Directriz de Seguridad de la Información

Vigencia: Mayo 2026

SISCONVE
SISTEMA DE CONTROL VEHICULAR

Propósito

SISCONVE reconoce la información y los activos tecnológicos asociados como recursos estratégicos para la operación del negocio. La presente directriz tiene como propósito establecer los lineamientos generales para proteger la confidencialidad, integridad y disponibilidad de la información, asegurando la continuidad de los servicios y el cumplimiento de los requisitos legales, regulatorios, contractuales y corporativos aplicables.

Compromiso de la dirección

La dirección del SISCONVE manifiesta su compromiso con la protección de la información y con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), alineado con los requisitos de la norma ISO/IEC 27001:2022 y con los lineamientos corporativos de ANCAP.

Para ello, se compromete a:

- Implementar y mantener controles de seguridad de la información adecuados al contexto del negocio y a los riesgos identificados.
- Proteger la confidencialidad, integridad y disponibilidad de la información y de los activos tecnológicos asociados.
- Gestionar los riesgos de seguridad de la información mediante un enfoque basado en riesgos.
- Establecer y revisar periódicamente objetivos de seguridad de la información alineados a las necesidades estratégicas y operativas.
- Cumplir los requisitos legales, regulatorios, contractuales y corporativos aplicables en materia de seguridad de la información y ciberseguridad.
- Promover una cultura organizacional de seguridad mediante actividades de concientización y capacitación continua para colaboradores y terceros.
- Asignar los recursos, roles y responsabilidades necesarios para la gestión efectiva del SGSI.
- Gestionar y responder oportunamente ante incidentes de seguridad de la información, minimizando su impacto operativo y reputacional.
- Supervisar los riesgos asociados a proveedores, terceros que participen en la operación de BackOffice de SISCONVE.
- Garantizar la continuidad operativa y resiliencia de los servicios críticos mediante medidas de protección, respaldo y recuperación.
- Evaluar periódicamente la efectividad de los controles implementados y promover la mejora continua del SGSI.
- Integrar la seguridad de la información en los procesos, proyectos, tecnologías y decisiones estratégicas.