Política de Auditoría y Logging

Fecha: 10/10/2025

Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
10/10/2025	0.1	Creación del Documento	PM SGSI
17/10/2023	1.0	Revisión del Documento	Comité de Seguridad de la Información

Contenido

1 Objetivo

Establecer los lineamientos que aseguren la captura, conservación, revisión y protección de los registros de auditoría y eventos generados por los sistemas de información de Interfase ISA, garantizando la trazabilidad de las actividades, la detección oportuna de incidentes y el cumplimiento de los requisitos normativos y contractuales.

Esta política se basa en los controles A.8.15 y A.8.16 de la norma ISO/IEC 27001:2022 y define las directrices para la captura, protección y revisión de registros de auditoría (logs), asegurando la trazabilidad, integridad y disponibilidad de la información registrada, de acuerdo con el análisis de riesgos del SGSI.

2 Alcance

Aplica a todas las sedes, sistemas, aplicaciones, infraestructuras, plataformas y servicios de Interfase ISA, incluyendo entornos locales, virtualizados o en la nube, que generen o gestionen registros de actividad relacionados con los activos de información de la organización.

Abarca tanto los registros técnicos (sistemas, bases de datos, dispositivos de red, servidores, aplicaciones) como los registros administrativos y de seguridad (accesos, auditorías, incidentes, configuraciones, cambios, etc.).

3 Roles y responsabilidades

La auditoría y gestión de registros es una responsabilidad compartida entre las áreas de tecnología, seguridad y gestión de la información.

- Directorio: aprueba esta política y supervisa su cumplimiento durante la Revisión por la Dirección.
- Comité de Seguridad: supervisa el cumplimiento de esta política, define los requerimientos de auditoría y revisa los resultados consolidados.
- PM del SGSI: coordina la integración de esta política con los procedimientos de gestión de incidentes, cambios y cumplimiento.
- Área de TI: administra las herramientas de monitoreo y logging, implementa los controles técnicos, conserva los registros y garantiza su integridad y confidencialidad.

- Responsables de Área: verifican que los sistemas bajo su gestión mantengan habilitados los registros requeridos y reportan hallazgos o anomalías.
- Auditores internos o externos: ejecutan revisiones planificadas bajo la coordinación del Comité de Seguridad, respetando los principios de independencia, confidencialidad y trazabilidad.

Las responsabilidades específicas se documentan en la Matriz RACI del SGSI, constituyendo evidencia formal de auditoría.

4 Principios de auditoría y registro

Interfase ISA adopta los siguientes principios para la gestión de registros y auditorías:

- Trazabilidad: todo acceso, modificación o eliminación de información deberá quedar registrado de forma verificable.
- Integridad: los registros deberán estar protegidos contra alteración o eliminación no autorizada.
- Confidencialidad: los logs y reportes de auditoría se considerarán información sensible y su acceso estará restringido.
- Disponibilidad: los registros deberán conservarse durante los períodos definidos por el SGSI y las normas aplicables.
- Transparencia y legalidad: toda auditoría deberá realizarse conforme a la legislación vigente y a los contratos con clientes o proveedores.
- Segregación de funciones: quienes auditan no podrán modificar los registros objeto de revisión.
- Evidencia verificable: los registros y resultados de auditoría deberán conservarse como evidencia trazable y verificable.
- Revisión periódica: los registros deberán ser revisados con una frecuencia definida según la criticidad del sistema (diaria, semanal o mensual), conforme a los procedimientos operativos del SGSI.

- Correlación y monitoreo centralizado: los eventos críticos deberán integrarse en herramientas de monitoreo centralizado (por ejemplo, SIEM o equivalentes), que permitan detectar patrones anómalos o incidentes de seguridad.
- Retención mínima: los registros de sistemas críticos deberán conservarse al menos durante 12 meses, salvo requerimientos legales o contractuales más exigentes.

5 Gestión y conservación de eventos (logs)

- Todos los registros deberán almacenarse en repositorios seguros, protegidos contra modificación o eliminación no autorizada. Dichos repositorios deberán contar con controles de acceso restringidos, cifrado en tránsito y reposo, y mecanismos de verificación de integridad (hash o firma digital).
- El Área de TI será responsable de mantener la matriz de retención de logs, indicando por tipo de sistema el período de conservación, ubicación y responsable técnico.
- Los sistemas y servicios críticos deberán mantener habilitados mecanismos automáticos de registro y almacenamiento seguro de logs, con marcas de tiempo sincronizadas.
- Los registros deberán contener como mínimo: usuario, evento, fecha/hora, origen, acción y resultado.
- Los logs se conservarán conforme a los tiempos de retención definidos en los procedimientos del SGSI, o según requisitos legales o contractuales específicos.
- Los registros se almacenarán en repositorios protegidos, con acceso limitado a personal autorizado y cifrado en tránsito y reposo.
- Toda eliminación o purga de registros deberá ser aprobada por el Comité de Seguridad y quedar documentada.
- Los respaldos de logs deberán almacenarse en ubicaciones separadas del entorno operativo y sujetas a las mismas políticas de seguridad y confidencialidad.
- Cualquier eliminación de registros por expiración del período de retención deberá ser documentada y aprobada por el Comité de Seguridad, dejando evidencia en el SGSI.

6 Monitoreo y revisión de eventos

- El Área de TI, bajo supervisión del Comité de Seguridad, deberá revisar periódicamente los registros de auditoría para identificar anomalías, intentos de acceso indebido, errores recurrentes o comportamientos inusuales. La frecuencia de revisión dependerá de la criticidad del sistema, conforme a la Matriz de Revisión de Logs definida en el SGSI.
- Los eventos críticos o sospechosos deberán ser gestionados según el Procedimiento de Gestión de Incidentes de Seguridad.
- Los resultados de auditorías internas y revisiones de registros se consolidarán en reportes formales presentados al Directorio.
- El Comité de Seguridad podrá establecer controles adicionales de monitoreo proactivo, en función de los niveles de riesgo y criticidad de los activos.
- Los resultados de las revisiones deberán documentarse en el Registro de Monitoreo de Logs y Auditorías, indicando fecha, sistemas revisados, hallazgos y acciones correctivas. En caso de detectar incidentes o irregularidades, se activará el Procedimiento de Gestión de Incidentes de Seguridad, asegurando la trazabilidad desde la detección hasta el cierre.

7 Indicadores y revisión de eficacia

El Comité de Seguridad y el PM del SGSI medirán la eficacia de esta política a través de los siguientes indicadores:

- Porcentaje de sistemas con logging habilitado y auditado.
- Tiempo medio entre detección y análisis de incidentes.
- Número de revisiones de logs realizadas vs planificadas.
- Porcentaje de registros con integridad verificada.

Los resultados se incluirán en el Informe Anual de Cumplimiento del SGSI y se presentarán durante la Revisión por la Dirección, como parte del ciclo de mejora continua.

8 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio para todas las áreas, colaboradores y proveedores que administren o utilicen sistemas de información bajo el SGSI.

El Comité de Seguridad, junto con el Área de TI y el PM del SGSI, supervisará la aplicación de esta política y consolidará los resultados en un informe anual de cumplimiento presentado al Directorio durante la Revisión por la Dirección.

Las desviaciones o hallazgos deberán gestionarse mediante acciones correctivas o preventivas, garantizando la mejora continua del SGSI y la confiabilidad de los registros.

9 Vigencia y Publicación

Esta política es de aplicación obligatoria a partir de su aprobación por el Directorio de Interfase ISA.

La versión vigente será comunicada mediante los canales institucionales y publicada en la intranet corporativa, dentro del repositorio del SGSI.

El Comité de Seguridad garantizará su difusión, revisión anual y control de versiones, o antes si se producen cambios tecnológicos o normativos significativos.

Toda modificación deberá contar con la aprobación formal del Directorio antes de su aplicación, asegurando su adecuada comunicación y registro bajo control documental.

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