Política de Continuidad de Negocio y Recuperación ante Desastres

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
17/11/2023	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

El propósito de esta política es establecer el marco de referencia para asegurar la continuidad de los procesos críticos de negocio de Interfase ISA frente a interrupciones no planificadas, y garantizar la recuperación ordenada de los servicios tecnológicos y de la información. Su objetivo principal es minimizar el impacto de incidentes disruptivos sobre la confidencialidad, integridad, disponibilidad y cumplimiento normativo, en línea con los requisitos de la norma ISO/IEC 27001:2022.

2 Alcance

Esta política aplica a todas las sedes de Interfase ISA y cubre los procesos críticos de negocio, la infraestructura tecnológica (local y en la nube), los servicios ofrecidos a clientes, los esquemas de teletrabajo autorizados y los proveedores que respalden la operación.

El cumplimiento de esta política es obligatorio para todos los colaboradores, contratistas y terceros que participen en la operación de procesos críticos o que tengan responsabilidad en la continuidad de negocio y la recuperación ante desastres.

Este alcance se alinea con los procesos críticos definidos en el Análisis de Impacto al Negocio (BIA), que constituye la base para los planes de continuidad y recuperación.

3 Roles y responsabilidades

La continuidad de negocio y la recuperación ante desastres son responsabilidades compartidas:

- Directorio: aprueba esta política, asigna los recursos necesarios y valida los planes de continuidad y recuperación.
- Comité de Seguridad: supervisa la implementación de los planes, revisa periódicamente los resultados de pruebas y simulacros, y eleva reportes al Directorio.
- PM del SGSI: coordina la elaboración, mantenimiento y revisión de los planes de continuidad y recuperación, garantizando la integración con el resto de las políticas y controles del SGSI.
- Responsables de Área: identifican procesos críticos bajo su control, definen requerimientos de continuidad y participan en la ejecución de pruebas y simulacros.

- Área de TI: implementa y mantiene las soluciones de respaldo, redundancia, recuperación de datos y sistemas tecnológicos asociados.
- Colaboradores: cumplen con los lineamientos definidos en los planes, participan en capacitaciones y en ejercicios de prueba cuando corresponda.

Las responsabilidades específicas se encuentran documentadas en la Matriz RACI del SGSI, que complementa esta política y constituye evidencia de auditoría. Cada rol es responsable de garantizar que los planes bajo su custodia sean actualizados tras cambios relevantes en procesos, infraestructura o proveedores críticos, informando al Comité de Seguridad para su consolidación.

4 Principios rectores

La continuidad de negocio en Interfase ISA se rige por los siguientes principios:

- Preparación anticipada: toda interrupción significativa debe estar prevista mediante análisis de impacto al negocio (BIA) y planes de respuesta.
- Priorización: los recursos se orientan primero a la recuperación de procesos y servicios críticos para clientes y para la operación interna.
- Redundancia y resiliencia: la infraestructura tecnológica debe contar con respaldos periódicos, medidas de redundancia y capacidades de recuperación verificables.
- Mejora continua: las lecciones aprendidas de incidentes y simulacros alimentan la revisión y actualización de los planes.

5 Planes de continuidad y recuperación

Interfase ISA contará con planes documentados que detallen:

- Los procesos críticos identificados y sus tiempos máximos de tolerancia a la interrupción (RTO) y niveles aceptables de pérdida de datos (RPO).
- Estrategias de respaldo de información y sistemas, incluyendo copias fuera de sitio y almacenamiento seguro en la nube.
- Procedimientos de recuperación de infraestructura tecnológica y comunicaciones, incluyendo ambientes alternos o contingentes.

- Roles, responsables y mecanismos de coordinación durante una crisis.
- Protocolos de comunicación interna y externa en caso de incidentes mayores.

Los planes deberán incluir criterios de activación, procedimientos escalonados de respuesta y responsables de aprobación del retorno a la normalidad. Estos documentos estarán bajo control documental y sujetos a revisiones tras cada prueba programada o incidente real, asegurando su vigencia y mejora continua.

Para proveedores críticos, se exigirá la existencia de planes de continuidad y recuperación equivalentes, que deberán ser presentados, revisados y validados por Interfase ISA como condición contractual. Estos planes se evaluarán periódicamente, y sus resultados se integrarán al BIA, la Matriz de Riesgos y los procedimientos de recuperación de ISA.

El detalle técnico de cada plan se desarrollará en los Procedimientos de Continuidad de Negocio y DRP (Disaster Recovery Plan), los cuales serán elaborados y mantenidos por el Comité de Seguridad junto con las áreas responsables.

6 Pruebas, simulacros y mantenimiento

Los planes de continuidad y recuperación deberán ser probados al menos una vez al año mediante simulacros que contemplen distintos escenarios, tales como indisponibilidad de sistemas, cortes de energía, fallas en proveedores críticos o incidentes de ciberseguridad.

Adicionalmente, deberán realizarse pruebas extraordinarias siempre que ocurran cambios significativos en los procesos críticos, la infraestructura tecnológica o tras incidentes reales que afecten la continuidad.

El Comité de Seguridad será responsable de:

- Planificar y coordinar las pruebas y simulacros, definiendo su alcance y periodicidad.
- Asegurar que las pruebas incluyan tanto ejercicios de escritorio como pruebas técnicas de restauración y recuperación.
- Documentar los resultados, hallazgos y acciones de mejora en informes oficiales.
- Validar la efectividad de los tiempos de recuperación (RTO) y los niveles de pérdida de datos (RPO) frente a los objetivos establecidos.
- Coordinar el mantenimiento de los planes, asegurando su actualización bajo control documental después de cada prueba o incidente real.

Los resultados de las pruebas deberán consolidarse en reportes oficiales, incluir evidencias y hallazgos, y ser elevados al Comité de Seguridad en un plazo máximo de 30 días. Estos reportes alimentarán el plan de mejora continua y deberán mantenerse bajo control documental.

7 Integración con el SGSI

La continuidad de negocio se integra con:

- Política de Gestión de Incidentes, para responder a incidentes mayores que deriven en interrupciones.
- Política de Operaciones TI, para garantizar que los respaldos y configuraciones de seguridad estén alineados a los planes de recuperación.
- Política de Seguridad en Proveedores, para asegurar que terceros críticos mantengan planes equivalentes y contractualmente exigibles.
- Política de Riesgos, para que los escenarios de continuidad se reflejen en la matriz de riesgos y en el SoA.

Esta integración asegura que los escenarios de continuidad estén alineados con la Declaración de Aplicabilidad (SoA) y con los controles definidos en ISO/IEC 27001:2022.

8 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 Comité de Seguridad medirá la eficacia de los planes mediante indicadores como: % de pruebas realizadas en plazo, % de hallazgos corregidos en tiempo, RTO/RPO alcanzados frente a lo planificado y nº de proveedores críticos con planes validados.

Los indicadores de eficacia deberán ser revisados en cada sesión del Comité de Seguridad y en la Revisión por la Dirección, garantizando la trazabilidad de los resultados y la priorización de las acciones correctivas.

9 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