Política de Gestión de Incidentes

Fecha: 17/09/2025
Versión: 2.0

Control de versiones

Fecha	Versión	Descripción	Autor
10/11/2022	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
18/11/2023	1.1	Revisión de la Documento	Comité de Seguridad de la Información
17/09/2025	2.0	Actualización de Política según alcance e implementación de SGSI	Comité de Seguridad de la Información

Contenido

1 Objetivo

Establecer el marco formal para identificar, registrar, clasificar, tratar y cerrar los incidentes de seguridad de la información en Interfase ISA, protegiendo la confidencialidad, integridad y disponibilidad de la información y cumpliendo con ISO/IEC 27001:2022.

2 Alcance

Aplica a todas las operaciones de Interfase ISA en todas las sedes, incluyendo teletrabajo y terceros con acceso a nuestros sistemas. Abarca eventos e incidentes que afecten datos, aplicaciones, infraestructura, redes, servicios en la nube y activos de clientes procesados por Interfase ISA.

3 Definiciones

- Evento de seguridad: Suceso observable que puede o no impactar la seguridad (p. ej., múltiples intentos fallidos).
- Incidente de seguridad: Evento o serie de eventos que comprometen o podrían comprometer CIA, cumplimiento o continuidad.
- Severidad: Grado de impacto y urgencia (Crítico, Alto, Medio, Bajo).

4 Roles y responsabilidades

La gestión de incidentes es una responsabilidad compartida:

- Directorio: aprueba esta política, asigna recursos, y recibe reportes consolidados.
- Comité de Seguridad: supervisa el proceso, aprueba decisiones clave y excepciones, analiza tendencias y eleva informes a la Dirección.
- PM del SGSI: coordina el proceso end-to-end, consolida evidencias y métricas, y asegura la mejora continua.
- Infraestructura/Soporte TI: ejecuta contención, erradicación y recuperación; mantiene registros técnicos y evidencia.
- Responsables de Área/Propietarios de Activos: notifican, validan impacto de negocio, priorizan acciones y aprueban cierre funcional.

- Colaboradores y terceros: reportan de inmediato cualquier sospecha o incidente por los canales oficiales.

Todas las responsabilidades y la segregación de funciones están documentadas en la Matriz RACI del SGSI. Esta matriz constituye evidencia formal de auditoría y deberá mantenerse actualizada ante cualquier cambio organizacional o de funciones.

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 verificable en auditorías internas y externas.

5 Principios de gestión incidente

La gestión de incidentes en Interfase ISA se rige por principios que aseguran una respuesta rápida, coordinada y eficaz, minimizando el impacto sobre las operaciones y garantizando el aprendizaje organizacional. Estos principios son:

Registro obligatorio

Todos los incidentes de seguridad, sin importar su nivel de criticidad, deben ser reportados y registrados en los canales oficiales definidos por el Comité de Seguridad. A su vez es obligatorio informar incidentes a entes reguladores cuando la ley lo requiera.

Clasificación y priorización

Los incidentes serán clasificados según su impacto en la confidencialidad, integridad, disponibilidad, cumplimiento normativo o reputación de Interfase ISA. Su priorización determinará los tiempos de respuesta y los responsables de su gestión.

Contención y erradicación

Se aplicarán medidas inmediatas de contención para limitar los efectos del incidente, seguidas de acciones correctivas para eliminar la causa raíz y restaurar la operación segura.

Aprendizaje y mejora continua

Cada incidente dará lugar a un análisis de causa raíz y a la definición de acciones preventivas, que quedarán documentadas en los registros oficiales del SGSI.

Integración con otras políticas

La gestión de incidentes se integra con la Política de Continuidad de Negocio y Recuperación ante Desastres, la Política de Gestión de Cambios y la Política de Clasificación y Manejo de la Información, asegurando coherencia en la respuesta y tratamiento de los eventos.

Procedimientos técnicos de soporte

El detalle operativo de los canales de reporte, tiempos de respuesta, responsables técnicos y formatos de registro será definido en el Procedimiento de Gestión de Incidentes de TI, a elaborar y mantener por el Comité de Seguridad junto al área de Infraestructura

Estos principios se aplican a incidentes originados tanto interna como externamente, incluyendo los relacionados con proveedores, clientes y terceros con acceso a los sistemas de Interfase ISA.

6 Clasificación de severidad (criterios de alto nivel)

Para priorizar la gestión de incidentes, Interfase ISA establece cuatro niveles de severidad:

- Crítico: fuga de datos sensibles; ransomware activo; caída de servicio core; impacto legal/regulatorio inminente.
- Alto: compromiso de cuentas privilegiadas; malware contenido sin cifrado; degradación severa de servicio.
- Medio: acceso indebido limitado; error de configuración con exposición acotada; phishing con clics sin ejecución.
- Bajo: intentos fallidos, alertas de IDS sin impacto, hallazgos preventivos.

La severidad final se determina por impacto + urgencia, y puede ajustarse durante el ciclo del incidente.

Los ejemplos aquí establecidos complementan la metodología formal de valoración de incidentes, definida en el Procedimiento de Gestión de Incidentes, donde se detallan los criterios específicos de probabilidad e impacto sobre la confidencialidad, integridad, disponibilidad, cumplimiento y continuidad

7 Proceso de gestión de incidentes

El proceso de gestión de incidentes en Interfase ISA se desarrolla de manera estructurada y continua, abarcando todas las fases necesarias para garantizar una respuesta eficaz:

- Detección y Reporte: todo colaborador o tercero debe reportar de inmediato (máximo 24hs) usando el canal oficial definido (ticketing o correos dedicados). TI registra el evento/incidente y asigna un responsable de gestión.
- Registro y Clasificación: se documenta fecha, hora, fuente, activos afectados, síntomas, alcance preliminar, severidad inicial y responsable.
- Análisis y Diagnóstico: confirmación del incidente, escenario de amenaza, vectores, alcance e impacto a CIA/continuidad/cumplimiento. Se preservan evidencias con cadena de custodia.
- Contención: se aplican acciones inmediatas para limitar el impacto (aislar hosts/usuarios, bloquear IPs, revocar credenciales), sin comprometer la preservación de evidencia.
- Erradicación y Recuperación: eliminación de artefactos maliciosos, corrección de configuraciones, aplicación de parches y restauración desde backups verificados. Se valida que los servicios se restablezcan de forma segura.
- Comunicación y Escalamiento: notificaciones internas según la severidad; el Comité de Seguridad se involucra en incidentes de nivel Alto o Crítico. La comunicación externa con clientes, proveedores o reguladores será realizada únicamente por los voceros designados por el Directorio. Cuando la normativa aplicable lo exija, Interfase ISA notificará los incidentes a las autoridades o entes reguladores competentes dentro de los plazos legales, coordinando dicha comunicación con Asesoría Legal y los voceros designados por el Directorio.
- Cierre y Lecciones Aprendidas: los incidentes se cierran solo cuando el servicio esté estable, los riesgos mitigados y la documentación completa, con aprobación del propietario del activo. Para incidentes Alto o Crítico, se realizará un análisis post-mortem en un plazo máximo de 10 días hábiles.

El detalle operativo de cada fase del proceso será documentado en el Procedimiento Técnico de Gestión de Incidentes, bajo la custodia del Comité de Seguridad y del área de Infraestructura TI, asegurando trazabilidad y coherencia con el SGSI.

8 Tiempos objetivos (SLA internos de referencia)

Interfase ISA establece tiempos de referencia (SLA internos) para asegurar una respuesta oportuna y proporcional a la criticidad de los incidentes:

- Registro / Acknowledge: ≤ 1 h (Crítico/Alto), ≤ 4 hs (Medio), ≤ 8 hs (Bajo).

- Contención inicial: ≤ 4 hs (Crítico/Alto), ≤ 1 día (Medio).
- Informe ejecutivo inicial: ≤ 24 hs (Crítico/Alto).
- Post-mortem: ≤ 10 días hábiles (Alto/Crítico).

Estos tiempos servirán como referencia para medir la eficacia de la respuesta, pudiendo ser ajustados por el Comité de Seguridad según las capacidades técnicas, las lecciones aprendidas de incidentes previos y la evolución del contexto tecnológico y organizacional. Toda excepción deberá documentarse y contar con justificación formal.

9 Evidencia y cadena de custodia

Toda evidencia generada o recolectada durante la gestión de incidentes (logs, volcados de memoria, imágenes forenses, correos electrónicos, entre otros) debe preservarse de manera íntegra, asegurando su validez como prueba técnica y legal.

La preservación de evidencias seguirá estos principios:

- Cada evidencia deberá contar con un hash, fecha/hora de captura, custodio asignado y ubicación segura de almacenamiento.
- Solo personal autorizado podrá manipular las evidencias; toda transferencia deberá registrarse formalmente.
- El plazo de retención se ajustará a la normativa legal vigente del país, a los contratos con clientes y a las directrices del Comité de Seguridad.

La gestión de evidencias se encuentra alineada con la Política de Protección de Datos y constituye parte del cumplimiento normativo y contractual de Interfase ISA.

10 Integración del proceso

El proceso de gestión de incidentes en Interfase ISA no opera de manera aislada, sino que se encuentra integrado con otros procesos y políticas del SGSI:

- Gestión de Cambios: los cambios urgentes derivados de un incidente deberán gestionarse conforme al procedimiento de cambios de emergencia.
- Continuidad de Negocio y Recuperación ante Desastres (BCP/DRP): en incidentes que generen indisponibilidad mayor, se activarán los planes correspondientes para asegurar la recuperación de los servicios críticos.

- Proveedores y Terceros: los incidentes que involucren servicios prestados por terceros se gestionarán en coordinación con los proveedores, conforme a lo establecido en los SLA y cláusulas contractuales de seguridad.
- Protección de Datos y Asesoría Legal: en incidentes que involucren datos personales o que tengan impacto regulatorio, se deberá coordinar con asesoría legal externa y con los responsables de procesos afectados, garantizando el cumplimiento normativo.

Las integraciones aquí descritas se encuentran reflejadas en la Declaración de Aplicabilidad (SoA), asegurando coherencia entre los riesgos identificados, los controles aplicados y las políticas corporativas de Interfase ISA.

11 Métricas y mejora continua

La gestión de incidentes de seguridad en Interfase ISA será objeto de seguimiento permanente a través de métricas que permitan evaluar la eficacia del proceso y orientar acciones de mejora.

Los indicadores mínimos a medir incluyen:

- Número de incidentes registrados por severidad y por causa raíz.
- Tiempo medio de detección (MTTD) y tiempo medio de resolución (MTTR), segmentados por severidad.
- Porcentaje de incidentes con análisis post-mortem realizado dentro del plazo definido.
- Porcentaje de acciones correctivas y preventivas cerradas en los plazos comprometidos.
- Nivel de cumplimiento de los SLA internos definidos para registro, contención, comunicación y cierre.
- Cumplimiento de los requisitos de preservación de evidencias y cadena de custodia.

El Comité de Seguridad consolidará estas métricas en informes periódicos y elaborará un reporte anual que será elevado al Directorio en el marco de la Revisión por la Dirección. Dicho reporte incluirá tendencias, brechas identificadas, propuestas de acciones de mejora y un análisis comparativo respecto al periodo anterior.

La información derivada de estas métricas será utilizada como insumo para el plan de mejora continua del SGSI, garantizando que las lecciones aprendidas de los incidentes se traduzcan en la implementación de nuevos controles, capacitaciones, actualizaciones de políticas y revisiones de procedimientos cuando corresponda.

12 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.

13 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.

tuid
FIRMA DIGITAL
Leonardo Adrian Noach Meierovich

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