

Objetivo:

Implementar la segregación adecuada de redes para limitar el acceso y reducir riesgos de seguridad, asegurando la protección de sistemas y datos críticos.

Declaración:

La organización ha establecido políticas, procedimientos y controles técnicos para segmentar las redes según niveles de sensibilidad, función o riesgo, facilitando el control del tráfico y la protección contra accesos no autorizados.

Alcance:

Este control aplica a todas las redes gestionadas por la organización, incluyendo redes internas, externas y de terceros.

Directrices:

- Se identifican y clasifican las zonas de red según el nivel de seguridad requerido.
- Se implementan mecanismos de segmentación como VLANs, firewalls y zonas desmilitarizadas (DMZ).
- Se controlan estrictamente los accesos entre segmentos y se monitorean las comunicaciones.
- Se documentan las configuraciones y cambios relacionados con la segregación de redes.
- Se realizan pruebas y auditorías para validar la efectividad de la segmentación.
- Se capacita al personal en la gestión y mantenimiento de la segregación de redes.

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 y diagramas de segmentación de redes.
- Registros de configuraciones y cambios de segmentación.
- Informes de auditoría y monitoreo de tráfico entre segmentos.
- Registros de capacitación y sensibilización del personal.
- Reportes de incidentes y acciones correctivas relacionadas con la segregación.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO