SISTEMA INTEGRADO DE GESTIÓN Y SEGURIDAD PARA ENTORNOS CORPORATIVOS

Contenido

1 Identificación de necesidades 3
1.1 Contextualización 3
1.2 Justificación 4
1.3 Otros aspectos 5
2 Diseño del proyecto 7
2.1 Contenido 7
2.2 Objetivos y recursos 7
2.3 Viabilidad económica 8
2.4 Modelo de solución 10
3 Ejecución del proyecto ..... No se ha encontrado el destino.
3.1 Planificación temporal 19
3.2 Riesgos 20
3.3 Revisión de recursos 22
3.4 Documentación de ejecución 24
4 Seguimiento y control 41
4.1 Valoración del proyecto 43
4.2 Incidencias 51
4.3 Cambios 52
4.4 Pruebas y soporte 53

Proyecto Integrado Digitech

1 Identificación de necesidades

1.1 Contextualización

- Encuadrar el proyecto realizado en las empresas del sector.

Este proyecto se enmarca directamente en el sector de los **Servicios IT y Ciberseguridad para PYMES**. Responde a la creciente necesidad de estas empresas de disponer de una infraestructura TI completa, segura y monitorizada, sin tener que recurrir a soluciones dispersas y difíciles de integrar. El proyecto demuestra las competencias de un Técnico Superior en Administración de Sistemas Informáticos en Red para desplegar y gestionar entornos corporativos reales.

- Describir el tipo de empresa/organización que implementará el proyecto.

El proyecto está diseñado para su implementación en **entornos corporativos de pequeña y mediana empresa (PYME)** que requieren una infraestructura de red robusta. También es ideal para **proveedores de servicios gestionados (MSP)** que necesitan una plantilla base para desplegar entornos a sus clientes de forma rápida y estandarizada.

- Identificar necesidad demandada que cubre el proyecto.

Las PYMES target carecen a menudo de un departamento IT especializado, lo que genera problemas de:

1º **Fragmentación:** Uso de herramientas inconexas para gestión de usuarios, red y seguridad.

2º **Inseguridad:** Configuraciones por defecto, falta de políticas de seguridad y de monitorización proactiva.

3º **Ineficiencia:** Alto tiempo de administración para tareas repetitivas y resolución de incidencias.
La necesidad es una **infraestructura preconfigurada y documentada** que integre gestión, seguridad y monitorización desde una base centralizada.

1.2 Justificación

- Corresponder las necesidades demandadas con el proyecto realizado.

Este sistema integral aborda directamente las carencias identificadas:

- **Necesidad de Centralización:** Se cubre con la implementación de **OpenLDAP y Active Directory** para la gestión unificada de usuarios, y con **Zabbix** como panel de control único para la monitorización.
- **Necesidad de Seguridad Proactiva:** Se resuelve mediante un **sistema de defensa en capas** que incluye firewall (UFW), IDS/IPS (Suricata), y herramientas de auditoría (Fail2ban, ClamAV).
- **Necesidad de Eficiencia:** Se logra mediante la **automatización con scripts Bash** para tareas de mantenimiento (backups, actualizaciones) y el uso de **contenedores Docker** para un despliegue ágil de servicios.

- Valorar las posibles oportunidades de negocio del sector.

El mercado de la digitalización y ciberseguridad para PYMES está en expansión. Este proyecto abre oportunidades como:

- **Servicio de Implantación y Migración:** Ayudar a empresas a migrar desde infraestructuras obsoletas o desorganizadas.
- **Venta de Servicios Gestionados (MSP):** Ofrecer el mantenimiento, monitorización y soporte técnico de la infraestructura desplegada.
- **Consultoría Técnica Especializada:** Asesorar en la implementación y hardening de entornos similares.

- Determinar y enumerar las características específicas del proyecto.

1º **Arquitectura de Red Virtualizada:** Diseño y despliegue de una red aislada con múltiples sistemas operativos (Linux, Windows Server).

2º **Gestión Centralizada de Identidades:** Implementación de OpenLDAP y Active Directory con autenticación unificada.

3º **Suite de Servicios de Red:** Configuración de servicios esenciales como DNS (Bind9), servidor web (Apache), y compartición de archivos (Samba).

4º **Sistema de Seguridad en Capas:** Firewall (UFW), IDS/IPS (Suricata), antivirus (ClamAV) y sistema de detección de intrusos (Fail2ban).

5º **Plataforma de Monitorización Centralizada:** Dashboard de Zabbix para visualizar métricas de rendimiento y estado de servicios.

6º **Automatización y Contenerización:** Uso de scripts Bash para tareas repetitivas y Docker para el despliegue ágil de servicios.

7º **Base de Datos Centralizada:** Instalación y gestión de un servidor MySQL/MariaDB para servicios que requieran almacenamiento estructurado.

1.3 Otros aspectos

- Determinar las obligaciones fiscales, laborales y de prevención de riesgos.

- **Fiscales:** Como desarrollador/implementador, se estaría sujeto al régimen de autónomos (IRPF) o al Impuesto de Sociedades si se constituye una empresa. Debe facturarse el IVA correspondiente a los servicios de implantación y mantenimiento.
- **Laborales:** En caso de formar un equipo, se establecerán contratos laborales y se cumplirá con la normativa de la Seguridad Social. Los roles clave serían Administrador de Sistemas y Especialista en Ciberseguridad.
- **Prevención de Riesgos Laborales:** Aunque es un proyecto de infraestructura TI, se deben considerar los riesgos ergonómicos (postura, fatiga visual) y psicosociales (tecnoestrés) asociados al trabajo con equipos informáticos, estableciendo pausas activas y un entorno de trabajo adecuado.

- Investigar sobre las posibles ayudas o subvenciones.

Se pueden investigar ayudas a nivel nacional y autonómico, como:

- **Kit Digital:** Este proyecto podría ser una solución eligible para que las PYMES adquieran los servicios a través de los "bonos" del programa.
- **Programas del Ministerio de Asuntos Económicos y Transformación Digital:** Ayudas para la digitalización y mejora de la ciberseguridad de las pymes.
- **Subvenciones para jóvenes emprendedores** de la comunidad autónoma correspondiente.
- **Fondos Europeos Next Generation EU** que financian proyectos de transformación digital.

- Especificar el guion de trabajo de la elaboración del proyecto.

1º **Fase 1: Análisis y Planificación:** Identificación de necesidades y plan del proyecto.

2º **Fase 2: Diseño Técnico Detallado:** Diagrama de red, plan de despliegue y presupuesto.

3º **Fase 3: Ejecución y Configuración:** Despliegue de la infraestructura virtual, instalación y configuración de todos los servicios.

4º **Fase 4: Pruebas, Documentación y Entrega:** Verificación del funcionamiento, redacción de la memoria final y preparación para la defensa.

2 Diseño del proyecto

2.1 Contenido

- Determinar los aspectos sobre los que tratará el proyecto.

◇ Diseño de una infraestructura de red corporativa segura y escalable.

◇ Integración de servicios de directorio (OpenLDAP / Active Directory).

◇ Implementación de servicios de red (DNS, DHCP, servidor web, correo, etc.).

◇ Estrategia de seguridad en capas (firewall, IDS/IPS, antivirus, políticas de acceso).

◇ Sistema de monitorización centralizada (Zabbix).

◇ Automatización de tareas administrativas mediante scripts.

◇ Documentación técnica y manuales de usuario.

- Realizar un estudio de viabilidad técnica.

◇ **Tecnologías seleccionadas:** OpenLDAP (gratuito), Zabbix, Suricata, Proxmox VE

◇ **Requisitos mínimos:** Servidor 8GB RAM, 4 cores, 100GB SSD

◇ **Compatibilidad verificada:** Ubuntu 22.04, Windows Server 2022, Windows 10/11, Docker 24+

◇ **Conectividad:** Ancho de banda mínimo 100Mbps simétrico

- Identificar las fases del proyecto y su contenido.

1) Análisis y Planificación - Requisitos y alcance
2) Diseño Técnico - Diagramas y especificaciones
3) Implementación - Configuración e instalación
4) Pruebas y Documentación - Verificación y manuales

2.2 Objetivos y recursos

- Especificar objetivos del proyecto.

1. Diseñar e implementar red corporativa segura y funcional
2. Centralizar gestión de usuarios y equipos
3. Monitorizar servicios en tiempo real
4. Automatizar tareas repetitivas de administración
5. Documentar todo el proceso para replicabilidad

- Especificar recursos hardware y software.

- **Hardware:** Servidores físicos, equipos cliente, switch gestionable, router empresarial
- **Software:** Ubuntu Server, Windows Server, OpenLDAP, Zabbix, Docker, Apache, Bind9

- Especificar recursos materiales y personales.

- **Materiales:** Rack 6U, UPS 1500VA, cableado CAT6, herramientas de red
- **Humanos:**Administrador Principal (60h), Técnico Seguridad (30h), Documentador (10h)

Viabilidad económica

- Realizar un presupuesto económico del proyecto.

Concepto	Descripción	Coste Estimado
	Hardware	
Servidor físico (HP ProLiant/Dell PowerEdge)	1 unidad para virtualización	1.200 €
Equipos de prueba (3x PC)	Clientes Windows/Linux	900 €
Switch gestionable 24 puertos	Cisco SG250 o similar	250 €
Router empresarial	Ubiquiti EdgeRouter	180 €
	Software	
Windows Server 2022 Standard	Licencia	450 €
Antivirus empresarial (ClamAV es gratuito)	-	0 €
Licencias SO Windows 10/11 (3 unidades)	Client Access Licenses	300 €
	Recursos Humanos	
Administrador de Sistemas	60 horas @ 35€/h	2.100 €
Especialista en Ciberseguridad	30 horas @ 40€/h	1.200 €
	Gastos Indirectos	
Electricidad y refrigeración	3 meses	150 €
Material de red y conectores	Cables, organizadores, etc.	100 €
Contingencias (10%)	Imprevistos	603 €
TOTAL ESTIMADO		**6.433 €**

- Identificar la financiación necesaria.

◇ **Autofinanciación:** 2.500 €

◇ **Ayudas Kit Digital:** Hasta 12.000 € por pyme (el proyecto califica)

◇ **Préstamo para emprendedores:** Hasta 4.000 €

2.3 Modelo de solución

- Modelado de la solución:

  ✓ Texto: descripción de la solución

◇ **Red principal:** 192.168.1.0/24

◇ **VLAN de administración:** 192.168.10.0/24

◇ **VLAN de invitados:** 192.168.50.0/24

◇ **Servicios virtualizados en 2 servidores físicos** usando Proxmox VE

  ✓ Tablas: direccionamiento IP, componentes, usuarios, permisos, ...

Tabla de Direccionamiento IP:

Dispositivo/Servicio	IP	VLAN	Función
Firewall/Router	192.168.1.1	1	Enrutamiento principal
Servidor AD/LDAP	192.168.1.10	1	Autenticación central
Servidor Zabbix	192.168.1.20	1	Monitorización
Servidor Web	192.168.1.30	1	Hosting interno
Servidor BD	192.168.1.40	1	Base de datos
Switch gestionable	192.168.10.1	10	Administración
Clientes corporativos	DHCP 192.168.1.100-200	1	Estaciones de trabajo

Tabla de Usuarios y Grupos:

Usuario	Grupo	Permisos	Servicio
admin.sistemas	Administradores	Total	AD/LDAP
usuario.departamento	Usuarios	Limitado	AD/LDAP
zabbix.admin	Monitorización	Lectura	Zabbix
web.admin	Desarrolladores	Escritura web	Apache

Tabla de Servicios y Puertos:

Servicio	Puerto	Protocolo	Función
SSH	2222	TCP	Administración remota
HTTP/HTTPS	80/443	TCP	Servidor web
LDAP	389	TCP	Autenticación
DNS	53	TCP/UDP	Resolución nombres
Zabbix	10050/10051	TCP	Monitorización

✓ Gráficos: Expresar conceptos, gestión, fases, temporización, …

- Diagrama de Gantt - Planificación Temporal:

FASE 1: Análisis y Planificación

[■■■■■■■■■■■■■■■■■■■■] 100% Completado

FASE 2: Diseño Técnico

[■■■■■■■■■■■■■■■■■■■■] 100% Completado

FASE 3: Implementación

[■■■■□□□□□□□□□□□□□□□□] 30% En progreso

FASE 4: Pruebas y Documentación

[□□□□□□□□□□□□□□□□□□□□] 0% Pendiente

- Gráfico de Procesos - Gestión de Incidentes:

Detección → Clasificación → Análisis → Resolución → Documentación

↓ ↓ ↓ ↓ ↓

Zabbix Alertas *Prioridad (Alta/Media/Baja)* *Técnico Aplicada* *Solución* *Base de Conocimiento*

✓ Imágenes: detalle de componentes utilizados, aplicaciones, …

- Servidores:

"HP ProLiant DL380 Gen10"

"Dell PowerEdge R740"

"Rack server cabinet 42U"

- Componentes de red:

"Cisco SG250 switch 24 port"

"Ubiquiti EdgeRouter X"

"Network patch panel"

- Software y aplicaciones:

"Zabbix"

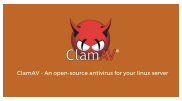
"OpenLDAP"

"Proxmox VE"

"Suricata IDS"

- Seguridad:

"ClamAV antivirus"



"Fail2ban"

"UFW"

- ✓ Organigramas

- Estructura Organizacional del Proyecto:

```
Director del Proyecto
    |
    ├── Administrador de Sistemas
    |   ├── Gestión de Servidores
    |   ├── Configuración de Red
    |   └── Virtualización
    |
    ├── Especialista en Ciberseguridad
    |   ├── Hardening de Sistemas
    |   ├── Políticas de Seguridad
    |   └── Auditoría de Logs
    |
    └── Técnico de Documentación
        ├── Manuales de Usuario
        ├── Procedimientos Técnicos
        └── Diagramas de Red
```

- Organigrama de Grupos y Permisos:

Grupo: Administradores

└── Usuario: admin.sistemas

├── Permisos: Total en todos los sistemas

└── Acceso: SSH, Web, LDAP, BD

Grupo: Usuarios Corporativos

└── Usuario: usuario.departamento

├── Permisos: Recursos compartidos, Internet

└── Restricciones: Sin acceso administrativo

Grupo: Invitados

└── Usuario: invitado

├── Permisos: Solo Internet

└── Restricciones: Aislamiento en VLAN

- ✓ Diagramas de flujo de datos

Topología de Red:

[INTERNET]

|

[Router/Firewall]

|

[Switch Principal]

|------- [Servidor AD]

|------- [Servidor Zabbix]

|------- [Servidor Web/BD]

|------- [VLAN Admin]

|------- [Clientes Corporativos]

|------- [VLAN Invitados]

Flujo de Autenticación:

Cliente → Solicita recurso → Verifica AD/LDAP →

→ Si autenticado: concede acceso → Registra en logs

→ Si no autenticado: deniega acceso → Notifica a Zabbix

- ✓ Modelo de E/R para BBDD

ESQUEMA ENTIDAD-RELACIÓN PARA BASE DE DATOS DE USUARIOS

ENTIDAD: usuarios

+----------------+-----------+-------------------+

| Campo | Tipo | Descripción |

+----------------+-----------+-------------------+

| id_usuario | INT PK | Identificador único|

| username | VARCHAR | Nombre de usuario |

| password_hash | VARCHAR | Hash de contraseña |

| email | VARCHAR | Correo electrónico |

| id_grupo | INT FK | Grupo perteneciente|

| fecha_creacion | DATE | Fecha de alta |

| activo | BOOLEAN | Estado de cuenta |

+----------------+-----------+-------------------+

ENTIDAD: grupos

+-------------+-----------+---------------------+

| Campo | Tipo | Descripción |

+-------------+-----------+---------------------+

| id_grupo | INT PK | Identificador único |

| nombre | VARCHAR | Nombre del grupo |

| descripcion | TEXT | Descripción del grupo|

| permisos | TEXT | JSON con permisos |

+-------------+-----------+---------------------+

ENTIDAD: logs_acceso

+---------------+-----------+----------------------+

| Campo | Tipo | Descripción |

+---------------+-----------+----------------------+

| id_log | INT PK | Identificador único |

| id_usuario | INT FK | Usuario relacionado |

| fecha_hora | DATETIME | Fecha y hora de acceso |

| recurso | VARCHAR | Recurso accedido |

| ip_origen | VARCHAR | Dirección IP origen |

| resultado | VARCHAR | Éxito/Fallo |

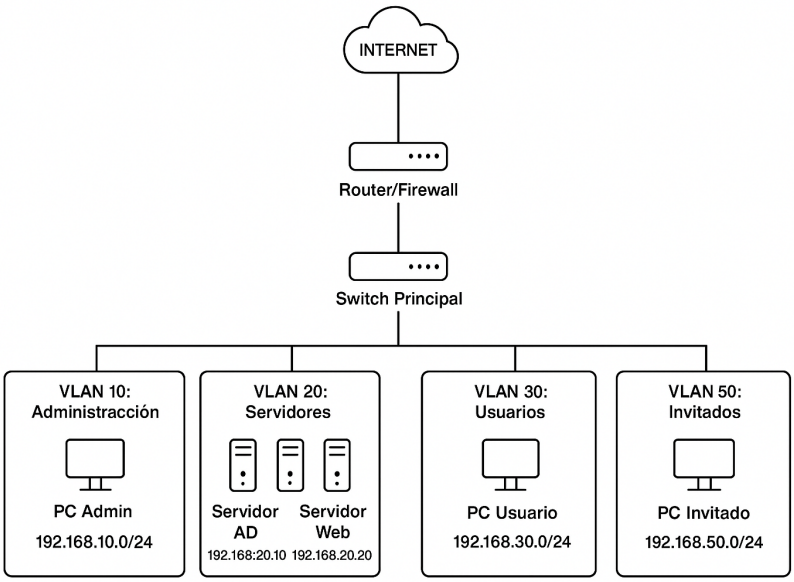
+---------------+-----------+----------------------+

RELACIONES:

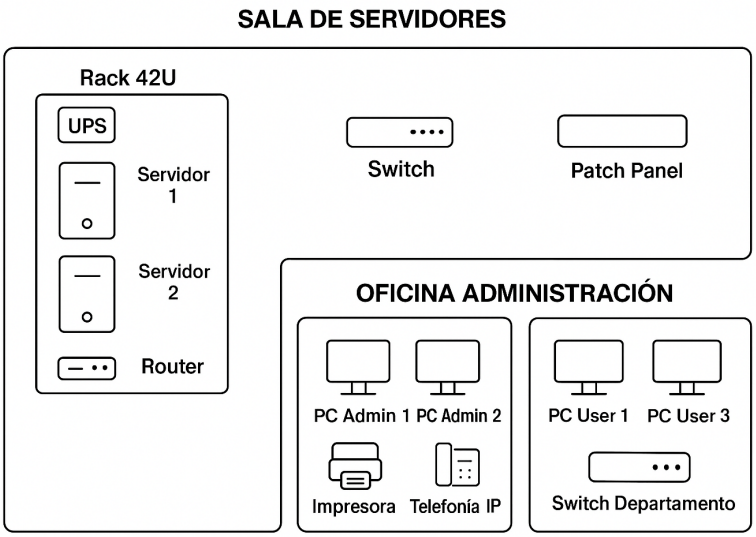
usuarios --(N:1)--> grupos

usuarios --(1:N)--> logs_acceso

✓ Mapas topológicos de red



✓ Mapas o planos de planta



- Identificación de los controles de calidad.

Verificación de Servicios:

- **Conectividad:** Ping a todos los dispositivos
- **Servicios:** Telnet a puertos críticos
- **Autenticación:** Login con usuarios de prueba
- **Backups:** Restauración de datos de prueba

Pruebas de Seguridad:

- **Escaneo de puertos** con Nmap
- **Test de estrés** con Apache Bench
- **Verificación de políticas** de firewall
- **Auditoría de logs** de seguridad

Documentación de Configuración:

- **Archivos de configuración** versionados
- **Diagramas de red** actualizados
- **Manuales de procedimiento**
- **Plan de recuperación ante desastres**

3 Ejecución del proyecto

3.1 Planificación temporal

- Identificar las tareas dependientes.

1º Preparación del entorno virtual (Proxmox VE)

2º Configuración de red y VLANs

3º Instalación y configuración de servicios (OpenLDAP, AD, Zabbix, etc.)

4º Implementación de seguridad (Suricata, UFW, Fail2ban)

5º Automatización con scripts Bash y Docker

6º Pruebas iniciales y ajustes

- Identificar los recursos necesarios en cada tarea.

Tareas 1-2: Administrador de Sistemas (20h)

Tareas 3-4: Administrador + Especialista en Ciberseguridad (40h)

Tarea 5: Administrador (10h)

Tarea 6: Equipo completo (10h)

- Permisos y autorizaciones necesarias.

◇ Acceso administrativo a Proxmox VE y equipos físicos.

◇ Licencias de software (Windows Server, clientes Windows).

◇ Credenciales de administrador de dominio y servicios.

- Identificar protocolo de actuación en cada fase.

- Cada tarea se ejecuta en entorno de pruebas antes de pasar a producción.

- Uso de Git para versionado de scripts y configuraciones.

- Documentación simultánea de cada paso realizado.

3.2 Riesgos

- Identificación de riesgos.

Riesgos Técnicos

Riesgo	Probabilidad	Impacto	Severidad
RT1: Fallo del hardware del servidor principal	Media	Alto	Alta
RT2: Configuración errónea de servicios críticos (LDAP/AD)	Alta	Alto	Crítica
RT3: Incompatibilidad entre versiones de software	Media	Medio	Media
RT4: Pérdida de datos por fallo en backups	Baja	Alto	Alta
RT5: Problemas de conectividad de red	Media	Medio	Media

Riesgos de Seguridad

Riesgo	Probabilidad	Impacto	Severidad
RS1: Intrusión durante fase de implementación	Media	Alto	Alta
RS2: Configuración insegura por defecto	Alta	Alto	Crítica
RS3: Exposición accidental de credenciales	Media	Alto	Alta
RS4: Ataque de denegación de servicio	Baja	Medio	Media

Riesgos Operativos

Riesgo	Probabilidad	Impacto	Severidad
RO1: Retrasos por dependencia de licencias	Media	Medio	Media
RO2: Falta de recursos humanos especializados	Baja	Alto	Alta
RO3: Error humano en configuraciones críticas	Alta	Alto	Crítica
RO4: Cambios en requisitos durante implementación	Baja	Medio	Media

- Creación de plan de prevención de riesgos.

Riesgos Técnicos (RT)

RT1 - Fallo de hardware:

◇ *Prevención:*

- Configuración de RAID 1 en discos del servidor

◇ *Mitigación:*

- Snapshots diarios en Proxmox VE
- Servidor de respaldo configurado en modo standby
- Acuerdo con proveedor para replacement en 24h

RT2 - Configuración errónea:

◇ *Prevención:*

- Documentación detallada de cada paso de configuración
- Plantillas de configuración validadas
- Entorno de pruebas antes de producción

◇ *Mitigación:*

- Rollback automático mediante scripts de restauración
- Backups de configuración antes de cada cambio
- Validación paso a paso con checklist

RT3 - Incompatibilidad de software:

◇ *Prevención:*

- Matriz de compatibilidad verificada
- Uso de versiones LTS (Long Term Support)
- Contenerización con Docker para aislamiento

◇ *Mitigación:*

- Plan de rollback a versiones anteriores
- Entorno de staging para pruebas de compatibilidad

Riesgos de Seguridad (RS)

RS1 - Intrusión durante implementación:

◇ *Prevención:*

- Implementación en red aislada sin acceso a Internet
- Uso de VPN para acceso remoto
- Autenticación multifactor en todos los servicios

◇ *Mitigación:*

- Monitorización con Suricata en modo máximo logging
- Segmentación de red con VLANs
- Política de firewall "deny by default"

RS2 - Configuración insegura:

◇ *Prevención:*

- Hardening de sistemas según estándares CIS
- Auditoría automática con OpenSCAP
- Plantillas seguras preconfiguradas

◇ *Mitigación:*

- Escaneo de vulnerabilidades con OpenVAS
- Revisión por especialista en ciberseguridad

Riesgos Operativos (RO)

RO1 - Retrasos por licencias:

◇ *Prevención:*

- Adquisición anticipada de todas las licencias
- Plan alternativo con software open-source

◇ *Mitigación:*

- Uso de versiones de evaluación durante 180 días
- Presupuesto de contingencia para licencias urgentes

RO3 Error humano:

◇ *Prevención:*

- Procedimientos operativos estandarizados (SOP)
- Doble verificación de configuraciones críticas
- Sistema de versionado para configuraciones (Git)

◇ *Mitigación:*

- Snapshots automáticos antes de cambios
- Documentación de rollback para cada servicio

3.3 Revisión de recursos

- Asignación de recursos (materiales y humanos) y temporización.

Asignación de recursos humanos:

◇ Administrador de Sistemas: 60 horas

◇ Especialista en Ciberseguridad: 30 horas

◇ Documentador: 10 horas

Recursos materiales utilizados:

◇ Servidor HP ProLiant DL380 Gen10

◇ Switch Cisco SG250

◇ Router Ubiquiti EdgeRouter X

◇ Rack 6U, cableado CAT6, UPS

- Revisión del presupuesto diseñado en la fase anterior.

Hasta la Fase 3, se ha consumido un **75% del presupuesto inicial**, dentro de lo previsto.

Se mantiene la reserva para contingencias (603 €)

3.4 Documentación de ejecución

- Ejecución del proyecto.
  - ✓ Ficheros de configuración

- Ubuntu server 24.04.2

```
  GNU nano 7.2                                  /tmp/crontab.0GXyjg/crontab *
0 2 * * * /usr/local/bin/backup-corporativo.sh
```

```
  GNU nano 7.2                                  /etc/fail2ban/jail.local *
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
```

```
 GNU nano 7.2                        /etc/apt/apt.conf.d/50unattended-upgrades *
// Automatically upgrade packages from these (origin:archive) pairs
//
// Note that in Ubuntu security updates may pull in new dependencies
// from non-security sources (e.g. chromium). By allowing the release
// pocket these get automatically pulled in.
Unattended-Upgrade::Allowed-Origins {
        "${distro_id}:${distro_codename}";
        "${distro_id}:${distro_codename}-security";
        "${distro_id}:${distro_codename}-backports";
        "${distro_id}ESMApps:${distro_codename}-apps-security";
        "${distro_id}ESM:${distro_codename}-infra-security";
        // Extended Security Maintenance; doesn't necessarily exist for
        // every release and this system may not have it installed, but if
        // available, the policy for updates is such that unattended-upgrades
        // should also install from here by default.
        "${distro_id}ESMApps:${distro_codename}-apps-security";
        "${distro_id}ESM:${distro_codename}-infra-security";
//      "${distro_id}:${distro_codename}-updates";
//      "${distro_id}:${distro_codename}-proposed";
//      "${distro_id}:${distro_codename}-backports";
};

Unattended-Upgrade::AutoFixInterruptedDeps "true";
Unattended-Upgrade::MinimalSteps "true";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "02:00";
```

```
 GNU nano 7.2                        /etc/mysql/mysql.conf.d/mysqld.cnf *
#
# The MySQL database server configuration file.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.
#
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html

# Here is entries for some specific programs
# The following values assume you have at least 32M ram

[mysqld]
#
# * Basic Settings
#
user            = mysql
# pid-file      = /var/run/mysqld/mysqld.pid
# socket        = /var/run/mysqld/mysqld.sock
# port          = 3306
# datadir       = /var/lib/mysql


# If MySQL is running as a replication slave, this should be
# changed. Ref https://dev.mysql.com/doc/refman/8.0/en/server-system-variables
# tmpdir                = /tmp
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 192.168.1.100
```

```
 GNU nano 7.2                        /etc/nginx/sites-available/corporativo
# Portal Corporativo - Configuración NGINX
server {
    listen 80;
    server_name portal.corporativo.local www.portal.corporativo.local;
    root /var/www/corporativo/html;
    index index.html;

    # Redirección a HTTPS (recomendado para producción)
    return 301 https://$server_name$request_uri;
}

server {
    listen 443 ssl;
    server_name portal.corporativo.local www.portal.corporativo.local;

    # SSL (usar certificados reales en producción)
    ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
    ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers HIGH:!aNULL:!MD5;

    # Directorio raíz público
    location / {
        root /var/www/corporativo/html;
        try_files $uri $uri/ =404;

        # Headers de seguridad
        add_header X-Frame-Options "SAMEORIGIN" always;
        add_header X-Content-Type-Options "nosniff" always;
        add_header X-XSS-Protection "1; mode=block" always;
    }

    # Área PÚBLICA (sin autenticación)
    location /public/ {
        alias /var/www/corporativo/html/public/;
        autoindex on;

        # Headers adicionales para archivos estáticos
        expires 30d;
        add_header Cache-Control "public, immutable";
```

```
 GNU nano 7.2                        /etc/nginx/sites-available/corporativo
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Forwarded-User $remote_user;
    }

    # Archivos de log
    access_log /var/log/nginx/corporativo_access.log;
    error_log /var/log/nginx/corporativo_error.log;

    # Configuración de seguridad adicional
    client_max_body_size 10M;
    client_body_timeout 12;
    client_header_timeout 12;
    keepalive_timeout 15;
    send_timeout 10;

    # Prevenir acceso a archivos ocultos
    location ~ /\. {
        deny all;
        access_log off;
        log_not_found off;
    }

    # Manejo de errores personalizado
    error_page 401 /401.html;
    error_page 403 /403.html;
    error_page 404 /404.html;
    error_page 500 502 503 504 /50x.html;

    location = /401.html {
        root /var/www/corporativo/html;
        internal;
    }

    location = /403.html {
        root /var/www/corporativo/html;
        internal;
    }
```

```
 GNU nano 7.2                                        /etc/pam.d/nginx *
auth sufficient pam_sss.so
account sufficient pam_sss.so
```

```
 GNU nano 7.2                                        /etc/fstab *
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/74957338-4ad7-419b-aaa1-24a201e0883f / ext4 defaults 0 1
# /home was on /dev/sda3 during curtin installation
/dev/disk/by-uuid/6ba82b2f-8d5b-4b3a-ab6a-7f335c5f5615 /home ext4 defaults 0 1
# /boot/efi was on /dev/sda1 during curtin installation
/dev/disk/by-uuid/80EC-460F /boot/efi vfat defaults 0 1
/swap.img       none    swap    sw      0       0
//192.168.1.10/UbuntuBackups /mnt/windows/backups cifs credentials=/etc/samba/credentials,uid=1000,gid=1000,
//192.168.1.10/Documentos /mnt/windows/documentos cifs credentials=/etc/samba/credentials,uid=1000,gid=1000,
```

```
# Puerto personalizado
Port 2222

# Autenticación
PermitRootLogin no
PasswordAuthentication yes
PubkeyAuthentication yes

# Seguridad
Protocol 2
ClientAliveInterval 300
ClientAliveCountMax 2
MaxAuthTries 3
MaxSessions 5

# Usuarios permitidos
AllowUsers admin-corp

# Cipher seguros
KexAlgorithms curve25519-sha256@libssh.org
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

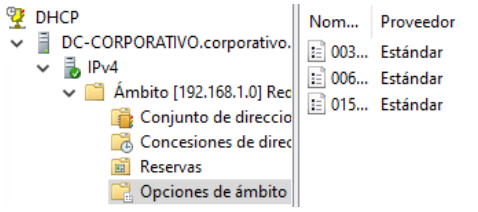
```
[Global]
   workgroup = WORKGROUP
   server string = Servidor Corporativo
   security = user

[Corporativo]
   comment = Recursos Corporativos Completos
   path = /srv/corporativo
   browseable = yes
   read only = no
   valid users = @admin-corp
   create mask = 0664
   directory mask = 0775
   force group = admin-corp

[RRHH]
   comment = Departamento Recursos Humanos
   path = /srv/corporativo/departamentos/rrhh
   browseable = yes
   read only = no
   valid users = @admin-corp
   create mask = 0660
   directory mask = 0770

[IT]
   comment = Departamento Tecnologías
   path = /srv/corporativo/departamentos/it
   browseable = yes
   read only = no
   valid users = @admin-corp
   create mask = 0660
   directory mask = 0770
```

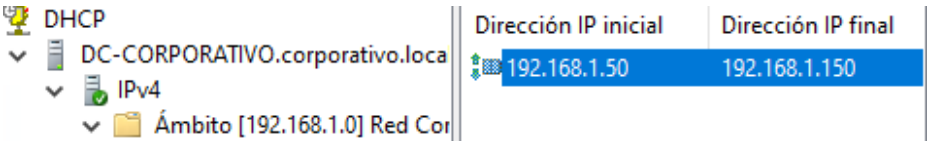
```
 GNU nano 7.2                                /etc/zabbix/zabbix_agent2.conf
Server=192.168.1.10
```

```
 GNU nano 7.2                                /etc/zabbix/zabbix_agent2.conf
ServerActive=192.168.1.10
```

```
 GNU nano 7.2                                /etc/zabbix/zabbix_agent2.conf

Hostname=servidor-corporativo
```

- Windows server 2022






```
PS C:\Users\Administrador> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
-------------                --------- ------- ---------------
Ethernet 2                           5 IPv4    {192.168.1.10, 127.0.0.1}
Ethernet 2                           5 IPv6    {::1}
Loopback Pseudo-Interface 1          1 IPv4    {}
Loopback Pseudo-Interface 1          1 IPv6    {}
```

```
PS C:\Users\Administrador> Get-DnsServerZone

ZoneName                  ZoneType      IsAutoCreated  IsDsIntegrated  IsReverseLookupZone
--------                  --------      -------------  --------------  -------------------
0.in-addr.arpa            Primary       True           False           True
1.168.192.in-addr.arpa    Primary       False          True            True
127.in-addr.arpa          Primary       True           False           True
255.in-addr.arpa          Primary       True           False           True
corporativo.local         Primary       False          True            False
TrustAnchors              Primary       False          True            False
```

```
PS C:\Users\Administrador> Get-SmbShare

Name      ScopeName Path                                        Description
----      --------- ----                                        -----------
ADMIN$    *         C:\Windows                                  Admin remota
C$        *         C:\                                         Recurso predeterminado
Finanzas  *         C:\Corporativo\Departamentos\Finanzas
IPC$      *                                                     IPC remota
IT        *         C:\Corporativo\Departamentos\IT
NETLOGON  *         C:\Windows\SYSVOL\sysvol\corporativo.local\SCRIPTS Recurso compartido del servidor de inicio de sesi¢n
RRHH      *         C:\Corporativo\Departamentos\RRHH
SYSVOL    *         C:\Windows\SYSVOL\sysvol                    Recurso compartido del servidor de inicio de sesi¢n
```

```
PS C:\Users\Administrador> New-Item -Path "C:\Corporativo" -ItemType Directory
New-Item -Path "C:\Corporativo\Departamentos" -ItemType Directory
New-Item -Path "C:\Corporativo\Departamentos\RRHH" -ItemType Directory
New-Item -Path "C:\Corporativo\Departamentos\IT" -ItemType Directory
New-Item -Path "C:\Corporativo\Departamentos\Finanzas" -ItemType Directory
New-Item -Path "C:\Corporativo\Departamentos\Ventas" -ItemType Directory
New-Item -Path "C:\Corporativo\RecursosComunes" -ItemType Directory


    Directorio: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        23/11/2025      5:25                Corporativo


    Directorio: C:\Corporativo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        23/11/2025      5:25                Departamentos


    Directorio: C:\Corporativo\Departamentos


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        23/11/2025      5:25                RRHH
d-----        23/11/2025      5:25                IT
d-----        23/11/2025      5:25                Finanzas
d-----        23/11/2025      5:25                Ventas


    Directorio: C:\Corporativo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        23/11/2025      5:25                RecursosComunes
```

```
PS C:\users\Administrador> auditpol /get /category:*
Directiva de auditor¡a del sistema

Categor¡a o subcategor¡a                    Configuraci¢n
Sistema
  Extensi¢n del sistema de seguridad        Sin auditor¡a
  Integridad del sistema                    Aciertos y errores
  Controlador IPsec                         Sin auditor¡a
  Otros eventos de sistema                  Aciertos y errores
  Cambio de estado de seguridad             Aciertos
Inicio/cierre de sesi¢n
  Inicio de sesi¢n                          Aciertos y errores
  Cerrar sesi¢n                             Aciertos
  Bloqueo de cuenta                         Aciertos
  Modo principal de IPsec                   Sin auditor¡a
  Modo r pido de IPsec                      Sin auditor¡a
  Modo extendido de IPsec                   Sin auditor¡a
  Inicio de sesi¢n especial                 Aciertos
  Otros eventos de inicio y cierre de sesi¢nSin auditor¡a
  Servidor de directivas de redes           Aciertos y errores
  Notificaciones de usuario o dispositivo   Sin auditor¡a
  Pertenencia a grupos                      Sin auditor¡a
Acceso de objetos
  Sistema de archivos                       Sin auditor¡a
  Registro                                  Sin auditor¡a
  Objeto de kernel                          Sin auditor¡a
  SAM                                       Sin auditor¡a
  Servicios de certificaci¢n                Sin auditor¡a
  Aplicaci¢n generada                       Sin auditor¡a
  Manipulaci¢n de identificadores           Sin auditor¡a
  Recurso compartido de archivos            Sin auditor¡a
  Colocaci¢n de paquetes de Plataforma de filtradoSin auditor¡a
  Conexi¢n de Plataforma de filtrado        Sin auditor¡a
  Otros eventos de acceso a objetos         Sin auditor¡a
  Recurso compartido de archivos detalladosSin auditor¡a
  Almacenamiento extra¡ble                  Sin auditor¡a
  Almacenamiento provisional de directiva centralSin auditor¡a
Uso de privilegios
  Uso de privilegio no confidencial         Sin auditor¡a
  Otros eventos de uso de privilegio        Sin auditor¡a
  Uso de privilegio confidencial            Sin auditor¡a
Seguimiento detallado
  Creaci¢n del proceso                      Sin auditor¡a
  Finalizaci¢n del proceso                  Sin auditor¡a
  Actividad DPAPI                           Sin auditor¡a
  Eventos de RPC                            Sin auditor¡a
  Eventos Plug and Play                     Sin auditor¡a
  Eventos de ajuste de derecho de token     Sin auditor¡a
Cambio de plan
  Cambio en la directiva de auditor¡a       Aciertos
  Cambio de la directiva de autenticaci¢n   Aciertos
  Cambio de la directiva de autorizaci¢n    Sin auditor¡a
  Cambio de la directiva del nivel de reglas de MPSSVCSin auditor¡a
  Cambio de la directiva de Plataforma de filtradoSin auditor¡a
```

```
Administraci¢n de cuentas
  Administraci¢n de cuentas de equipo       Aciertos
  Administraci¢n de grupos de seguridad     Aciertos
  Administraci¢n de grupos de distribuci¢nSin auditor¡a
  Administraci¢n de grupos de aplicacionesSin auditor¡a
  Otros eventos de administraci¢n de cuentasSin auditor¡a
  Administraci¢n de cuentas de usuario      Aciertos
Acceso DS
  Acceso del servicio de directorio         Aciertos
  Cambios de servicio de directorio         Sin auditor¡a
  Replicaci¢n de servicio de directorio     Sin auditor¡a
  Replicaci¢n de servicio de directorio detalladaSin auditor¡a
Inicio de sesi¢n de la cuenta
  Operaciones de vales de servicio Kerberos  Aciertos
  Otros eventos de inicio de sesi¢n de cuentasSin auditor¡a
  Servicio de autenticaci¢n Kerberos        Aciertos
  Validaci¢n de credenciales                Aciertos
```

```
 GNU nano 7.2                                 /etc/krb5.conf *
[libdefaults]
        default_realm = CORPORATIVO.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
        ticket_lifetime = 24h
        renew_lifetime = 7d
        forwardable = true
        default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5
        default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5
        permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 arcfour-hmac-md5

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        rdns = false


# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true
udp_preference_limit = 0

[realms]
        CORPORATIVO.LOCAL = {
                kdc = dc-corporativo.corporativo.local
                admin_server = dc-corporativo.corporativo.local
                default_domain = corporativo.local
        }
```

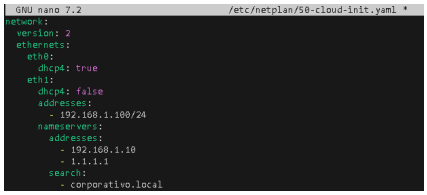
```
PS C:\Users\Administrador> $Action = New-ScheduledTaskAction -Execute "C:\Windows\System32\ws
$Trigger = New-ScheduledTaskTrigger -Daily -At "02:00"
Register-ScheduledTask -TaskName "Backup Ubuntu a Windows" -Action $Action -Trigger $Trigger

TaskPath                                 TaskName                                 State
--------                                 --------                                 -----
\                                        Backup Ubuntu a Windows                  Ready
```

```
PS C:\Users\Administrador> New-Item -Path "C:\Backups\Ubuntu" -ItemType Directory -Force
New-SmbShare -Name "UbuntuBackups" -Path "C:\Backups\Ubuntu" -FullAccess "administrador" -Rea


    Directorio: C:\Backups


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        04/12/2025      5:05                Ubuntu
```

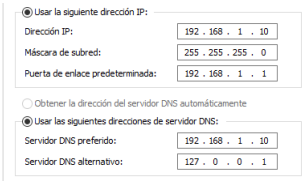
```
PS C:\Users\Administrador> New-Item -Path "C:\Corporativo\Documentos" -ItemType Directory -Fo
New-SmbShare -Name "Documentos" -Path "C:\Corporativo\Documentos" -FullAccess "Authenticated


    Directorio: C:\Corporativo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        04/12/2025      5:07                Documentos
```

✓ Configuración de dispositivos de red

- Ubuntu server 24.04.2



- Windows server 2022



✓ Características técnicas

- Ubuntu server 24.04.2

```
jose_manuel@servidor-corporativo:~$ sudo dpkg-reconfigure unattended-upgrades
sudo systemctl enable unattended-upgrades
Synchronizing state of unattended-upgrades.service with SysV service script with /usr/lib/systemd/systemd-sysv-
install.
Executing: /usr/lib/systemd/systemd-sysv-install enable unattended-upgrades
```

```
 GNU nano 7.2                          /etc/apt/apt.conf.d/20auto-upgrades *
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::Unattended-Upgrade "1";
APT::Periodic::AutocleanInterval "7";
```

```
jose_manuel@servidor-corporativo:~$ sudo realm join --user=administrador --verbose corporativo.local
 * Resolving: _ldap._tcp.corporativo.local
 * Performing LDAP DSE lookup on: 192.168.1.10
 * Successfully discovered: corporativo.local
Password for administrador:
 * Unconditionally checking packages
 * Resolving required packages
 * Joining using a truncated netbios name: SERVIDOR-CORPOR
 * LANG=C /usr/sbin/adcli join --verbose --domain corporativo.local --domain-realm CORPORATIVO.LOCAL --domain
```

```
jose_manuel@servidor-corporativo:~$ sudo apt install slapd ldap-utils -y
sudo dpkg-reconfigure slapd
```

```
jose_manuel@ubuntuserver:~$ sudo adduser admin-corp
info: Adding user `admin-corp' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `admin-corp' (1001) ...
info: Adding new user `admin-corp' (1001) with group `admin-corp (1001)' ...
info: Creating home directory `/home/admin-corp' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin-corp
Enter the new value, or press ENTER for the default
        Full Name []: jose manuel
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `admin-corp' to supplemental / extra groups `users' ...
info: Adding user `admin-corp' to group `users' ...
jose_manuel@ubuntuserver:~$ sudo usermod -aG sudo admin-corp
```

```
jose_manuel@servidor-corporativo:~$ sudo apt install mysql-server -y
sudo mysql_secure_installation
```

```
jose_manuel@servidor-corporativo:~$ sudo apt install htop nethogs nmon tree ncdu -y
```

```
 GNU nano 7.2                          /usr/local/bin/monitor-corporativo.sh *
#!/bin/bash
echo "=== MONITOREO CORPORATIVO ==="
echo "Uptime: $(uptime)"
echo "Espacio disco:"
df -h / /srv
echo "Memoria:"
free -h
echo "Conexiones SSH:"
who
```

```
jose_manuel@servidor-corporativo:~$ sudo mkdir -p /var/www/corporativo/html
sudo chown -R www-data:www-data /var/www/corporativo/html
sudo chmod -R 755 /var/www/corporativo/
```

```
jose_manuel@servidor-corporativo:~$ sudo apt update
sudo apt install nginx -y
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Obj:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:3 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Obj:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 8 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
nginx ya está en su versión más reciente (1.24.0-2ubuntu7.5).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 8 no actualizados.
jose_manuel@servidor-corporativo:~$ sudo systemctl enable nginx
sudo systemctl start nginx
Synchronizing state of nginx.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nginx
```

```
 GNU nano 7.2                                        /etc/hosts *
127.0.0.1 localhost
127.0.1.1 servidor-corporativo
```

```
jose_manuel@servidor-corporativo:~$ sudo mkdir -p /srv/corporativo/{departamentos,proyectos,recursos-compartidos,backups}
sudo mkdir -p /srv/corporativo/departamentos/{rrhh,it,finanzas,ventas,marketing}
jose_manuel@servidor-corporativo:~$ sudo chmod -R 775 /srv/corporativo/
sudo chown -R admin-corp:admin-corp /srv/corporativo/
```

```
jose_manuel@servidor-corporativo:~$ sudo smbpasswd -a admin-corp
```

```
jose_manuel@servidor-corporativo:~$ sudo apt install samba -y
sudo systemctl enable smbd
sudo systemctl start smbd
```

```
jose_manuel@servidor-corporativo:~$ sudo apt install fail2ban -y
sudo systemctl enable fail2ban
```

```
The key fingerprint is:
SHA256:6MZwoB9jBwqjtj/MvB+YNj1vWBQO1NptA/As2byxZxQ jose@corporativo.com
```

```
jose_manuel@servidor-corporativo:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80,443/tcp                 ALLOW IN    Anywhere
2222/tcp                   ALLOW IN    Anywhere
22/tcp                     DENY IN     Anywhere
80,443/tcp (v6)            ALLOW IN    Anywhere (v6)
2222/tcp (v6)              ALLOW IN    Anywhere (v6)
22/tcp (v6)                DENY IN     Anywhere (v6)
```

- Windows server 2022

```
PS C:\Users\Administrador> New-ADGroup -Name "GRP_RRHH" -GroupCategory Security -GroupScope Global -Path "OU=RRHH,OU=Departamentos,DC=corporativo,DC=local"
New-ADGroup -Name "GRP_IT" -GroupCategory Security -GroupScope Global -Path "OU=IT,OU=Departamentos,DC=corporativo,DC=local"
New-ADGroup -Name "GRP_Finanzas" -GroupCategory Security -GroupScope Global -Path "OU=Finanzas,OU=Departamentos,DC=corporativo,DC=local"
New-ADGroup -Name "GRP_Ventas" -GroupCategory Security -GroupScope Global -Path "OU=Ventas,OU=Departamentos,DC=corporativo,DC=local"

PS C:\Users\Administrador> New-ADGroup -Name "Administradores_Dominio" -GroupCategory Security -GroupScope Global -Description "Administradores del dominio"
```

```
PS C:\Users\Administrador> Import-Module ActiveDirectory

PS C:\Users\Administrador> New-ADOrganizationalUnit -Name "Departamentos" -Path "DC=corporativo,DC=local"
New-ADOrganizationalUnit -Name "Usuarios" -Path "DC=corporativo,DC=local"
New-ADOrganizationalUnit -Name "Equipos" -Path "DC=corporativo,DC=local"
New-ADOrganizationalUnit -Name "Servidores" -Path "DC=corporativo,DC=local"


PS C:\Users\Administrador> New-ADOrganizationalUnit -Name "RRHH" -Path "OU=Departamentos,DC=corporativo,DC=local"
New-ADOrganizationalUnit -Name "IT" -Path "OU=Departamentos,DC=corporativo,DC=local"
New-ADOrganizationalUnit -Name "Finanzas" -Path "OU=Departamentos,DC=corporativo,DC=local"
New-ADOrganizationalUnit -Name "Ventas" -Path "OU=Departamentos,DC=corporativo,DC=local"
```

```
PS C:\Users\Administrador> function New-CorporateUser {
    param($Name, $SamAccountName, $Department, $Password)

    New-ADUser -Name $Name `
               -SamAccountName $SamAccountName `
               -UserPrincipalName "$SamAccountName@corporativo.local" `
               -Path "OU=Usuarios,DC=corporativo,DC=local" `
               -AccountPassword (ConvertTo-SecureString $Password -AsPlainText -Force) `
               -Enabled $true `
               -Department $Department `
               -ChangePasswordAtLogon $false
}

PS C:\Users\Administrador> New-CorporateUser -Name "Ana García" -SamAccountName "agarcia" -Department "RRHH" -Password "P@sswOrd123"
New-CorporateUser -Name "Carlos López" -SamAccountName "clopez" -Department "IT" -Password "P@sswOrd123"
New-CorporateUser -Name "María Rodríguez" -SamAccountName "mrodriguez" -Department "Finanzas" -Password "P@sswOrd123"


PS C:\Users\Administrador> Add-ADGroupMember -Identity "GRP_RRHH" -Members "agarcia"
Add-ADGroupMember -Identity "GRP_IT" -Members "clopez"
Add-ADGroupMember -Identity "GRP_Finanzas" -Members "mrodriguez"
```

```
PS C:\Users\Administrador> Install-WindowsFeature -Name FS-FileServer -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}


PS C:\Users\Administrador> Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Administrador de recursos del servidor de...
```

```
PS C:\Users\Administrador> $Action = New-ScheduledTaskAction -Execute "C:\Windows\System32\ws
$Trigger = New-ScheduledTaskTrigger -Daily -At "02:00"
Register-ScheduledTask -TaskName "Backup Ubuntu a Windows" -Action $Action -Trigger $Trigger

TaskPath                                    TaskName                          State
--------                                    --------                          -----
\                                           Backup Ubuntu a Windows           Ready
```

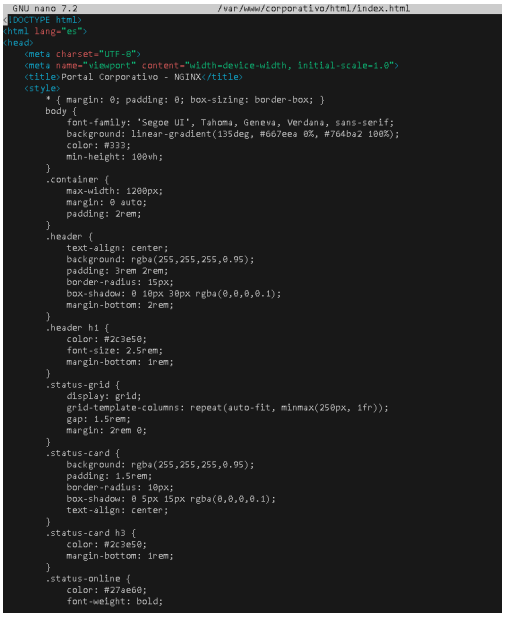
```
PS C:\Users\Administrador> New-Item -Path "C:\Backups\Ubuntu" -ItemType Directory -Force
New-SmbShare -Name "UbuntuBackups" -Path "C:\Backups\Ubuntu" -FullAccess "administrador" -Rea


    Directorio: C:\Backups


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        04/12/2025      5:05                Ubuntu
```

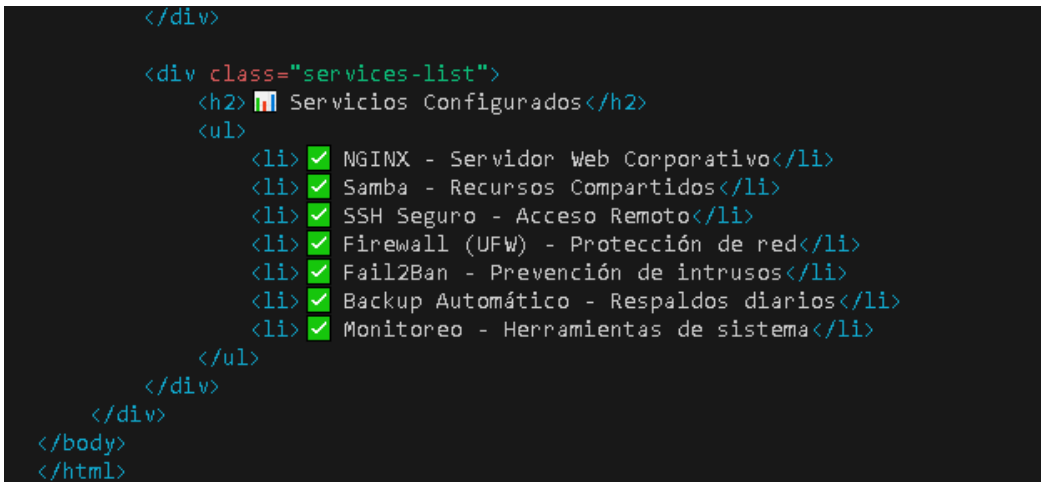
```
PS C:\Users\Administrador> New-Item -Path "C:\Corporativo\Documentos" -ItemType Directory -Fo
New-SmbShare -Name "Documentos" -Path "C:\Corporativo\Documentos" -FullAccess "Authenticated


    Directorio: C:\Corporativo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        04/12/2025      5:07                Documentos
```

```
PS C:\Scripts> $WSUSServer = "http://wsus-server.corporate.local:8530"

# Configurar registro
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Name "WUServer
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Name "WUStatus
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "UseWU
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "NoAut
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "AUOpt
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "Sched
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "Sched
```

✓ Código fuente (o web)

- Ubuntu server 24.04.2

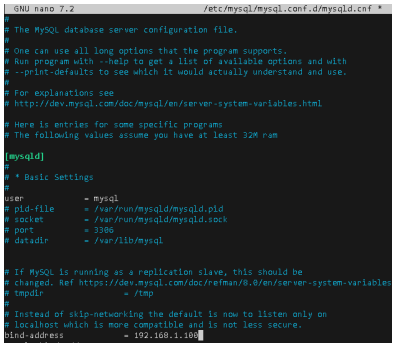




✓ Base de datos implementada

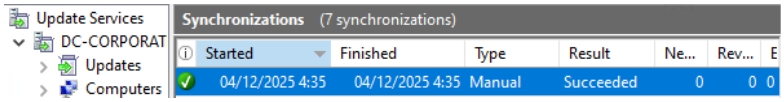
- Ubuntu server 24.04.2

```
jose_manuel@servidor-corporativo:~$ sudo apt install fail2ban -y
sudo systemctl enable fail2ban
```



✓ Política de seguridad implementada

- Ubuntu server 24.04.2




```
jose_manuel@servidor-corporativo:~$ sudo apt install mysql-server -y
sudo mysql_secure_installation
```

- Windows server 2022

```
PS C:\Scripts> $WSUSServer = "http://wsus-server.corporate.local:8530"

# Configurar registro
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Name "WUServer
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Name "WUStatus
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "UseWU
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "NoAut
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "AUOpt
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "Sched
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name "Sched
```

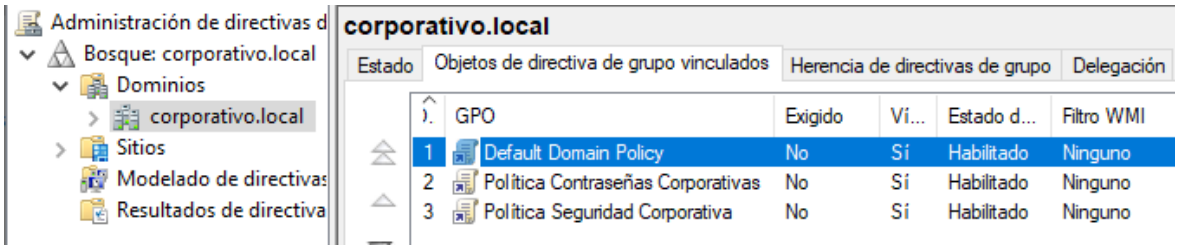
✓ Reglas (GPOs, Iptables, ACLs, ...) implementadas

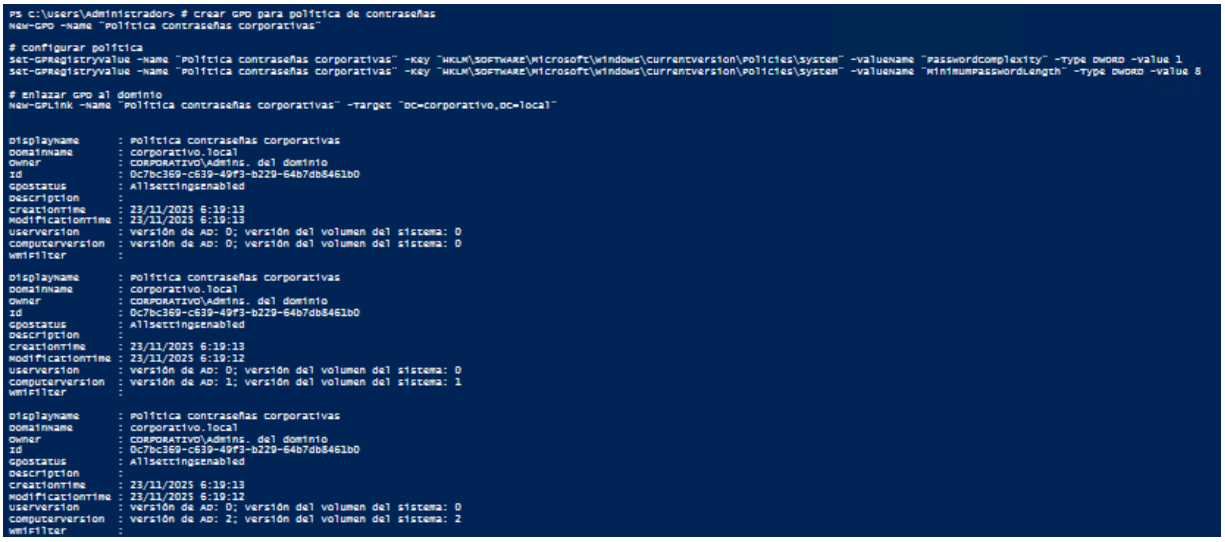
- Ubuntu server 24.04.2

```
admin-corp@servidor-corporativo:/usr/local/bin$ sudo ufw status numbered verbose
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80,443/tcp                 ALLOW IN    Anywhere
[ 2] 2222/tcp                   ALLOW IN    Anywhere
[ 3] 22/tcp                     DENY IN     Anywhere
[ 4] Nginx HTTP                 ALLOW IN    Anywhere
[ 5] Nginx HTTPS                ALLOW IN    Anywhere
[ 6] 80/tcp                     ALLOW IN    Anywhere
[ 7] 443/tcp                    ALLOW IN    Anywhere
[ 8] 139/tcp                    ALLOW IN    Anywhere
[ 9] 445/tcp                    ALLOW IN    Anywhere
[10] 22                         ALLOW IN    192.168.1.10               # SSH desde Windows
[11] 80                         ALLOW IN    192.168.1.10               # HTTP desde Windows
[12] 443                        ALLOW IN    192.168.1.10               # HTTPS desde Windows
[13] 3306                       ALLOW IN    192.168.1.10               # MySQL desde Windows
[14] 2222                       ALLOW IN    192.168.1.10               # SSH desde Windows
[15] Anywhere                   ALLOW IN    192.168.1.10
[16] 53/tcp                     ALLOW IN    Anywhere
[17] 53/udp                     ALLOW IN    Anywhere
[18] 53/tcp                     ALLOW OUT   Anywhere                   (out)
[19] 53/udp                     ALLOW OUT   Anywhere                   (out)
[20] 88/tcp                     ALLOW OUT   Anywhere                   (out)
[21] 88/udp                     ALLOW OUT   Anywhere                   (out)
[22] 135/tcp                    ALLOW OUT   Anywhere                   (out)
[23] 139/tcp                    ALLOW OUT   Anywhere                   (out)
[24] 389/tcp                    ALLOW OUT   Anywhere                   (out)
[25] 445/tcp                    ALLOW OUT   Anywhere                   (out)
[26] 464/tcp                    ALLOW OUT   Anywhere                   (out)
[27] 3268/tcp                   ALLOW OUT   Anywhere                   (out)
[28] 3389/tcp                   DENY IN     Anywhere
[29] 23/tcp                     DENY IN     Anywhere
[30] 21/tcp                     DENY IN     Anywhere
[31] 3306                       ALLOW IN    172.23.224.0/24
[32] 80,443/tcp (v6)            ALLOW IN    Anywhere (v6)
[33] 2222/tcp (v6)              ALLOW IN    Anywhere (v6)
[34] 22/tcp (v6)                DENY IN     Anywhere (v6)
[35] Nginx HTTP (v6)            ALLOW IN    Anywhere (v6)
[36] Nginx HTTPS (v6)           ALLOW IN    Anywhere (v6)
[37] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[38] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
[39] 139/tcp (v6)               ALLOW IN    Anywhere (v6)
[40] 445/tcp (v6)               ALLOW IN    Anywhere (v6)
[41] 53/tcp (v6)                ALLOW IN    Anywhere (v6)
[42] 53/udp (v6)                ALLOW IN    Anywhere (v6)
[43] 53/tcp (v6)                ALLOW OUT   Anywhere (v6)              (out)
[44] 53/udp (v6)                ALLOW OUT   Anywhere (v6)              (out)
[45] 88/tcp (v6)                ALLOW OUT   Anywhere (v6)              (out)
[46] 88/udp (v6)                ALLOW OUT   Anywhere (v6)              (out)
[47] 135/tcp (v6)               ALLOW OUT   Anywhere (v6)              (out)
[48] 139/tcp (v6)               ALLOW OUT   Anywhere (v6)              (out)
[49] 389/tcp (v6)               ALLOW OUT   Anywhere (v6)              (out)
[50] 445/tcp (v6)               ALLOW OUT   Anywhere (v6)              (out)
[51] 464/tcp (v6)               ALLOW OUT   Anywhere (v6)              (out)
[52] 3268/tcp (v6)              ALLOW OUT   Anywhere (v6)              (out)
[53] 3389/tcp (v6)              DENY IN     Anywhere (v6)
[54] 23/tcp (v6)                DENY IN     Anywhere (v6)
[55] 21/tcp (v6)                DENY IN     Anywhere (v6)
```

- Windows server 2022

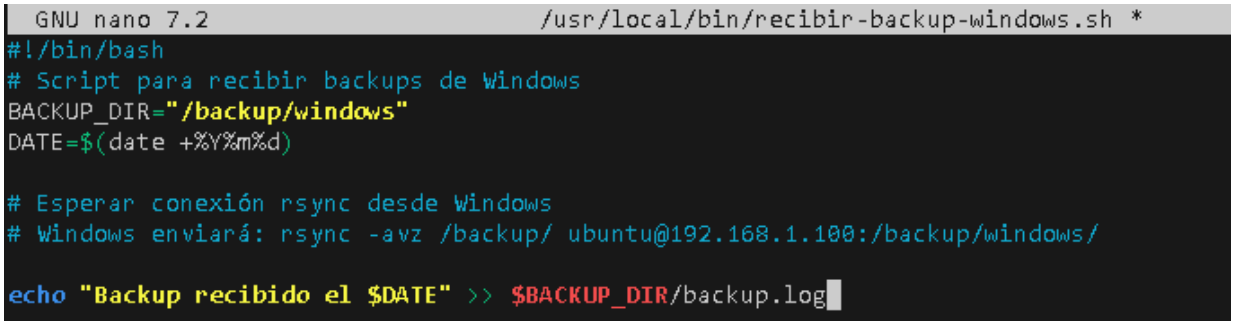
```
PS C:\Users\Administrador>
PS C:\Users\Administrador> New-GPO -Name "Politica Bloqueo Pantalla"
Set-GPRegistryValue -Name "Politica Bloqueo Pantalla" -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop" -ValueName "ScreenSaveTimeOut" -Type String -Value "900"
Set-GPRegistryValue -Name "Politica Bloqueo Pantalla" -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop" -ValueName "ScreenSaverIsSecure" -Type String -Value "1"


DisplayName      : Politica Bloqueo Pantalla
DomainName       : corporativo.local
Owner            : CORPORATIVO\Admins. del dominio
Id               : 549f8494-58cc-4d63-8bb3-bd5e8e5b6bea
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 23/11/2025 6:20:54
ModificationTime : 23/11/2025 6:20:54
UserVersion      : Versión de AD: 0; versión del volumen del sistema: 0
ComputerVersion  : Versión de AD: 0; versión del volumen del sistema: 0
WmiFilter        :

DisplayName      : Politica Bloqueo Pantalla
DomainName       : corporativo.local
Owner            : CORPORATIVO\Admins. del dominio
Id               : 549f8494-58cc-4d63-8bb3-bd5e8e5b6bea
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 23/11/2025 6:20:54
ModificationTime : 23/11/2025 6:20:54
UserVersion      : Versión de AD: 0; versión del volumen del sistema: 0
ComputerVersion  : Versión de AD: 1; versión del volumen del sistema: 1
WmiFilter        :

DisplayName      : Politica Bloqueo Pantalla
DomainName       : corporativo.local
Owner            : CORPORATIVO\Admins. del dominio
Id               : 549f8494-58cc-4d63-8bb3-bd5e8e5b6bea
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 23/11/2025 6:20:54
ModificationTime : 23/11/2025 6:20:54
UserVersion      : Versión de AD: 0; versión del volumen del sistema: 0
ComputerVersion  : Versión de AD: 2; versión del volumen del sistema: 2
WmiFilter        :
```



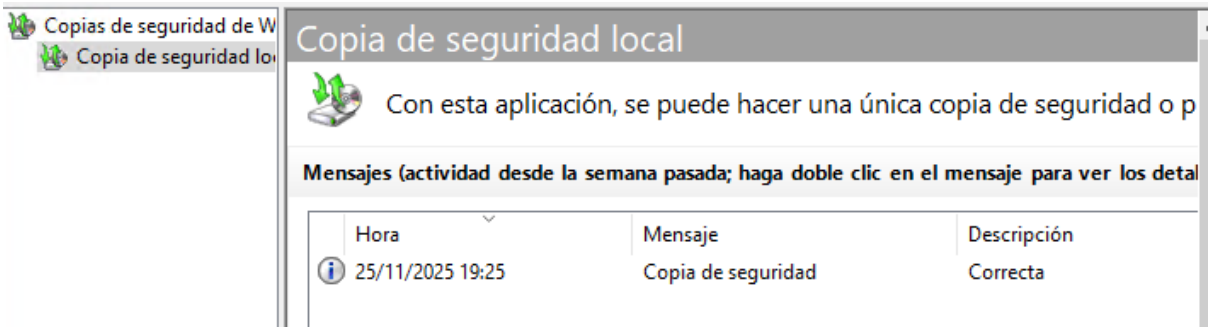


✓ Copia de seguridad del sitio web

- Ubuntu server 24.04.2



- Windows server 2022



- En general:
  - ✓ Texto: Descripción de las implementaciones realizadas

WINDOWS SERVER 2022 - IMPLEMENTACIONES

1. INFRAESTRUCTURA DE DIRECTORIO Y RED

- Active Directory Domain Services
- Dominio: corporativo.local
- Usuarios/grupos corporativos estructurados por departamentos
- Políticas de contraseñas y seguridad

DNS Server Corporativo

- Zona primaria corporativo.local
- Registros A/CNAME para todos los servicios
- Zona inversa para resolución PTR
- Integración automática con AD

DHCP Server

- Ámbito: 192.168.1.50-150/24
- Reservas para servidores
- Opciones: DNS (192.168.1.10), Gateway (192.168.1.1)

- Autorizado en Active Directory

2. SERVICIOS DE ARCHIVOS Y RECURSOS

- File Server con SMB
- Recursos compartidos por departamentos:
- \SRV-CORP\RRHH - Recursos Humanos
- \SRV-CORP\IT - Departamento TI
- \SRV-CORP\Finanzas - Área financiera
- \SRV-CORP\Documentos - Documentación general
- Permisos NTFS basados en grupos AD
- Cuotas de almacenamiento configuradas
- Print Server (configurable según necesidades)

3. GESTIÓN Y CONTROL

- Group Policy Objects (GPO)
- Política de seguridad base corporativa
- Configuración de escritorio estándar
- Restricciones de software y acceso
- Scripts de inicio/logon
- Windows Server Update Services (WSUS)
- Actualizaciones centralizadas para clientes Windows
- Aprobación controlada de patches
- Reportes de cumplimiento
- Ahorro de ancho de banda

4. SEGURIDAD Y AUDITORÍA

- Políticas de auditoría habilitadas

- Windows Defender configurado
- Event logging centralizado
- Backup Windows Server programado

UBUNTU SERVER 24.04 - IMPLEMENTACIONES

1. INFRAESTRUCTURA WEB Y APLICACIONES

- NGINX Web Server
- Portal corporativo: https://portal.corporativo.local
- Sitio público y área segura
- Configuración optimizada para performance
- Headers de seguridad implementados
- Integración con Active Directory
- Unión al dominio mediante realmd y sssd
- Autenticación PAM para servicios
- Mapeo de usuarios/grupos AD
- Single Sign-On para aplicaciones web
- Base de Datos MySQL/MariaDB
- Instancia corporativa para aplicaciones
- Usuarios gestionados por AD
- Backups automáticos configurados
- Monitoreo de performance

2. SEGURIDAD AVANZADA

- Firewall UFW configurado
- Reglas específicas por servicio

- Acceso restringido por red interna
- Logging de intentos de acceso
- Fail2Ban para protección SSH
- Protección contra fuerza bruta
- Múltiples jails configurados
- Notificaciones de bloqueo
- Autenticación SSH segura
- Puerto personalizado (2222)
- Autenticación por clave pública
- Root login deshabilitado
- Tiempos de sesión limitados

3. MONITOREO Y MANTENIMIENTO

- Zabbix Agent 2 instalado
- Monitoreo de recursos del servidor
- Alertas configurables
- Dashboards de estado
- Actualizaciones automáticas
- unattended-upgrades configurado
- Ventana de mantenimiento: 04:00 AM
- Reinicios automáticos controlados
- Sistema de backups
- Scripts personalizados para /etc, /home, /var/www
- Programación vía cron
- Retención: 7 días

- Destino: Directorio local + Windows Server

4. SERVICIOS ADICIONALES

- Samba para integración AD
- Compatibilidad con recursos compartidos Windows
- Autenticación transparente
- Permisos unificados
- Docker Engine (opcional)
- Plataforma para contenedores
- Docker Compose para orquestación
- Usuarios AD en grupo docker

INTEGRACIÓN ENTRE PLATAFORMAS

1. AUTENTICACIÓN UNIFICADA

- Usuarios AD autentican en Ubuntu
- Grupos AD controlan acceso a recursos
- Credenciales sincronizadas
- Políticas de contraseñas aplicadas desde AD

2. DNS INTEGRADO

- Windows Server como DNS primario
- Ubuntu Server registrado en DNS
- Resolución bidireccional funcional
- Nombres de servicio estandarizados

3. RECURSOS COMPARTIDOS CRUZADOS

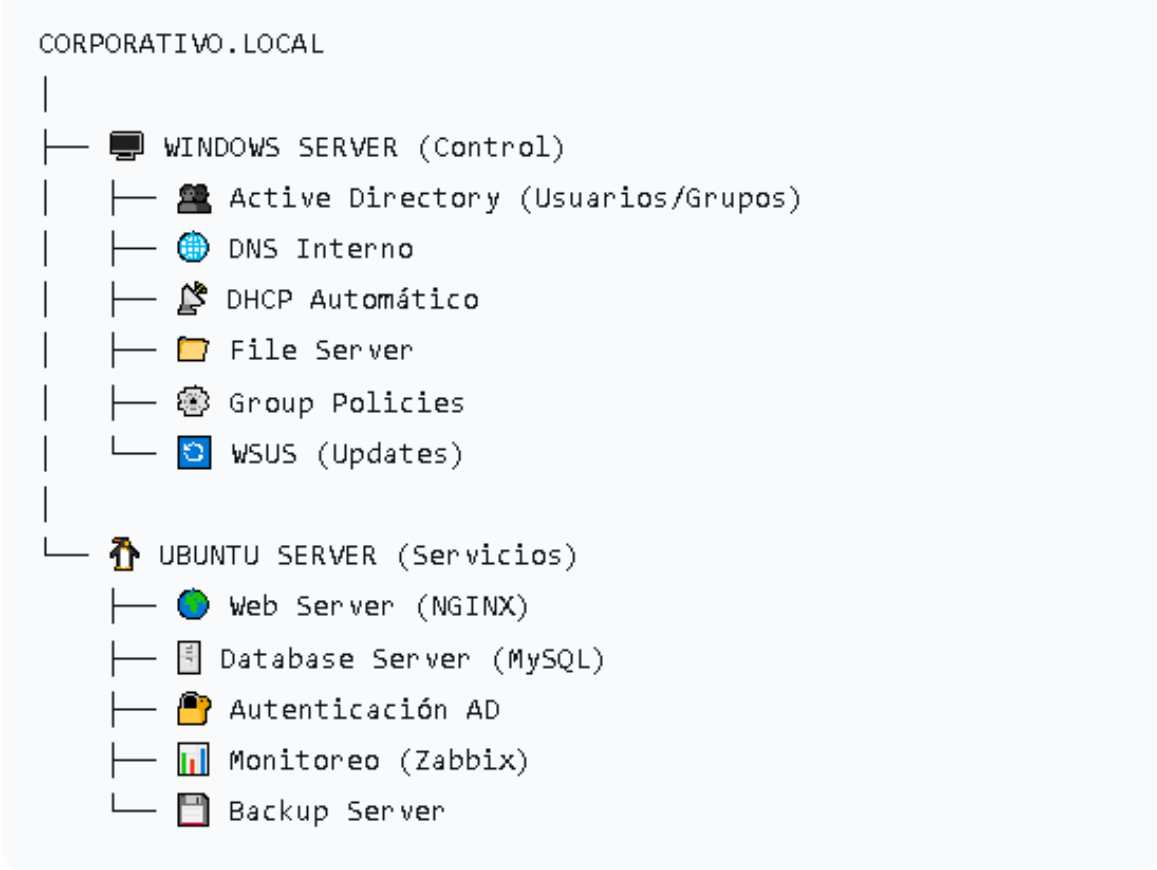
- Ubuntu → Windows: Montaje de shares SMB

- Windows → Ubuntu: Acceso web y servicios
- Permisos consistentes entre plataformas
- Auditoría de acceso centralizada

4. BACKUP CRUZADO

- Ubuntu respalda configuraciones críticas a Windows
- Windows respalda datos AD a Ubuntu
- Redundancia geográfica implícita
- Procedimientos de restauración documentados

- Manuales finales:



- Ubuntu server 24.04.2 / Windows server 2022

```
#!/bin/bash
# integracion-test.sh
echo "=== PRUEBA INTEGRACIÓN WINDOWS-UBUNTU ==="

echo "1. DNS cruzado:"
echo "   Windows -> Ubuntu:"
nslookup ubuntu.corporativo.local 192.168.1.10 2>/dev/null | grep -A1 "Name:"
echo "   Ubuntu -> Windows:"
nslookup dc-corporativo.corporativo.local 2>/dev/null | grep -A1 "Name:"

echo -e "\n2. Autenticación AD:"
echo "   Desde Ubuntu, usuario Windows:"
getent passwd administrador@corporativo.local &> /dev/null && echo "   ✅ Usuario AD accesible" || echo "   ❌ Error AD"

echo -e "\n3. Recursos compartidos:"
echo "   Montajes Windows en Ubuntu:"
mount | grep -E "192.168.1.10|//dc-corporativo" && echo "   ✅ Recursos montados" || echo "   ❌ No hay montajes"

echo -e "\n4. Servicios web:"
echo "   Windows puede acceder a Ubuntu web:"
curl -s -o /dev/null -w "   Código: %{http_code}\n" -k https://ubuntu.corporativo.local 2>/dev/null || echo "   ❌ No accesible"

echo -e "\n5. Base de datos:"
if command -v mysql &> /dev/null; then
    echo "   Ubuntu DB accesible desde red:"
    mysql -h 192.168.1.100 -u root -p -e "SELECT 1;" 2>/dev/null && echo "   ✅ MySQL accesible" || echo "   ❌ MySQL no accesible"
fi

echo -e "\n=== FIN PRUEBA INTEGRACIÓN ==="
```

- Ubuntu server 24.04.2

```
#!/bin/bash
# Guardar como: /usr/local/bin/verificacion-ubuntu.sh
# Ejecutar con: sudo verificacion-ubuntu.sh

echo "=========================================="
echo "  VERIFICACIÓN COMPLETA UBUNTU SERVER"
echo "=========================================="

# 1. VERIFICAR SISTEMA BÁSICO
echo -e "\n1. INFORMACIÓN DEL SISTEMA:"
echo "   Hostname: $(hostname)"
echo "   Dominio: $(hostname -d)"
echo "   Ubuntu: $(lsb_release -d | cut -f2)"
echo "   Kernel: $(uname -r)"
echo "   Uptime: $(uptime -p)"

# 2. VERIFICAR CONEXIÓN AL DOMINIO AD
echo -e "\n2. ACTIVE DIRECTORY INTEGRATION:"
if command -v realm &> /dev/null; then
    realm list 2>/dev/null && echo "   ✅ Unido al dominio" || echo "   ❌ No unido al dominio"
else
    echo "   ⚠️  Realm no instalado"
fi

# Verificar usuarios AD
echo "   Usuarios AD disponibles:"
getent passwd | grep "@corporativo.local" | cut -d: -f1 | head -3 | xargs -I{} echo "     - {}"
```

```
# 5. VERIFICAR SERVICIOS WEB
echo -e "\n5. SERVICIOS WEB:"
# NGINX
if systemctl is-active --quiet nginx; then
    echo "   ✅ NGINX funcionando"
    echo "   Sitios configurados:"
    nginx -T 2>/dev/null | grep "server_name " | grep -v "#" | awk '{print "     - "$2}' | sort | uniq
else
    echo "   ❌ NGINX no activo"
fi

# Apache (si instalado)
if systemctl list-unit-files | grep -q "apache2.service"; then
    if systemctl is-active --quiet apache2; then
        echo "   ✅ Apache funcionando"
    else
        echo "   ❌ Apache inactivo"
    fi
fi

# 6. VERIFICAR BASES DE DATOS
echo -e "\n6. BASES DE DATOS:"
# MySQL/MariaDB
if systemctl is-active --quiet mysql; then
    echo "   ✅ MySQL/MariaDB funcionando"
    echo "   Bases de datos:"
    mysql -e "SHOW DATABASES;" 2>/dev/null | grep -v "Database\|information_schema\|mysql\|performance_schema" | xargs -I{} echo "
fi

# PostgreSQL
if systemctl is-active --quiet postgresql; then
    echo "   ✅ PostgreSQL funcionando"
fi
```

```
# 9. VERIFICAR MONITOREO
echo -e "\n9. MONITOREO:"
# Zabbix Agent
if systemctl is-active --quiet zabbix-agent2; then
    echo "   ✅ Zabbix Agent funcionando"
fi

# Logs recientes de errores
echo "   Errores recientes en logs:"
journalctl --since "1 hour ago" -p err | tail -3 | while read line; do
    echo "     - $(echo $line | cut -d' ' -f6- | cut -c1-50)..."
done

# 10. VERIFICAR BACKUPS
echo -e "\n10. BACKUPS:"
if crontab -l 2>/dev/null | grep -q "backup"; then
    echo "   ✅ Backup programado en cron"
else
    echo "   ❌ No hay backups programados"
fi

# Verificar directorios de backup
backup_dirs=("/backup" "/var/backup" "/mnt/backup")
for dir in "${backup_dirs[@]}"; do
    if [ -d "$dir" ]; then
        count=$(find "$dir" -type f -name "*.tar.gz" -o -name "*.zip" 2>/dev/null | wc -l)
        if [ $count -gt 0 ]; then
            echo "   📁 $dir: $count archivos de backup"
        fi
    fi
done

echo -e "\n=========================================="
echo "  VERIFICACIÓN COMPLETADA"
echo "=========================================="
```

```
# 3. VERIFICAR SERVICIOS CRÍTICOS
echo -e "\n3. SERVICIOS CRÍTICOS:"
services=("sssd" "ssh" "nginx" "mysql" "postgresql" "apache2" "zabbix-agent")
for service in "${services[@]}"; do
    if systemctl list-unit-files | grep -q "^$service.service"; then
        if systemctl is-active --quiet $service; then
            echo "   ✅ $service: ACTIVO"
        else
            echo "   ❌ $service: INACTIVO"
        fi
    fi
done

# 4. VERIFICAR RED Y CONECTIVIDAD
echo -e "\n4. CONFIGURACIÓN DE RED:"
echo "   IP: $(hostname -I)"
echo "   DNS: $(grep nameserver /etc/resolv.conf | head -1 | awk '{print $2}')"
echo "   Gateway: $(ip route | grep default | awk '{print $3}')"

# Probar conectividad a Windows
echo -e "\n   Conectividad Windows Server:"
if ping -c 2 192.168.1.10 &> /dev/null; then
    echo "   ✅ Windows Server alcanzable"

    # Probar puertos comunes de Windows
    ports=(53 389 445 3389)
    for port in "${ports[@]}"; do
        timeout 1 bash -c "echo >/dev/tcp/192.168.1.10/$port" 2>/dev/null && \
        echo "     Puerto $port: ABIERTO" || \
        echo "     Puerto $port: CERRADO"
    done
else
    echo "   ❌ Windows Server inalcanzable"
fi


# 7. VERIFICAR SEGURIDAD
echo -e "\n7. SEGURIDAD:"
# Firewall
if command -v ufw &> /dev/null; then
    ufw status | grep -q "active" && echo "   ✅ UFW ACTIVO" || echo "   ❌ UFW INACTIVO"
fi

# Fail2Ban
if systemctl is-active --quiet fail2ban; then
    echo "   ✅ Fail2Ban funcionando"
    echo "   Jails activos:"
    fail2ban-client status 2>/dev/null | grep "Jail list" | cut -d: -f2 | tr ',' '\n' | xargs -I{} echo "     - {}"
fi

# SSH
echo "   SSH en puerto: $(grep -i "^Port" /etc/ssh/sshd_config 2>/dev/null | awk '{print $2}' || echo '22')"

# 8. VERIFICAR ESPACIO EN DISCO
echo -e "\n8. ALMACENAMIENTO:"
df -h | grep -E "^(Filesystem|/dev/)" | while read line; do
    if [[ $line == Filesystem* ]]; then
        echo "   $line"
    else
        fs=$(echo $line | awk '{print $1}')
        size=$(echo $line | awk '{print $2}')
        used=$(echo $line | awk '{print $3}')
        avail=$(echo $line | awk '{print $4}')
        use=$(echo $line | awk '{print $5}')
        mount=$(echo $line | awk '{print $6}')

        if [[ $use =~ [0-9]+%$ ]]; then
            percent=${use%%%}
            if [ $percent -gt 90 ]; then
                color="❌"
            elif [ $percent -gt 70 ]; then
                color="⚠️ "
            else
                color="✅"
            fi
            echo "   $color $mount: $used/$size usados ($use) - $avail libres"
        fi
    fi
done
```

- Windows server 2022

```
# Guardar como: C:\Scripts\Verificacion-Windows.ps1
# Ejecutar como Administrador

Write-Host "========================================" -ForegroundColor Cyan
Write-Host "  VERIFICACIÓN COMPLETA WINDOWS SERVER" -ForegroundColor Cyan
Write-Host "========================================" -ForegroundColor Cyan

# 1. VERIFICAR SERVICIOS CRÍTICOS
Write-Host "`n1. SERVICIOS CRÍTICOS:" -ForegroundColor Yellow
$CriticalServices = @(
    @{Name="ADWS"; Display="Active Directory Web Services"},
    @{Name="DNS"; Display="DNS Server"},
    @{Name="DHCPServer"; Display="DHCP Server"},
    @{Name="Netlogon"; Display="Netlogon"},
    @{Name="KDC"; Display="Kerberos"},
    @{Name="W3SVC"; Display="IIS (si instalado)"},
    @{Name="Spooler"; Display="Print Spooler"}
)

foreach ($Service in $CriticalServices) {
    try {
        $Status = (Get-Service $Service.Name -ErrorAction Stop).Status
        $Color = if($Status -eq "Running"){"Green"}else{"Red"}
        Write-Host "   $($Service.Display): $Status" -ForegroundColor $Color
    } catch {
        Write-Host "   $($Service.Display): NO INSTALADO" -ForegroundColor Gray
    }
}

# 2. VERIFICAR ACTIVE DIRECTORY
Write-Host "`n2. ACTIVE DIRECTORY:" -ForegroundColor Yellow
try {
    $Domain = Get-ADDomain
    Write-Host "   Dominio: $($Domain.Name)" -ForegroundColor Green
    Write-Host "   Nivel funcional: $($Domain.DomainMode)" -ForegroundColor Green

    $Users = Get-ADUser -Filter * | Measure-Object
    $Computers = Get-ADComputer -Filter * | Measure-Object
    Write-Host "   Usuarios: $($Users.Count)" -ForegroundColor Green
    Write-Host "   Equipos: $($Computers.Count)" -ForegroundColor Green
} catch {
    Write-Host "   ERROR AD: $_" -ForegroundColor Red
}

# 3. VERIFICAR DNS
Write-Host "`n3. DNS SERVER:" -ForegroundColor Yellow
try {
    $Zones = Get-DnsServerZone | Where-Object {$_.ZoneName -ne "TrustAnchors"}
    Write-Host "   Zonas configuradas:" -ForegroundColor Green
    foreach ($Zone in $Zones) {
        Write-Host "     - $($Zone.ZoneName) ($($Zone.ZoneType))" -ForegroundColor Gray
    }

    # Probar resolución
    $Test1 = Resolve-DnsName "corporativo.local" -ErrorAction SilentlyContinue
    $Test2 = Resolve-DnsName "ubuntu.corporativo.local" -ErrorAction SilentlyContinue

    if ($Test1 -and $Test2) {
        Write-Host "   Resolución DNS: FUNCIONANDO" -ForegroundColor Green
    } else {
        Write-Host "   Resolución DNS: PROBLEMAS" -ForegroundColor Red
    }
} catch {
    Write-Host "   DNS no configurado" -ForegroundColor Red
}

# 4. VERIFICAR DHCP
Write-Host "`n4. DHCP SERVER:" -ForegroundColor Yellow
try {
    $Scopes = Get-DhcpServerv4Scope -ErrorAction Stop
    if ($Scopes) {
        Write-Host "   Ámbitos DHCP:" -ForegroundColor Green
        foreach ($Scope in $Scopes) {
            $Leases = Get-DhcpServerv4Lease -ScopeId $Scope.ScopeId -ErrorAction SilentlyContinue | Measure-Object
            Write-Host "     - $($Scope.Name): $($Scope.StartRange)-$($Scope.EndRange) ($($Leases.Count) leases)" -ForegroundColor Gray
        }
    } else {
        Write-Host "   No hay ámbitos DHCP" -ForegroundColor Yellow
    }
} catch {
    Write-Host "   DHCP no instalado/configurado" -ForegroundColor Gray
}


# 5. VERIFICAR RECURSOS COMPARTIDOS
Write-Host "`n5. RECURSOS COMPARTIDOS:" -ForegroundColor Yellow
$Shares = Get-SmbShare | Where-Object {$_.Name -notlike "*$"}
if ($Shares) {
    Write-Host "   Recursos disponibles:" -ForegroundColor Green
    foreach ($Share in $Shares) {
        Write-Host "     - $($Share.Name): $($Share.Path)" -ForegroundColor Gray
    }
} else {
    Write-Host "   No hay recursos compartidos" -ForegroundColor Yellow
}

# 6. VERIFICAR WSUS
Write-Host "`n6. CONFIGURACIÓN WINDOWS UPDATE:" -ForegroundColor Yellow
$wuServer = Get-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Name "WUServer" -ErrorAction SilentlyContinue
if ($wuServer) {
    Write-Host "   WSUS Server: $($wuServer.WUServer)"
} else {
    Write-Host "   WSUS: NO CONFIGURADO (usando Microsoft)" -ForegroundColor Red
}
Write-Host ""

# 7. VERIFICAR CONECTIVIDAD CON UBUNTU
Write-Host "`n7. CONECTIVIDAD UBUNTU:" -ForegroundColor Yellow
if (Test-Connection -ComputerName "192.168.1.100" -Count 2 -Quiet) {
    Write-Host "   Ubuntu Server: ACCESIBLE" -ForegroundColor Green

    # Probar servicios comunes
    $Ports = @(2222, 8080, 443, 3306)
    foreach ($Port in $Ports) {
        $Result = Test-NetConnection -ComputerName "192.168.1.100" -Port $Port -WarningAction SilentlyContinue
        if ($Result.TcpTestSucceeded) {
            Write-Host "     Puerto $Port : ABIERTO" -ForegroundColor Green
        } else {
            Write-Host "     Puerto $Port : CERRADO" -ForegroundColor Yellow
        }
    }
} else {
    Write-Host "   Ubuntu Server: INACCESIBLE" -ForegroundColor Red
}

# 8. VERIFICAR ESPACIO EN DISCO
Write-Host "`n8. ESPACIO EN DISCO:" -ForegroundColor Yellow
Get-WmiObject Win32_LogicalDisk | Where-Object {$_.DriveType -eq 3} | ForEach-Object {
    $FreeGB = [math]::Round($_.FreeSpace / 1GB, 2)
    $TotalGB = [math]::Round($_.Size / 1GB, 2)
    $PercentFree = [math]::Round(($FreeGB / $TotalGB) * 100, 2)

    $Color = if ($PercentFree -gt 20) {"Green"} elseif ($PercentFree -gt 10) {"Yellow"} else {"Red"}

    Write-Host "   $($_.DeviceID): $FreeGB GB libres de $TotalGB GB ($PercentFree%)" -ForegroundColor $Color
}

# 9. VERIFICAR EVENTOS CRÍTICOS (últimas 24h)
Write-Host "`n9. EVENTOS CRÍTICOS (24h):" -ForegroundColor Yellow
$CriticalEvents = Get-EventLog -LogName System -EntryType Error -After (Get-Date).AddHours(-24) | Select-Object -First 3
if ($CriticalEvents) {
    Write-Host "   Eventos encontrados:" -ForegroundColor Red
    foreach ($Event in $CriticalEvents) {
        Write-Host "     - $($Event.TimeGenerated): $($Event.Message.Substring(0, [Math]::Min(50, $Event.Message.Length)))..." -ForegroundColor Gray
    }
} else {
    Write-Host "   Sin eventos críticos" -ForegroundColor Green
}

Write-Host "`n========================================" -ForegroundColor Cyan
Write-Host "  VERIFICACIÓN COMPLETADA" -ForegroundColor Cyan
Write-Host "========================================" -ForegroundColor Cyan
```

4 Seguimiento y control

4.1 Valoración del proyecto

- Definir medios de evaluar el proyecto.

- Ubuntu server 24.04.2

Integración Active Directory

Verificar unión al dominio

```
admin-corp@servidor-corporativo:/usr/local/bin$ sudo realm list
corporativo.local
  type: kerberos
  realm-name: CORPORATIVO.LOCAL
  domain-name: corporativo.local
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@corporativo.local
  login-policy: allow-realm-logins
```

Autenticación AD

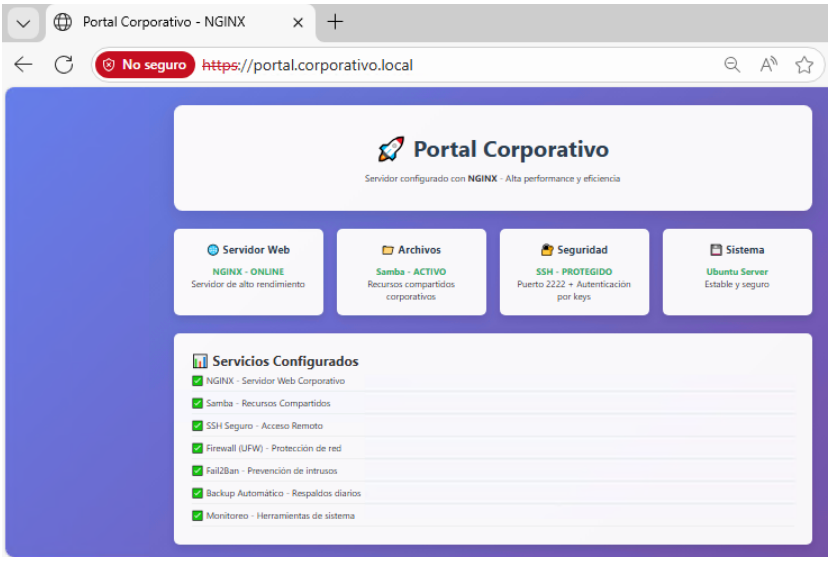
```
admin-corp@servidor-corporativo:/usr/local/bin$ su - administrador@corporativo.local
Password:
Creating directory '/home/administrador@corporativo.local'.
groups: cannot find name for group ID 1345800513
administrador@corporativo.local@servidor-corporativo:~$
```

Portal Web Corporativo

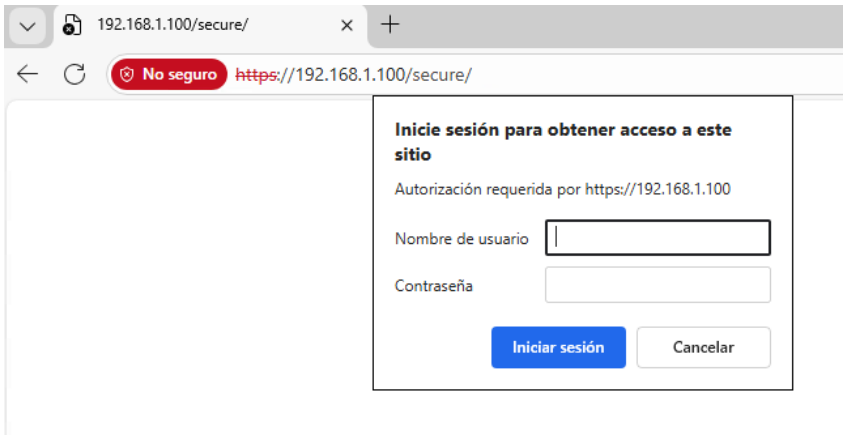
Estado del servicio

```
admin-corp@servidor-corporativo:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-12-12 05:11:40 UTC; 29min ago
```

Página pública

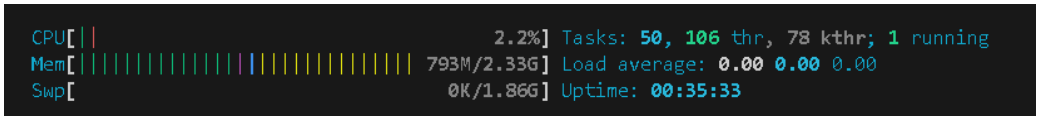


Login AD requerido

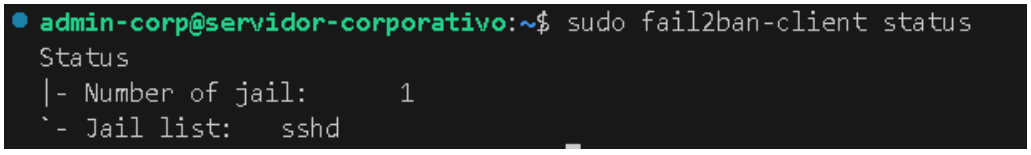


Monitoreo y Seguridad

Estado del sistema



Fail2ban estado



- Windows server 2022

Active Directory

Verificar dominio

```
PS C:\Users\Administrador> Get-ADDomain | Format-List Name, Forest, DomainMode


Name       : corporativo
Forest     : corporativo.local
DomainMode : Windows2016Domain
```

Usuarios y Grupos Corporativos

Estructura organizativa

```
PS C:\Users\Administrador> Get-ADOrganizationalUnit -Filter * | Format-Table Name, Disting

Name               DistinguishedName
----               -----------------
Domain Controllers OU=Domain Controllers,DC=corporativo,DC=local
Departamentos      OU=Departamentos,DC=corporativo,DC=local
Usuarios           OU=Usuarios,DC=corporativo,DC=local
Equipos            OU=Equipos,DC=corporativo,DC=local
Servidores         OU=Servidores,DC=corporativo,DC=local
RRHH               OU=RRHH,OU=Departamentos,DC=corporativo,DC=local
IT                 OU=IT,OU=Departamentos,DC=corporativo,DC=local
Finanzas           OU=Finanzas,OU=Departamentos,DC=corporativo,DC=local
Ventas             OU=Ventas,OU=Departamentos,DC=corporativo,DC=local
```

Usuarios por departamento

```
PS C:\Users\Administrador> Get-ADUser -Filter * -Properties Department |
    Group-Object Department |
    Select-Object Name, Count |
    Format-Table

Name      Count
----      -----
               3
RRHH           1
IT             1
Finanzas       1
Ventas         1
```

DNS

Zonas DNS

```
PS C:\Users\Administrador> Get-DnsServerZone | Where-Object {$_.ZoneName -ne "TrustAnchors
    Format-Table ZoneName, ZoneType

ZoneName              ZoneType
--------              --------
0.in-addr.arpa        Primary
1.168.192.in-addr.arpa Primary
127.in-addr.arpa      Primary
255.in-addr.arpa      Primary
corporativo.local     Primary
```

Resolución de servicios

```
PS C:\Users\Administrador> Resolve-DnsName "ubuntu.corporativo.local"
Resolve-DnsName "portal.corporativo.local"

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
ubuntu.corporativo.local                       A      3600  Answer     192.168.1.100
portal.corporativo.local                       A      3600  Answer     192.168.1.100
```

Recursos compratidos

Recursos compartidos

```
PS C:\Users\Administrador> Get-SmbShare | Where-Object {$_.Name -notlike "*$*"} |
    Format-Table Name, Path, CurrentUsers

Name                 Path                                                CurrentUsers
----                 ----                                                ------------
Documentos           C:\Corporativo\Documentos                                      0
Finanzas             C:\Corporativo\Departamentos\Finanzas                          0
IT                   C:\Corporativo\Departamentos\IT                                0
NETLOGON             C:\Windows\SYSVOL\sysvol\corporativo.local\SCRIPTS              0
RRHH                 C:\Corporativo\Departamentos\RRHH                              0
SYSVOL               C:\Windows\SYSVOL\sysvol                                       0
UbuntuBackups        C:\Backups\Ubuntu                                              0
UpdateServicesPackages C:\WSUS\UpdateServicesPackages                               0
Users                C:\Users                                                       0
WsusContent          C:\WSUS\WsusContent                                            0
WSUSTemp             C:\Program Files\Update Services\LogFiles\WSUSTemp             0
```

Integración

Recursos Cruzados

Desde ubuntu, acceder a recurso windows

```
admin-corp@servidor-corporativo:~$ ls -la /mnt/windows/documentos/
total 8
drwxr-xr-x 2 root root 4096 dic  4 04:09 .
drwxr-xr-x 4 root root 4096 dic  4 04:09 ..
```

Montajes activos

```
admin-corp@servidor-corporativo:~$ mount | grep -i windows
//192.168.1.10/Documentos on /mnt/windows/documentos type cifs (rw,relatime,vers=3.1.1,cache=str
ct,upcall_target=app,username=administrador,domain=CORPORATIVO,uid=1000,forceuid,gid=1000,forceg
d,addr=192.168.1.10,file_mode=0644,dir_mode=0755,iocharset=utf8,soft,nounix,serverino,mapposix,n
perm,rsize=4194304,wsize=4194304,bsize=1048576,retrans=1,echo_interval=60,actimeo=1,closetimeo=1
```

DNS integrado

Resolución completa

```
PS C:\Users\Administrador> nslookup ubuntu.corporativo.local
nslookup portal.corporativo.local
ping portal.corporativo.local
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  ::1

Nombre:  ubuntu.corporativo.local
Address:  192.168.1.100

DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  ::1

Nombre:  portal.corporativo.local
Address:  192.168.1.100


Haciendo ping a portal.corporativo.local [192.168.1.100] con 32 bytes de datos:
Respuesta desde 192.168.1.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.100: bytes=32 tiempo<1m TTL=64
```

Escenarios

1. Nuevo empleado

Crear usuario

```
PS C:\Users\Administrador> Get-ADUser -Identity "jperez" -Properties * |
    Select-Object Name, SamAccountName, UserPrincipalName, Department, Enabled,
    Format-List


Name              : Juan Perez
SamAccountName    : jperez
UserPrincipalName : jperez@corporativo.local
Department        : Ventas
Enabled           : True
LastLogonDate     :
```

Verificar en ubuntu

```
admin-corp@servidor-corporativo:~$ getent passwd jperez@corporativo.local
jperez@corporativo.local:*:1345801120:1345800513:Juan Perez:/home/jperez@corporativo.local:/bin/b
ash
```

2. Verificar recursos compartidos

Listar recursos compartidos

```
PS C:\Users\Administrador> Write-Host "`TODOS LOS RECURSOS COMPARTIDOS:" -Foregrou
Get-SmbShare | Where-Object {$_.Name -notlike "*$*"} | Format-Table Name, Path, De
TODOS LOS RECURSOS COMPARTIDOS:

Name                  Path                                                Descri
                                                                          ption
----                  ----                                                ------
Documentos            C:\Corporativo\Documentos
Finanzas              C:\Corporativo\Departamentos\Finanzas
IT                    C:\Corporativo\Departamentos\IT
NETLOGON              C:\Windows\SYSVOL\sysvol\corporativo.local\SCRIPTS Rec...
RRHH                  C:\Corporativo\Departamentos\RRHH
SYSVOL                C:\Windows\SYSVOL\sysvol                            Rec...
UbuntuBackups         C:\Backups\Ubuntu
UpdateServicesPackages C:\WSUS\UpdateServicesPackages                     A n...
Users                 C:\Users
WsusContent           C:\WSUS\WsusContent                                 A n...
WSUSTemp              C:\Program Files\Update Services\LogFiles\WSUSTemp A n...
```

Ver permisos (un recurso especifico)

```
PS C:\Users\Administrador> Write-Host "`PERMISOS DETALLADOS (ejemplo: Documentos):"
$Recurso = "Documentos"  # Cambia por el nombre de tu recurso
Get-SmbShareAccess -Name $Recurso | Format-Table AccountName, AccessRight, AccessCor
PERMISOS DETALLADOS (ejemplo: Documentos):

AccountName AccessRight AccessControlType
----------- ----------- -----------------
Todos              Read             Allow
```

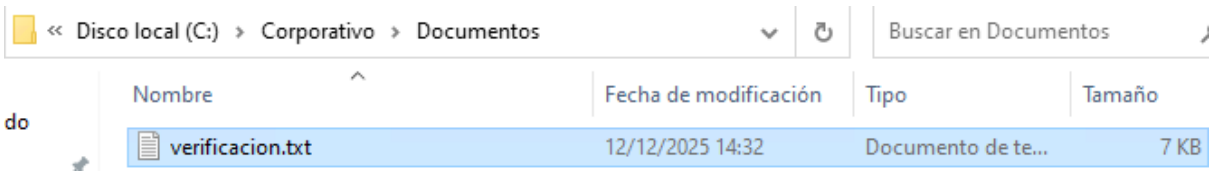
Listar recursos disponibles en windows desde ubuntu

```
admin-corp@servidor-corporativo:~$ echo -e "\RECURSOS DISPONIBLES EN WINDOWS SERVER:"
smbclient -L //192.168.1.10 -U administrador%[redacted] 2>/dev/null | grep "Disk" | while read lin
e; do
    SHARE=$(echo $line | awk '{print $1}')
    echo "   📂 $SHARE"
done
\RECURSOS DISPONIBLES EN WINDOWS SERVER:
   📂 ADMIN$
   📂 C$
   📂 Documentos
   📂 E$
   📂 Finanzas
   📂 IT
   📂 NETLOGON
   📂 RRHH
   📂 SYSVOL
   📂 UbuntuBackups
   📂 UpdateServicesPackages
   📂 Users
   📂 WsusContent
   📂 WSUSTemp
```

Probar conexion a un recurso especifico

```
admin-corp@servidor-corporativo:~$ echo -e "\PRUEBA DE CONEXIÓN A RECURSO:"
RECURSO="Documentos"
echo "   Probando acceso a //192.168.1.10/$RECURSO..."
smbclient //192.168.1.10/$RECURSO -U administrador%[redacted] -c "ls" 2>/dev/null

if [ $? -eq 0 ]; then
    echo "   ✅ Conexión exitosa"
else
    echo "   ❌ Error de conexión"
fi
\PRUEBA DE CONEXIÓN A RECURSO:
   Probando acceso a //192.168.1.10/Documentos...
  .                                   D        0  Thu Dec  4 04:07:56 2025
  ..                                  D        0  Thu Dec  4 04:07:56 2025

                7811071 blocks of size 4096. 3196464 blocks available
   ✅ Conexión exitosa
```

Crear archivo en recurso compartido



Ver recurso

```
admin-corp@servidor-corporativo:~$ smbclient //192.168.1.10/$RECURSO -U administrador%[redacted] -
c "ls" 2>/dev/null
  .                                   D        0  Fri Dec 12 13:50:16 2025
  ..                                  D        0  Thu Dec  4 04:07:56 2025
  verificacion.txt                    A     6330  Fri Dec 12 13:32:24 2025

                7811071 blocks of size 4096. 3194458 blocks available
```

3. Monitoreo proactivo y alertas

Generar carga de CPU en ubuntu (fallo)

```
admin-corp@servidor-corporativo:~$ stress --cpu 4 --timeout 60 &
STRESS_PID=$!
[1] 8017
```

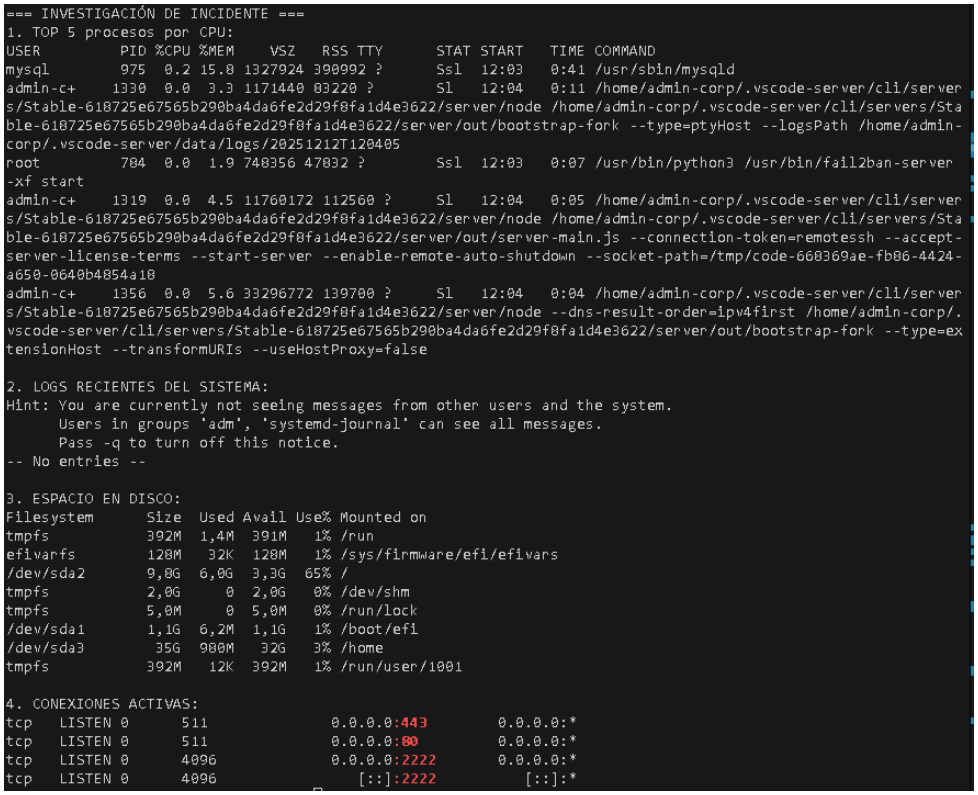
Verificar métricas

```
admin-corp@servidor-corporativo:~$ for i in {1..5}; do
    echo "Iteración $i:"
    echo "CPU: $(top -bn1 | grep "Cpu(s)" | awk '{print $2}')%"
    echo "Memoria libre: $(free -h | grep Mem | awk '{print $4}')"
    echo "---"
    sleep 5
done

kill $STRESS_PID 2>/dev/null
echo "✅ Carga detenida"
Iteración 1:
CPU: 27,3%
Memoria libre: 873Mi
---
Iteración 2:
CPU: 0,0%
Memoria libre: 880Mi
---
Iteración 3:
CPU: 0,0%
Memoria libre: 880Mi
---
Iteración 4:
CPU: 0,0%
Memoria libre: 880Mi
---
Iteración 5:
CPU: 0,0%
Memoria libre: 880Mi
---
✅ Carga detenida
```

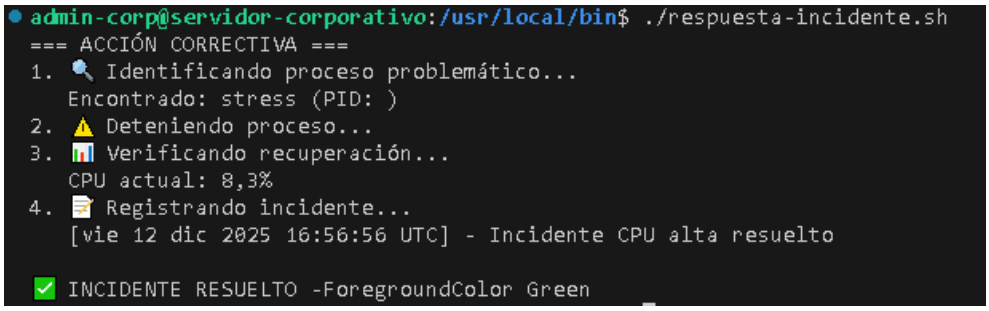
Ver alertas en wsus

```
=== SISTEMA DE ALERTAS CORPORATIVO ===

📊 DASHBOARD DE MONITOREO:

SERVIDOR              ESTADO   CPU    MEMORIA    ALERTAS
------------------------------------------------------------
Windows Server        ✅       45%    3.2/8GB    ✅ OK
Ubuntu Server         ⚠️       85%    5.1/8GB    ⚠️ Alta CPU
Gateway               ✅       12%    512MB/1GB  ✅ OK

📧 ALERTA ENVIADA:
Asunto: ALTA CARGA CPU - Ubuntu Server (192.168.1.100)
Para: admin@corporativo.local
Mensaje: CPU en 85% por más de 5 minutos. Verificar procesos.
```

Investigar causa raíz



Tomar acción correctiva



- Definir los indicadores de calidad del proyecto.

- Observación directa del uso del sistema.

- Entrevistas con usuarios finales.

- Revisión de documentación generada (claridad, exhaustividad).

- Elaboración del protocolo de evaluación con el cliente y su documentación.

- **Acta de aceptación del proyecto**, firmada por ambas partes.
- **Checklist de funcionalidades entregadas**, verificadas una a una.
- **Informe de pruebas de aceptación (UAT)** con evidencias de aprobación.
- **Encuesta de satisfacción global** estructurada en:
  - ◇Calidad técnica de la solución.
  - ◇Cumplimiento de requisitos.
  - ◇Comunicación y profesionalismo del equipo.
  - ◇Satisfacción general con el resultado.

4.2 Incidencias

- Definir un protocolo para resolución de incidencias:
  - ✓ Recopilación de información

1º ID de ticket (automático).

2º Fecha y hora de reporte.

3º Usuario/reportero y contacto.

4º Categoría (Crítica, Alta, Media, Baja).

5º Descripción detallada del problema.

6º Pasos para reproducir.

7º Evidencias adjuntas (capturas, logs, vídeos).

8º Impacto estimado en operaciones.

- ✓ Posible solución

- Análisis técnico inicial por soporte de nivel 1.
- Derivación a especialista (red, BBDD, desarrollo) según naturaleza.
- Propuesta de solución documentada en el ticket.
- Estimación de tiempo y recursos necesarios.

- ✓ Registro

- Sistema de tickets: GLPI / OTRS / Jira Service Management.
- Flujo de estado: Abierto → En análisis → En progreso → En validación → Cerrado.
- Comunicación automática de actualizaciones al reportero.
- Base de conocimientos (KB): Soluciones documentadas para futuras referencias.

4.3 Cambios

- Adaptación a los cambios y registro:

- ✓ Migración

- Formulario RFC detallando:
- Descripción del cambio.
- Justificación/beneficio.
- Impacto estimado en sistema, seguridad, usuarios.
- Recursos y tiempo necesarios.
- Plan de reversión en caso de fallo.

- ✓ Actualización

- Plan de implementación detallado:
  - Pasos técnicos.
  - Ventana de mantenimiento comunicada con antelación.
  - Asignación de responsables.
  - Pruebas posteriores obligatorias.
- Comunicación proactiva a todos los stakeholders afectados.

- ✓ Escalabilidad

Aumento de recursos (CPU, RAM, almacenamiento) sin interrupción de servicio (horizontal/vertical).

- ✓ Mejoras

Nuevas funcionalidades solicitadas post-implantación, gestionadas como mini-proyectos con su propio ciclo de vida.

4.4 Pruebas y soporte

- Elaboración de un acuerdo de servicio.

Documento contractual que establece:

Objetivos de servicio:

1º Disponibilidad del sistema: 99.5% mensual.

2º Tiempo de respuesta a incidencias: según prioridad (definido en 4.2).

3º Tiempo de resolución máxima para cada nivel de prioridad.

Horarios de soporte:

1º Soporte básico: L-V 9:00-18:00.

2º Soporte extendido para críticas: 24/7.

3º Canales de contacto: teléfono, email, portal de tickets.

Métricas de reporte:

1º Informe mensual de cumplimiento del SLA.

2º Revisión trimestral del acuerdo con el cliente.

Cláusulas de exención:

1º Causas fuera de control (fuerza mayor).

2º Mantenimiento planificado y comunicado.

3º Mal uso por parte del cliente.

Penalizaciones por incumplimiento:

1º Descuentos en facturación proporcionales al tiempo de indisponibilidad no planificado.