autentia

# POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

| Autor | | Aprobado por | Nivel de Confidencialidad |
|---|---|---|---|
| Gerencia de Riesgo Operacional | | Gerencia General | Público |
| **Código** | **Versión** | **Fecha de Versión** | **Ubicación** |
| SGSI-POL-001 | 2.0 | 22-06-2022 | Sistema Google Drive |

## Historial de modificaciones

Toda modificación, que se realice al procedimiento descrito en este documento, deberá ser registrada e identificada en el siguiente control de cambios.

| Fecha | Versión | Creado por | Descripción de la modificación |
|---|---|---|---|
| 06-08-2019 | 1.0 | Gerencia de Riesgo Operacional | Publicación versión 1.0. |
| 01-04-2020 | 1.1 | Gerencia de Riesgo Operacional | Actualización de formato y contenido según metodología Advisera. |
| 02-11-2020 | 1.2 | Gerencia de Riesgo Operacional | Se incluye medios de difusión de la Política (4.6) |
| 19-01-2022 | 1.3 | Gerencia de Riesgo Operacional | Revisión de contenido y actualización de documentación. |
| 22-06-2022 | 2.0 | Gerencia de Riesgo Operacional | Se elimina la sección de Partes Interesadas, cuyo análisis se lleva al documento Contexto y partes interesadas. Ajuste del objetivo en sección 4.1. Se modifica redacción del punto 4.3. Se modifica el propietario del documento y se eliminan criterios para evaluar cambios al documento. En el párrafo Objetivo se agrega mención al tipo de proyectos gestionados dentro del alcance del SGSI. Se agrega en el párrafo 4.3 el tratamiento de datos personales. |
| | | | |
| | | | |

## Tabla de contenido

# 1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de Gestión de Seguridad de la Información (en adelante SGSI), según se define en el Documento del Alcance del SGSI. En este contexto, Autentia gestiona solamente proyectos de desarrollo de software.

La Política de Seguridad de la Información se aplica, dentro del alcance indicado, a tecnologías, información, procesos, infraestructura y recursos humanos de Autentia S.A., y se extiende a sus clientes y proveedores por medio de contratos, servicios y alcances definidos entre ambas partes.

# 2. Documentos de referencia

- Norma ISO/IEC 27001.
- Norma ISO/IEC 27001 Anexo 27002.
- Documento sobre el alcance del SGSI
- Metodología de gestión de riesgos
- Metodología de riesgos y oportunidades
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales
- Plan de Continuidad del Negocio
- Contexto y partes interesadas
- Roles y responsabilidades en el SGSI
- Matriz de medición de objetivos SGSI
- Procedimiento disciplinario

# 3. Terminología básica sobre seguridad de la información

- **Confidencialidad**: característica de la información por la cual solo está disponible para personas o sistemas autorizados.
- **Integridad**: característica de la información por la cual solo es modificada por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad**: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información (SGSI)**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

# 4. Gestión de la Seguridad de la Información

## 4.1. Objetivos

Esta Política, la cual es el eje principal del Sistema de Gestión de Seguridad de la Información (SGSI) de Autentia S.A., tiene como objetivo brindar los lineamientos relacionados a la disminución de los riesgos de seguridad de información que afectan a los activos o recursos de información a través de amenazas internas y externas, deliberadas o accidentales. Estos lineamientos están en concordancia con las estrategias y objetivos de negocio.

En particular:

- Mantener los niveles de disponibilidad, confidencialidad e integridad requeridos, para los recursos que operan en sus instalaciones o estén alojados y administrados por terceros en dependencias de un Data Center u otro proveedor de tecnología.
- Utilizar las mejores prácticas (probadas y aplicadas) de seguridad de la información para mejorar la oferta de productos y servicios hacia los clientes, y con ello resguardar la marca Autentia S.A. como uno de los principales activos de la Organización.
- Cumplir con la legislación vigente relacionada con aspectos de reserva y privacidad de la información de los titulares de datos.

## 4.2. Medición de objetivos del SGSI

El Oficial de Seguridad propondrá los indicadores de gestión del SGSI y medirá su progreso y cumplimiento de acuerdo a la periodicidad definida para cada uno de estos, los cuales se encuentran en el documento “Matriz de medición de objetivos SGSI”.

Las métricas de estado de los indicadores deberán ser presentadas, analizadas y evaluadas por el Comité de Seguridad de la información (de ahora en adelante Comité de SI), de acuerdo a la periodicidad con que éste sesiona.

## 4.3. Requisitos para la Seguridad de la Información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales, que están definidos en el documento “Lista de obligaciones legales, normativas y contractuales”.

En cuanto a la privacidad de los datos, se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.

Se desarrollan e implementan Políticas y procedimientos que indican cómo la organización se preocupa de la privacidad y protección de información de identificación personal. Estos documentos deben ser comunicados a todas las personas involucradas en el tratamiento de la información de identificación personal siendo sus objetivos principales:

- Limitación de la finalidad: los datos personales serán recogidos con fines determinados, explícitos y legítimos.
- Minimización de datos: los datos personales recogidos serán únicamente los estrictamente necesarios en relación con los fines para los que son tratados.
- Exactitud: los datos personales deben ser exactos y serán siempre actualizados.
- Limitación del plazo de conservación: los datos personales solamente serán mantenidos de forma que se permita la identificación de la persona usuaria durante el tiempo necesario para los fines de su tratamiento.
- Integridad y confidencialidad: los datos personales serán tratados de manera que se garantice su seguridad y confidencialidad.
- Responsabilidad proactiva: la persona responsable del tratamiento será responsable de asegurar que los principios anteriores se cumplan.

### 4.4. Controles de Seguridad de la información

El proceso de selección de los controles está definido en la metodología de evaluación y tratamiento de riesgos. Los controles seleccionados y su estado de implementación se detallan en la Declaración de Aplicabilidad.

### 4.5. Continuidad de Negocio

La Gestión de la continuidad del negocio está reglamentada en Plan de Continuidad de Negocio.

### 4.6. Responsabilidades

De esta Política General, se desprenden las restantes Políticas de Seguridad de la Información, que constituyen la definición fundamental de los planteamientos de seguridad de Autentia S.A. en materias específicas, haciendo hincapié en el rol que asumen todos los funcionarios, para lograr el resguardo de la información y los recursos asociados.

- La estructura del SGSI y sus roles están definidos en el documento Roles y responsabilidades en el SGSI

- Todo el personal de Autentia S.A. será responsable del cumplimiento de las políticas y procedimientos, su incumplimiento será sancionado a través de acciones disciplinarias establecidas en el Procedimiento disciplinario. Dichas sanciones estarán en directa relación con las faltas en que pueda incurrir respecto del marco normativo, desde amonestaciones verbales o escritas hasta la desvinculación del empleado y/o acciones legales civiles.

- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.

- Todos los incidentes o debilidades de seguridad deben ser informados al Comité de Seguridad de la Información.

### 4.7. Comunicación de la Política

El Oficial de Seguridad de la Información debe asegurarse que todos los empleados de AUTENTIA S.A., como también los participantes externos correspondientes, estén familiarizados con esta Política y sus actualizaciones, la cual será difundida oportunamente mediante correo electrónico y adicionalmente estará disponible en el sitio web de Autentia.

## 5. Apoyo para la implementación del SGSI

El Gerente General de AUTENTIA declara que en la implementación y mejora continua del SGSI se contará con el apoyo y recursos necesarios para lograr todos los objetivos aquí establecidos, así como también para cumplir con todos los requisitos identificados.

## 6. Validez y gestión de documentos

Este documento es válido a partir de su fecha de publicación.

El propietario de este documento es el Oficial de Seguridad, siendo encargado de revisarlo al menos una vez al año, a objeto de determinar si es necesaria su actualización.

**********

En AUTENTIA S.A. a la fecha de su publicación.

**Fernando Acuña**
**Gerente General**