POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo, Alcance y Usuarios

El objetivo de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.
El Alcance de esta política se aplica a todo el Sistema de gestión de seguridad de la información (SGSI), según se define en el Documento del Alcance del SGSI y es ampliada mediante las políticas específicas, que profundizan la implementación de los controles de seguridad de la información.
Los usuarios de este documento son todos los empleados de Minder S.A., como también partes externas relevantes.

Postulados de la seguridad de la Información

Los postulados de seguridad de la información tomados como base para esta política son:

La **confidencialidad**: Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

La **integridad** Propiedad de la información de exactitud y completitud de la información incluyendo que no sea alterada de manera no autorizada.

La **disponibilidad**: Propiedad de ser accesible y estar listo en el momento que se lo requiera para su uso a demanda de una entidad autorizada.

Estos principios y otros conceptos clave como la autenticidad, la trazabilidad y no repudio serán tenidos en cuenta para todas las políticas y procedimientos que deriven de ésta.

Política Contractual

Todas las relaciones contractuales con terceros (proveedores, socios, clientes, etc.) deben cumplir con estos postulados de seguridad de la información, por lo que la redacción de las cláusulas de los acuerdos que impliquen manejo de información deben respetarlos.

Terminología básica sobre seguridad de la información

Activo de información: En el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

Propietario de activo de información: persona o área de la organización que tiene la responsabilidad y autoridad sobre dicho activo, y debe asegurar que se implementen las medidas de seguridad adecuadas para protegerlo.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

Sistema de gestión de seguridad de la información (SGSI): consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos. El análisis de los requisitos para la protección de los activos de información y la

aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.

Objetivos y medición

Los objetivos generales para el sistema de gestión de seguridad de la información son los siguientes:

· Preservar la confidencialidad, integridad y disponibilidad de la información de la empresa, de sus clientes y terceros, conforme a los requisitos legales, normativos y obligaciones contractuales.
· Analizar, gestionar y tratar los riesgos de seguridad de los activos de información, incluyendo el incumplimiento legal.
· Prevenir, evitar y reducir el daño ocasionado por potenciales incidentes de seguridad de la Información.
· Promover la formación y concientización en materia de seguridad de la información de los colaboradores.
· Promover la mejora continua del sistema de gestión de seguridad de la información.

La Dirección de la empresa es responsable de establecer, revisar y aprobar periódicamente los objetivos medibles de seguridad de la información, alineados con la estrategia organizacional. Estos objetivos se monitorean y gestionan a través de un tablero de control interno, cuyo seguimiento y cumplimiento es responsabilidad de la Dirección.

Apoyo para la implementación del SGSI

La Dirección de Minder S.A. reconoce la importancia de la Seguridad de la información y los activos relacionados con los servicios que proporciona la empresa para fines comerciales.
Para ello:

· Establece, implementa y opera el sistema de gestión de la seguridad de la información (SGSI) conforme la norma ISO/IEC 27001:2022.
· Brinda los recursos para el correcto funcionamiento del SGSI a partir del análisis del riesgo.
· Protege la confidencialidad e integridad de los datos, aplicaciones e infraestructuras de Minder S.A. conforme a las normas legales vigentes.
· Brindar los servicios acordados con los clientes de acuerdo al SLA comprometido.

Roles y responsabilidades

La presente política define las responsabilidades de los principales roles involucrados en el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. Las funciones y responsabilidades generales de cada puesto se encuentran detalladas en el documento "Funciones y Responsabilidades" de la empresa. A continuación, se detallan las responsabilidades específicas de cada rol en relación con el SGSI.

Dirección de la empresa

· Establecer, revisar y aprobar la política de seguridad de la información.
· Definir, revisar y aprobar los objetivos medibles de seguridad de la información.
· Asegurar la disponibilidad de recursos necesarios para la implementación y mantenimiento del SGSI.
· Liderar y promover una cultura de seguridad de la información en la organización.
· Revisar periódicamente el desempeño del SGSI y tomar acciones correctivas cuando sea necesario.
· Asegurar el cumplimiento de esta política y de tomar las medidas disciplinarias o legales necesarias en caso de infracciones.

Gerente de seguridad de la información (CISO -Chief Information Security Officer)

· Desarrollar, implementar y mantener el SGSI de acuerdo a la norma ISO 27001.
· Asesorar a la Dirección en temas de seguridad de la información.
· Gestionar los riesgos de seguridad de la información.

· Coordinar la implementación de controles de seguridad.
· Gestionar incidentes de seguridad y coordinar las acciones de respuesta.
· Promover la concientización y capacitación en seguridad de la información.

Comité de seguridad
· Revisar y aprobar políticas, procedimientos y estándares de seguridad.
· Monitorear el desempeño del SGSI y proponer mejoras.
· Resolver conflictos y excepciones relacionadas con la seguridad.
· Promover la mejora continua del SGSI.

Propietarios de activos
· Clasificar y proteger adecuadamente los activos de información bajo su custodia.
· Definir y revisar los requisitos de seguridad para los activos.
· Asegurar que los controles de seguridad se implementen correctamente.
· Monitorear el uso y acceso a los activos de información según Políticas específicas del SGSI.

Empleados
· Conocer, comprender y cumplir con la política de seguridad de la información.
· Participar en las actividades de concientización y capacitación.
· Reportar incidentes de seguridad o sospecha de violaciones.
· Proteger adecuadamente la información y los activos a su cargo.

Proveedores
· Cumplir con los requisitos de seguridad de la información establecidos en los contratos y acuerdos de nivel de servicio (SLAs).
· Reportar incidentes de seguridad que puedan afectar a la organización.
· Mantener la confidencialidad de la información de la organización.
· Participar en las actividades de seguridad cuando sea requerido.

Cumplimiento
El incumplimiento de esta Política de Seguridad de la Información y de los procedimientos y controles establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI) puede llevar medidas disciplinarias según el Código de Conducta de la empresa y el Procedimiento de Acciones Disciplinarias.

Todos los empleados y partes externas relevantes deben cumplir con los requisitos de seguridad de la información definidos en esta política y en los documentos que la complementan. El incumplimiento intencional o negligente de dichos requisitos será considerado una falta y podrá dar lugar a sanciones, incluyendo la terminación del contrato de trabajo o de la relación contractual, según corresponda.
Adicionalmente, la organización se compromete a cumplir con todos los requisitos legales, normativos y contractuales aplicables a la seguridad de la información. El incumplimiento de estos requisitos también podrá conllevar acciones legales y sanciones.

La presente Política es revisada periódicamente para asegurar su continua adecuación a las necesidades y servicios de Minder.

Fecha de revisión: 08/11/2024