, dentro de un marco general de gestión de los riesgos de ciberseguridad, haciendo compatible estas medidas con la necesaria trasmisión de información y conocimiento entre las diversas áreas organizativas de ACCIONA.

A efectos de coordinación, existen distintos Comités de Ciberseguridad operativos, donde participan los principales responsables de ciberseguridad de las distintas áreas, funciones, empresas o territorios que se determinen en cada caso.

Sin perjuicio de lo anterior, todo empleado de ACCIONA es responsable cumplir con los requisitos de ciberseguridad dentro del ejercicio de sus funciones, de tal forma que exista una corresponsabilidad compartida entre empleados, directivos, colaboradores y la organización de ciberseguridad.

## 6. AUDITORÍA

Se realizan periódicamente auditorías, ya sean de carácter total o parcial, con el objetivo de verificar el grado de cumplimiento de lo definido en el Cuerpo Normativo de Ciberseguridad de ACCIONA.

## 7. VIGENCIA Y REVISIONES

Esta política entrará en vigor el siguiente día hábil a su aprobación por el Comité de Dirección de Ciberseguridad de ACCIONA. Su vigencia se mantendrá mientras no sea modificada o derogada por otra posterior.

Las excepciones a lo establecido en esta política serán tratadas y aprobadas por el Comité de Dirección de Ciberseguridad de ACCIONA.

Desde su entrada en vigor, se dispone de tres meses para adecuar las incompatibilidades con lo dispuesto en este documento que puedan existir en otras normas, tanto globales como locales.

Este documento se revisará periódicamente y en función de los cambios organizativos, legales o de negocio que se produzcan en cada momento, con el fin de mantener su pertinencia, suficiencia y eficacia. En caso de producirse cambios en el mismo, éstos serán comunicados y publicados en el espacio de Ciberseguridad de la intranet de ACCIONA (InterACCIONA).

Esta política está disponible en la Intranet (InterACCIONA) para todos los empleados y en la web corporativa para todos los grupos de interés de la Compañía.

Esta política entrará en vigor el siguiente día hábil a su aprobación por la Comisión de Auditoría y Sostenibilidad del Consejo de Administración de Acciona, SA. Su vigencia se mantendrá mientras no sea modificada o derogada por otra posterior.

Las excepciones a lo establecido en esta política serán tratadas y aprobadas por la Comisión de Auditoría y Sostenibilidad del Consejo de Administración de Acciona, SA a propuesta del Comité de Dirección de Ciberseguridad de ACCIONA.

**16 de diciembre de 2022**