					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P21S					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	-
ISO/IEC 27002:2022	control 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
RGPD de la UE	artículo 32	-
Directiva NIS2 de la UE	artículos 21(2)(d), (e)	-
DORA de la UE	artículos 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Propósito

1.1. El propósito de esta política es garantizar que todas las comunicaciones de red internas y externas estén protegidas frente al acceso no autorizado, la manipulación, la interceptación o el uso indebido mediante controles de seguridad claramente definidos.

1.2. Establece reglas para el diseño, uso y gestión seguros de la infraestructura de red, incluidos routers, puntos de acceso inalámbrico, conexiones de acceso remoto y redes segmentadas.

1.3. Tiene por objeto minimizar la exposición a amenazas basadas en Internet, garantizar la confidencialidad de los datos transmitidos a través de redes internas y externas, y mantener la disponibilidad de los servicios críticos.

1.4. Esta política respalda la certificación ISO/IEC 27001:2022 y contribuye directamente al cumplimiento de las obligaciones legales y reglamentarias en virtud del RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE, al tiempo que proporciona garantías técnicas a clientes y auditores.

2. Alcance

2.1. Esta política se aplica a todos los componentes de la red de TI de la organización, incluidos:

2.1.1. Infraestructura cableada e inalámbrica en las ubicaciones de oficina

2.1.2. Routers, switches, puntos de acceso, cortafuegos y pasarelas

2.1.3. Conexiones de acceso remoto (VPN, gestión de dispositivos móviles), incluidas VPN, RDP y túneles en la nube

2.1.4. Aplicaciones en la nube a las que se accede desde redes internas o externas

2.1.5. Dispositivos conectados a la red por empleados, contratistas o invitados

2.2. Esta política regula tanto los segmentos de red físicos como lógicos, incluidas las zonas de invitados, los dispositivos del Internet de las Cosas (IoT) y los sistemas de back-office.

2.3. La política se aplica a todo el personal con acceso a la red de la organización, incluidos:

2.3.1. Empleados internos

2.3.2. Trabajadores remotos y personal híbrido

2.3.3. Proveedores externos, consultores y prestadores de servicios

2.3.4. Invitados que utilicen acceso Wi-Fi temporal

3. Objetivos

3.1. Garantizar que la red de la organización esté protegida frente al acceso no autorizado y las amenazas cibernéticas externas

3.2. Aplicar una segmentación adecuada entre redes de confianza y no confiables (por ejemplo, Wi-Fi de invitados, acceso de proveedores)

3.3. Permitir una conectividad remota segura sin comprometer los sistemas internos

3.4. Prevenir la propagación de software malicioso y la exfiltración de datos a través de canales de red

3.5. Proporcionar supervisión, alertas y trazabilidad de auditoría de la actividad de red para respaldar la detección de incidentes y el cumplimiento

3.6. Garantizar que solo los dispositivos aprobados y protegidos puedan conectarse a las redes internas

3.7. Cumplir las obligaciones establecidas por ISO 27001, el RGPD de la UE y los marcos de ciberseguridad relacionados

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Es responsable de esta política y garantiza la asignación de recursos adecuados para el diseño y la gestión seguros de la red

4.1.2. Revisa las excepciones a los controles de seguridad de red y aprueba los acuerdos de acceso a la red de proveedores

4.1.3. Revisa los incidentes o hallazgos de auditoría relacionados con debilidades de seguridad de la red

4.2. Proveedor de soporte de TI / función interna de TI

4.2.1. Implementa, configura y mantiene todos los cortafuegos, routers, switches y controladores inalámbricos

4.2.2. Gestiona la segmentación entre redes internas, de invitados y externas

4.2.3. Supervisa los registros y alertas para detectar intentos de acceso no autorizado o anomalías de red

4.2.4. Garantiza que las actualizaciones de firmware y configuración se apliquen de forma segura y oportuna

[... 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. Revisión anual

9.1.1. Esta política debe revisarse al menos una vez al año por el Director General junto con el proveedor de soporte de TI y el Coordinador de Privacidad.

9.2. Desencadenantes de revisión intermedia

9.2.1. La revisión de la política también debe activarse por:

9.2.1.1. Cambios importantes en la arquitectura de red (por ejemplo, nuevos sistemas VPN o cortafuegos)

9.2.1.2. Un incidente relacionado con la red (por ejemplo, intrusión, propagación de ransomware o exfiltración de datos)

9.2.1.3. Actualizaciones legales, reglamentarias o de marcos que afecten a la protección de red

9.2.1.4. Nuevas plataformas de proveedores que requieran métodos o protocolos de acceso alternativos

9.3. Gestión de versiones y documentación

9.3.1. Las revisiones de la política deben registrarse con número de versión, fecha y resumen de cambios

9.3.2. Las versiones anteriores deben archivarse durante no menos de 3 años

9.3.3. Las actualizaciones deben comunicarse a los empleados afectados, con acuse de recibo de la política cuando se introduzcan cambios significativos de comportamiento

10. Políticas relacionadas y vinculaciones

10.1. Esta política debe implementarse junto con las siguientes políticas de seguridad para pymes:

10.1.1. P9S – Política de Trabajo Remoto: aplica métodos seguros de acceso remoto, requisitos de VPN y protección de endpoints para usuarios que trabajan fuera de las instalaciones.

10.1.2. P12S – Política de Gestión de Activos: garantiza que todos los sistemas conectados a la red estén identificados, categorizados y sujetos a seguimiento con estados de seguridad actualizados.

10.1.3. P17S – Política de Protección de Datos y Privacidad: garantiza que la segmentación de red, los controles de acceso y el registro de eventos respalden los principios de privacidad y protección de datos conforme al RGPD de la UE.

10.1.4. P22S – Política de Registro de Eventos y Supervisión: especifica los requisitos para capturar y revisar registros de dispositivos de red, conexiones remotas y controladores inalámbricos.

10.1.5. P30S – Política de Respuesta a Incidentes: define las acciones requeridas en respuesta a brechas de red, intentos de acceso no autorizado o propagación de software malicioso a través de redes internas.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 8.1 – Requiere la implementación de controles para garantizar operaciones seguras y resilientes, incluidas las redes.

11.2. ISO/IEC 27002

11.2.1. Control 8.20 – Proporciona directrices técnicas y procedimentales para proteger el acceso a la red, la segmentación y la supervisión.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Exige el control del flujo de información dentro de las redes y entre sistemas.

11.3.2. SC-7 – Requiere protección perimetral, enrutamiento seguro y segmentación de red para reducir el riesgo de acceso no autorizado.

11.4. RGPD de la UE

11.4.1. Artículo 32 – Exige medidas técnicas y organizativas apropiadas para garantizar la confidencialidad, integridad y disponibilidad de los sistemas y servicios en red que tratan datos personales.

11.5. Directiva NIS2 de la UE

11.5.1. Artículo 21(2)(d) – Exige medidas técnicas basadas en riesgos, incluidas la seguridad de red y el control de acceso.

11.5.2. Artículo 21(2)(e) – Requiere segmentación y aislamiento de sistemas para impedir la propagación de incidentes cibernéticos.

11.6. DORA de la UE

11.6.1. Artículo 9 – Exige que las entidades implementen controles de gestión del riesgo de las TIC, incluidos los relativos a redes y comunicaciones seguras.

11.6.2. Artículo 10 – Exige que las estrategias de resiliencia digital incluyan la protección de la infraestructura de red y de la conectividad remota.

11.7. COBIT 2019

11.7.1. DSS05.02 – Requiere protección eficaz de la infraestructura de TI y de los entornos de red frente a amenazas internas y externas.

11.7.2. APO13.01 – Requiere estrategias de gestión de riesgos que incluyan segmentación de red y supervisión como parte de la mitigación de amenazas.