					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P21					Título del documento: **Política de Seguridad de Redes**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	N/A
ISO/IEC 27002:2022	Controles 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
RGPD de la UE	Artículo 32	N/A
Directiva NIS2 de la UE	Artículo 21(2)(d)	N/A
DORA de la UE	Artículo 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Propósito

1.1 El propósito de esta política es definir los requisitos de la organización para proteger sus redes internas y externas frente al acceso no autorizado, la interrupción del servicio, la interceptación de datos y el uso indebido.

1.2 Garantiza que toda la infraestructura de red, incluidas las infraestructuras físicas, virtuales, en la nube e híbridas, esté protegida mediante un modelo de defensa en profundidad con controles como la segmentación, la aplicación de reglas de cortafuegos, el enrutamiento seguro y la monitorización centralizada de sistemas.

1.3 Esta política aplica la cláusula 8.1 de ISO/IEC 27001 y los controles 8.20 a 8.22 del anexo A, garantizando el cumplimiento de las obligaciones regulatorias aplicables conforme al artículo 32 del RGPD de la UE, al artículo 21 de la Directiva NIS2 de la UE y al artículo 9 de DORA de la UE.

2. Alcance

2.1 Esta política se aplica a todas las redes y componentes de infraestructura asociados, incluidos:

2.1.1 Routers, switches, puntos de acceso inalámbrico y cortafuegos

2.1.2 Redes virtuales en la nube (p. ej., AWS VPC, Azure VNet), concentradores VPN y sistemas SD-WAN

2.1.3 Redes de área local internas, zonas desmilitarizadas (DMZ), vías de acceso remoto (VPN, gestión de dispositivos móviles) y conexiones entre sedes o con terceros

2.1.4 Sistemas de soporte como DNS, DHCP, servidores proxy y dispositivos de monitorización

2.2 La política es de obligado cumplimiento para todo el personal y los proveedores de servicios externos que gestionen, configuren, supervisen o se interconecten con las redes de la organización, ya sea en las instalaciones o en la nube.

2.3 Todos los sistemas y aplicaciones conectados a las redes de la organización, con independencia de su ubicación o titularidad, deben cumplir estos requisitos de seguridad de red.

3. Objetivos

3.1 Garantizar la confidencialidad, integridad y disponibilidad de los datos transmitidos a través de las redes mediante controles de acceso robustos, enrutamiento seguro y monitorización.

3.2 Prevenir el acceso no autorizado, el movimiento lateral y la explotación de recursos conectados en red mediante la aplicación de segmentación, zonificación y protección perimetral.

3.3 Mantener configuraciones de red coherentes basadas en estándares del sector e inteligencia de amenazas para defenderse frente a ciberamenazas en evolución.

3.4 Proteger las comunicaciones externas, la interconectividad en la nube y el acceso remoto mediante canales cifrados, autenticación multifactor y validación de endpoints.

3.5 Proporcionar visibilidad de la actividad de red mediante registro de eventos centralizado, inspección del tráfico en tiempo real y generación automatizada de alertas.

3.6 Garantizar el cumplimiento normativo alineando todas las operaciones de red con los requisitos de ISO/IEC 27001:2022, RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE y COBIT 2019.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de esta política y garantiza su revisión y alineación con la estrategia general de ciberseguridad de la organización.

4.1.2 Aprueba los modelos de segmentación de red, los conjuntos de reglas de cortafuegos para sistemas sensibles y las solicitudes de excepción.

4.2 Responsable de Seguridad de Redes / Responsable de Seguridad de Infraestructura

4.2.1 Gestiona la arquitectura de defensa de red, incluidos cortafuegos, sistemas de detección y prevención de intrusiones (IDS/IPS), VPN y enrutamiento seguro.

4.2.2 Supervisa la segmentación de red, las asignaciones de redes de área local virtuales (VLAN), la zonificación del tráfico y la conectividad externa.

4.2.3 Garantiza la revisión continua del filtrado de tráfico entrante y saliente y la aplicación del modelo de confianza cero en todos los niveles de red.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política será revisada anualmente por el Responsable de Seguridad de Redes en colaboración con el Director de Seguridad de la Información y se actualizará en función de:

9.1.1 Amenazas emergentes (p. ej., nuevas técnicas de ataque, vulnerabilidades de protocolos)

9.1.2 Cambios en la infraestructura (p. ej., migraciones a la nube, despliegues de SD-WAN)

9.1.3 Actualizaciones normativas o de estándares que afecten a las protecciones de red

9.1.4 Hallazgos de auditoría, tendencias de incidentes o degradación del rendimiento causada por los controles

9.2 Las revisiones también deben activarse por:

9.2.1 Cambios significativos en la arquitectura de red

9.2.2 Implantación de nuevas plataformas de cortafuegos, VPN o redes en la nube

9.2.3 Retirada de activos clave o de zonas de confianza

9.3 Las actualizaciones deben registrarse en el Registro de Control Documental del SGSI y comunicarse a:

9.3.1 Infraestructura y Operaciones de Red

9.3.2 Equipos del SOC e ingeniería de seguridad

9.3.3 Equipos de aplicaciones con dependencias del sistema respecto de los flujos de red

9.3.4 Todos los proveedores externos con interconectividad activa

9.4 Todas las versiones anteriores de la política deben archivarse de forma segura con anotaciones del historial de cambios para preservar la auditabilidad y la trazabilidad de los cambios.

10. Políticas relacionadas y vinculaciones

10.1 P1 - Política de Seguridad de la Información. Establece los principios fundamentales de seguridad y exige protecciones en capas, incluidos controles de acceso y de amenazas basados en red.

10.2 P4 - Política de Control de Acceso. Garantiza que la segmentación de red se aplique de forma alineada con las funciones de los usuarios, los principios de mínimo privilegio y las reglas de aprovisionamiento de accesos.

10.3 P5 - Política de Gestión de Cambios. Regula las modificaciones de cortafuegos, los ajustes de reglas de VPN y los cambios de enrutamiento mediante un proceso documentado y auditable.

10.4 P12 - Política de Gestión de Activos. Da soporte a la identificación y clasificación de sistemas conectados en red y garantiza que todos los activos conectados se gestionen dentro de los alcances definidos por la política.

10.5 P22 - Política de Registro de Eventos y Monitorización. Rige la recopilación, correlación y conservación de registros de red, incluidos eventos de cortafuegos, intentos de acceso y detecciones de anomalías.

10.6 P30 - Política de Respuesta a Incidentes. Define los procedimientos de escalado, contención y erradicación en respuesta a amenazas o intrusiones propagadas por la red, como DDoS, movimiento lateral o acceso no autorizado.

11. Normas y marcos de referencia

11.1 Esta política se alinea con normas internacionales y mandatos regulatorios que definen operaciones de red seguras, segmentación, protección perimetral y acceso remoto seguro.

11.2 ISO/IEC 27001

11.2.1 Cláusula 8.1 - Planificación y control operacional: requiere que los controles técnicos, incluidas las salvaguardas de red, se integren en los procesos operativos.

11.3 ISO/IEC 27002:2022

11.3.1 Controles 8.20-8.22. Proporciona orientación sobre la protección de redes, la segmentación de servicios y la seguridad de los servicios de red mediante controles de acceso y monitorización.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Protección perimetral: requiere controles perimetrales, segmentación e interconexiones seguras.

11.4.2 AC-4 - Aplicación del flujo de información: respalda la zonificación y las restricciones de tráfico basadas en reglas.

11.4.3 SC-32 - Partición de sistemas de información: promueve la separación lógica de los sistemas de información.

11.5 RGPD de la UE (2016/679)

11.5.1 Artículo 32 - Seguridad del tratamiento: exige medidas técnicas, como cortafuegos y segmentación, para proteger los datos personales.

11.6 Directiva NIS2 de la UE (2022/2555)

11.6.1 Artículo 21(2)(d): exige seguridad eficaz de las redes y sistemas de información, protección perimetral, configuración segura y controles de segregación.

11.7 DORA de la UE (2022/2554)

11.7.1 Artículo 9 - Gestión del riesgo de las TIC: obliga a las entidades financieras a proteger las redes e interconexiones frente al acceso no autorizado, la fuga de datos y la interrupción operativa.

11.8 COBIT 2019

11.8.1 DSS01.03 - Supervisar la infraestructura: requiere control proactivo sobre el estado de la red y la conectividad.

11.8.2 DSS05.01 - Proteger contra el código malicioso: incluye segmentación y control perimetral para minimizar la propagación.

11.8.3 MEA03 - Supervisar, evaluar y valorar el cumplimiento: refuerza la aplicación de la política de red y las evaluaciones de cumplimiento.