POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

Open Computación S.A. (OPENSA) se compromete a proteger la confidencialidad, integridad, disponibilidad y privacidad de la información que crea, recibe, procesa, almacena, transmite y resguarda, en apoyo de sus objetivos estratégicos, operativos y comerciales.

La presente Política General de Seguridad de la Información establece los lineamientos y principios fundamentales que orientan la gestión de la seguridad de la información en OPENSA, así como el compromiso de la organización de establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los requisitos de la norma ISO/IEC 27001:2022.

La seguridad de la información constituye un componente esencial para la prestación confiable de los servicios de OPENSA, la protección de la información propia y de terceros, y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

2. OBJETIVOS

Los objetivos de esta política, alineados con la estrategia y necesidades de la organización, son los siguientes:

- Establecer un marco general para la implementación, operación, seguimiento, revisión, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.
- Proteger los activos de información de OPENSA frente a amenazas internas y externas, deliberadas o accidentales.
- Definir y comunicar responsabilidades y autoridades en materia de seguridad de la información en todos los niveles de la organización.
- Promover la aplicación de controles adecuados para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.
- Asegurar el cumplimiento de los requisitos legales, regulatorios, contractuales y de otra índole aplicables a la seguridad de la información y a la protección de datos personales.
- Fortalecer la cultura organizacional en materia de seguridad de la información mediante acciones de concientización, capacitación y participación activa del personal.
- Establecer las bases para la gestión sistemática de riesgos de seguridad de la información.

3. ALCANCE

Esta política aplica a toda la información gestionada por OPENSA, cualquiera sea su formato o medio de soporte; a todos los procesos, sistemas, servicios, recursos tecnológicos y activos asociados comprendidos dentro del alcance del SGSI; y a todos los empleados, contratistas, terceros, proveedores y otras partes interesadas que accedan, procesen, administren o custodien información de OPENSA o de sus clientes.

El alcance del SGSI de OPENSA comprende:

Desarrollo, implementación, mantenimiento y soporte de soluciones de software e infraestructura IT.

Esta política resulta aplicable tanto a las actividades realizadas en las instalaciones de la organización como a aquellas ejecutadas de forma remota o mediante infraestructura y servicios tecnológicos utilizados por OPENSA.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información en OPENSA se basa en los siguientes principios:

4.1 Confidencialidad

La información debe ser accesible únicamente por personas, procesos, sistemas o terceros debidamente autorizados. OPENSA implementará medidas para prevenir la divulgación no autorizada de la información, tanto en reposo como en tránsito.

4.2 Integridad
La información debe mantenerse exacta, completa y protegida frente a alteraciones no autorizadas. OPENSA aplicará controles orientados a preservar la integridad de la información durante todo su ciclo de vida.

4.3 Disponibilidad
La información y los sistemas que la soportan deben encontrarse disponibles para su uso por parte de quienes estén autorizados, cuando resulte necesario para la operación del negocio. La organización implementará medidas razonables para fortalecer la continuidad operativa y la recuperación ante incidentes o interrupciones.

4.4 Cumplimiento
OPENSA desarrollará sus actividades en cumplimiento con la legislación vigente, los requisitos regulatorios, contractuales y demás compromisos aplicables a la seguridad de la información, la privacidad y la protección de datos.

4.5 Privacidad
OPENSA se compromete a proteger los datos personales que trate en el desarrollo de sus actividades, asegurando que su recolección, acceso, uso, almacenamiento, transmisión, conservación y eliminación se realicen de acuerdo con los principios aplicables de privacidad y con la normativa legal, regulatoria y contractual vigente. La organización implementará medidas técnicas y organizativas apropiadas para prevenir el acceso, uso, divulgación, alteración o destrucción no autorizada de dichos datos.

4.6 Gestión de riesgos
La seguridad de la información será gestionada con base en un enfoque sistemático de identificación, análisis, evaluación y tratamiento de riesgos, priorizando aquellos que puedan afectar los objetivos del negocio y el cumplimiento de obligaciones asumidas.

4.7 Necesidad de saber y mínimo privilegio
El acceso a la información y a los sistemas deberá otorgarse sobre la base de la necesidad de negocio y con el nivel mínimo de privilegios requerido para el desempeño de las funciones asignadas.

4.8 Responsabilidad
La seguridad de la información es responsabilidad de todos. Cada persona que acceda a información o activos asociados deberá actuar de forma diligente, cumpliendo los lineamientos definidos por la organización.

4.9 Concientización
OPENSA promoverá una cultura de seguridad de la información mediante programas de formación, comunicación y concientización adecuados al rol y nivel de responsabilidad de cada persona.

4.10 Mejora continua
El SGSI será revisado y mejorado de manera continua para responder adecuadamente a cambios tecnológicos, organizacionales, regulatorios y del contexto de amenazas.

5. RESPONSABILIDADES

5.1 Alta Dirección

La Alta Dirección de OPENSA es responsable de:

- Aprobar esta política y promover su cumplimiento.
- Asegurar que la seguridad de la información sea coherente con la dirección estratégica de la organización.
- Proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.
- Impulsar una cultura organizacional alineada con la protección de la información.
- Asegurar que se definan objetivos de seguridad de la información y que éstos sean revisados periódicamente.
- Respaldar la gestión de riesgos de seguridad de la información.
- Asegurar la asignación y comunicación de roles, responsabilidades y autoridades pertinentes.

5.2 Responsable o función de Seguridad de la Información

El responsable o la función designada por OPENSA para la seguridad de la información tendrá las siguientes responsabilidades principales:

- Coordinar el establecimiento, implementación, mantenimiento y mejora continua del SGSI.
- Promover el desarrollo y actualización de políticas, normas, procedimientos y controles de seguridad de la información.
- Asistir a la dirección en temas vinculados con riesgos, incidentes, cumplimiento y mejora del SGSI.
- Coordinar la identificación, análisis, evaluación y tratamiento de riesgos.
- Promover el monitoreo del cumplimiento de los controles establecidos.
- Coordinar la gestión de incidentes de seguridad de la información.
- Impulsar actividades de concientización y capacitación.

5.3 Gerentes y Líderes de Área

Los responsables de área deberán:

- Asegurar que el personal bajo su supervisión conozca y cumpla las políticas, normas y procedimientos de seguridad de la información.
- Velar por que los accesos a información y sistemas se asignen y revisen de acuerdo con las necesidades del negocio.
- Colaborar en la identificación y tratamiento de riesgos dentro de sus procesos.

- Reportar oportunamente incidentes, debilidades o incumplimientos detectados.
- Impulsar el cumplimiento de los controles definidos dentro de su ámbito de responsabilidad.

5.4 Empleados, contratistas y terceros

Toda persona que acceda a información o activos asociados de OPENSA deberá:

- Conocer, comprender y cumplir esta política y la documentación asociada.
- Proteger adecuadamente las credenciales, dispositivos y recursos puestos a su disposición.
- Utilizar los activos de información de manera ética, responsable y exclusivamente para fines autorizados.
- Reportar de forma inmediata cualquier incidente, evento sospechoso, vulnerabilidad o incumplimiento detectado a través de los canales definidos por la organización.
- Proteger la información sensible contra accesos, divulgaciones, modificaciones o destrucciones no autorizadas.
- Participar, cuando corresponda, en las actividades de formación y concientización definidas por la organización.
- Cooperar con las investigaciones derivadas de incidentes de seguridad de la información.

6. CUMPLIMIENTO

El cumplimiento de esta Política General de Seguridad de la Información, así como de las demás políticas, normas, procedimientos y controles relacionados, es obligatorio para todo el personal de OPENSA, contratistas y terceros que accedan a la información o a activos asociados de la organización.

El incumplimiento de esta política podrá dar lugar a la aplicación de medidas disciplinarias, contractuales o legales, según corresponda, en función de la gravedad del incumplimiento y del marco normativo aplicable.

La organización comunicará esta política a las partes pertinentes y la mantendrá disponible como información documentada dentro del SGSI.

7. MEJORA CONTINUA

OPENSA se compromete a mejorar continuamente la eficacia de su Sistema de Gestión de Seguridad de la Información mediante el seguimiento de objetivos e indicadores, la revisión de incidentes, eventos, hallazgos, no conformidades y oportunidades de mejora, la ejecución de auditorías internas, la revisión por la dirección y la implementación de acciones correctivas y demás acciones de mejora que resulten necesarias.

8. POLÍTICAS Y DOCUMENTOS RELACIONADOS

La presente política se complementa con otras políticas, normas, procedimientos y documentos del SGSI de OPENSA.

9. DOCUMENTOS Y REFERENCIAS

- ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos.
- ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información.
- Requisitos legales, regulatorios y contractuales aplicables a OPENSA
- Documentación interna vigente del SGSI.

10.REVISIÓN

La presente política será revisada al menos una vez al año, o ante cambios significativos en la organización, los procesos o servicios, la infraestructura o tecnología utilizada, el contexto de riesgos y amenazas, o los requisitos legales, regulatorios o contractuales aplicables.

Toda modificación deberá ser aprobada por la autoridad competente definida por OPENSA.

11.HISTÓRICO DE CAMBIOS

Revisión	Fecha	Resumen de Cambios / Comentarios
01	16/06/26	Versión inicial.

12. APROBACIONES

	Confección	Revisión	Aprobación
Nombre	Félix Ghersi	Marcelo Ramondino	Malena Gonzalez
Cargo	Responsable SGSI	Responsable SGC	Gerente General – CEO
Fecha	04/06/26	16/06/26	16/06/26