I. Política

Esta Política General se fundamenta en los siguientes principios adoptados por Camanchaca, los cuales deben integrarse dentro de las funciones de cada colaborador:

Principios Estratégicos:

1) Promover las prácticas de Seguridad de la Información como parte integral de los valores y exigencias de la organización de cara a los clientes, sus asociados y la comunidad.
2) Centrar la estrategia de Seguridad de la Información en requerimientos y objetivos del negocio mediante un modelo de gestión y gobierno, que incluye personas, procesos y procedimientos.
3) Involucrar a los principales interesados de la Seguridad de la Información (responsables de activos de información y roles estratégicos relacionados) para asegurar altos estándares de protección de los activos en un entorno de colaboración.
4) Mantener vigente y actualizado el marco de controles de Seguridad de la Información y alinearlo a los controles de seguridad de la información y seguridad corporativa.
5) Gestionar riesgos de Seguridad de la Información, sean operacionales, organizacionales o aportados por terceros, manteniendo la exposición dentro de límites aceptables.
6) Asegurar que los controles de ciberseguridad son proporcionales, balancean costo-beneficio y facilitan y acompañan la innovación.

Principios Operacionales:

7) Comunicar efectivamente la existencia y características, además del desempeño y cumplimiento de los controles de Seguridad de la Información a todos los interesados.
8) Alinear los controles corporativos de Seguridad de la Información a la legislación y regulación vigente.
9) Instaurar una cultura de ciberseguridad en todo el personal, incluido en plantas y entornos operacionales, así como en terceros y proveedores involucrados en la producción, incluido las obligaciones de cuidado en los contratos de trabajo
10) Brindar un marco de controles de Seguridad de la Información que ayude a proteger y rentabilizar las tecnologías de información, las tecnologías operacionales y activos relacionados.
11) Aplicar los controles con foco en la continuidad operacional e integrar los controles de Seguridad de la Información dentro de los planes de continuidad de la organización.
12) Atender oportunamente eventos e incidentes de Seguridad de la Información para disminuir el impacto financiero, reputacional, regulatorio y medioambiental.

II. Roles y Responsabilidades

Comité de Seguridad de la Información: Es la entidad definida para el gobierno de la ciberseguridad TI (Tecnologías de la Información) y TO (Tecnologías de la Operación), lo que incluye la responsabilidad de sancionar, validar y aprobar el conjunto normativo requerido para la gestión de ciberseguridad TI y TO y todas aquellas actividades de supervisión y control relacionadas con los programas de Seguridad de la Información. Este comité sesionará de forma trimestral y estará conformado por: Gerente Corporativo de TI, Gerente Corporativo de Finanzas, Gerente Corporativo de Auditoría, Responsable de Continuidad de Negocios TI, Ingeniero de Ciberseguridad, y Gerente de Asuntos Legales (opcional), Gerente General Corporativo (opcional) y Gerentes Generales Unidades de Negocio (opcional). Su ámbito de acción y responsabilidades estarán definidas en un reglamento específico.

Comité de directores: Supervisar la estrategia de ciberseguridad y seguridad de la información de la compañía, además de participar en sesiones para evaluar y analizar los diferentes riesgos, ya sean operacionales, financieros, tecnológicos, etc.