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	1.3	19-01-2022	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.

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.

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 evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales
- Plan de Continuidad del Negocio
- Procedimiento para gestión de incidentes

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 protección de activos o recursos de información, de todas las 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

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por el Oficial de Seguridad de la Información y son aprobados por el Gerente General en la Declaración de aplicabilidad.

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

Sin embargo, 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. Partes interesadas

Las partes interesadas son todas aquellas personas u organizaciones, públicas o privadas, internas o externas, que de alguna forma pueden influir o impactar en los objetivos del SGSI, considerando que estas corresponden a las partes que pudiesen verse afectadas por las actividades que desempeñe la organización en el SGSI.

A continuación, se detalla las partes interesadas definidas para el SGSI y sus respectivas necesidades y requerimientos:

Partes interesadas internas:

- Directivos de Autentia
- Accionistas/Propietarios de Autentia
- Todo el personal que atiende el Servicio de verificación biométrica

Partes interesadas externas:

- Todos los clientes del Servicio de verificación biométrica
- Proveedores externos del Servicio de verificación biométrica
- Gobierno (País)

Requisito	Cumplir con los requisitos legales, normativos y de seguridad de la información, impuestos por las partes interesadas.
Partes interesadas	● Accionistas/Propietarios de Autentia. ● Directivos de Autentia. ● Gobierno (País). ● Todo el personal de Autentia que atiende el Servicio de verificación biométrica. ● Todos los clientes del Servicio de verificación biométrica.
Riesgos y Oportunidades	● **Riesgos**: ○ Vulneración de la integridad de la información gestionada por el Servicio de verificación biométrica. ○ Vulneración de la confidencialidad de la información gestionada por el Servicio de verificación biométrica. ○ Vulneración de la disponibilidad de la información gestionada por el Servicio de verificación biométrica. ○ Incumplimiento de legislación vigente del País. ○ Incumplimiento de normativas organizacionales dentro del alcance del Servicio de verificación Biométrica. ● **Oportunidades**: ○ A través del desarrollo e implementación del SGSI, se busca que Autentia S.A logre garantizar y demostrar su compromiso con la seguridad de la información y ciberseguridad, además de velar por el cumplimiento de la legislación y normativas vigente.

Requisito	Cumplir las condiciones contractuales asociadas a la Seguridad de la información y Ciberseguridad.
Partes interesadas	● Todos los clientes del Servicio de verificación biométrica ● Proveedores externos del Servicio de verificación biométrica
Riesgos y Oportunidades	● **Riesgos**: ○ Indisponibilidad de requerimientos mínimos contractuales para la entrega del servicio del proveedor. ○ Brecha de SI organizacional que imposibilite la entrega del servicio del proveedor. ● **Oportunidades**:

	○ Brindar un servicio seguro y de calidad, alineado a las disposiciones de SI de nuestros clientes y proveedores.

Requisito	Cumplir con los objetivos estratégicos dispuestos por la organización
Partes interesadas	● Directivos
Riesgos y Oportunidades	● **Riesgos**: ○ Pérdida de oportunidades de negocio, por ausencia de disposiciones de SI a nivel organizacional. ○ Daño reputacional sobre la imagen de la organización a causa de una ex filtración de datos de clientes. ● **Oportunidades**: ○ Crecimiento organizacional a raíz de la integración de nuevos clientes. ○ A través del desarrollo e implementación del SGSI, se busca que Autentia S.A pueda ofrecer mayor seguridad en la entrega de sus servicios y la información que éstos gestionan.

4.4. 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. En el documento *"Lista de obligaciones legales, normativas y contractuales"* se detallan los requisitos contractuales y legales.

4.5. 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.

4.6. Continuidad de Negocio

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

4.7. 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. De lo anterior se identifican las siguientes responsabilidades:

- El Gerente General es responsable de impulsar, patrocinar y promover el proyecto SGSI, así como aprobar las políticas y procedimientos del SGSI.

- El Gerente de Riesgo Operacional es responsable de la coordinación operativa del SGSI, informar su desempeño y del diseño de las políticas y procedimientos.

- El Oficial de Seguridad de la Información es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política.

- Comité de Seguridad de la Información tiene periodicidad de revisiones generales de manera trimestral.

- El Comité de Seguridad de la Información debe medir el nivel de desempeño del SGSI en cada sesión de este. El objetivo de las verificaciones por parte de este Comité es establecer la conveniencia, adecuación y eficacia del SGSI.

- El Comité de Seguridad de la Información está integrado por los siguientes cargos:

    - Gerente General
    - Gerente de Riesgo Operacional
    - Oficial de Seguridad de la Información
    - Jefe de Unidad de Sistemas/Infraestructura
    - Jefe de Desarrollo

- 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. 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.

4.8. 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 Gerente de Riesgo Operacional, siendo encargado de revisarlo al menos una vez al año, a objeto de determinar si es necesaria su actualización.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y participantes externos que cumplen una función en el SGSI pero que no están familiarizados con el presente documento
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización
- Ineficacia de la implementación y mantenimiento del SGSI
- Responsabilidades ambiguas para la implementación del SGSI

****

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

Fernando Acuña
Gerente General