

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Política de Seguridad de la Información

La Dirección de “SOLUSOFT” a través del Comité Seguridad de la Información (CSI), establece, impulsa y difunde a todos los niveles de la organización la siguiente Política y objetivos para la gestión de la seguridad de la información.

La información que genera y gestiona “SOLUSOFT”, constituye un activo estratégico clave para asegurar la continuidad del negocio. En este contexto, la Política de Seguridad de la Información está orientada a proteger: la información en la totalidad de su ciclo de vida (creación, difusión, modificación, almacenamiento, preservación y eliminación), los medios que permiten dicho ciclo y las personas que acceden a la información y/o la manipulan. Lo anterior, con el fin de garantizar su integridad, disponibilidad y confidencialidad.

Declaración de Intención de la Dirección

“SOLUSOFT” protegerá los recursos de información y la tecnología usada para su procesamiento de las amenazas internas o externas, deliberadas o accidentales; con el fin de asegurar el cumplimiento de la integridad, disponibilidad y confidencialidad de la información. Además de poder garantizar la continuidad de los sistemas de información, minimizar riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos estratégicos.

Principios de Seguridad de la Información

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación nacional vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a Solusoft.

En atención a esta base normativa, Solusoft establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de la información:

- **Visión estratégica:** La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de la empresa de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- **Seguridad integral:** La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información

deberá considerarse como parte integral de todas las operaciones y funcionamiento de la empresa, aplicándose de manera continua durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información

- **Administración y manejo de riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad y los lineamientos de esta política se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
- **Seguridad por diseño o seguridad por defecto:** Bajo este concepto, los sistemas y servicios que se originen en la empresa deberán configurarse y diseñarse de forma tal que se garantice un grado suficiente de seguridad desde su concepción, previniendo futuros problemas.

Esta empresa considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal. Adicionalmente, esta Política deberá ser conocida, comprendida y puesta en práctica por todos sus colaboradores.

Para la consecución de los objetivos de esta Política, Solusoft ha establecido una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación.

Objetivos de la Gestión de Seguridad de la Información

Objetivos Generales

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios que desarrolla “SOLUSOFT” mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

Es esencial que esta normativa se convierta en la piedra angular sobre la cual se construyan todas las decisiones y acciones referentes al manejo y administración de la información, para beneficio de la empresa, sus colaboradores, los clientes y entes externos con los cuales Solusoft interactúa.

Objetivos Específicos

1. Crear e implementar procedimientos de seguridad para toda la organización y promover las responsabilidades de cada colaborador para la seguridad de la información.
2. Proveer a los colaboradores herramientas para el adecuado resguardo de la seguridad de la información dentro y fuera de la organización.
3. Monitorizar el cumplimiento de los procedimientos de seguridad de la información aprobados y establecidos dentro del comité de seguridad de la información.
4. Tener menos de 10 incidentes de Seguridad de la Información al año.
5. Capacitar a los colaboradores sobre la Seguridad de la Información un mínimo de una vez cada trimestre.
6. Ejecución de pruebas de penetración anuales.

Alcance de la Política de Seguridad de la Información

Alcance General

- La Política de Seguridad de la Información de “SOLUSOFT”, se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información.
- La presente política debe ser conocida y cumplida por todo el personal de “SOLUSOFT” (directivos, empleados, subcontratistas), para lo cual será comunicada dentro de “SOLUSOFT”. Estará disponible como información documentada inclusive para partes interesadas (cuando así corresponda).
- Esta Política se aplica en todo el ámbito de “SOLUSOFT”, a sus recursos y a la totalidad de los procesos, internos y externos, vinculados a la entidad a través de contratos o acuerdos con terceros.
- De acuerdo con lo anterior, la información que genera y gestiona “SOLUSOFT”, constituye un activo estratégico clave para asegurar la continuidad del negocio, por lo que la Seguridad de la Información es una herramienta para garantizar su integridad, disponibilidad y confidencialidad.

Definición de los Activos de Información

Son todos aquellos activos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para “SOLUSOFT”, en la que se distinguen tres niveles:

- La Información propiamente dicha, independientemente de su formato (papel, digital, texto, imagen, audio, video, etc.)
- Los equipos/sistemas/infraestructura que soportan esta información
- Las personas que dan tratamiento y/o utilizan esta información, y que tienen el conocimiento de los procesos institucionales.

Definición de la Seguridad de la Información

“SOLUSOFT” entiende que la Seguridad de la Información es el conjunto de medidas preventivas y reactivas de la organización, a través de los sistemas que permiten resguardar y proteger sus activos de información, buscando mantener la confidencialidad, la disponibilidad e integridad de esta y asegurar la continuidad de las operaciones. Es decir que refiere a la protección de los activos de información, fundamentales para el éxito de nuestra organización.

Marco General de las Políticas de Seguridad de “SOLUSOFT”

Aspectos Generales

- Las Políticas de Seguridad de la Información han sido elaboradas en concordancia con la legislación vigente en el país.
- La Dirección se compromete a realizar las acciones que estén a su alcance para permitir la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Aprobación de la Política

- La política de seguridad de la información será aprobada por la Dirección, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de seguridad de la información en “SOLUSOFT”.

Difusión de la Política

- Será responsabilidad del OSI (oficial de la seguridad de la información), difundir los temas relevantes en materia de seguridad.
- Las políticas de seguridad de la información serán comunicadas a todo el personal de “SOLUSOFT” y a terceros que presten servicios en la organización y a las entidades externas relevantes.
- Para la difusión de los contenidos de las políticas de seguridad de la información al interior de “SOLUSOFT” se deberán utilizar los medios de difusión que disponga “SOLUSOFT” así como también instancias de sensibilización y capacitación llevadas a cabo para este efecto.
- Para lo anterior se definirá, implementará y evaluarán las acciones e iniciativas contenidas en un Plan de Difusión, Sensibilización y Capacitación en materia de seguridad de la información.
- La Política deberá estar disponible en la página web corporativa de Solusoft www.solusoft.com de forma que sea accesible por todas las personas y partes interesadas.

Revisión de la Política

- La Política de Seguridad de la Información será revisada anualmente a efectos de mantenerla actualizada. Asimismo, se efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser: cambios tecnológicos; impacto de los incidentes de seguridad; cambios estructurales en “SOLUSOFT”; cambios de las condiciones y/o requisitos legales; o a solicitud de la Dirección.
- La modificación del presente documento está a cargo del Comité Seguridad de la Información y será aprobado por la Dirección.

I. CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
01	26-07-2023	Aprobación final del documento por los miembros del Comité de Seguridad de la Información.
02	19-02-2025	Cambio del formato.

II. APROBADO POR	
FECHA	FIRMA