Política General de Seguridad de la Información de Minderest

Política General de Seguridad de la Información

La Dirección de Minderest reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, casos de estudio, códigos fuente, proyectos de I+D+i, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información conforme con la norma ISO 27001.

La Seguridad de la Información se caracteriza como la preservación de:

a) su **confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;
b) su **integridad**, asegurando que la información y sus métodos de proceso son exactos y completos;
c) su **disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles han sido establecidos para asegurar que se cumplen los objetivos específicos de seguridad de la empresa.

Es política de Minderest que:

1. Se establezcan anualmente objetivos con relación a la Seguridad de la Información.
2. Se desarrolle un proceso de análisis del riesgo y de acuerdo a su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos en el Manual del Sistema de Gestión de Seguridad de la Información en Minderest.
3. Se establezcan los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de análisis de riesgos manejado.
4. Se cumpla con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad.

5. Se brinde concienciación y entrenamiento en materia de seguridad de la información a todo el personal.
6. Se establezcan los medios necesarios para garantizar la continuidad del negocio de la empresa.
7. Se sancione cualquier violación a esta política y a cualquier política o procedimiento del SGSI.

Esta política aplica a Minderest, sus trabajadores, colaboradores externos, partners y proveedores.

Todo empleado de Minderest es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas, así como de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al Sistema de Gestión de Seguridad de la Información.

El Security Manager de Minderest es responsable directo sobre el mantenimiento de esta política por brindar consejo y guía para su implementación, así como también investigar toda violación reportada de la misma.

Revisión	5
Aprobado por	Antonio Tomás, CEO
Fecha	18 Abril 2024