



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.0




	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0 Fecha: 11/09!2023

VERSIÓN	SOLICITADO POR	REALIZADO POR	DESCRIPCIÓN DEL CAMBIO	REVISÓ	APROBÓ	FECHA
1.0	GERENTE GENERAL	COORDINADOR DE SGSI	Versión 1.0	JEFE DE SEGURIDAD INFORMÁTICA	GERENTE GENERAL	11/09/2023

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0
	Fecha: 11/09!2023

Contenidos

1. Objetivo.....	4
2. Alcance	4
3. Referencias normativas	5
4. Definiciones	5
5. Roles y responsabilidades	6
6. Descripción de la Política	6
6.1. Relación con proveedores (A.5.19, A.5.20, A.5.21)	7
7. Actualización de la Política	8
8. Difusión de la Política	8
9. Control de Registros	8

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0


1. Objetivo

Establecer las directrices del Sistema de Gestión de Seguridad de la Información basado en las Norma Internacionales ISO 27001:2022, para implementar, mantener y mejorar un Sistema de Seguridad de la Información en INTELIDATA, que permita el cumplimiento de los objetivos de seguridad de la información, mediante el cumplimiento de los requisitos aplicables relacionados a la seguridad de la información, garantizando la confidencialidad, disponibilidad e integridad de la información

2. Alcance

Esta política de Sistema de Gestión de Seguridad de la Información aplica a INTELIDATA y a:

- Sus colaboradores, independientemente de la relación contractual con la Organización, proveedores de servicios externos, consultores, auditores, contratistas que accedan a las instalaciones de la compañía, ya sea física o remotamente para realizar trabajos y/o empleen recursos de tecnologías de información de INTELIDATA.
- Todas las instalaciones, equipamiento (incluyendo equipos portátiles y accesorios móviles) para procesar o almacenar información de INTELIDATA.
- Todo el software para el procesamiento de datos o transporte de comunicaciones, sin importar el o los medios de almacenamiento o método de procesamiento que INTELIDATA disponga para sus fines.
- La utilización de hardware, software y recursos de terceros que INTELIDATA tenga en propiedad o bajo su dominio o licenciamiento o derecho de uso.
- Los ambientes y recintos de INTELIDATA en los cuales se procesa información y comunicaciones.

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0

3. Referencias normativas

La presente política se define considerando las recomendaciones de las siguientes normativas:

- Norma NCh-ISO 27000:2018, Sistemas de gestión de la seguridad de la información - Visión general y vocabulario.
- Norma NCh-ISO 27001:2022 Sistemas de gestión de la seguridad de la información – Control A.5.1 Políticas de seguridad de la información
- Norma NCh-ISO 27002:2022, Código de prácticas para los controles de seguridad de la información, Control 5.1 Políticas de seguridad de la información

4. Definiciones


Confidencialidad: La información debe ser conocida únicamente por aquellas personas que estén autorizadas para acceder información específica del negocio. Esto es necesario para proteger los asuntos reservados como planes estratégicos, información legal, de recursos humanos, información de los empleados y cualquier dato sensible. La información de INTELIDATA solamente puede ser agregada, modificada o eliminada por personas y/o procesos debidamente autorizados.

Integridad: La información que soporta el negocio es precisa y completa para que las decisiones que se tomen utilizándola produzcan los resultados que se esperan.

Disponibilidad: La información debe estar cuando se necesita en el formato requerido para su procesamiento, para asegurar que los procesos de negocio y las decisiones sean oportunas.

Propietarios de la Información y otros activos asociados: Es el dueño del proceso que utiliza o genera dicha información o maneja el activo asociado.

Usuarios de la Información y otros activos asociados: Es aquella persona, colaborador interno o externo, que con la debida autorización introduce, borra, cambia o lee información de la compañía o tener acceso a dichos activos.

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0
	Fecha: 11/09!2023

5. Roles y responsabilidades

Gerente General: Asegurar que las materias abordadas en esta política se ejecutan y se cumplen, identificar cómo se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la presente política detectando y proponiendo mejoras.


Coordinador de SGSI: Apoyar al Gerente General en la supervisión de la implementación de la presente política. Recibir y dar respuesta a los incidentes de seguridad de la información ocurridos.

Colaboradores: Dar cumplimiento a la presente política de seguridad de la información y a todas las responsabilidades en materia de seguridad de la información que hayan sido definidas y asignadas.

6. Descripción de la Política

En INTELIDATA prestamos Servicios para la Generación y administración de Comunicaciones de Clientes de empresas tipo B2C en general, establecemos un Sistema de Gestión de Seguridad de la Información, asumiendo los compromisos de:

- Mejorar continuamente la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
- Cumplir con los requisitos legales y los aplicables a la seguridad de la información, según lo establecido en la norma ISO 27001:2022
- Proteger la confidencialidad de la información sensible relacionada con la empresa y sus clientes.
- Garantizar la integridad de la información de la empresa y de los clientes, que la misma sea precisa y completa.
- Asegurar la disponibilidad de la información cuando se necesite, para asegurar la continuidad de los procesos

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0

- Contar con profesionales altamente calificados, que garanticen su compromiso constante con el conocimiento, aplicación y mejora continua del SGSI.
- Promover en sus colaboradores el conocimiento de las Políticas de Seguridad de la Información, así como la importancia de su contribución a la eficacia del SGSI.

6.1. Relación con proveedores (A.5.19, A.5.20, A.5.21)

Todo proveedor crítico externo de la compañía debe contar con un documento formal que respalde la relación con la Compañía, ya sea un acuerdo de servicios o un Contrato. En dicho documento se deben abordar todos los requisitos de seguridad de información pertinentes, para mitigar riesgos asociados al acceso del proveedor a los activos de la Compañía.

Al momento de definir cada acuerdo de servicio o contrato de servicio se deben tener en cuenta los siguientes ámbitos de acción a controlar según sean los servicios por contratar:

- Control de accesos físicos.
- Control de accesos a información.
- Control de activos.
- Confidencialidad de información
- Seguridad en las operaciones y todos aquellos ámbitos regulados por la presente política de seguridad de la información.


En caso de ausencia de un documento formal, el proveedor crítico debe aceptar explícitamente la presente cláusula 6.1 de la presente **POL-01 Política de Seguridad de la Información** de la compañía, y comprometerse a su cumplimiento.

Dicho proveedor debe comprometerse a administrar y tratar la información de INTELIDATA con la debida confidencialidad y uso de información únicamente con fin de cumplir con las obligaciones contractuales.

Queda formalmente prohibido que los proveedores hagan uso de la información de la compañía o de sus clientes para fines personales o fuera del alcance del contrato de servicio.

En caso de tener proveedores que generen una cadena de suministro de tecnologías de información y comunicación, dichos proveedores deben velar por el cumplimiento de la presente política según la aplicabilidad.

Es decir, para los servicios de tecnologías de información y comunicación, se requiere que se propaguen los requisitos de seguridad de la información en toda la cadena de suministro, si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados a INTELIDATA.

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0 Fecha: 11/09!2023

Igualmente para los productos de tecnologías de información y comunicación, se requiere que se propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro, si estos productos incluyen componentes comprados a otros proveedores.

También se debe obtener una garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado y que la garantía de los componentes críticos y su origen, se puede rastrear a través de toda la cadena de suministro.

7. Actualización de la Política

Dentro de la mejora continua de las políticas de seguridad de la información, esta política debe ser revisada al menos una vez al año, a partir de la fecha de entrada en vigor. El proceso se debe realizar según las definiciones del procedimiento **PRO-01 Información Documentada**.


8. Difusión de la Política

La totalidad de las políticas deben ser informadas a las Jefaturas para que las difundan según el nivel de acceso permitido a cada colaborador.

El mecanismo formal de comunicación es el correo institucional de la Compañía.

9. Control de Registros

N°	Nombre	Responsable	Almacenamiento			
			Lugar / Responsable	Medio / Recuperación	Tiempo	Disposición final
	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica

	Documento : POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Proyecto : PRO - ISO 27001
	N° de Ticket : N/A
	Área : SEGURIDAD INFORMÁTICA
	Versión : 1.0