Política de Gestión de Riesgo

Fecha: 15/09/2025
Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
15/09/2024	0.1	Creación del Documento	PM SGSI
15/09/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información

Contenido

1 Objetivo

El propósito de esta política es establecer un marco formal para la gestión de riesgos de seguridad de la información en Interfase ISA. Su objetivo es garantizar que los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, el cumplimiento legal y contractual, y la continuidad de las operaciones sean identificados, evaluados, tratados y monitoreados de manera sistemática, de acuerdo con los requisitos de la norma ISO/IEC 27001:2022.

2 Alcance

Esta política aplica a todas las sedes de Interfase ISA. Su cobertura incluye los procesos internos de negocio, las soluciones digitales ofrecidas a clientes, la infraestructura tecnológica en entornos locales y en la nube, los esquemas de teletrabajo autorizados y los servicios prestados por proveedores críticos. El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y terceros que procesen información en nombre de la organización.

La gestión de riesgos se aplicará también de forma preventiva ante nuevas sedes, ampliaciones de operación, apertura de mercados o cambios relevantes del contexto, de modo que antes del inicio de actividades se realicen identificación, valoración y tratamiento de riesgos, incorporando los resultados a la Matriz de Riesgos, Planes de Tratamiento y SoA.

3 Roles y responsabilidades

La gestión de riesgos en Interfase ISA es una responsabilidad transversal que involucra a todas las áreas de la organización. La gobernanza de este proceso se estructura de la siguiente manera:

- Directorio: aprueba esta política, asigna los recursos necesarios y se reserva la autoridad para aceptar los riesgos de nivel crítico. Asimismo, asegura que la gestión de riesgos esté integrada en los procesos de negocio y en la toma de decisiones estratégicas.
- Comité de Seguridad actúa como responsable de supervisar la aplicación de esta política. Revisa periódicamente la eficacia del proceso, valida la metodología de gestión de riesgos, aprueba los planes de tratamiento significativos y eleva los resultados al Directorio. También tiene la función de aprobar excepciones en casos justificados.
- PM del SGSI coordina el proceso de gestión de riesgos, mantiene actualizada la Matriz de Riesgos, centraliza la información proveniente de las diferentes áreas y asegura la correcta comunicación entre las unidades de negocio, el Comité y el Directorio.

- Responsables locales en Uruguay y Paraguay aplican la política en sus respectivas sedes, coordinando con las áreas locales para identificar y tratar los riesgos que puedan afectar sus operaciones.

- Todos los colaboradores de Interfase ISA son responsables de cumplir esta política, proteger los activos de información bajo su control y reportar cualquier situación que pueda convertirse en un riesgo para la seguridad de la información. Además, deberán participar en instancias de formación periódica en gestión de riesgos de seguridad de la información, con el fin de comprender plenamente sus responsabilidades y contar con las competencias necesarias para aplicar esta política. Las capacitaciones quedarán registradas como evidencia del cumplimiento.

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

El cumplimiento de esta política es obligatorio para todos los colaboradores y áreas de Interfase ISA. Las consecuencias por incumplimiento están definidas en la Política General de Seguridad de la Información y en los reglamentos internos vigente.

4 Criterios de aceptación

Los riesgos en Interfase ISA se valoran considerando su probabilidad de ocurrencia y el impacto que podrían tener sobre la confidencialidad, integridad y disponibilidad de la información, el cumplimiento legal y la continuidad de las operaciones. Para esta valoración se utiliza una escala del 1 al 5 en cada dimensión, obteniéndose un valor de riesgo calculado como el producto de probabilidad por impacto ($R = P \times I$), con un rango posible de 1 a 25.

La clasificación y los criterios de aceptación son los siguientes:

- Riesgos de nivel bajo o medio (valores entre 1 y 9) podrán ser aceptados por el propietario del riesgo en conjunto con el PM del SGSI, siempre que se mantengan dentro de los umbrales establecidos por la organización.

- Riesgos de nivel alto (valores entre 10 y 15) requerirán la aprobación del Comité de Seguridad y deberán estar acompañados de un plan de tratamiento en curso.

- Riesgos de nivel crítico (valores entre 16 y 25) solo podrán ser aceptados por el Directorio y de manera excepcional, exigiéndose en estos casos la aplicación de controles compensatorios documentados.

Estos criterios y umbrales serán revisados de manera anual o cuando se produzcan cambios significativos en el contexto interno o externo de la organización, garantizando que la gestión de riesgos se mantenga alineada con la tolerancia al riesgo definida por el Directorio.

5 Proceso y Registros

La gestión de riesgos en Interfase ISA se desarrolla de manera estructurada y continua. El proceso inicia con la identificación de activos de información, amenazas, vulnerabilidades y escenarios que puedan afectar a la organización. Posteriormente, cada riesgo identificado es sometido a una valoración, aplicando la metodología definida en esta política y en los procedimientos asociados.

A partir de esta valoración, se definen las decisiones de tratamiento que pueden incluir la mitigación mediante controles, la transferencia a terceros, la aceptación conforme a los criterios establecidos o la eliminación de la actividad que lo origina.

Todos los riesgos y sus tratamientos deben contar con un responsable designado y estar documentados en los registros oficiales del SGSI. Estos registros incluyen:

- Matriz de Riesgos, que centraliza la información;
- Planes de Tratamiento, donde se detallan acciones, responsables, recursos y plazos;
- Registro de Riesgos Residuales, que documenta aquellos riesgos aceptados; y
- Declaración de Aplicabilidad (SoA), que vincula los riesgos con los controles de ISO/IEC 27001 y las políticas implementadas en la organización.

Todos estos documentos se encuentran bajo control documental y forman parte del repositorio oficial del SGSI, asegurando su trazabilidad y disponibilidad para fines de auditoría.

6 Integración con el SGSI

La gestión de riesgos en Interfase ISA no se desarrolla de manera aislada, sino como un componente integrado del Sistema de Gestión de Seguridad de la Información. Esta integración asegura que los riesgos sean considerados de forma transversal en los principales procesos de la organización y que los controles definidos mantengan coherencia y efectividad.

- Gestión de cambios, toda modificación en la infraestructura tecnológica, en aplicaciones o en configuraciones debe incluir una evaluación de riesgos previa a su aprobación, con el fin de evitar la introducción de vulnerabilidades.

- Gestión de incidentes, los eventos reportados sirven como insumo para actualizar la matriz de riesgos y ajustar los controles de seguridad, fortaleciendo así la capacidad de respuesta de la organización.
- Continuidad de negocio, la organización reconoce la necesidad de establecer objetivos de recuperación y planes de contingencia específicos. Actualmente, esta actividad se encuentra en etapa de planificación y será formalizada en la siguiente fase de implementación del SGSI, tomando como insumo principal los riesgos de indisponibilidad identificados en la matriz de riesgos.
- Gestión de proveedores, la evaluación de riesgos se incorpora en la etapa de contratación y en el seguimiento de servicios considerados críticos, de modo que se reflejen las obligaciones de seguridad en los acuerdos contractuales.
- Ciclo de desarrollo de software, los riesgos de seguridad se consideran en todas las fases del proceso, desde el diseño hasta la puesta en producción, garantizando que la seguridad se integre desde el inicio y no de forma reactiva.

Las evidencias de estas integraciones quedan reflejadas en los registros oficiales del SGSI, lo que asegura la trazabilidad del proceso y la disponibilidad de información para auditorías internas y externas.

7 Medición, Revisión y Excepciones

La eficacia del proceso de gestión de riesgos en Interfase ISA se evalúa a través de indicadores definidos por el Comité de Seguridad. Estos indicadores permiten verificar el grado de actualización de la matriz de riesgos, el cumplimiento de los planes de tratamiento en los plazos acordados, la existencia de controles activos sobre los riesgos críticos y la vigencia de las evaluaciones de proveedores críticos.

Los resultados obtenidos son revisados bimestralmente en el Comité de Seguridad y se consolidan en un informe anual que se presenta en la Revisión por la Dirección, constituyendo la base para la mejora continua del SGSI.

Las excepciones a esta política solo podrán autorizarse de manera formal mediante una solicitud escrita, en la que se justifique la necesidad, se detallen los controles compensatorios propuestos y se establezca un plazo máximo de noventa días. Dichas excepciones deberán ser aprobadas por el Comité de Seguridad y, en el caso de riesgos críticos, por el Directorio. Todas las excepciones aprobadas quedarán registradas en el Registro de Excepciones del SGSI, lo que asegura su trazabilidad y permite demostrar la gestión responsable de estas situaciones frente a auditorías internas o externas.

8 Vigencia y publicación

Esta política entra en vigor a partir de su aprobación por el Directorio de Interfase ISA. La versión vigente será comunicada a todos los colaboradores mediante los canales institucionales oficiales y permanecerá disponible en la intranet corporativa, 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:
1.0	DD/MM/AAAA	DD/MM/AAAA	Directorio – Interfase ISA

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich