Política de Seguridad en Operaciones TI

Fecha: 19/09/2025

Versión: 2.0

Control de versiones

Fecha	Versión	Descripción	Autor
05/11/2022	0.1	Creación del Documento	Comité de Seguridad de la Información
10/11/2022	1.0	Revisión del Documento	Comité de Seguridad de la Información
12/12/2023	1.1	Revisión del documento	Comité de Seguridad de la Información
19/09/2025	2.0	Actualización de Política según alcance e implementación de SGSI	Comité de Seguridad de la Información

Contenido

1 Objetivo

Establecer los lineamientos generales para garantizar la seguridad en las operaciones tecnológicas de Interfase ISA, asegurando la confidencialidad, integridad y disponibilidad de la información en todas sus sedes, conforme a los requisitos de la norma ISO/IEC 27001:2022.

2 Alcance

Esta política aplica a todas las operaciones tecnológicas de Interfase ISA en todas sus sedes, incluyendo infraestructura local, servicios en la nube, redes corporativas, estaciones de trabajo, entornos de desarrollo, pruebas y producción, así como a proveedores externos que brinden servicios críticos relacionados con la operación TI.

3 Roles y responsabilidades

La seguridad en las operaciones TI es responsabilidad compartida entre todas las áreas:

- Directorio: aprueba la política, asigna los recursos necesarios y supervisa el cumplimiento de los objetivos estratégicos.
- Comité de Seguridad: supervisa la aplicación de esta política, valida excepciones y revisa periódicamente la eficacia de los controles operativos.
- Área de TI: responsable de la implementación de los lineamientos aquí definidos, el mantenimiento de la infraestructura tecnológica y la ejecución de los procedimientos técnicos.
- Responsables de Área: notifican necesidades específicas y colaboran en la aplicación de controles operativos.
- Colaboradores y terceros: cumplen con esta política y reportan cualquier incidente o situación anómala relacionada con las operaciones TI.

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

4 Seguridad en la gestión de operaciones

Las operaciones TI deberán regirse por los siguientes principios:

- Monitoreo permanente de sistemas y servicios críticos.
- Gestión segura de registros y logs, garantizando su integridad y disponibilidad para auditorías.
- Control de cambios y actualizaciones siguiendo procedimientos formales documentados.
- Mantenimiento preventivo y correctivo planificado sobre los activos de TI.

5 Gestión de cambios

Todo cambio en la infraestructura tecnológica, aplicaciones o servicios debe ser gestionado conforme a un proceso formal de gestión de cambios aprobado por el Comité de Seguridad.

- Los cambios serán clasificados según su impacto (menor, mayor, emergencia).
- Cada solicitud deberá contar con una evaluación de riesgos, aprobación previa y registro en el repositorio oficial.
- Los cambios de emergencia deberán ser documentados y revisados posteriormente por el Comité.

Los detalles operativos del proceso estarán documentados en el Procedimiento de Gestión de Cambios de TI, mantenido por el área de TI y supervisado por el Comité de Seguridad.

6 Copias de seguridad y restauración

La gestión de respaldos es parte esencial de la continuidad de operaciones y de la protección de los activos de información.

- Alcance: incluye servidores, bases de datos, aplicaciones críticas, configuraciones de red y archivos relevantes.
- Periodicidad: las copias deberán realizarse con la frecuencia definida por el Comité de Seguridad y documentada en los procedimientos técnicos de TI.

- Almacenamiento: en ubicaciones seguras, con controles de acceso restringidos y, cuando corresponda, redundancia geográfica.
- Pruebas de restauración: al menos una vez al año, para validar la integridad y disponibilidad de la información.
- Se deberán ejecutar pruebas de restauración inmediatas tras incidentes críticos que afecten la disponibilidad o integridad de la información (p. ej., ransomware, corrupción de datos), a fin de validar la recuperabilidad real y documentar tiempos logrados frente a los objetivos definidos.
- Retención y eliminación: se conservarán según los plazos legales, contractuales o de negocio, eliminándose de manera segura.
- Controles técnicos: las copias deberán estar cifradas y protegidas frente a accesos no autorizados.
- Responsables: el área de TI ejecuta los respaldos; el Comité de Seguridad supervisa su eficacia.

Los procesos de respaldo y restauración deberán estar formalmente definidos, documentados y actualizados en los procedimientos técnicos de TI, asegurando la trazabilidad de su ejecución y de las pruebas realizadas. El Comité de Seguridad revisará periódicamente los resultados y métricas asociadas —como el porcentaje de respaldos exitosos y de pruebas de restauración validadas— para garantizar la eficacia y mejora continua del proceso.

~~El Comité de Seguridad revisará métricas periódicas como el porcentaje de respaldos exitosos y el porcentaje de pruebas de restauración validadas, para asegurar la eficacia del proceso.~~

Commented [RA1]: Aca capaz pondría de que los respaldos y las pruebas de restauración deberán estar debidamente definidos en procedimientos y documentados

7 Gestión de la capacidad y disponibilidad

La capacidad y disponibilidad de los recursos tecnológicos de Interfase ISA deberán gestionarse de manera proactiva, asegurando que las operaciones soporten la demanda actual y futura sin degradar los niveles de servicio comprometidos con clientes internos y externos.

El área de TI deberá:

- Monitorear continuamente el rendimiento de servidores, redes, aplicaciones y servicios en la nube mediante herramientas de supervisión autorizadas.

- Definir y reportar al Comité de Seguridad indicadores clave, como porcentaje de disponibilidad mensual de servicios críticos, tiempo medio entre fallas (MTBF), tiempo medio de recuperación (MTTR) y nivel de utilización de recursos.
- Planificar ampliaciones o mejoras de capacidad con base en proyecciones de crecimiento de carga, nuevos proyectos o requerimientos contractuales.
- Documentar incidentes de disponibilidad, análisis de causa raíz y planes de acción, integrándolos con la Política de Gestión de Incidentes y la de Continuidad de Negocio.

El Comité de Seguridad revisará semestralmente los informes de capacidad y disponibilidad, proponiendo acciones de mejora cuando se detecten riesgos de degradación del servicio.

8 Gestión de vulnerabilidades y parches

El área de TI deberá implementar un proceso sistemático de gestión de vulnerabilidades y parches que asegure la protección oportuna de los sistemas de Interfase ISA. Este proceso incluirá:

- Identificación proactiva de vulnerabilidades mediante escaneos periódicos, alertas de fabricantes y fuentes reconocidas de ciberseguridad.
- Evaluación del riesgo asociado a cada vulnerabilidad, considerando impacto en la confidencialidad, integridad, disponibilidad, cumplimiento legal y contractual.
- Aplicación de actualizaciones de seguridad en plazos máximos de: 15 días para vulnerabilidades críticas, 30 días para vulnerabilidades altas y 45 días para medias.
- Documentación de excepciones justificadas, con aprobación del Comité de Seguridad e implementación de controles compensatorios.
- Mantenimiento de registros verificables de parches aplicados, excepciones autorizadas y resultados de validación.

El Comité de Seguridad revisará trimestralmente los informes de vulnerabilidades y el estado de aplicación de parches como parte del proceso de mejora continua del SGSI.

9 Acceso a redes y teletrabajo

El acceso a las redes internas y externas de Interfase ISA estará estrictamente controlado bajo el principio de mínimo privilegio y en concordancia con la Política de Control de Accesos.

- Todo acceso remoto se habilitará únicamente a través de canales seguros, empleando VPN corporativa, autenticación multifactor (MFA) y cifrado de extremo a extremo.
- Los dispositivos utilizados para teletrabajo deberán cumplir con los estándares de seguridad definidos por TI, incluyendo actualizaciones vigentes, protección antivirus y cifrado de disco.
- Queda prohibido el uso de dispositivos personales no autorizados para conectarse a las redes corporativas.
- El área de TI deberá monitorear y registrar todas las conexiones remotas y de red, conservando logs de acceso como evidencia de auditoría.
- Terceros que requieran acceso remoto deberán contar con un contrato o acuerdo de confidencialidad firmado, y su acceso será limitado en alcance y tiempo.

El Comité de Seguridad revisará semestralmente los informes de accesos remotos y el cumplimiento de los controles de teletrabajo, proponiendo mejoras cuando se detecten desviaciones.

10 Cumplimiento y seguimiento

El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y terceros que utilicen activos de Interfase ISA.

El incumplimiento será gestionado conforme a la Política General de Seguridad de la Información y a los reglamentos internos de la organización.

El Comité de Seguridad supervisará periódicamente la aplicación de esta política, evaluará la eficacia de los controles implementados y elaborará un reporte anual de cumplimiento que será elevado al Directorio como parte de la Revisión por la Dirección.

El reporte anual de cumplimiento incluirá métricas de disponibilidad, incidencias operativas, aplicación de parches y resultados de pruebas de restauración, y será elevado al Directorio como parte de la Revisión por la Dirección.

11 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 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 esté publicada y accesible, así como de coordinar su revisión periódica. La política será revisada al menos una vez al año o antes si ocurren cambios relevantes en el contexto legal, contractual, organizacional o tecnológico.

Toda modificación deberá registrarse bajo control de versiones y ser aprobada por el 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