



---

# **Política de Criptografía y Protección de Datos**

---

**Fecha:** 10/10/2025

**Versión:** 1.0

 	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página:</b> 2 de 8

## Control de versiones

Fecha	Versión	Descripción	Autor
10/10/2025	0.1	Creación del Documento	PM SGSI
17/10/2023	1.0	Revisión del Documento	Comité de Seguridad de la Información

 	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página:</b> 3 de 8

## Contenido

Control de versiones.....	2
1 Objetivo .....	4
2 Alcance .....	4
3 Roles y responsabilidades .....	4
4 Principios de seguridad criptográfica .....	5
5 Gestión y uso de los controles criptográficos .....	6
6 Revisión, monitoreo y mejora continua .....	7
7 Indicadores de eficacia .....	7
8 Cumplimiento y mejora continua.....	8
9 Vigencia y Publicación .....	8

	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página:</b> 4 de 8

## 1 Objetivo

Establecer los lineamientos que aseguren la implementación, gestión y control efectivo de los mecanismos criptográficos utilizados por Interfase ISA para proteger la confidencialidad, integridad, autenticidad y disponibilidad de la información, reduciendo los riesgos de exposición o uso indebido.

Esta política orienta el uso responsable de la criptografía dentro del SGSI y asegura su integración con los controles de red, comunicaciones y cumplimiento normativo aplicables. Forma parte integral del SGSI y su aplicación se enmarca en el ciclo PDCA (Planificar–Hacer–Verificar–Actuar).

El uso de criptografía en Interfase ISA deberá basarse en el análisis de riesgos del SGSI, de forma que cada mecanismo implementado responda a una necesidad específica de protección (confidencialidad, integridad, autenticidad o no repudio), documentada y aprobada por el Comité de Seguridad.

## 2 Alcance

Aplica a todas las sedes, sistemas, servicios y entornos tecnológicos de Interfase ISA, incluyendo operaciones en la nube y servicios gestionados por terceros.

Es de cumplimiento obligatorio para colaboradores, contratistas y proveedores que intervengan en la implementación, administración o uso de mecanismos criptográficos o en el tratamiento de información sensible protegida mediante cifrado.

## 3 Roles y responsabilidades

La gestión de controles criptográficos es una responsabilidad compartida entre las áreas de tecnología, seguridad, legal y de gestión de la información.

- Directorio: aprueba esta política, asigna los recursos necesarios y supervisa su cumplimiento durante la Revisión por la Dirección.
- Comité de Seguridad: supervisa la aplicación de los controles criptográficos, aprueba estándares y revisa resultados de auditoría.
- PM del SGSI: coordina la integración de esta política con las demás del SGSI y el seguimiento de acciones correctivas.

 	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página:</b> 5 de 8

- Área de TI: implementa, administra y monitorea los mecanismos criptográficos, garantizando la correcta gestión de claves.
- Asesoría Legal: verifica que el uso de criptografía y firma electrónica cumpla con las leyes vigentes.
- Responsables de Área: aseguran la protección de los datos bajo su custodia conforme a esta política.
- Colaboradores, contratistas y terceros: cumplen las disposiciones establecidas y reportan cualquier incidente o irregularidad.

Las decisiones sobre adopción, renovación o reemplazo de mecanismos criptográficos deberán basarse en los resultados del análisis de riesgos del SGSI, revisados y aprobados por el Comité de Seguridad.

## 4 Principios de seguridad criptográfica

Interfase ISA adopta los siguientes principios rectores para el uso, gestión y supervisión de los mecanismos criptográficos, asegurando su aplicación coherente en todas las sedes y servicios bajo el SGSI:

- Propósito y necesidad justificada: todo uso de criptografía deberá responder a una necesidad específica de protección identificada en el análisis de riesgos o en un requisito legal, contractual o normativo.
- Confidencialidad: la información clasificada o sensible deberá cifrarse utilizando algoritmos y configuraciones aprobadas por el Comité de Seguridad, garantizando su protección durante almacenamiento, transmisión y respaldo.
- Integridad y autenticidad: los mecanismos de firma digital, hash o validación criptográfica deberán asegurar que la información y las transacciones no sean alteradas ni manipuladas, y que la identidad de las partes involucradas sea verificable y auditable.
- Estandarización técnica: solo se permitirán algoritmos, claves y protocolos criptográficos que cumplan con estándares internacionales reconocidos (por ejemplo, NIST, ISO/IEC, ETSI), y cuya fortaleza sea proporcional al nivel de sensibilidad de la información tratada.
- Gestión del ciclo de vida: toda clave o certificado deberá tener un ciclo de vida definido, que contemple su generación, distribución, rotación, almacenamiento, renovación y eliminación segura, conforme a los procedimientos documentados del SGSI.

**Uruguay**  
España 2094 esq. Pablo de María  
Montevideo  
Teléfonos +598 2 4193914  
www.interfaseisa.uy

**Paraguay**  
España 2028 c/Brasilia  
Asunción  
Teléfonos +595 21 3280171  
www.interfaseisa.com.py

 	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página:</b> 6 de 8

- Control y segregación de funciones: la generación y administración de claves deberán realizarse por personal autorizado, garantizando la segregación entre quienes crean, custodian y utilizan los mecanismos criptográficos, con trazabilidad completa.
- Legalidad y cumplimiento: el uso de criptografía deberá cumplir con las leyes nacionales e internacionales sobre cifrado, firma electrónica y protección de datos, así como con los compromisos contractuales adquiridos por Interfase ISA.
- Supervisión y revisión continua: las prácticas criptográficas estarán sujetas a revisiones y auditorías periódicas para garantizar su vigencia, eficacia y resistencia frente a vulnerabilidades o cambios tecnológicos.
- Trazabilidad y registro: toda actividad relevante relacionada con la gestión de claves, certificados o mecanismos criptográficos deberá registrarse para su verificación por el Comité de Seguridad o auditores externos.
- Niveles mínimos de cifrado: los mecanismos de cifrado deberán cumplir con los estándares definidos por el Comité de Seguridad, garantizando un nivel mínimo de seguridad equivalente a AES-256 para datos en reposo y TLS 1.3 para comunicaciones seguras.
- Evaluación de algoritmos: los algoritmos y protocolos criptográficos deberán revisarse al menos una vez al año o cuando existan vulnerabilidades publicadas que afecten su fortaleza, documentando los resultados en el Registro de Controles Criptográficos del SGSI.

## 5 Gestión y uso de los controles criptográficos

El Área de TI mantendrá un Inventario de Claves y Certificados Criptográficos, que incluirá su propietario, propósito, fecha de creación, algoritmo utilizado, fecha de expiración y responsable de renovación o eliminación. Dicho inventario estará bajo control de versiones y revisado al menos una vez al año por el Comité de Seguridad.

La gestión de claves, certificados y materiales criptográficos deberá realizarse bajo procedimientos documentados que aseguren su generación, distribución, almacenamiento, rotación y eliminación segura, preservando su confidencialidad y disponibilidad.

Las claves maestras y certificados corporativos serán administrados exclusivamente por el Área de TI, bajo supervisión del Comité de Seguridad y conforme al inventario de activos del SGSI.

 	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página:</b> 7 de 8

Los mecanismos y responsabilidades operativas asociadas al uso y protección de la criptografía se desarrollan en los Procedimientos de Gestión de Claves y Uso de Controles Criptográficos, parte integrante del SGSI de Interfase ISA.

La revocación, rotación y destrucción de claves deberán realizarse conforme al Procedimiento de Gestión del Ciclo de Vida de Claves Criptográficas, asegurando la eliminación segura mediante métodos aprobados (por ejemplo, borrado criptográfico o sobrescritura segura).

Los cambios relevantes (renovación, revocación o pérdida) deberán registrarse como evidencia auditable dentro del SGSI, con trazabilidad a la solicitud y aprobación correspondiente.

## 6 Revisión, monitoreo y mejora continua

El Comité de Seguridad deberá revisar al menos una vez al año la eficacia de los controles criptográficos implementados, incluyendo:

- Vigencia y fortaleza de los algoritmos utilizados.
- Cumplimiento del calendario de renovación de certificados.
- Evaluación de incidentes o vulnerabilidades relacionadas con cifrado o firma digital.

Los resultados de esta revisión se documentarán en el Informe de Revisión Criptográfica Anual y servirán como base para las acciones de mejora del SGSI.

## 7 Indicadores de eficacia

El Comité de Seguridad y el PM del SGSI medirán la eficacia de esta política a través de los siguientes indicadores:

- Porcentaje de certificados vigentes y auditados.
- Tiempo medio de renovación de claves antes del vencimiento.
- Número de incidentes relacionados con cifrado o pérdida de confidencialidad.
- Porcentaje de algoritmos revisados conforme a plan anual.

Los resultados se presentarán durante la Revisión por la Dirección y se utilizarán para planificar las mejoras técnicas y organizativas del SGSI

 	<b>Política de Criptografía y Protección de Datos</b>	C-1 Información Pública
Versión: 1.0 Fecha: 10/10/2025		<b>Página: 8 de 8</b>

## 8 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio para todas las áreas, colaboradores y proveedores que utilicen mecanismos criptográficos.

El Comité de Seguridad, junto con el Área de TI y el PM del SGSI, medirá la eficacia de los controles a través de indicadores como:

- Porcentaje de certificados vigentes auditados.
- Tiempo medio de renovación de claves.
- Incidentes relacionados con cifrado o pérdida de confidencialidad.

Los resultados se incluirán en el informe anual de cumplimiento presentado al Directorio durante la Revisión por la Dirección, asegurando la mejora continua del SGSI.

## 9 Vigencia y Publicación

Esta política es de aplicación obligatoria a partir de su aprobación por el Directorio de Interfase ISA.

La versión vigente será comunicada mediante los canales institucionales y publicada en la intranet corporativa, dentro del repositorio del SGSI.

El Comité de Seguridad garantizará su difusión, revisión anual y control de versiones, o antes si se producen cambios tecnológicos o regulatorios significativos.

Esta política deberá revisarse al menos una vez al año o cuando se produzcan cambios relevantes en tecnologías de cifrado, infraestructura o normativas aplicables (por ejemplo, RGPD o Ley 18.331 UY).

Toda modificación deberá contar con la aprobación formal del Directorio de Interfase ISA, asegurando su adecuada comunicación y registro bajo control documental.

Versión	Fecha de aprobación	Próxima revisión	Aprobado por:
1.0	DD/MM/AAAA	DD/MM/AAAA	Directorio – Interfase ISA