

Objetivo:

Proteger la infraestructura de red para garantizar la confidencialidad, integridad y disponibilidad de la información transmitida y prevenir accesos no autorizados o interrupciones en el servicio.

Declaración:

La organización ha implementado políticas, procedimientos y controles técnicos para asegurar la seguridad de las redes, incluyendo la segmentación, monitoreo y protección contra amenazas internas y externas.

Alcance:

Este control aplica a todas las redes, conexiones y dispositivos de comunicación gestionados por la organización.

Directrices:

- Se diseñan y mantienen arquitecturas de red seguras, incluyendo segmentación y zonas de confianza.
- Se implementan controles de acceso a redes, incluyendo firewalls, VPNs y sistemas de detección de intrusos.
- Se monitorean continuamente las redes para detectar actividades sospechosas o anómalas.
- Se aplican políticas para el uso seguro de redes inalámbricas y cableadas.
- Se capacita al personal en buenas prácticas de seguridad de redes.
- Se realizan auditorías y pruebas de penetración periódicas para evaluar la seguridad de la red.

Referencias relacionadas:

- POL 001 — Política de Seguridad de la Información
- PRO 014 — Procedimiento para el Registro y Supervisión de Accesos
- PSC 007 — Monitoreo y Medición
- PSC 009 — Sensibilización y Capacitación

Evidencias de implementación:

- Documentación de arquitectura y políticas de seguridad de red.
- Registros de monitoreo y análisis de tráfico de red.
- Informes de auditoría y pruebas de penetración.
- Registros de capacitación del personal.
- Reportes de incidentes y acciones correctivas relacionadas con la seguridad de la red.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO