Sistemas Informáticos

UD7. Actividad 1

Diseño seguro de una red local corporativa

Pavel Miron

Índice

Introducción

En este trabajo propongo el diseño de una red local para una empresa pequeña de 20 personas. La idea es que la red sea segura, organizada y funcione bien para que todos puedan trabajar sin problemas. La empresa está dividida en varios departamentos: Administración, Recursos Humanos, Ventas, Soporte Técnico y Dirección. Cada uno tiene funciones diferentes y necesita acceso a distintos recursos.

Es muy importante que la red tenga buenas medidas de seguridad, porque cada vez hay más riesgos en internet como virus, robos de datos o accesos no autorizados. Con una buena red, protegemos la información de la empresa y evitamos problemas graves. En este diseño, también se incluyen servidores, contraseñas seguras, y herramientas para controlar lo que pasa en la red.

Desarrollo

1. Diseño de perfiles de usuario y asignación de permisos/derechos.

Dirección: 2 personas
Administración: 4 personas
Recursos Humanos: 3 personas
Ventas: 6 personas
Soporte Técnico: 5 personas

La red estará estructurada con distintos perfiles de usuario que definen los niveles de acceso según el rol de cada trabajador. Esto se gestiona mediante Active Directory (AD), lo que permite centralizar la administración de usuarios y grupos.

- Dirección: Los usuarios de este grupo tienen acceso a informes globales, documentos corporativos sensibles y permisos de lectura sobre los demás departamentos. Sus equipos están protegidos mediante autenticación múltiple (MFA).

- Administración: Acceden a sistemas contables, documentos financieros y bases de datos compartidas con RRHH. Su acceso está limitado a carpetas y aplicaciones del área administrativa.

- Recursos Humanos: Manejan información confidencial como contratos, nóminas y evaluaciones de personal. Solo ellos pueden acceder a esta información, protegida por permisos NTFS y GPOs específicas.

- Ventas: Utilizan un CRM interno, acceden a listados de clientes y generan presupuestos. No tienen acceso a carpetas de otros departamentos.

- Soporte Técnico: Cuentan con privilegios especiales para realizar tareas de mantenimiento, instalación de software y revisión de logs. Están divididos entre soporte de usuarios y administración de red.

La correcta definición de permisos minimiza el riesgo de accesos indebidos, permite auditorías claras y reduce la superficie de ataque de la red.

2. Política de directivas de seguridad.

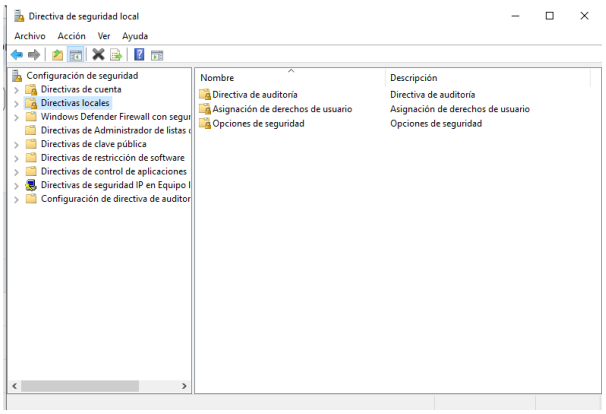
La política de seguridad se configura desde el controlador de dominio mediante GPOs. Las directivas más relevantes incluyen:

- Contraseñas seguras: Deben tener mínimo 10 caracteres, incluir letras mayúsculas, minúsculas, números y símbolos. Las contraseñas expiran cada 90 días y no se pueden repetir las últimas 5 usadas.

- Bloqueo de cuenta: A los 5 intentos fallidos, la cuenta se bloquea durante 30 minutos. Esto evita ataques de fuerza bruta.

- Auditoría de eventos: Se registran accesos exitosos y fallidos, modificaciones de archivos importantes y actividades de administradores. Los logs se almacenan en un servidor Syslog centralizado.

- MFA y acceso remoto: Se aplica MFA para administradores y personal con acceso remoto mediante VPN.

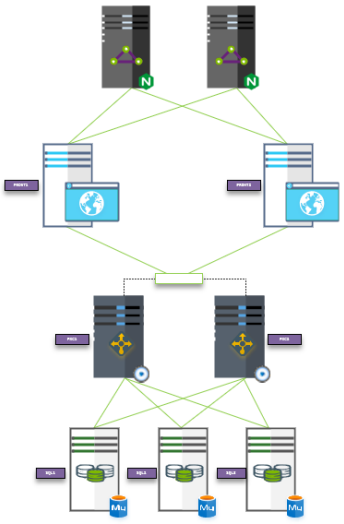


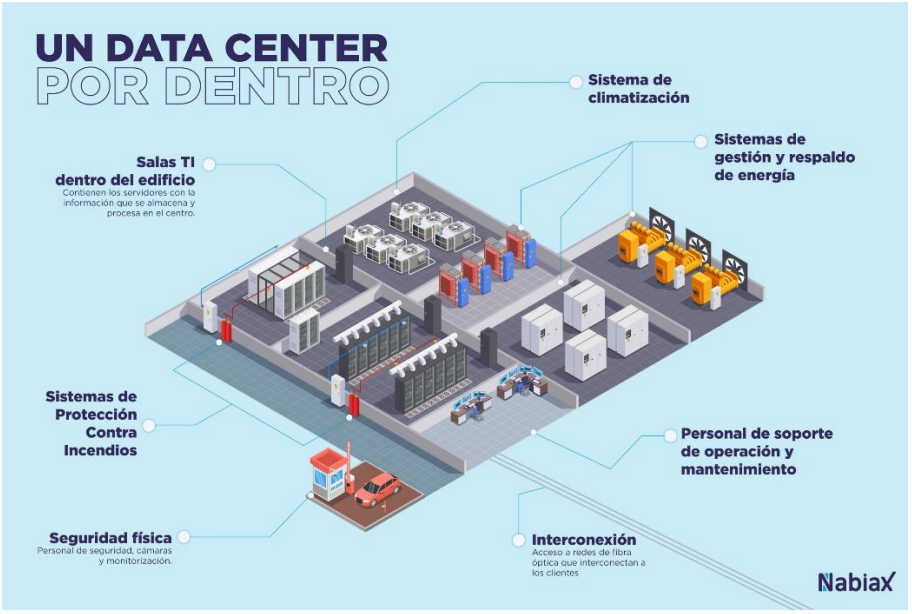
Estas medidas refuerzan la seguridad interna y garantizan trazabilidad sobre cualquier acción realizada dentro de la red.

3. Diseño de la infraestructura de servidores.

La arquitectura del sistema se apoya en una topología cliente-servidor. La empresa contará con los siguientes servidores:

- **Servidor de archivos** (Windows Server/NAS): centraliza todos los documentos corporativos, divididos por departamentos mediante carpetas compartidas y permisos.
- **Controlador de dominio (AD)**: gestiona usuarios, permisos, directivas de grupo y autenticación.
- **Servidor de correo electrónico** (Postfix o Exchange): para la gestión de correos internos y externos con dominio propio.
- **Servidor web corporativo** (Apache/Nginx): alojado en una zona DMZ para acceso externo.
- **Servidor de copias de seguridad** (NAS con RAID): programa backups automáticos diarios de todos los archivos y configuraciones importantes.

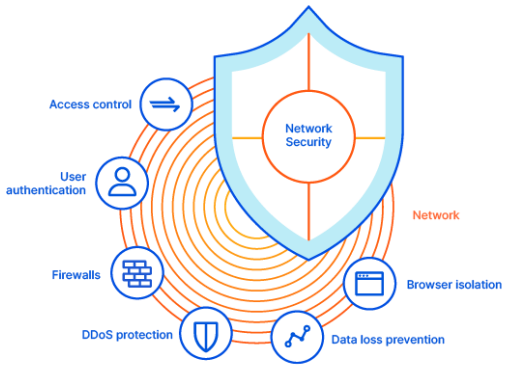




4. Medidas de seguridad en red.

El sistema de seguridad estará compuesto por múltiples capas:

- Firewall perimetral: Inspecciona el tráfico entrante y saliente, bloqueando accesos no autorizados.
- Segmentación por VLANs: Los departamentos estarán separados en diferentes redes virtuales para limitar la propagación de amenazas.
- DMZ (zona desmilitarizada): El servidor web se aloja en una zona aislada para evitar comprometer la red interna si es atacado.
- Cifrado de comunicaciones: Uso de TLS en correo, VPN para accesos remotos y HTTPS en navegación.
- Seguridad física: El acceso a la sala de servidores estará limitado mediante tarjeta o autenticación biométrica.
- Antivirus/EDR corporativo: Software de protección instalado en todos los endpoints, con actualizaciones automáticas y detección proactiva de amenazas.



5. Monitorización y administración.

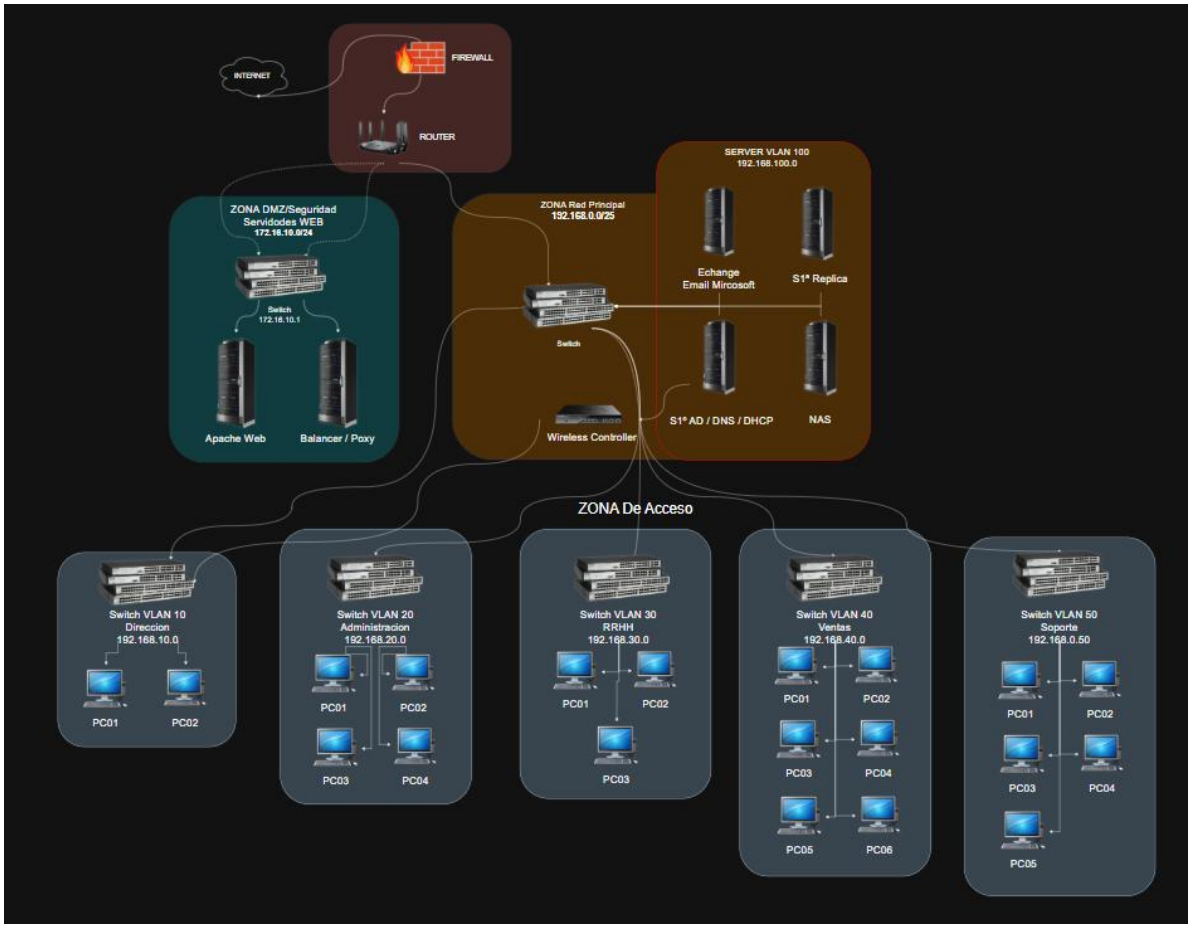
Para asegurar el funcionamiento continuo y detectar posibles incidentes, se usarán herramientas de monitorización y gestión:

- Zabbix/Nagios: Supervisión de servidores, almacenamiento y dispositivos de red. Alertas automáticas por caídas o anormalidades.
- Wireshark: Análisis de tráfico para detectar comportamientos sospechosos.
- GLPI/OCS Inventory: Gestión de tickets, inventario de hardware y software, control de incidencias.
- Syslog/Splunk: Centralización de registros de logs, permitiendo analizar ataques, errores y accesos.

Ante un incidente de seguridad:

- Se aísla el dispositivo afectado.
- Se consultan los logs para identificar el origen.
- Se recuperan datos desde la copia de seguridad.
- Se documenta el incidente y se fortalecen las políticas afectadas.

6. Diseño de red y explicación.



1. Internet: La Carretera Principal

Es como la autopista que conecta tu empresa con el mundo.
El router del ISP (proveedor de internet) es como la salida a esa autopista.

2. Firewall: La Aduana/Policía de Fronteras

Es un muro de seguridad que revisa todo lo que entra y sale.
Firewall Cluster significa que hay dos policías trabajando en equipo (si uno falla, el otro sigue protegiendo).

3. DMZ: Zona de Visitantes

Aquí ponemos servidores que necesitan contacto con Internet (como la web de la empresa).
Balancer/Proxy para gestión y intermediario entre usuario y servidor web u otro servicio en red.
Apache para ajorar y gestionar sitios web en internet.
Está separada de la red interna por seguridad (como un edificio con vigilancia antes de entrar a la oficina).

4. Core Switch: El Gran Intercambiador

Conecta todas las zonas y dirige el tráfico.

5. Servidores Internos: Las Oficinas Importantes

AD (Active Directory): Es como el "director de personal" que controla quién entra y qué permisos tiene.
NAS (Servidor de Archivos): Un archivador gigante donde todos guardan documentos.
Exchange (Correo): La oficina de mensajería interna.
REPLICA (Backup): La caja fuerte con copias de seguridad.

6. VLANs: Barrios de la Ciudad

Cada departamento tiene su zona separada (como calles con nombres distintos):
VLAN 10 (Dirección): Solo para los jefes.
VLAN 20 (Administración): Para contabilidad y recursos.
VLAN 30 (RRHH): Para el personal de contrataciones.
VLAN 40 (Ventas): Para el equipo comercial.
VLAN 50 (Soporte): Para los técnicos.

¿Por qué separarlas?
Para que si hay un problema en Ventas (ej. un virus), no afecte a Dirección.
Cada una tiene su propia "dirección IP" (como un código postal).

7. WiFi y Otros Detalles

Wireless Controller: Es el "jefe de los WiFi" que controla todos los puntos de acceso.
Switches de acceso: Son como "extensiones" del Core Switch para conectar más dispositivos.

Conclusión

Hacer este diseño me ayudó a entender lo que implica tener una red segura en una empresa. No es solo poner computadoras y conectar cables. Hay que pensar en los usuarios, en proteger los datos, en hacer copias de seguridad y estar preparado para cualquier problema. También aprendí que las herramientas de monitoreo son muy importantes para detectar errores o ataques a tiempo.

Bibliografía

https://learn.microsoft.com/es-es/windows-server/storage/folder-redirection/deploy-roaming-user-profiles

https://sistemasyoperativos.com/2023/04/20/directivas-de-seguridad-local-en-windows/

https://www.datacentermarket.es/dcm-xl/arquitectura-e-infraestructura-de-un-data-center-todas-las-claves/

https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/

https://www.ikusi.com/mx/blog/seguridad-de-redes/

https://docs.johnsoncontrols.com/bas/r/Metasys/es-ES/Boletin-tecnico-de-orientaciones-sobre-redes-y-TI/10.1/Consideraciones-sobre-redes-y-TI/Arquitectura-del-sistema-Metasys