Política de Seguridad de la Información

Fecha: 15/09/2025
Versión: 2.0

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
15/09/2025	2.0	Actualización de Política según alcance e implementación de SGSI	Comité de Seguridad de la Información

Contenido

1 Objetivo

El Directorio de Interfase ISA reconoce la importancia de identificar y proteger los activos de información propios y de sus clientes.

El objetivo de esta política es establecer el marco de actuación para preservar la confidencialidad, integridad y disponibilidad de la información, evitando su destrucción, divulgación, modificación o uso no autorizado.

Para ello, Interfase ISA se compromete a desarrollar, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos de la norma ISO/IEC 27001:2022.

2 Alcance

Esta política aplica a todas las sedes de Interfase ISA, incluyendo operaciones presenciales y entornos de teletrabajo autorizados.

Su cumplimiento es obligatorio para todos los colaboradores de Interfase ISA, independientemente de su cargo o situación contractual, así como para contratistas, proveedores críticos y terceros que procesen información en nombre de la organización.

3 Declaración de la Dirección

El Directorio de Interfase ISA declara su compromiso con la seguridad de la información como un activo estratégico esencial para la continuidad y competitividad del negocio. Se compromete a:

- Asignar recursos suficientes para implementar y mantener el SGSI.
- Aprobar esta política y los objetivos asociados.
- Participar activamente en la Revisión por la Dirección al menos una vez al año.
- Exigir y verificar el cumplimiento de esta política en todas las unidades y terceros relacionados.

La aprobación y firma del Directorio constituyen evidencia del liderazgo en materia de seguridad de la información.

4 Definición de Seguridad de la Información

En Interfase ISA, la seguridad de la información se entiende como la preservación de:

- Confidencialidad: acceso solo a personas autorizadas.
- Integridad: exactitud y completitud de la información y sus procesos.
- Disponibilidad: acceso a la información y a los sistemas cuando sean requeridos para la operación del negocio.

La seguridad de la información se logra implementando controles adecuados de tipo organizativo, procedimental y técnico, como políticas, procedimientos, estructuras organizativas, software e infraestructura tecnológica.

5 Principios rectores

Los siguientes principios guían todas las decisiones y acciones relacionadas con la seguridad de la información en Interfase ISA. Constituyen el marco conceptual sobre el cual se desarrolla el Sistema de Gestión de Seguridad de la Información (SGSI) y aseguran coherencia en la aplicación de políticas, procedimientos y controles en todas las áreas y sedes de la organización:

- Confidencialidad, integridad y disponibilidad (CIA): la protección de la información se centra en garantizar que solo accedan personas autorizadas, que la información sea exacta y completa, y que esté disponible cuando se requiera.
- Cumplimiento legal y contractual: toda actividad deberá ajustarse a las leyes aplicables en Uruguay y Paraguay, así como a los contratos y acuerdos con clientes, proveedores y aliados.
- Responsabilidad compartida: la seguridad de la información es un compromiso de todos los colaboradores y no recae exclusivamente en el área de TI.
- Proporcionalidad: los controles aplicados deben ser adecuados al nivel de riesgo y al valor de los activos de información, evitando tanto la sobrecarga como la insuficiencia de medidas.
- Mejora continua: el SGSI se mantiene dinámico, con revisiones y actualizaciones regulares basadas en evidencias, incidentes, cambios en el contexto y oportunidades de optimización.

Este marco se implementa bajo el ciclo de mejora continua PDCA (Plan–Do–Check–Act) del SGSI: Plan (definir el contexto, riesgos, objetivos y controles); Do (implementar controles, roles y

procedimientos); Check (medir desempeño mediante KPIs, auditorías internas y Revisión por la Dirección); y Act (corregir desviaciones, gestionar acciones de mejora y actualizar políticas y controles). El Directorio y el Comité de Seguridad asegurarán evidencia trazable de cada fase del PDCA en el repositorio del SGSI.

6 Gobernanza y responsabilidades

La seguridad de la información en Interfase ISA es una responsabilidad transversal que involucra a todas las áreas de la organización. La gobernanza del SGSI se estructura de la siguiente manera:

- Directorio: aprueba esta política, asigna los recursos necesarios y lidera con el ejemplo el compromiso con la seguridad de la información. Es responsable de que el SGSI se integre en los procesos de negocio y de que se alcancen los objetivos definidos.
- Comité de Seguridad: órgano colegiado que supervisa la implementación del SGSI, revisa periódicamente su eficacia, valida las decisiones estratégicas (alcance, políticas, riesgos) y aprueba excepciones a la política. Eleva reportes y recomendaciones al Directorio.
- PM SGSI: coordina la implementación y el mantenimiento del SGSI, gestiona el cronograma de actividades, asegura la comunicación entre las unidades de negocio y el Comité, y supervisa el cumplimiento de esta política y de los controles asociados.
- Responsables locales en Uruguay y Paraguay: aseguran la aplicación del SGSI en sus respectivas sedes, coordinando con las áreas locales para cumplir con los lineamientos corporativos.
- Colaboradores: todos los colaboradores de Interfase ISA, sin excepción, tienen la responsabilidad de cumplir esta política, proteger los activos de información bajo su control y reportar cualquier incidente o situación que ponga en riesgo la seguridad de la información.

Las responsabilidades específicas y la segregación de funciones se encuentran documentadas en la Matriz RACI del SGSI, la cual complementa esta política y constituye evidencia formal de la asignación de roles

7 Gestión de riesgos

Interfase ISA aplicará una metodología de gestión de riesgos basada en ISO/IEC 27005 y alineada con la cláusula 6.1 de ISO/IEC 27001:2022.

- Los riesgos se identificarán y valorarán en términos de probabilidad e impacto.

- Se mantendrá una matriz de riesgos actualizada en el repositorio del SGSI.
- Los riesgos serán tratados mediante planes de acción aprobados por el Comité de Seguridad, priorizando controles técnicos, organizativos o compensatorios.
- El Comité de seguridad revisará la matriz de riesgos al menos trimestralmente y el Directorio en la Revisión por la Dirección.
- Se mantendrá un registro histórico de riesgos y tratamientos como evidencia auditable.

8 Cumplimiento legal y regulatorio

Interfase ISA mantendrá un inventario de requisitos legales y contractuales aplicables a la seguridad de la información en todos los países donde Interfase ISA opere o tenga requisitos regulatorios.

- El inventario será revisado anualmente por el Comité de Seguridad y el área Legal externa.
- Se realizarán análisis de impacto regulatorio (DPIA u otros) cuando corresponda.
- Todo contrato con proveedores críticos incluirá cláusulas de seguridad de la información, supervisadas por Finanzas/Admin y validadas por Legal.
- El cumplimiento se evidenciará en auditorías internas y revisiones contractuales.

9 Directrices de alto nivel

Estas directrices marcan el marco general de actuación y se desarrollarán en políticas y procedimientos específicos. Su cumplimiento será supervisado por el Comité de Seguridad:

- Clasificación de la información: toda la información debe clasificarse según criticidad y tratarse conforme a procedimientos documentados.
- Control de accesos: el acceso a sistemas y datos se concederá bajo mínimo privilegio y revisado periódicamente.
- Uso aceptable de activos: los colaboradores deberán utilizar equipos, redes y aplicaciones conforme a la política de uso aceptable.
- Gestión de incidentes: todo incidente debe ser reportado y registrado siguiendo el procedimiento de respuesta a incidentes.

- Continuidad de negocio: se mantendrán planes documentados de continuidad y recuperación probados al menos una vez al año.
- Seguridad en teletrabajo y móviles: se aplicarán cifrado, autenticación multifactor y control de dispositivos.
- Criptografía: todo uso de cifrado se ajustará a estándares definidos en el SGSI.
- Desarrollo seguro: las prácticas de DevSecOps estarán integradas en el ciclo de vida del software.
- Redes y nube: deberán contar con controles perimetrales, monitoreo y configuraciones seguras.
- Proveedores: se evaluarán riesgos antes de contratación y durante la vigencia del contrato.

10 Concientización y formación

Todos los colaboradores recibirán formación obligatoria en seguridad de la información:

- Inducción inicial: al incorporarse.
- Refrescos anuales: para todo colaborador activo.
- Capacitaciones específicas: para roles críticos (TI, desarrollo, operaciones).

La asistencia será registrada y reportada al Comité de Seguridad como evidencia. Además, se realizarán campañas de concientización semestrales sobre riesgos comunes como phishing, contraseñas débiles o teletrabajo seguro.

11 Excepciones

Cualquier excepción a esta política deberá ser:

- Solicitada formalmente por el responsable del área.
- Evaluada por el Comité de Seguridad.
- Aprobada por el Comité de Seguridad, documentando motivo, alcance, controles compensatorios y fecha de expiración.
- Registrada en el Registro de Excepciones del SGSI. Ninguna excepción podrá superar los 90 días sin renovación formal y justificación adicional.

12 Medición y mejora continua

El cumplimiento de esta política se evaluará mediante indicadores clave de desempeño (KPI), tales como:

- % de activos críticos inventariados.
- % de colaboradores capacitados.
- Tiempo medio de respuesta a incidentes críticos.
- % de proveedores críticos evaluados.

Los indicadores tendrán metas definidas (ejemplo: 90% de colaboradores capacitados al año, 95% de activos críticos inventariados) y se revisarán trimestralmente en el Comité y anualmente en la Revisión por la Dirección.

La política será actualizada al menos una vez al año o ante cambios relevantes.

13 Cumplimiento y sanciones

El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y proveedores críticos.

- Para colaboradores: el incumplimiento podrá implicar medidas disciplinarias según reglamentos internos.
- Para contratistas y proveedores: podrá implicar la terminación de contratos o penalidades previstas.
- Casos graves serán elevados al Directorio y al área Legal externa para acciones adicionales.

Todo incumplimiento y su resolución deberán documentarse como parte del SGSI.

14 Vigencia y publicación

Esta política entra en vigor a partir de su aprobación por el Directorio de Interfase ISA. La versión vigente será comunicada y permanecerá disponible para todos los colaboradores mediante los canales institucionales oficiales, dentro del repositorio del SGSI.

El Comité de Seguridad es responsable de garantizar que únicamente la versión aprobada se encuentre publicada y accesible, así como de coordinar su revisión periódica. La presente política

deberá revisarse al menos una vez al año, o antes si ocurren cambios relevantes en el contexto legal, contractual, organizacional o tecnológico.

Toda modificación deberá quedar registrada bajo control de versiones y ser sometida a aprobación del Directorio antes de su entrada en vigor.

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

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich