# Política de Seguridad de la Información

Cibergestión

| 1. Acerca del Documento | |
|---|---|
| Código: | PO-SGSI-01 |
| Versión: | 1 |
| Fecha Inicio: | 18/07/2025 |
| Responsable: | Comité de Dirección LATAM |
| Clasificación de Información | Pública |

| 2. Control de Aprobaciones | | |
|---|---|---|
| | **Nombre** | **Fecha** |
| Elaboró | CISO | 30/06/2025 |
| | Responsables del Sistema de Gestión | 30/06/2025 |
| | Director de Infraestructura | 30/06/2025 |
| | Director de Cumplimiento y Auditoria | 30/06/2025 |
| Revisó | Comité de Dirección LATAM | 16/07/2025 |
| Aprobó | Comité de Dirección LATAM | 18/07/2025 |

| 3. Control de Cambios | | | |
|---|---|---|---|
| **Fecha** | **Versión** | **Revisión** | **Descripción de la Modificación** |
| 18/07/2025 | 1 | 1 | Documento de nueva creación |

**Tabla de contenido**

## 4. Objetivo

Entregar disposiciones, basadas en buenas prácticas, consideradas como lineamientos estratégicos necesarios, para el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de Cibergestión LATAM.

## 5. Alcance

Esta política es aplicable a Cibergestión LATAM, y considera en su alcance todos los procesos y recursos clave, el contexto en el que opera, incluyendo a todos los colaboradores internos, externos, y terceras partes, que participen en las actividades de establecer, implementar, operar, monitorear, mantener y mejorar el SGSI.

## 6. Política del SGSI

Cibergestion LATAM, a través de su Comité de Dirección y en cumplimiento con las políticas internas de la empresa, manifiesta su compromiso para implementar un Sistema de Gestión de Seguridad de la Información para proteger y preservar la confidencialidad, disponibilidad e integridad de la información que se recibe, procese, almacene o transfiera en los **Sistemas de información para Externalización de procesos de Gestión de Expedientes** para el cumplimiento de los objetivos organizacionales, apoyándose en diversas políticas complementarias, procesos y controles de seguridad basados en mejores prácticas, y marcos nacionales e internacionales como la norma nacional y la norma internacional ISO/IEC 27001:2022.

Cibergestion LATAM, garantiza los recursos necesarios para la elaboración, autorización, difusión, ejecución, supervisión y mejora del SGSI de acuerdo con el alcance establecido.

La presente política es de carácter obligatorio para todo el personal de la organización dentro del alcance establecido, incluyendo proveedores y terceras partes, conforme a los roles y responsabilidades correspondientes, siendo la seguridad de la información responsabilidad de todos.

Con apego al marco de cumplimiento tal como leyes, regulaciones y normatividad interna, el Comité de Dirección establece su compromiso para realizar revisiones, adecuaciones y mejoras al Sistema de Gestión de Seguridad de la Información de manera anual o cuando exista algún cambio significativo para mejora continua del mismo.

## 7. Política del Seguridad de la Información

- La Dirección de Cumplimiento y Auditoría, CISO y los Analistas de Seguridad deben revisar y/o actualizar las Políticas de seguridad de la información, anualmente y/o cuando existan cambios significativos.

- Los cambios deberán ser expuestos a la Alta Dirección LATAM, para su revisión y aprobación. De igual forma, de no existir modificaciones, se deberá ratificar su vigencia.

- La Alta Dirección LATAM debe asegurar los mecanismos para que esta Política y sus modificaciones sean conocidas y estén disponibles permanentemente para todos los integrantes de la organización y de terceros.

- Se debe preservar la confidencialidad, integridad y disponibilidad de la información y sus activos de información mediante la implementación de controles. Para ello la organización debe:
    - Mantener inventarios de todos sus activos de información.
    - Establecer, implementar y mantener un proceso formal de evaluación de riesgos que sistemáticamente identifique, analice y evalúe las amenazas y vulnerabilidades a las que se encuentran expuestos los activos.
    - Evaluar las medidas de mitigación adecuadas para cada riesgo, de acuerdo con el tratamiento de riesgo de seguridad de la información vigente, e implementar los planes correspondientes.

- La Alta Dirección LATAM debe determinar y proporcionar el apoyo y los recursos necesarios que permitan establecer, implementar y mantener un SGSI, alineado con los objetivos estratégicos de la organización.

- La Alta Dirección LATAM debe designar uno o más responsables, con atribuciones y competencias necesarias para gestionar la seguridad de la información, con roles y responsabilidades claramente establecidos.

- Se debe disponer de un protocolo de respuesta ante incidentes, con una estructura de roles y responsabilidades definidas.

- Se debe fomentar una cultura de gestión de riesgos en materia de seguridad de la información, mediante planes formales de concientización/difusión y capacitación, de forma apropiada, entendible y accesible hacia los colaboradores de la organización.

- La gestión de seguridad de la información se debe alinear a las directrices y exigencias propias del cumplimiento de las normativas aplicables, requisitos de los clientes y del marco de referencia ISO 27001, en su versión vigente.

- Se debe llevar a cabo auditorías internas a intervalos planificados, para verificar la conformidad del SGSI con los requerimientos internos, normativos y las buenas prácticas adoptadas.

- Los documentos del SGSI de Cibergestión deben estar disponibles para todos los colaboradores que se defina, y deben ser actualizados anualmente y/o cuando existan cambios significativos.

- Se debe identificar las oportunidades de mejora, así como los incumplimientos y no conformidades relativas al SGSI, y determinar las causas para poner en práctica las acciones correctivas apropiadas, que permitan alcanzar los resultados esperados.

- Se deben realizar mejoras continuas al SGSI para asegurar su actualización, idoneidad, adecuación y eficacia.