Política General de Seguridad de la información y Protección de Datos

Cod.	POL-001
Versión	4.0
Fecha de Vigencia	18-06-2025
Tipo de documento	Política
Clasificación	Público

Tabla de contenidos

Control de cambios

Versión	Descripción	Fecha	Realizado por	Aprobado por
1.0	Versión inicial del documento	16-03-2018	Felipe Seguel	Víctor Cortés
2.0	Modificaciones con actividades específicas de seguridad.	26-01-2021	Felipe Seguel	Víctor Cortés
3.0	-Se amplía el documento a los sistemas del Grupo.	27-03-2025	Gerente de TI: Felipe Seguel	Gerente General: Paula Vidal Director Ejecutivo: Víctor Cortés
3.5	Cambio de Nombre a Política general de Seguridad de información y separación en Procedimiento y Política	28-05-2025	Gerente de TI: Felipe Seguel	
4.0	Cambios específicos en controles vigentes. Por sugerencias comité-	16-06-2025	Gerente de TI	Comité de Seguridad (18/06/2025)

1. Introducción

Grupo Mitiga reconoce a la información como un activo relevante e imprescindible para el cumplimiento de sus objetivos estratégicos, siendo su adecuada custodia responsabilidad de todos quienes tengan acceso a ella, independiente de la región en que se encuentren y la solución sobre la que presten servicio (B-GRC, Ética en Línea, Regulatek y RIS). Debiendo sus lineamientos ser cumplidos por los directores, ejecutivos, desarrolladores y cualquier colaborador; así como por oferentes, proveedores, asesores o prestadores de servicios.

Dado que la mayor parte de la información se procesa, distribuye y almacena en medios tecnológicos, se hace imprescindible que todos quienes trabajen o colaboren con Grupo Mitiga observen y respeten las normas de seguridad de la información, custodiando adecuadamente ésta, así como la tecnología por dónde transita o se almacena.

Se entenderá como “Seguridad de la Información” la preservación de la confidencialidad, integridad y disponibilidad de la información y la protección de ésta, de una amplia gama de amenazas, a fin de minimizar el daño, garantizar la continuidad operacional, de manera de cumplir los objetivos estratégicos del Grupo.

Este documento presenta la política general de seguridad de la información y protección de datos adoptadas en el desarrollo, uso y administración de los sistema para Grupo Mitiga, y entrega los lineamientos y principios básicos que permitirán el correcto resguardo de la información, los que se complementarán con diversas políticas, normas y procedimientos de carácter específicas, desarrollando de esta forma un adecuado entorno de seguridad y control, que permita alcanzar los objetivos estratégicos y dar un apropiado cumplimiento a los requisitos de seguridad de la información y protección de datos de nuestros clientes, la legislación y regulación específica de nuestros clientes y cualquier persona relacionada con nuestras soluciones. .

De esta manera, se hace imprescindible el conocimiento de esta política por nuestros colaboradores, clientes, proveedores y diversas partes relacionadas. Para este fin, la misma será de carácter público y estará a disposición de las partes interesadas en el sitio web oficial de Grupo Mitiga.

2. Objetivo

Establecer los principios, directrices y compromisos de Grupo Mitiga respecto a la Seguridad de la Información y protección de datos, con el fin de proteger sus activos de información y a sus clientes y partes interesadas, contra amenazas internas o externas, deliberadas o accidentales, asegurando su confidencialidad,

integridad y disponibilidad. Esta política es parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) implementado por la organización.

3. Objetivos específicos

Las Política de Seguridad de la Información contenidas en el presente documento se dictan teniendo como objetivo realizar una gestión adecuada que permita garantizar la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la organización contemplando:

- La creación y definición de políticas generales y específicas que faciliten la ejecución de las actividades de tecnología de la información en las diferentes áreas de la organización.
- Promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos con los que cuenta la compañía.
- Normar los procesos de información con la finalidad de mejorar el rendimiento de la organización.
- Establecer las políticas para resguardo y garantía de acceso apropiado de la información de la organización.

4. Alcance

Los lineamientos contenidos en este documento deben ser conocidos y cumplidos por todo el personal, proveedores y/o agentes externos que intervengan o interactúen con Grupo Mitiga. haciendo uso de las herramientas computacionales dispuestas por ésta y/o tengan acceso a información de propiedad de la entidad.

Adicionalmente cabe mencionar que:

- Si existiese conflicto entre la normativa legal aplicable y la Política de Seguridad de la Información prevalecerá la normativa legal.
- Las tecnologías de información dispuestas por Grupo Mitiga deben de ser empleadas de acuerdo con los lineamientos establecidos por la compañía. De existir excepciones y/o modificaciones a esta regla, estas tendrán que ser informadas al comité de Seguridad de la información y protección de datos.

5. Valores

La Política General de Seguridad de la Información de Grupo Mitiga, se basa en los siguientes valores los cuales debe de ser cumplidos por todos los miembros de la organización:

- Integridad: Toda la información y todas las operaciones deben de encontrarse libres de errores y/o irregularidades de cualquier índole, garantizando así la integridad y exactitud de esta.
- Disponibilidad: Los sistemas y la información contenida en ellos, así como la información almacenada en cualquier dispositivo o servicio del grupo, deben ser correctamente resguardados, permitiendo su recuperación en forma rápida y completa ante cualquier hecho contingente que interrumpa su operatoria y dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento. Así también, se deben implementar los controles apropiados para garantizar la adecuada disponibilidad de los sistemas y la información propiedad de nuestros clientes.
- Confidencialidad: La información de Grupo Mitiga y de sus clientes debe estar protegida del uso no autorizado y de revelaciones accidentales, errores, fraudes, sabotaje, espionaje industrial, violación de privacidad y otras acciones que pudieran perjudicarla.

6. Funciones y Responsabilidades para la Seguridad de la Información y protección de datos

- Grupo Mitiga establece la implementación de un Sistema de Gestión de Seguridad de la Información -SGSI-, con la finalidad de asegurar la existencia y ejecución de controles periódicos, minimizando de esta forma los riesgos de Seguridad de la Información y protegiendo los activos de información frente a amenazas del entorno.
- Se conforma un Comité de Seguridad de la información y protección de datos, quien tiene como responsabilidad la aprobación de las políticas y normas para la adecuada administración y gestión del riesgo de Seguridad de la Información. La elaboración de estas políticas debe contemplar la ejecución de revisiones periódicas, las cuales se efectuarán de forma anual. Este comité sesionará de forma mensual, sancionando nuevas políticas y procedimientos, evaluando

presupuestos y proyectos de seguridad de la información y protección de datos, generando lineamientos de seguridad, aprobando modificaciones y/o implementaciones de controles que afecten al negocio, iniciativas que pueden surgir desde cualquier miembro de la organización.

- Es responsabilidad de todos los colaboradores de Grupo Mitiga el participar activamente en las distintas capacitaciones y procesos de concientización al que la organización lo invite, para efecto de obtener conocimientos de sus responsabilidades y deberes para con la información de Grupo Mitiga y sus clientes.
- El Director Ejecutivo, en conjunto con el Gerente General entregan su apoyo al proceso de administración y gestión del riesgo de Seguridad de la Información, proporcionando directrices claras, destinando recursos, definiendo prioridades y potenciando una cultura de Seguridad de la Información y protección de datos en Grupo Mitiga.
- El Oficial de Seguridad de la Información es responsable de difundir las políticas, reglamentos y procedimientos de Seguridad de la Información y Protección de Datos a todos los trabajadores de Grupo de Mitiga, como también a sus Proveedores y Terceros que participen directamente en los procesos críticos del negocio, reforzando que todas las partes entiendan y cumplan con su responsabilidad.
- El Oficial de Seguridad de la Información es responsable de controlar el cumplimiento de requerimientos legales relacionados a Seguridad de la Información y protección de datos y supervisando la aplicación de todos los controles, a través de revisiones periódicas, con el objetivo de reaccionar de forma proactiva ante cualquier hallazgo y mejorar la efectividad del SGSI.
- Es responsabilidad de cada Trabajador, Proveedor y/o Tercero reportar al Oficial de Seguridad de la Información cualquier Incumplimiento de la Política, normas y/o procedimientos asociados a Seguridad de la Información y protección de datos.
- La Gerencia de Tecnología y Ciberseguridad, es responsable de definir, difundir y controlar la identificación de riesgos de Seguridad de la Información, su reporte y el adecuado tratamiento de este.

7. Lineamientos Generales de la Seguridad de la Información

- Cada persona, incluido proveedores, asesores y/o prestadores de servicios externos que en sus funciones hagan uso de sistemas de información dispuestos por Grupo Mitiga, es responsable de las cuentas y credenciales asignadas. Se implementarán controles a las contraseñas, los que incluirán al menos un rango mínimo de 8 caracteres en los que se incluya el uso de mayúsculas, minúsculas, números y caracteres especiales. Para las soluciones de clientes se incluye el uso de doble factor de autenticación. Estas cuentas serán de uso personal e intransferible, no permitiendo, salvo excepciones documentadas, el uso de cuentas genéricas.
- No es permitido enviar información confidencial de Grupo Mitiga o de sus clientes por canales no autorizados (ya sea un disco en la Nube -OneDrive, GoogleDrive, etc., WeTransfer, correos personales u otros). En caso de necesidad de negocio, el usuario responsable debe tomar los resguardos necesarios, encriptando la información para su envío e informando al Oficial de Seguridad de la Información para efecto de proponer medidas de control.
- La seguridad de los activos tecnológicos asignados por Grupo Mitiga, tales como Laptop, Celulares, Tablets, etc., tanto para personal interno como externo de la compañía, son de responsabilidad del asignado, debiendo éste tomar las precauciones necesarias para evitar su pérdida, hurto, robo, extravío o divulgación de información contenida.
- Es responsabilidad del usuario garantizar la confidencialidad de la información contenida en su estación de trabajo, Laptop, Celular, Tablet u otro, por tanto, debe garantizar el resguardo de ésta haciendo un correcto uso de herramientas tales como; bloqueo de pantalla, evitar siempre que se pueda el uso de redes públicas, entre otros.
- La gestión de vulnerabilidades será controlada por el Oficial de Seguridad de la Información quien deberá detectar, identificar y junto al equipo de TI corregir de manera oportuna cualquier incidente.
- En el manejo de información sensible, el usuario y personal TI deben de velar por la correcta realización de respaldos que garanticen el resguardo de su contenido, y en temas de material físico una adecuada ejecución de la eliminación o reconfiguración (en caso de reutilización) del mismo.

- El Comité de crisis será responsable de gestionar los incidentes informáticos emergentes priorizando, la rápida recuperación de los sistemas y la recuperación íntegra de su contenido.
- El área de desarrollo es responsable de seguir las mejores prácticas de desarrollo y en especial de desarrollo seguro, garantizando que los distintos componentes cumplan adecuados estándares de seguridad y al menos los controles recomendados por OWASP.
- El equipo de desarrollo, soporte u otro, no podrá trabajar o procesar bases de datos con información de clientes. En caso de necesitar probar con datos reales, las mismas deben pasar por un proceso de ofuscación.
- Los accesos a ambientes de desarrollo y productivo de clientes, deben poseer controles por segregación de funciones y adecuados controles de contraseñas. Las excepciones a estas reglas deben ser documentadas y aprobadas por el comité de seguridad de la información y protección de datos.
- Para efecto de los clientes SaaS, Grupo Mitiga utilizará la nube propuesta por Amazon Web Services, adoptando las medidas de seguridad que ofrece esta plataforma y componentes específicos de monitoreo y seguridad aprobados por el Comité.
- Todas las soluciones a clientes deben contar con certificados de seguridad que cifren la comunicación en tránsito, manteniendo estándares y certificados actualizados para estos fines. En caso que sea posible se aplicarán mecanismos de encriptación a las bases de datos.
- En clientes On-Premise las reglas de seguridad serán dictadas por el cliente, no siendo responsabilidad de Grupo Mitiga su mantención, instalación y seguimiento de aplicaciones monitoreo y parches de vulnerabilidades.
- Las soluciones a clientes son actualizadas semanalmente a la última versión estable.
- Las soluciones de clientes son respaldadas diariamente de manera automática. En el caso de información en estaciones de trabajo, es responsabilidad de los colaboradores de Grupo Mitiga el trabajar en los entornos cloud provistos para estos fines.
- Las distintas soluciones a clientes, se someterán a procesos de evaluación de seguridad, los que incluyen Ethical Hacking y auditorías internas, con el objeto de garantizar la mejora continua del sistema. Estas evaluaciones serán realizadas al menos 1 al año.

- Grupo Mitiga reconoce que sus sistemas manejan información sensible para nuestros clientes, incluyendo algunos datos personales de colaboradores, proveedores y clientes, por lo cual se rige por los principios de: licitud y transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia e información, y confidencialidad. Para asegurar un tratamiento legítimo, necesario, seguro, transparente y solo para fines específicos dentro de sus sistemas, protegiéndose con medidas adecuadas de seguridad.
- Cada cliente es responsable de obtener los consentimientos para el uso y tratamiento de datos personales que sean utilizados en las soluciones proporcionadas por Grupo Mitiga. El titular de los datos, para hacer exigible sus derechos ARCO, debe comunicarse con el cliente que posee dicha información. Grupo Mitiga implementará medidas de seguridad que garanticen la confidencialidad de los datos y el borrado seguro en caso de ser necesario. Para datos personales administrados por Grupo Mitiga, se implementarán los canales apropiados de comunicación para que se reporten incidentes de datos y solicitudes de derechos ARCO.
- Los usuarios tanto interno como personal externo, dícese proveedores y demás agentes que cuenten con acceso a información sensible para la compañía, están obligados a mantener la confidencialidad de su contenido pudiendo en caso contrario enfrentarse a acciones legales interpuestas por Grupo Mitiga.

8. Estándares, normativas y procedimientos relacionados

Manual del SGSI
Roles y responsabilidades seguridad de la información
Política de clasificación de la información
Procedimiento de gestión de usuarios y roles
Estándar de contraseñas usuarios TI
Procedimiento de Manejo de Base de Datos de Clientes
ISO 27001:2022
Estándar OWASP

9. Definiciones y términos

N/A