# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## Nuestro compromiso

ITS InfoCom reconoce la información como uno de sus activos más valiosos y esenciales para la prestación de sus servicios. Por ello, mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) orientado a proteger la información de clientes, colaboradores, proveedores y demás partes interesadas.

La Alta Dirección respalda el desarrollo, mantenimiento y mejora continua del SGSI, promoviendo una cultura organizacional basada en la seguridad de la información, la protección de datos personales, la ciberseguridad, la gestión de riesgos y la continuidad del negocio.

ITS InfoCom integra la seguridad de la información como un habilitador estratégico de sus servicios de soporte, monitoreo, operación y gestión tecnológica, buscando proteger la información confiada por sus clientes y contribuir a la prestación segura, confiable y continua de sus servicios.

## Objetivo

Establecer los lineamientos generales que permitan proteger la confidencialidad, integridad y disponibilidad de la información, gestionar adecuadamente los riesgos de seguridad de la información y ciberseguridad, fortalecer la resiliencia operacional y generar confianza en clientes, colaboradores, proveedores y demás partes interesadas.

## Alcance

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que tengan acceso a la información o a los activos de información administrados por ITS InfoCom en el desarrollo de sus actividades y en la prestación de los servicios de la organización.

## Principios de Seguridad de la Información

ITS InfoCom se compromete a:

- Proteger la confidencialidad de la información, garantizando el acceso únicamente a personas autorizadas.
- Preservar la integridad de la información, asegurando su exactitud, consistencia y confiabilidad.

- Garantizar la disponibilidad de la información y de los servicios cuando sean requeridos.
- Gestionar y proteger los activos de información durante todo su ciclo de vida.
- Gestionar de manera sistemática los riesgos relacionados con la seguridad de la información y la ciberseguridad.
- Implementar controles para prevenir, detectar, responder y recuperarse de eventos e incidentes de seguridad de la información.
- Promover una cultura de seguridad mediante actividades de formación, sensibilización y adopción de buenas prácticas.
- Mantener controles para la gestión de accesos y la protección de la información de acuerdo con las necesidades del negocio.
- Fomentar relaciones seguras con proveedores y terceros que tengan acceso a información o activos de la organización.
- Cumplir los requisitos legales, regulatorios, contractuales y demás obligaciones aplicables.
- Mantener un enfoque de mejora continua que permita fortalecer la eficacia del Sistema de Gestión de Seguridad de la Información.

**Protección de Datos Personales**

ITS InfoCom reconoce la importancia de la protección de los datos personales y se compromete a tratarlos de manera responsable, segura y conforme a la legislación vigente aplicable. La organización implementa medidas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información personal, previniendo su acceso no autorizado, alteración, divulgación, pérdida o uso indebido, y garantizando el respeto de los derechos de los titulares de los datos.

**Ciberseguridad**

ITS InfoCom promueve la adopción de prácticas de ciberseguridad orientadas a proteger sus servicios, sistemas de información, infraestructura tecnológica y activos digitales frente a amenazas internas y externas. Para ello, fortalece continuamente sus capacidades de prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad, contribuyendo a la continuidad del negocio y a la resiliencia operacional.

La organización promueve la colaboración con clientes, proveedores, aliados estratégicos y demás partes interesadas para fortalecer la seguridad de la

información, la ciberseguridad y la protección de los datos personales dentro del ecosistema digital en el que opera.

**Gestión de Riesgos**

La organización identifica, analiza, evalúa y trata los riesgos asociados a la seguridad de la información, la ciberseguridad y la protección de datos personales, estableciendo medidas de control proporcionales al contexto del negocio y a las necesidades de protección de los activos de información.

**Responsabilidades**

Todos los colaboradores, contratistas, proveedores y terceros que tengan acceso a la información o a los activos de información de ITS InfoCom son responsables de cumplir esta política, proteger la información bajo su custodia, aplicar las buenas prácticas de seguridad definidas por la organización y reportar oportunamente cualquier evento o incidente que pueda comprometer la seguridad de la información.

**Cumplimiento y Mejora Continua**

ITS InfoCom revisa de manera periódica su Sistema de Gestión de Seguridad de la Información para garantizar su adecuación, eficacia y alineación con las necesidades del negocio, los requisitos aplicables y las expectativas de las partes interesadas.

Con el propósito de fortalecer la confianza y la seguridad en sus operaciones, ITS InfoCom mantiene un Sistema de Gestión de Seguridad de la Información basado en los principios y mejores prácticas de la norma ISO/IEC 27001:2022, promoviendo la mejora continua, la gestión de riesgos, la protección de datos personales, la gestión de accesos, la gestión de incidentes de seguridad y la protección de los activos de información en todos sus procesos.

ITS InfoCom reafirma su compromiso con la protección de la información, la ciberseguridad, la privacidad de los datos personales, el cumplimiento de los requisitos legales y regulatorios, la gestión de riesgos y la mejora continua de sus prácticas de seguridad, contribuyendo a la generación de confianza y al fortalecimiento de las relaciones con clientes, colaboradores, proveedores y demás partes interesadas.

Esta política es comunicada a colaboradores, clientes, proveedores y demás partes interesadas como evidencia del compromiso de ITS InfoCom con la seguridad de la información, la protección de datos personales, la ciberseguridad, la continuidad del

negocio, el cumplimiento normativo, la gestión de riesgos y la prestación segura y confiable de sus servicios.

Publico