



PG-AD-01 Política general de seguridad de la información

Elaborado por	Revisado por	Aprobado por
Camilo Hoffmann	Adrián Armando	Adrián Armando
Oficial de Seguridad de la Información	Gerente General	Gerente General
26-08-2024		

1. ALCANCE

Esta política aplica a todo el sistema de gestión de seguridad de la información de Drimo SpA.

2. OBJETIVO

Establecer las directrices generales de la organización para la protección de sus activos de información, según un sistema de gestión enfocado en la mitigación de riesgos de seguridad de información, la mejora continua y demás principios de la ISO/IEC 27001.

3. DEFINICIONES

Activo de información: Elemento o conjunto de elementos necesarios para el uso y tratamiento de información (documentos en físico/digital, bases de datos, aplicaciones, softwares, sistemas operativos, equipos, hardware, infraestructura, servicios, personas, incluyendo la información)

Información: Se refiere a un conjunto organizado de datos que los trabajadores de la organización generan, obtienen, transforman o controlan.

Mejora continua: Principio de los sistemas de gestión que se honra para que una organización supere sus niveles actuales de desempeño, y reaccione a los cambios en sus condiciones internas y externas con el fin de crear nuevas oportunidades.

Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

Seguridad de la información: Preservación de la integridad, disponibilidad y confidencialidad de la información.

Sistema de gestión: Actividades mediante las que la organización identifica sus objetivos, determina y gestiona los procesos y recursos requeridos para lograr los resultados deseados.

4. RESPONSABILIDADES

Oficial de Seguridad de la Información:

- Asegurar que el sistema de gestión de seguridad de la información es conforme con los requisitos de la ISO/IEC 27001
- Informar a la alta dirección sobre el comportamiento del sistema de gestión de seguridad de la información
- Proponer adecuaciones a la política general de seguridad de la información
- Asegurarse de que la integridad del sistema de gestión se mantiene cuando se planifican e implementan cambios.
- Asegurar una adecuada comunicación de la política de seguridad de la información

Gerente General:

- Asegurar que se establece la política general del sistema de gestión y que esta sea compatible con la dirección estratégica de la organización.
- Aprobar la política general del sistema de gestión.

Personal de la organización:

- Dar cumplimiento a la política general de seguridad de la información.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Drimo SpA. es una empresa que desarrolla y da soporte a soluciones tecnológicas innovadoras, ágiles y confiables, diseñadas a la medida de las necesidades de sus clientes; por lo que la información tanto propia como de sus clientes y de otras partes interesadas es un activo valioso a preservar, de manera que se enfoca en mantener sus niveles de:

- **Confidencialidad:**

Para garantizar que toda la información esté protegida, según una clasificación, de accesos no autorizados que puedan afectar los intereses de la organización y de sus partes interesadas.

- **Integridad:**

Para garantizar que toda la información solo pueda ser modificada, agregada o eliminada por personas o sistemas autorizados, de tal forma de salvaguardar la exactitud y completitud de esta.

- **Disponibilidad:**

Para garantizar que la información, y los activos que la mantienen, estén disponibles oportunamente para las operaciones o personas que la requieran.

Todo esto a través de un sistema de gestión de seguridad de la información (SGSI) conforme a la ISO/IEC 27001, dirigido por los siguientes principios:

- El mantenimiento de la **confidencialidad, integridad y disponibilidad** de la información del cliente acorde a sus necesidades, mediante el establecimiento de controles eficaces en el desarrollo, prueba y liberación del software.
 - El tratamiento oportuno de **riesgos de la seguridad de la información**, para que permanezcan en niveles aceptables.
 - La atención de **solicitudes del cliente e incidencias de seguridad de la información** de manera oportuna.
 - La aplicación de un **programa de concientización** pertinente en materia de seguridad de la información, tanto para los integrantes de la empresa como para sus partes interesadas.

Y un **compromiso** con el **cumplimiento de los requisitos aplicables** a la seguridad de la información y con la **mejora continua del SGSI**. El cumplimiento de estos principios es esencial para la organización y su SGSI, por lo que se asegura mediante su comunicación y disponibilidad, no sólo al personal interno sino a todas las partes interesadas pertinentes.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad de la información se implementa en los procesos de diseño, desarrollo, prueba, liberación (cuando aplique) y soporte al cliente de los softwares producidos por la organización, así como aquellos que los complementan, dirigen y soportan. Esta declaración se complementa con lo contenido en el documento OT-AD-01 Alcance del SGSI que se encuentre vigente.

7. CONTROL DE MODIFICACIONES

Fecha	Modificación	Versión
05-08-2024	Documento inicial	1.0