#somoslogística

Política de Ciberseguridad

Abril 2023

BERGÉ
Moved by Logistics

ÍNDICE

1. Introducción y objeto

La presente Política de Ciberseguridad (en adelante la "Política") tiene como objeto el establecimiento de los principios generales que aplican al marco de control relativo a la seguridad de la información, la gestión de los riesgos y resiliencia frente a incidentes de ciberseguridad que puedan afectar a Bergé Infraestructuras y Servicios Logísticos, S.L. y sus sociedades dependientes (en adelante, "BERGÉ"), así como formalizar el compromiso del Consejo de Administración con la implementación, mantenimiento y mejora de la ciberseguridad en la organización.

BERGÉ considera la información y los sistemas asociados, como activos importantes y esenciales para el correcto funcionamiento de la organización y el desarrollo de su actividad, por ello, asume la ciberseguridad como una responsabilidad asociada a la protección de las amenazas internas y externas que puedan afectar a dichos activos en términos de confidencialidad, integridad y disponibilidad.

La Política está alineada con los principios establecidos en el Código de Conducta y demás políticas internas de BERGÉ, y se complementará con el resto de procedimientos, manuales e instrucciones emitidas por la función de Ciberseguridad y el Área de GRC.

2. Alcance y obligatoriedad

La presente Política está dirigida a todos los profesionales de BERGÉ y sus sociedades dependientes.

Se entenderá por sociedades dependientes aquellas compañías en las que BERGÉ ostente una participación en el capital social que le permita tener control, conforme a lo previsto en el artículo 42 del Código de Comercio.

La Política constituye una norma interna de obligado cumplimiento para todos los profesionales de BERGÉ, independientemente de su ubicación geográfica, jerárquica o funcional, y de la modalidad contractual que determine su relación con BERGÉ.

No se aprobarán excepciones generales a la aplicación de la Política. Si se precisa una excepción puntual por motivos justificados, será necesaria la autorización previa del Área de GRC.

3. Principios rectores

A continuación, se detallan los principios y directrices generales que deben guiar la actuación de BERGÉ en la gestión de la ciberseguridad:

+ Asegurar y comunicar el cumplimiento normativo en materia de ciberseguridad a toda la organización.
+ Garantizar que la información, los activos y los sistemas que soportan la gestión de la ciberseguridad en BERGÉ dispongan de un nivel de seguridad y resiliencia adecuado, implantando los controles necesarios para proteger la confidencialidad, integridad y disponibilidad en función de su nivel de criticidad y los riesgos existentes.
+ Cumplir con la legislación vigente, acuerdos contractuales y requisitos reglamentarios en materia de ciberseguridad que sean aplicables de forma directa o indirecta a BERGÉ.
+ Impulsar las actividades de identificación, valoración y gestión de los riesgos identificados en materia de ciberseguridad.
+ Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a incidentes de ciberseguridad y nuevas amenazas.
+ Establecer requisitos de ciberseguridad adecuados sobre las relaciones contractuales con proveedores y colaboradores.
+ Promover la implantación de mecanismos de ciberseguridad y resiliencia adecuados para los activos y sistemas gestionados por terceros que presten servicios a BERGÉ.
+ Concienciar y sensibilizar a todos los profesionales y colaboradores de BERGÉ sobre los riesgos relativos a la ciberseguridad y garantizar que tengan, de una forma entendible y accesible, los conocimientos, habilidades y capacidades necesarias para la identificación de dichos riesgos.
+ Asegurar la disposición de los recursos materiales, económicos y humanos necesarios para cumplir con los objetivos relacionados con la ciberseguridad.
+ Facilitar la comunicación y colaboración con organizaciones, organismos, agencias gubernamentales y asociaciones relevantes para contribuir a la mejora de la ciberseguridad en la organización.

4. Misión de ciberseguridad en Bergé

El Departamento de Ciberseguridad de BERGÉ tiene como misión proteger los activos de información de la compañía frente a las amenazas de ciberseguridad, desarrollando procesos y operaciones resilientes. Para ello, se atribuyen los siguientes objetivos:

+ Asegurar el cumplimiento en materia de ciberseguridad mediante el desarrollo e implementación de un Sistema de Gestión de Seguridad de la Información.
+ Identificar, analizar y gestionar riesgos de ciberseguridad en los activos de información.
+ Asesorar y acompañar a las áreas afectadas en la mitigación de riesgos.
+ Establecer una cultura de ciberseguridad en la compañía, a través de formación y capacitación.
+ Proveer de información a la Dirección sobre el estado de la ciberseguridad (amenazas, riesgos, vulnerabilidades y tendencias).

BERGÉ dispone de un Comité de Ciberseguridad como órgano de gobierno de la ciberseguridad con las siguientes funciones:

+ Supervisión del avance del grado de madurez de la organización en materia de ciberseguridad.
+ Revisión, coordinación y toma de decisiones sobre los incidentes de ciberseguridad.

5. Comunicación y difusión

El texto íntegro de la Política se hará llegar a la totalidad de los profesionales que componen BERGÉ, todos los cuales vendrán obligados a cumplir estrictamente su contenido y será objeto de acciones de comunicación, formación y sensibilización para su oportuna comprensión y aplicación.

La Política estará disponible a través de la Intranet corporativa y de la página web de la organización para su promoción a terceros.

6. Aprobación y revisión

La Política ha sido aprobada por el Consejo de Administración de BERGÉ en fecha 25 de abril de 2023, se incorpora a la normativa interna y podrá ser revisada y/o modificada para adaptarse a las necesidades resultantes de la normativa aplicable, avances tecnológicos, y otros cambios relevantes en la organización.

La actualización de las sucesivas versiones de la Política y/u otros documentos necesarios para cumplir sus disposiciones será competencia del Departamento de Ciberseguridad.