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
Para garantizar la protección de las cuentas de usuario, las contraseñas deben cumplir con los siguientes requisitos mínimos:

- Longitud mínima de 10 caracteres.
- Inclusión obligatoria de letras mayúsculas, minúsculas, números y símbolos especiales.
- Caducidad automática cada 90 días, obligando a los usuarios a renovar sus contraseñas periódicamente.
- Restricción para no reutilizar ninguna de las últimas 5 contraseñas anteriores, evitando patrones repetitivos que puedan ser vulnerables.

Esta política fortalece la defensa contra accesos no autorizados mediante técnicas de ingeniería social o ataques automatizados.

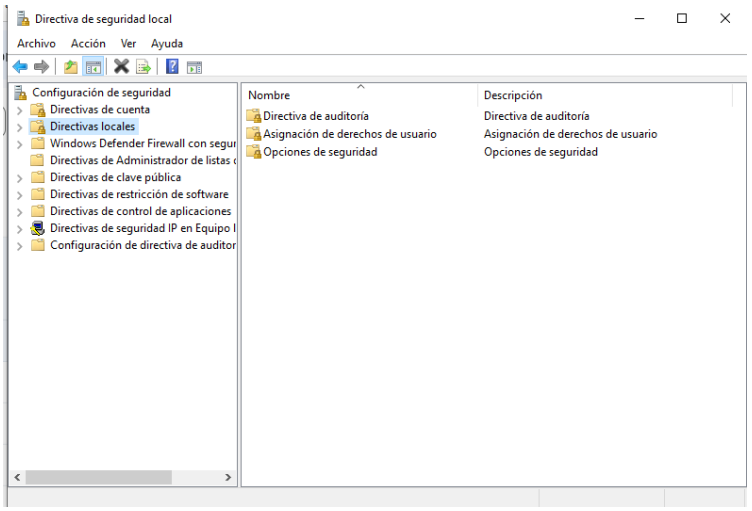
Bloqueo de Cuenta por Intentos Fallidos
Para proteger las cuentas contra ataques de fuerza bruta, se implementa un bloqueo automático de la cuenta tras 5 intentos fallidos consecutivos de inicio de sesión. El bloqueo dura 30 minutos, durante los cuales el usuario no podrá intentar acceder nuevamente. Esta medida limita significativamente el riesgo de acceso no autorizado mediante pruebas masivas de contraseñas.

Auditoría de Eventos y Registro de Logs
Se lleva un registro exhaustivo de eventos de seguridad para facilitar la detección temprana de incidentes y la investigación posterior:

- Accesos exitosos y fallidos a sistemas críticos.

- Modificaciones en archivos importantes o sensibles, incluyendo documentos corporativos y configuraciones de servidores.

- Actividades realizadas por administradores y usuarios con permisos elevados.
  Todos estos eventos se almacenan en un servidor Syslog centralizado, que consolida los registros provenientes de distintos dispositivos y servidores, facilitando su análisis mediante herramientas SIEM o auditorías manuales.



Autenticación Multifactor (MFA) y Acceso Remoto Seguro
Para reforzar la seguridad en accesos con mayores riesgos, se exige la implementación de MFA:

- Administradores de sistemas y personal con privilegios elevados deben autenticarse mediante un segundo factor, como tokens físicos, aplicaciones móviles (OTP) o biometría.

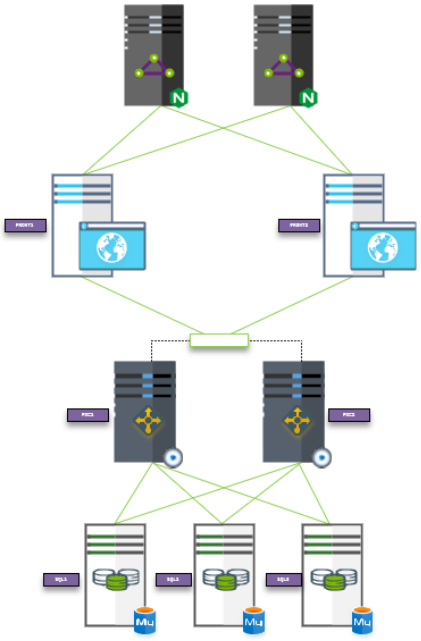
- El acceso remoto a la red corporativa se realiza exclusivamente mediante VPN segura, que además requiere MFA para validar la identidad del usuario.
  Estas medidas aseguran que incluso si una contraseña se ve comprometida, el acceso no autorizado sea impedido por la barrera adicional del segundo factor.

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)
  Este servidor centraliza todos los documentos corporativos, organizados por departamentos a través de carpetas compartidas con permisos específicos para cada grupo.



Esto asegura que solo los usuarios autorizados puedan acceder o modificar la información relevante para su área, facilitando la colaboración y el control de acceso.

- Controlador de Dominio (Active Directory)
  El controlador de dominio gestiona la autenticación de usuarios, permisos y directivas de grupo (GPO), centralizando la administración de cuentas y políticas de seguridad en la red.

Esto permite una gestión eficiente de usuarios, grupos y recursos, garantizando que cada empleado tenga los permisos adecuados según su rol.

- Servidor de Correo Electrónico (Postfix o Exchange)
  Para la comunicación interna y externa, se utiliza un servidor de correo con dominio propio. Postfix es una opción robusta y flexible en entornos Linux, mientras que Exchange ofrece integración profunda con entornos Windows.

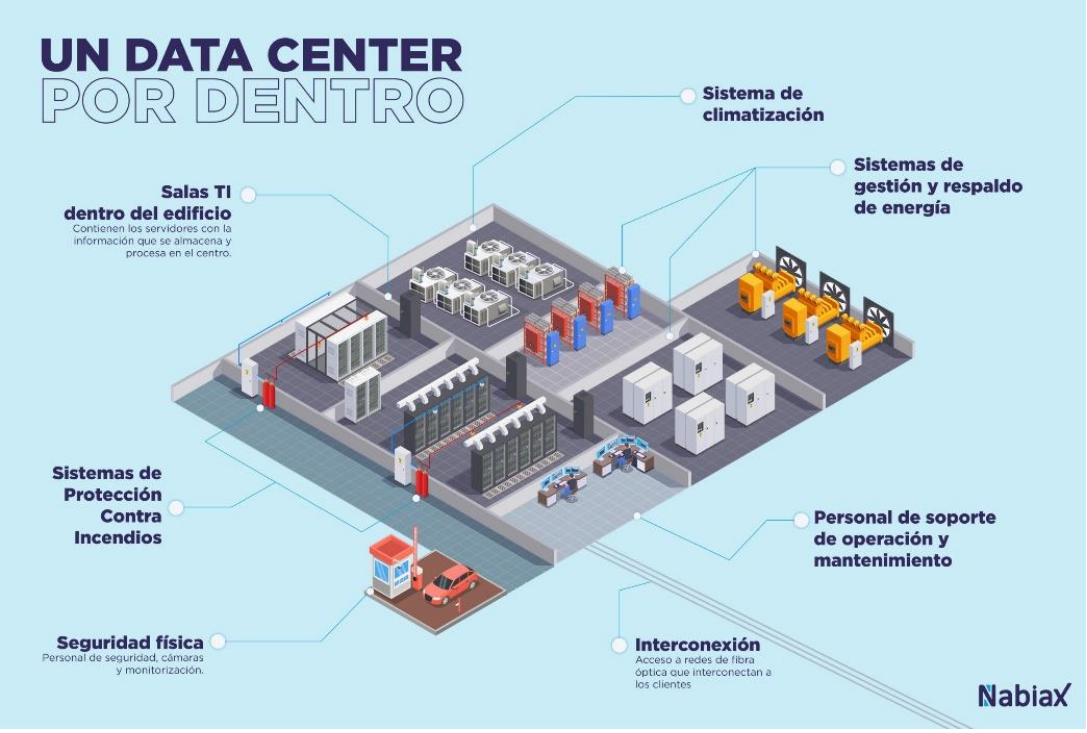
Ambos permiten gestionar buzones, listas de distribución y filtros anti-spam, asegurando un flujo de correo seguro y confiable.

- Servidor Web Corporativo (Apache/Nginx)
  El servidor web está alojado en una zona DMZ para permitir acceso seguro desde el exterior, protegiendo la red interna.

Apache o Nginx se encargan de servir la página web corporativa, aplicaciones web o portales internos, configurados con certificados SSL para cifrado de la comunicación y reglas de firewall específicas para limitar accesos.

- Servidor de Copias de Seguridad (NAS con RAID)
  Un NAS configurado con RAID proporciona almacenamiento redundante y seguro para backups automáticos diarios.

Este sistema realiza copias de seguridad de los archivos corporativos y configuraciones críticas, permitiendo una rápida recuperación en caso de fallos de hardware, errores humanos o ataques informáticos.



4. Medidas de seguridad en red.

El sistema de seguridad estará compuesto por múltiples capas:

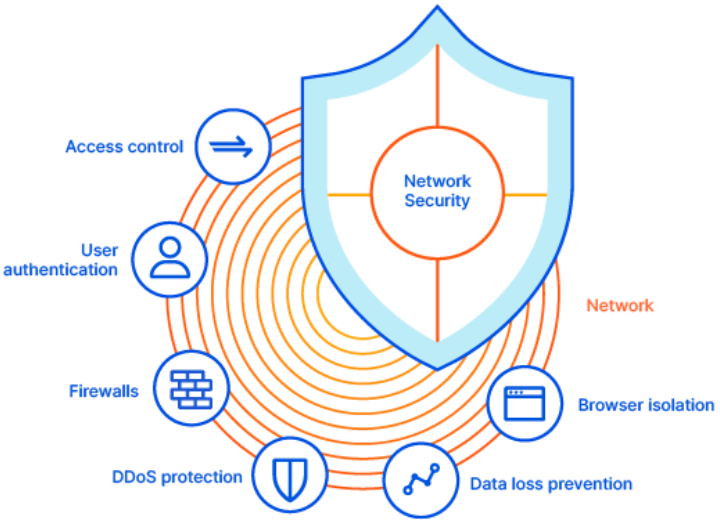
Firewall Perimetral
Este es como una barrera que controla todo el tráfico que entra y sale de la red. Solo permite el paso a las conexiones autorizadas y bloquea cualquier intento sospechoso o no permitido. Así evitamos que personas no autorizadas puedan acceder a nuestra red desde afuera.

Segmentación por VLANs
Vamos a dividir la red en varias redes virtuales separadas según los departamentos (por ejemplo, Finanzas, Ventas, IT). Esto significa que si alguien infecta un equipo en un departamento, no podrá fácilmente afectar a los demás porque cada uno está aislado. Es como tener varias habitaciones con puertas cerradas dentro de la oficina.

DMZ (Zona Desmilitarizada)
El servidor web estará en un área especial y separada de la red interna, llamada DMZ. Esto es para que, si el servidor web sufre un ataque, los hackers no puedan entrar fácilmente a la red principal de la empresa y robar información importante.

Cifrado de Comunicaciones
Todas las comunicaciones importantes estarán protegidas:

- El correo electrónico usará TLS para que los mensajes viajen seguros y nadie pueda espiarlos.
- El acceso remoto será siempre por VPN, que crea un "túnel seguro" para conectarse desde fuera.
- Las páginas web de la empresa funcionarán con HTTPS, lo que garantiza que la información que enviamos o recibimos esté cifrada y protegida.



Seguridad Física
No solo cuidamos la red, también protegemos el lugar donde están los servidores. El acceso a la sala de servidores estará restringido y solo podrá entrar personal autorizado mediante tarjetas especiales o sistemas biométricos como huellas digitales. Esto evita que alguien entre físicamente para manipular o robar equipos.

Antivirus y EDR Corporativo
En todos los computadores y dispositivos de la empresa instalaremos un software antivirus y un sistema de detección y respuesta avanzada (EDR). Este software se actualiza automáticamente y puede identificar amenazas nuevas o desconocidas para proteger los equipos antes de que causen daño.

5. Monitorización y administración.

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

Zabbix / Nagios
Estas herramientas nos ayudan a supervisar todo lo que pasa en los servidores, el almacenamiento y los dispositivos de red (como routers y switches). Nos envían alertas automáticas si algún equipo deja de funcionar o si detectan algo fuera de lo normal. Así podemos reaccionar rápido antes de que un problema grande afecte a la empresa.

Wireshark
Es una herramienta que analiza el tráfico de red. Nos permite "ver" los datos que se mueven por la red para detectar si hay comportamientos extraños o intentos de ataques. Es muy útil para investigar qué está pasando cuando sospechamos que alguien intenta hacer algo raro en la red.

GLPI / OCS Inventory
Con estas herramientas gestionamos el inventario de todos los equipos de la empresa (hardware y software), además de controlar las incidencias o problemas que surjan. También nos ayudan a llevar un seguimiento de los tickets o solicitudes que hacen los usuarios para que nada se quede sin resolver.

Syslog / Splunk
Estas plataformas nos permiten juntar todos los registros de eventos (logs) de los diferentes equipos en un solo lugar. Con eso podemos analizar y entender mejor si hubo ataques, errores o accesos no autorizados. Es fundamental para investigar incidentes y mantener la seguridad.

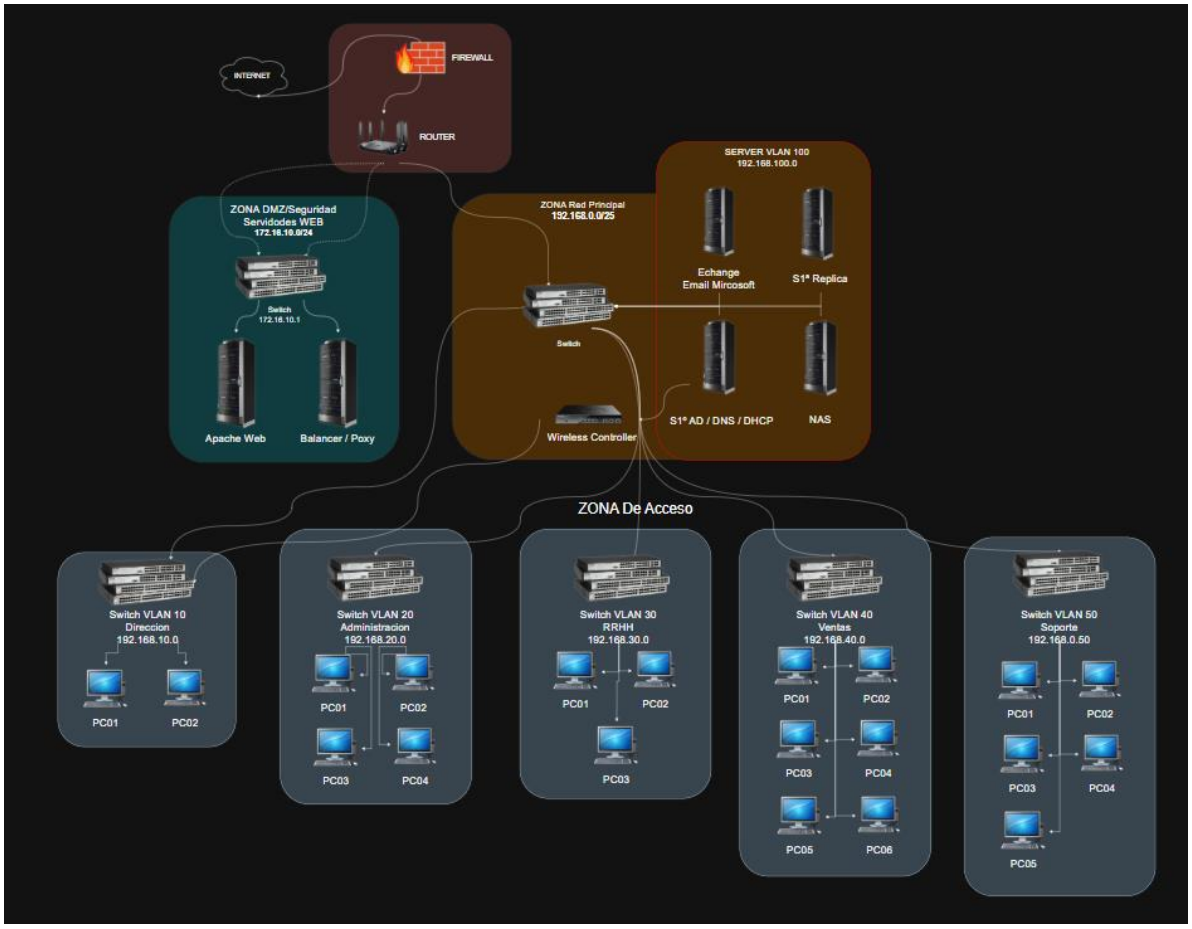
Qué hacer ante un incidente de seguridad?
Si detectamos un problema o un ataque, seguimos estos pasos:

Aislar el dispositivo afectado
Lo primero es desconectar o aislar el equipo que está dando problemas para evitar que la amenaza se propague a otros dispositivos o a la red completa.

Revisar los logs
Consultamos los registros para entender qué pasó, cuándo y cómo comenzó el incidente. Esto nos ayuda a identificar el origen y la naturaleza del problema.
Recuperar datos desde la copia de seguridad
Si el incidente afectó archivos o sistemas importantes, restauramos la información desde las copias de seguridad para minimizar pérdidas y volver a la normalidad lo antes posible.

Documentar el incidente y mejorar las políticas
Finalmente, registramos todo lo ocurrido para aprender del problema. Con esa información fortalecemos las políticas de seguridad o las configuraciones para evitar que algo parecido vuelva a pasar.

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