




---

# **Política de Seguridad de la Información**


---

**Fecha: 29/11/2024**  
**Versión: 1.0**

	<b>ISA Uruguay</b>	C-1 Información Pública
Versión: 1.0 Fecha: 29/11/2024	<b>Política de Seguridad de la Información</b>	<b>Página: 2 de 6</b>

### Control de versiones

Fecha	Versión	Descripción	Autor
13/11/2024	0.1	Creación del Documento	Comité de Seguridad de la Información
29/11/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información

	<b>ISA Uruguay</b>	C-1 Información Pública
Versión: 1.0 Fecha: 29/11/2024	<b>Política de Seguridad de la Información</b>	<b>Página: 3 de 6</b>

## Contenido

1	Objetivo.....	4
2	Descripción.....	4
2.1	Vigencia .....	5
2.2	Roles y Responsabilidades.....	5
3	Referencias Normativas .....	6
3.1	Marcos Legales .....	6
3.2	Estándares Externos .....	6

	<b>ISA Uruguay</b>	C-1 Información Pública
Versión: 1.0 Fecha: 29/11/2024	<b>Política de Seguridad de la Información</b>	<b>Página: 4 de 6</b>

## 1 Objetivo

La Dirección de ISA Uruguay reconoce la importancia de identificar y proteger los activos de información de la empresa y sus clientes. Para ello, evitará la destrucción, divulgación, modificación y utilización no autorizada de toda la información, comprometiéndose a desarrollar, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

La Dirección de ISA Uruguay declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

La Seguridad de la Información se caracteriza como la preservación de:

- Su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información.
- Su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

La seguridad de la información se consigue implementando un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura. Estos controles deberán ser establecidos para asegurar los objetivos de Seguridad.


La presente política de Seguridad de la Información debe ser conocida y cumplida por todos los Colaboradores de ISA Uruguay, independiente del cargo que desempeñe y de su situación contractual.

Esta Política de Seguridad de la Información se integrará a la normativa básica de ISA Uruguay, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de esta, así como de los documentos relacionados.

## 2 Descripción

Es política de ISA Uruguay:

- Establecer objetivos anuales con relación a la Seguridad de la información.
- Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, y de acuerdo con su resultado implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción.
- Clasificar y proteger la información de acuerdo con la normativa vigente y a los criterios de valoración en relación con la importancia que posee para ISA Uruguay.

	<b>ISA Uruguay</b>	C-1 Información Pública
Versión: 1.0 Fecha: 29/11/2024	<b>Política de Seguridad de la Información</b>	<b>Página:</b> 5 de 6

- d. Brindar concientización y formación en seguridad de la información a todos los integrantes de ISA Uruguay.
- e. Establecer que todos los integrantes de ISA Uruguay son responsables reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes
- f. ISA Uruguay se compromete a la mejora continua del Sistema de Gestión de Seguridad de la Información de ahora en más SGSI.

El presente documento es revisado por el comité de seguridad de la empresa y aprobada en reunión de Directorio.

## 2.1 Vigencia

La presente norma entra en vigor a partir de su aprobación y publicación por parte del Directorio de la empresa.

Esta política será revisada en un período no mayor a tres años, o ante cambios que así lo ameriten.

## 2.2 Roles y Responsabilidades

**Dirección** es responsable de la aprobación del presente documento.


**Chief Information Security Officer (CISO)** es el responsable de la elaboración, actualización y publicación del presente documento.

**Todos los Colaboradores** deberán estar en conocimiento, cumplir y hacer cumplir la presente Política de Seguridad de la Información publicada y comunicada por el equipo de Seguridad de la información.

Para toda excepción o salvedad a estas políticas es necesario:

- Documentar, justificar y autorizar según corresponda
- Realizar un análisis y gestión de riesgos
- En caso de que aplique, realizar análisis de vulnerabilidades
- Establecer controles compensatorios

**Comité de Seguridad de la Información** - grupo interdisciplinario conformado por los Gerentes de cada una de las áreas que componen la empresa, cuya principal responsabilidad es velar por el cumplimiento de las Políticas de Seguridad y en el futuro elaborar las nuevas versiones de estas.

	<b>ISA Uruguay</b>	C-1 Información Pública
Versión: 1.0 Fecha: 29/11/2024	<b>Política de Seguridad de la Información</b>	<b>Página: 6 de 6</b>

El mismo es responsable de:

- Identificar y analizar las normas relativas a la seguridad de la información incluidas en Leyes, Decretos y Reglamentaciones de organismos nacionales e internacionales que sean de aplicación obligatoria a los efectos de asesorar en su cumplimiento a las unidades según corresponda.
- Elaborar las nuevas versiones de las Políticas de Seguridad de la Información.
- Velar por el cumplimiento de las Políticas de Seguridad de la Información.
- Difundir el Compromiso de Confidencialidad Corporativo a todas las áreas y la obligatoriedad de su utilización.
- Definir referentes de seguridad de la información que permitan permear la presente política a cada una de las áreas de la organización.

### 3 Referencias Normativas

#### 3.1 Marcos Legales

- Ley 18.331 y Decreto 414/009 Ley de Protección de Datos Personales y su Decreto reglamentario.
- Ley 18.600 sobre Firma Digital.

#### 3.2 Estándares Externos

- ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos.