


---

# Política de Seguridad de la Información

---




**Fecha:** 18/02/2023  
**Versión:** 1.0

	<b>ISA Paraguay</b>	
<b>Fecha:</b> 10/11/2022 <b>Versión:</b> 1.0	<b>Política de Seguridad de la Información</b>	<b>Página:</b> 2 de 9


### Control de versiones

Fecha	Versión	Descripción	Autor
10/11/2022	0.9	Creación del Documento	Comité de Seguridad de la Información
18/02/2023	1.0	Revisión del Documento	Comité de Seguridad de la Información

	<b>ISA Paraguay</b>	
<b>Fecha:</b> 10/11/2022 <b>Versión:</b> 1.0	<b>Política de Seguridad de la Información</b>	<b>Página:</b> 3 de 9

## Contenido

Control de versiones .....	2
1 Objetivo .....	4
1.1 Vigencia .....	5
1.2 Involucradas/os y Partes Interesadas .....	5
2 Referencias Normativas .....	5
2.1 Marcos Legales que aplican a la Política.....	5
2.2 Estándares Externos .....	5
3 Definiciones, abreviaturas y símbolos.....	6
4 Clasificación de la información.....	8
5 Comité de Seguridad de la Información:.....	8

	<b>ISA Paraguay</b>	
Fecha: 10/11/2022 Versión: 1.0	<b>Política de Seguridad de la Información</b>	Página: 4 de 9

## 1 Objetivo

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

La Dirección de ISA Paraguay 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:

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

La seguridad de la información se consigue implantando 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 todo el Personal de ISA Paraguay, 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 Paraguay, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de esta, así como de los documentos relacionados.

Es política de ISA Paraguay:

- a. Establecer objetivos anuales con relación a la Seguridad de la información
- b. 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.
- c. 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 Paraguay.

El presente documento es elaborado por el comité de seguridad conformado por los gerentes de cada una de las áreas que conforman la empresa.

La aprobación de la presente política se realiza en reunión de Directorio.

	<b>ISA Paraguay</b>	
Fecha: 10/11/2022 Versión: 1.0	<b>Política de Seguridad de la Información</b>	Página: 5 de 9

## 1.1 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.

## 1.2 Involucradas/os y Partes Interesadas

Todos los usuarios y terceras partes 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 todo apartamiento, 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

Es responsabilidad del Comité de Seguridad de ISA Paraguay que todas las partes se encuentren informadas del contenido de la presente política y garantizar el cumplimiento de la misma.


## 2 Referencias Normativas

### 2.1 Marcos Legales que aplican a la Política

- Ley 1682 - REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO
- Ley 1969 - QUE MODIFICA, AMPLÍA Y DEROGA VARIOS ARTICULOS DE LA LEY N° 1682/2001
- Ley N 5282 – Libre Acceso Ciudadano a la Información Pública y Transparencia Gubernamental

### 2.2 Estándares Externos


- ISO/IEC 27000: Tecnología de la Información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario.

	<b>ISA Paraguay</b>	
<b>Fecha:</b> 10/11/2022 <b>Versión:</b> 1.0	<b>Política de Seguridad de la Información</b>	<b>Página:</b> 6 de 9

- ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos
- ISO/IEC 27002: Buenas prácticas para gestión de la seguridad de la información


### 3 Definiciones, abreviaturas y símbolos

- **Activo de Información** - Cualquier información o elemento relacionado con el tratamiento de esta que tenga valor para la organización. La información puede ser almacenada en muchas formas, incluyendo: formato digital (por ejemplo, archivos de datos almacenados en medios ópticos o electrónicos), medio material (por ejemplo, en papel), así como información no representada, en forma de conocimiento de los empleados.  
Ejemplos de activos de información:
  - a. Información: bases de datos, archivos de datos, documentación, contratos, acuerdos.
  - b. Software: sistemas de información (propios o subcontratados), software de base (sistemas operativos, manejadores de base de datos, etc.), herramientas de desarrollo, y utilitarios.
  - c. Físicos: equipamiento de computación, equipamiento de comunicaciones, medios de almacenamiento de información removibles y otros equipamientos.
  - d. Instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.
  - e. Servicios: servicios de cómputo y de comunicaciones, servicios generales (calefacción, iluminación, energía, y aire acondicionado, etc.).
  - f. Intangibles personales: conocimientos, calificaciones, habilidades y experiencia del usuario.
- **Amenaza** - Causa potencial de un incidente de seguridad de la información, que puede dar lugar a daños en un sistema de información.
- **Área Segura:** Instalaciones que:
  - a. Contienen información no publica
  - b. Procesan información
- **Asegurar** – Acciones para el mejor cumplimiento de objetivos o controles establecidos
- **Compromiso de Confidencialidad Corporativo** - Contrato o acuerdo de confidencialidad que se firma cuando se va a tener conocimiento de información que requiere discreción y se trata de evitar que las partes implicadas puedan divulgar o utilizar dicha información para fines diferentes a los establecidos en el contrato.
- **Confidencialidad** - Propiedad que determina que la información esté disponible y sea revelada únicamente a individuos, entidades o procesos autorizados.
- **Criptografía** - Método de cifrado para lograr que un mensaje no pueda ser leído por un tercero sin autorización, es decir, asegurar la confidencialidad de la información.
- **Disponibilidad** - Propiedad de la información de ser accesible y utilizable por solicitud de individuos, entidades o procesos autorizados.
- **Dispositivos Móviles – Dispositivos Transportables** - Todo equipo que proporcione portabilidad y posea capacidad de almacenamiento y/o procesamiento de información, con

	<b>ISA Paraguay</b>	
<b>Fecha:</b> 10/11/2022 <b>Versión:</b> 1.0	<b>Política de Seguridad de la Información</b>	<b>Página:</b> 7 de 9

conexión permanente o intermitente a la red. Por ejemplo: Notebooks, Laptop o PDA, Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Cintas, Pendrive o similar, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

- **Evento de Seguridad de la Información** - Ocurrencia identificada de un estado de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de controles, o una situación previamente desconocida que pueda ser relevante para la seguridad.
- **Incidente de Seguridad de la Información** - Un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de ISA y amenazar la seguridad de la información.
- **Integridad** - Propiedad de exactitud y completitud de la información, manteniendo los datos libres de modificaciones no autorizadas
- **Medio** - Refiere a medios de almacenamiento lógico, físico, o cualquier otro medio tangible que oficie de contenedor de información.
- **Necesidad de Saber, Necesidad de Hacer**- Principio de seguridad de la información que indica el otorgamiento de permisos de acceso a recursos e información con los mínimos privilegios necesarios para cumplir con las tareas asignadas.
- **Normativa Vigente Incidente** - Disposiciones (jurídica, contractual, etc) que aplican al caso concreto. Oposición de Intereses: Operación realizada con la intervención de varios actores con diferentes funciones de control.
- **Procesos Críticos** - Aquellos que en caso de falla afectan la satisfacción del cliente y exponen a ISA a pérdidas económicas, de imagen y demandas legales.
- **Responsable de Activo de Información** - Usuario responsable de asegurar que el activo de información bajo su responsabilidad está protegido y seguro.
- **Riesgo** - El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a ISA o sus clientes.
- **Seguridad de la Información** - Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Separación de Funciones** - Principio que establece la segregación de tareas para reducir el riesgo de que un usuario y/o terceras partes puedan cometer errores o fraudes.
- **Sistema de Información** - Infraestructura de tecnología, procesos, aplicaciones de negocios y software, disponibles a los usuarios para el desarrollo de las tareas.
- **Usuarios** - Funcionarios (en cualquier carácter), personas físicas o jurídicas (consultores, personal contratado, proveedores y terceras partes) que hacen uso de información y/o activos de información de ISA.
- **Vulnerabilidad**- Debilidad de un activo o control que puede ser explotada por una o más amenazas.

	<b>ISA Paraguay</b>	
<b>Fecha:</b> 10/11/2022 <b>Versión:</b> 1.0	<b>Política de Seguridad de la Información</b>	<b>Página:</b> 8 de 9

## 4 Clasificación de la información


ISA Paraguay clasifica la información según los siguientes criterios basados en las normativas vigentes.

- **Información Personal** – Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Según Ley 18331 art. 4 numeral E o normas homologas en los países donde ISA opera.
- **Dato Sensible** - Datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual sensible Ley 18.331 art. 4 numeral E o normas homologas en los países donde ISA opera.
- **Información Pública** - Es toda la información que emana, produce, esté en posesión de, o bajo el control de ISA, con independencia del soporte en el que esté contenida, salvo las excepciones o secretos establecidos por Ley, así como la información reservada o confidencial.
- **Información Reservada** - Aquella información cuya difusión pueda:
  - Comprometer la seguridad pública o la defensa nacional.
  - Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado a ISA.
  - Dañar la estabilidad financiera, económica o monetaria de ISA.
  - Poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona. o Suponer una pérdida de ventajas competitivas para el sujeto obligado o pueda dañar su proceso de producción.
  - Desproteger descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de los sujetos obligados.
- **Información Confidencial** - Se considera información confidencial:
  - Aquella entregada en tal carácter a los sujetos obligados siempre que:
    - Refiera al patrimonio de la persona.
    - Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica que pudiera ser útil para un competidor.
    - Esté amparada por una cláusula contractual de confidencialidad.
  - Los datos personales que requieran previo consentimiento informado (Ley N° 18.381, arts. 9 y 10).

## 5 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 Paraguay</b>	
Fecha: 10/11/2022 Versión: 1.0	<b>Política de Seguridad de la Información</b>	<b>Página: 9 de 9</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.