POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Confecámaras reconoce que la información es un activo estratégico y esencial para el cumplimiento de su misión organizacional. En consecuencia, se compromete a planear, implementar, mantener y mejorar continuamente su Sistema de Gestión de Seguridad de la Información (SGSI), de conformidad con la norma ISO/IEC 27001:2022, alineado con su estrategia organizacional, su estructura de gobierno y su modelo de gestión.

Este compromiso incluye:

- La protección de la confidencialidad, integridad, disponibilidad y privacidad de la información.
- La definición, seguimiento y revisión periódica de objetivos de seguridad de la información, medibles y coherentes con el contexto organizacional.
- La identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, considerando amenazas cibernéticas, riesgos tecnológicos, operativos y de privacidad.
- La asignación de roles, responsabilidades y recursos necesarios para la operación eficaz del SGSI.
- El cumplimiento de los requisitos legales, regulatorios, contractuales y otros aplicables, incluidos los relacionados con la protección de la privacidad.
- La integración del SGSI con los procesos del negocio y la adopción de un enfoque de mejora continua, basado en el ciclo Planear–Hacer–Verificar–Actuar (PHVA).

OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Confecámaras establece como objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) los siguientes:

- Desarrollar e implementar iniciativas y proyectos de mejora continua que fortalezcan la eficacia del Sistema de Gestión de Seguridad de la Información de Confecámaras.
- Identificar, evaluar y reducir el nivel de los riesgos de seguridad de la información dentro del alcance del SGSI a un estado aceptable, mediante la implementación de controles que protejan la confidencialidad, integridad y disponibilidad de la información.
- Detectar, gestionar y responder oportunamente a los incidentes de seguridad de la información, conforme a los procedimientos establecidos, minimizando su impacto operativo, legal y reputacional.
- Promover la conciencia y cultura de seguridad de la información en los colaboradores y terceros que hacen parte del SGSI, mediante programas de capacitación, comunicación y sensibilización.
- Garantizar la observabilidad y monitoreo de los activos de información que soportan los servicios tecnológicos críticos dentro del alcance del SGSI.