Política de Seguridad en Redes y Comunicaciones

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

Control de versiones 2
1 Objetivo 4
2 Alcance 4
3 Roles y responsabilidades 4
4 Principios de seguridad en redes y comunicaciones 5
5 Gestión y protección de la red 5
6 Protección de claves y materiales criptográficos 6
7 Monitoreo, resiliencia y continuidad 7
8 Indicadores y revisión de eficacia 7
9 Cumplimiento y mejora continua 8
10 Vigencia y Publicación 8

1 Objetivo

Establecer los lineamientos que garanticen la seguridad, integridad y disponibilidad de las redes y comunicaciones de Interfase ISA, asegurando la protección de la información que se transmite, procesa o almacena a través de ellas.

Esta política establece los principios para la protección, monitoreo y gestión segura de las redes y comunicaciones de Interfase ISA, abarcando infraestructuras físicas, inalámbricas, virtuales y en la nube.

Se alinea con los controles A.8.20 a A.8.23 de la norma ISO/IEC 27001:2022 y forma parte integral del SGSI, asegurando un enfoque basado en riesgos, resiliencia operativa y mejora continua.

2 Alcance

Esta política aplica a todas las sedes, sistemas y servicios de comunicación de Interfase ISA, así como a colaboradores, contratistas y proveedores que administren, utilicen o mantengan redes, infraestructuras o servicios de conectividad bajo control o gestión de la organización.

Incluye las redes internas, inalámbricas, perimetrales, enlaces externos, VPN corporativas y servicios en la nube utilizados para la transmisión de información institucional.

3 Roles y responsabilidades

La gestión segura de las redes y comunicaciones es una responsabilidad compartida, bajo la supervisión del Comité de Seguridad y el liderazgo del Directorio.

- Directorio: aprueba esta política y supervisa su cumplimiento durante la Revisión por la Dirección.
- Comité de Seguridad: controla la aplicación de los lineamientos, analiza resultados de auditorías y aprueba medidas de mejora.
- Área de Tecnología de la Información (TI): implementa y mantiene los controles técnicos de red, incluyendo configuración segura, monitoreo y control de accesos.
- PM del SGSI: asegura la coherencia de esta política dentro del SGSI, coordina auditorías y seguimiento de acciones correctivas.

- Responsables de Área: garantizan el uso seguro de los servicios de red por su personal y notifican incidentes.
- Proveedores y terceros: cumplen los requisitos de seguridad contractual definidos por Interfase ISA.

Las funciones específicas y la segregación de responsabilidades se detallan en la Matriz RACI del SGSI, que constituye evidencia formal de auditoría.

4 Principios de seguridad en redes y comunicaciones

Interfase ISA adopta los siguientes principios rectores para garantizar la seguridad de sus redes y comunicaciones:

- Evaluación de riesgos: todas las redes y servicios de comunicación deberán ser evaluados periódicamente en función de su criticidad y exposición a amenazas.
- Segregación y control: las redes internas, externas y de invitados deberán mantenerse segmentadas, con controles de acceso definidos y monitoreados.
- Disponibilidad y resiliencia: los servicios de red deberán diseñarse para soportar fallos o incidentes, garantizando la continuidad operativa y la recuperación ante desastres.
- Protección en tránsito: toda información sensible transmitida por redes deberá cifrarse utilizando protocolos y algoritmos aprobados por el Comité de Seguridad.
- Responsabilidad y trazabilidad: toda actividad relevante deberá quedar registrada mediante mecanismos de auditoría y logging controlados por el SGSI.
- Cumplimiento normativo: las configuraciones y servicios de red deberán cumplir con las políticas de seguridad internas, requisitos legales y contractuales aplicables.

5 Gestión y protección de la red

El Área de TI mantendrá un Inventario y Diagrama de Red actualizado, incluyendo todos los dispositivos, enlaces, zonas de seguridad y servicios críticos. Dicho inventario estará bajo control de versiones y se revisará al menos una vez al año o cuando ocurran cambios significativos en la infraestructura.

Interfase ISA garantizará la gestión segura de sus redes mediante la aplicación de controles técnicos y organizativos que contemplen:

- Configuración segura de los equipos de red y documentación de sus parámetros bajo control de versiones.
- Autenticación individual y registro de actividad para todo acceso a dispositivos o servicios de red.
- Segmentación y control de acceso lógico, limitando privilegios según funciones y criticidad.
- Actualización periódica de firmware y parches de seguridad, siguiendo los procedimientos de mantenimiento establecidos.
- Monitoreo continuo del tráfico de red, detección de anomalías y registro de eventos relevantes.
- Protección perimetral y de red interna mediante firewalls, IDS/IPS y mecanismos equivalentes.
- Gestión de cambios documentada, garantizando que las modificaciones sean evaluadas, aprobadas y registradas.
- Las actividades técnicas de configuración, control y monitoreo se documentan en el Procedimiento de Seguridad en Redes y Comunicaciones, parte integrante del SGSI.
- La configuración de red deberá someterse a pruebas de seguridad periódicas (por ejemplo, escaneos de vulnerabilidades, revisiones de firewall y pruebas de penetración) cuyos resultados se documentarán y analizarán en el Comité de Seguridad.
- Los mecanismos de monitoreo (IDS/IPS, SIEM, firewalls, etc.) deberán generar alertas automáticas ante eventos inusuales, manteniendo registros por el tiempo definido en el Procedimiento de Gestión de Logs y Auditoría.

6 Protección de claves y materiales criptográficos

- Las claves criptográficas deberán generarse, almacenarse, distribuirse y eliminarse conforme a procedimientos documentados que aseguren su integridad y confidencialidad.

- Las claves maestras y certificados digitales deberán mantenerse en repositorios seguros, accesibles únicamente al personal autorizado.
- Las copias de respaldo de claves deberán estar cifradas y protegidas mediante controles de acceso.
- La revocación o expiración de certificados deberá gestionarse antes de su vencimiento para evitar interrupciones o vulnerabilidades.
- El Comité de Seguridad deberá mantener un registro actualizado de claves y certificados corporativos como parte del inventario de activos del SGSI.
- Los dispositivos de red que utilicen certificados digitales o claves criptográficas (por ejemplo, VPN, routers, firewalls o servicios SSL/TLS) deberán registrarse en el Inventario de Certificados y Claves del SGSI, asegurando su renovación antes del vencimiento.
- Toda eliminación o sustitución de certificados deberá documentarse y ser aprobada por el Comité de Seguridad.

7 Monitoreo, resiliencia y continuidad

El Área de TI deberá mantener mecanismos de supervisión continua sobre la disponibilidad y rendimiento de la red, con alertas automáticas ante fallas o anomalías.

Los servicios críticos de red deberán estar respaldados por configuraciones redundantes y enlaces alternos, de modo que se garantice la continuidad del servicio ante interrupciones.

Los resultados de las pruebas de contingencia o restauración deberán documentarse y formar parte del Plan de Continuidad de Negocio y Recuperación Tecnológica.

8 Indicadores y revisión de eficacia

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

- Porcentaje de dispositivos de red auditados en el año.
- Número de vulnerabilidades críticas detectadas y corregidas.
- Porcentaje de disponibilidad de los enlaces críticos.

- Tiempo promedio de resolución de incidentes de red.

Los resultados se presentarán en la Revisión por la Dirección y se utilizarán como insumo para el plan anual de mejora continua del SGSI.

9 Cumplimiento y mejora continua

El cumplimiento de esta política es obligatorio para todas las personas y áreas que utilicen o administren redes corporativas.

El Comité de Seguridad, junto con el Área de TI y el PM del SGSI, revisará periódicamente la eficacia de los controles, consolidará los resultados de auditorías y presentará un informe anual de cumplimiento al Directorio durante la Revisión por la Dirección.

Las desviaciones o hallazgos deberán gestionarse mediante acciones correctivas o preventivas, asegurando la mejora continua del SGSI y la infraestructura de red.

10 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.

Esta política deberá revisarse al menos una vez al año o cuando se produzcan cambios significativos en la infraestructura tecnológica, la arquitectura de red o las amenazas detectadas.

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

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