POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REALIZADO	**REVISADO**	**APROBADO**
Área / Rol Equipo implementador SGSI 03/02/2025	**Área / Rol** Equipo implementador SGSI 04/02/2025	**Área / Rol** R-SGSI 04/02/2025

1. Objetivo

Esta Política de Seguridad de la Información (en adelante, “la Política”) tiene como fin establecer los lineamientos generales para la implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI) en CDT Soluciones Tecnológicas (en adelante, “CDT”). Se persigue la protección de los activos de información de la organización, la mitigación de los riesgos y el debido cumplimiento de los requisitos legales y contractuales vigentes, en especial la Ley 25.326 de Protección de Datos Personales, la Ley 11.723 de Propiedad Intelectual, y las previsiones sobre ciberdelitos en el ordenamiento jurídico argentino.

2. Alcance

La presente Política es aplicable a todos los procesos de negocio de CDT y a toda persona (empleados, contratistas, proveedores, socios comerciales, entre otros) que maneje información de la organización o utilice sus recursos tecnológicos. No obstante, se podrán definir controles adicionales y específicos para aquellos procesos de negocio que formen parte del alcance de certificación ISO 27001.

Los requisitos establecidos en esta Política se extienden a toda la información, independientemente de su formato (electrónico, papel, medios portátiles, entre otros) o del lugar donde se encuentre (instalaciones de CDT o ubicaciones externas autorizadas).

3. Principios y objetivos de seguridad

Se establecen a continuación los principios y asimismo objetivos de la Gestión de la Seguridad de la Información de la CDT:

- Confidencialidad: Garantizar que la información sea accedida únicamente por personas debidamente autorizadas.
- Integridad: Asegurar la exactitud, completitud y veracidad de la información, impidiendo su alteración no autorizada.
- Disponibilidad: Facilitar el acceso oportuno a la información y a los sistemas que la soportan cuando se requiera, manteniendo la continuidad operativa.

Para alcanzar estos objetivos y principios, se implementará un conjunto de medidas técnicas, organizativas y legales de acuerdo con las mejores prácticas internacionales, en especial las contenidas en ISO 27001:2022 e ISO 27002, siempre alineadas con la normativa local aplicable.

Esta estipulación no debe interpretarse en detrimento o como la negativa de otros objetivos o principios, conforme lo articulado al respecto en el apartado 6 de la presente, pero el espíritu del resto de instrumentos del SGSI no debe ser contrario a los mismos.

4. Alineación con estándares y requisitos

CDT establece como referencia primaria la Norma ISO 27001:2022 y las buenas prácticas de la ISO 27002 para la definición de requisitos de seguridad. Adicionalmente, garantiza la

adaptación y cumplimiento de los requisitos legales y contractuales aplicables a la organización mediante su revisión continua por parte de asesores letrados y demás profesionales competentes a efectos de las adaptaciones que fueran relevantes.

Se define que esta política se complementa con normas internas, procedimientos y guías que definen y profundizan controles atinentes a la Gestión de la Seguridad de la Información en su más amplio sentido. Dichos documentos deberán:

- Establecer controles y metodologías alineadas a los objetivos de seguridad.
- Mantenerse actualizados conforme a cambios normativos, tecnológicos y de riesgo, por lo menos una vez al año.
- Ser comunicados y accesibles a todas las partes interesadas dentro de CDT, según corresponda.

5. Controles prioritarios

Sin perjuicio de la potestad de regulación respecto a otros aspectos relevantes para la Seguridad de la Información, se consideran como prioritarios y relevantes los aspectos establecidos en el anexo A de la ISO 27001, expuestos a continuación;

A.5 NORMAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN:
Debe regularse la creación, revisión y aprobación de documentos que establezcan lineamientos claros para la protección de la información.

A.6 ORGANIZACIÓN DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:
Debe definirse la estructura de responsabilidades que garantice la operación eficaz y el mantenimiento del SGSI, incluyendo aspectos relacionados con el trabajo remoto y el uso de dispositivos móviles.

A.7 RECURSOS HUMANOS:
Deben regularse los procesos de incorporación, permanencia y desvinculación del personal, estableciendo controles de concientización y obligaciones de confidencialidad.

A.8 GESTIÓN DE ACTIVOS:
Debe regularse la identificación, clasificación, etiquetado y protección de los activos, asegurando la confidencialidad, integridad y disponibilidad de la información.

A.9 CONTROL DE ACCESOS:
Debe establecerse la regulación de los requisitos para el acceso lógico y físico a la información, otorgando únicamente los privilegios necesarios según el rol y función.

A.10 CRIPTOGRAFÍA:
Deben definirse lineamientos para el cifrado de datos que requieran protección reforzada, contemplando algoritmos y protocolos adecuados.

A.11 SEGURIDAD FÍSICA Y AMBIENTAL:
Debe regularse la protección de instalaciones y equipamiento, estableciendo controles para prevenir accesos no autorizados, robos, daños o pérdida de información.

A.12 SEGURIDAD DE LAS OPERACIONES:
Deben regularse los procedimientos operativos, la protección contra malware, la realización de copias de seguridad, el registro de incidentes, la integridad del software, la gestión de vulnerabilidades y la ejecución de auditorías.

A.13 COMUNICACIONES:
Debe regularse la protección de la información en tránsito, tanto en medios digitales como físicos o verbales, haciendo especial énfasis en la confidencialidad e integridad de los datos.

A.14 MANTENIMIENTO DEL SISTEMA:
Deben definirse controles para asegurar que los sistemas se mantengan operativos y eficientes mediante actualizaciones, soporte y verificaciones continuas.

A.15 GESTIÓN DE PROVEEDORES:
Deben establecerse cláusulas y requisitos de seguridad en los acuerdos con terceros, garantizando que la cadena de suministro cumpla con los mismos estándares de protección.

A.16 INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:
Debe regularse el procedimiento para el reporte, análisis y respuesta a incidentes, con el fin de evitar su repetición y mitigar su impacto.

A.17 CONTINUIDAD DEL NEGOCIO:
Debe, como mínimo, definirse planes y medidas que permitan la recuperación de los servicios ante incidentes críticos que puedan interrumpir las operaciones.

A.18 CUMPLIMIENTO:
Debe regularse el cumplimiento de normas, leyes y reglamentaciones aplicables, incluyendo la realización de auditorías internas y externas para evaluar el SGSI.

6. Cumplimiento y mejora continua

El conjunto de normas, políticas, procedimientos e instrumentos del SGSI deberá estar alineado al logro de los objetivos de seguridad y orientado a garantizar el cumplimiento de los requisitos legales y contractuales.

Se buscará, cuando resulte razonable, designar propósitos normativos e indicadores específicos que permitan medir de forma objetiva la eficacia y el progreso en cada uno de los controles y procesos descritos.

Asimismo, CDT revisará y actualizará periódicamente, al menos una vez por año, la totalidad de instrumentos del SGSI para adaptarlos a la evolución tecnológica y a nuevas exigencias legales y contractuales, de manera de asegurar la mejora continua de su SGSI.

7. Responsabilidades

ALTA DIRECCIÓN: Aprobar la presente Política, asignar los recursos necesarios y liderar la mejora continua del SGSI.

RESPONSABLE DEL SGSI: Impulsar, implementar, supervisar y evaluar el cumplimiento de la política y de los instrumentos del SGSI; proponer actualizaciones ante cambios que le fueran conocidos en la organización o en el entorno.

PROPIETARIOS DE LA INFORMACIÓN: Clasificar, cuando una norma así lo indique, los requerimientos de seguridad de la información bajo su control, y cumplir con los establecidos, en todos los casos.

COLABORADORES, EMPLEADOS, CONTRATISTAS Y PROVEEDORES: Cumplir la Política, las normas del SGSI que le son disponibilizadas y los procedimientos asociados, reportar incidentes conforme al Procedimiento de Gestión ante Incidentes en Seguridad de la Información, actuar con debida diligencia y conforme a los principios de confidencialidad, integridad y disponibilidad en todas y cada una de las interacciones con los activos de CDT.

8. Sanciones

Todo incumplimiento deliberado o negligente de las disposiciones establecidas en esta Política o en cualquier otra norma del SGSI podrá dar lugar a medidas disciplinarias, de conformidad con la normativa laboral aplicable y el proceso disciplinario o equivalente de CDT.

Asimismo, en caso de infracciones relacionadas con la Ley 25.326, la Ley 11.723, el Código Penal argentino u otras normas legales vigentes, además de las medidas disciplinarias, se podrá, a criterio de la Organización y de acuerdo a lo permitido o exigido por la normativa, dar intervención a las autoridades competentes.

En el caso de proveedores, contratistas y terceros vinculados contractualmente, cualquier incumplimiento de las obligaciones de seguridad establecidas en esta Política o en el SGSI podrá ser sancionado mediante la aplicación de medidas contractuales, que podrán incluir la suspensión o terminación de la relación contractual, sin perjuicio de las acciones legales adicionales que correspondan, como las acciones por daños y perjuicios.

9. Historial del Documento

Fecha	Autor	Versión	Descripción
04/02/2025	R-SGSI	01	CREACIÓN DEL DOCUMENTO