





Política de Seguridad en Relaciones con Proveedores



Fecha: 07/10/2025

Versión: 1.0

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 2 de 9



Control de versiones

Fecha	Versión	Descripción	Autor
07/10/2025	0.1	Creación del Documento	PMO SGSI
10/10/2023	1.0	Revisión del Documento	Comité de Seguridad de la Información

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 3 de 9

Contenido

Control de versiones.....	2
1 Objetivo	4
2 Alcance	4
3 Roles y responsabilidades	4
4 Principios de seguridad en relaciones con proveedores.....	5
5 Evaluación y selección de proveedores.....	6
6 Obligaciones contractuales y confidenciales.....	6
7 Monitoreo y control de proveedores	7
8 Terminación o renovación de servicios	7
9 Indicadores y revisión de eficacia	8
10 Cumplimiento y mejora continua.....	8
11 Vigencia y Publicación	8

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 4 de 9

1 Objetivo

Establecer los lineamientos que aseguren que las relaciones con proveedores y terceros que acceden, procesan o administran información de Interfase ISA se gestionen bajo principios de seguridad, confidencialidad y cumplimiento normativo.

Esta política establece los principios para gestionar la seguridad de la información en toda la cadena de suministro, garantizando que los proveedores, subcontratistas o terceros que accedan a los activos de Interfase ISA cumplan con los controles del SGSI, los requisitos legales, contractuales y las mejores prácticas internacionales.

Se alinea con los controles A.5.19 y A.5.20 de la norma ISO/IEC 27001:2022 y forma parte integral del ciclo de mejora continua (PDCA) del SGSI.

2 Alcance



Aplica a todas las sedes de Interfase ISA, y a todas las áreas, colaboradores y contratistas que participen en procesos de selección, contratación, evaluación o supervisión de proveedores que tengan acceso, directo o indirecto, a información, sistemas, infraestructuras o servicios críticos de la organización.

Incluye tanto a proveedores de bienes y servicios tecnológicos, como a proveedores de soporte, consultoría, mantenimiento, servicios en la nube o subcontratistas, cuyas actividades puedan afectar la seguridad, disponibilidad o confidencialidad de los activos de información.

3 Roles y responsabilidades

La gestión segura de las relaciones con proveedores es una responsabilidad compartida entre las áreas usuarias, de compras, tecnología y seguridad de la información.

- Directorio: aprueba esta política, asigna los recursos necesarios y supervisa su cumplimiento mediante la Revisión por la Dirección.
- Comité de Seguridad: supervisa la aplicación de esta política, evalúa resultados de auditorías y aprueba excepciones justificadas.
- PM del SGSI: coordina la integración de esta política con los demás procesos del SGSI, mantiene actualizada la documentación de soporte y promueve la mejora continua.

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 5 de 9


- Área de Compras o quien cumpla sus funciones: garantiza que los procesos de licitación, contratación y renovación de proveedores incluyan criterios de seguridad de la información.
- Área de TI: evalúa la seguridad técnica de los proveedores con acceso a infraestructura o sistemas críticos y supervisa el cumplimiento de los controles técnicos.
- Responsables de Área: verifican que los proveedores bajo su gestión cumplan los compromisos de confidencialidad y seguridad establecidos contractualmente.
- Colaboradores y contratistas: deben respetar los lineamientos establecidos en esta política y notificar al Comité de Seguridad cualquier situación de incumplimiento o riesgo detectado.

Las funciones y responsabilidades específicas se documentan en la Matriz RACI del SGSI, que constituye evidencia formal de auditoría.

4 Principios de seguridad en relaciones con proveedores

Interfase ISA adopta los siguientes principios para la gestión de relaciones con proveedores:

- Evaluación basada en riesgos: toda relación con proveedores deberá considerar el nivel de riesgo asociado al acceso o tratamiento de información.
- Transparencia y trazabilidad: las obligaciones de seguridad deben documentarse y ser verificables.
- Cumplimiento contractual: los contratos deberán incluir cláusulas específicas sobre confidencialidad, seguridad, protección de datos y notificación de incidentes.
- Monitoreo continuo: las relaciones con proveedores deberán revisarse periódicamente para validar el cumplimiento de los controles definidos.
- Finalización controlada: al término de la relación, se deberá garantizar la devolución o eliminación segura de la información.
- Evaluación basada en riesgo residual: la criticidad de cada proveedor deberá determinarse considerando el nivel de acceso a la información, el impacto potencial en caso de incumplimiento y los resultados del análisis de riesgos del SGSI.

 Versión: 1.0 Fecha: 07/10/2025	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública Página: 6 de 9



- Responsabilidad compartida: los acuerdos con proveedores deberán establecer claramente las responsabilidades de ambas partes en materia de seguridad de la información, continuidad operativa y respuesta ante incidentes.

5 Evaluación y selección de proveedores

- Los proveedores deberán ser evaluados previamente a su contratación, considerando criterios de seguridad, cumplimiento normativo, reputación y capacidad técnica.
- La evaluación incluirá, cuando corresponda, revisión de políticas de seguridad, certificaciones (por ejemplo, ISO 27001), procedimientos de protección de datos y antecedentes de cumplimiento.
- El resultado de la evaluación formará parte del proceso de gestión de riesgos del SGSI y deberá conservarse como evidencia documental.
- Los resultados de la evaluación deberán documentarse en el Registro de Evaluación de Proveedores, que incluirá los criterios de selección, la clasificación de criticidad y la fecha de última revisión. Este registro formará parte del repositorio documental del SGSI y será revisado al menos una vez al año por el Comité de Seguridad.
- Los proveedores clasificados como críticos deberán contar con acuerdos de confidencialidad firmados, cláusulas contractuales de seguridad verificables y evidencia de cumplimiento (por ejemplo, certificaciones ISO/IEC 27001, informes SOC 2, o auditorías externas).

6 Obligaciones contractuales y confidenciales

- Todos los contratos con proveedores deberán incluir cláusulas de confidencialidad, protección de datos y seguridad de la información, acordes con los niveles de riesgo y los requisitos legales vigentes.
- Los acuerdos deberán especificar claramente los roles, responsabilidades, niveles de servicio (SLA), obligaciones de notificación de incidentes y condiciones de acceso a la información.
- El incumplimiento de las obligaciones de seguridad podrá constituir causal de suspensión o terminación del contrato, según corresponda.

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 7 de 9



- Los contratos deberán especificar mecanismos de control para el uso de subcontratistas, requiriendo la aprobación previa del Comité de Seguridad antes de cualquier delegación de servicios que implique tratamiento de información de Interfase ISA. Además, deberá contemplarse una cláusula que establezca el derecho de auditoría de Interfase ISA o sus representantes sobre los controles de seguridad aplicados por el proveedor, según el nivel de riesgo y criticidad del servicio.

7 Monitoreo y control de proveedores

- Los proveedores críticos o con acceso a información sensible serán objeto de monitoreo continuo mediante revisiones de desempeño, auditorías o reportes de cumplimiento, conforme a la clasificación de riesgos definida en el SGSI. El Comité de Seguridad y el Área de TI deberán conservar evidencia de cada revisión en el Registro de Seguimiento de Proveedores, donde se documenten los hallazgos, acciones correctivas y resultados de verificación.
- Se deberán realizar revisiones o auditorías documentadas, cuyos resultados serán reportados al Comité de Seguridad.
- Cualquier hallazgo o incidente de seguridad deberá registrarse y gestionarse según los procedimientos de Gestión de Incidentes y Riesgos del SGSI.
- Los incidentes o incumplimientos detectados deberán gestionarse conforme al Procedimiento de Gestión de Incidentes del SGSI, asegurando la trazabilidad desde la detección hasta el cierre documentado. En caso de incumplimiento grave, el Comité de Seguridad podrá suspender temporalmente el servicio y notificar al Directorio para la evaluación de medidas disciplinarias o contractuales.

8 Terminación o renovación de servicios

- Al finalizar un contrato o relación comercial, el proveedor deberá devolver o eliminar de forma segura toda información, documentación o acceso otorgado por Interfase ISA.
- La revocación de accesos, recuperación de activos y baja de cuentas deberá realizarse en coordinación con el Área de TI y registrarse como evidencia.
- En caso de renovación o ampliación de servicios, se deberá reevaluar el riesgo del proveedor y actualizar los compromisos de seguridad conforme a la situación vigente.

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 8 de 9

9 Indicadores y revisión de eficacia

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

- Porcentaje de proveedores evaluados y clasificados por riesgo.
- Número de auditorías o revisiones de proveedores completadas.
- Incidentes de seguridad reportados por terceros.
- Porcentaje de contratos que incluyen cláusulas de seguridad actualizadas.

Los resultados se consolidarán durante la Revisión por la Dirección y servirán como base para el plan anual de mejora continua del SGSI.

10 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio para todas las áreas involucradas en la gestión de proveedores.

El Comité de Seguridad, junto con el PM del SGSI, el Área de Compras y el Área de TI, supervisará su aplicación y consolidará los resultados de auditorías y revisiones en un informe anual de cumplimiento presentado al Directorio durante la Revisión por la Dirección.

Los hallazgos o desviaciones detectadas deberán gestionarse mediante acciones correctivas o preventivas, asegurando la mejora continua del proceso de gestión de proveedores y de la seguridad asociada a terceros.

11 Vigencia y Publicación

Esta política entra en vigencia a partir de su aprobación por el Directorio de Interfase ISA.



La versión vigente será comunicada a todos los colaboradores mediante los canales institucionales y estará disponible en la intranet corporativa, dentro del repositorio del SGSI.

El Comité de Seguridad es responsable de garantizar su difusión, control de versiones y revisión anual, o antes si ocurren cambios normativos, contractuales o tecnológicos significativos.

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

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

 	Política de Seguridad en Relaciones con Proveedores	C-1 Información Pública
Versión: 1.0 Fecha: 07/10/2025		Página: 9 de 9

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