Minderest

# Política General de Seguridad de la información de Minderest

# Índice

# 1. 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, bases de conocimiento, manuales, casos de estudio, códigos fuente, 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 objetivos de control y 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.

Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.

Todo empleado es responsable 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 Manual del Sistema de Gestión de Seguridad de la Información en Minderest.

El Jefe de Seguridad de la Información es responsable directo sobre el mantenimiento de esta política por brindar consejo y guía para su implementación, así como también investigar toda violación reportada por el personal.

# 2. Política General de Seguridad y Privacidad de la Información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de Minderest con respecto a la protección de los activos de información (los empleados, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instrucciones, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La dirección de Minderest, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Minderest, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus trabajadores, colaboradores externos, partners y proveedores, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instrucciones en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los empleados, terceros y clientes de Minderest.
- Garantizar la continuidad del negocio frente a incidentes.

Minderest ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, los requerimientos regulatorios, y la norma ISO 27001.

A continuación se establecen 12 principios de seguridad que soportan el SGSI de Minderest:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
2. Minderest protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
3. Minderest protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. Minderest protegerá su información de las amenazas originadas por parte del personal.
5. Minderest protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. Minderest controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. Minderest implementará control de acceso a la información, sistemas y recursos de red.
8. Minderest garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. Minderest garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10. Minderest garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
11. Minderest garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
12. Minderest se compromete a la formación, concienciación y sensibilización continua en materia de seguridad de la información a todas las personas que forman parte de la organización.

| | |
|---|---|
| **Revisión** | 4 |
| **Aprobado por** | Antonio Tomás, CEO |
| **Fecha** | 15 Junio 2023 |