

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

EN COLBÚN SOMOS UNA EMPRESA QUE ASPIRA A SER UNA COMPAÑÍA LÍDER EN LA INDUSTRIA DE ENERGÍA. EN ESTE ASPECTO, LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD ES UN PROCESO IMPORTANTE DENTRO DE NUESTRO MODELO DE CREACIÓN DE VALOR. ES POR ESTO, QUE NOS COMPROMETEMOS A APLICAR LAS MEDIDAS NECESARIAS PARA MITIGAR LOS RIESGOS PROVENIENTES DEL MUNDO DIGITAL CON EL QUE INTERACTÚA LA COMPAÑÍA, RELACIONADOS PRIMERAMENTE A LAS PERSONAS, A LOS ACTIVOS FÍSICOS, INSTALACIONES, INFORMACIÓN Y CONTINUIDAD OPERACIONAL.

ESTA POLÍTICA ES COMUNICADA A LOS TRABAJADORES(AS), CONTRATISTAS, DIRECTORES(AS) DE COLBÚN Y FILIALES, POR LO TANTO, TODAS LAS PERSONAS EN COLBÚN SOMOS RESPONSABLES DE APLICAR LOS PRINCIPIOS DESCRITOS A CONTINUACIÓN.

1. CULTURA Y CONCIENCIA

En Colbún, conscientes de los riesgos e impactos referentes a seguridad de la información y ciberseguridad en nuestras actividades, nos preocupamos de desarrollar cultura y conciencia en el uso adecuado de la información, los recursos y las plataformas tecnológicas por medio de programas continuos de sensibilización y capacitación, que entregan conocimientos, habilidades, experiencias y capacidades para todos los trabajadores de la compañía.

La seguridad de la información y ciberseguridad es responsabilidad de todos quienes trabajan para la compañía; es por esto que cada uno debe ser un activo promotor de estos ámbitos en el desarrollo de sus actividades diarias.

2. IMPLEMENTACIÓN DE CONTROLES Y PRÁCTICAS

Las personas, gerencias y comités que forman el modelo de gobierno de seguridad de la información y ciberseguridad de la compañía deben:

- Potenciar las capacidades de identificación, protección, detección, respuesta y recuperación bajo estándares de clase mundial, frente a eventos e incidentes, que puedan comprometer la información, los datos, los ciberactivos, disponibilidad de operaciones, daño reputacional, pérdida de ventaja competitiva u otro impacto negativo a la compañía.

- Informar a las gerencias respectivas y adoptar medidas de recuperación urgentes ante la ocurrencia de infracciones o eventos que atenten contra la seguridad de la información o ciberseguridad.
- Mitigar los riesgos a través de controles lógicos y físicos, aplicando el principio de mínimo privilegio requerido.
- Adaptar con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas, a través de procesos, procedimientos y herramientas 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.
- Colaborar con organizaciones, reguladores y asociaciones relevantes de la industria, para contribuir a la mejora global de la seguridad de la información y ciberseguridad.

José Ignacio Escobar T.

CEO Colbún

- La presente política ha sido aprobada por el Directorio de Colbún con fecha 30 de agosto de 2022.
- Quienes forman parte del modelo de gobierno de seguridad y ciberseguridad de la compañía tienen la responsabilidad de gestionar el cumplimiento de los lineamientos aquí descritos.