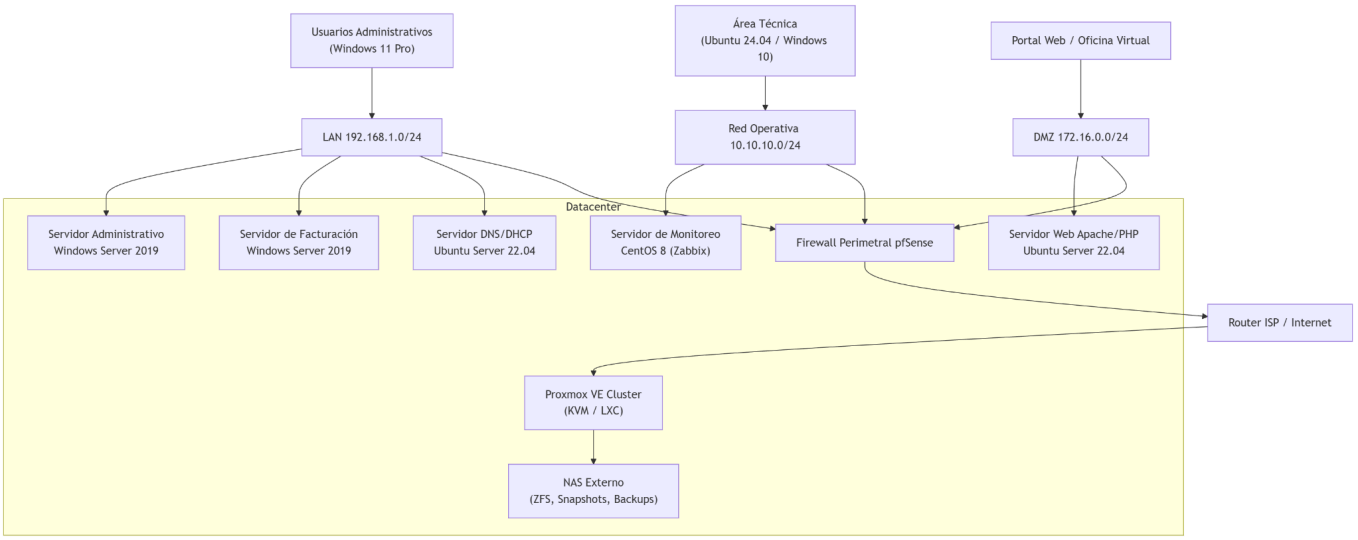
1. Presentacion

Empresa

Cooperativa de Telecomunicaciones (CTMdP) organización ficticia inspirada en el sector ISP/cooperativo local.
Actividad principal: provisión de Internet, telefonía IP y servicios digitales (portal Oficina Virtual, facturación/gestión, soporte técnico).
Requisitos: alta disponibilidad de servicios públicos (DNS, web, VPN), continuidad operativa en administración y soporte, y cumplimiento de buenas prácticas de seguridad.



Topología (LAB con VirtualBox)
El laboratorio corre en un host con **Oracle VirtualBox**. Se despliegan:

- **pfSense 2.7.x** (Firewall perimetral)
    - **LAN**: 10.10.10.0/24 (GW 10.10.10.254)
    - **OPERATIVA** 10.10.20.0/24,
    - **DMZ** 10.10.30.0/24.
- **Windows Server 2022 GUI (DC1.ctmdp.local)**: DNS/AD en 10.10.10.10.
- **OpenVPN Remote Access**: red de túnel 10.10.40.0/24.
- **Cliente Windows** (la propia VM) que se conecta a la VPN.
  El acceso remoto en el LAB se implementa con OpenVPN (TLS),

manteniendo para el diseño corporativo la alternativa IPSec IKEv2 + RADIUS/MFA para producción.

2. Sistemas operativos

a. Determinar el o los sistemas operativos que posee la empresa.

La empresa utiliza distintos sistemas operativos según el servicio:

- pfSense CE 2.7.2 (firewall/IDS/IPS).
- Windows Server 2022 GUI (AD DS/DNS) en 10.10.10.10/24 (LAN).
- Ubuntu Server 22.04 (web de prueba) en 10.10.30.10/24 (DMZ).
- Cliente Windows (la propia host o VM) para probar OpenVPN.

b. Tipo de virtualización que posee

Hipervisor: Oracle VirtualBox en un único host.

pfSense: 2 interfaces (LAN/DMZ).

Windows Server 2022: 1 interfaz en LAN.

Ubuntu Server: 1 interfaz en DMZ.

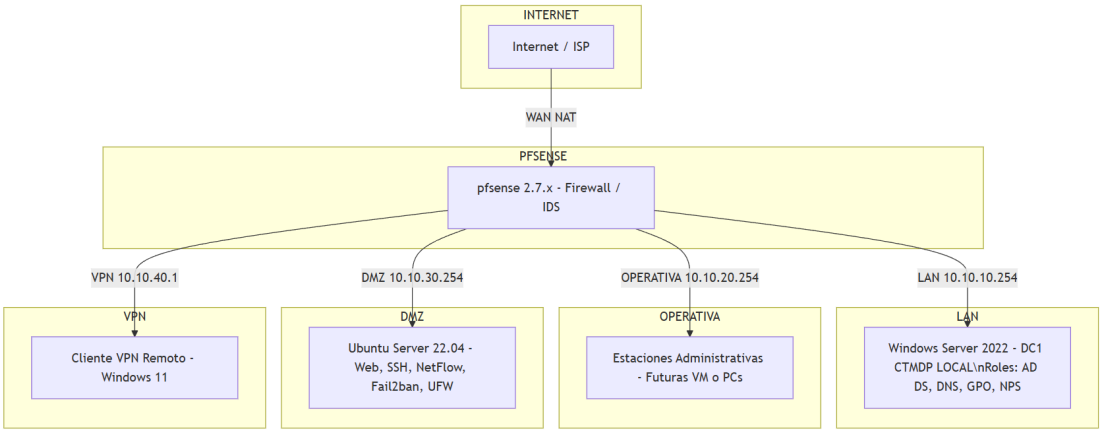
Diseño futuro (no implementado en el LAB): Proxmox VE en clúster, alta disponibilidad, almacenamiento ZFS/Ceph, etc. (Se deja como arquitectura objetivo, no ejecutada en este trabajo práctico.)

c. Virtualización de las aplicaciones, si lo tuviese.

La empresa en un futuro agrega virtualización de aplicaciones para el personal administrativo y para la atención al cliente. Implementándose Microsoft RemoteApp sobre Windows Server para permitir la ejecución de aplicaciones de oficina, gestion y contabilidad sin necesidad de instalarlas localmente.

En Docker se levantan contenedores para aislar servicios de monitoreo de red y distintas pruebas de configuración.

d. Diagrama de los servidores y sus SO.



e. Seguridad implementada en los virtualizadores.

- VMs separadas por redes lógicas (LAN y DMZ).
- Uso de discos dinámicos (crecimiento bajo demanda).
- Snapshots puntuales antes de cambios relevantes.
- Copias de seguridad automáticas de todas las VMs
- Gestión de permisos por roles (solo administradores pueden modificar VMs o redes virtuales).
- Actualizaciones periódicas y parches de seguridad en los hipervisores y sistemas operativos invitados.

3) Sistemas de archivos

a) Sistemas de archivos seleccionados:

- Windows Server 2022: NTFS (por defecto).

- Ubuntu Server: ext4 (por defecto).

b) Seguridad y permisos:

- En Windows, se probó carpeta compartida con permisos NTFS: “Domain Admins” (control total) y “Domain Users” (lectura).

- En Ubuntu (DMZ) se aplicó UFW (firewall local) para limitar servicios y fail2ban para protección de SSH.

- Separación de cuentas: una cuenta personal sin privilegios y una cuenta administrativa separada para tareas de administración.
- Políticas de contraseñas obligatorias y bloqueo por intentos fallidos.
- Permisos en archivos y carpetas por grupos (no por usuarios sueltos).
- Registros de auditoría activados (inicio de sesión, cambios de políticas y de archivos).
- Cortafuegos local activo en todos los equipos.
- En Linux: solo acceso por “clave pública” para acceso remoto y deshabilitar acceso del usuario “root”.
- “Principio de mínimo privilegio” aplicado en servicios (cuentas de servicio sin derechos extra).
- Comparticiones de archivos con permisos NTFS (Windows) y permisos POSIX (Linux), con herencia controlada.

c) Encriptación y compresión:

Windows: cifrado de disco con BitLocker en el servidor y en equipos críticos.

Linux: cifrado en reposo con LUKS (partición o todo el disco).

Compresión:

- Windows: compresión NTFS en carpetas de documentos y backups.
- Linux: compresión de respaldos con tar.gz y compresión automática de logs con logrotate.

4. Autenticación, autorización y control de acceso

a) Mecanismos de seguridad implementados en sistema operativo

En los tres sistemas del laboratorio se configuraron mecanismos de seguridad nativos para garantizar control de acceso y protección del entorno:

- **Windows Server 2022 (Controlador de Dominio)**
    - Implementación del Active Directory (AD DS) para la autenticación centralizada de usuarios y equipos del dominio ctmdp.local.
    - Políticas de contraseñas seguras configuradas mediante GPO: longitud mínima de 12 caracteres, complejidad activada, y bloqueo tras 3 intentos fallidos.
    - Deshabilitación del usuario “Invitado” y renombrado del “Administrador” por seguridad.
    - Cortafuegos Windows Defender Firewall activo con reglas personalizadas.
    - Auditoría de inicio de sesión, cambios de políticas y accesos a archivos habilitada mediante Directiva de Auditoría Avanzada.
- **Ubuntu Server 22.04 (DMZ)**
    - Configuración de UFW (Uncomplicated Firewall) para bloquear todo el tráfico entrante excepto servicios permitidos (SSH restringido, HTTP/HTTPS).
    - Fail2ban activo para bloquear intentos de fuerza bruta.
    - Deshabilitación de login del usuario root.
    - Acceso SSH configurado solo por clave pública.
    - Permisos de archivos ajustados (chmod y chown) según principio de mínimo privilegio.
- **pfSense Firewall (Perímetro)**
    - Control de acceso web por usuario administrador con autenticación local.
    - IDS/IPS Suricata activo en la interfaz DMZ (em3) en modo Inline (bloqueo automático de tráfico malicioso).
    - Segmentación de red en tres zonas: LAN (10.10.10.0/24), Operativa (10.10.20.0/24) y DMZ (10.10.30.0/24), aplicando principio de separación de dominios de seguridad.

    - Bloqueo por defecto “deny all” y reglas explícitas de acceso mínimo necesario.

b) Gestión de identidad sobre los sistemas operativos

La gestión de identidad se centralizó en Active Directory (Windows Server 2022) bajo el dominio ctmdp.local, permitiendo una autenticación unificada y administración de usuarios, grupos y políticas.

- Se crearon usuarios y grupos de trabajo según roles: por ejemplo, “Administración” y “Operativa”.

- Se aplicaron Directivas de Grupo (GPOs) para forzar políticas de seguridad en los equipos del dominio (contraseñas, bloqueo de cuenta, firewall).

- Se definieron permisos NTFS por grupo en carpetas compartidas, siguiendo el principio de mínimo privilegio.

- Integración planificada con pfSense mediante RADIUS/NPS para autenticación centralizada en servicios VPN y futuros accesos administrativos.

- En Ubuntu, se gestionan identidades locales con adduser y permisos por grupos (chown, chmod).

c) Auditoría de seguridad implementada. Resguardo

Se implementaron políticas de auditoría de seguridad y monitoreo en los tres niveles:

- **Windows Server 2022**

    - Activación de auditorías por inicio de sesión, cambios de políticas, accesos a objetos y modificaciones de grupos de seguridad.

    - Los eventos se almacenan en el Visor de Eventos → Seguridad, permitiendo rastrear incidentes y accesos indebidos.

    - Respaldo del sistema mediante Copia de seguridad de Windows Server (incluyendo “Estado del sistema”), programada semanalmente.

- **Ubuntu Server**
    - Registro detallado de accesos en /var/log/auth.log y de servicios en /var/log/syslog.
    - Logrotate configurado con compresión (compress) para retención y ahorro de espacio.
    - Respaldos automáticos comprimidos y cifrados (tar.gz + gpg) de /etc y /home.
- **pfSense**
    - Registro de alertas y bloqueos del IDS/IPS Suricata en “Services → Suricata → Logs”.

  Suricata es un sistema de detección y prevención de intrusiones. Analiza el tráfico de red en tiempo real usando reglas (firmas) y motores de inspección. Tiene dos modos:

- Detección (IDS): solo alerta.
- Prevención (IPS): además bloquea en línea.
  Puede inspeccionar HTTP, DNS, TLS (SNI), SMB, SSH y más, y exportar registros a Syslog o a un colector.
    - Backups cifrados del archivo config.xml mediante “Diagnostics → Backup/Restore”.

d) Seguridad implementada en el desarrollo seguro de las aplicaciones

El entorno implementado sigue el principio de defensa en profundidad y las prácticas de desarrollo seguro, aplicando controles tanto en infraestructura como en software:

- Los servicios expuestos (por ejemplo, Apache o SSH en Ubuntu DMZ) fueron restringidos por firewall (UFW) y corren bajo usuarios no privilegiados.
- Comunicación cifrada por TLS/HTTPS (para servicios web en DMZ).
- Validación de entrada de comandos y tráfico mediante Suricata (detección de ataques por inyección, XSS o exploits conocidos).

- Separación de entornos: DMZ para servicios públicos, LAN para administración, y VPN para acceso remoto.

- Backups cifrados de código y configuración (gpg).

- Actualizaciones automáticas habilitadas (unattended-upgrades) para reducir exposición a vulnerabilidades.

- Política de “mínimo privilegio” aplicada también a cuentas de servicio y permisos de ejecución.

e) Gestión de claves criptográficas

- **pfSense:**
    - Autoridad Certificadora (CA) interna creada para OpenVPN.
    - Claves y certificados exportados y resguardados fuera de la VM.
    - Política de rotación anual y revocación ante bajas de usuarios.
- **Windows Server:**
    - Uso de **certificados digitales** para VPN y servicios RDP.
    - Repositorio central de certificados administrado desde “certlm.msc”.
    - Contraseñas críticas almacenadas en KeePass (archivo cifrado con AES-256).
- **Ubuntu Server:**
    - Par de claves SSH (RSA 4096 bits) para autenticación sin contraseña.
    - Claves y passphrases almacenadas de forma segura en gestor cifrado local (KeePassXC o archivo protegido).
    - Preparado para implementar cifrado LUKS en disco completo en reinstalación guiada.

5. Encriptación de archivos y File System

a. Técnicas de encriptación utilizadas.

- Para servidores Ubuntu utilizamos LUKS (Linux Unified Key Setup) para el cifrado de particiones o dispositivos de almacenamiento.
- En Windows se utiliza BitLocker para el cifrado completo del disco
- Para respaldos y archivos compartidos utilizamos GnuPG (GNU Privacy Guard) para cifrar archivos antes de enviarlos y luego compartir la clave de desencriptación de manera segura con el destinatario.

b. Encriptación de datos en movimiento

- El acceso remoto a los servidores Ubuntu se realiza a través de SSH con intercambio de clave asimétrico (clave publica y privada) RSA de 4096 bits.
- Las comunicaciones internas están encapsuladas mediante túneles OpenVPN para cifrar y asegurar el tráfico de datos.
- El tráfico entre hipervisores VirtualBox y las máquinas virtuales se realiza en redes virtuales privadas y aisladas del tráfico público.

c. Encriptación de las comunicaciones entre sistemas operativos

- Entre los servidores Linux y Windows se optó por implementes SMB 3.0 para compartir archivos, directorios, impresoras y demás recursos de una red entre sí de manera segura.
- Las sesiones entre Windows y Linux utilizan RDP (Remote Desktop Protocol) para poder controlar los equipos de manera cifrada.

6. Hardening

a. Hardening implementado sobre los sistemas operativos.

- Limpieza total de servicios innecesarios en todos los sistemas, de forma que solo se cuente con los servicios necesarios.
- Implementación y configuración de Windows Defender Firewall y UFW (Uncomplicated Firewall) para solo permitir conexiones necesarias para el funcionamiento necesario del sistema y aplicaciones.
- Auditoría continua de puertos con NMAP y cierre de aquellos sin utilizar.
- Configuración de logs centralizados a través de Rsyslog y Zabbix con alertas de seguridad.

- pfSense (WAN): bloqueo de redes privadas y bogon.

- pfSense (DMZ): reglas mínimas necesarias (DNS hacia el DC, y navegación HTTP/HTTPS; bloqueo final explícito).

- Ubuntu (DMZ): UFW, fail2ban, y unattended-upgrades.

- Windows Server: políticas de contraseña y bloqueo; firewall habilitado.

b. Gestión de la contraseña de los sistemas operativos utilizados.

- Políticas de contraseñas robustas (mínimo 12 caracteres, mayúsculas y minúsculas, números y caracteres especiales).
- Cambio de contraseñas periódico (90 dias), denegación de acceso y bloqueo automático tras 3 intentos fallidos. Se notificará cada 2do intento fallido ocasionado.
- Uso de autenticación multifactor (MFA) en accesos administrativos.

c. Control de acceso y privilegios implementados.

- Asignar permisos y privilegios únicamente a los usuarios y servicios que realmente lo necesiten (Principio de privilegio mínimo).
- Utilizar sistemas de permisos basado en usuarios y grupos para administrar permisos de archivos y carpetas (chmod, chown).
- Utilizar cuentas de usuario no privilegiadas para tareas cotidianas y evitar el uso de la cuenta superusuario (root) si no es estrictamente necesario.
- Monitoreos continuos de sesiones administrativas y registros de auditoría.

d. Estrategia para mantener actualizados los sistemas operativos.

- Linux: *unattended-upgrades* permite descargar e instalar automáticamente actualizaciones de seguridad de las aplicaciones y servicios.
- Windows: Windows Server Update Services (WSUS) permite a los administradores controlar y distribuir actualizaciones en los equipos de la red corporativa.
- Revisión mensual de parches de seguridad, nuevas CVEs que puedan afectar a nuestros sistemas y planificaciones de mantenimiento programados.

7. Riesgos

a. Análisis de riesgo para la infraestructura.

Riesgo	Probabilidad	Gravedad	Impacto	Mitigación
Fallo del hipervisor	Baja	Medio	Bajo	Redundancia y backups diarios
Ataque por ransomware	Media	Alta	Alto	Copias cifradas fuera de línea + antivirus centralizado.
Acceso no autorizado	Media	Alta	Alto	MFA, VPN, RBAC
Pérdida de datos por error humano	Media	Media	Medio	Versionado, copias de seguridad y permisos limitados.
Vulnerabilidades sin parchear	Media	Alta	Alto	Actualizaciones y monitoreo continuo, revisión de CVEs.
Interrupción eléctrica	Baja	Media	Medio	Sistema de Alimentación Ininterrumpida (UPS) y política de respaldo automatizada.

b. Estrategia de mitigación de riesgos

- Mantener equipos actualizados al día con los últimos parches de seguridad.
- Mantener los privilegios mínimos para cada usuario.
- Realizar copias de seguridad de manera regular.
- Cifrar datos sensibles y/o críticos de la organización.
- Mantener y garantizar que los servidores no sufran una desconexión repentina o no programada.
- Implementar sistemas de detección y prevención de intrusiones (IDS/IPS) como Suricata.
- Monitorear continuamente los recursos críticos mediante herramientas como Zabbix con alertas automáticas ante fallos o sobrecargas.
- Aplicar segmentación de red y VLANs para aislar entornos administrativos, técnicos y públicos para limitar el alcance de un posible ataque.
- Realizar pruebas periódicas de vulnerabilidades y pentesting interno/externo.
- Contar con un plan de respuesta ante incidentes, que defina claramente los pasos a seguir, responsables y tiempos de acción ante una brecha o ataque.
- Mantener logs centralizados y auditables con revisión periódica para detectar accesos no autorizados o actividades sospechosas.
- Capacitar al personal periódicamente en ciberseguridad, reforzando la detección de correos de phishing y buenas prácticas de manejo de información.
- Usar redundancia para tener una alta disponibilidad en servicios críticos reduciendo así el impacto de caídas o fallos de hardware.
- Verificar la integridad de las copias de seguridad mediante restauraciones de prueba regulares.

c. Rutina de auditoría de seguridad para los sistemas operativos.

- Auditoría trimestral de configuración de sistemas y puertos.
- Revisión mensual de alertas Suricata y logs críticos de Windows/Linux.
- Revisión de logs de acceso y alertas de Zabbix semanalmente.
- Pruebas de vulnerabilidad con OpenVAS cada seis meses.
- Pruebas de pentesting interno/externo cada cinco meses.
- Verificación anual de cumplimiento de políticas de seguridad internas.
- Evaluación trimestral a empleados sobre buenas practicas de ciberseguridad y concientización.

8. Políticas de seguridad

a. Definir y aplicar políticas de seguridad sobre la infraestructura.

- Todo acceso remoto debe realizarse mediante VPN y MFA.
- Los usuarios deben usar contraseñas seguras y únicas para cada sistema.
- Está prohibido el uso de dispositivos externos no autorizados (pendrives, discos).
- Se exige el cifrado de discos en servidores y notebooks corporativos.
- Toda instalación de software debe ser aprobada por el departamento de TI.
- Los registros de eventos deben conservarse durante 6 meses como mínimo.

b. Plan de capacitación sobre seguridad.

Objetivo: *concientizar al personal sobre las mejores prácticas de ciberseguridad.*

Temas a tratar:

1. Ingeniería social y phishing.
2. Buenas prácticas de contraseñas y MFA.
3. Seguridad en correos electrónicos.
4. Manejo seguro de datos y documentos sensibles.
5. Política de uso aceptable de equipos y redes.
6. Actualizaciones y parches de seguridad.
7. Procedimiento ante incidentes y reportes.

9) Seguridad perimetral

9.a) Medidas implementadas (diseño)

- Firewall perimetral (pfSense) con política por defecto “deny all” y reglas explícitas por servicio.
- Segmentación: VLAN 10 (Admin), 20 (Operativa), 30 (DMZ), 99 (Gestión). Tráfico inter-VLAN restringido (principio de mínimo privilegio).
- DMZ para servicios públicos (Web/Oficina Virtual). Publicación controlada vía NAT 1:1/port-forward y reverse proxy endurecido.
- IDS/IPS (Suricata) en el perímetro (bloqueo de firmas críticas, inspección TLS SNI, thresholding para evitar falsos positivos).
- Antibot/GeoIP: listas reputacionales y bloqueos por país si corresponde al negocio.
- DDoS light: rate-limit en firewall, SYN cookies, y “blackhole” ante volumetrías simples (coordinado con ISP).
- WAF a nivel reverse proxy (ModSecurity/OWASP CRS) para la Oficina Virtual.
- NAT y egress filtering fuerte: solo salen puertos necesarios (HTTP/HTTPS, DNS autoritativos, NTP corporativo, SMTP relay autenticado).
- VPN IPSec IKEv2 para acceso remoto.
- Registro y trazabilidad: Syslog remoto, NetFlow/sFlow hacia colector, alertas Zabbix.

9.b) Política de acceso remoto (tecnología)

Acceso remoto (LAB): Se implementa OpenVPN Remote Access en pfSense.

- Red de túnel 10.10.40.0/24
- Rutas a redes internas 10.10.10.0/24
- DNS entregado al cliente: 10.10.10.10 (DC).
- Validación: conexión exitosa desde Windows, ping a 10.10.10.254 y resolución de dc1.ctmdp.local.

Diseño futuro: IPSec IKEv2 con autenticación centralizada RADIUS/NPS + MFA; WAF para publicar Oficina Virtual; listas GeoIP; NetFlow y Zabbix.

9.c) Monitoreo de la seguridad perimetral

- Zabbix: salud del firewall, latencias WAN, consumo CPU/RAM, estado HA (CARP), colas.
- Suricata → Alertas: enviar a Syslog y Zabbix (triggers por severidad/volumen).
- NetFlow/sFlow: detección de anomalías de tráfico, top talkers, puertos inusuales.
- Dashboards diarios y alertas por umbrales (correo al equipo técnico + canal interno).

Punto 10 Redundancia

10.a)

Explicación general

En la Cooperativa de Telecomunicaciones Mar del Plata (CTMdP) la continuidad operativa es crítica: los servicios de Internet, telefonía IP y portal web no pueden interrumpirse sin afectar a usuarios y facturación.
Por eso, se considera necesario implementar mecanismos de redundancia y replicación, tanto en el nivel de servidores como en la infraestructura de red.

💡 En el laboratorio (implementado)

En el LAB, la redundancia se simula mediante:

- Máquinas virtuales independientes en VirtualBox, que pueden restaurarse rápidamente desde snapshots.
- pfSense como único firewall, con backup del config.xml exportado para recuperación rápida.
- Windows Server (DC) con rol de Active Directory y DNS, configurado de forma que pueda ser replicado fácilmente si se crea un segundo DC en el futuro.
- Ubuntu Server con servicios web independientes, que pueden reinstalarse o restaurarse a partir de backups o imágenes.

En esta escala, no es necesario un clúster real, pero se demuestra el concepto de redundancia lógica (copias de configuración y restauración rápida).

💡 En producción (propuesta futura)

En la infraestructura final se recomienda:

Capa	Redundancia / Replicación	Justificación
Hipervisor	Cluster de Proxmox VE (2 nodos + QDevice)	Alta disponibilidad, migración en caliente y failover automático.
Firewall	pfSense en modo HA (CARP)	Si un firewall falla, el otro asume el rol inmediatamente.
Active Directory	2 controladores de dominio (multi-master)	Evita pérdida de autenticación y DNS si un servidor se apaga.
Servidores web / aplicaciones	Replicación o balanceo (HAProxy o Keepalived)	Permite distribuir carga y mantener disponibilidad ante caídas.
Base de datos (si existiera)	Replicación nativa (MariaDB Galera / PostgreSQL Streaming)	Redundancia de datos en tiempo real.

🔹 10.b) Método de recuperación de sistema operativo (Runbook)

Un Runbook de recuperación documenta paso a paso qué hacer si un servidor falla, para reducir tiempos de recuperación (RTO) y evitar pérdida de datos (RPO).

El procedimiento de recuperación se basa en:

1. **pfSense**
    - Backup automático del config.xml (System > Backup/Restore > Download).
    - Restauración rápida: arrancar desde ISO, elegir *Recover configuration*, y montar partición /dev/ada0p2 para restaurar.
2. **Windows Server (DC)**
    - Snapshot manual en VirtualBox antes de cambios grandes.
    - Restauración rápida desde ese snapshot o exportación de VM.
    - En producción: se usaría wbadmin o Windows Server Backup.
3. **Ubuntu Server**
    - Backup de /var/www y archivos de configuración (/etc/apache2, /etc/ssh).
    - Restauración simple desde copia comprimida o imagen .ova.

En producción (propuesta)

Método estandarizado de recuperación (Runbook):

Etapa	Acción	Herramienta / Observación
Detección	Monitoreo (Zabbix) detecta falla y envía alerta.	Email / Dashboard.

Verificación	Confirmar causa: software, hardware o red.	Consola o logs.
Restauración rápida	Si es VM → restaurar snapshot o copia de PBS.	Proxmox / VirtualBox.
4 Validación	Verificar conectividad (ping, DNS, servicios).	ping, ss -lntup, navegador.
Documentación	Registrar evento, acciones y resultado.	Bitácora interna.

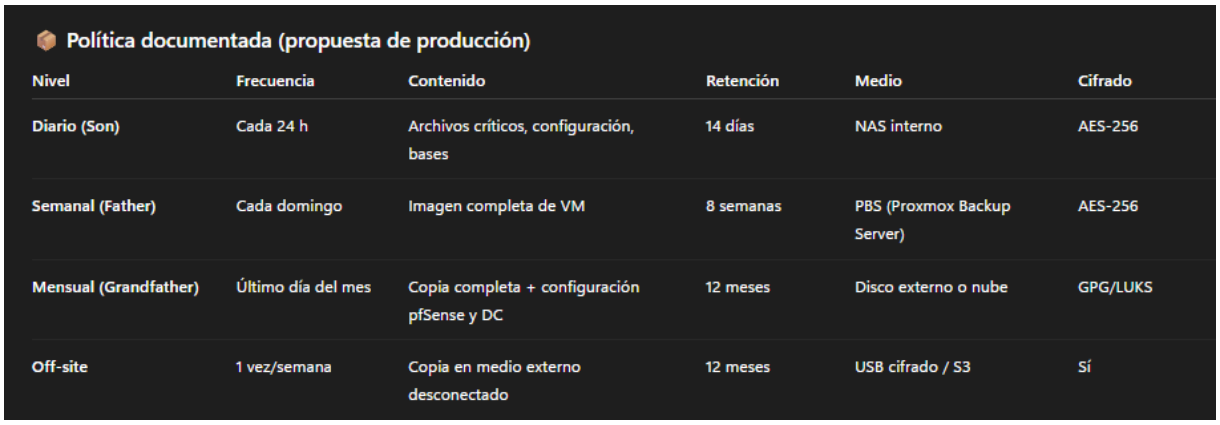
10.c) Política de backup para los sistemas operativos

Los respaldos garantizan la disponibilidad de datos críticos ante fallas o ataques (por ejemplo, ransomware).
La política se diseña bajo el esquema GFS (Grandfather-Father-Son) para mantener copias diarias, semanales y mensuales, con cifrado y pruebas periódicas de restauración.

En el laboratorio (implementado)

- pfSense: Backup manual del config.xml (descargado desde interfaz web).
- Windows Server: Snapshots en VirtualBox y exportación de la VM.

- Ubuntu: Script simple de copia de /var/www comprimido (tar -czvf backup_web.tar.gz /var/www/html).



📦 Política documentada (propuesta de producción)

Nivel	Frecuencia	Contenido	Retención	Medio	Cifrado
Diario (Son)	Cada 24 h	Archivos críticos, configuración, bases	14 días	NAS interno	AES-256
Semanal (Father)	Cada domingo	Imagen completa de VM	8 semanas	PBS (Proxmox Backup Server)	AES-256
Mensual (Grandfather)	Último día del mes	Copia completa + configuración pfSense y DC	12 meses	Disco externo o nube	GPG/LUKS
Off-site	1 vez/semana	Copia en medio externo desconectado	12 meses	USB cifrado / S3	Sí

📋 Verificación de integridad

- En ZFS/PBS: verificación automática de hash.
- En Linux: sha256sum backup.tar.gz para comprobar integridad.
- Prueba de restauración cada 15 días de un backup aleatorio.