SGSI.POL.01 Política de Seguridad de la Información y Ciberseguridad

CANVIA y sus filiales, en el marco de sus Sistemas Integrados de Gestión (SIG), establecen el Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema está compuesto por un conjunto de políticas, procedimientos, guías, recursos y actividades asociadas que, mediante su implementación, operación, monitoreo y mejora continua, garantizan la conservación de la confidencialidad, integridad y disponibilidad de la información para alcanzar los objetivos estratégicos de la organización.

En ese sentido, CANVIA implementa mecanismos de seguridad de la información y ciberseguridad para proteger todo tipo de información, considerándola un activo crítico. Estos mecanismos aseguran la protección adecuada contra cualquier amenaza interna o externa que pueda comprometer la seguridad de la información, garantizando la continuidad operativa y la resiliencia de la organización y sus clientes frente a incidentes graves.

El SGSI, también abarca la ciberseguridad y tiene como objetivos estratégicos proteger los activos de información del negocio, controlar los riesgos asociados, anticiparse a los eventos de seguridad de la información y responder de manera inmediata a los incidentes.

Para gestionar de manera efectiva y permanente los riesgos de seguridad de la información y ciberseguridad, se establecen controles organizacionales, de personas, físicos y tecnológicos, los cuales ayudan a minimizar el impacto en los sistemas y servicios de la organización.

CANVIA, se compromete a satisfacer los requisitos legales, normativos y regulatorios aplicables a la seguridad de la información y ciberseguridad, apoyando la mejora continua y la eficacia del SGSI.

La Alta Dirección de CANVIA, determina y asigna la responsabilidad del gobierno de la Seguridad de la Información y la Ciberseguridad siguiendo los lineamientos mencionados anteriormente. Además, se enfoca en fortalecer las capacidades y conocimientos de nuestros colaboradores y partes interesadas, promoviendo las mejores prácticas en seguridad de la información y ciberseguridad.

Políticas y documentos relacionados:

- ✓ SGCP.R.01 Reglamento Interno de Gestión del Canal Ético
- ✓ SGCP.POL.04 Código de Ética y Conducta
- ✓ SGCP.I.01 Protocolo para el uso del Canal Ético
- ✓ GH.R.01 Reglamento Interno
- ✓ SGSI.POL.02 Política de control de acceso
- ✓ SGSI.POL.03 Política para la clasificación de información
- ✓ SGSI.POL.04 Política de seguridad física
- ✓ SGSI.POL.05 Política de seguridad para usuarios finales
- ✓ SGSI.POL.06 Política de respaldo de información
- ✓ SGSI.POL.07 Política para el intercambio de información
- ✓ SGSI.POL.08 Política de protección contra el malware
- ✓ SGSI.POL.09 Política de gestión de vulnerabilidades técnicas
- ✓ SGSI.POL.10 Política de uso de controles criptográficos
- ✓ SGSI.POL.11 Política de seguridad en las comunicaciones
- ✓ SGSI.POL.12 Política de privacidad y protección de datos personales
- ✓ SGSI.POL.13 Política de seguridad con proveedores y terceras partes
- ✓ SGSI.POL.14 Política de seguridad en aplicaciones
- ✓ SGSI.POL.15 Política de gestión del riesgo de seguridad de la información
- ✓ SGSI.POL.16 Política de uso de programas de computadoras
- ✓ SGSI.POL.17 Política de Prevención de Pérdida de Datos

Hugo Goicochea
CEO

Fecha: 18/06/2024
Versión: 07