POLITICA GENERAL

SEGURIDAD DE LA INFORMACIÓN

Versión: 1.0

POLÍTICA GENERAL
DE SEGURIDAD DE LA INFORMACIÓN

Introducción

En EIKON S.A. reconocemos que la información y los datos personales que administramos constituyen activos esenciales para nuestro negocio y para la confianza de clientes, aliados y colaboradores. Con el avance constante de la tecnología y la creciente digitalización, las ciber amenazas y las exigencias regulatorias, es fundamental establecer políticas y prácticas sólidas para garantizar la confidencialidad, integridad y disponibilidad de los activos de información bajo nuestra custodia.

La presente política de seguridad de la información se basa en los principios y requisitos establecidos en la norma ISO/IEC 27001:2022 de Seguridad de la Información, así como en la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP) y demás normativa aplicable.

La Alta Dirección de EIKON S.A. respalda plenamente esta política y se compromete a proporcionar los recursos necesarios para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo, a la vez que promueve una cultura organizacional basada en la seguridad, la privacidad y la mejora continua.

Alcance

Esta política aplica a todos los procesos, sistemas, servicios y activos de información que EIKON S.A. administra, así como a toda la información corporativa recolectada, procesada, transmitida, almacenada o custodiada por la organización, independientemente de su formato o medio.

Su cumplimiento es obligatorio para todo el personal interno, contratistas, proveedores, terceros y aliados que tengan acceso a dichos activos y datos personales, e incluye también la infraestructura tecnológica, las plataformas en la nube y el personal que participa en la operación.

Objetivos de seguridad de la información

Objetivo General

Establecer un marco de referencia para proteger los activos de información EIKON S.A., garantizando su **confidencialidad, integridad, disponibilidad y privacidad**, en cumplimiento con los requisitos de la norma ISO/IEC 27001:2022, además de los requisitos legales, regulatorios y contractuales aplicables.

Objetivos Específicos

1. **Autenticación y control de acceso. -** Garantizar que solo los usuarios autorizados tengan acceso a los sistemas y activos de información, mediante la implementación de mecanismos de autenticación y control de acceso efectivos.
2. **Cumplimiento normativo. -** Asegurar que la organización cumpla con todas las leyes, regulaciones y normativas aplicables relacionadas con la seguridad de la información.
3. **Gestión de riesgos. -** Identificar, evaluar y gestionar los riesgos de seguridad de la información de manera sistemática, implementando controles adecuados para mitigarlos y minimizar su impacto.
4. **Concienciación y capacitación. -** Promover la conciencia y la capacitación en seguridad de la información entre los empleados y partes interesadas de la organización, para fomentar buenas prácticas de seguridad y reducir el riesgo de incidentes de seguridad.

La Alta Dirección define, evalúa y actualiza estos objetivos conforme a los riesgos y prioridades del negocio.

Principios

1. **Liderazgo comprometido. -** La Alta Dirección provee liderazgo y los recursos necesarios para implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI).
2. **Gestión de riesgos. -** El SGSI se rige por una metodología de gestión de riesgos basada en ISO/IEC 27005 e ISO 31000, la Alta Dirección aprueba los criterios de evaluación y el nivel de riesgo aceptable. Se

identifican y evalúan los riesgos de seguridad de la información, y se implementan controles adecuados para mitigarlos.

3. **Cumplimiento legal y normativo. -** La organización cumple con todas las leyes, regulaciones y normativas aplicables relacionadas con la seguridad de la información.
4. **Responsabilidad y rendición de cuentas. -** Todos los empleados y partes interesadas son responsables de proteger la información y cumplir con las políticas y controles establecidos.
5. **Concienciación y formación. -** Se promueve la conciencia y capacitación en seguridad de la información para todos los empleados y partes interesadas relevantes.
6. **Mejora continua. -** Se busca la mejora continua del SGSI a través de la revisión regular, la identificación de áreas de mejora y la implementación de acciones correctivas y preventivas.

Compromiso de la dirección

La Alta Dirección provee los recursos humanos, tecnológicos y financieros para implementar, operar y mejorar el SGSI; designa roles y responsabilidades, aprueba los objetivos, indicadores de gestión y participará anualmente en la revisión por la dirección, asegurando la mejora continua y el alineamiento con la estrategia del negocio.

Asignación de responsabilidades

- **Alta Dirección. -** Proporciona liderazgo y recursos para la implementación del SGSI.
- **Líderes de proceso. -** Aseguran la aplicación de los controles de seguridad y la difusión de las buenas prácticas en sus equipos.
- **Empleados y partes interesadas. -** Cumplen con esta política y reportan cualquier incidente o vulnerabilidad detectada.

Cambios y excepciones

La Alta Dirección debe aprobar cualquier cambio en la política de seguridad de la información, así como también aprobar formalmente cualquier excepción a los controles aplicados al SGSI.

Comunicación

Esta política será comunicada a todos los colaboradores, contratistas y proveedores, publicada en los canales oficiales de la organización y revisada anualmente o cuando se produzcan cambios significativos en el negocio, la normativa o los riesgos asociados.