POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y SEGURIDAD DE LOS ACTIVOS

COLBUN ES UNA EMPRESA LÍDER EN EL MERCADO ENERGÉTICO Y TENEMOS COMO PROPÓSITO TRANSFORMAR LA ENERGÍA, EN EQUILIBRIO CON EL PLANETA, PARA IMPULSAR TUS PROYECTOS Y SUEÑOS. EN ESTE ASPECTO, LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LOS ACTIVOS, LA INFORMACIÓN Y CIBERSEGURIDAD SON ACTIVIDADES IMPORTANTES DENTRO DE NUESTRO MODELO DE CREACIÓN DE VALOR, ES POR ESTO QUE NOS COMPROMETEMOS A APLICAR LAS MEDIDAS NECESARIAS PARA PROTEGER Y MITIGAR LOS RIESGOS PROVENIENTES DEL MUNDO DIGITAL, JUNTO CON LA PROTECCIÓN DE LA SEGURIDAD FÍSICA DE LAS PERSONAS, NUESTRAS INSTALACIONES Y LOS BIENES QUE SE ENCUENTRAN EN ELLAS.

ESTA POLÍTICA ES COMUNICADA A TODOS LOS TRABAJADORES, CONTRATISTAS, DIRECTORES Y FILIALES, POR LO TANTO, TODOS QUIENES INTEGRAN LA COMPAÑÍA TIENEN LA RESPONSABILIDAD DE APLICAR LOS PRINCIPIOS DESCRITOS A CONTINUACIÓN.

1. CULTURA Y CONCIENCIA

- Conscientes de los riesgos asociados a la seguridad de la información, la ciberseguridad y la protección de nuestros activos, nos comprometemos a fomentar una cultura de uso adecuado de la información, los recursos y las plataformas tecnológicas. Esto se logrará a través de programas continuos de sensibilización y capacitación, que proporcionen conocimientos, habilidades, experiencias y capacidades a todos los trabajadores de la compañía.

- La seguridad de la información, la ciberseguridad y la protección de los activos son responsabilidades compartidas, tanto por el personal interno como por terceros que interactúan con la Compañía. Por ello, cada uno de nosotros debe convertirse en un promotor activo de estas prácticas en el desarrollo de sus actividades diarias, identificando riesgos y escalando los casos alertas si es requerido.

2. IMPLEMENTACIÓN DE CONTROLES Y PRÁCTICAS

Las personas, gerencias, mesas y comités que conforman los modelos de gobierno de seguridad de la información, ciberseguridad y de protección de los activos de la Compañía deben:

- Administrar los riesgos de seguridad de la información, ciberseguridad y de protección de los activos, implementando medidas de identificación, protección, detección, respuesta y recuperación, evaluando la vulnerabilidad de los sistemas.

- Informar a las gerencias respectivas y adoptar medidas de recuperación urgentes ante la ocurrencia de infracciones o eventos que amenacen contra la seguridad de la información, ciberseguridad y seguridad de los activos.

- Implementar y mantener actualizadas las tecnologías de verificación, autorización y control de acceso a los sistemas e instalaciones de la Compañía, mediante controles lógicos y físicos, aplicando el principio de mínimo privilegio requerido. Todo lo anterior, siendo coherente con los principios de no discriminación y buen trato, establecidos en nuestro Código de Ética y Política de Derechos Humanos.

- Adaptarse con agilidad a las condiciones cambiantes del entorno de la seguridad de la información, ciberseguridad y la protección de las instalaciones, utilizando procesos y herramientas tecnológicas que permitan dar respuesta en forma rápida e innovadora a las necesidades de la Compañía.

- Cumplir con los requerimientos establecidos en la legislación vigente, estándares regulatorios, normas técnicas, políticas y procedimientos internos.

- Cumplir con los requerimientos establecidos en la legislación vigente, estándares regulatorios, normas técnicas, políticas y procedimientos.

- Colaborar con organizaciones, reguladores y asociaciones relevantes de la industria, con el fin de contribuir a la mejora global de la seguridad de la información, ciberseguridad y seguridad de los activos.

José Ignacio Escobar T.

CEO Colbún

- La presente política ha sido aprobada por el Directorio de Colbún con fecha 26 de Noviembre de 2024.