

Plan de Seguridad de Red

Infraestructura con pfSense, Active Directory, SQL Server y CUPS

Objetivo

- Aplicar medidas de seguridad para proteger los activos de una red basada en pfSense, Active Directory, SQL Server y CUPS, garantizando la confidencialidad, integridad y disponibilidad.






Identificación de Activos

- - pfSense (192.168.1.1): VPN, DHCP, DNS, firewall
- - Servidor Windows (192.168.1.100): Active Directory, SQL Server
- - Servidor Ubuntu (192.168.1.101): Web, CUPS
- - Clientes VPN
- - Base de datos SQL Server
- - Logs de eventos

Amenazas y Vulnerabilidades

- - VPN sin MFA y firewall permisivo
- - Contraseñas débiles en AD
- - Exposición de servicios en Ubuntu
- - SQL sin cifrado ni backups
- - Falta de centralización de logs

Análisis y Evaluación de Riesgos

- - Acceso VPN no autorizado:  Crítico
- - Ataques a servicios en Ubuntu:  Alto
- - Robo de credenciales AD:  Crítico
- - Pérdida de base de datos:  Crítico
- - Falta de logs:  Alto

Tratamiento y Mitigación

- - Activar MFA y certificados para VPN
- - Hardening de Ubuntu (UFW, actualizaciones)
- - Políticas de contraseñas y logs en AD
- - Backups cifrados y monitoreo SQL
- - Centralización y retención de logs

Plan de Acción y Seguimiento

- - Auditorías mensuales
- - Revisión de reglas de pfSense
- - Pruebas de backups
- - Simulaciones de incidentes
- - Formación a usuarios