

SIMULACIÓN DE INFRAESTRUCTURA DE TELETRABAJO



Guillermo De La Torre Aguilera
Proyecto Integrado
2º ASIR- IES LUIS VÉLEZ DE GUEVARA
Curso 2024-2025

ÍNDICE

1. Introducción.....	5
2. Objetivos del proyecto.....	6
2.1 Objetivo general.....	6
2.2 Objetivos específicos.....	6
3. Descripción general de la infraestructura.....	7
3.1 Componentes virtualizados.....	7
3.2 Red y direccionamiento.....	8
3.3 Herramientas utilizadas.....	8
4. Planificación y estrategia de trabajo.....	9
5. Implantación técnica paso a paso.....	11
5.1 Instalación del hipervisor Proxmox VE.....	11
5.2 Creación de máquinas virtuales.....	11
5.2.1 Windows Server 2025.....	11
5.2.2 Windows 11 (VDI).....	12
5.2.3 OPNsense.....	12
5.3 Configuración del dominio y servicios de red.....	12
5.4 Gestión de usuarios, grupos y equipos.....	13
5.5 Configuración de escritorios remotos y GPOs.....	13
5.6 Configuración de VPN con OPNsense y DNS dinámico.....	13
5.7 Pruebas funcionales y validación final.....	13
6. Resultados obtenidos.....	14
7. Conclusiones.....	16
8. Manual básico de uso para usuarios finales.....	17
9. Dificultades encontradas y soluciones aplicadas.....	19
9.1 Instalación de Proxmox en entorno real.....	19
9.2 Configuración del cliente DDNS en OPNsense.....	19
9.3 Problemas de RAM en la VM de OPNsense.....	20
9.4 Aplicación de GPOs no inmediata.....	20
10. Posibles mejoras y ampliaciones futuras.....	21
10.1 Integración del acceso VPN con Active Directory.....	21
10.2 Automatización del despliegue de VDIs.....	21
10.3 Implementación de un servidor WSUS.....	21
10.4 Monitorización y alertas.....	22
10.5 Segmentación lógica por departamentos.....	22
11. Recursos utilizados (hardware, software y servicios).....	22
11.1 Hardware.....	22
11.2 Software.....	23
11.3 Servicios online.....	23
12. Fuentes de información.....	24
12.1 Documentación oficial.....	24
12.2 Foros y comunidades técnicas.....	25
Anexo 1: Instalación inicial del hipervisor Proxmox VE.....	28
A1.1. Creación del USB booteable con Proxmox.....	29
A1.1. Selección del dispositivo USB.....	29
A1.2. Carga de la imagen ISO de Proxmox.....	29

A1.3. Configuración de esquema de partición y sistema destino.....	29
A1.4. Inicio del proceso y formateo del USB.....	30
A1.5. Finalización y verificación.....	30
A1.2. Instalación de Proxmox VE en el SSD físico.....	31
A1.2.1 Inicio del instalador.....	31
A1.2.2 Acuerdo de licencia.....	32
A1.2.3 Selección del disco de instalación.....	33
A1.2.4 Configuración regional.....	34
A1.2.5 Contraseña y correo del administrador.....	35
A1.2.6 Configuración de red.....	36
A1.2.7 Confirmación final e instalación.....	37
A1.2.8 Reboot y finalización.....	38
A1.3. Acceso a la interfaz gráfica de Proxmox.....	39
A1.3.1. Dirección de acceso web.....	39
A1.3.2. Advertencia de seguridad del navegador.....	40
A1.3.4 Pantalla de inicio de sesión.....	40
Anexo 2: Creación de la máquina virtual: Windows Server 2025.....	42
A2.1. Subida de la imagen ISO a Proxmox.....	42
A2.2. Creación de la máquina virtual.....	44
A2.3. Inicio de Instalación.....	49
A2.4. Instalación base y primeros ajustes del sistema.....	55
A2.4.1. Instalacion de drivers VirtIO.....	55
A2.4.2. Configuración de IP fija.....	59
A2.4.3. Cambiar nombre de equipo.....	60
Anexo 3: Creación de la máquina virtual: Windows 11 (VDI).....	61
A3.1. Subida de la imagen ISO a Proxmox.....	61
A3.2. Creación de la VM en Proxmox.....	62
A3.3. Instalación de Windows 11 de la instalación y carga del controlador de disco.....	70
A3.4. Instalación de drivers VirtIO post-instalación.....	76
A3.5. Configuración de IP estática.....	77
A3.6. Verificación de conectividad con el servidor.....	78
Anexo 4 – Creación de la máquina virtual: OPNsense.....	80
A4.1. Subida de la imagen ISO de OPNsense.....	80
A4.2. Creación de la MV para OpnSense.....	81
A4.3. Instalación OPNsense.....	88
A4.4. Dirección IP LAN estática para acceso a Web GUI.....	98
Anexo 5 – Instalación del rol de AD DS y promoción a controlador de dominio.....	105
A5.1. Inicio del asistente de instalación de roles.....	106
A5.2. Promoción del servidor a controlador de dominio y creación del bosque de dominio.....	111
Anexo 6 - Creación de usuarios, grupos y Unidades Organizativas.....	117
A6.1. Creación de Unidades Organizativas (UO).....	117
A6.2. Creación de Usuarios.....	119
A6.3. Asignación de usuarios a grupos.....	121
A6.4. Unión de la máquina Windows 11 al dominio.....	122
Anexo 7 – Configuración y validación del acceso remoto mediante Escritorio Remoto RDP.....	128
A7.1. Organización de equipos en Unidades Organizativas.....	129
A7.1.1. Creación de UO para el equipo VDI en cuestión.....	129
A7.1.2. Añadir un el equipo VDI a su UO.....	131

A7.2. Configuración del acceso a Escritorio Remoto en la VDI.....	132
A7.2.1. Habilitar el Escritorio Remoto.....	132
A7.2.2. Configuración de usuario autorizado.....	133
A7.2.3. Añadir el grupo <i>Admins</i> como usuarios permitidos por RDP.....	134
A7.3. Aplicación de GPO específica para acceso RDP.....	136
A7.4. Validación del acceso remoto con usuarios del dominio.....	145
Pruebas de acceso permitido.....	147
Pruebas de acceso denegado.....	148
Anexo 8 – Acceso remoto seguro mediante VPN y DNS dinámico (No-IP).....	151
A8.1. Actualización y preparación del sistema OPNsense.....	152
A8.2. Configuración de DNS dinámico con No-IP.....	154
A8.3. Configuración del servidor OpenVPN en OPNsense.....	155
A8.3.1. Creación de la Autoridad Certificadora (CA).....	155
A8.3.2. Creación del certificado del servidor VPN.....	157
A8.3.3. Configuración del servidor OpenVPN usando el asistente (Wizard).....	159
A8.3.4. Creación del usuario VPN local.....	165
A8.3.5. Creación de la instancia del servidor OpenVPN.....	169
A8.3.6. Exportar perfil de conexión para el cliente OpenVPN.....	172
A8.4. Redireccionamiento de puertos en el router de borde.....	173
A8.5. Prueba de conexión.....	175
A8.5.1. Prueba de conexión VPN.....	176
A8.5.2. Prueba de conexión a VDI con usuario autorizado.....	178
A8.5.3. Conclusión de las pruebas.....	180

1. Introducción

El presente proyecto tiene como objetivo la simulación de una infraestructura técnica de teletrabajo, diseñada para ofrecer a los empleados de una organización acceso remoto seguro y controlado a sus puestos de trabajo y recursos corporativos. Esta simulación reproduce las condiciones técnicas que podrían encontrarse en una pequeña o mediana empresa, permitiendo evaluar y validar una arquitectura de red moderna basada en tecnologías ampliamente utilizadas en entornos reales.

Para ello, se ha desplegado un entorno virtualizado completo sobre el hipervisor Proxmox VE, donde se han configurado tres componentes clave: un servidor Windows con Active Directory para la gestión centralizada de usuarios y políticas, un cliente Windows 11 preparado como estación VDI de acceso remoto, y un firewall OPNsense que actúa como servidor VPN (OpenVPN), con integración de DNS dinámico para facilitar el acceso desde el exterior sin necesidad de IP pública fija.

Este entorno permite a los usuarios autenticarse mediante una conexión VPN segura y, una vez dentro de la red interna, acceder a su escritorio remoto personal (VDI) a través de RDP. El control de acceso se gestiona de forma centralizada mediante directivas de grupo (GPO), con restricciones según el rol del usuario, asegurando que solo los usuarios autorizados puedan acceder a sus estaciones de trabajo desde ubicaciones remotas.

El desarrollo del proyecto ha seguido un enfoque técnico riguroso y progresivo, documentado paso a paso en los anexos. Se han cubierto aspectos como la instalación y configuración de los sistemas virtuales, la estructura de dominio, la implementación de políticas de acceso, la creación de certificados digitales y la validación práctica mediante pruebas reales de conexión remota.

Esta simulación, además de servir como práctica formativa del módulo de Proyecto del ciclo formativo de grado superior en Administración de Sistemas Informáticos en Red (CFGSS ASIR), constituye un modelo funcional, reproducible y adaptable para escenarios reales de teletrabajo.

2. Objetivos del proyecto

2.1 Objetivo general

Diseñar, implementar y documentar una infraestructura virtual que simule un entorno empresarial de teletrabajo seguro, con acceso remoto mediante VPN, gestión centralizada de usuarios y escritorios remotos, utilizando tecnologías reales como Proxmox VE, Windows Server, Windows 11 y OPNsense.

2.2 Objetivos específicos

- Instalar y configurar el hipervisor Proxmox VE como plataforma base de virtualización.
- Desplegar una máquina virtual con Windows Server 2025, configurada como controlador de dominio (AD DS), servidor DNS y DHCP.
- Crear y organizar usuarios, grupos y unidades organizativas (UO) en Active Directory.
- Desplegar una máquina virtual con Windows 11, unirla al dominio y prepararla como estación de trabajo remota (VDI).
- Aplicar directivas de grupo (GPO) para definir políticas de acceso remoto seguras y controladas.
- Instalar y configurar una máquina virtual con OPNsense como firewall y servidor OpenVPN.
- Implementar una solución de DNS dinámico con No-IP y ddclient para permitir el acceso sin IP pública fija.
- Realizar pruebas funcionales de conexión VPN y acceso remoto por RDP, validando las políticas de acceso establecidas.
- Documentar el proceso completo con capturas y evidencias en los anexos técnicos.

3. Descripción general de la infraestructura

La infraestructura desarrollada en este proyecto simula un entorno empresarial orientado al teletrabajo seguro, utilizando virtualización como base y componentes reales equivalentes a los empleados en redes corporativas de pequeña y mediana escala.

Toda la solución ha sido desplegada sobre un único equipo físico mediante el hipervisor Proxmox VE 8.4, que permite la gestión eficiente de múltiples máquinas virtuales (VM). La infraestructura incluye tres sistemas principales: un servidor Windows que actúa como núcleo del dominio, una máquina cliente con Windows 11 que representa el puesto de trabajo del usuario remoto, y una appliance OPNsense configurada como firewall y servidor VPN.

El acceso desde el exterior se realiza mediante OpenVPN, alojado en OPNsense, y autenticado con certificados digitales. Dado que el entorno se encuentra en una red sin IP pública fija, se ha integrado el servicio de DNS dinámico No-IP, mantenido actualizado mediante el cliente ddclient.

Una vez establecida la conexión VPN, los usuarios pueden acceder a su escritorio remoto (VDI) mediante el protocolo RDP, siempre que estén autorizados por las Directivas de Grupo (GPO) definidas en el dominio. La infraestructura está pensada para ser escalable, permitiendo la clonación de estaciones VDI para nuevos usuarios a partir de una plantilla base ya configurada.

3.1 Componentes virtualizados

Windows Server 2025

- Controlador de dominio (AD DS)
- DNS y DHCP
- Gestión de usuarios, grupos y UO
- Aplicación de GPOs y control de acceso a RDP

Windows 11 Pro (cliente VDI)

- Integrado en el dominio
- IP estática

- Acceso remoto mediante RDP
- Configurado como plantilla replicable

OPNsense 25.1.7_4

- Servidor OpenVPN
- Generación de certificados
- Integración con No-IP para DNS dinámico
- Redirección de puertos para acceso externo

3.2 Red y direccionamiento

- **Red LAN simulada:** 192.168.1.0/24
- **OPNsense (LAN):** 192.168.1.101
- **Servidor Windows Server:** 192.168.1.88
- **VDI (cliente):** 192.168.1.87
- **Subred VPN:** 10.8.0.0/24
- **Dominio interno:** mi-empresa.lan
- **Dominio externo (DDNS):** mi-empresa123.zapto.org

3.3 Herramientas utilizadas

- **Proxmox VE:** plataforma de virtualización
- **VirtIO Drivers:** para mejorar rendimiento de VMs Windows
- **Rufus:** creación de USB booteable
- **OpenVPN Connect:** cliente VPN para conexión remota
- **ddclient:** cliente de DNS dinámico en OPNsense
- **GPMC (Group Policy Management Console):** gestión de GPOs
- **Remote Desktop (mstsc):** acceso remoto a VDIs

4. Planificación y estrategia de trabajo

Antes de iniciar la implantación técnica de la infraestructura, se realizó una planificación secuencial del proyecto, basada en la experiencia práctica y en los requisitos funcionales que debía cumplir un entorno de teletrabajo seguro y centralizado.

La estrategia se centró en construir el entorno de forma modular, escalable y verificable, abordando cada fase de manera individual pero integrada en un conjunto funcional coherente. Esta metodología permitió identificar posibles errores, ajustar configuraciones, y asegurar que cada componente cumpliera su función correctamente antes de avanzar al siguiente paso.

Fases del trabajo

1. Preparación del entorno base de virtualización

Instalación del hipervisor Proxmox VE en un equipo físico, con creación del entorno de red necesario y subida de las ISOs requeridas para los sistemas virtuales.

2. Despliegue de las máquinas virtuales principales

Instalación de:

- Windows Server 2025, como controlador de dominio y núcleo de servicios de red.
- Windows 11, como estación de trabajo cliente (VDI).
- OPNsense, como firewall y servidor VPN.

3. Configuración de los servicios de red internos

- Dominio Active Directory (AD DS), DNS y DHCP.
- Organización lógica de usuarios, grupos y equipos.
- Unión de clientes al dominio.

4. Definición de políticas de acceso y escritorios remotos

Aplicación de directivas de grupo (GPO) para habilitar RDP de forma controlada y segura, diferenciando permisos entre usuarios normales y administradores.

5. Habilitación del acceso remoto mediante VPN

Configuración de OpenVPN sobre OPNsense y gestión de certificados.

Implementación de DNS dinámico con No-IP para permitir el acceso externo sin IP pública fija.

6. Pruebas funcionales y validación de la solución

Verificación del funcionamiento completo desde el exterior: conexión VPN, acceso a la red, inicio de sesión remoto con usuario autorizado y denegación para usuarios no permitidos.

Criterios aplicados

Reproducibilidad: cada paso ha sido documentado y verificado para poder ser replicado en entornos reales o formativos.

Escalabilidad: se diseñó la VDI como plantilla replicable para nuevos usuarios.

Seguridad y segmentación: se utilizaron certificados, GPOs y reglas de firewall para garantizar un acceso seguro y restringido.

Optimización de recursos: el entorno fue desplegado con recursos limitados, priorizando eficiencia y funcionalidad.

Este enfoque estructurado permitió construir una infraestructura sólida, funcional y alineada con buenas prácticas de administración de sistemas en red.

5. Implantación técnica paso a paso

A lo largo de este apartado se describen de forma resumida las fases principales llevadas a cabo para la construcción de la infraestructura virtual de teletrabajo. Cada paso técnico está documentado con mayor profundidad, incluyendo capturas y comandos reales, en los anexos que acompañan esta memoria.

5.1 Instalación del hipervisor Proxmox VE

Como base para la virtualización del entorno, se instaló Proxmox VE 8.4 directamente sobre un disco SSD dedicado en un equipo físico. Para ello, se creó un medio USB booteable utilizando la herramienta Rufus y se seleccionaron parámetros de red estáticos para asegurar el acceso a la interfaz web de gestión. La dirección asignada al nodo Proxmox fue 192.168.1.35.

El acceso a la consola de administración se realizó mediante navegador a través de la URL <https://192.168.1.35:8006>, desde donde se completaron las configuraciones iniciales del nodo y se subieron las ISOs necesarias para la creación de las máquinas virtuales.

(Véase Anexo 1 – Instalación de Proxmox VE.)

5.2 Creación de máquinas virtuales

Se crearon tres máquinas virtuales principales: una con Windows Server 2025, otra con Windows 11 (cliente VDI) y una tercera con OPNsense. Todas fueron configuradas con controladores VirtIO para mejorar el rendimiento y se les asignaron IPs estáticas dentro del rango de red local.

5.2.1 Windows Server 2025

La VM de Windows Server fue configurada con 4 núcleos, 8 GB de RAM y 60 GB de almacenamiento. Durante la instalación se cargaron los drivers VirtIO para el reconocimiento del disco y de la interfaz de red. Se asignó la dirección IP 192.168.1.88 y se preparó para actuar como servidor de dominio.

(Véase Anexo 2 – VM: Windows Server 2025.)

5.2.2 Windows 11 (VDI)

Se creó una máquina virtual con Windows 11 Pro destinada a simular un puesto de trabajo remoto. Tras superar las restricciones del instalador mediante OOBE\BYPASSNRO, se configuró la red con IP estática (192.168.1.87), se instalaron drivers de red y se verificó la conectividad con el servidor mediante ping.

(Véase Anexo 3 – VM: Windows 11 (VDI)).

5.2.3 OPNsense

La máquina de OPNsense fue desplegada con 3 GB de RAM y dos interfaces de red: una conectada a la LAN y otra a la red virtual del servidor. Se asignó la IP LAN 192.168.1.101 y se configuraron reglas básicas de firewall para permitir el acceso a su interfaz web. Posteriormente, actuaría como firewall y servidor OpenVPN.

(Véase Anexo 4 – VM: OPNsense.)

5.3 Configuración del dominio y servicios de red

En el servidor Windows Server se instaló el rol de Active Directory Domain Services (AD DS) y se promovió el equipo como controlador del dominio mi-empresa.lan. Se configuraron además los servicios DNS y DHCP, adaptados al entorno virtual, y se estableció la estructura básica de unidades organizativas.

(Véase Anexo 5 – Configuración del dominio (AD DS)).

5.4 Gestión de usuarios, grupos y equipos

Se crearon tres usuarios para las pruebas: Juan García (empleado), Francisco Gutiérrez (empleado sin acceso a RDP) y Guillermo de la Torre (administrador). Los usuarios fueron organizados en las unidades correspondientes y se crearon los grupos de seguridad “Empleados” y “Admins”. También se añadió la máquina cliente (VDI) al dominio, bajo el nombre *vdi-juangarcia*.

(Véase Anexo 6 – *Usuarios, grupos y unión al dominio.*)

5.5 Configuración de escritorios remotos y GPOs

En la máquina Windows 11 (VDI) se habilitó el acceso por Escritorio Remoto (RDP) y se añadieron los usuarios autorizados. Desde el servidor se aplicó una GPO vinculada a la unidad organizativa correspondiente para permitir el inicio de sesión remoto a los miembros del grupo “Admins” y al usuario Juan García.

(Véase Anexo 7 – *Escritorio remoto y GPOs.*)

5.6 Configuración de VPN con OPNsense y DNS dinámico

Se configuró el servidor OpenVPN en OPNsense mediante el asistente integrado, utilizando certificados internos y el puerto UDP 1194. Para garantizar la accesibilidad desde el exterior sin IP fija, se creó una cuenta en No-IP y se configuró ddclient como actualizador de DNS dinámico. El dominio externo utilizado fue mi-empresa123.zapto.org.

(Véase Anexo 8 – *VPN con OpenVPN y DNS dinámico.*)

5.7 Pruebas funcionales y validación final

Finalmente, se realizaron pruebas de conexión desde el exterior mediante un cliente OpenVPN con el archivo .ovpn exportado desde OPNsense. Una vez establecida la conexión, se accedió con éxito al escritorio remoto de la VDI asignada al usuario Juan García. También se verificó que los usuarios

no autorizados, como Francisco Gutiérrez, no pudieran iniciar sesión, cumpliendo así las restricciones impuestas por las GPOs.

(Véase Anexo 8 – VPN con OpenVPN y DNS dinámico (sección de pruebas finales).)

6. Resultados obtenidos

Tras completar la implantación técnica y la ejecución de todas las fases planificadas, se obtuvo una infraestructura funcional y coherente que reproduce de forma realista un entorno empresarial de teletrabajo seguro, con acceso remoto centralizado y controlado.

El sistema desplegado ha demostrado un comportamiento estable, cumpliendo todos los objetivos planteados inicialmente. Las pruebas realizadas validaron no solo la conectividad entre los distintos elementos del entorno virtual, sino también la correcta aplicación de políticas de seguridad, autenticación y restricciones de acceso según el perfil del usuario.

Infraestructura virtual operativa

- El hipervisor Proxmox VE gestionó las máquinas virtuales sin incidencias relevantes, permitiendo un despliegue ágil y controlado de los distintos sistemas.
- Las VMs fueron configuradas correctamente con recursos limitados pero suficientes para sus funciones:
 - Windows Server 2025: 8 GB de RAM, 4 núcleos, 60 GB de disco
 - Windows 11 (VDI): 6 GB de RAM, 2 núcleos, 64 GB de disco
 - OPNsense: 3 GB de RAM, 2 núcleos

Dominio y control de usuarios operativo

- Se configuró correctamente un dominio interno mi-empresa.lan con servicios DNS y DHCP activos.
- Se crearon Unidades Organizativas (UO), grupos de seguridad y usuarios con distintas asignaciones de permisos.

- La máquina cliente Windows 11 fue unida al dominio y organizada dentro de su propia UO específica, lo que permitió aplicar políticas personalizadas.

Control de acceso remoto mediante GPO

- Se habilitó el Escritorio Remoto (RDP) en la VDI y se restringió el acceso a usuarios autorizados mediante GPO.
- Las pruebas confirmaron que el usuario Juan García y los miembros del grupo “Admins” pudieron acceder correctamente a la VDI.
- Se comprobó que otros usuarios, como Francisco Gutiérrez o incluso el usuario Administrator, no tenían acceso, demostrando la eficacia de las políticas aplicadas.

VPN funcional y accesible desde el exterior

- El servidor OpenVPN configurado en OPNsense permitió establecer una conexión segura desde el exterior.
- Se configuró un dominio dinámico con No-IP (mi-empresa123.zapto.org) enlazado a la IP pública del router doméstico, mantenido mediante ddclient.
- La conexión VPN fue probada desde una red externa (compartida por el móvil) y permitió el acceso a recursos internos como la VDI, la interfaz de Proxmox y el servidor.

Validación técnica

- Se realizaron pruebas reales de conexión con distintos usuarios, desde el exterior, a través de la VPN y mediante RDP.
- El sistema se comportó correctamente ante los distintos escenarios de autenticación y control de acceso.
- La resolución DNS, el túnel VPN y la visibilidad entre máquinas funcionaron sin errores.

En conjunto, el entorno simulado cumple con las características que tendría una infraestructura de teletrabajo real para una pequeña empresa: es replicable, escalable, seguro, y controlado desde un único punto de administración.

7. Conclusiones

El desarrollo de este proyecto ha permitido simular con éxito una infraestructura de red orientada al teletrabajo, empleando herramientas y tecnologías comúnmente utilizadas en entornos profesionales. La solución planteada reproduce de forma realista las condiciones técnicas y organizativas que una pequeña o mediana empresa podría requerir para ofrecer acceso remoto seguro a sus recursos internos.

Desde el punto de vista técnico, se ha demostrado la viabilidad de montar un entorno completo utilizando únicamente recursos accesibles, software libre y versiones de evaluación. La virtualización mediante Proxmox VE ha ofrecido una base sólida para la implementación de todos los componentes necesarios, permitiendo gestionar de forma eficiente tanto el despliegue como el mantenimiento de las distintas máquinas virtuales.

La configuración de Active Directory sobre Windows Server ha permitido centralizar la gestión de usuarios, grupos, políticas y recursos, aplicando buenas prácticas de administración de sistemas en red. Del mismo modo, la preparación de una estación de trabajo remota con Windows 11 (VDI) ha evidenciado que es posible replicar un modelo escalable y reutilizable para usuarios finales, con control total desde el dominio.

Uno de los elementos más relevantes del proyecto ha sido la integración de una solución de acceso remoto basada en OpenVPN y gestionada a través de OPNsense. Esta parte del sistema, complementada con un servicio de DNS dinámico, ha permitido habilitar el acceso externo sin necesidad de contar con una IP fija, lo cual refleja una necesidad real y habitual en muchas organizaciones que operan desde redes domésticas o sin infraestructura dedicada.

Las pruebas realizadas han confirmado la funcionalidad del sistema, la correcta aplicación de las políticas de acceso, y la efectividad del modelo de seguridad implementado. Se ha verificado tanto el acceso autorizado como la restricción ante usuarios no permitidos, validando el comportamiento esperado en escenarios reales.

En definitiva, el proyecto no solo ha cumplido los objetivos iniciales, sino que ha generado una base técnica sólida, documentada y reproducible, que podría escalarse o adaptarse a diferentes contextos profesionales. Además, ha servido como experiencia práctica integral en la aplicación de conocimientos adquiridos a lo largo del ciclo formativo, integrando virtualización, redes, seguridad y administración de sistemas.

8. Manual básico de uso para usuarios finales

Este apartado está dirigido a los usuarios finales del sistema, con el objetivo de proporcionar una guía clara y sencilla para conectarse remotamente a su estación de trabajo (VDI) mediante el uso de la VPN y el Escritorio Remoto. Está redactado pensando en un perfil no técnico, pero con los conocimientos mínimos para seguir los pasos descritos.

Acceso remoto a la VDI

Paso 1: Instalación del cliente VPN

Para establecer la conexión con la red interna de la empresa, es necesario instalar el cliente OpenVPN.

1. Acceder a la página oficial:

<https://openvpn.net/client-connect-vpn-for-windows/>

2. Descargar e instalar el software en el equipo desde el que se desea conectar.

3. Solicitar al administrador el archivo de configuración .ovpn correspondiente al usuario.

Paso 2: Importar el perfil de conexión VPN

1. Abrir la aplicación **OpenVPN Connect**.

2. Hacer clic en “**+ Import Profile**”.

3. Seleccionar el archivo **.ovpn** recibido por parte del administrador.

Confirmar los datos importados y guardar el perfil.

Paso 3: Conexión a la VPN

1. Desde OpenVPN Connect, pulsar el botón “**Connect**” junto al perfil importado.
2. Introducir las credenciales si se solicita (según configuración).
3. Una vez conectado, se establece un túnel seguro con la red interna.

Paso 4: Conexión al escritorio remoto

1. Abrir el programa Conexión a Escritorio Remoto (buscar mstsc en el menú de inicio).
2. Introducir la IP o nombre del equipo asignado:
Ejemplo: *vdi-juangarcia.mi-empresa.lan* o *192.168.1.87*
3. En el cuadro de inicio de sesión, introducir las credenciales del dominio:
 - Usuario: MI-EMPRESA\juangarcia
 - Contraseña: (la proporcionada o definida por el usuario)

Recomendaciones de uso

- Es imprescindible conectarse primero a la VPN antes de iniciar sesión por Escritorio Remoto.
- Al finalizar la sesión, cerrar el acceso remoto y desconectar la VPN.
- Si el equipo remoto está apagado, contactar con el administrador para que lo encienda desde Proxmox.

Ante errores de conexión, verificar:

- Que la VPN está activa.
- Que el usuario tiene permisos mediante GPO.

- Que el equipo de destino esté encendido y accesible.

Los pasos descritos en este manual coinciden prácticamente con los seguidos durante la fase de pruebas finales, documentadas en el Anexo 8. Allí se puede consultar la validación real del proceso de conexión desde el exterior, incluyendo capturas de pantalla que demuestran el correcto funcionamiento de la VPN, el acceso RDP y las restricciones aplicadas por GPO. Esto confirma que el procedimiento es reproducible y fiable para cualquier usuario autorizado.

9. Dificultades encontradas y soluciones aplicadas

Durante el desarrollo del proyecto se presentaron varios obstáculos técnicos que requirieron análisis, búsqueda de información y aplicación de soluciones prácticas. A continuación se describen los más relevantes, así como la forma en que fueron resueltos.

9.1 Instalación de Proxmox en entorno real

Dificultad:

Inicialmente se intentó instalar Proxmox VE dentro de una máquina virtual en VirtualBox, utilizando virtualización anidada. Sin embargo, esta configuración provocaba fallos de compatibilidad y no permitía arrancar las máquinas virtuales dentro del hipervisor correctamente.

Solución:

Se descartó el uso de virtualización anidada y se instaló Proxmox directamente en un SSD físico, conectado como disco de arranque del equipo anfitrión. Esta decisión permitió utilizar todo el hardware de forma nativa, sin capas intermedias, garantizando un entorno estable y compatible.

9.2 Configuración del cliente DDNS en OPNsense

Dificultad:

El plugin oficial os-ddclient, incluido en OPNsense para gestionar la actualización dinámica de DNS, no funcionaba de forma persistente y no actualizaba correctamente la IP pública en el servicio de No-IP.

Solución:

Se desinstaló el plugin mediante línea de comandos (pkg remove os-ddclient) y se procedió a instalar y configurar manualmente el cliente ddclient. Para asegurar su ejecución periódica, se creó una tarea cron que ejecuta el cliente cada 5 minutos. Esta configuración manual demostró ser más estable y fiable.

9.3 Problemas de RAM en la VM de OPNsense

Dificultad:

Al asignar solo 2 GB de RAM a la máquina virtual de OPNsense, el sistema mostraba advertencias sobre rendimiento y funcionamiento limitado, especialmente al cargar servicios como OpenVPN.

Solución:

Se amplió la memoria RAM del equipo físico a 24 GB y posteriormente se aumentó la memoria asignada a OPNsense hasta 3 GB, tal como recomienda su documentación oficial. Tras el cambio, el sistema funcionó sin advertencias y con mayor fluidez.

9.4 Aplicación de GPOs no inmediata

Dificultad:

En algunos momentos, las políticas de grupo (GPO) aplicadas desde el servidor no surtían efecto inmediatamente en las máquinas cliente.

Solución:

Se forzó manualmente la actualización de políticas desde la línea de comandos mediante el comando gpupdate /force. Esto permitió verificar rápidamente la aplicación de las GPO durante las fases de prueba.

Estas dificultades forman parte del proceso habitual en entornos reales de despliegue y han contribuido a enriquecer la experiencia del proyecto, reforzando la capacidad para resolver incidencias y adaptarse a los requisitos de cada herramienta.

10. Posibles mejoras y ampliaciones futuras

Aunque el sistema implementado cumple con todos los objetivos funcionales planteados, existen diversas áreas en las que podría ampliarse o mejorarse la infraestructura en caso de contar con más tiempo, recursos o necesidades reales de producción. A continuación se enumeran algunas propuestas viables:

10.1 Integración del acceso VPN con Active Directory

Actualmente, el acceso a la VPN se gestiona mediante usuarios locales de OPNsense y certificados individuales. Como mejora, se podría integrar OpenVPN con el servicio de LDAP del dominio de Windows Server. Esto permitiría que los usuarios accedieran utilizando sus propias credenciales del dominio, facilitando la gestión centralizada de accesos y eliminando la necesidad de gestionar certificados uno por uno.

10.2 Automatización del despliegue de VDIs

El proceso de creación de nuevos puestos de trabajo (VDIs) se realiza de forma manual. Se podría mejorar mediante el uso de plantillas en Proxmox y herramientas como Sysprep o scripts de postinstalación. Esto reduciría el tiempo necesario para dar de alta nuevos usuarios y garantizaría uniformidad en la configuración de cada estación de trabajo.

10.3 Implementación de un servidor WSUS

Para completar la gestión del entorno, sería recomendable instalar un servidor WSUS (Windows Server Update Services), que permitiría centralizar la distribución de actualizaciones de seguridad y del sistema operativo. Esto contribuiría a mejorar el control, la eficiencia del ancho de banda y la seguridad general de la infraestructura.

10.4 Monitorización y alertas

La incorporación de una solución de monitorización, como Zabbix, Grafana o Telegraf integrado con OPNsense, permitiría realizar un seguimiento del estado de las máquinas virtuales, el tráfico de red, los usuarios conectados por VPN y otros servicios críticos. Con ello se podría anticipar problemas de rendimiento o caídas de servicio.

10.5 Segmentación lógica por departamentos

Aunque se ha realizado una organización básica de usuarios y equipos, sería posible extender esta estructura para simular distintos departamentos (por ejemplo, administración, desarrollo, soporte). Cada uno podría tener sus propias políticas de acceso, recursos compartidos y perfiles de usuario, aplicando GPOs específicas.

Además, se podría implementar segmentación de red mediante VLANs, configuradas en OPNsense y en un switch gestionado, para aislar el tráfico entre departamentos y reforzar la seguridad interna.

Estas propuestas no son imprescindibles para el funcionamiento actual del sistema, pero reflejan un enfoque realista y profesional hacia la mejora continua y la evolución de una infraestructura básica hacia un entorno más robusto, automatizado y escalable.

11. Recursos utilizados (hardware, software y servicios)

Para la realización del proyecto se han utilizado recursos tanto físicos como digitales, seleccionados en función de su disponibilidad, compatibilidad con los objetivos planteados y adecuación al entorno de trabajo simulado. A continuación se detallan los elementos empleados.

11.1 Hardware

Equipo anfitrión (servidor físico):

- Procesador: Intel Core i7-4790K @ 4.00 GHz (4 núcleos / 8 hilos)
- Memoria RAM: 24 GB DDR3

- Almacenamiento: SSD de 240 GB dedicado a Proxmox VE
- Conectividad de red: Ethernet 1 Gbps
- Otros elementos utilizados:
 - Router doméstico Movistar Smart WiFi (para redirección de puertos)
 - Pendrive USB (mínimo 8 GB) para crear medio de instalación booteable de Proxmox

11.2 Software

Sistemas operativos y plataformas:

- **Proxmox VE 8.4**: hipervisor de virtualización
- **Windows Server 2025** (versión de evaluación): servidor de dominio y servicios de red
- **Windows 11 Pro** (versión de evaluación): estación de trabajo remota (VDI)
- **OPNsense 25.1.7_4**: firewall y servidor OpenVPN

Drivers y utilidades:

- **VirtIO Drivers**: controladores optimizados para máquinas virtuales Windows (disco, red, dispositivos)
- **Rufus**: herramienta para generar USB de instalación booteable
- **OpenVPN Connect**: cliente VPN para Windows
- **ddclient**: cliente de actualización dinámica de DNS

11.3 Servicios online

- **No-IP** (<https://www.noip.com>): proveedor de DNS dinámico gratuito

Dominio utilizado: *mi-empresa123.zapto.org*

- **Repositorios oficiales de Proxmox, OPNsense y Microsoft**:

Descarga de ISOs, documentación técnica y foros de soporte

- Comunidad técnica:

Foros de Proxmox, Microsoft Tech Community, Reddit (/r/sysadmin), Stack Overflow

Estos recursos han sido suficientes para implementar una infraestructura completa, funcional y ajustada a un entorno de teletrabajo simulado, permitiendo cumplir con los requisitos académicos y técnicos del proyecto.

12. Fuentes de información

A lo largo del desarrollo del proyecto se ha recurrido a distintas fuentes técnicas, tanto oficiales como comunitarias, para resolver dudas, consultar configuraciones específicas, validar procedimientos y asegurar el correcto funcionamiento de cada componente del sistema. A continuación se enumeran las principales referencias utilizadas.

12.1 Documentación oficial

Proxmox VE

https://pve.proxmox.com/wiki/Main_Page

Guía oficial de instalación, gestión de almacenamiento, creación de máquinas virtuales, snapshots y configuración de red.

Microsoft Learn (Windows Server / GPO)

<https://learn.microsoft.com/>

Documentación oficial sobre Active Directory, DNS, DHCP, Group Policy Management, Escritorio Remoto y administración de usuarios.

OPNsense

<https://docs.opnsense.org/>

Manual de instalación, configuración de firewall, gestión de certificados y despliegue de OpenVPN.

No-IP Support

<https://www.noip.com/support/>

Instrucciones para la creación de dominios dinámicos, configuración de clientes DDNS y solución de problemas comunes.

12.2 Foros y comunidades técnicas

Proxmox Forum

<https://forum.proxmox.com/>

Resolución de errores comunes en instalación de VMs, drivers VirtIO, networking y almacenamiento.

Microsoft Tech Community

<https://techcommunity.microsoft.com/>

Casos prácticos y solución de problemas relacionados con GPO, acceso remoto, unión de equipos al dominio, etc.

Reddit – /r/homelab, /r/sysadmin

Participación y lectura de experiencias de otros usuarios sobre despliegue de entornos Proxmox, OPNsense, y teletrabajo en laboratorios domésticos.

Stack Overflow / Server Fault

Consultas puntuales sobre errores de red, configuración de servicios y scripts auxiliares.

Estas fuentes han sido fundamentales para guiar la implementación técnica y resolver incidencias, complementando la documentación propia generada durante el proyecto.

ANEXOS

Anexo 1: Instalación inicial del hipervisor Proxmox VE

Este anexo documenta de forma completa el proceso de preparación e instalación de Proxmox VE 8.4, desde la creación del medio booteable hasta el primer acceso a la interfaz de gestión web.

El proceso comienza con la creación de un USB de arranque usando la herramienta Rufus portable sobre Windows, continúa con la instalación de Proxmox en un SSD físico conectado al equipo anfitrión, y concluye con el acceso a la interfaz gráfica (GUI) a través del navegador.

Las siguientes secciones incluyen capturas de pantalla representativas y explicaciones detalladas que permiten reproducir con fidelidad todo el entorno base necesario para el despliegue de las máquinas virtuales.

A1.1. Creación del USB booteable con Proxmox

A1.1. Selección del dispositivo USB

Dispositivo: seleccionar la unidad que se desea usar como USB booteable, en mi caso un pen drive Kingston 64GB.

Es importante usar una unidad de al menos **2GB** de capacidad libre, aunque se recomienda **8GB o más** para asegurar compatibilidad con ISOs pesadas.

A1.2. Carga de la imagen ISO de Proxmox

Se elige la imagen híbrida ISO de Proxmox VE desde el botón “SELECCIONAR”

Rufus detecta automáticamente que la imagen es híbrida, pero lanza una advertencia: “La imagen seleccionada es ISOHybrid, pero sus creadores no la han creado compatible con el modo de copia ISO/FILE.”

A1.3. Configuración de esquema de partición y sistema destino

Esquema de partición: MBR

Sistema de destino: BIOS (o UEFI-CSM) — esto asegura compatibilidad con la mayoría de BIOS/UEFI modernas.

Sistema de archivos: Large FAT32

Tamaño de clúster: 32 kilobytes (por defecto)

Estos parámetros son adecuados para un entorno educativo o pruebas de laboratorio donde se prioriza la compatibilidad.

A1.4. Inicio del proceso y formateo del USB

Al pulsar “EMPEZAR”, se inicia el formateo del USB y la escritura de la ISO.

Se borran todos los datos previos del dispositivo, y se crea una estructura de arranque adecuada para Proxmox.

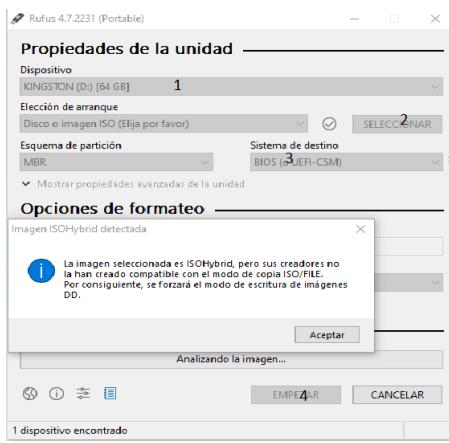


Figura 1: Unidad USB seleccionada y carga de ISO en Rufus

A1.5. Finalización y verificación

Al completar el proceso, Rufus mostrará un mensaje de éxito.

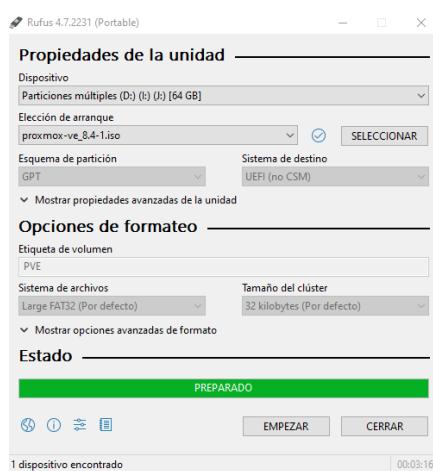


Figura 2: Aviso de imagen ISOHybrid al iniciar la escritura

El USB queda listo para arrancar el sistema e instalar Proxmox desde la BIOS del equipo físico.

Nota sobre entornos profesionales:

En un entorno de producción con servidores dedicados como **HP ProLiant (iLO)** o **Dell PowerEdge (iDRAC)**, el proceso de instalación no requiere la creación de un USB físico.

En estos casos, se accede a la interfaz de administración remota del servidor, desde donde es posible **montar una imagen ISO como unidad óptica virtual**. Esta funcionalidad permite iniciar la instalación del sistema operativo directamente desde la imagen, sin intervención física, lo que resulta ideal para tareas de mantenimiento o despliegue remoto en centros de datos.

A1.2. Instalación de Proxmox VE en el SSD físico

Una vez creado el USB booteable, el siguiente paso fue instalar Proxmox VE 8.4 en un disco SSD físico conectado directamente al equipo anfitrión. A continuación, se detalla el proceso completo tal como aparece en las capturas, explicando cada pantalla del instalador.

A1.2.1 Inicio del instalador

Para iniciar el instalador de Proxmox se conecta el USB y enciende el PC para arrancar el sistema desde el USB booteable creado anteriormente. Para ello presionar la tecla de función correspondiente para acceder al menú de arranque del sistema. En mi caso, la tecla es F11.

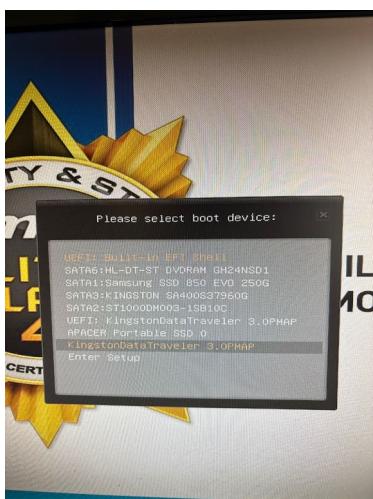


Figura 3: Menú de arranque

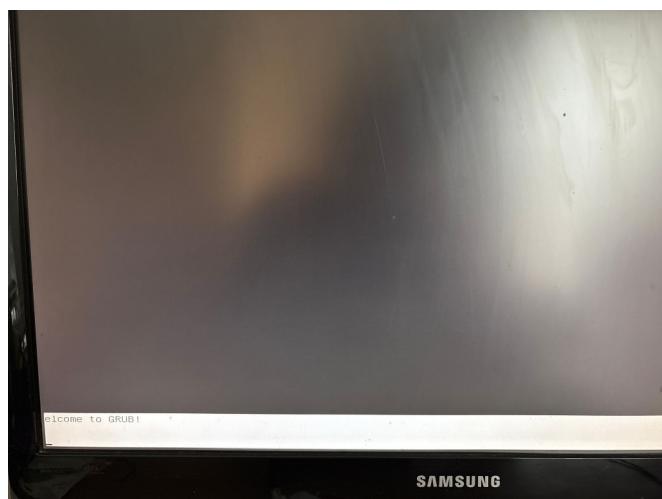


Figura 4: Arranque desde el USB booteable

Tras arrancar el sistema desde el USB creado con Rufus, aparece el menú de instalación.

Se selecciona la opción: Install Proxmox VE (Graphical).

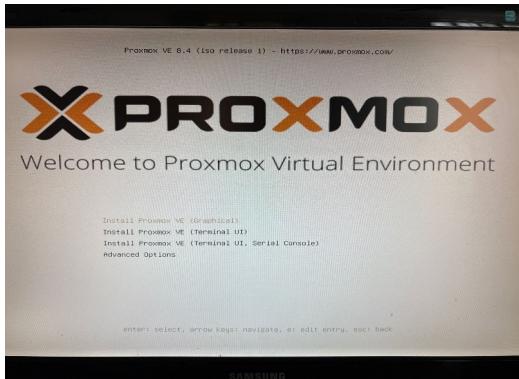


Figura 5: Menú Instalador proxmox



Figura 6: Instalador proxmox iniciando

Este modo ofrece una interfaz gráfica simple basada en texto que guía al usuario paso a paso.

A1.2.2 Acuerdo de licencia

Se muestra el acuerdo de licencia de usuario final. Aunque Proxmox es software libre, el instalador incluye una cláusula aclarando que los servicios de soporte (como repositorios empresariales) no están incluidos sin suscripción. Para continuar, se debe aceptar el acuerdo.

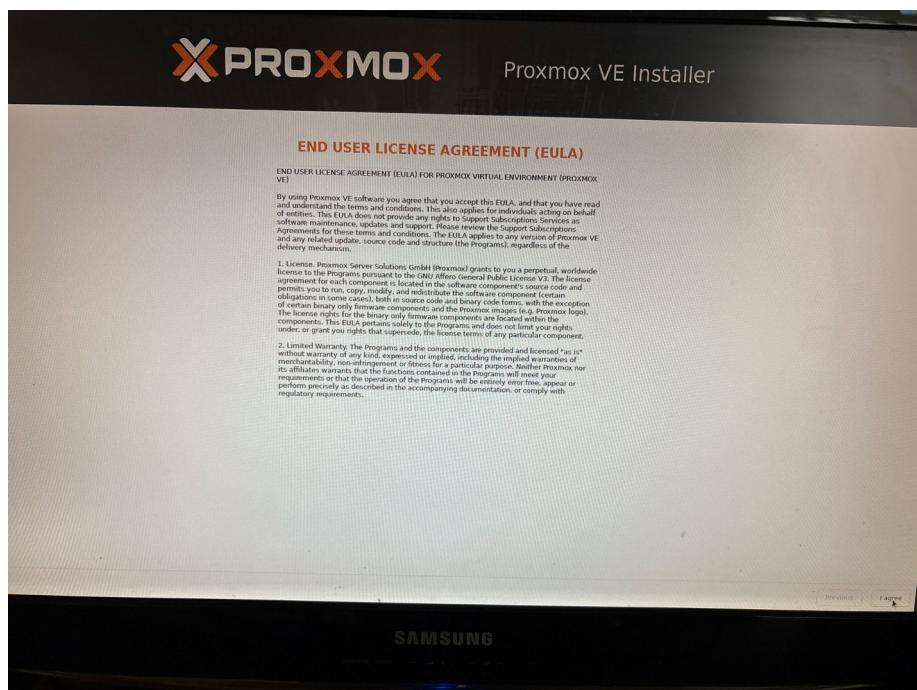


Figura 7: Acuerdo licencia proxmox

A1.2.3 Selección del disco de instalación

Se detecta el SSD donde se instalará Proxmox (por ejemplo, /dev/sda o Samsung SSD 850).

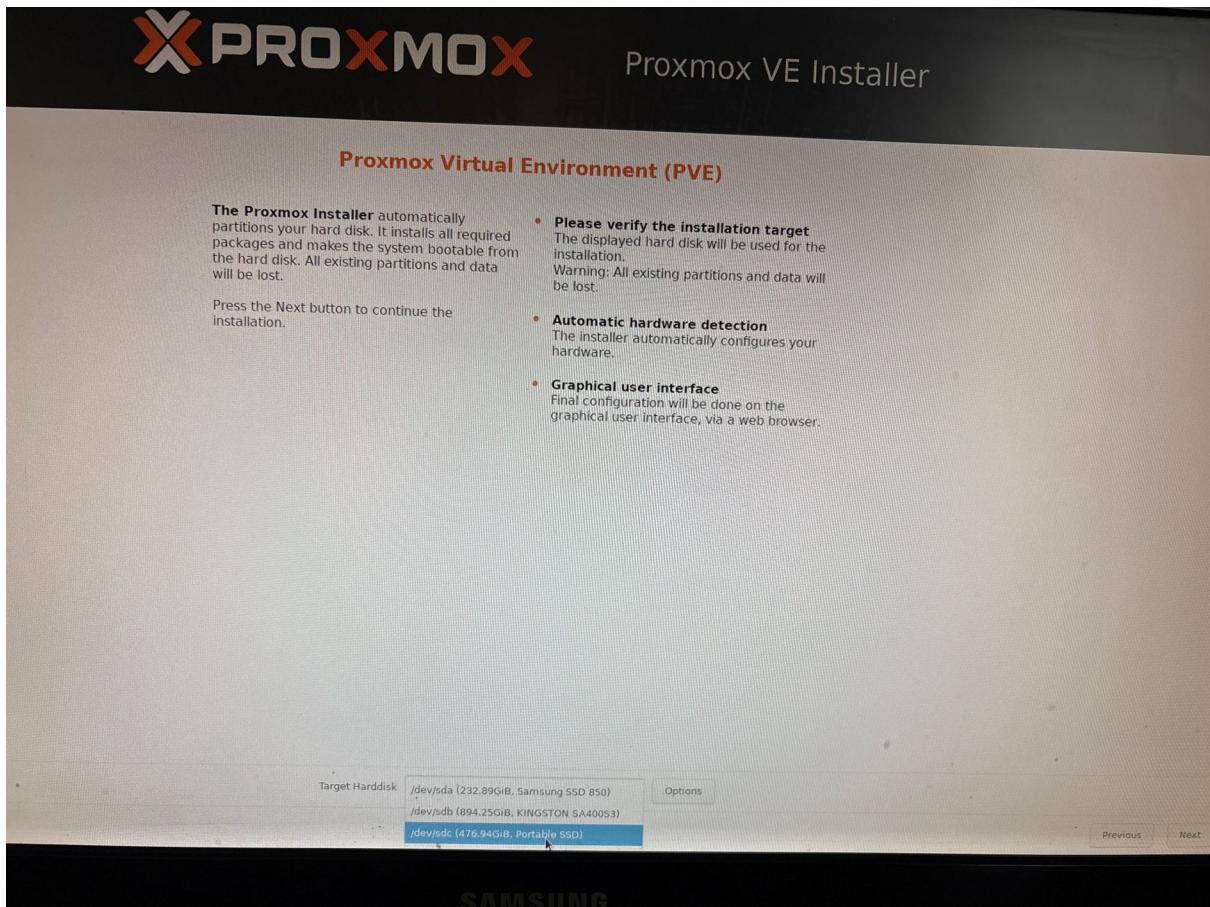


Figura 8: Instalación Proxmox – Selección de Disco

Es importante confirmar que el disco seleccionado es el que se quiere destinar para la instalación y no contiene datos importantes, ya que el instalador eliminará todas las particiones. Una vez verificado, se hace clic en Next.

A1.2.4 Configuración regional

País: España

Zona horaria: Europe/Madrid

Idioma del teclado: Español (ES)

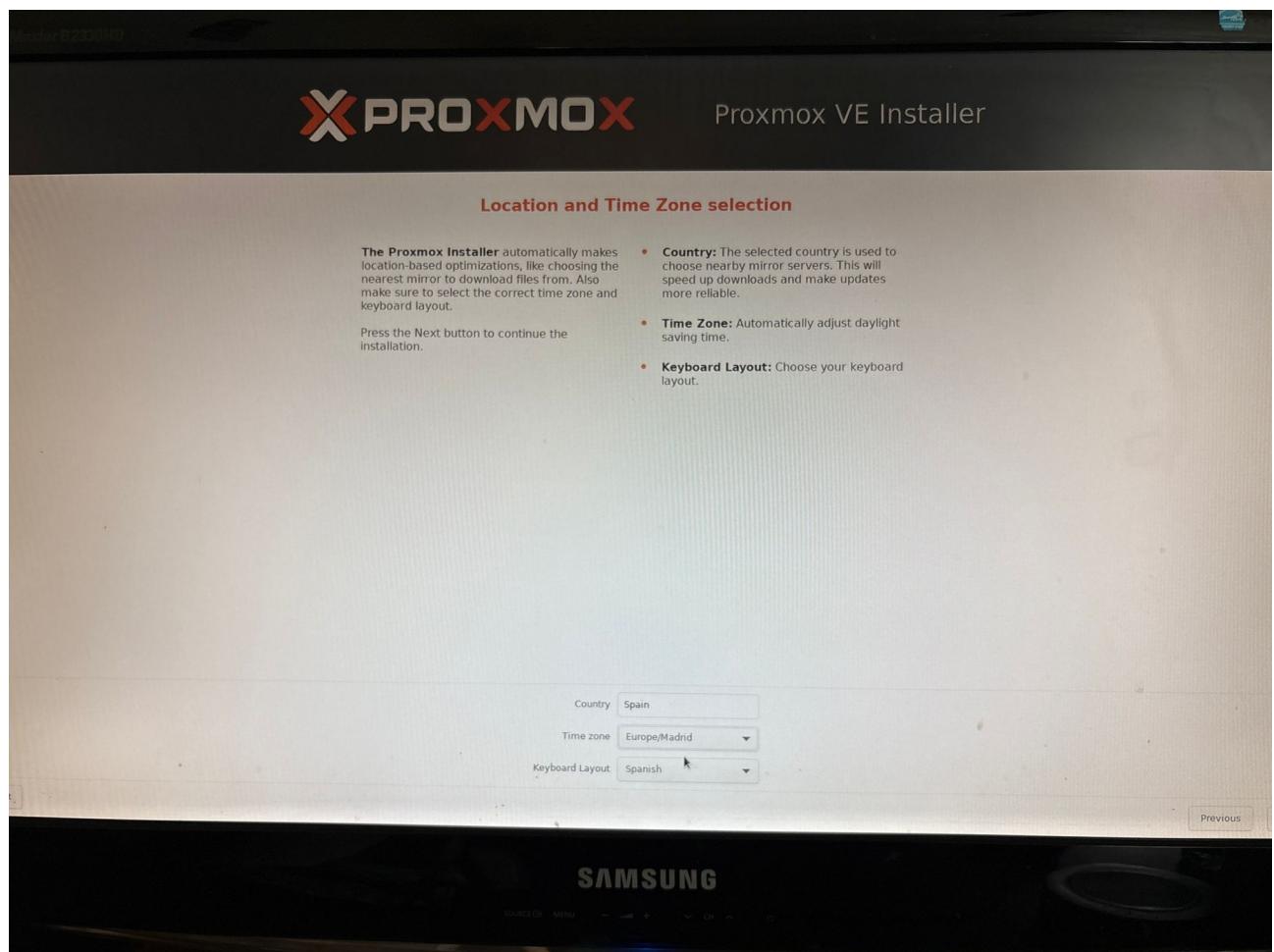


Figura 9: Instalación Proxmox – Selección de Disco

Estos valores permiten configurar adecuadamente la hora del sistema y facilitar la escritura posterior en la terminal.

A1.2.5 Contraseña y correo del administrador

Se define la contraseña del usuario root, quien tendrá acceso total al sistema.

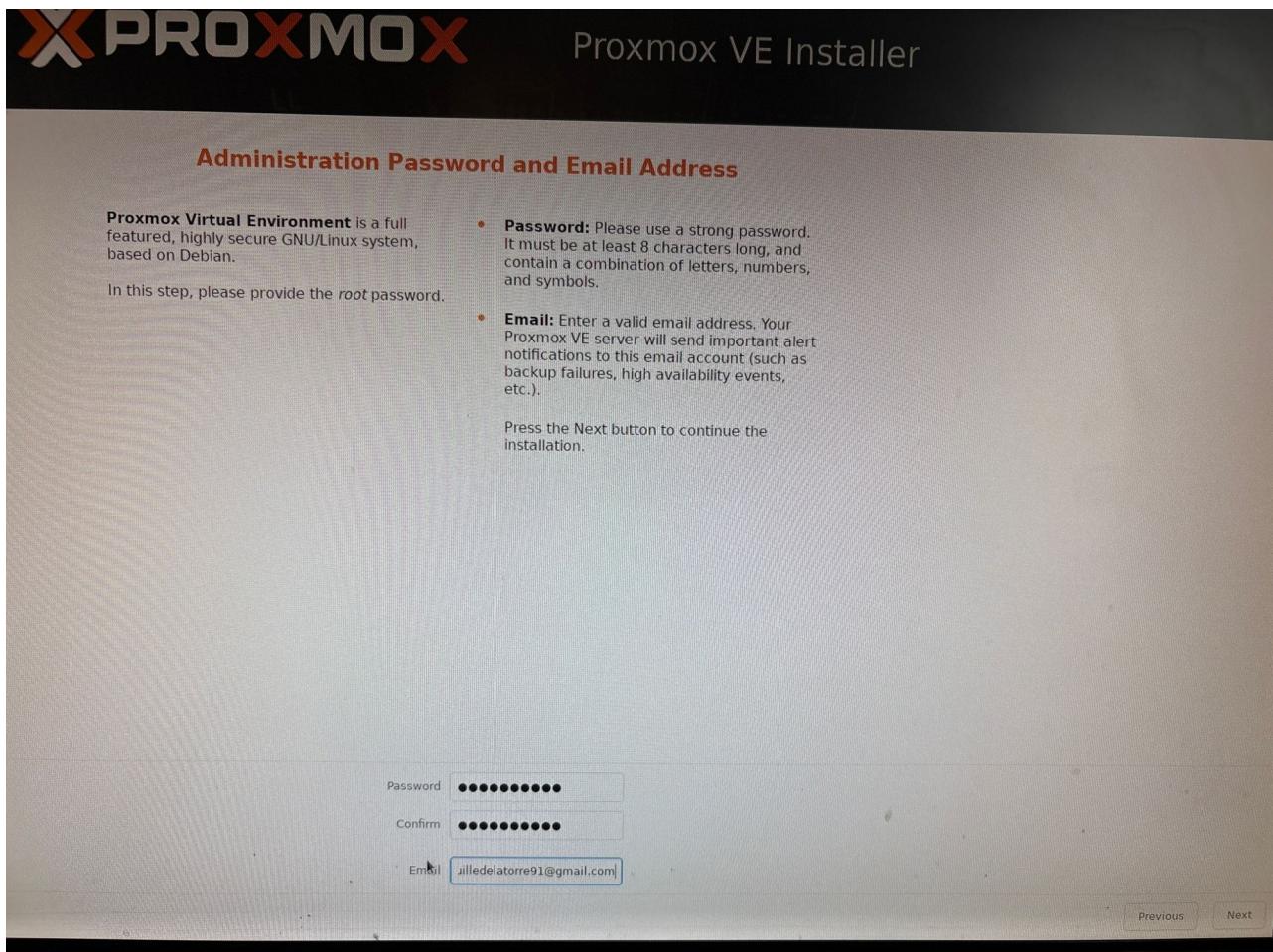


Figura 10: Instalación de Proxmox - Contraseña

También se introduce una dirección de correo válida, a la que el sistema puede enviar notificaciones (alertas de sistema, errores, etc.).

Es recomendable usar una contraseña segura (mínimo 8 caracteres, con símbolos, mayúsculas y números).

Nota: comprobar en el campo de “Email” los signos que usemos en nuestra contraseña por si no se ha configurado correctamente el teclado.

A1.2.6 Configuración de red

Se configura la interfaz principal (enp2s0) con una IP estática para asegurar acceso constante desde el navegador (si se configura por DHCP puede que en algún momento reciba una IP diferente y no sabremos en qué IP está).

Para este caso práctico he usado la que suele tener mi PC en la red doméstica, para asegurarme de que es una IP válida para proxmox en esta simulación. La puerta de enlace será mi router doméstico (192.168.1.1/24) y mi red doméstica será mi supuesta red de empresa.

Hostname (FQDN): pve001.mi-empresa.lan

IP address (CIDR): 192.168.1.35/24

Gateway: 192.168.1.1

DNS: 1.1.1.1

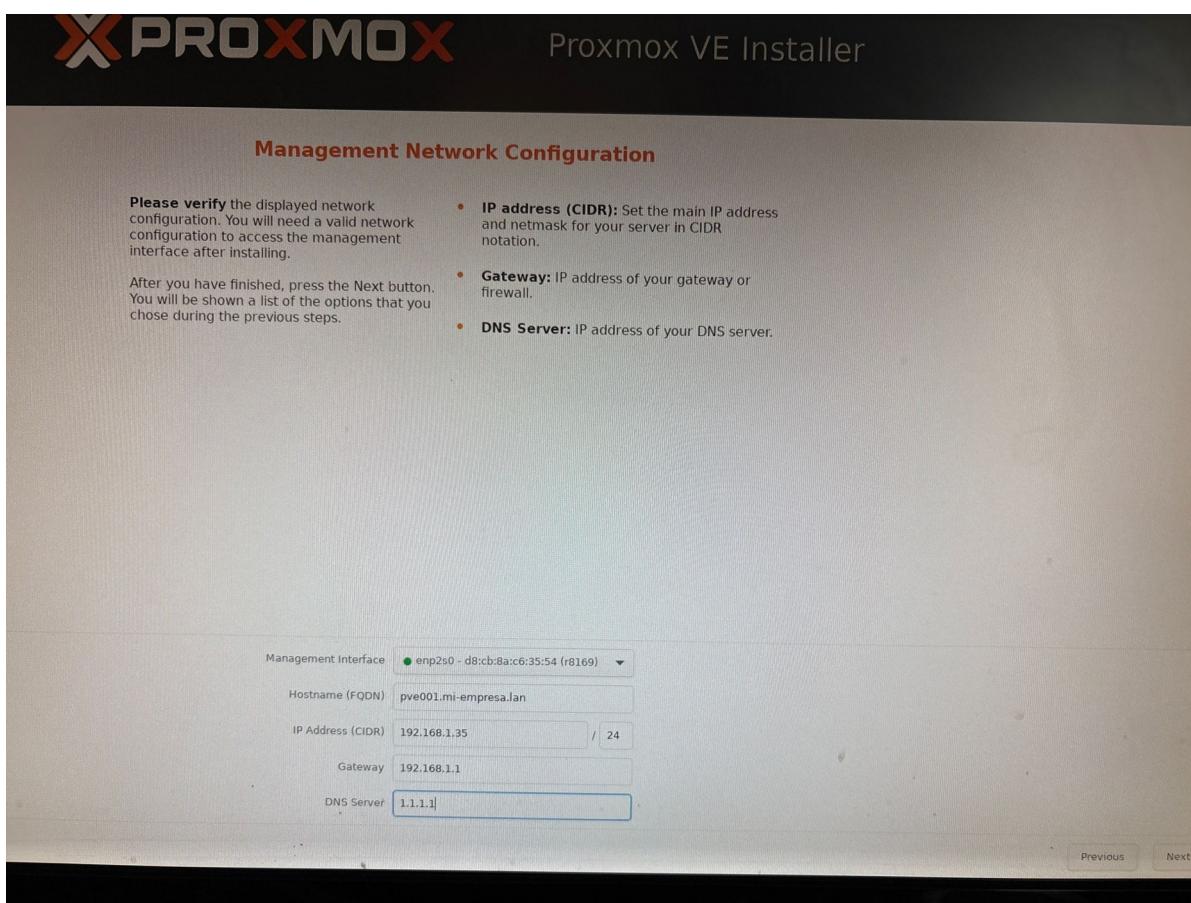


Figura 11: Instalación de Proxmox - Configuración de red

Esta IP será la usada posteriormente para acceder a la GUI de Proxmox.

A1.2.7 Confirmación final e instalación

Antes de iniciar la instalación, se presenta un resumen con todas las opciones seleccionadas.

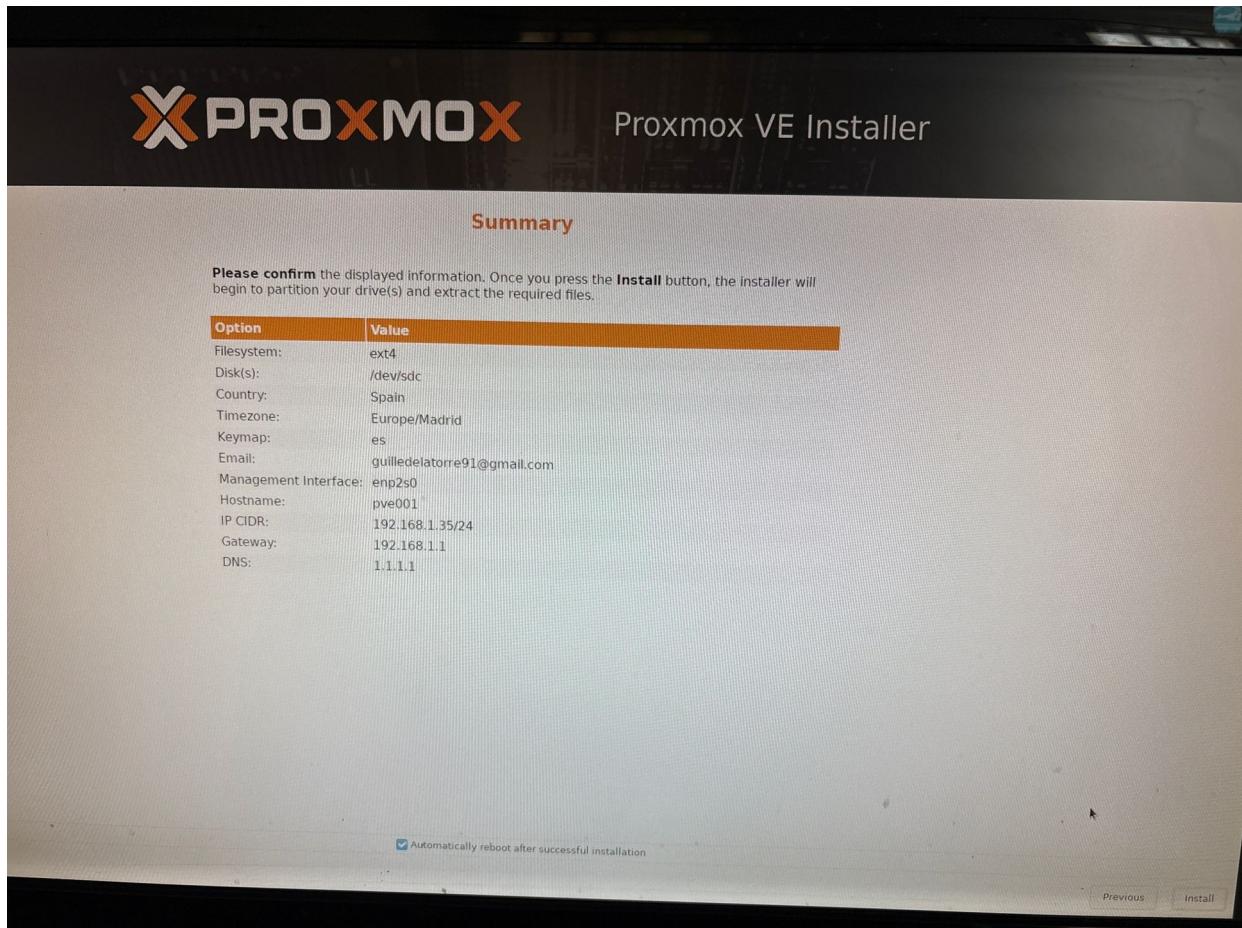


Figura 12: Instalación de Proxmox - Confirmación

Al pulsar Install, el instalador comienza a formatear el disco y copiar los archivos necesarios.

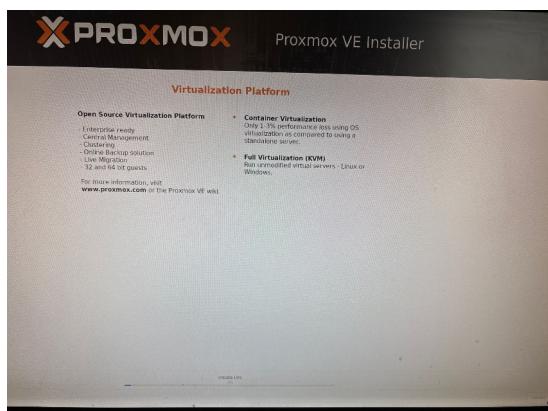


Figura 14: Instalación de Proxmox - Instalando

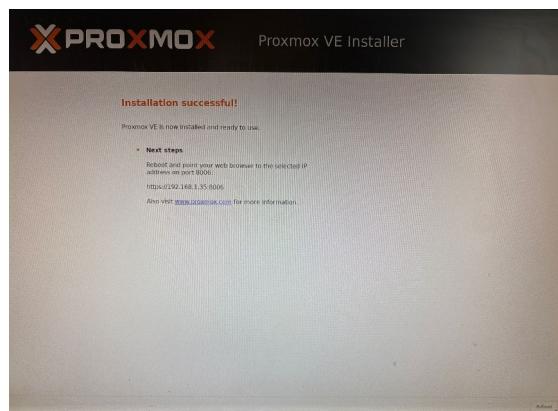


Figura 13: Instalación de Proxmox - Instalando 2

El proceso tardar dependiendo del hardware.

A1.2.8 Reboot y finalización

Al finalizar, el sistema solicita reiniciar el equipo. Se extrae el USB booteable antes de que vuelva a arrancar. (En mi caso al no ser la unidad de arranque habitual, selecciono en el menú de arranque el ssd donde se ha hecho la instalación).

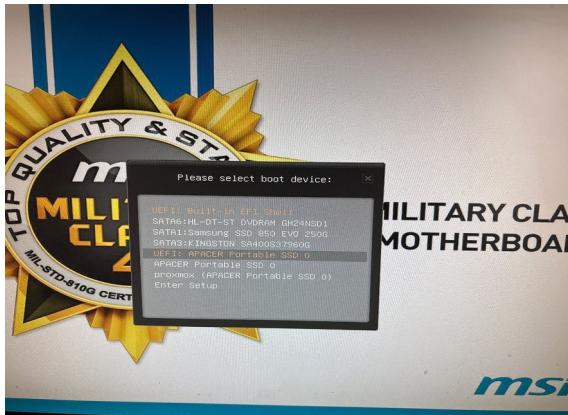


Figura 16: Selección de arranque desde el disco de instalación

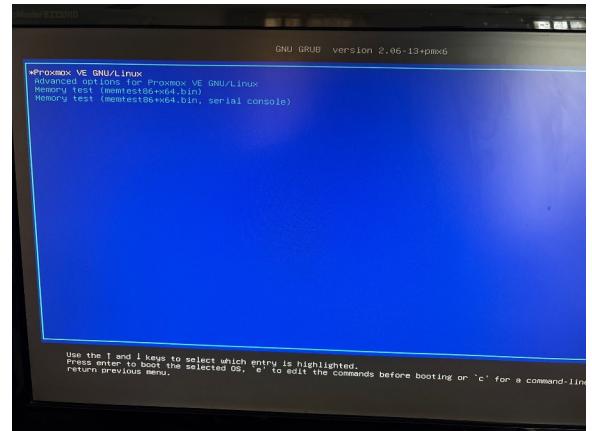


Figura 15: Primer inicio de Proxmox desde el SSD

El sistema queda listo para acceder y usarlo en modo terminal o acceder a la GUI desde otro equipo conectado a la misma red (al iniciar sesión aparece la dirección de red de acceso a la GUI).

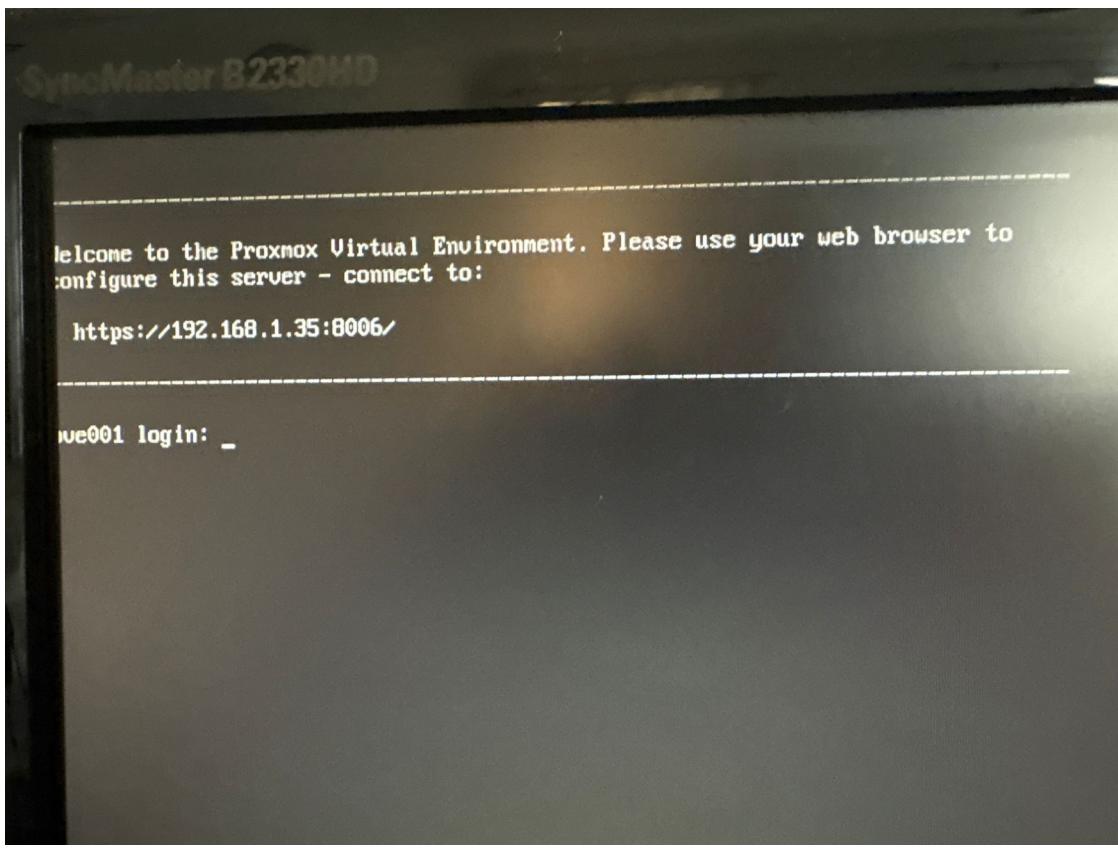


Figura 17: Login de Proxmox

Con esto, el hipervisor Proxmox queda instalado y operativo en el SSD físico, preparado para recibir y administrar máquinas virtuales.

A1.3. Acceso a la interfaz gráfica de Proxmox

Una vez instalado Proxmox VE en el SSD y reiniciado el equipo, el hipervisor queda accesible desde cualquier dispositivo conectado a la misma red, a través de su interfaz web. A continuación se detalla el procedimiento de acceso y los elementos clave visibles en el primer arranque.

A1.3.1. Dirección de acceso web

Proxmox se accede vía navegador utilizando el protocolo HTTPS y el puerto 8006.

Dirección de acceso : <https://192.168.1.35:8006>

Esta dirección debe introducirse en un navegador desde otro equipo conectado a la misma red LAN.

A1.3.2. Advertencia de seguridad del navegador

El navegador muestra una advertencia porque el certificado TLS de Proxmox no está firmado por una autoridad certificadora de confianza.

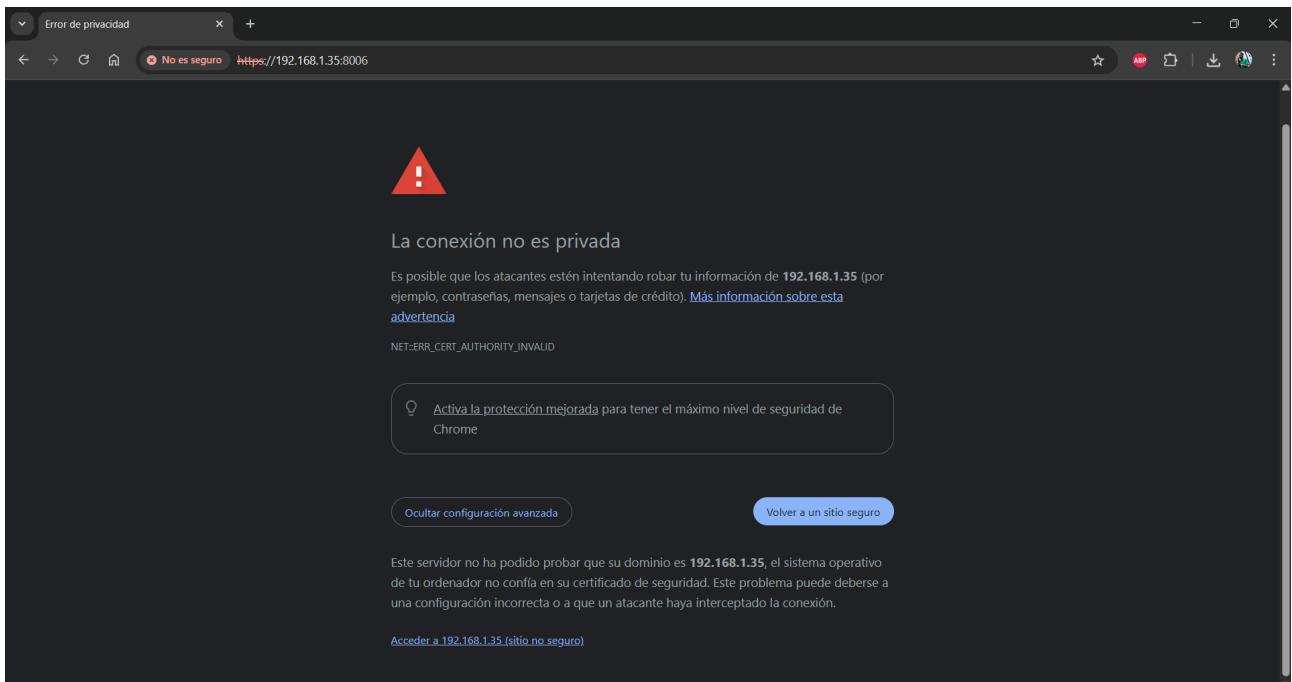


Figura 18: Advertencia de seguridad (certificado Self-signed)

Esto es normal en entornos locales (certificados autofirmados), en lugar certificados públicos de alguna CA reconocida.

Se puede avanzar haciendo clic en "*Avanzado*" > "*Acceder igualmente a 192.168.1.35 (sitio no seguro)*".

A1.3.4 Pantalla de inicio de sesión

Campos requeridos:

Username: root

Password: la definida durante la instalación

Realm: Linux PAM standard authentication (por defecto)

Idioma de la interfaz: seleccionable (se puede elegir "Spanish" si se desea)

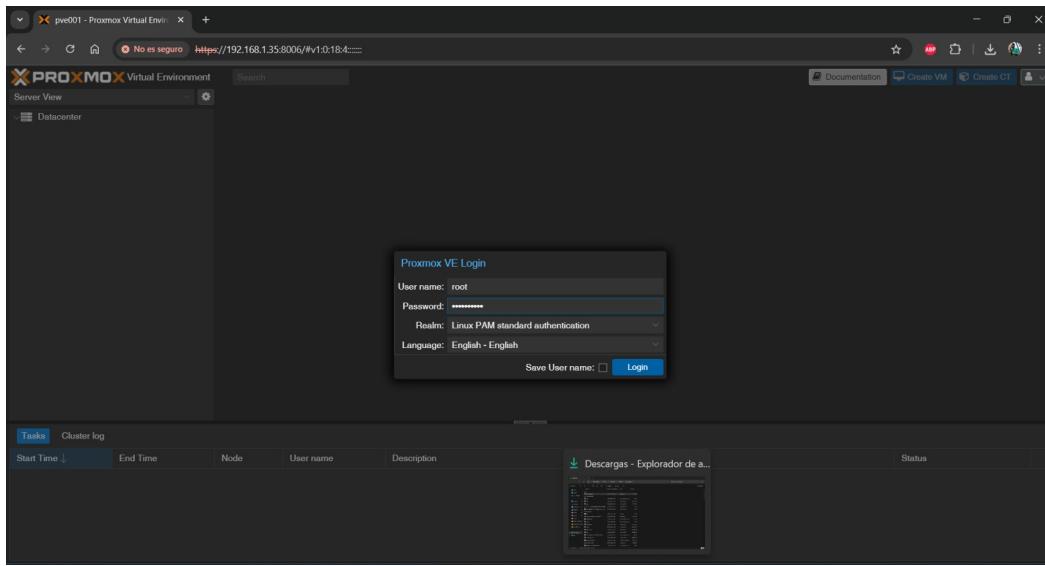


Figura 19: Interfaz Web Proxmox - login

Una vez introducidas las credenciales, se accede a la interfaz principal de gestión.

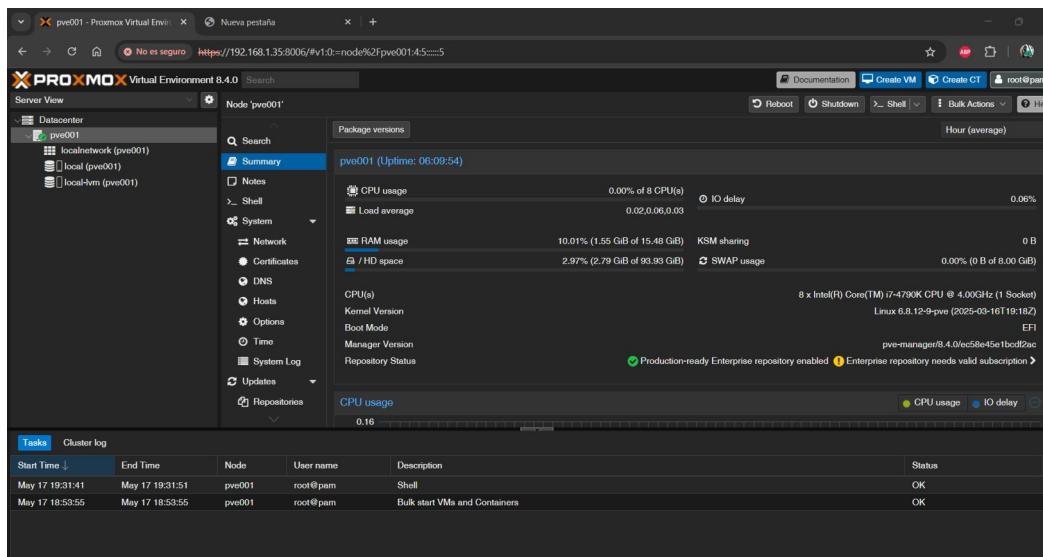


Figura 20: Interfaz Web Proxmox - Información del servidor

Anexo 2: Creación de la máquina virtual: Windows Server 2025

Este anexo documenta la instalación inicial de Windows Server 2025 como máquina virtual dentro del hipervisor Proxmox VE. Se detalla la carga de drivers VirtIO necesarios para reconocer el disco virtual, así como los primeros pasos de instalación desde la ISO oficial.

Este proceso representa la base para desplegar posteriormente los servicios de dominio, DNS y DHCP que centralizan la red simulada.

A2.1. Subida de la imagen ISO a Proxmox

Desde la interfaz web de Proxmox se accede al almacenamiento local del nodo (local).

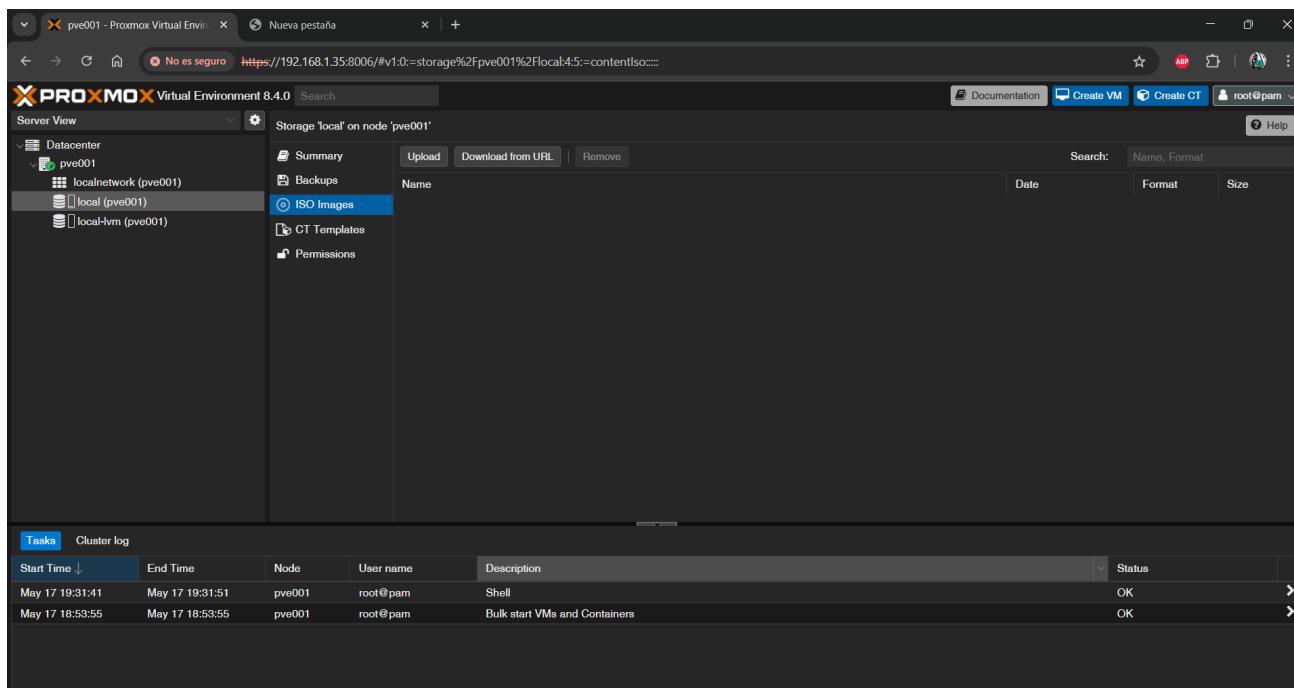


Figura 21: Interfaz Web Proxmox - Almacenamiento local

En la pestaña Content, se hace clic en Upload.

Se selecciona el archivo .iso correspondiente a Windows Server 2025 y se sube al almacenamiento para que esté disponible al crear la VM

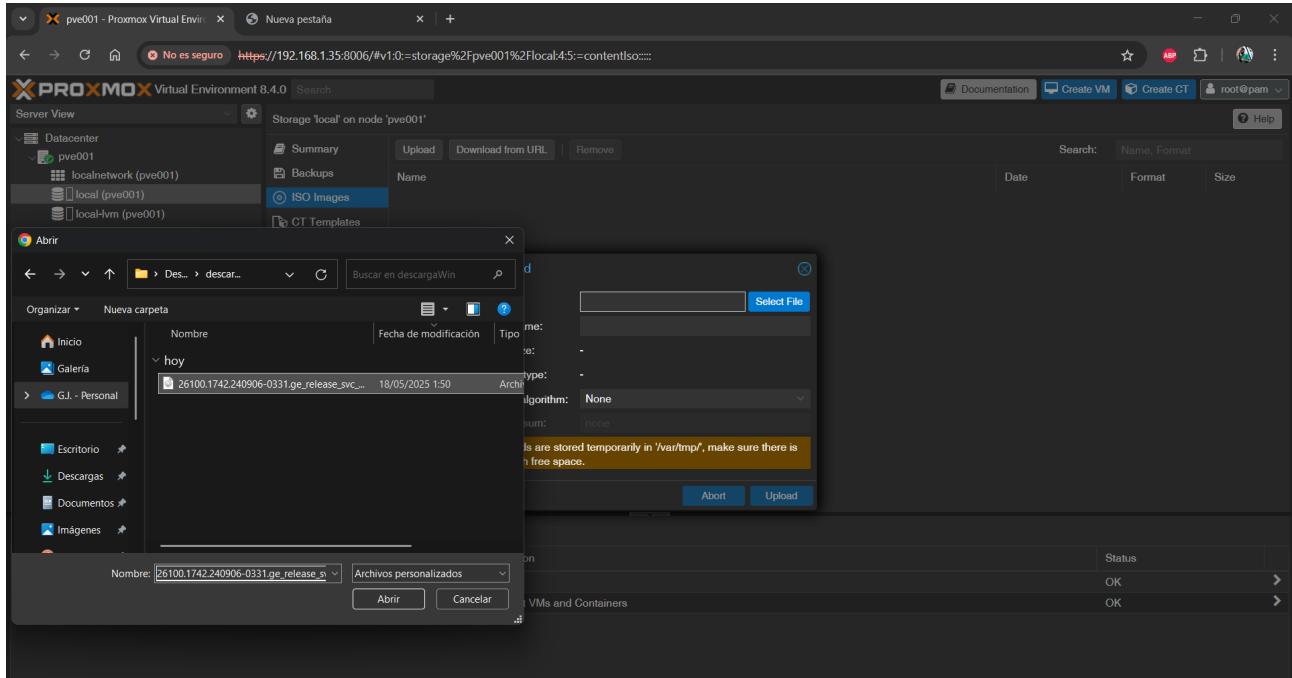


Figura 22: Proxmox - Seleccionar ISO

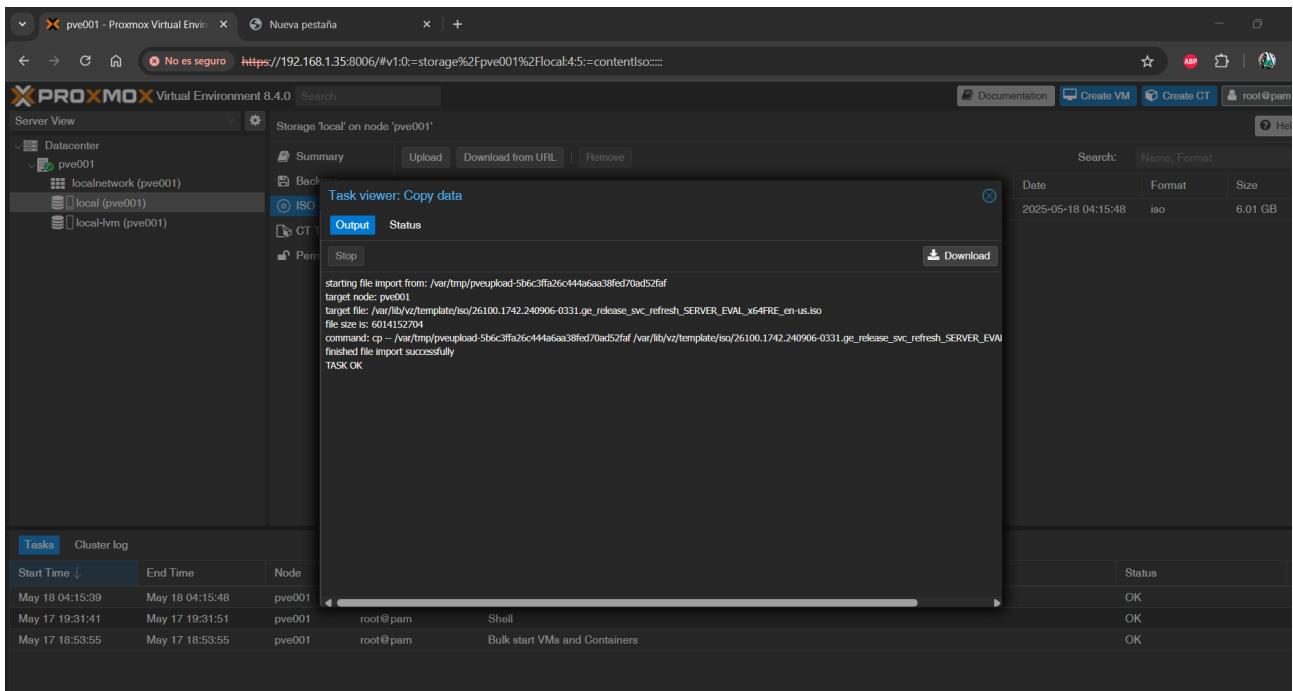


Figura 23: Confirmación subida ISO

Es necesario repetir este mismo paso para subir la ISO de drivers VirtIO, que se montará como segunda unidad de CD para instalar controladores durante la instalación de Windows.

A2.2. Creación de la máquina virtual

Desde el panel izquierdo se selecciona el nodo (pve001) y se pulsa en Create VM. Se asigna un nombre identificativo a la VM, como win-server-2025.

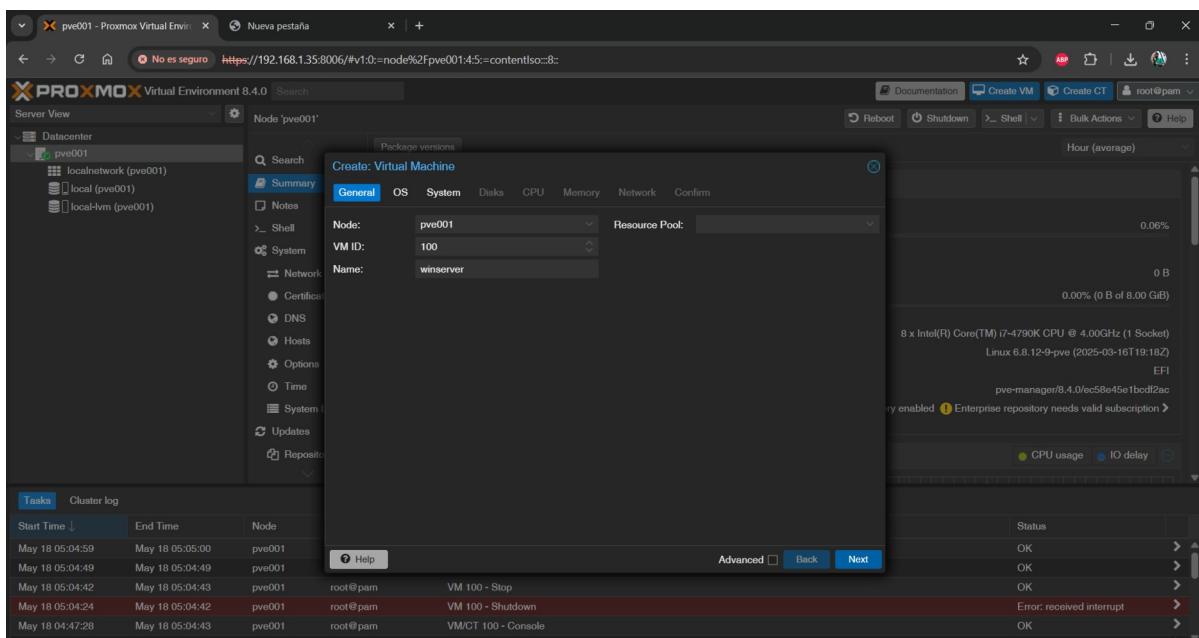


Figura 24: Configuración máquina Windows Server - General

Se elige la imagen ISO de instalación subida previamente. Si se activa la casilla “Add additional drive for VirtIO drivers” te permitirá introducir en la segunda unidad de CD debe configurarse con la ISO de VirtIO para poder cargar los controladores del disco y red durante la instalación.

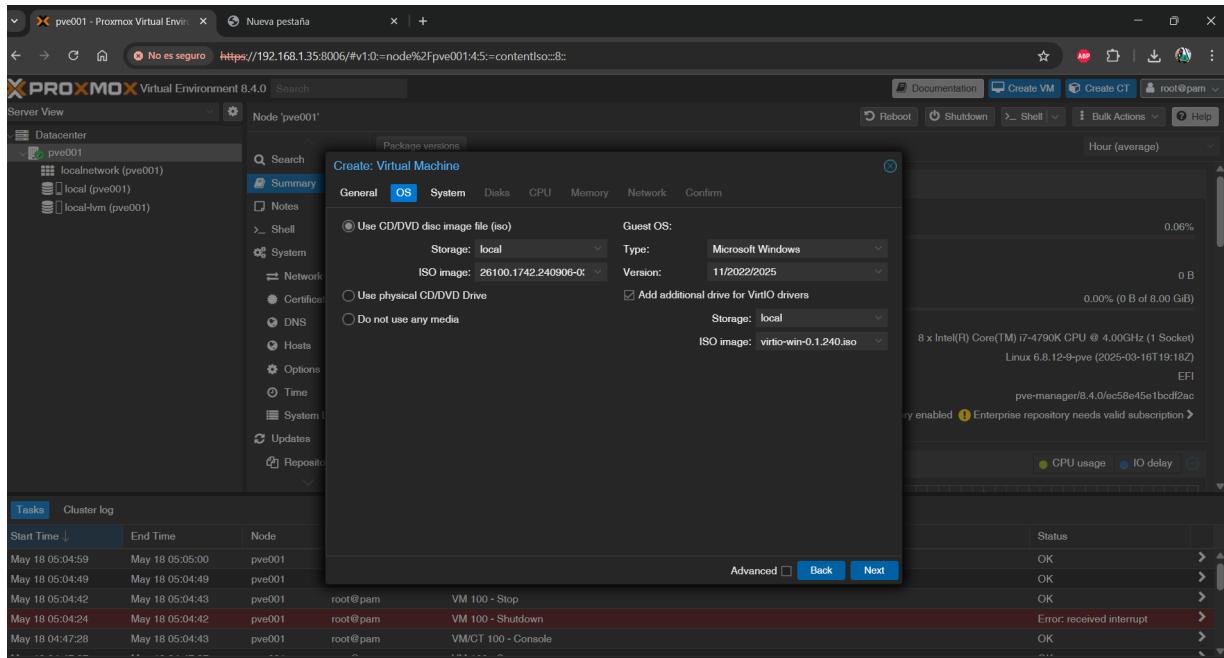


Figura 25: Configuración máquina Windows Server - OS

Configuración clave:

Sistema de disco: VirtIO SCSI single (mayor rendimiento en entornos virtualizados)

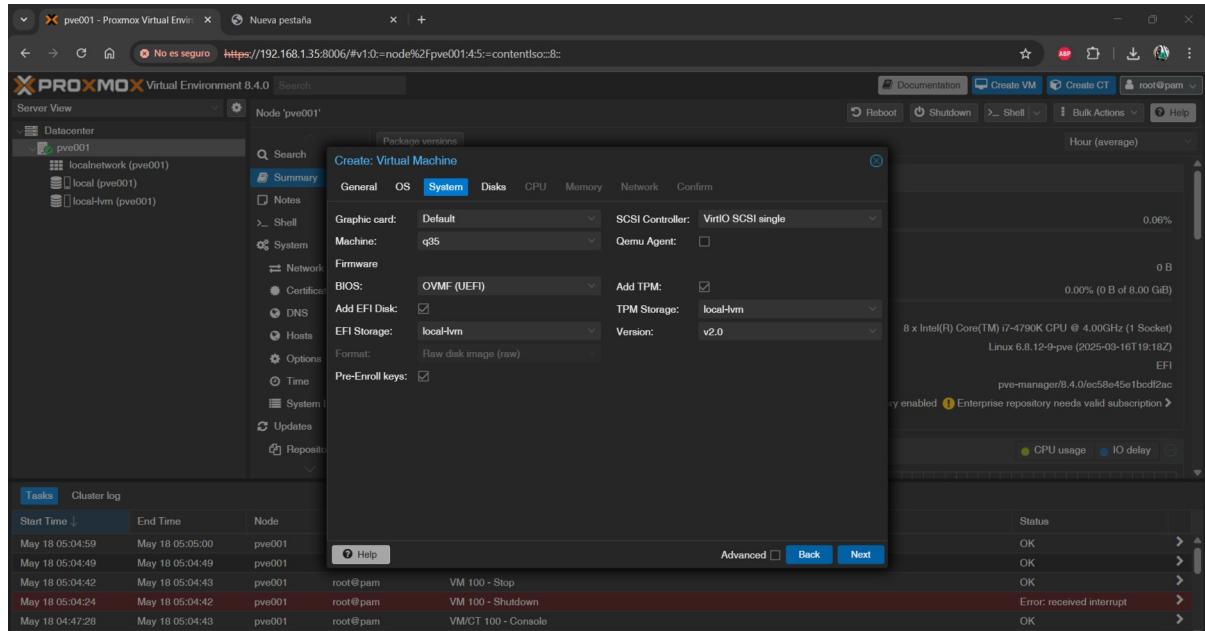


Figura 26: Configuración máquina Windows Server - System

Disco:

Ya que el ssd es de 512GB y hay espacio de sobre le he asignado 60GB a la máquina de Windows Server que para pruebas debe ser más que suficiente.

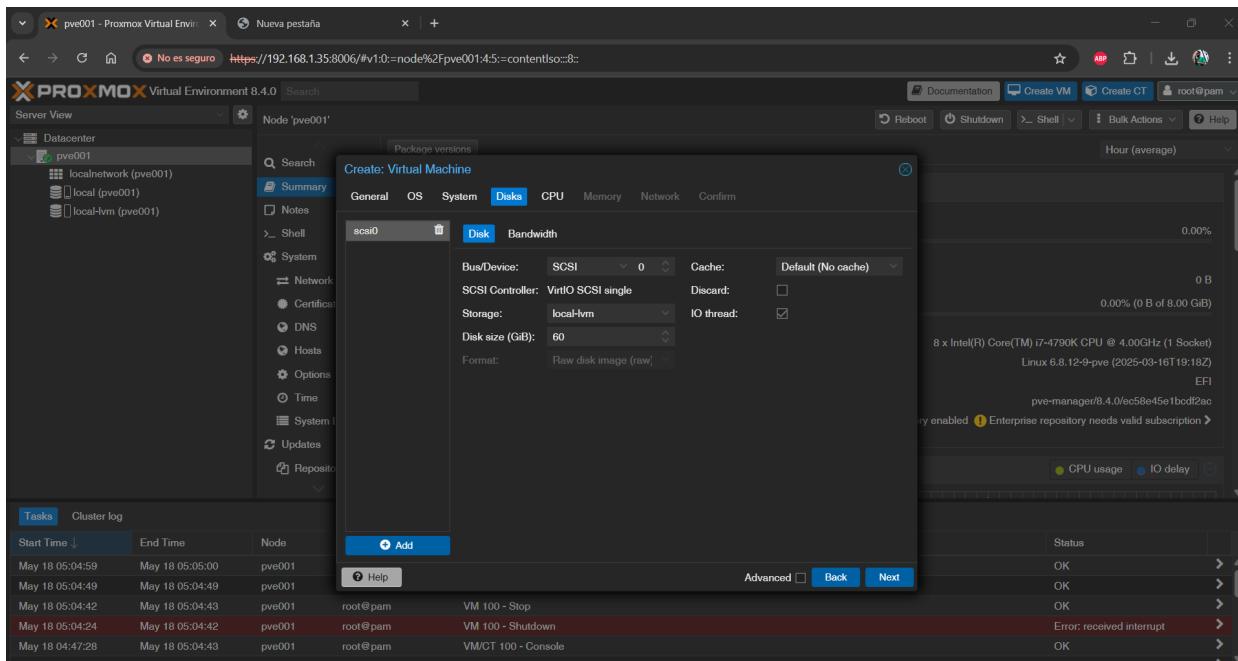


Figura 27: Configuración máquina Windows Server

Procesador: 2 o más núcleos (yo puse 4).

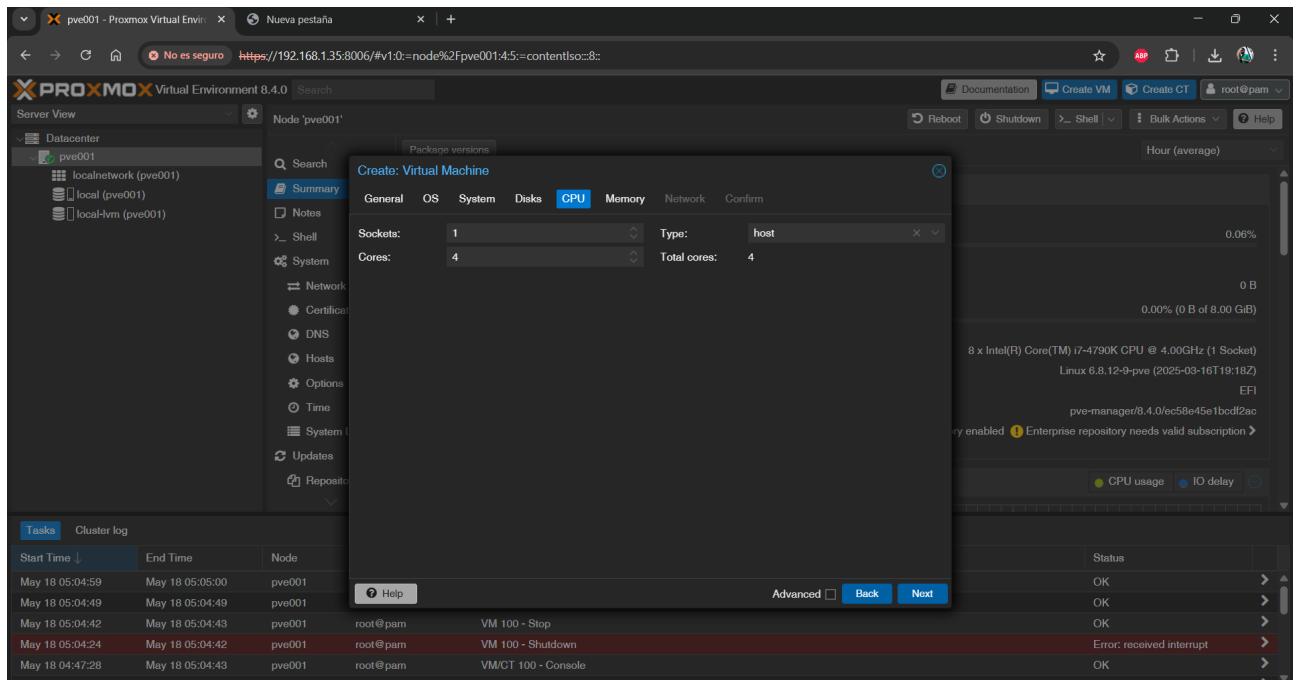


Figura 28: Configuración máquina Windows Server

Memoria RAM inicial: 16 GB

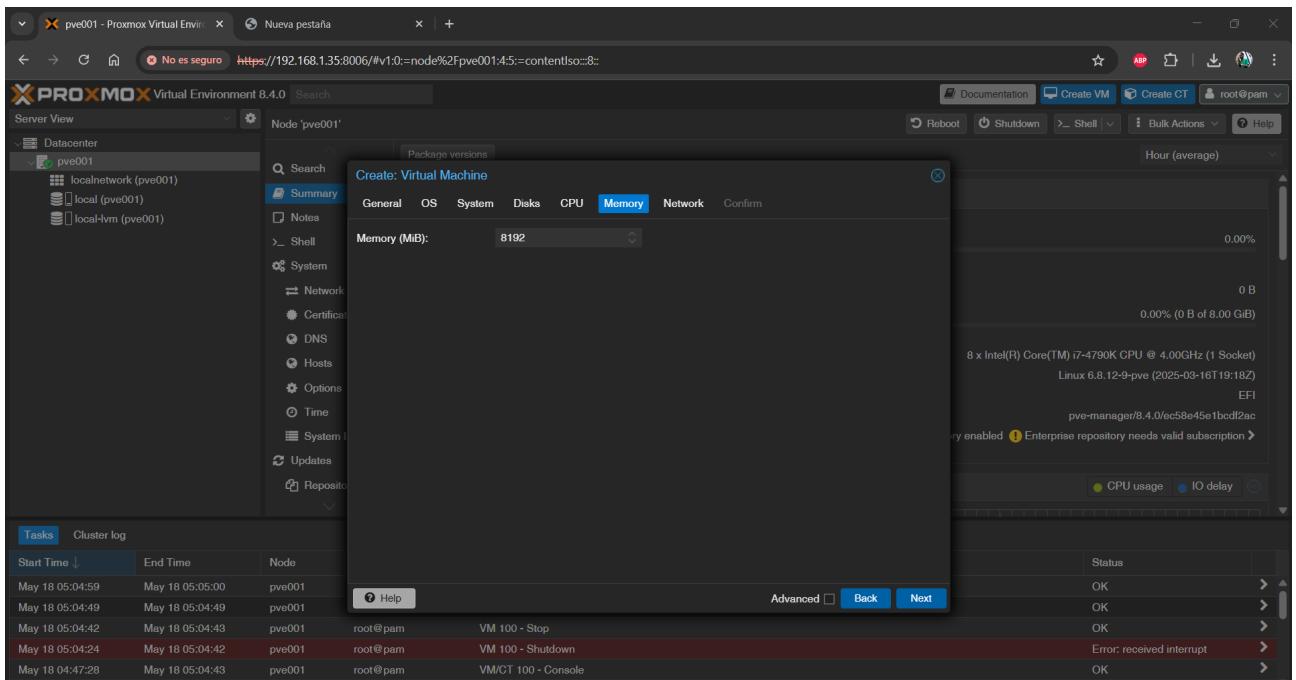


Figura 29: Configuración máquina Windows Server - memoria

Interfaces de red: seleccionar la interfaz bridge por defecto **vmbr0**, model: **VirtIO (paravirtualized)**.

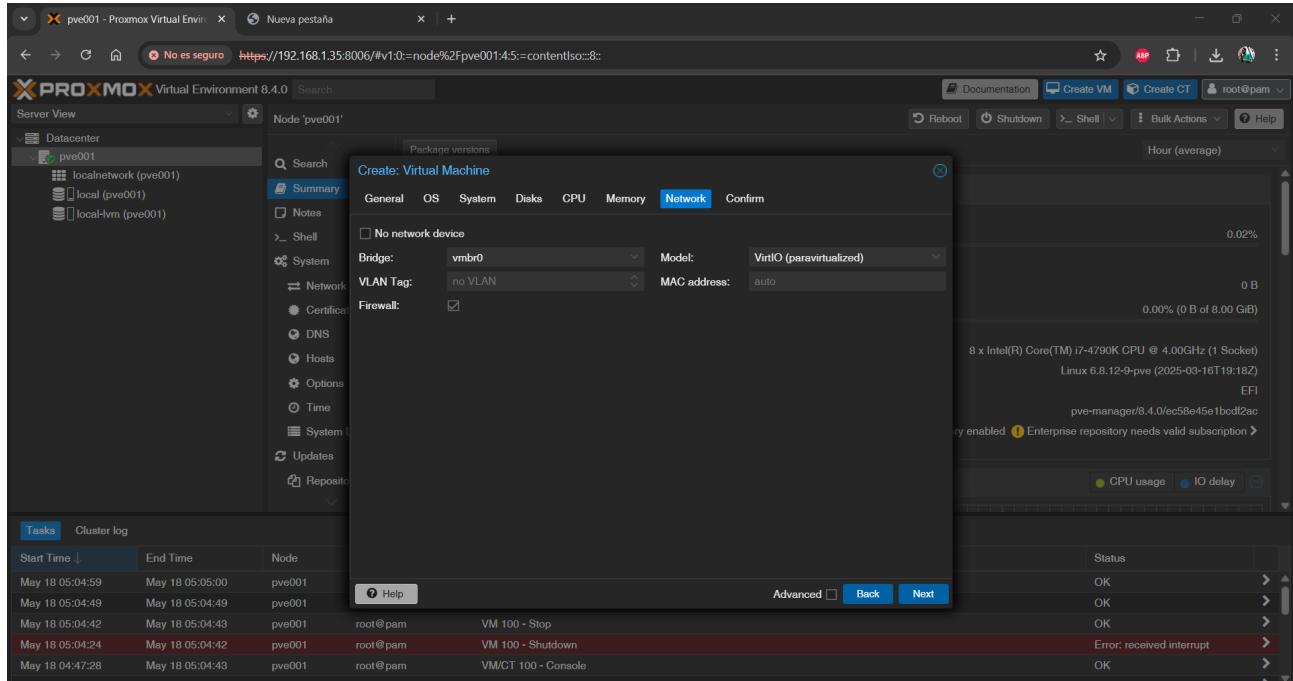


Figura 30: Configuración máquina Windows Server - Red

Nota: Para que funcione correctamente la interfaz ethernet de la VM se requieren drivers específicos que se instalarán más adelante).

Resumen final: en el ultimo paso para la creación de máquinas virtuales se muestra el resumen de

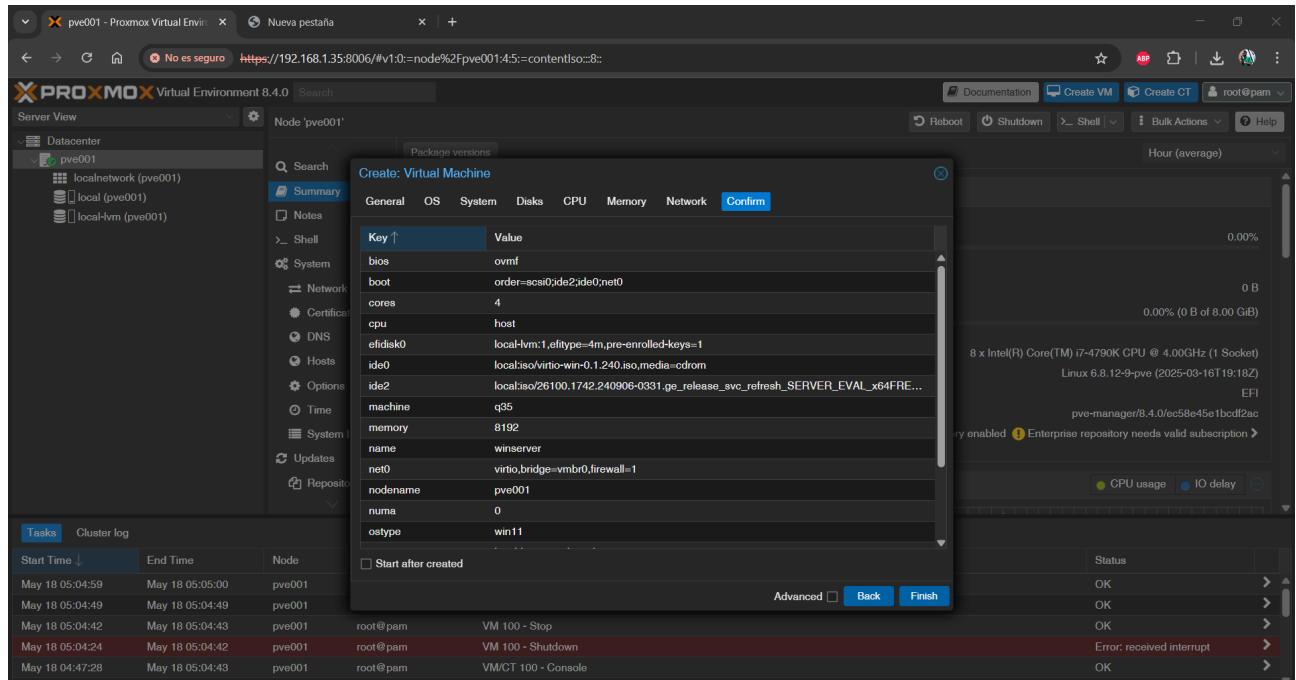


Figura 31: Configuración máquina Windows Server - confirmación final

la configuración que se le ha dado a través del asistente. Si esta todo correcto **Finish**

A2.3. Inicio de Instalación

Una vez finalice la creación de la máquina se puede arrancar haciendo clic derecho en el menú de la izquierda sobre ella y dandole a “**Start**”.

Para ver la salida de pantalla de la máquina: seleccionar la máquina creada para que se muestre su menú y seleccionar la pestaña **Console**.

Una vez hecho esto, proceder con la instalación normal de windows server hasta llegar a la selección de disco.

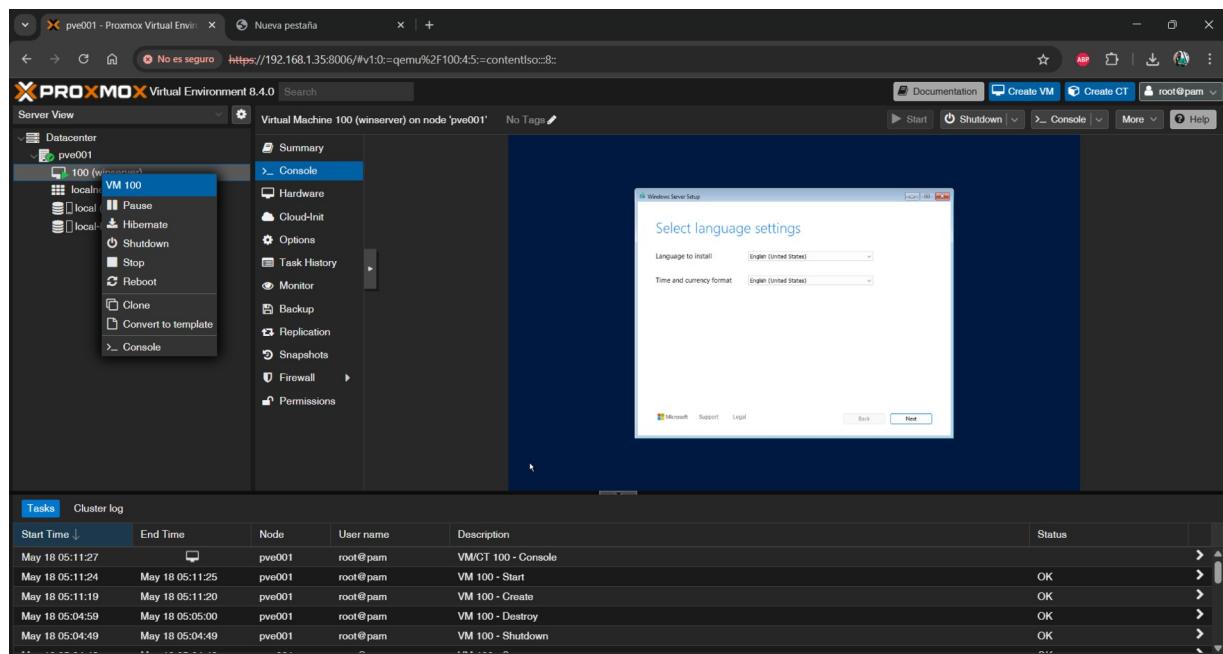


Figura 32: Instalación Windows Server - Lenguaje

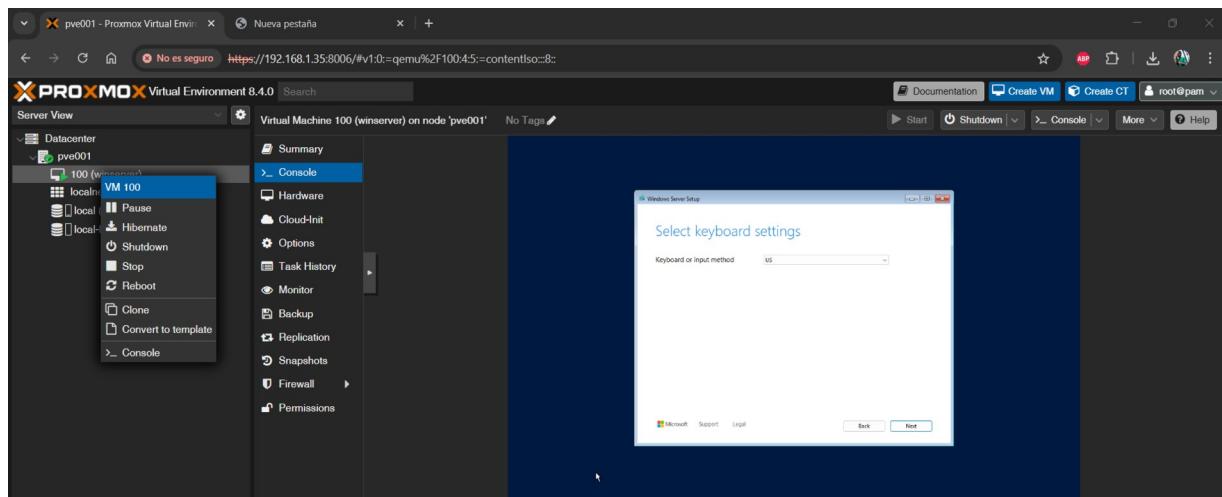


Figura 33: Instalación Windows Server - layout de teclado

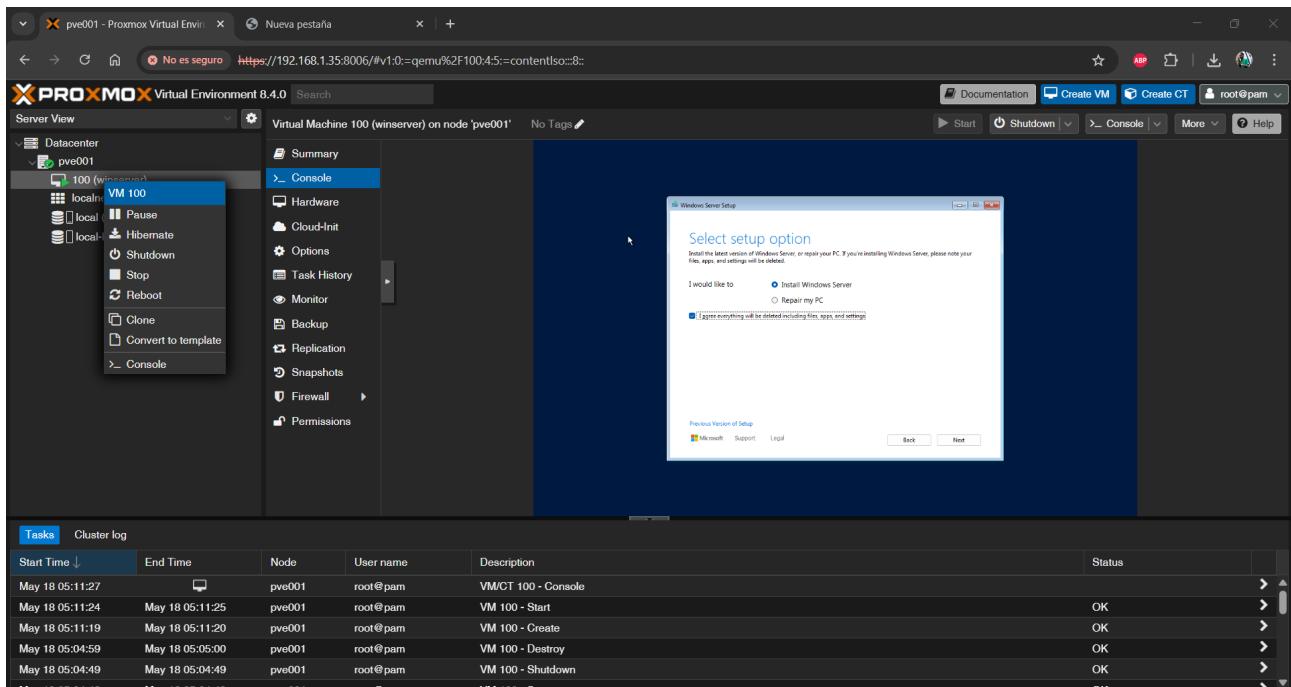


Figura 34: Instalación Windows Server

Importante: seleccionar la versión **Desktop** si se quiere una experiencia de escritorio.

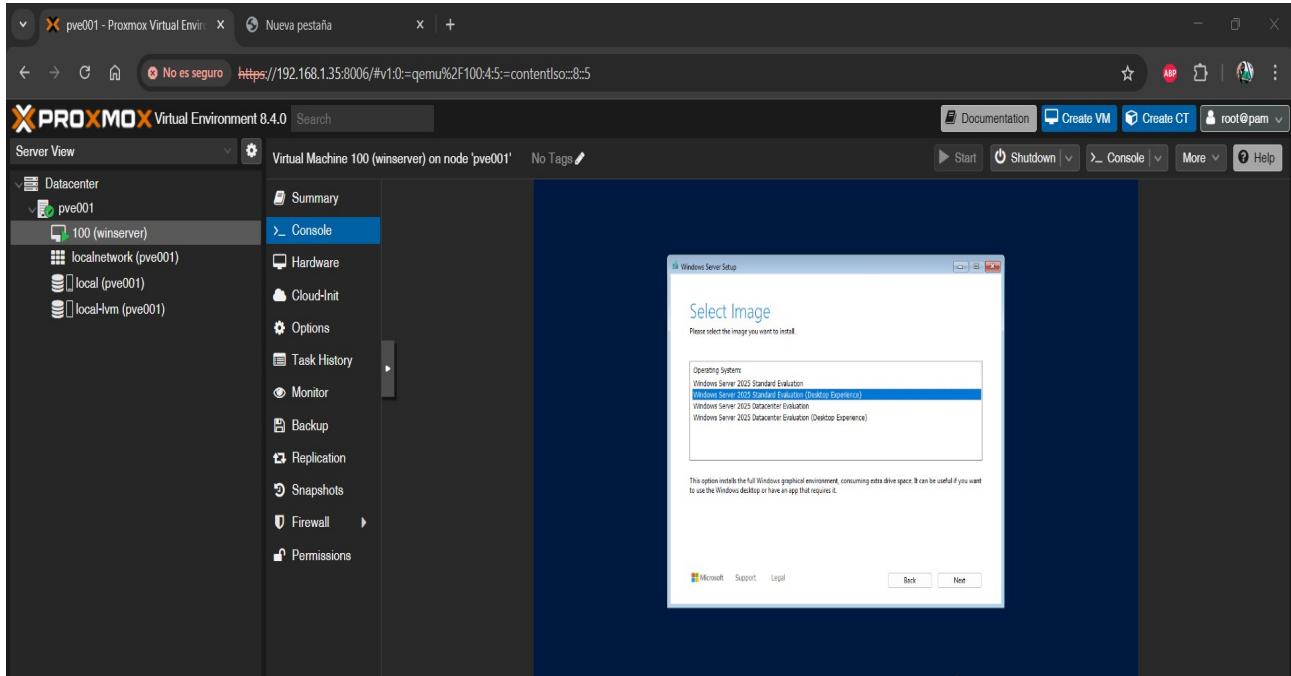


Figura 35: Instalación Windows Server -

Al llegar a la pantalla de selección de discos aparece vacía, esto es porque windows no reconoce el disco creado para la máquina virtual, necesita instalar drivers adicionales. Para ello pulsar en “**Load driver**”.

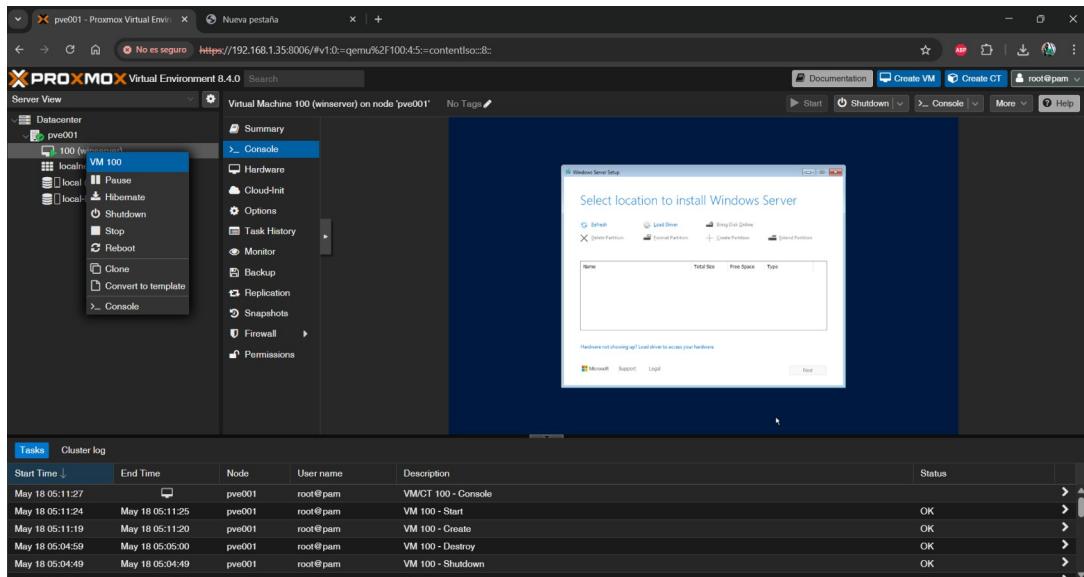


Figura 36: Instalación Windows Server - Drivers disco

En la ventana emergente, hacer clic en “**Browse**”. Navegar a la unidad que contiene la ISO de VirtIO (segunda unidad de CD configurada en Proxmox en la ruta `vioscsi > w11 > amd64`)

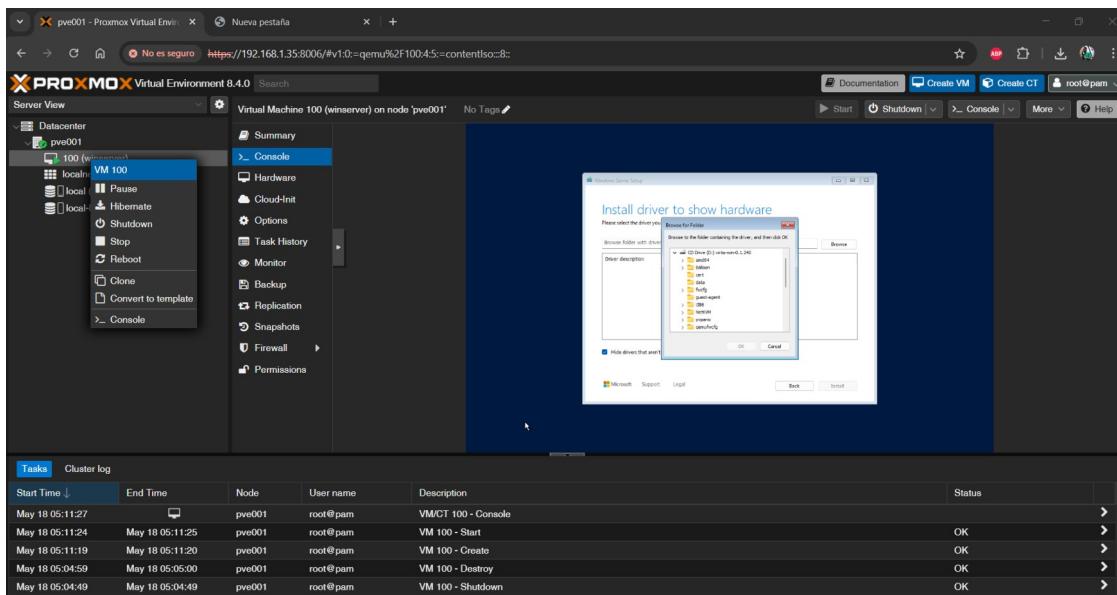


Figura 37: Instalación Windows Server – VirtIO

Aunque se está utilizando Windows Server 2025, la carpeta correspondiente a Windows 11 (w11/amd64) incluye controladores completamente compatibles debido a que ambas versiones comparten la misma base tecnológica moderna.

Una vez seleccionado el controlador adecuado, se pulsa “Next” y el sistema detecta el disco virtual

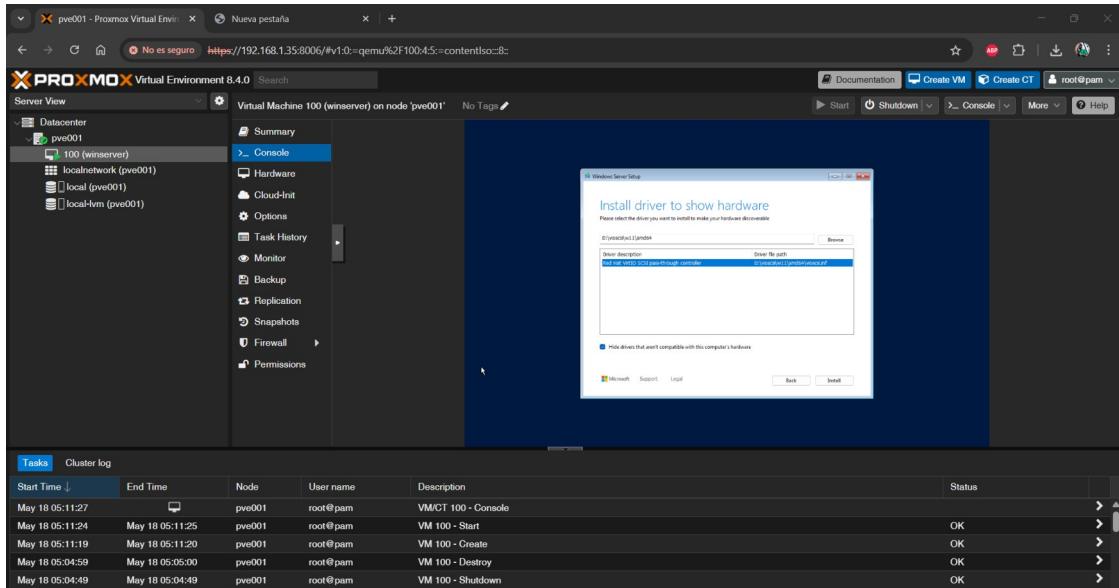


Figura 38: Instalación Windows Server – Drivers disco

correctamente, mostrándolo como unidad disponible para instalar. Seleccionar el disco y dar en “Siguiente”.

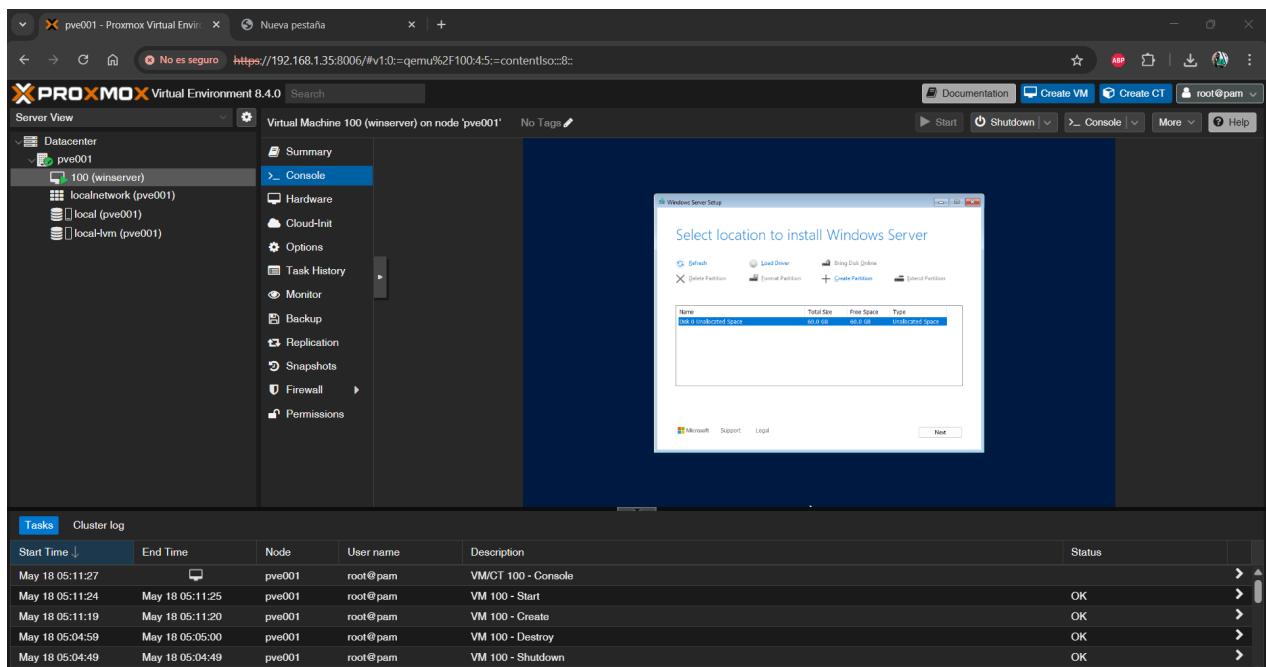


Figura 39: Instalación Windows Server - Selección de disco

Con esto ya está listo para seguir la instalación habitual.

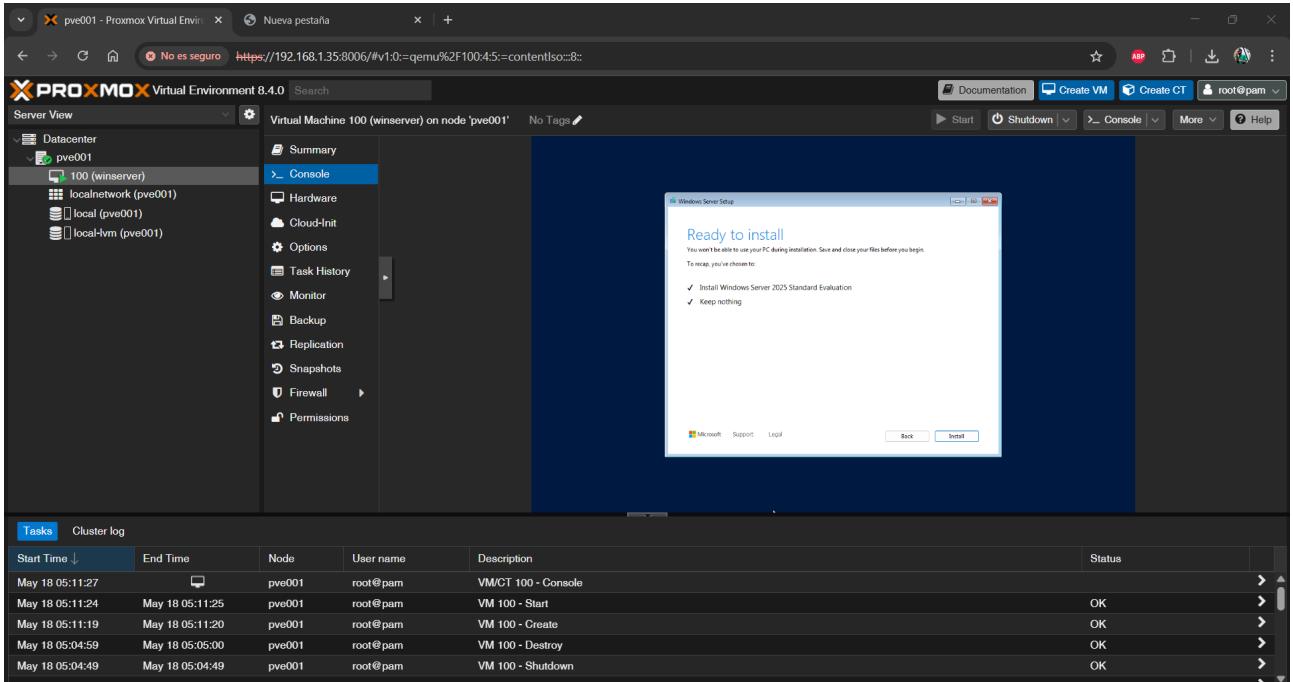


Figura 40: Instalación Windows Server

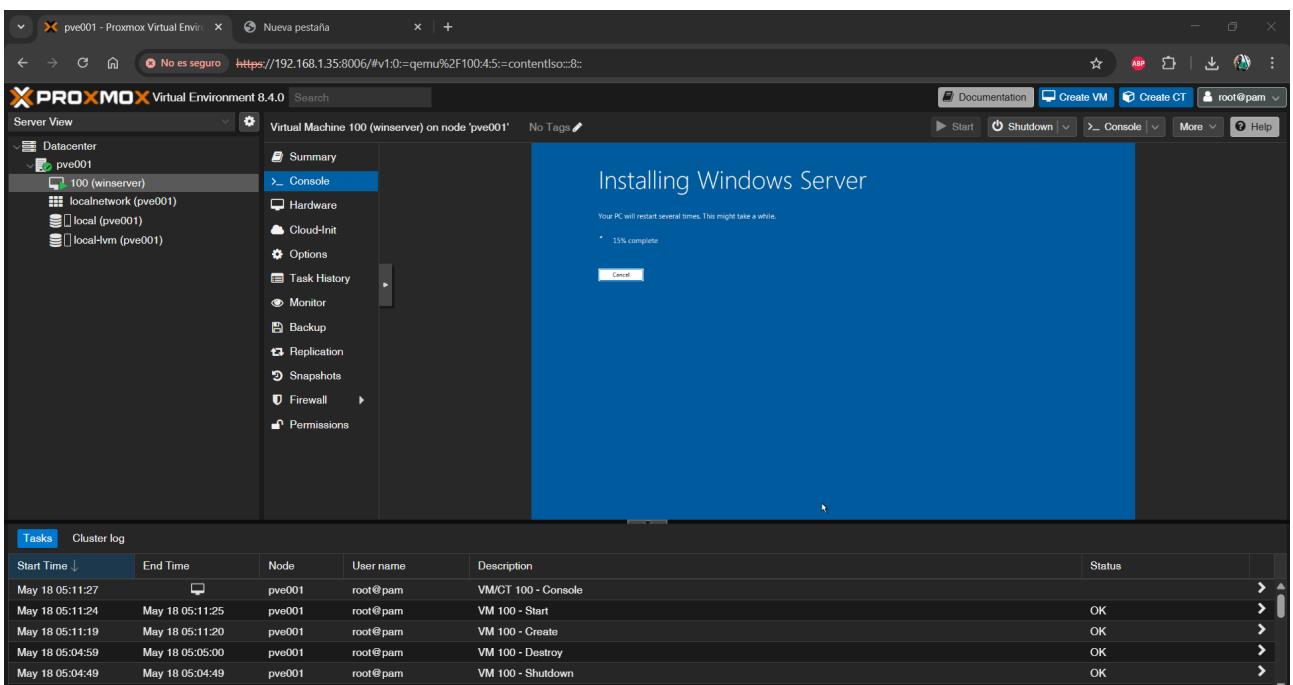


Figura 41: Instalación Windows Server

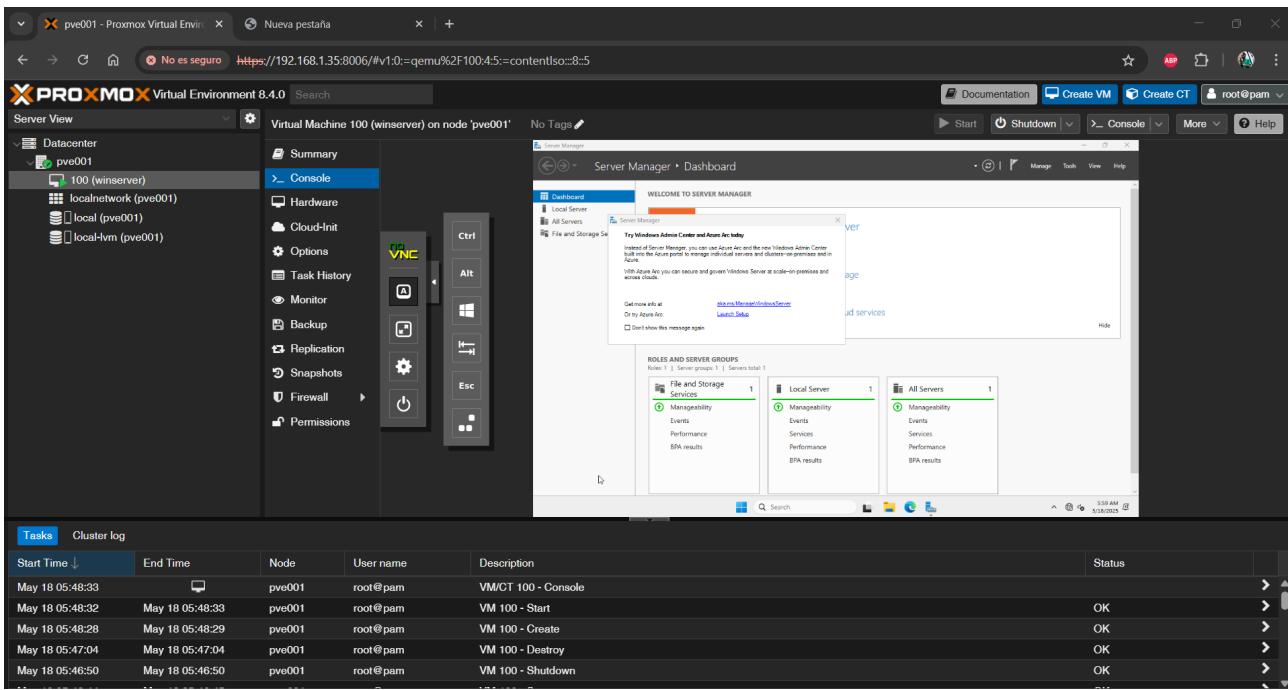


Figura 42: Instalación Windows Server - Primer arranque

A2.4. Instalación base y primeros ajustes del sistema

Tras completar la instalación del sistema operativo, Windows Server 2025 arranca por primera vez y solicita las credenciales configuradas durante la instalación. Una vez dentro del sistema, se realizan varios ajustes iniciales clave para preparar el entorno de dominio.

A2.4.1. Instalacion de drivers VirtIO

Al no tener aún instalado el controlador de red, el sistema no muestra conectividad y aparecen en **Device Manager (administrador de dispositivos)** algunos dispositivos con un símbolo de advertencia en algunos dispositivos de red sin reconocer, entre ellos las controladoras ethernet y pci (para que reconozca algunos dispositivos pci conectados).

Para instalar los drivers de red, hacer clic derecho en la entrada que pone “ehternet” con exclamación y hacer clic derecho propiedades

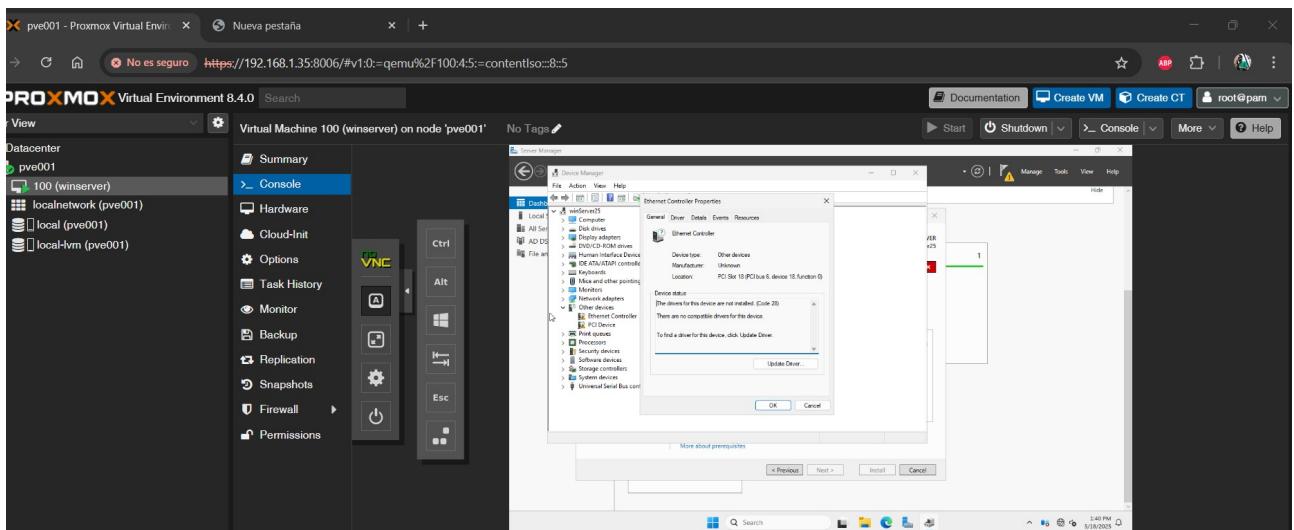


Figura 43: Maquina Windows Server - drivers VirtIO

Buscar en mi ordenador .

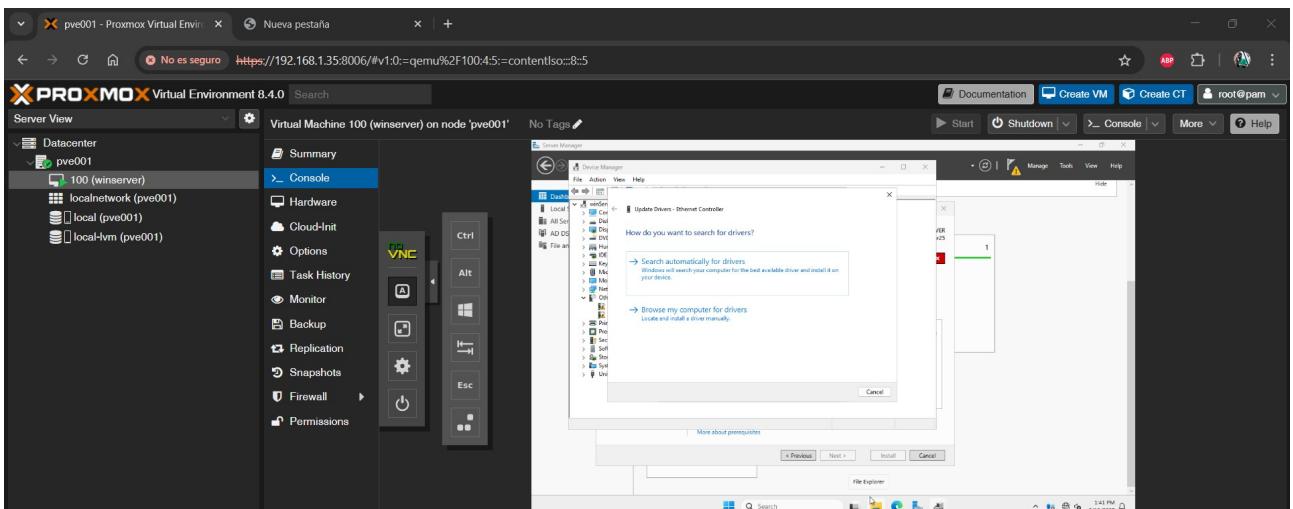
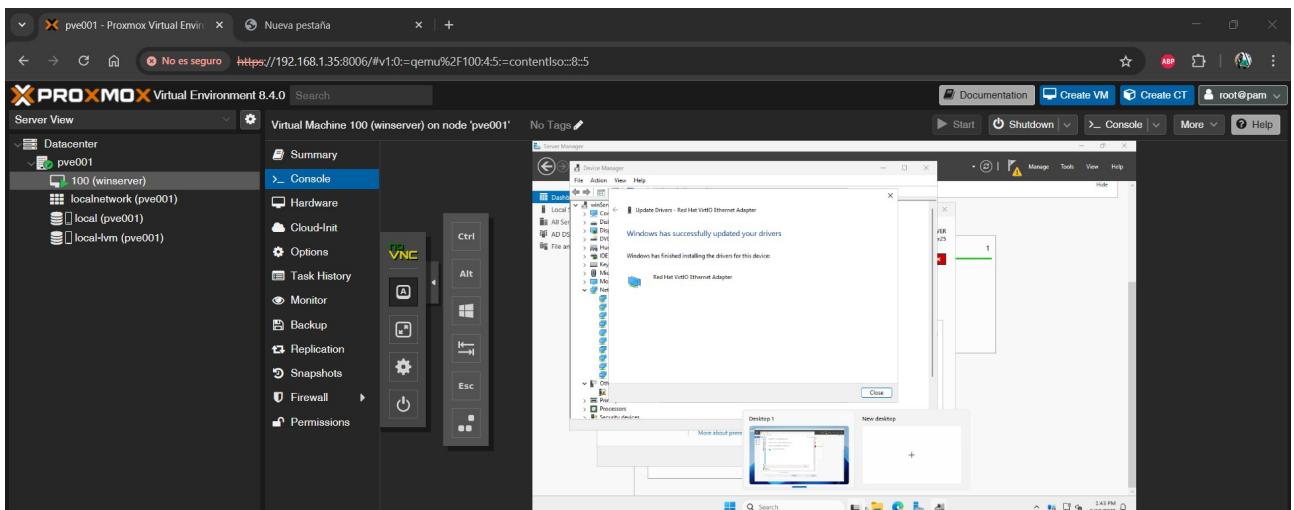
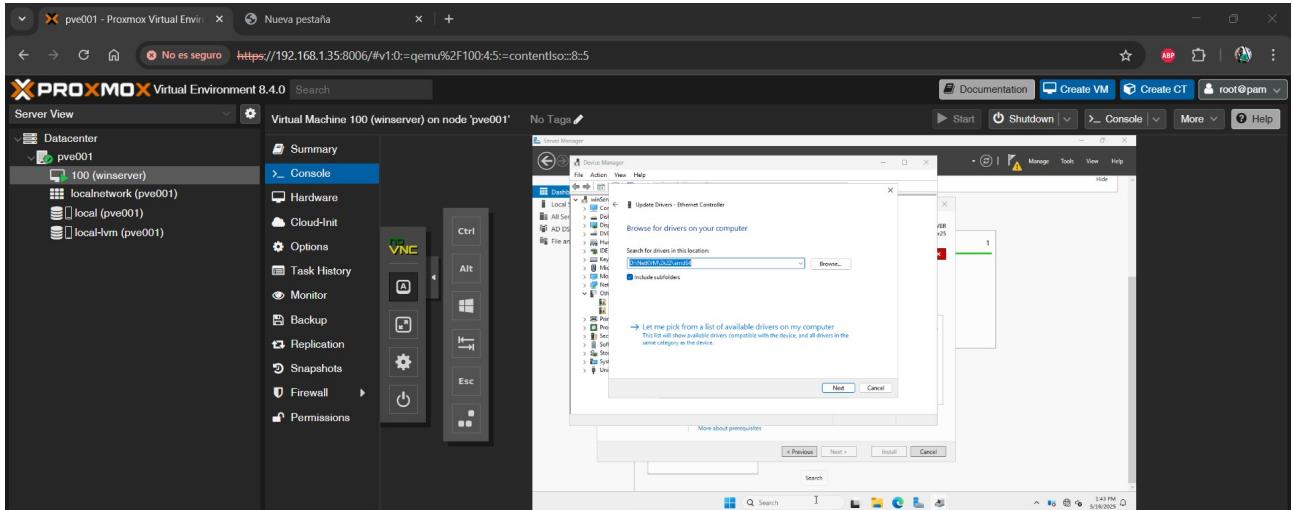
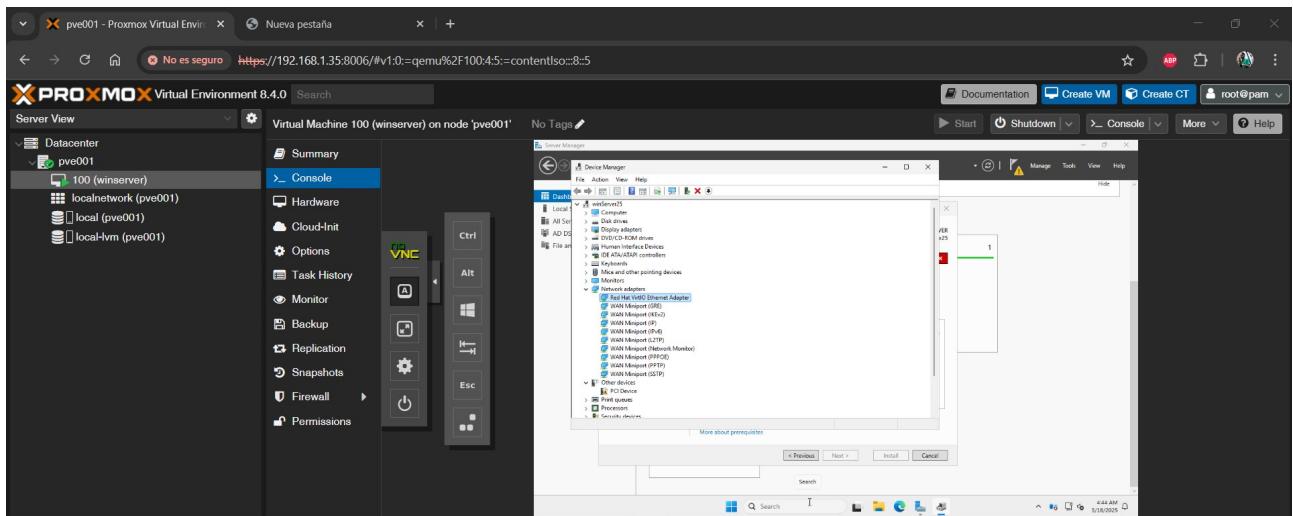


Figura 44: Maquina Windows Server - drivers VirtIO

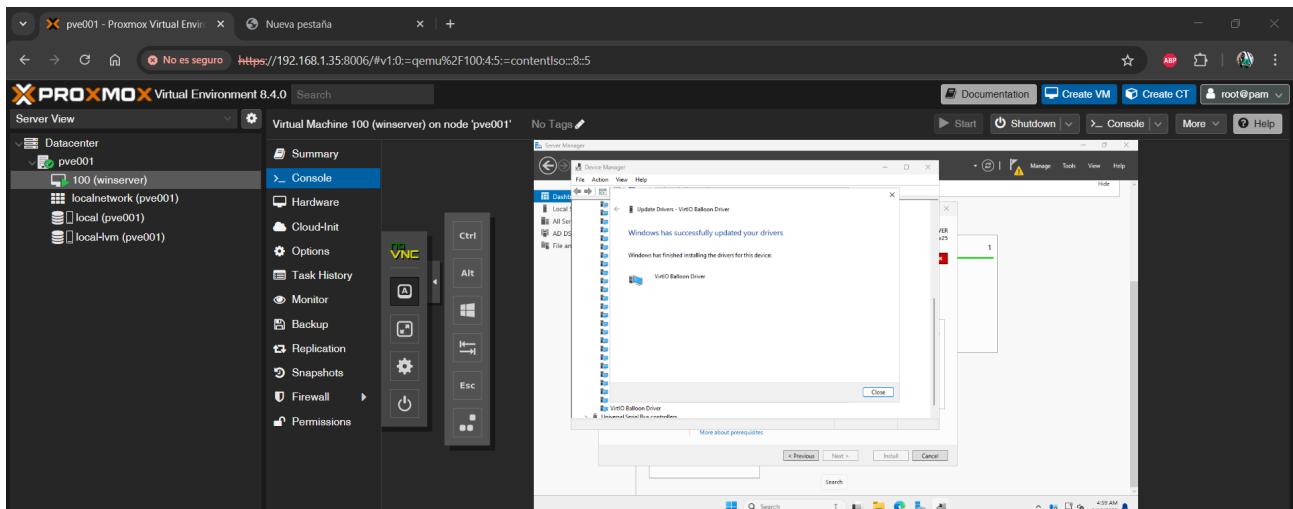
Buscar en los driver VirtIO la subcarpeta NetKVM/2k22



Una vez hecho esto ya aparece los dispositivos de red.

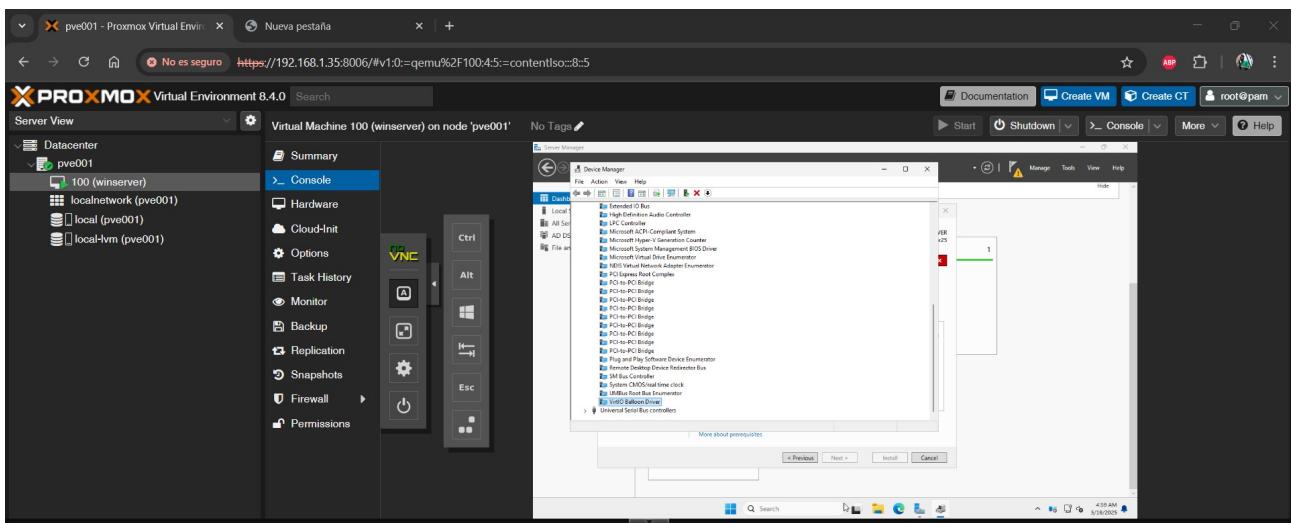


Para instalar los controladores VirtIO de PCE Devices seguir el mismo proceso hacer clic derecho



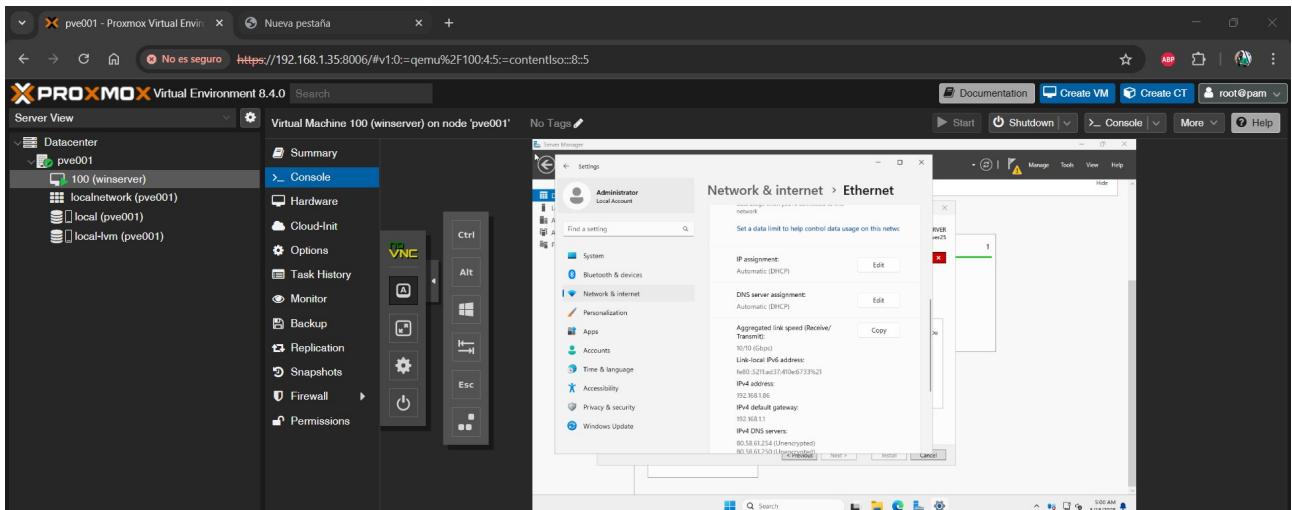
en la entrada pci con exclamación y elegir la subcarpeta `balloon/2k22/amd64`

Ya tendríamos los dispositivos con los controladores correspondientes.



A2.4.2. Configuración de IP fija

Ir a Propiedades del adaptador de red para configurar la interfaz de red (*Network & internet > Ethernet*)

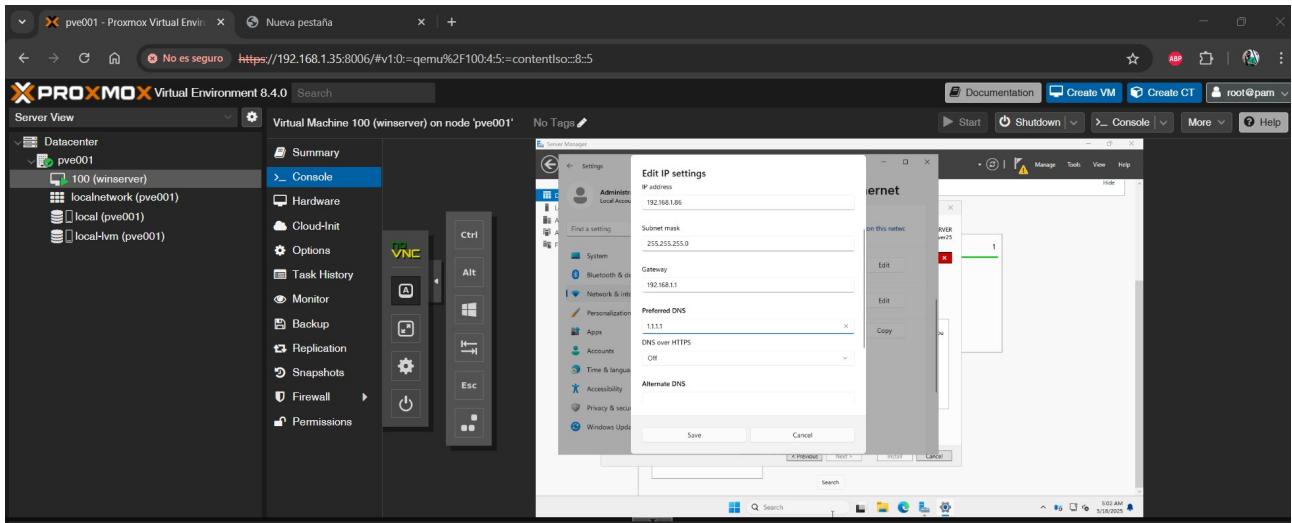


Dar a editar y dar la configuración necesaria:

- **IP:** 192.168.1.88

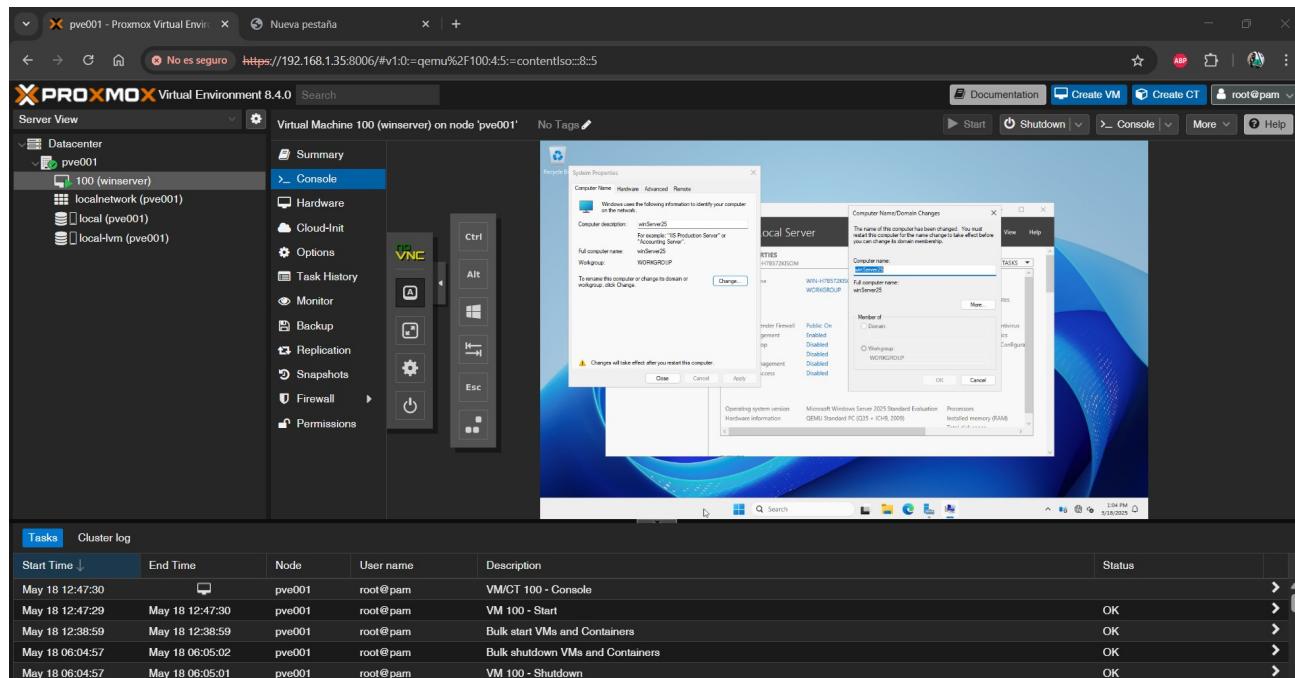
- **Máscara:** 255.255.255.0

- **DNS:** la dirección del propio servidor.



A2.4.3. Cambiar nombre de equipo

Ir a *Server Manager* > *Computer Name* > *Change* y cambiar el nombre y aplicar los cambios.



Anexo 3: Creación de la máquina virtual: Windows 11 (VDI)

Este anexo documenta la creación de una máquina virtual con **Windows 11 Pro**, destinada a actuar como **VDI** (Virtual Desktop Infrastructure) dentro de la infraestructura simulada del proyecto. Esta máquina está pensada para ser asignada a un usuario específico y accederse desde el exterior mediante Escritorio Remoto a través de la VPN.

A3.1. Subida de la imagen ISO a Proxmox

Se accede a Datacenter > pve001 > local y se selecciona la opción Upload como se hizo con Windows Server.

Se sube la ISO oficial de Windows 11 para tenerla disponible al crear la máquina virtual.

The screenshot shows the Proxmox VE 8.4.0 web interface. In the left sidebar, under 'Server View', the 'Datacenter' section is expanded, showing 'pve001' with its sub-nodes: '100 (winserver)', 'localnetwork (pve001)', 'local (pve001)', and 'local-lvm (pve001)'. The 'ISO Images' tab is selected in the main content area. A modal dialog titled 'Upload' is open, showing the file path 'C:\fakepath\Win11_24H2_Spanish_x64.iso' in the 'File:' input field. Below it, the file name is listed as 'Win11_24H2_Spanish_x64.iso', file size as '5.42 GiB', and MIME type as '-'. The 'Hash algorithm:' dropdown is set to 'None'. A note at the bottom of the dialog says: 'Uploads are stored temporarily in "/var/tmp", make sure there is enough free space.' At the bottom of the dialog are 'Abort' and 'Upload' buttons. The background shows a table of existing ISO images with columns for Name, Date, Format, and Size. At the bottom of the page, there is a 'Tasks' table listing recent system operations.

Start Time	End Time	Node	User name	Description	Status
May 18 20:18:19	May 18 20:18:19	pve001	root@pam	Bulk start VMs and Containers	OK
May 18 17:58:21	May 18 17:58:21	pve001	root@pam	Bulk shutdown VMs and Containers	OK
May 18 16:24:09	May 18 16:24:52	pve001	root@pam	VM/CT 100 - Console	OK
May 18 15:45:50	May 18 16:19:36	pve001	root@pam	VM/CT 100 - Console	OK
May 18 14:57:03	May 18 14:57:31	pve001	root@pam	VM/CT 100 - Console	OK

También se sube la ISO de VirtIO drivers, necesaria para que el instalador detecte el disco y la red.

A3.2. Creación de la VM en Proxmox

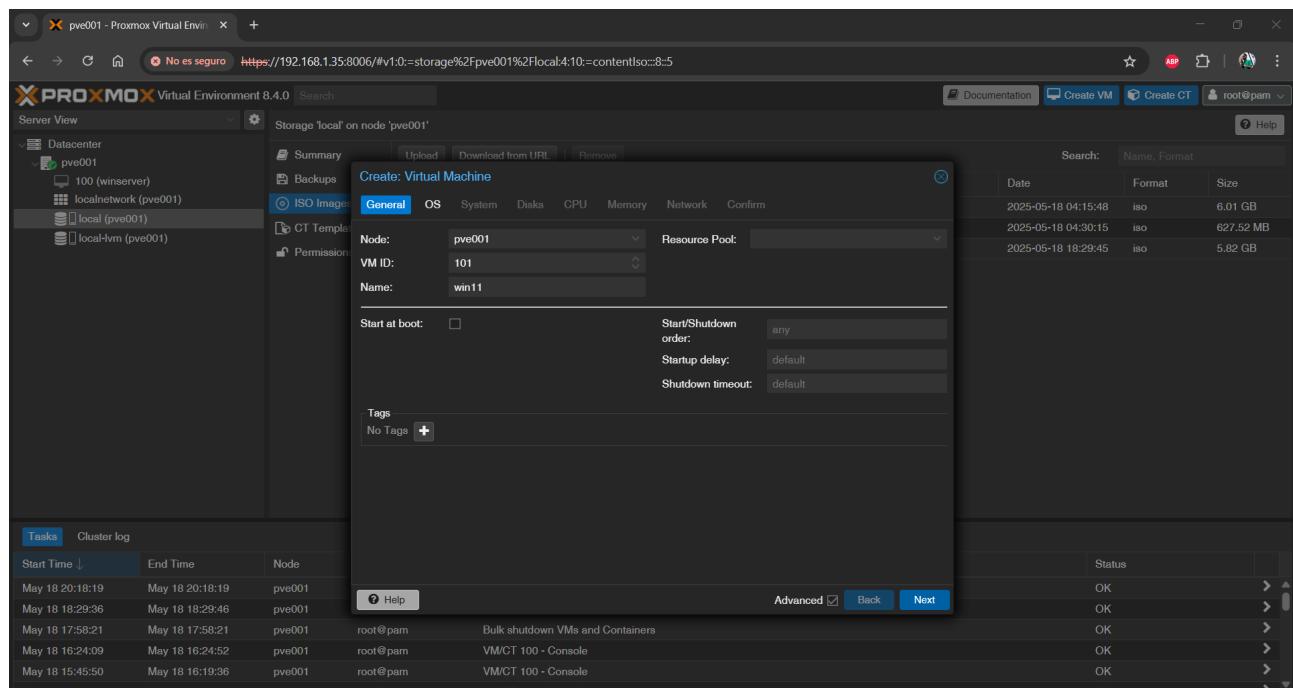
Abrir el asistente para la creación de máquinas virtuales (clicando en el nodo de proxmox **pve001** del menú izquierdo y dar en el botón “**Create VM**” que hay arriba a la derecha y seguir el asistente al igual que se ha hecho anteriormente con Windows Server.

General

Node: pve001 (nodo actual)

VM ID: asignado automáticamente

Name: win11-vdi

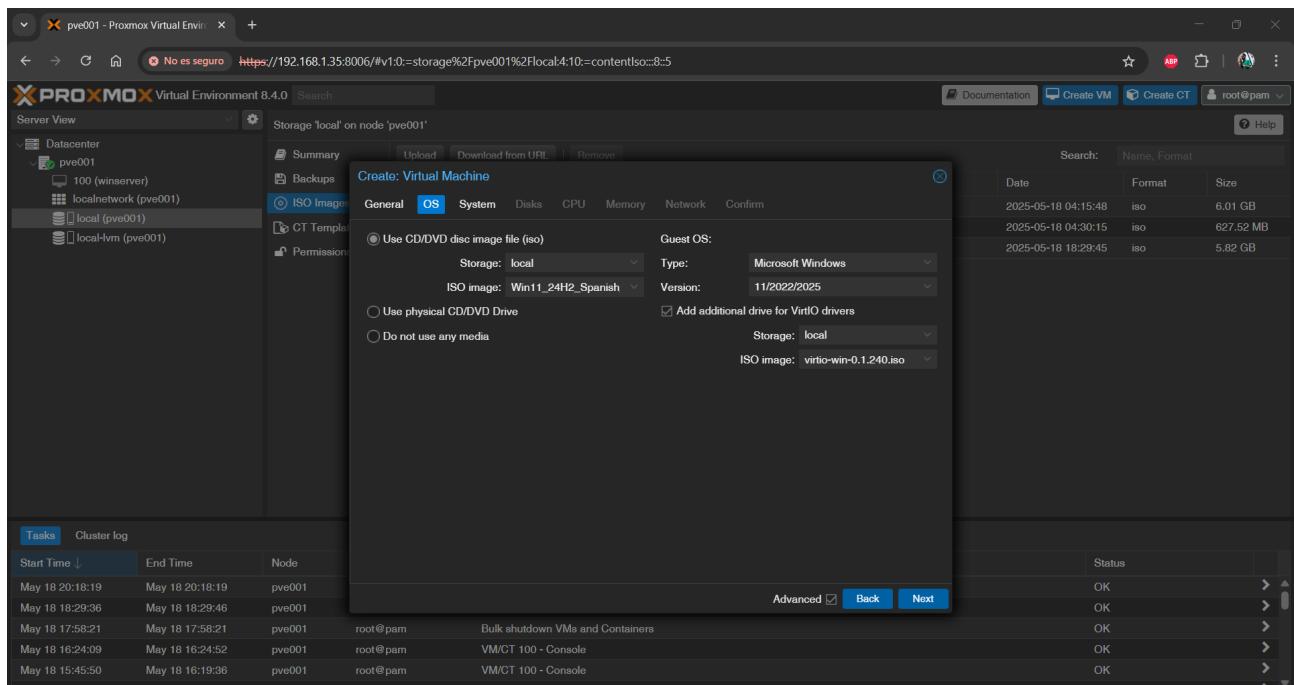


OS

ISO Image: Se selecciona la ISO previamente subida de Windows 11.

Guest OS Type: Microsoft Windows

Version: Se puede dejar como 11/2022 o la versión más cercana.



En la pantalla de OS seleccionar la iso de Windows 11, seleccionar al casilla de “*Add aditional drive for VirtIO drivers*” y añadir la iso de VirIO.

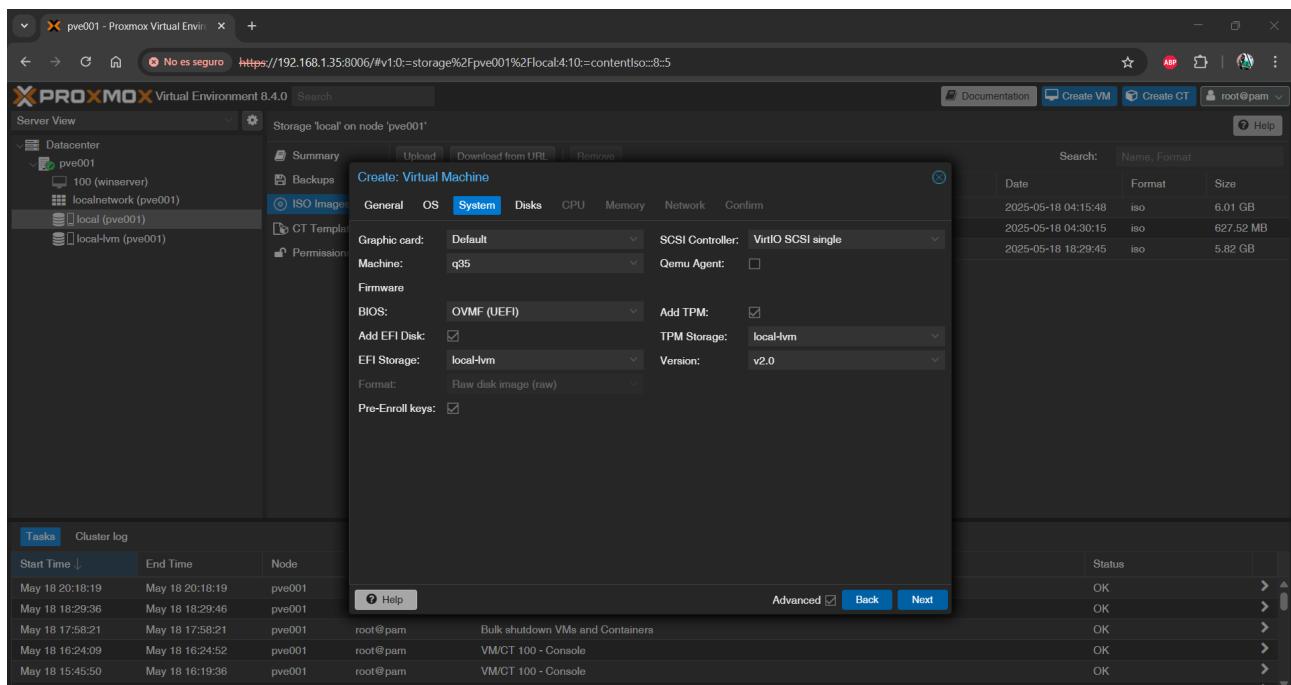
System

BIOS: Se deja en OVMF (UEFI) si se desea usar UEFI (opcional).

Machine: q35

EFI Disk: marcado si se usa UEFI (Proxmox lo creará automáticamente).

Add TPM: No se marca (no necesario en este proyecto).



Se puede usar BIOS tradicional o UEFI. Para evitar problemas, UEFI es más moderno pero debe estar soportado por la ISO.

Hard Disk

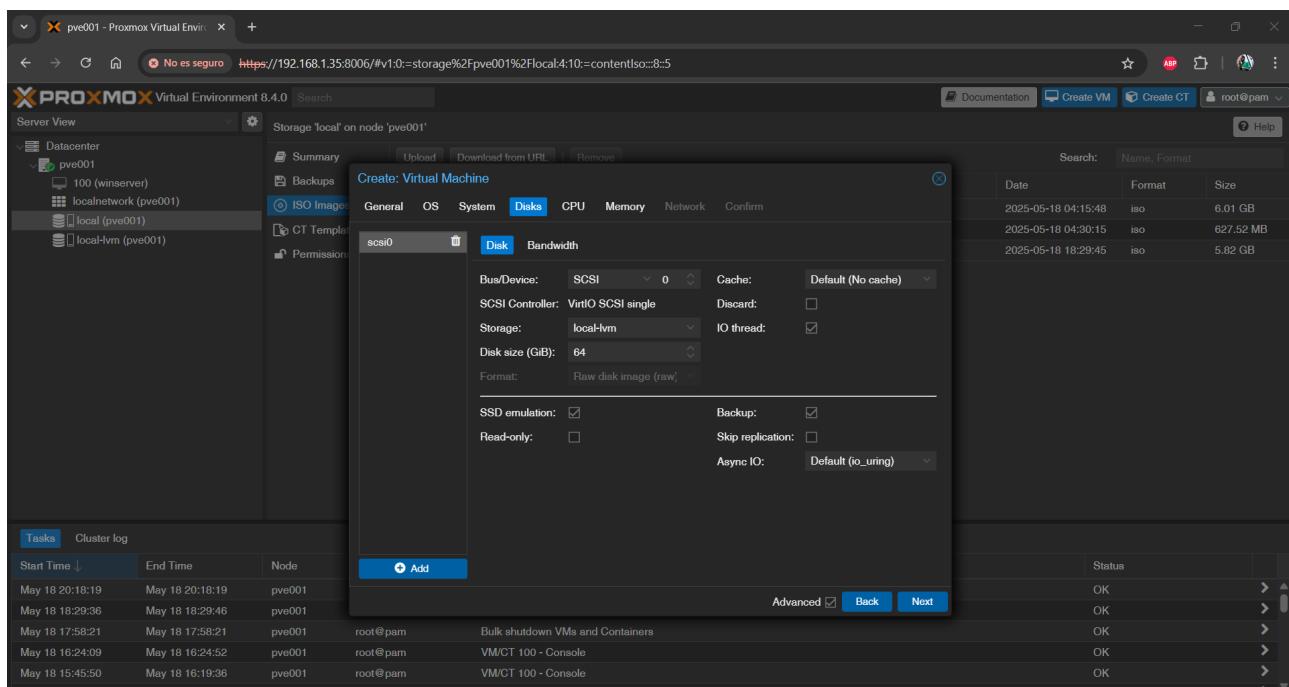
Bus/Device: VirtIO Block

Storage: local-lvm (o local, según configuración)

Disk size: 32–64 GB (según necesidades del puesto)

Cache: Write back o Default

El uso de VirtIO requiere cargar drivers durante la instalación, pero mejora el rendimiento significativamente.

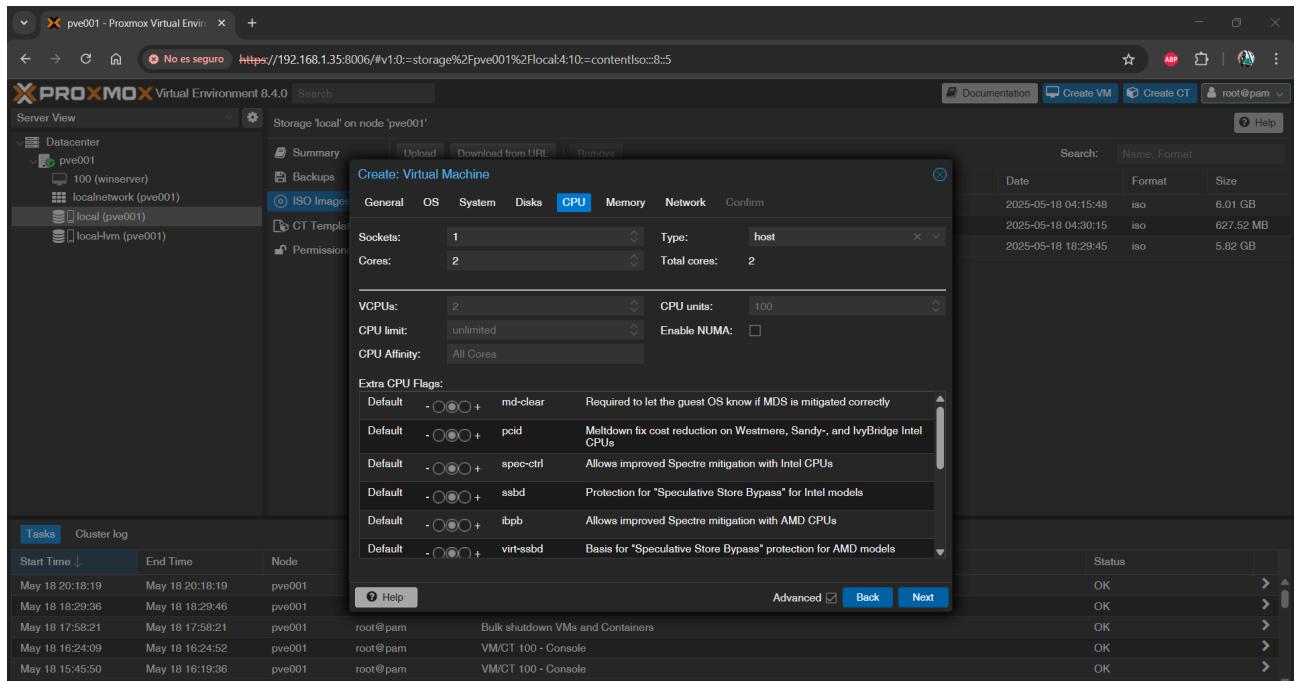


CPU

Cores: 2

Sockets: 1

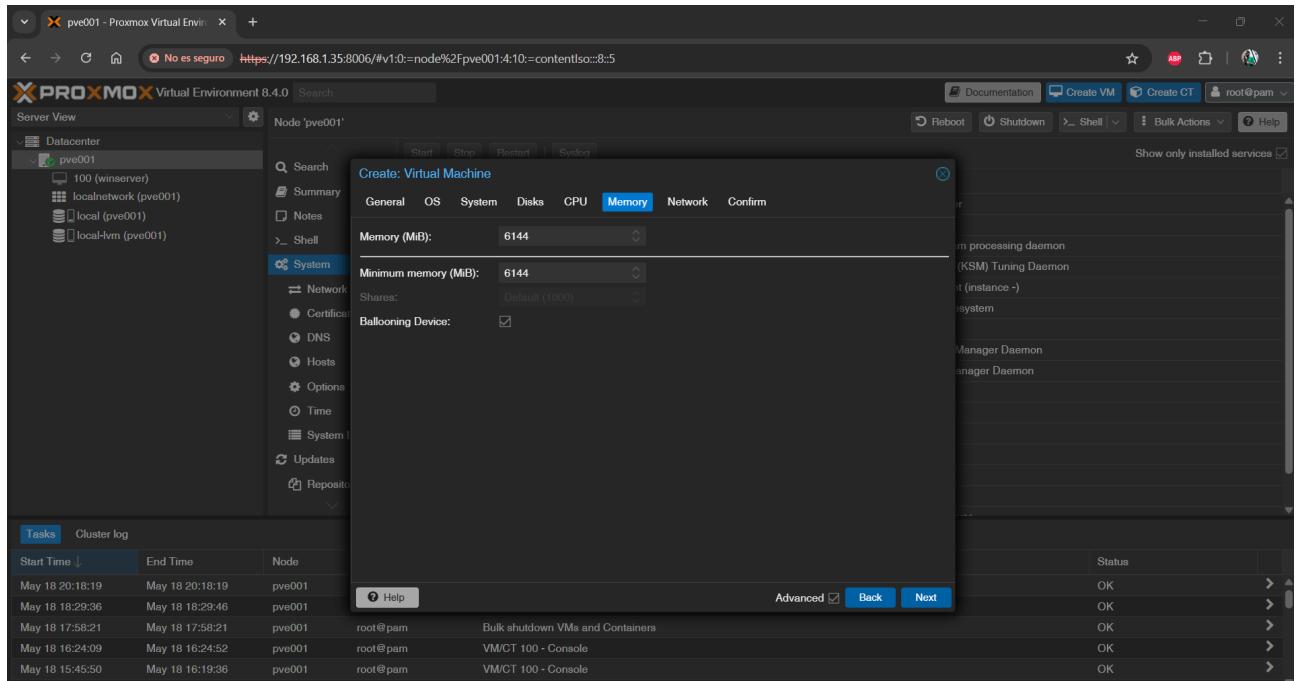
Type: host si se quiere mayor rendimiento.



Memory

Memory (RAM): 2048–4096 MB (2–4 GB, en mi caso puse 6GB para favorecer la instalación, si se desea se puede editar la configuración de la máquina más adelante).

Se recomienda 4 GB si se quiere un rendimiento fluido de Windows 11, aunque para pruebas básicas puede funcionar con 2 GB.

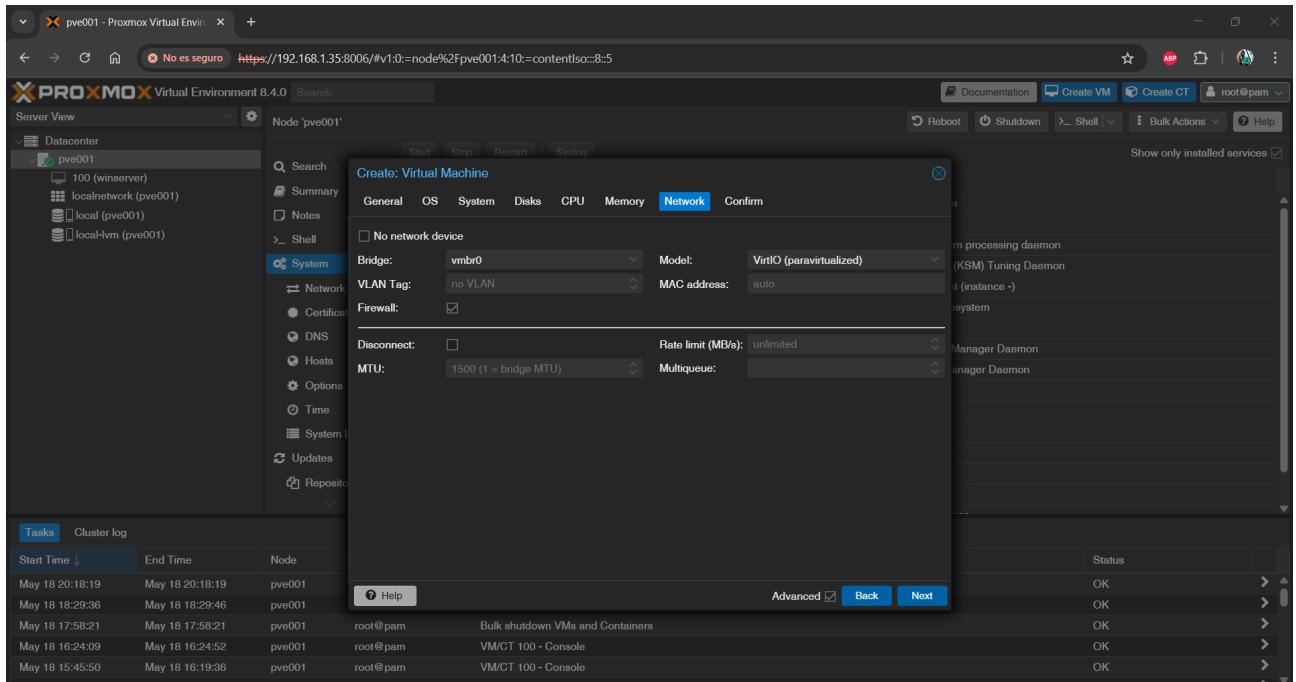


Network

Model: VirtIO (paravirtualized)

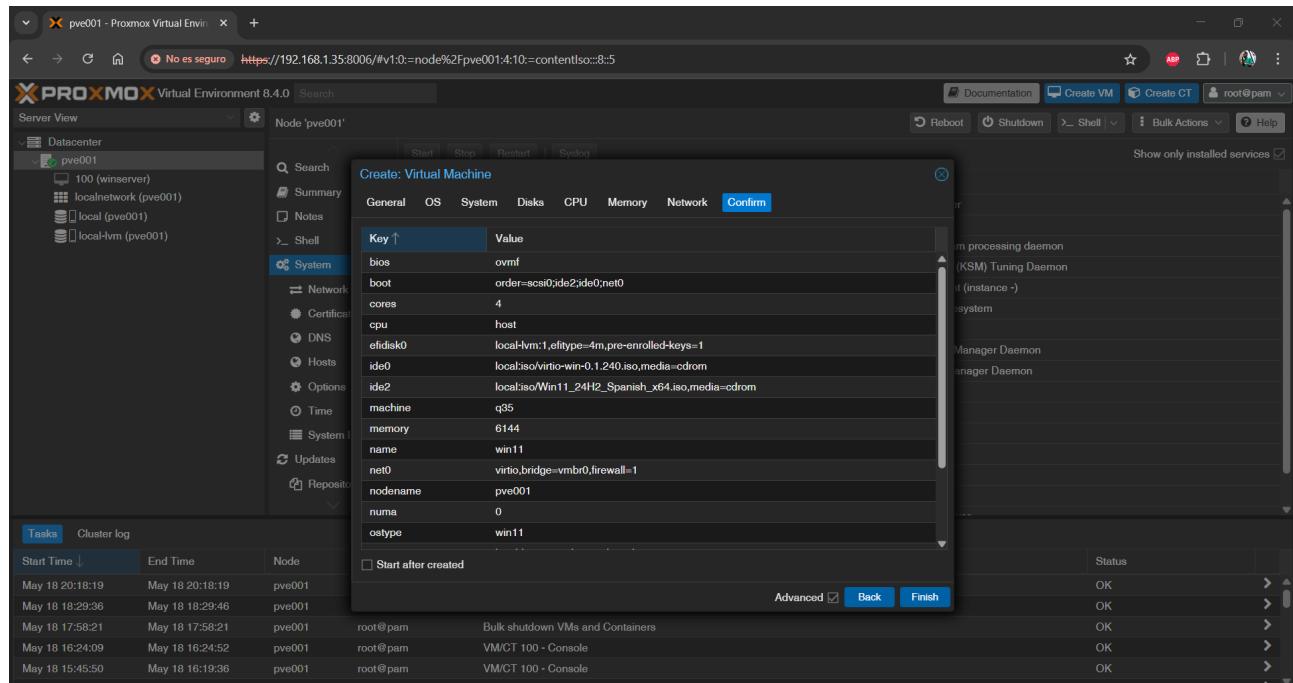
Bridge: vmbr0 (conectada a la red LAN)

Al igual que con el disco, VirtIO para red requiere cargar drivers durante la instalación del sistema.



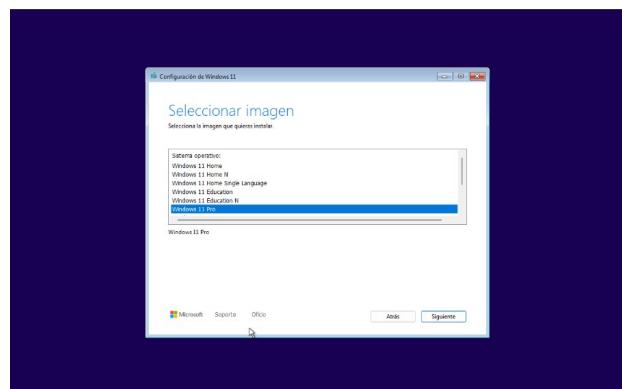
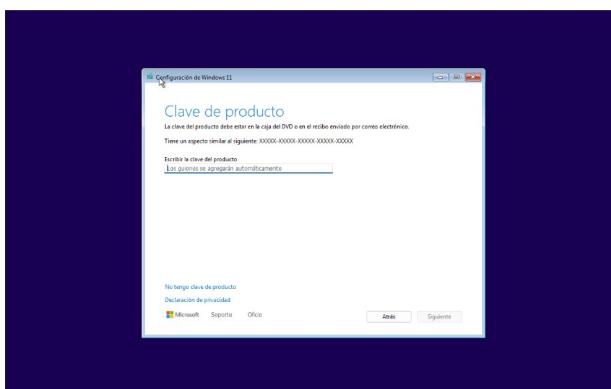
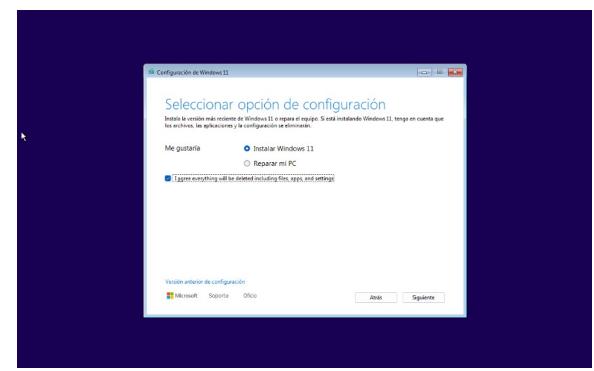
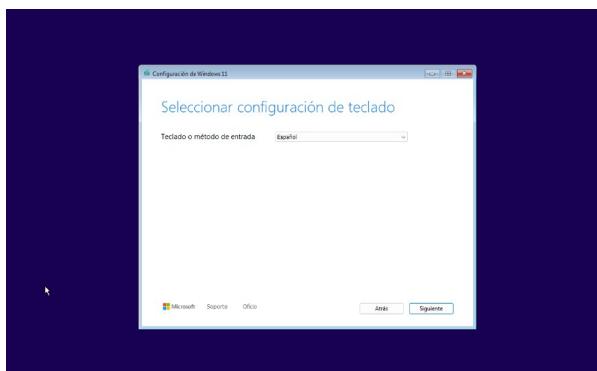
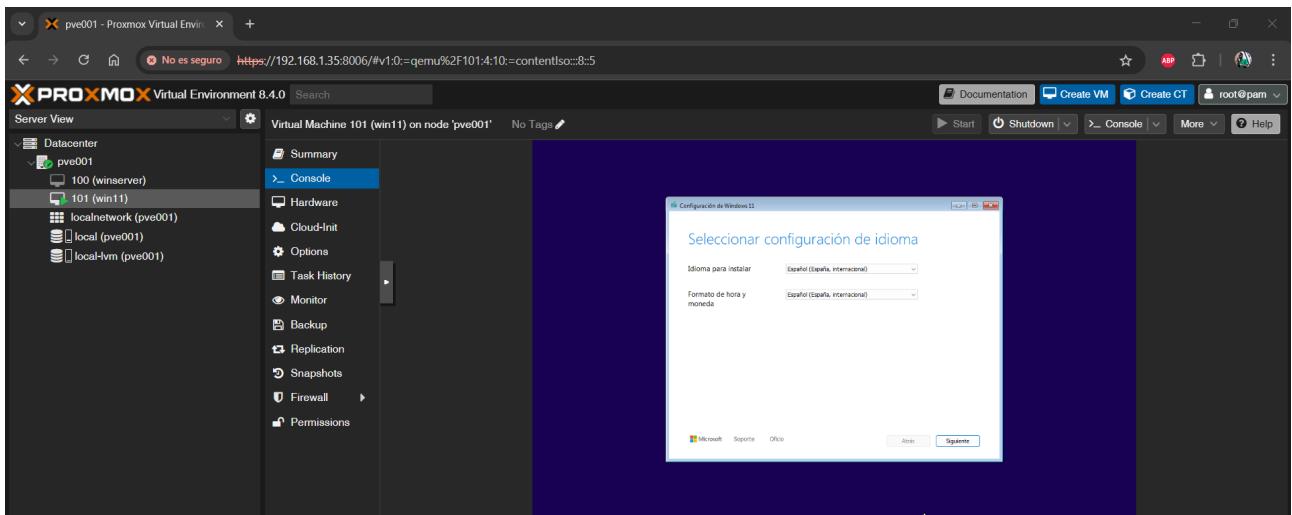
Confirmación final

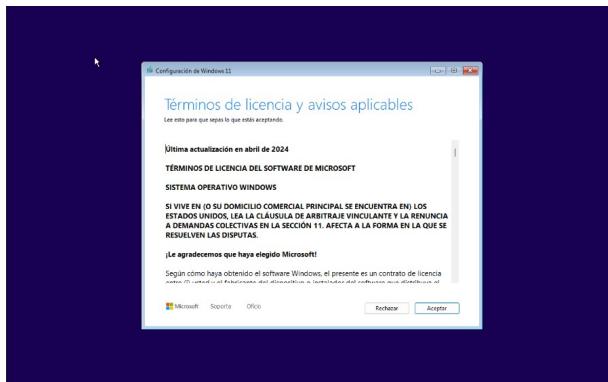
Antes de finalizar, se muestra un resumen con todos los parámetros seleccionados. Confirmar y crear la máquina



A3.3. Instalación de Windows 11 de la instalación y carga del controlador de disco

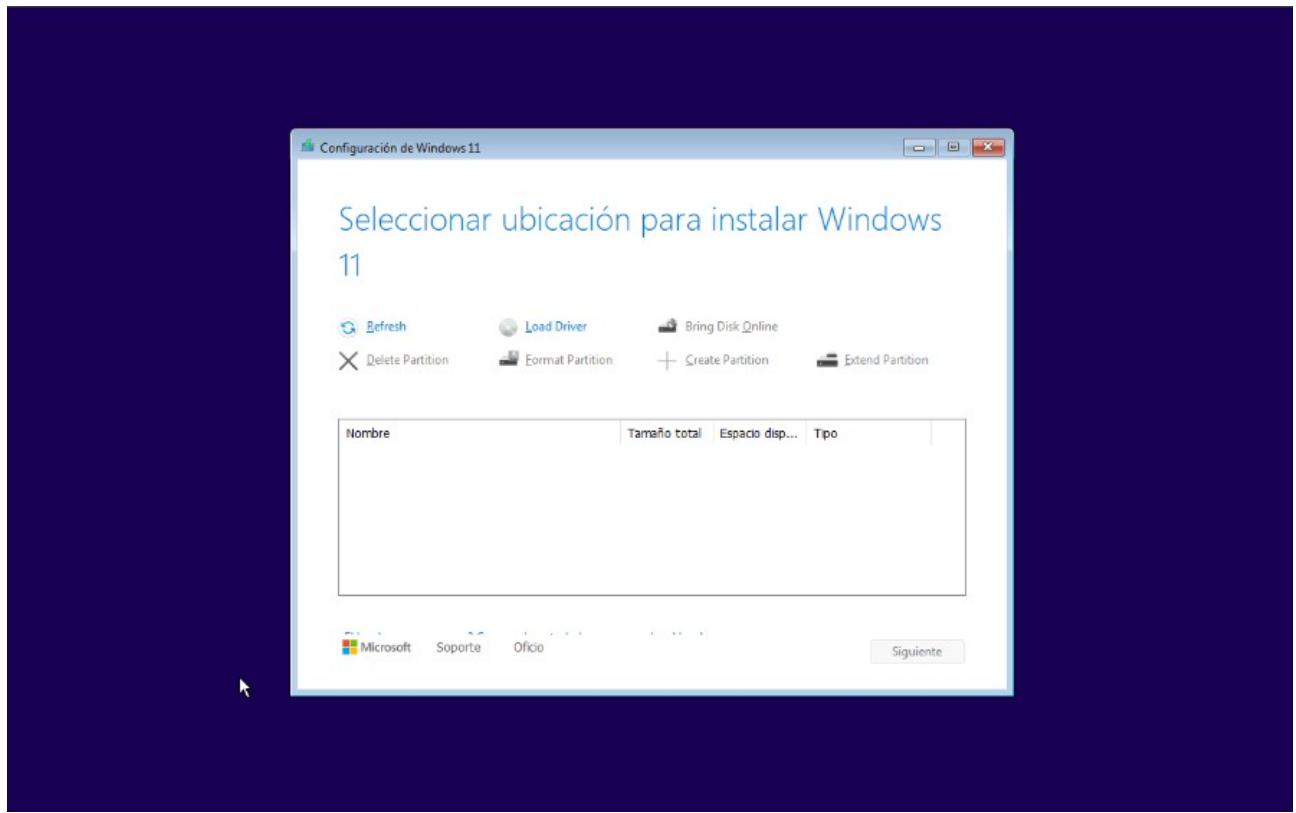
Iniciar la máquina virtual (clic derecho en la VM creada y “Start”) y comenzar la instalación de Windows 11 de forma habitual hasta llegar a la selección de disco. Al llegar al paso de selección de unidad, el instalador no muestra ningún disco. Es necesario cargar manualmente el driver desde la ISO de VirtIO.



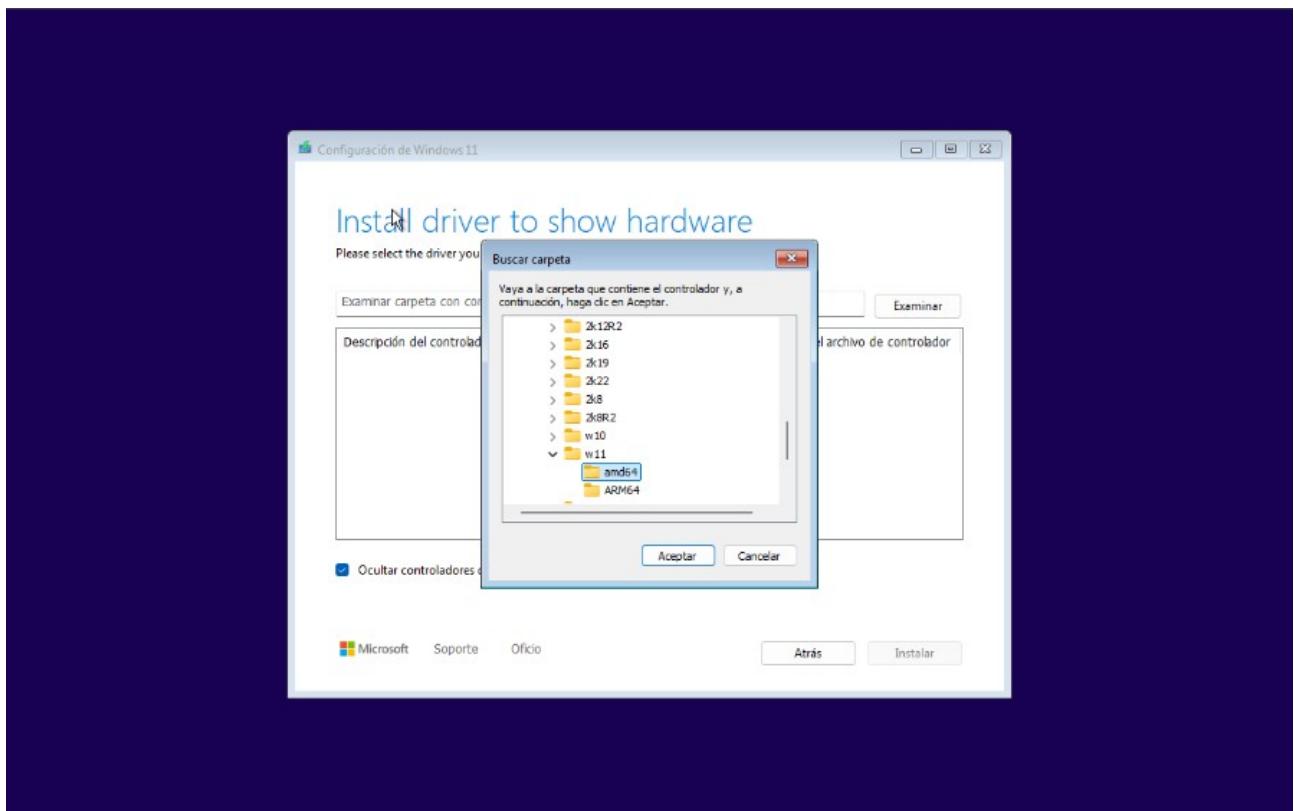


Al llegar al paso de selección de unidad, el instalador no muestra ningún disco. Es necesario cargar manualmente el driver desde la ISO de VirtIO.

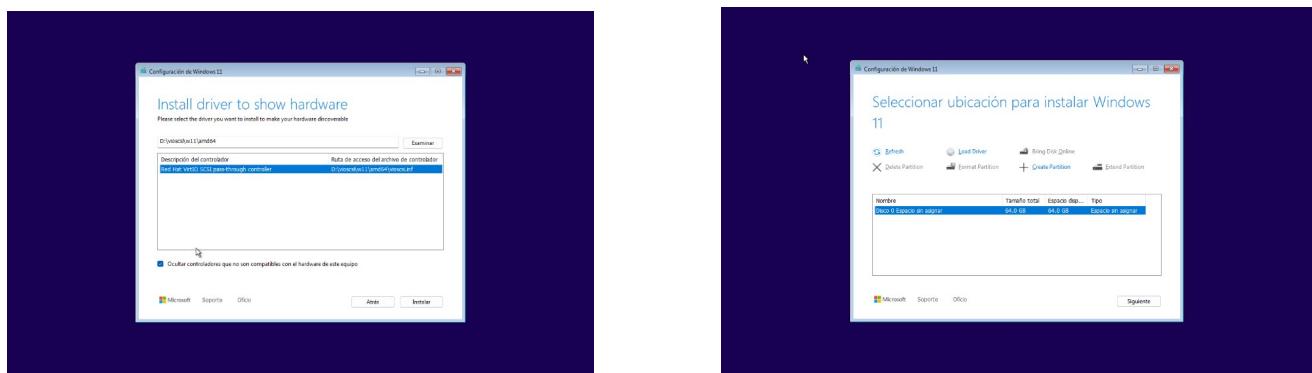
Hacer clic en Load Driver

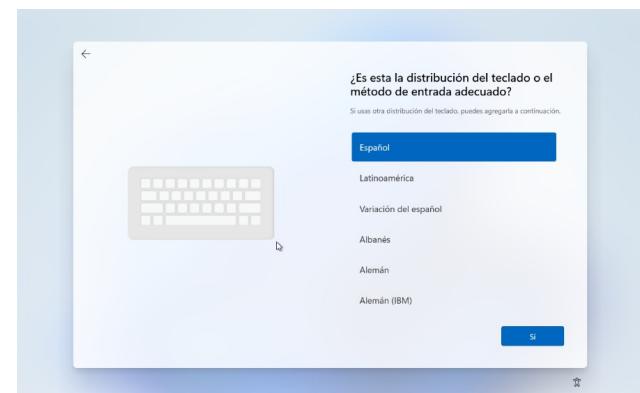
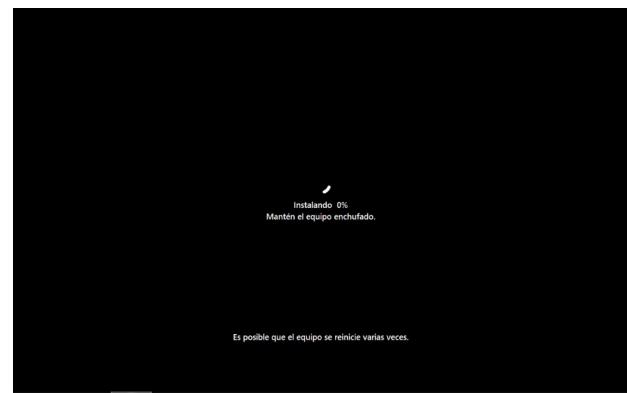
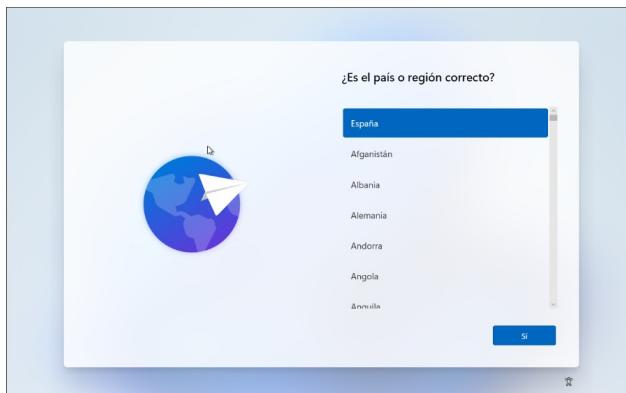
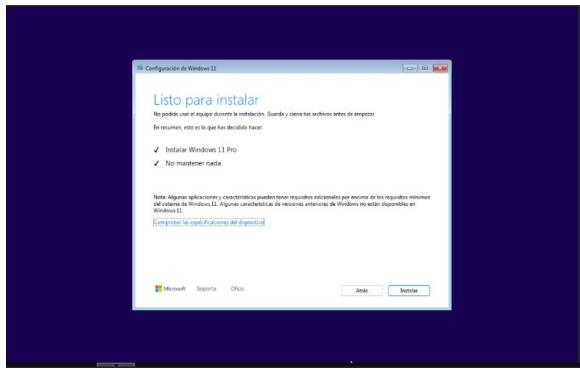


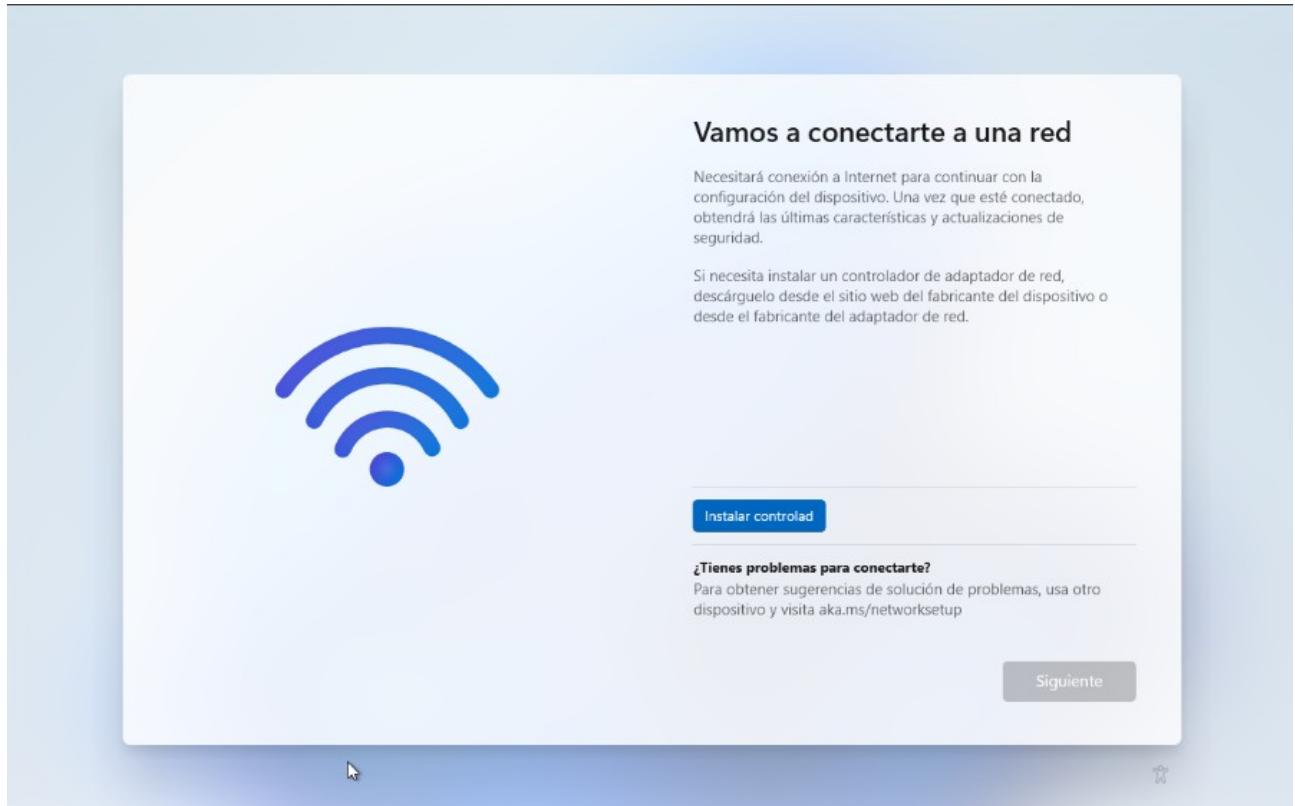
- Pulsar Browse y navegar a: VirtIO: *viosci/w11/amd64*



Instalar el Driver y seguir la instalación habitual de windows 11.

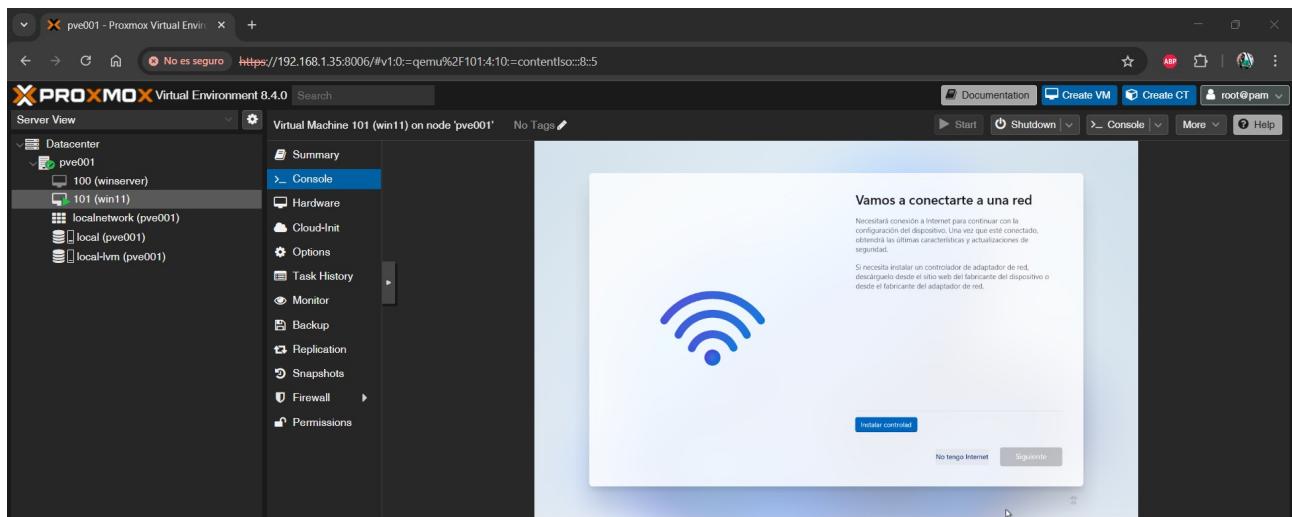




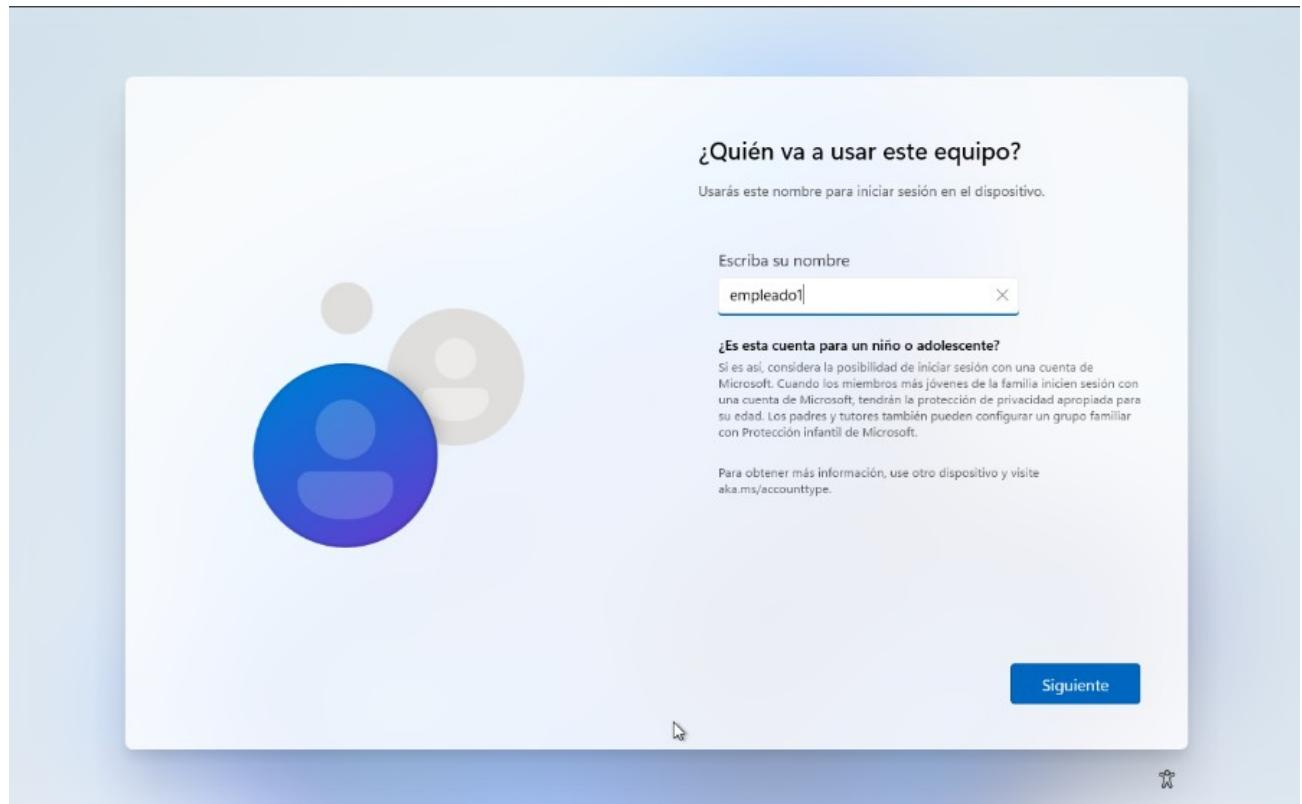


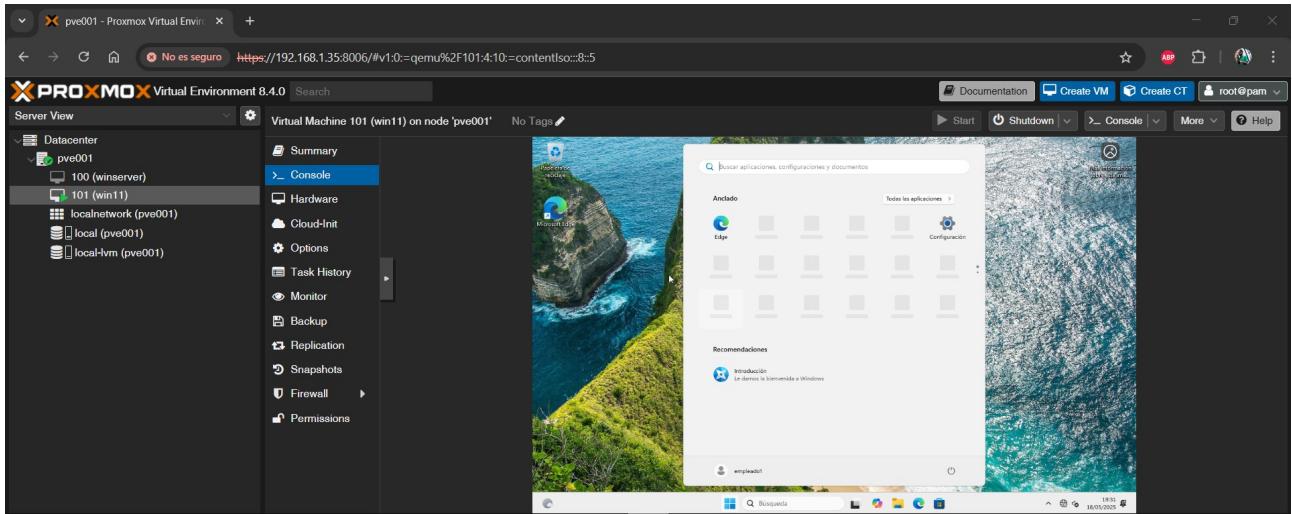
En este momento, si no aparece la opción de seguir sin acceso a internet, pulsar **shit+F10** y escribir en el cmd *Oobe\BYPASSNRO*, se reiniciará esta parte de la instalación y cuando llegue a este punto aparecerá el botón de seguir sin configurar la red.

Al reiniciar ya aparece el botón “**No tengo internet**” para poder continuar con al instalación.



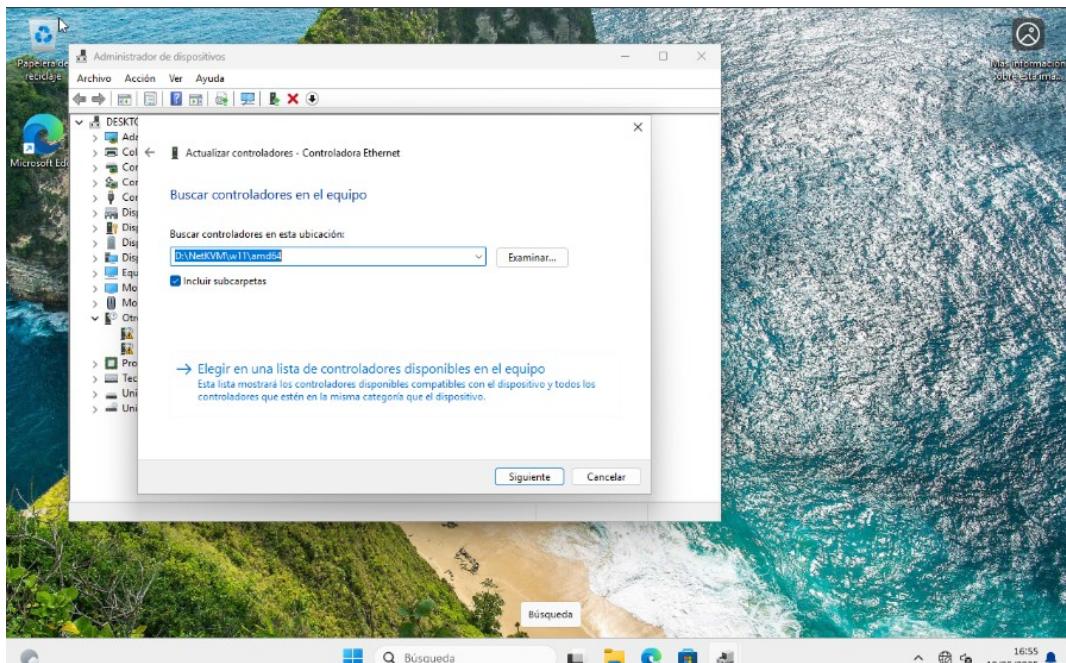
Seguir el asistente hasta terminar la instalación.



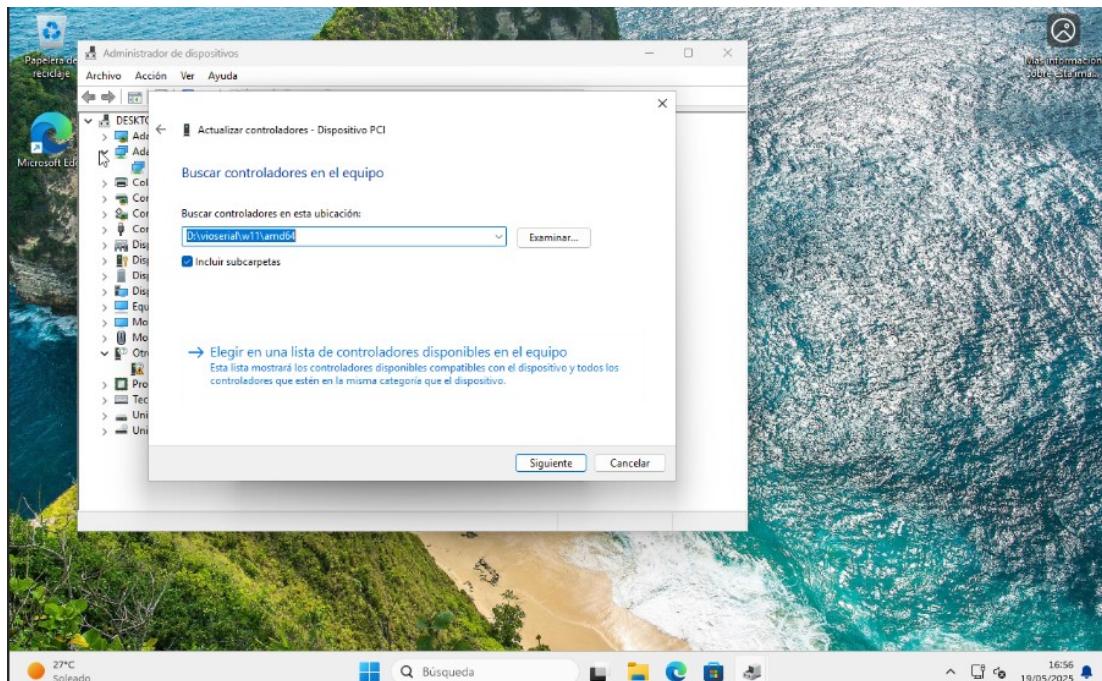


A3.4. Instalación de drivers VirtIO post-instalación

Ir al administrador de dispositivos e instalar los drivers de VirtIO como se hizo con Windows Server. Se instala el **driver de red: NetKVM > w11 > amd64**



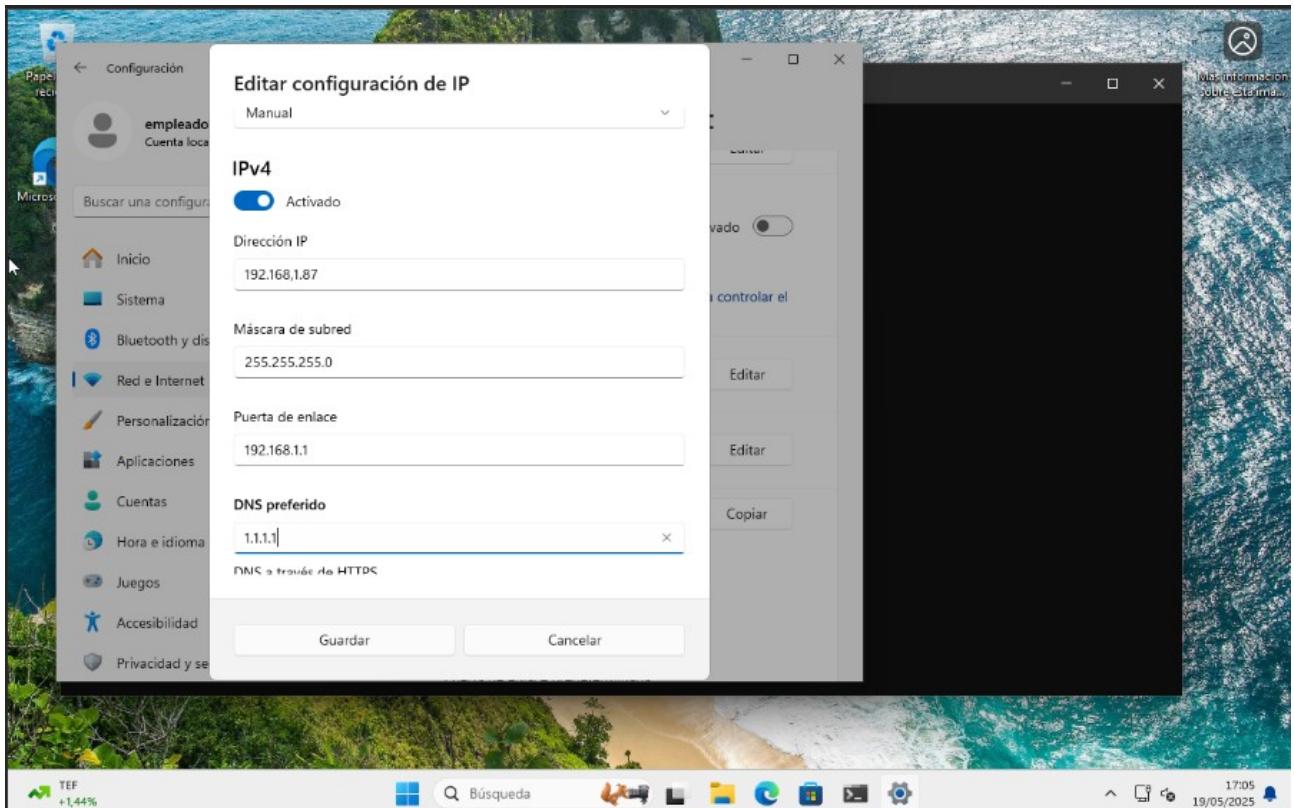
Y también el de dispositivo PCI: **Balloon > w11 > amd64**



A3.5. Configuración de IP estática

Ir a **Configuración de Red e internet** y configurar los parámetros de red.

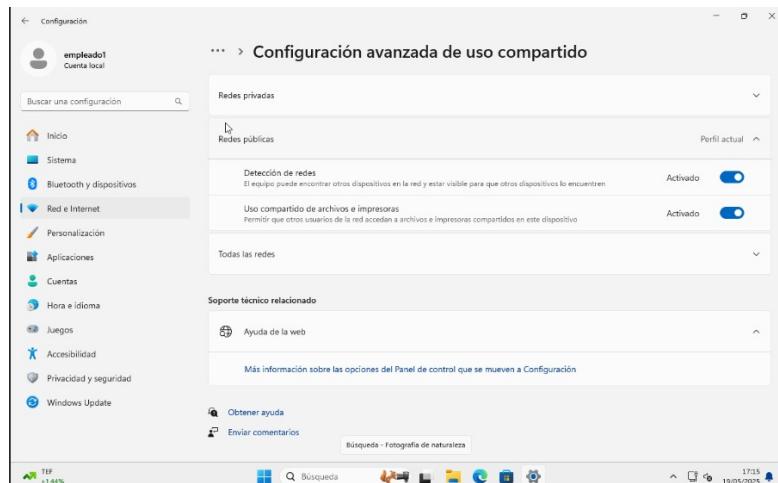
- **Dirección IP:** 192.168.1.87
- **Máscara:** 255.255.255.0
- **Puerta de enlace:** 192.168.1.1
- **DNS:** 192.168.1.88 (dirección del servidor)



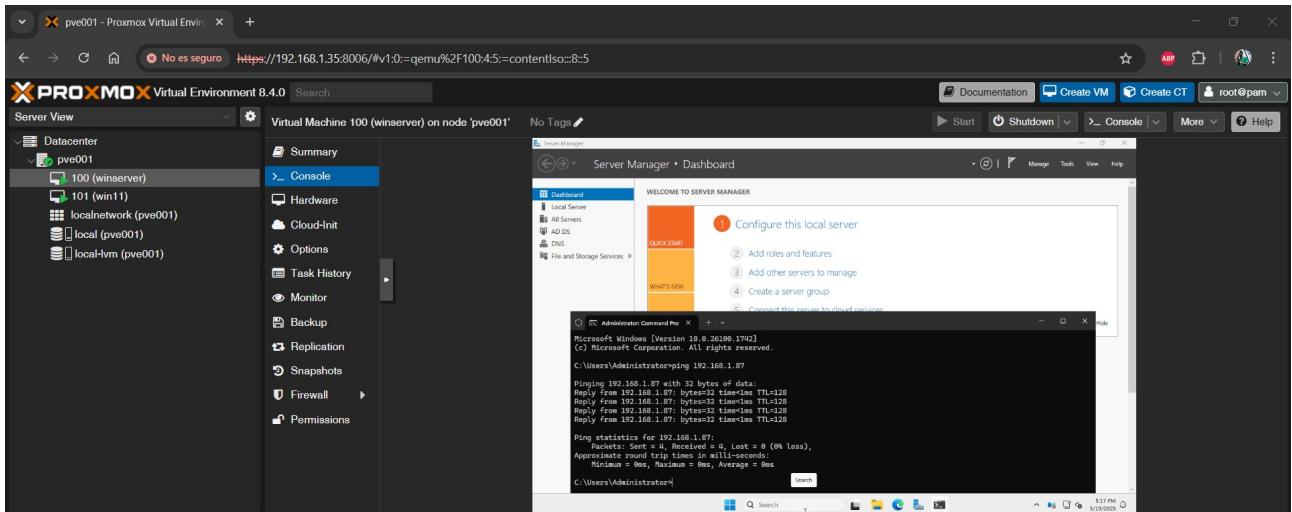
A3.6. Verificación de conectividad con el servidor

Para verificar la conectividad con el servidor se ha activado la detección de redes en el Firewall, para poder hacer un ping desde el Windows Server al equipo Windows 11.

Para ello ir a configuración avanzada de red y activar la detección de redes para permitir el ping desde el servidor a este equipo.



Ir al servidor windows Server y hacer un ping a la máquina de windows 11 para comprobar la visibilidad entre ambas



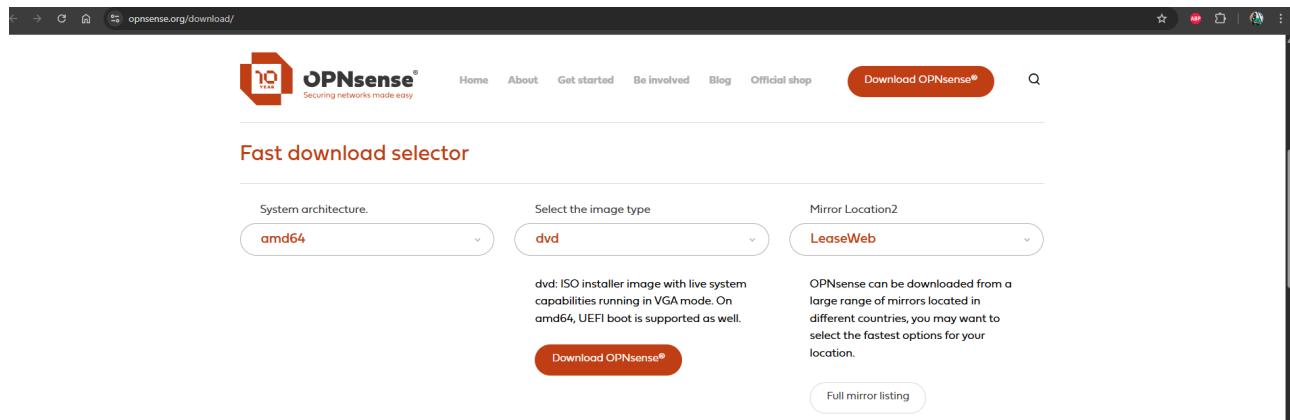
Anexo 4 – Creación de la máquina virtual: OPNsense

Este anexo describe el proceso de creación e instalación de la máquina virtual que alojará OPNsense, el firewall y servidor VPN de la infraestructura.

Aunque en el flujo del proyecto se configuró al final, la VM se preparó previamente para su instalación, quedando disponible para activar los servicios de red externa (VPN) una vez validada la red interna.

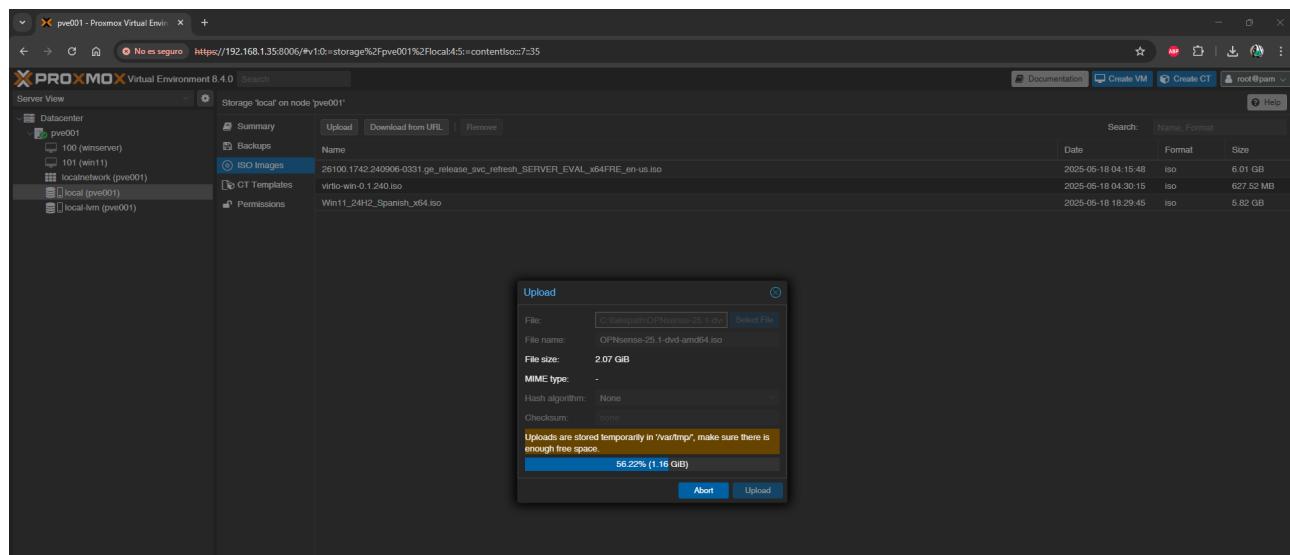
A4.1. Subida de la imagen ISO de OPNsense

Para ello descargar de su página oficial la versión dvd para montarla en proxmox



The screenshot shows the OPNsense download page at opnsense.org/download/. The interface includes a 'Fast download selector' section with dropdown menus for 'System architecture' (amd64), 'Select the image type' (dvd), and 'Mirror Location' (LeaseWeb). A descriptive text block explains that the dvd image is an ISO installer with live system capabilities running in VGA mode, supporting UEFI boot. A large orange 'Download OPNsense®' button is prominently displayed. To the right, there's a note about selecting mirrors for faster download and a link to a full mirror listing.

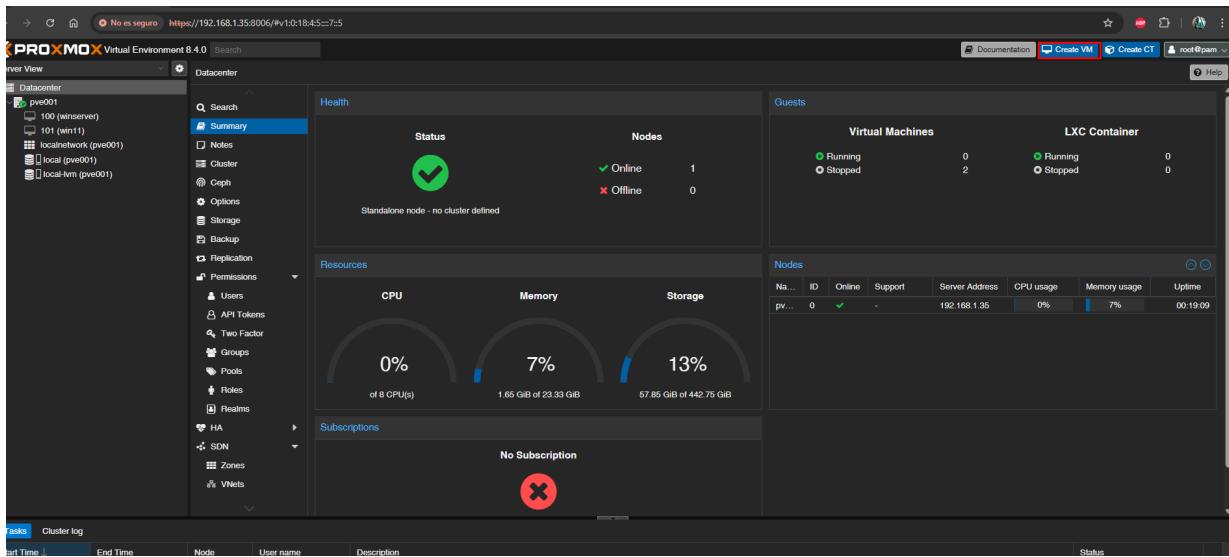
Se accede al almacenamiento local (local) en Proxmox y se sube la ISO oficial de OPNsense



The screenshot shows the Proxmox VE storage interface for node 'pve001'. On the left, the 'Datacenter' tree shows 'pve001' with its storage pools: '100 (winserver)', '101 (win11)', 'localnetwork (pve001)', 'local (pve001)', and 'local-lvm (pve001)'. In the center, the 'Storage 'local'' screen displays an 'ISO Images' table with three existing ISO files: '26100_1742_240906_0331_ge_release_svc_refresh_SERVER_EVAL_x64FRE_en-us.iso', 'virtio-win-0.1.240.iso', and 'Win11_24H2_Spanish_x64.iso'. On the right, a detailed view of the 'Upload' dialog shows a progress bar at 56.22% (1.16 GiB) for uploading 'OPNsense-25.1-dvd-amd64.iso'. The dialog also includes fields for 'File', 'File name', 'File size', 'MIME type', 'Hash algorithm', and 'Checksum'.

A4.2. Creación de la MV para OpnSense

La creación de una VM en Proxmox se realiza mediante un asistente guiado dividido en secciones.



A continuación se detalla la configuración utilizada para preparar la máquina que alojará OPNsense:

General

- **Node:** pve001
- **VM ID:** asignado automáticamente
- **Name:** opnsense

Create: Virtual Machine

General

Node:	pve001	Resource Pool:
VM ID:	102	
Name:	opnSense	

Start at boot:

Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Tags: No Tags

Advanced Back

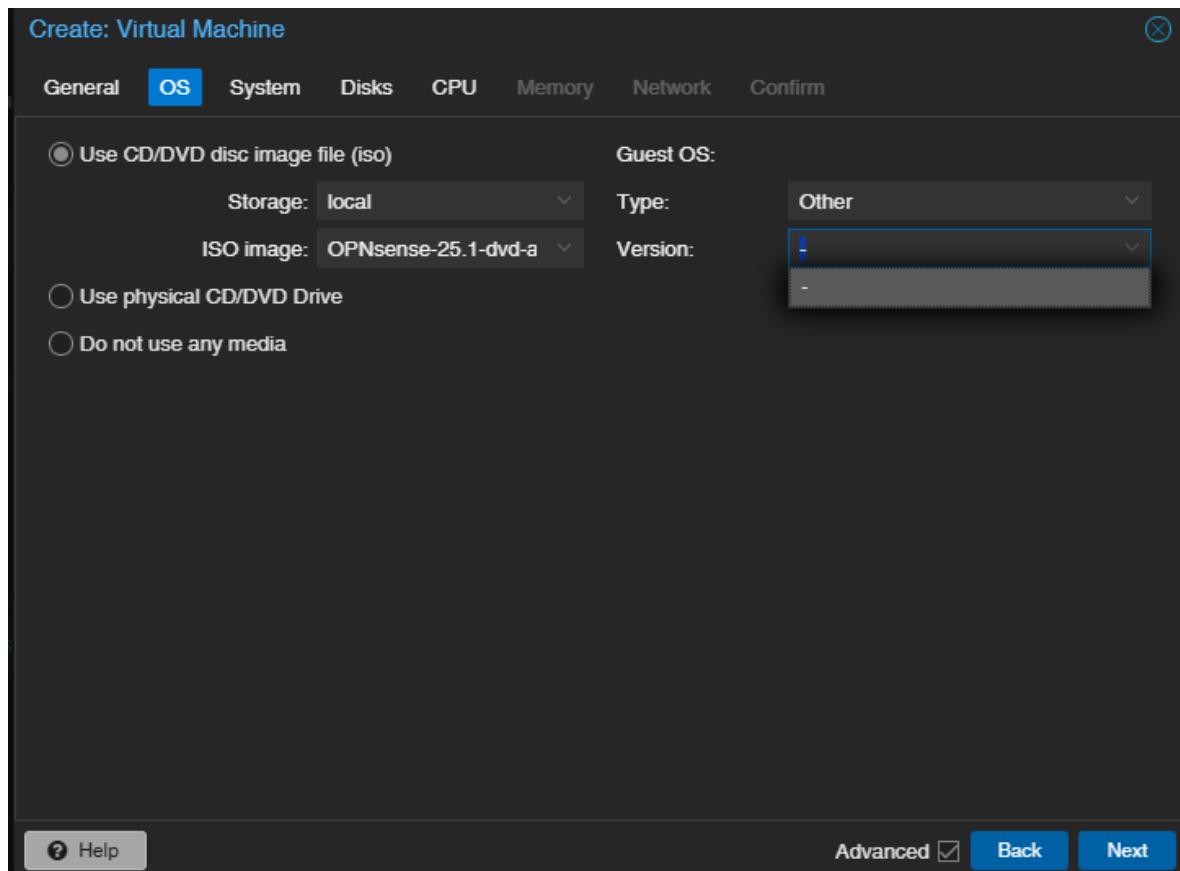
OS

ISO Image: OPNsense-25.1.7-amd64.iso (previamente subida al almacenamiento local)

Guest OS Type: Other

Version: Default (Other)

OPNsense no aparece en la lista de sistemas conocidos, pero funciona perfectamente bajo la opción genérica.



System

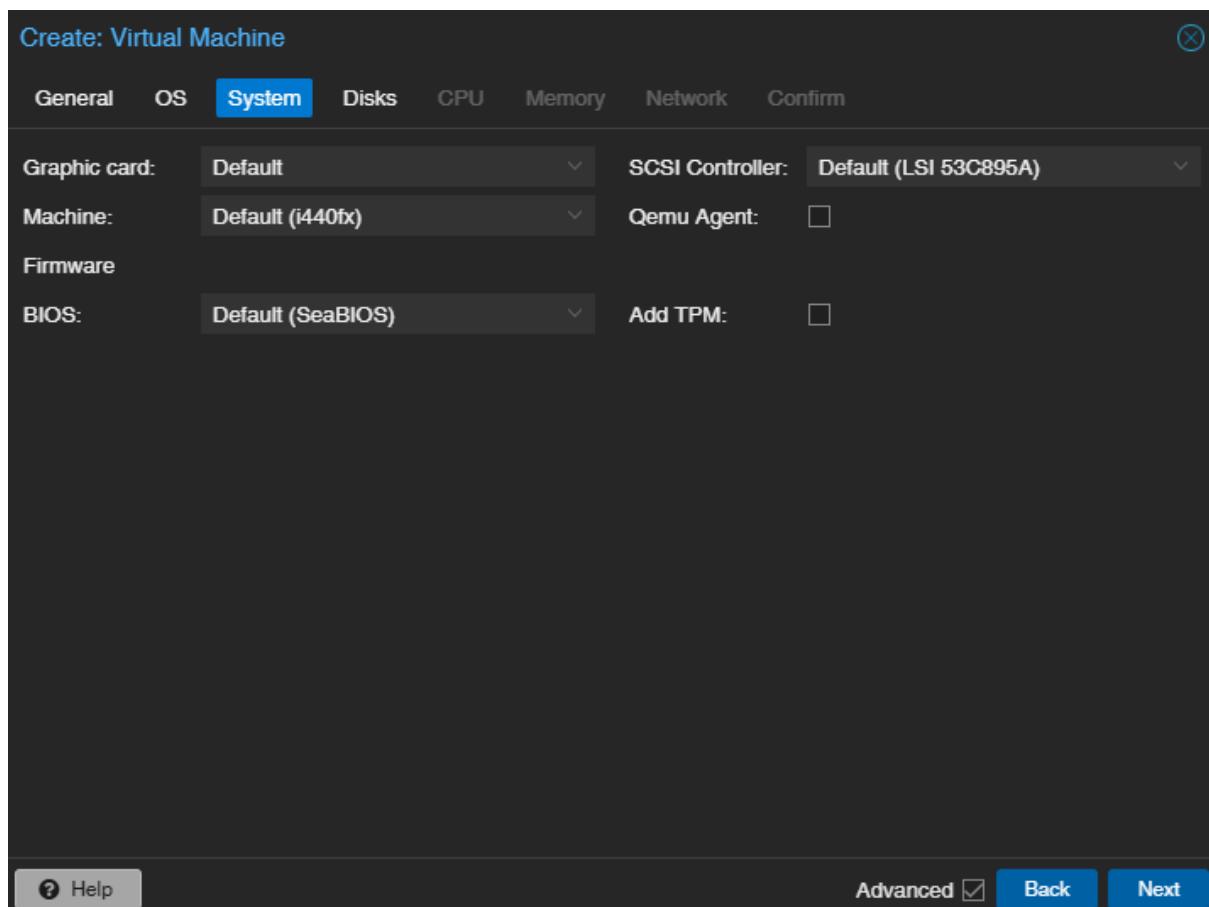
BIOS: SeaBIOS (opción tradicional compatible)

Machine: i440fx (por defecto o q35)

EFI Disk: No se marca

TPM: No requerido

SeaBIOS es suficiente y más simple para este tipo de instalación, evitando problemas con el arranque.



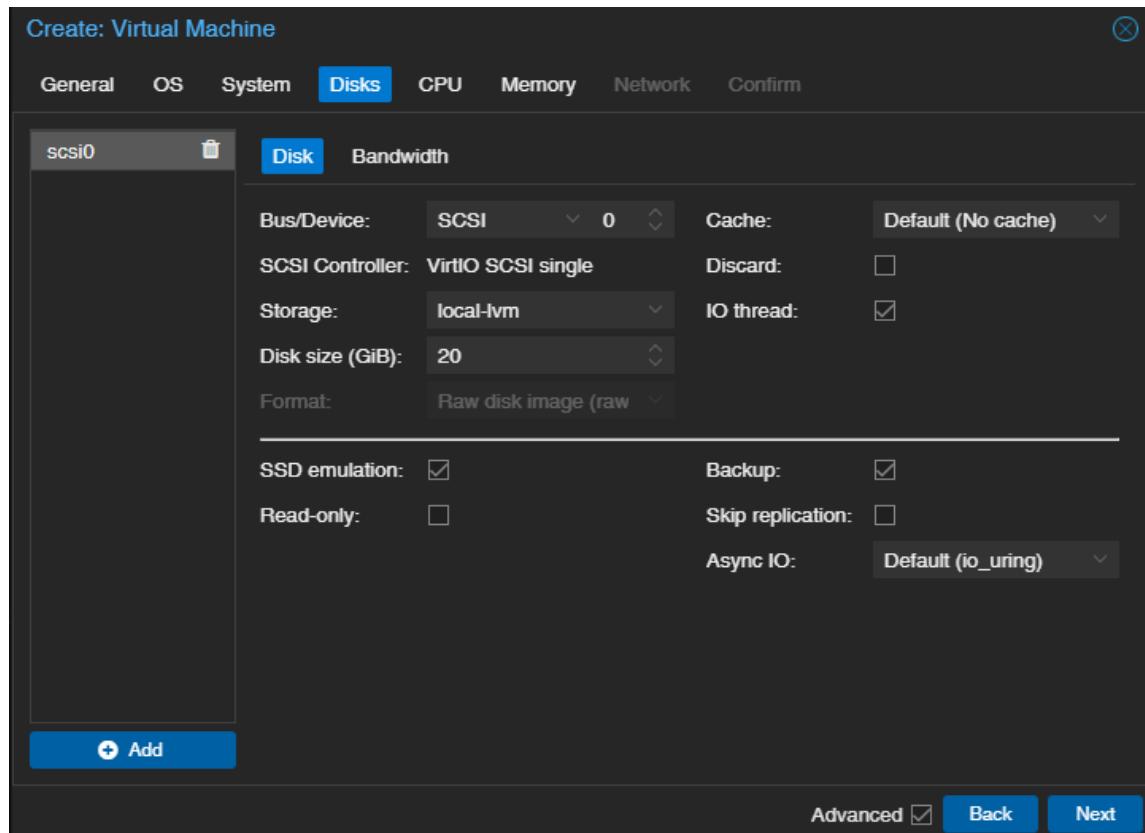
Hard Disk

Bus/Device: VirtIO Block o SCSI (ambos son compatibles con OPNsense)

Storage: local-lvm o local

Disk size: 20 GB (recomendados entre 16–32 GB)

Cache: Default



CPU

Sockets: 1

Cores: 2

Type: Default (kvm64)

Create: Virtual Machine ✖

CPU

General	OS	System	Disks	CPU	Memory	Network	Confirm
Sockets:	1			Type:	host		
Cores:	2			Total cores:	2		
VCPUs:	2			CPU units:	100		
CPU limit:	unlimited			Enable NUMA:	<input type="checkbox"/>		
CPU Affinity:	All Cores						

Extra CPU Flags:

Default	- ○○○ +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- ○○○ +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- ○○○ +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- ○○○ +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	- ○○○ +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	- ○○○ +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

Help Advanced Back Next

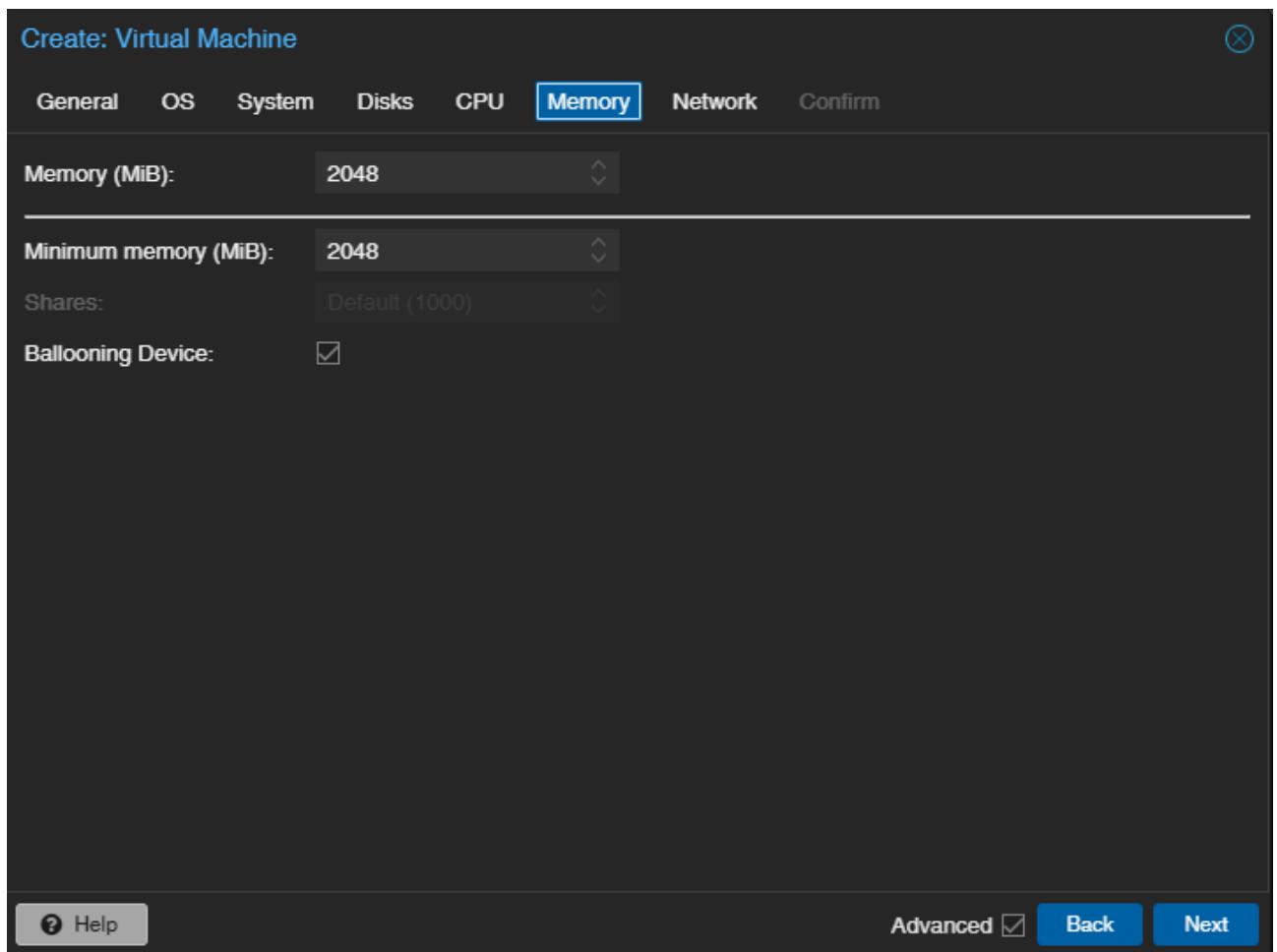
Dos núcleos son más que suficientes para ejecutar servicios de VPN, firewall y administración en entornos educativos o de pruebas.

Memory

Memory (RAM): 3072 MB (3 GB)

Inicialmente se configuraron 2 GB, pero el sistema mostró un mensaje advirtiendo que se recomienda mínimo 3 GB.

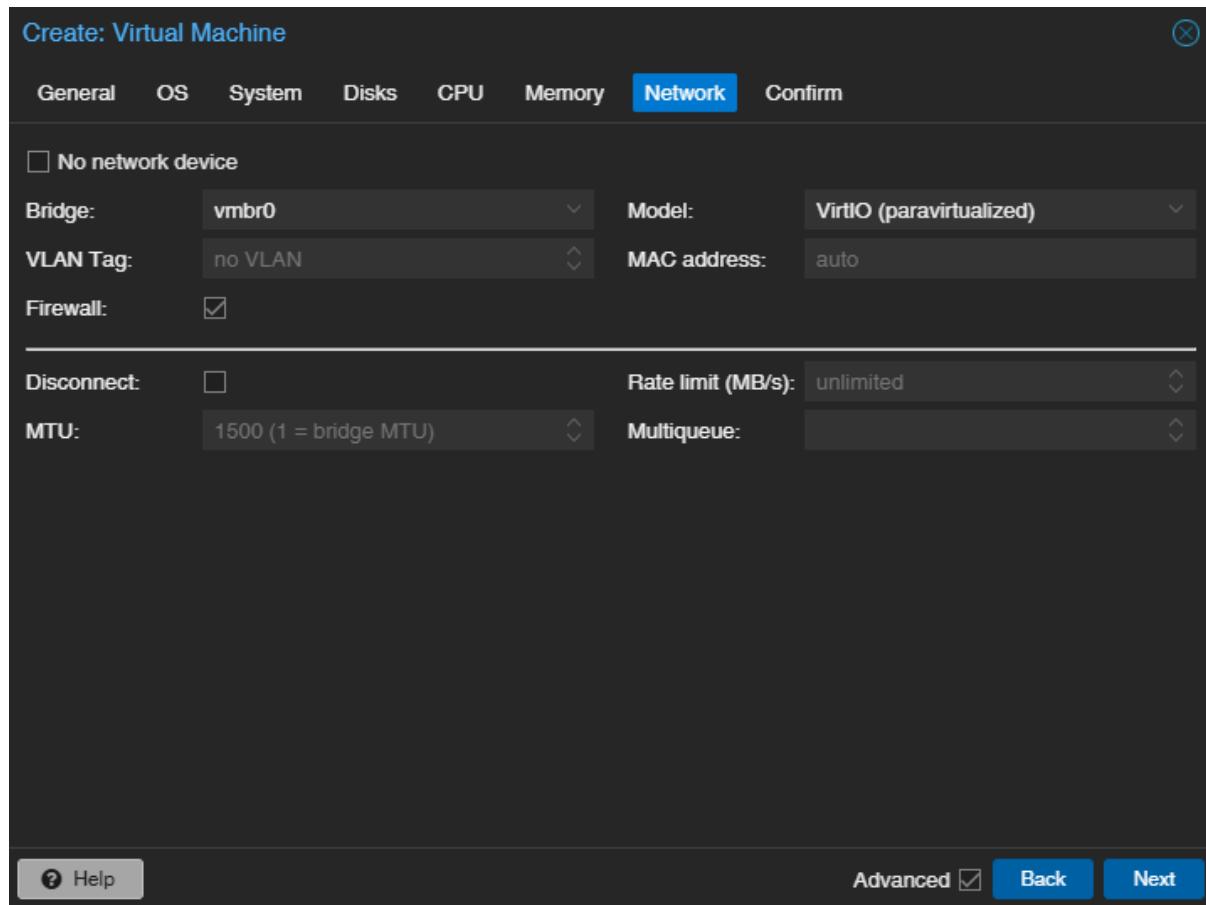
Se apagó la VM y se modificó la memoria desde la pestaña Hardware > Memory en Proxmox.



Network

Model: VirtIO (paravirtualized)

Bridge: vmbr0 (puente conectado a la red física/LAN real)



Confirmación final

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Key ↑	Value
cores	2
cpu	host
ide2	local:iso/OPNsense-25.1-dvd-amd64.iso,media=cdrom
memory	2048
name	opnsense
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve001
numa	0
ostype	other
scsi0	local-lvm:20,ssd=on
sockets	1
vmid	102

Start after created

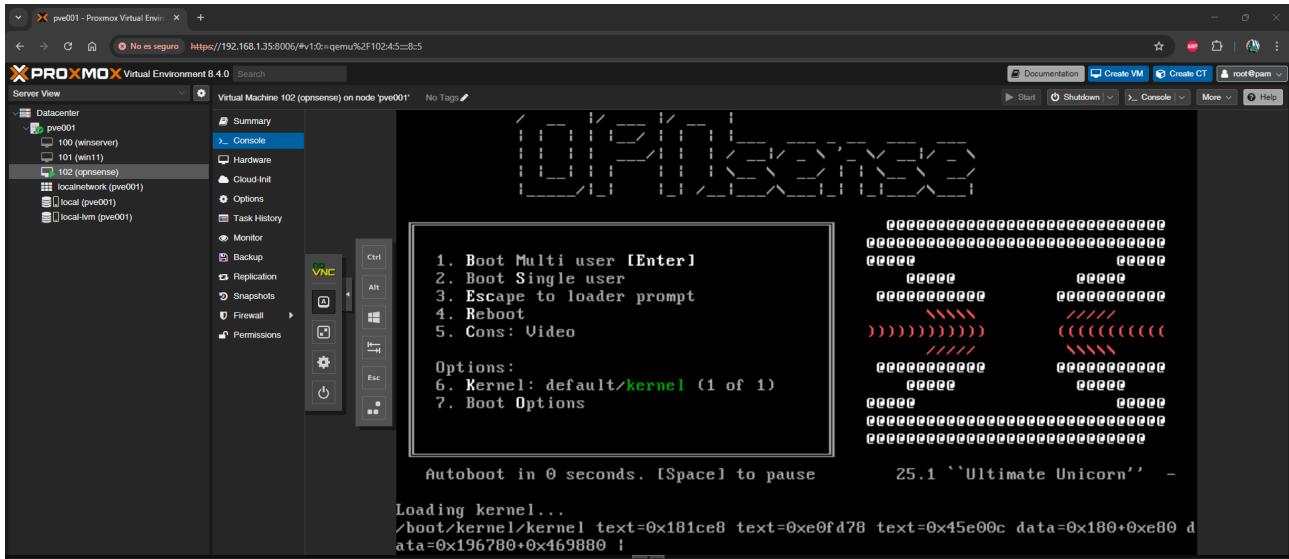
Advanced Back Finish

Se recomienda revisar la configuración realizada antes de pulsar en **Finish**

A4.3. Instalación OPNsense

Una vez creada la máquina virtual, se arranca por primera vez desde la ISO de OPNsense. El sistema carga automáticamente y presenta una serie de mensajes hasta llegar a la pantalla de login inicial del instalador.

Al arrancar la máquina no hace falta tocar nada hasta que aparezca una línea de comandos solicitando usuario y contraseña (usuario: **installer**, contraseña **opnsense**)



No es necesario interactuar con ninguna pantalla previa al login; el sistema arranca directamente en modo instalación.

```
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Sat May 24 01:15:24 UTC 2025

*** OPNsense.localedomain: OPNsense 25.1 (amd64) ***

LAN (vtnet0)      -> v4: 192.168.1.1/24

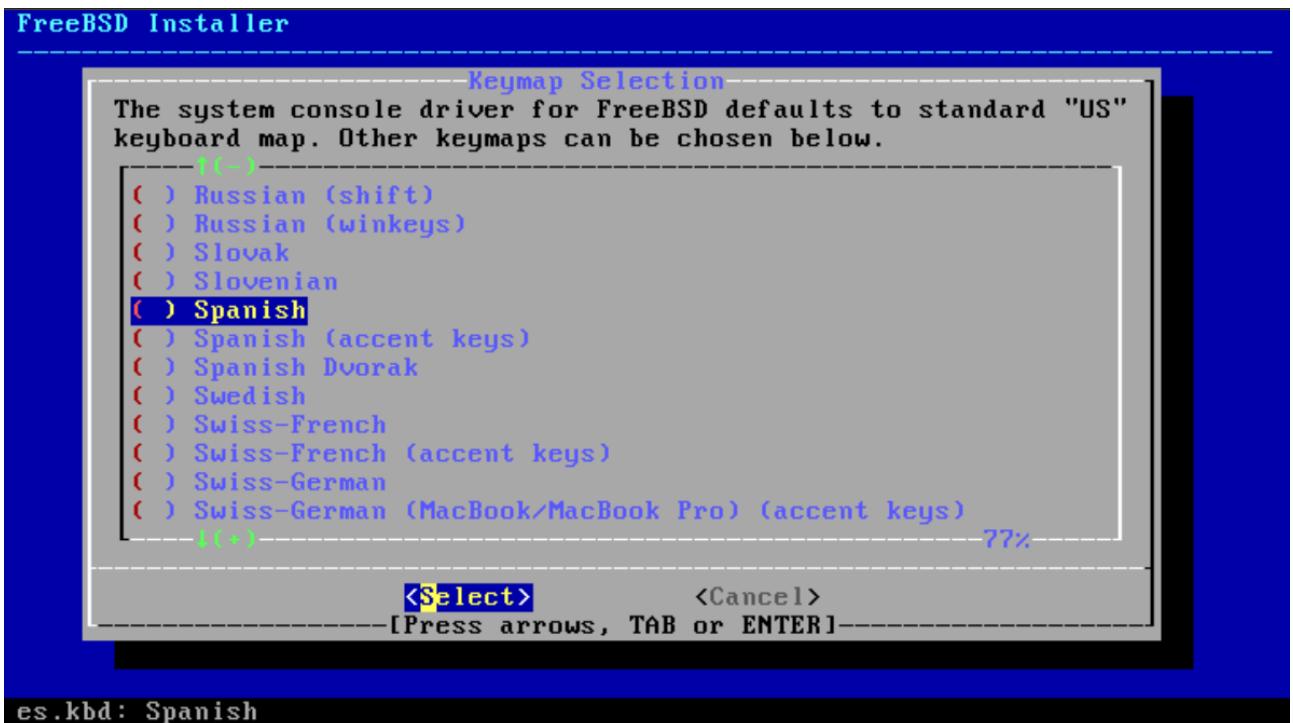
HTTPS: sha256 87 3C 70 34 E8 44 37 18 B9 5B ED 05 79 07 EF 77
        A7 B1 37 96 68 97 DE 96 33 59 DA 93 F2 0B 81 86
SSH:    SHA256 6WB3LG1C2K1hY/J78WYArb5hubSyUDBevXq4LvJsyxA (ECDSA)
SSH:    SHA256 biuBRowZuAFoQN1jaDisK5ARsUmKBVs0h3xVMWxjMs4 (ED25519)
SSH:    SHA256 zKDgZCAJ3XPBBcSnpmrjqS/ev6QBiu6A/110BvshJXQ (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

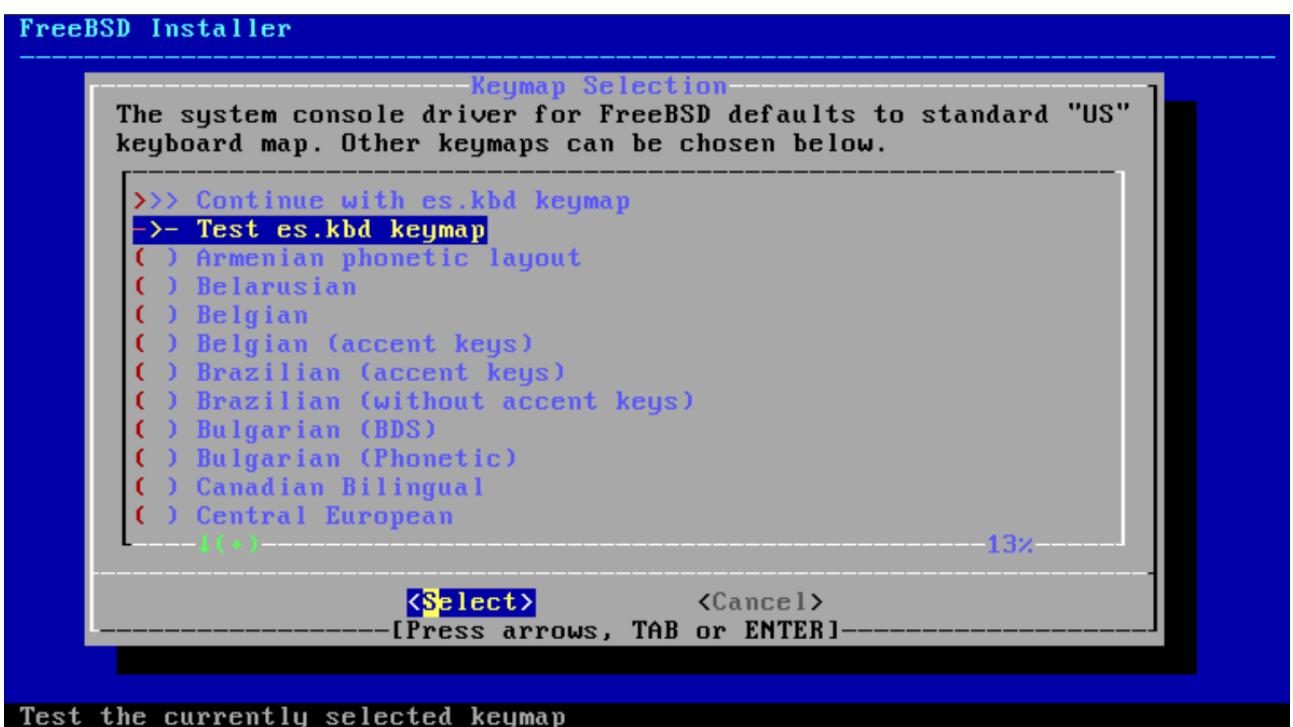
FreeBSD/amd64 (OPNsense.localedomain) (ttyv0)

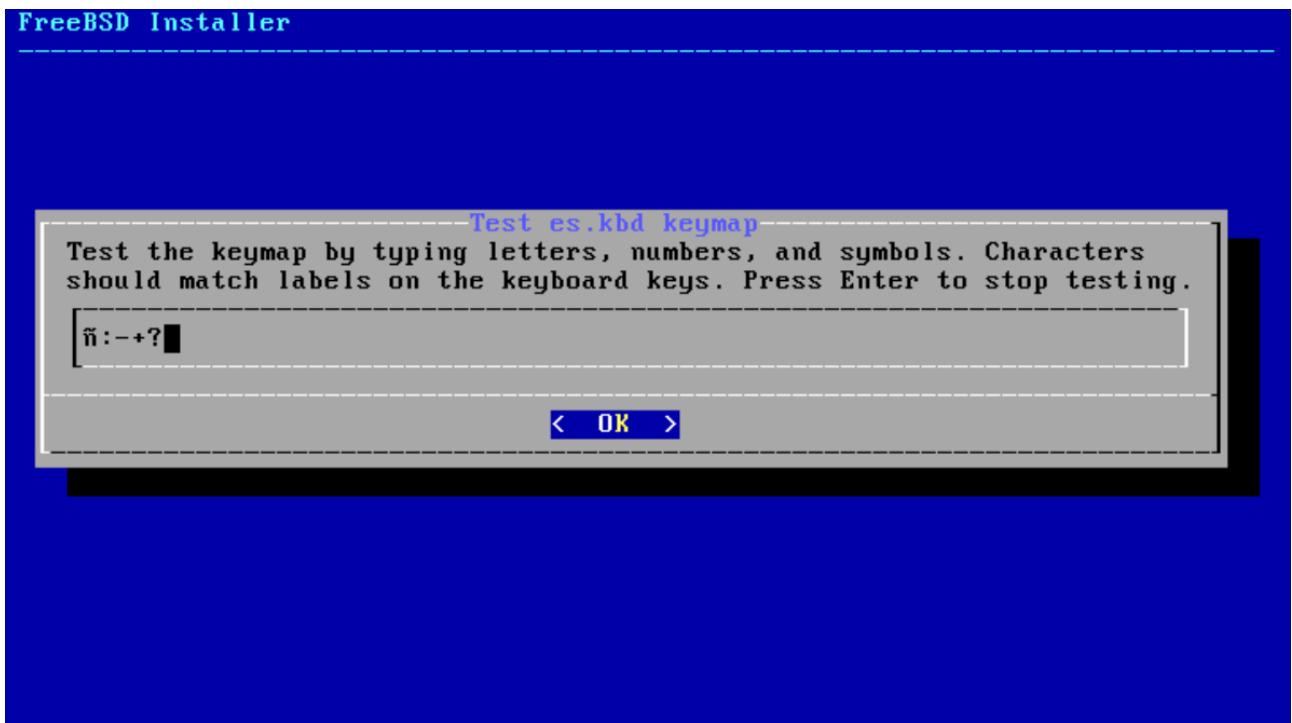
login: installer
Password: 
```

Seleccionar el layout de teclado

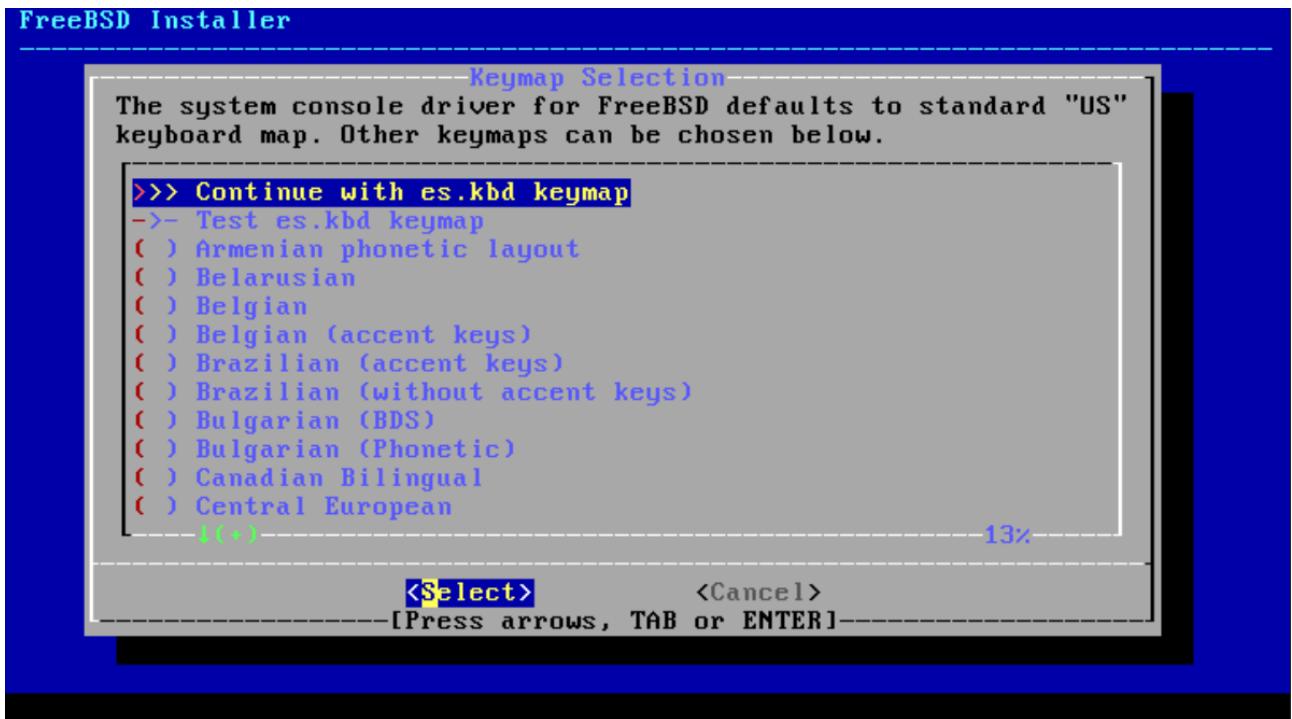


Se recomienda comprobar la opción de teclado con “Test es.kbd keymap”





Una vez comprobado que funciona correctamente continuar.

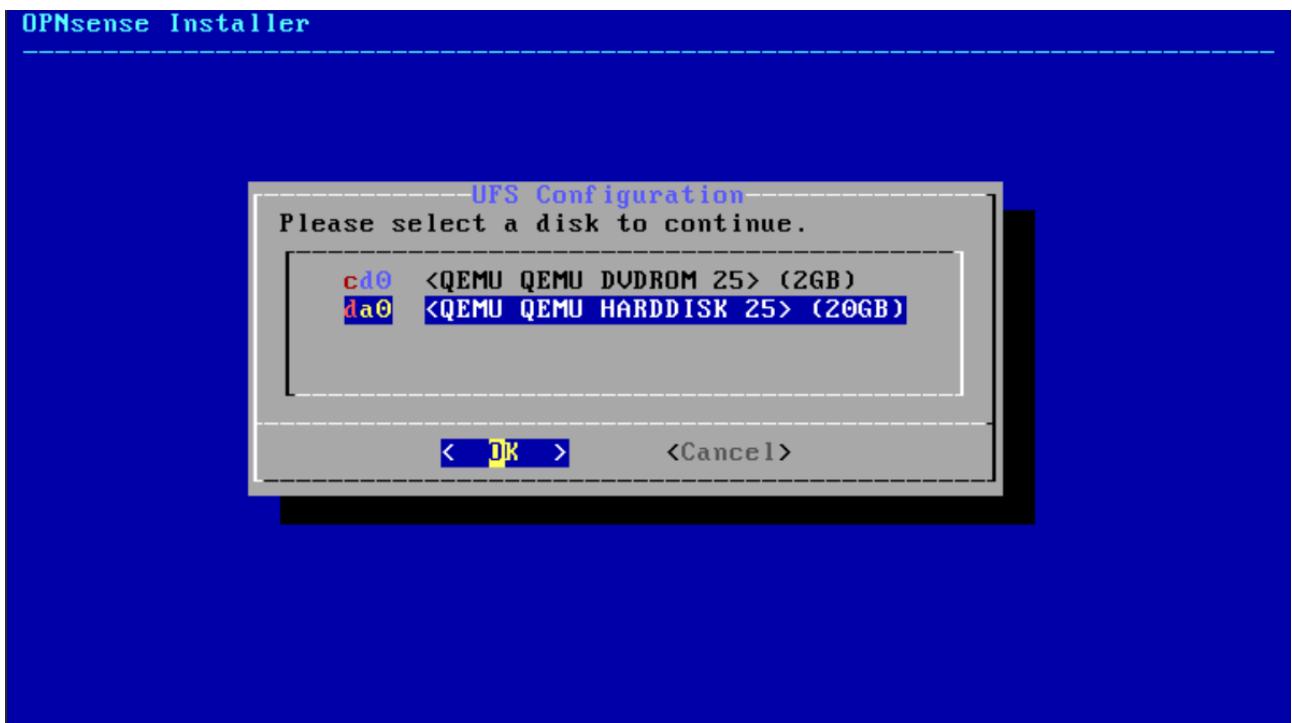


En este proyecto se configuró la máquina virtual con BIOS tradicional (SeaBIOS) en lugar de UEFI. Esto influye directamente en el tipo de sistema de archivos elegido: se seleccionó UFS, que es perfectamente compatible con BIOS y más ligero que ZFS.

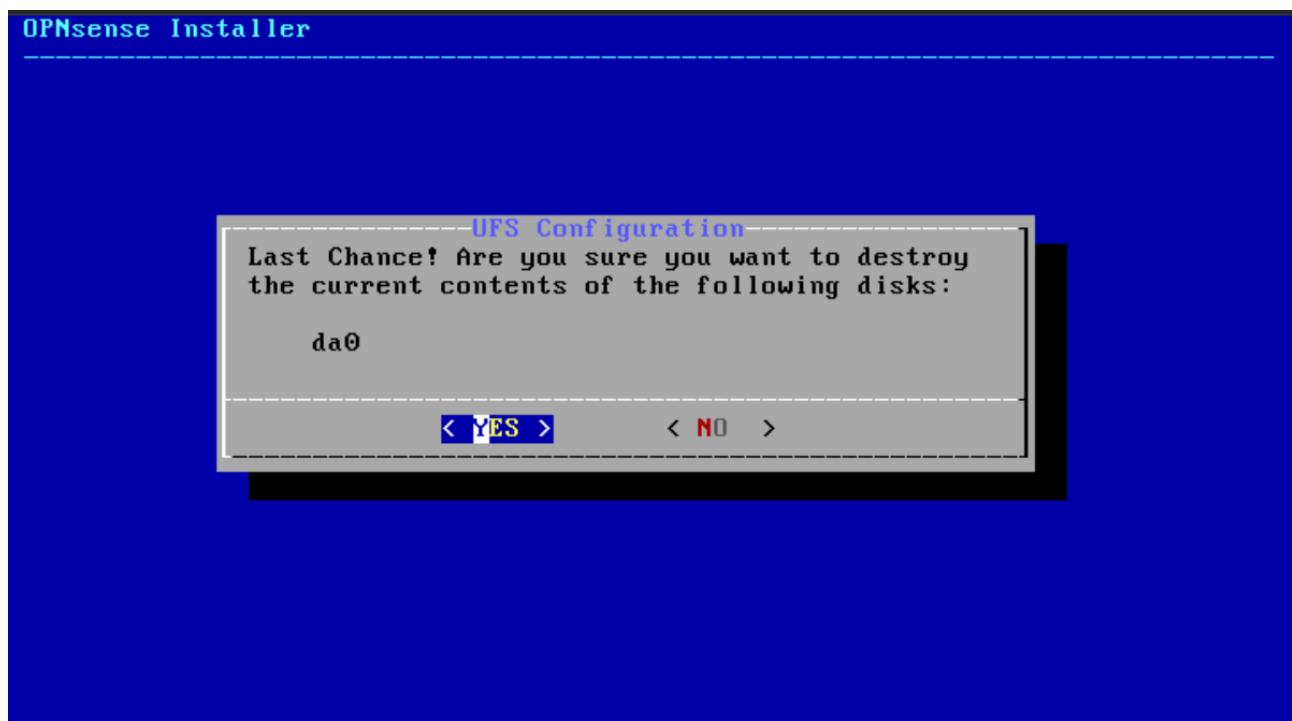
Aunque la opción indica GPT/UEFI Hybrid, UFS funciona correctamente sobre BIOS sin requerir EFI.



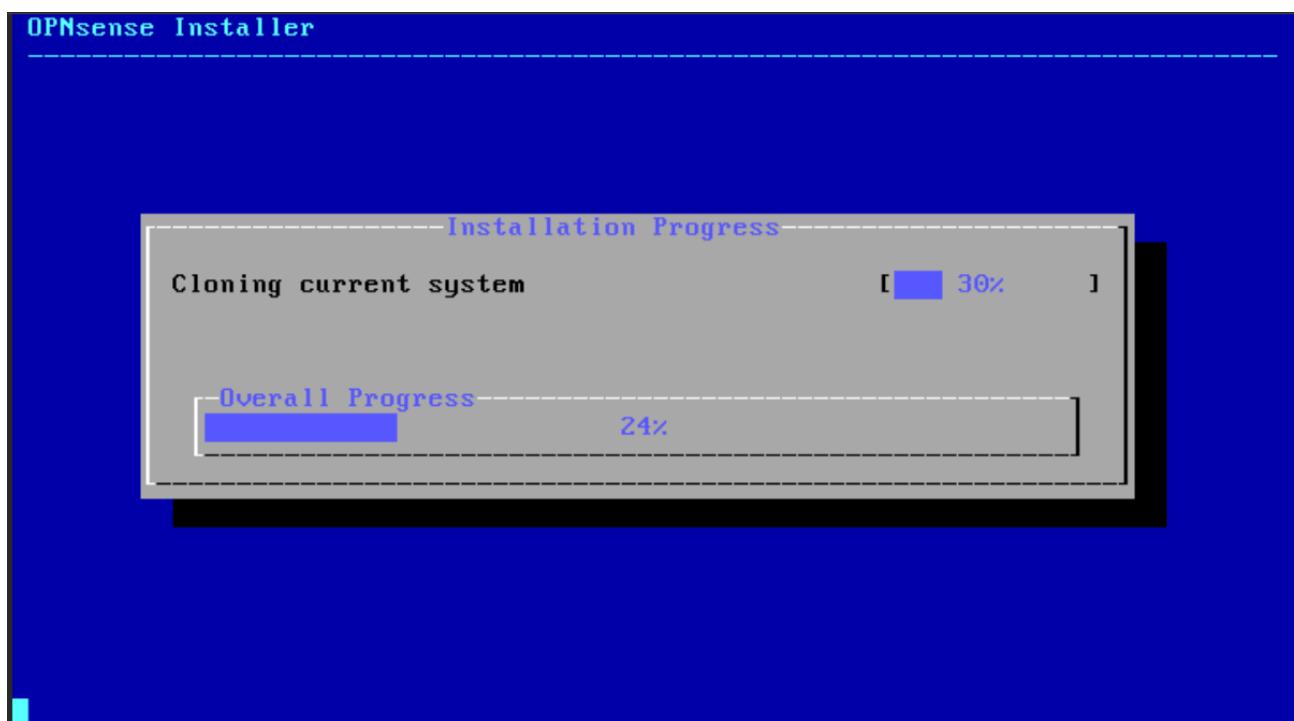
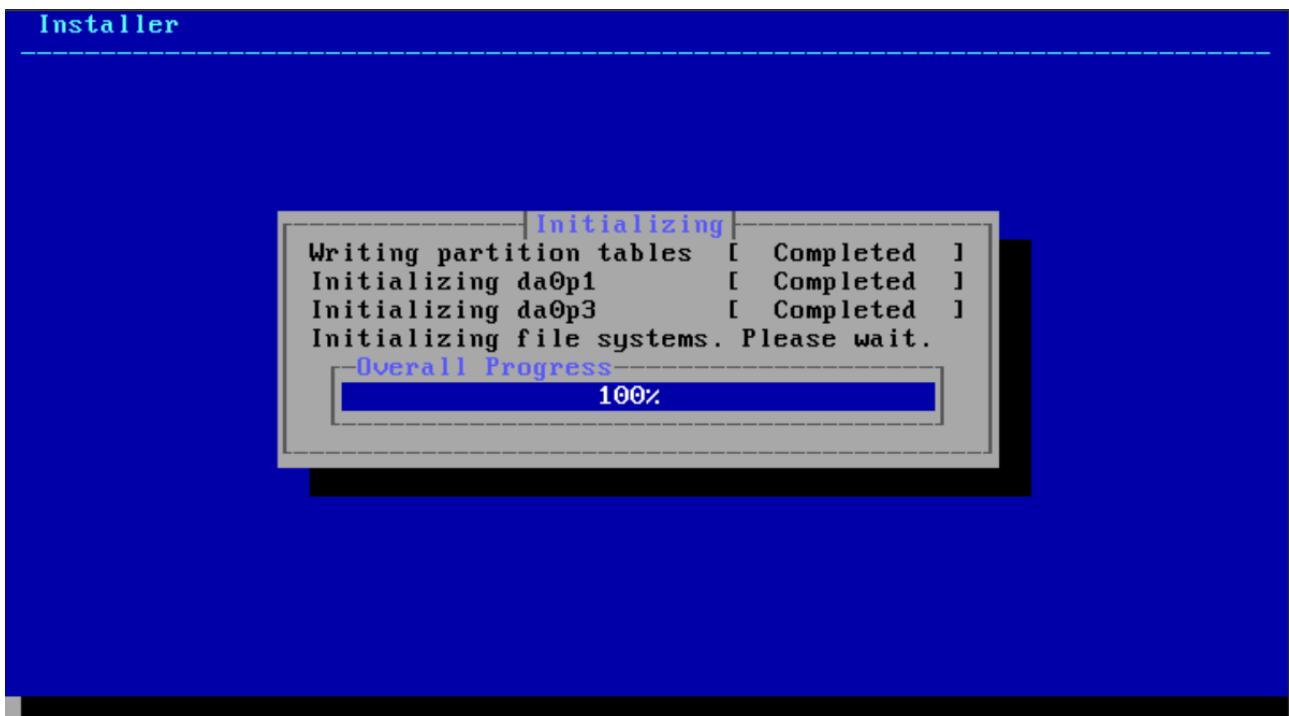
Una vez seleccionada la opción de instalación (UFS), el asistente muestra el disco virtual disponible. Se acepta el disco y se inicia la instalación, que consiste en formatear, particionar y copiar el sistema base.



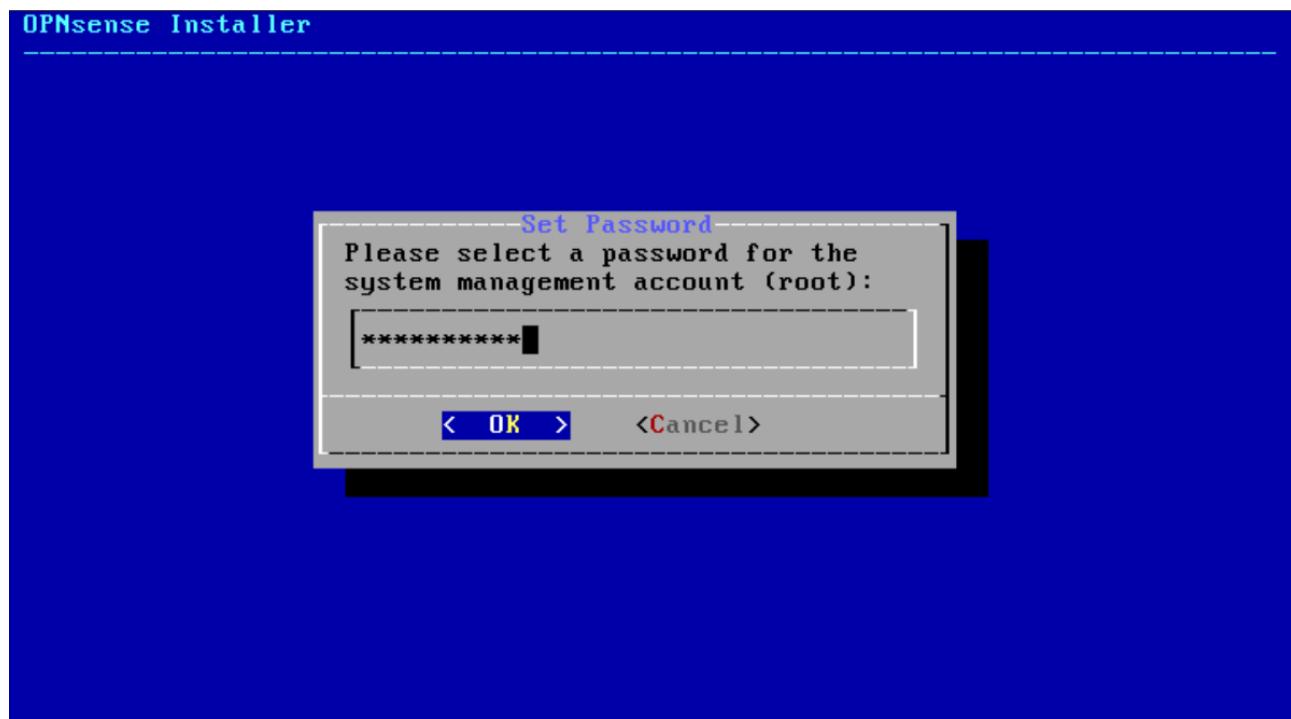
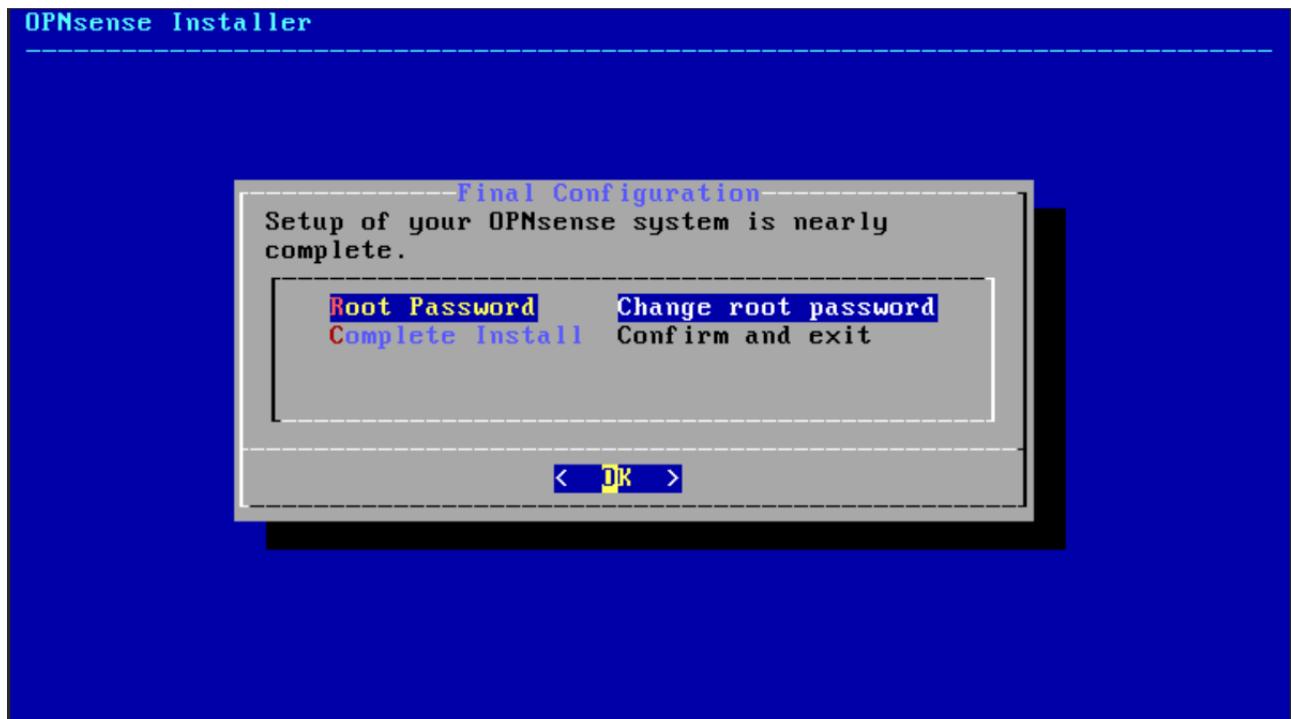
Nos avisa de que se perderá todo el contenido del disco.



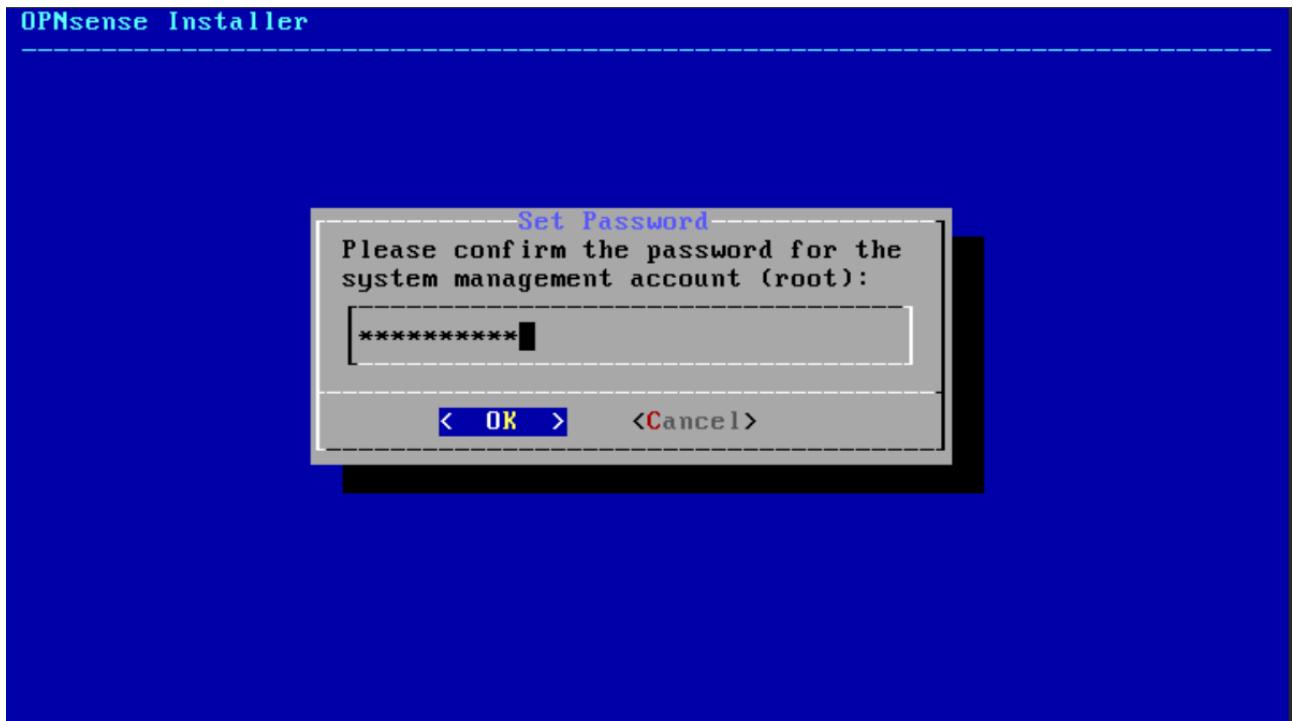
No se requieren ajustes adicionales durante esta fase. La instalación tarda pocos minutos. Al finalizar, se indica que es necesario reiniciar el sistema.



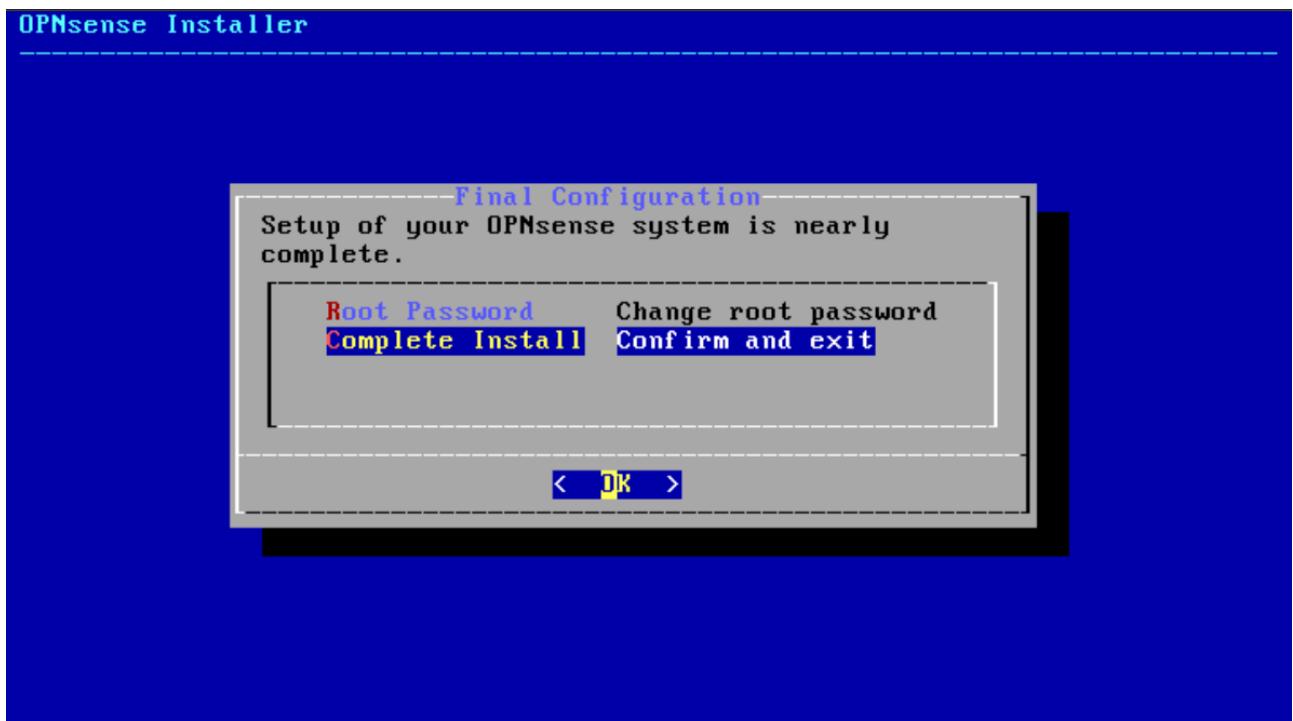
Antes de reiniciarse el sistema nos pide como medida de seguridad que cambiemos la contraseña root que viene por defecto.



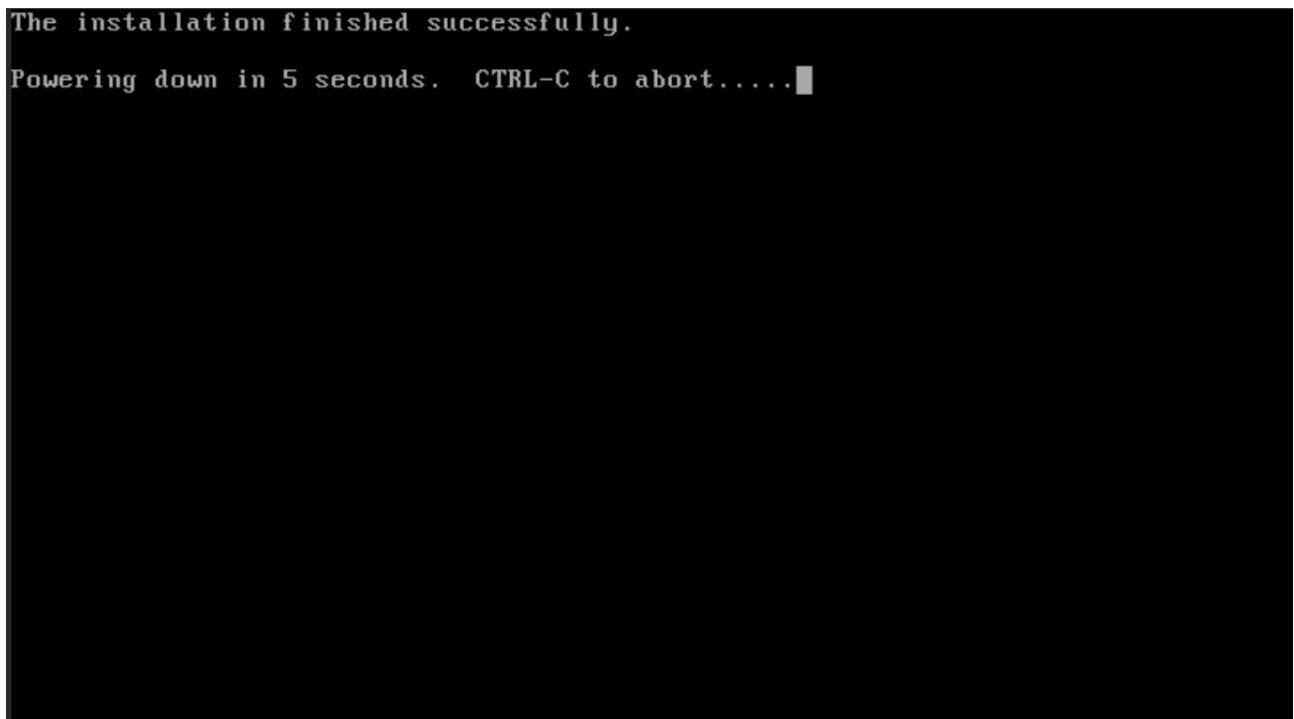
Confirmar la contraseña.



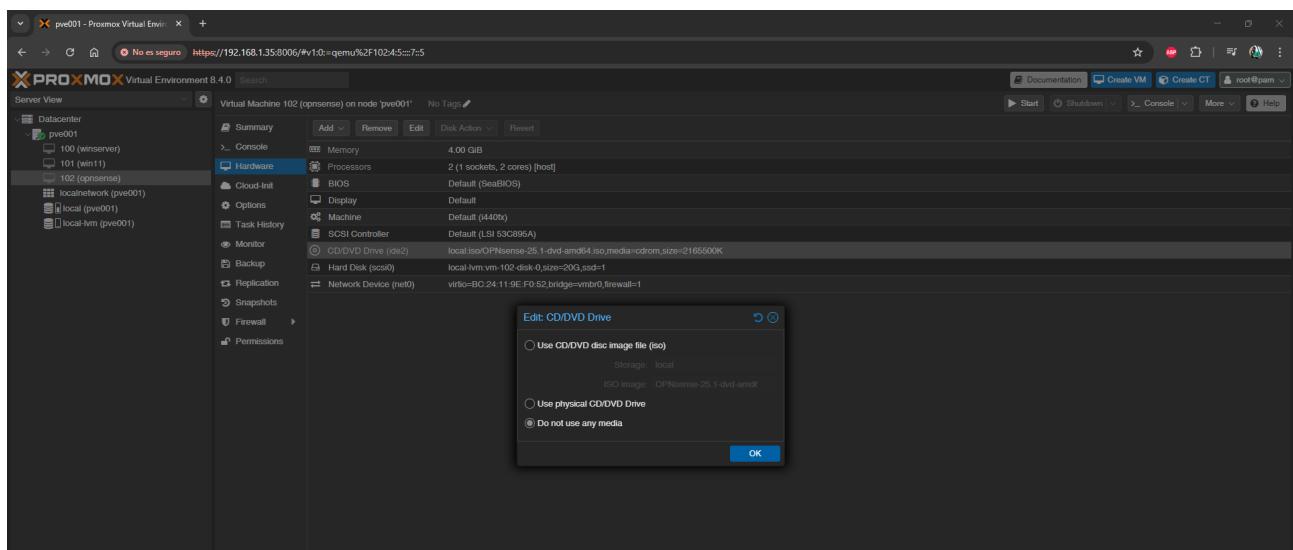
Y finalmente dar en “Complete Install – Confirm and exit”



Entonces se reinicia la máquina.



Nota: Quitar la imagen ISO antes de reiniciar el sistema entrando en su menú > Hardware > CD/DVD Drive, hacer clic en editar y en la ventana emergente marcar la opción “Do not use any media”



Una vez que reinicie ya se puede hacer login con el usuario root y la contraseña configurada en la instalación.

```
Starting Unbound DNS...done.
>>> Invoking start script 'newwanip'
>>> Invoking start script 'freebsd'
>>> Invoking start script 'syslog'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Sat May 24 01:38:44 UTC 2025

*** OPNsense.locaLdomain: OPNsense 25.1 (amd64) ***

LAN (vtnet0)      -> v4: 192.168.1.1/24

HTTPS: sha256 6D 17 4A B8 DB 19 88 A8 54 15 C5 1F 8E 92 21 93
       35 16 F7 C4 9A 01 28 47 4F EA 8F 32 B7 6F 4D 21

FreeBSD/amd64 (OPNsense.locaLdomain) (ttyv0)

login: root
Password: [REDACTED]
```

A4.4. Dirección IP LAN estática para acceso a Web GUI

La interfaz LAN es la interfaz de red por donde se accede a la interfaz Web de administración por lo que se debe configurar previamente para poder acceder.

Notese que la IP que asigna por defecto es la puerta de enlace habitual de cualquier router. Esto es porque OPNsense está pensado para ser un Firewall de borde. En este proyecto se usará opnsense como un servidor más de la red interna que hará la función de Servidor de conexión VPN por lo que se debe cambiar la IP por otra para que no haya conflicto con la puerta de enlace real y puedan tener acceso a internet tanto opnsense como los demás. Por lo que se le asignará una IP de la red interna disponible.

Para ello entrar en la opción 2 del menú.

```
| Hello, this is OPNsense 25.1 | 0000000000000000  
| Website: https://opnsense.org/ | 0000 0000  
| Handbook: https://docs.opnsense.org/ | 000\\ \\ //000  
| Forums: https://forum.opnsense.org/ | )))))))) (((((((  
| Code: https://github.com/opnsense | 000// / \\ \\ 000  
| Reddit: https://reddit.com/r/opnsense | 0000 0000  
-----  
*** OPNsense.localdomain: OPNsense 25.1 (amd64) ***  
  
LAN (vtnet0) -> v4: 192.168.1.1/24  
  
HTTPS: sha256 6D 17 4A B8 DB 19 88 A8 54 15 C5 1F 8E 92 21 93  
       35 16 F7 C4 9A 01 28 47 4F EA 8F 32 B7 6F 4D 21  
  
0) Logout 7) Ping host  
1) Assign interfaces 8) Shell  
2) Set interface IP address 9) pfTop  
3) Reset the root password 10) Firewall log  
4) Reset to factory defaults 11) Reload all services  
5) Power off system 12) Update from console  
6) Reboot system 13) Restore a backup  
  
Enter an option: 2
```

Le decimos que **no** se configure por **DHCP** para evitar que se cambie la IP sin nuestro conocimiento y evitar problemas de conexión.

```

| Code:      https://github.com/opnsense   |       0000          0000
| Reddit:    https://reddit.com/r/opnsense |       0000000000000000
-----



*** OPNsense.localdomain: OPNsense 25.1 (amd64) ***

LAN (vtnet0)    -> v4: 192.168.1.1/24

HTTPS: sha256 6D 17 4A B8 DB 19 88 A8 54 15 C5 1F 8E 92 21 93
        35 16 F7 C4 9A 01 28 47 4F EA 8F 32 B7 6F 4D 21

0) Logout          7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: 2

Configure IPv4 address LAN interface via DHCP? [y/N] N

Enter the new LAN IPv4 address. Press <ENTER> for none:
> █

```

Asignamos la dirección de red **192.168.1.101**, máscara de red **24**

```

2) Set interface IP address      9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system                13) Restore a backup

Enter an option: 2

Configure IPv4 address LAN interface via DHCP? [y/N] N

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.101

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █

```

Añadir el router como puerta de enlace.

```
2) Set interface IP address          9) pfTop
3) Reset the root password         10) Firewall log
4) Reset to factory defaults       11) Reload all services
5) Power off system                12) Update from console
6) Reboot system                  13) Restore a backup

Enter an option: 2

Configure IPv4 address LAN interface via DHCP? [y/N] N

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.101

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
```

Cuando pregunte si queremos usar el router como DNS le decimos que no, y cuando pida la IPv4 del servidor de nombres introducir uno válido (el de cloudflared 1.1.1.1 por ejemplo).

```
6) Reboot system                  13) Restore a backup

Enter an option: 2

Configure IPv4 address LAN interface via DHCP? [y/N] N

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.101

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1

Do you want to use the gateway as the IPv4 name server, too? [Y/n] n
Enter the IPv4 name server or press <ENTER> for none:
> 1.1.1.1
```

Dar que si (“y”) a que genere un certificado autofirmado para la conexión https. El resto de opciones dejarlas en blanco o responder con N

```
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1

Do you want to use the gateway as the IPv4 name server, too? [Y/n] n
Enter the IPv4 name server or press <ENTER> for none:
> 1.1.1.1

Configure IPv6 address LAN interface via DHCP6? [y/N] N

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] N

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] N
Do you want to generate a new self-signed web GUI certificate? [y/N] y
Restore web GUI access defaults? [y/N] N
```

Con esto ya tendría configurada la interfaz LAN hacia la red interna de la empresa.

```
Starting Unbound DNS...done.
Configuring firewall.....done.
Starting web GUI...done.

You can now access the web GUI by opening
the following URL in your web browser:

https://192.168.1.101

*** OPNsense.localdomain: OPNsense 25.1 (amd64) ***

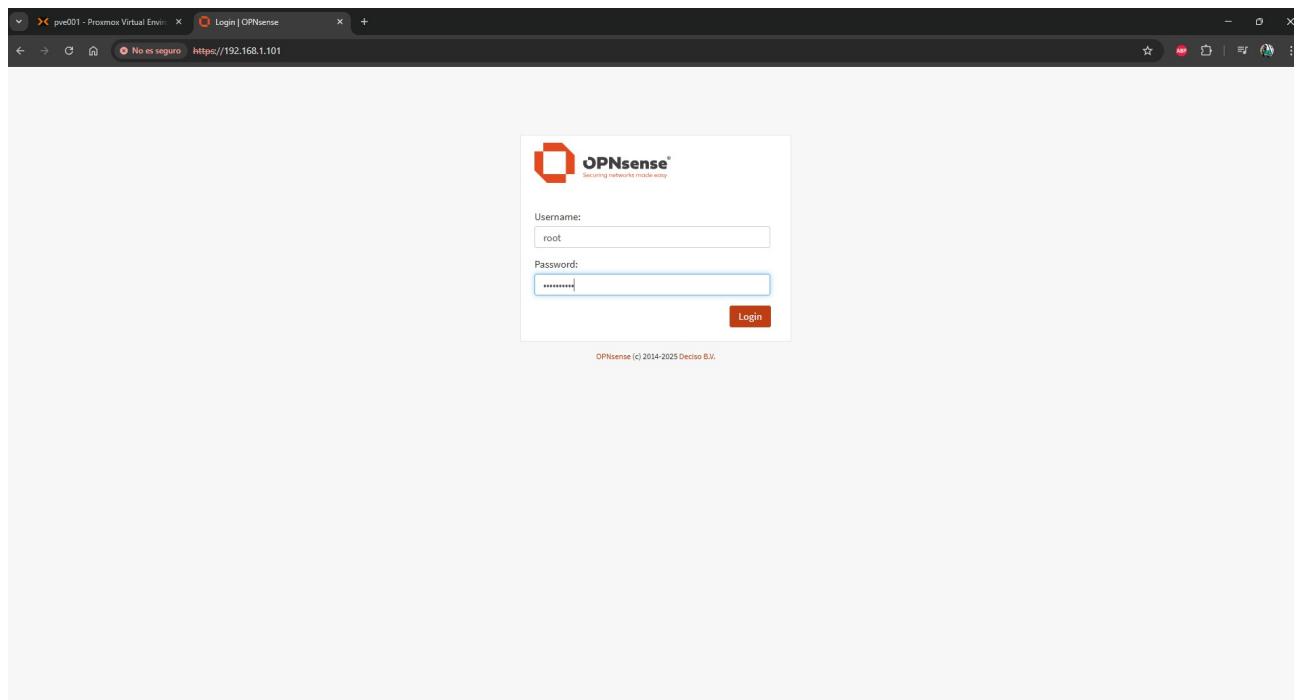
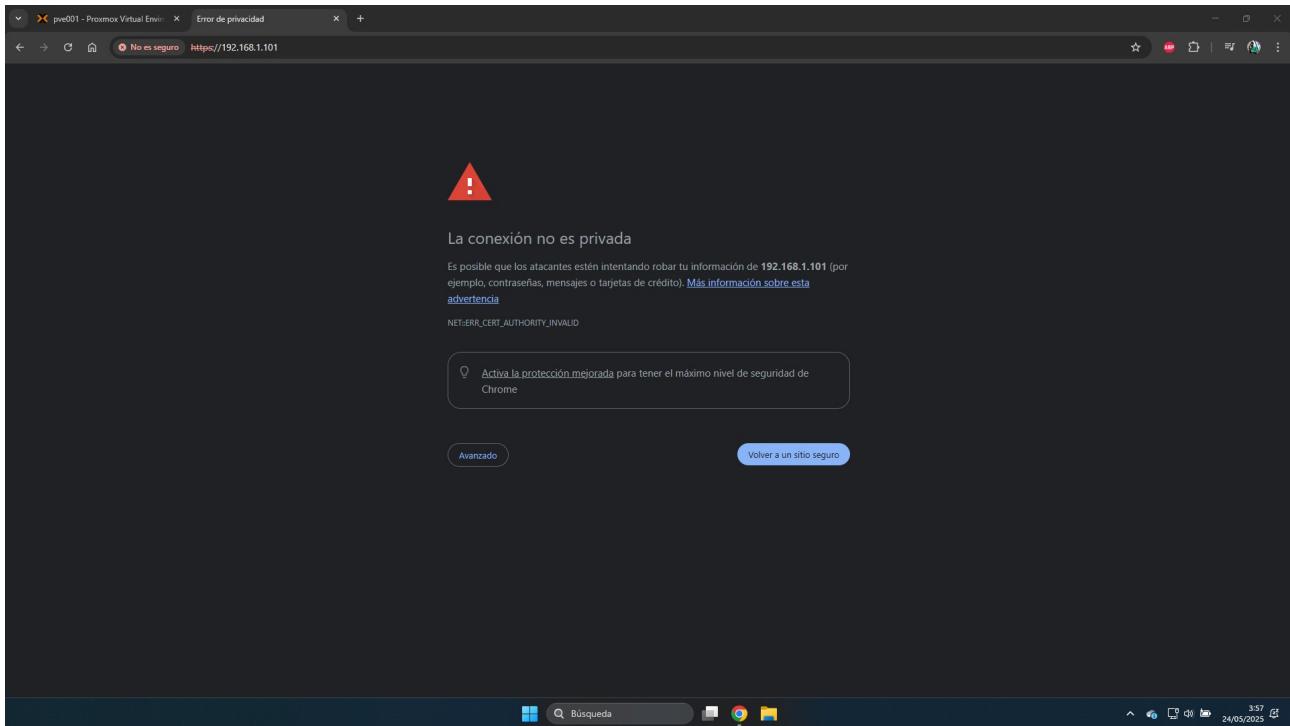
LAN (vtnet0)      -> v4: 192.168.1.101/24

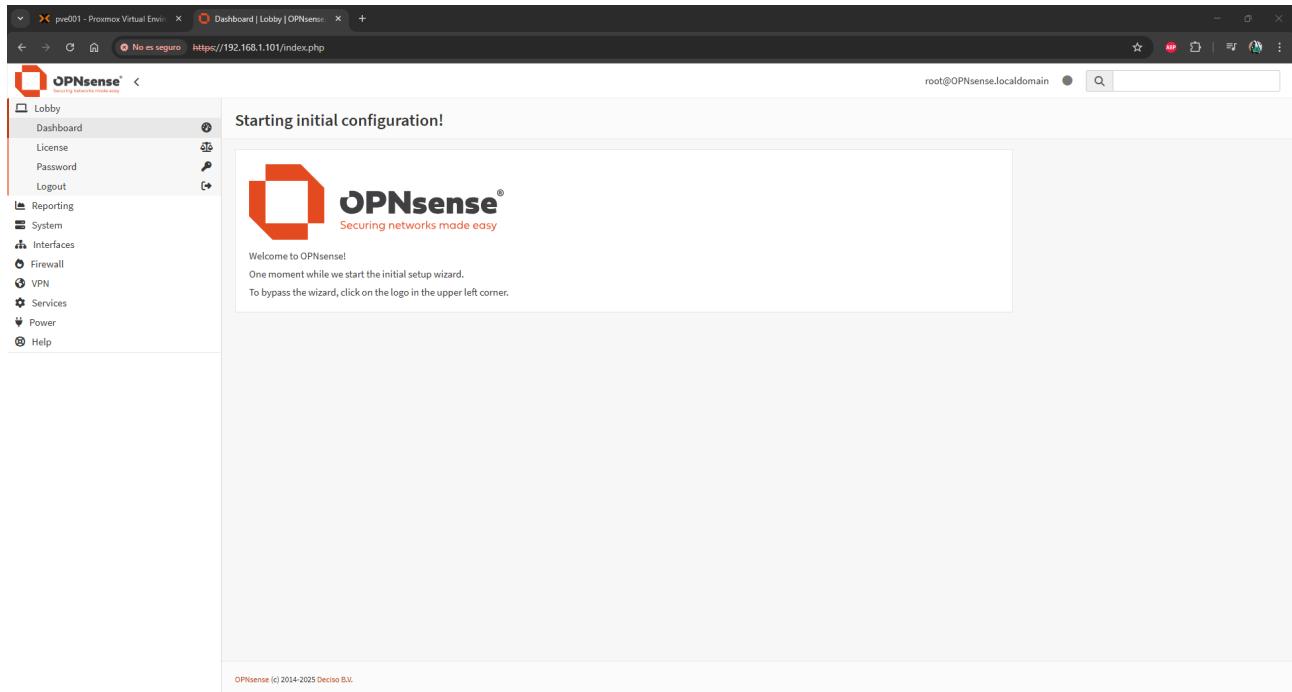
HTTPS: sha256 89 F5 18 C1 76 72 53 EF FC 2E 79 23 CB BE BC 6B
       A0 9A 15 66 34 CF 44 36 51 83 F5 CF FD 76 FF 42

 0) Logout                      7) Ping host
 1) Assign interfaces            8) Shell
 2) Set interface IP address    9) pfTop
 3) Reset the root password     10) Firewall log
 4) Reset to factory defaults   11) Reload all services
 5) Power off system             12) Update from console
 6) Reboot system                13) Restore a backup

Enter an option: ■
```

Y ya podemos acceder a su interfaz web





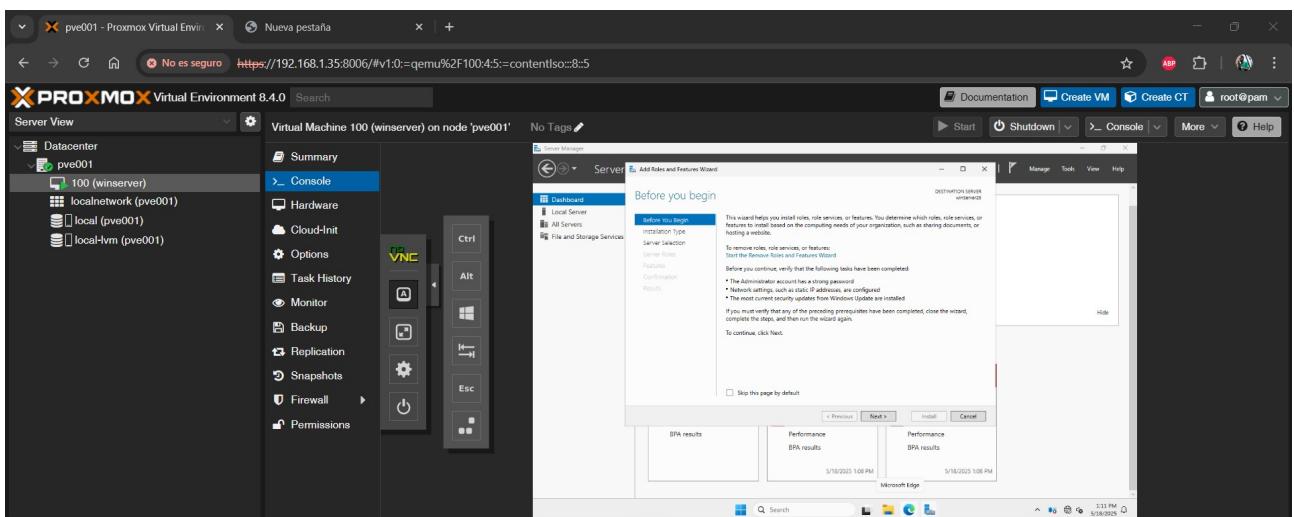
Anexo 5 – Instalación del rol de AD DS y promoción a controlador de dominio

Este anexo describe el proceso de instalación del rol Active Directory Domain Services (AD DS) en el servidor Windows, así como la promoción del equipo a controlador de dominio principal del entorno.

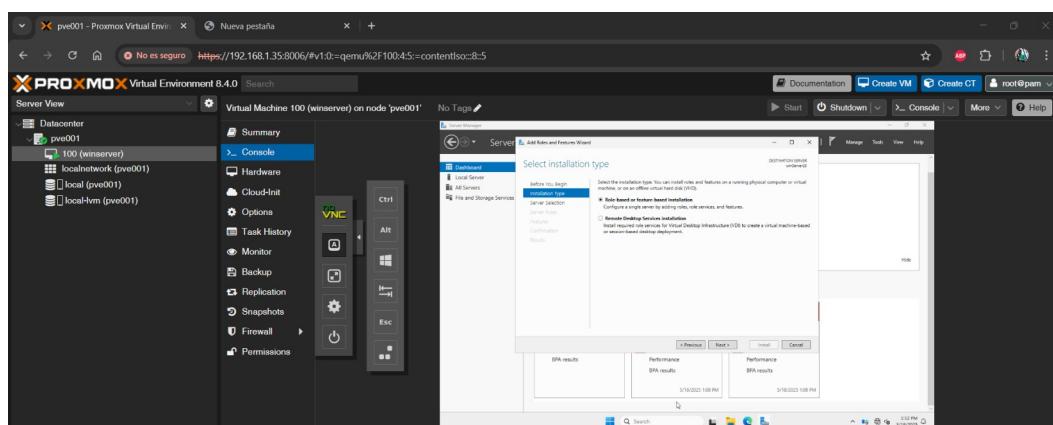
Esta acción representa el paso fundamental para iniciar la gestión centralizada de usuarios, políticas de grupo y autenticación dentro de la red simulada.

A5.1. Inicio del asistente de instalación de roles

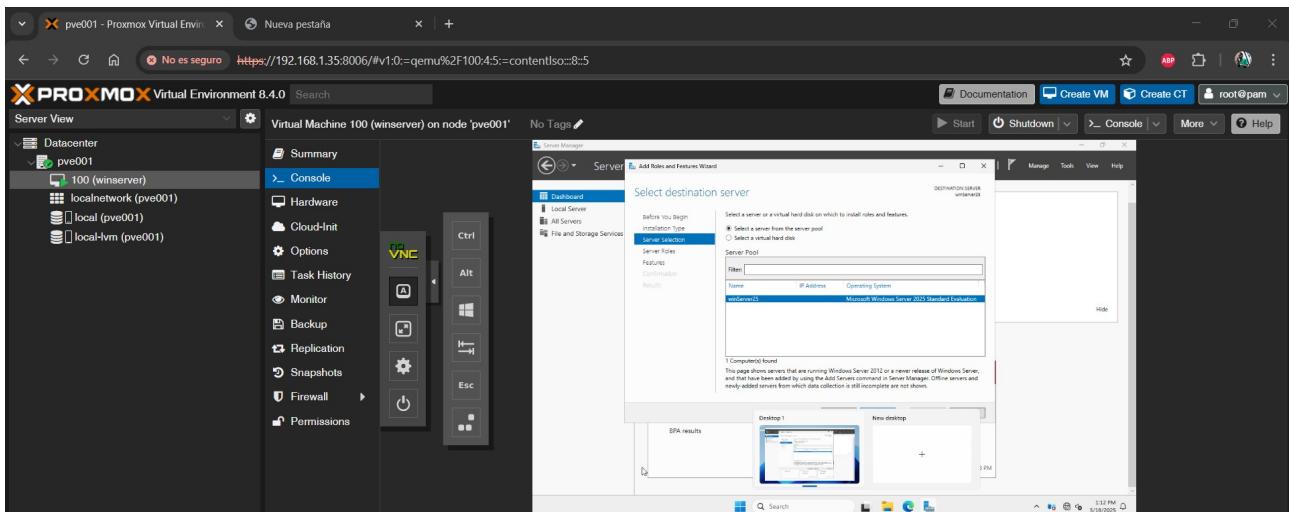
Desde Server Manager, se selecciona la opción “Aregar roles y características”. Se inicia el asistente gráfico correspondiente.



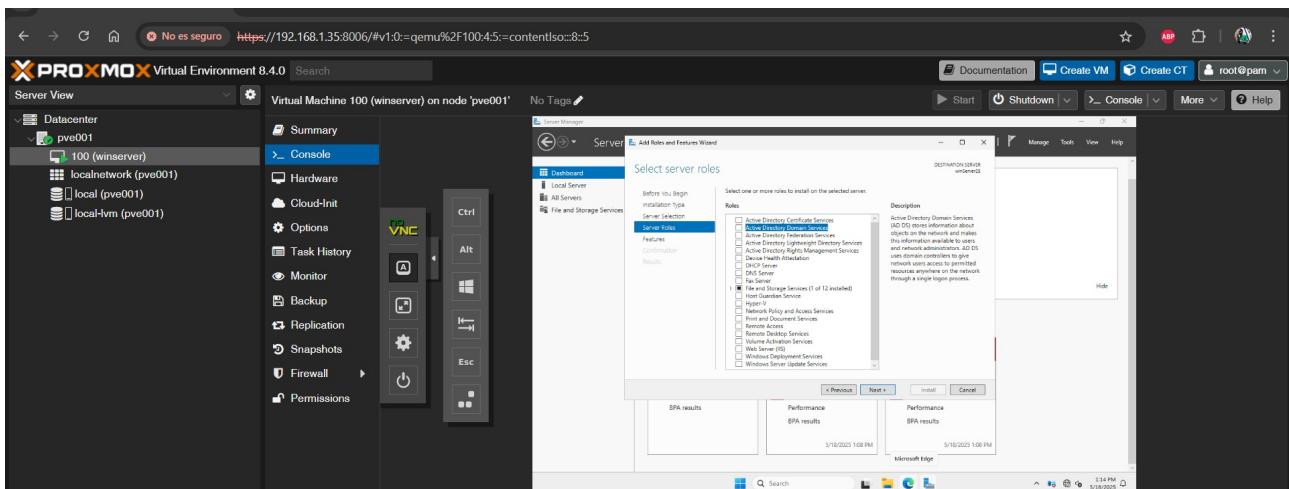
Seleccionar *Instalación basada en roles y características*



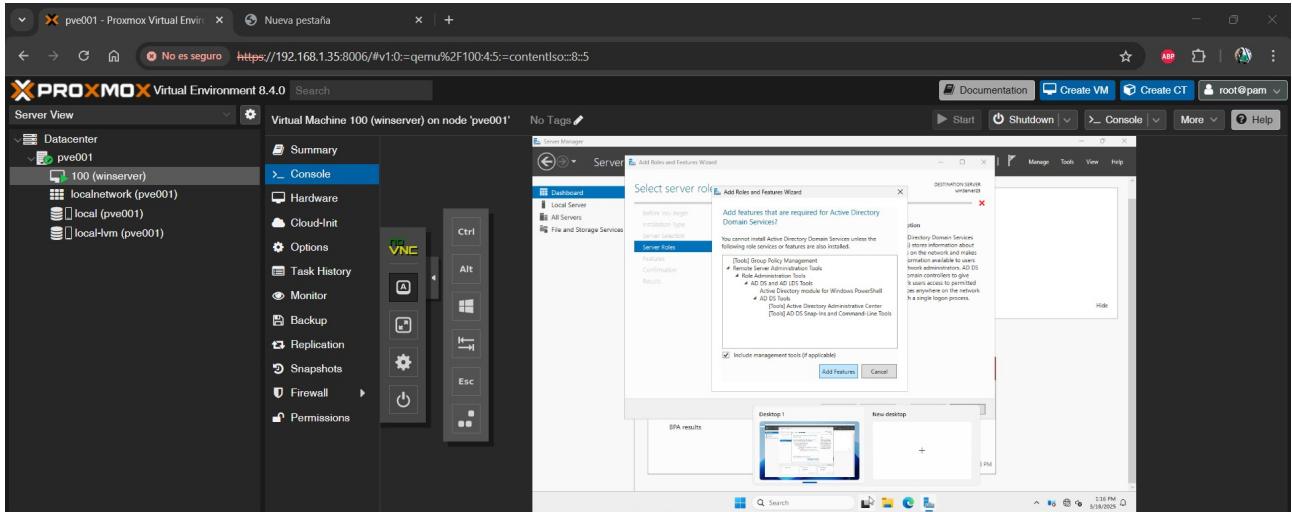
Seleccionar el servidor windows Server.



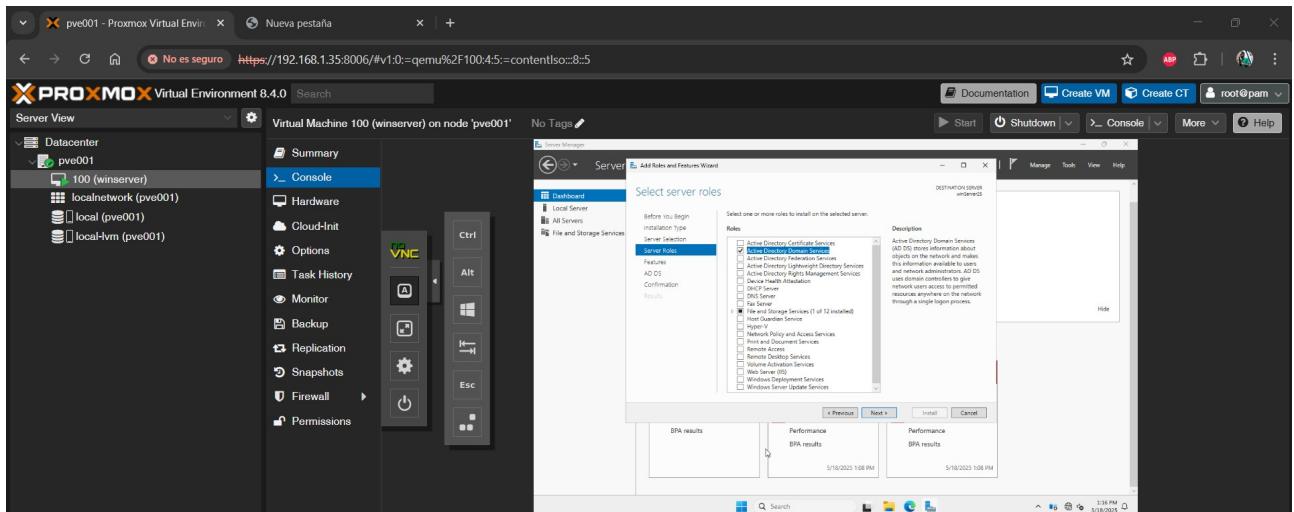
Elegir Acitve Directory Domain Service.



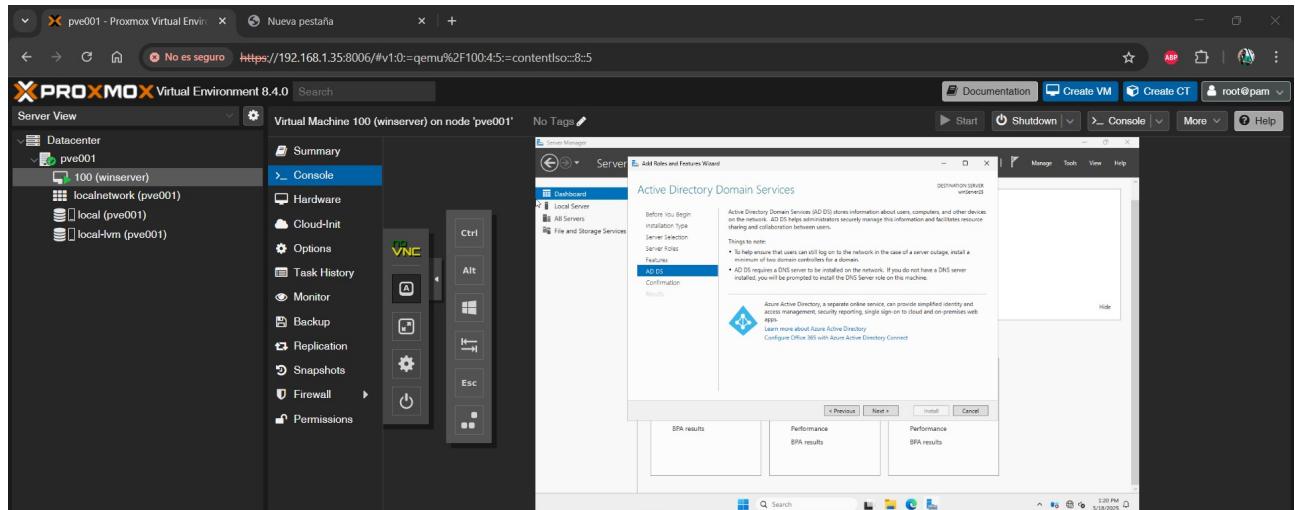
Add features



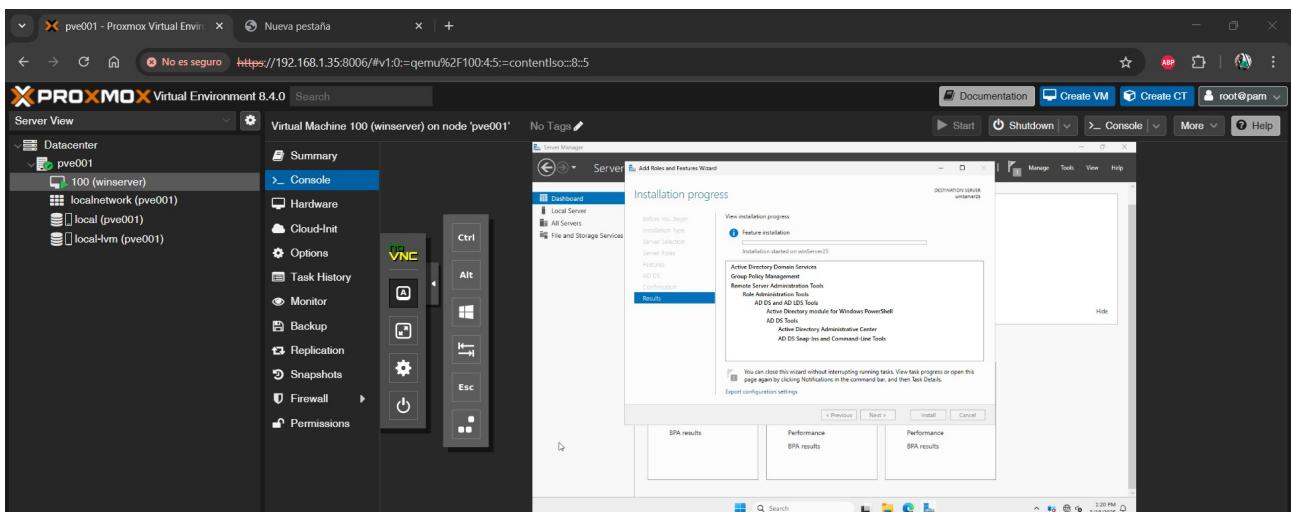
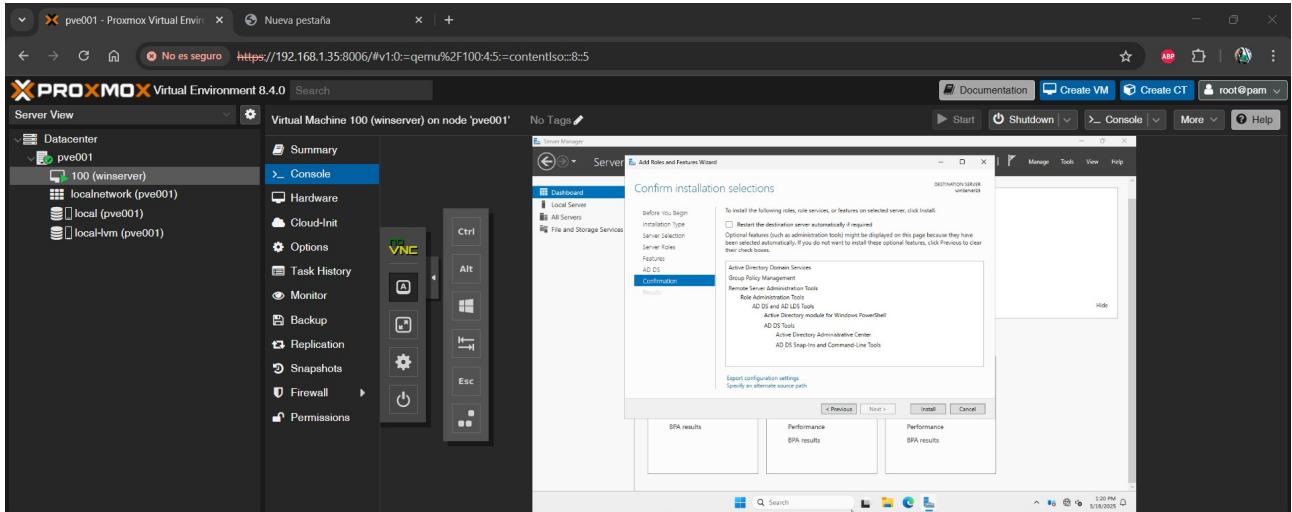
Start Time	End Time	Node	User name	Description	Status
May 18 12:47:30		pve001	root@pam	VM/CT 100 - Console	>
May 18 12:47:29	May 18 12:47:30	pve001	root@pam	VM 100 - Start	OK >
May 18 12:38:59	May 18 12:38:59	pve001	root@pam	Bulk start VMs and Containers	OK >
May 18 06:04:57	May 18 06:05:02	pve001	root@pam	Bulk shutdown VMs and Containers	OK >
May 18 06:04:57	May 18 06:05:01	pve001	root@pam	VM 100 - Shutdown	OK >



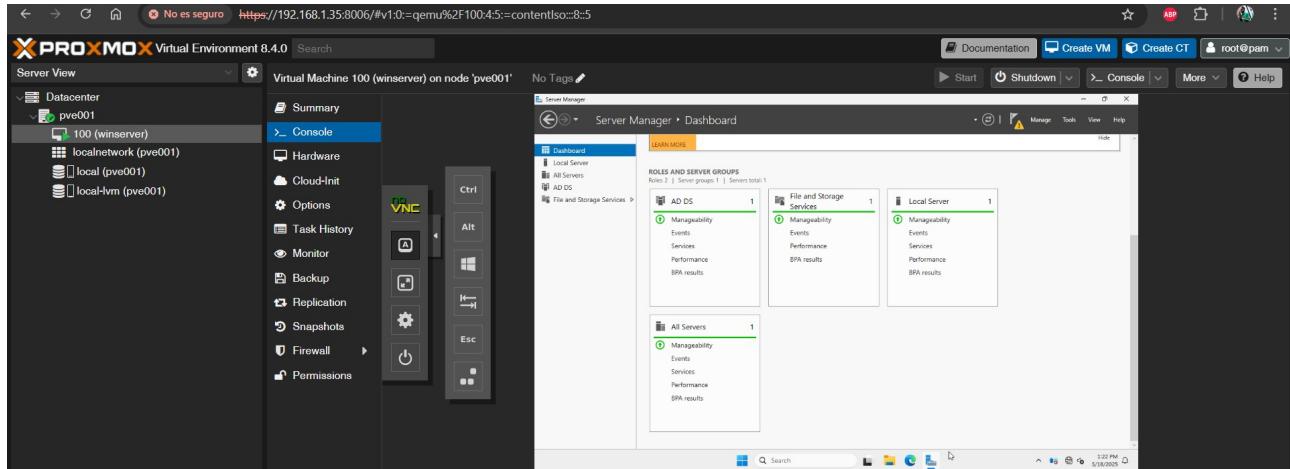
En features no es necesario tocar nada.



Seguir el asistente de hasta finalizar la instalación.

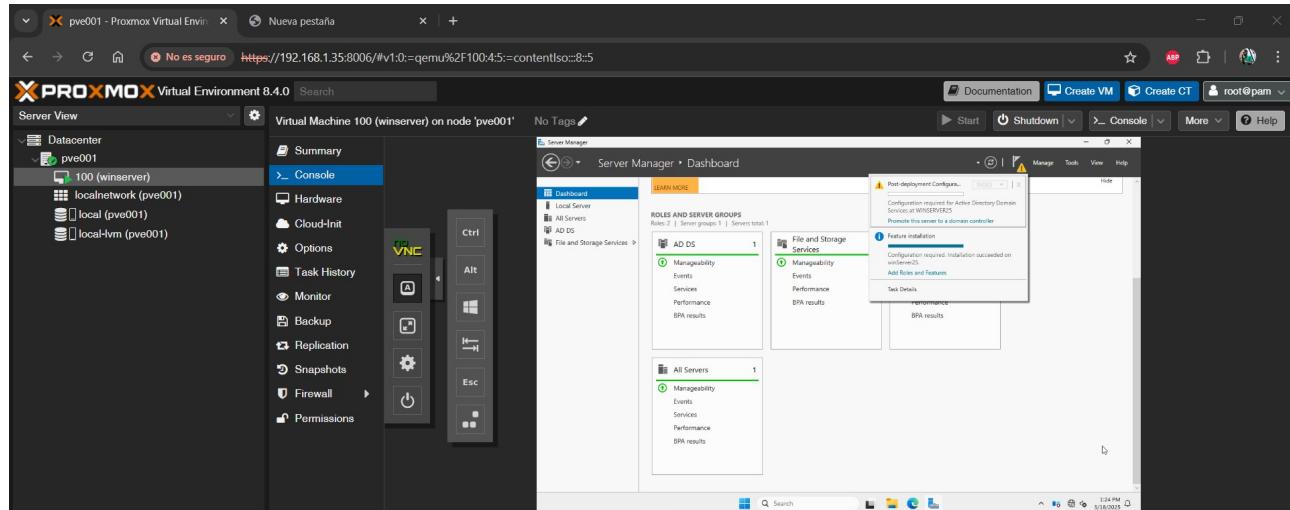


Y con esto ya estaría instalado AD DS.

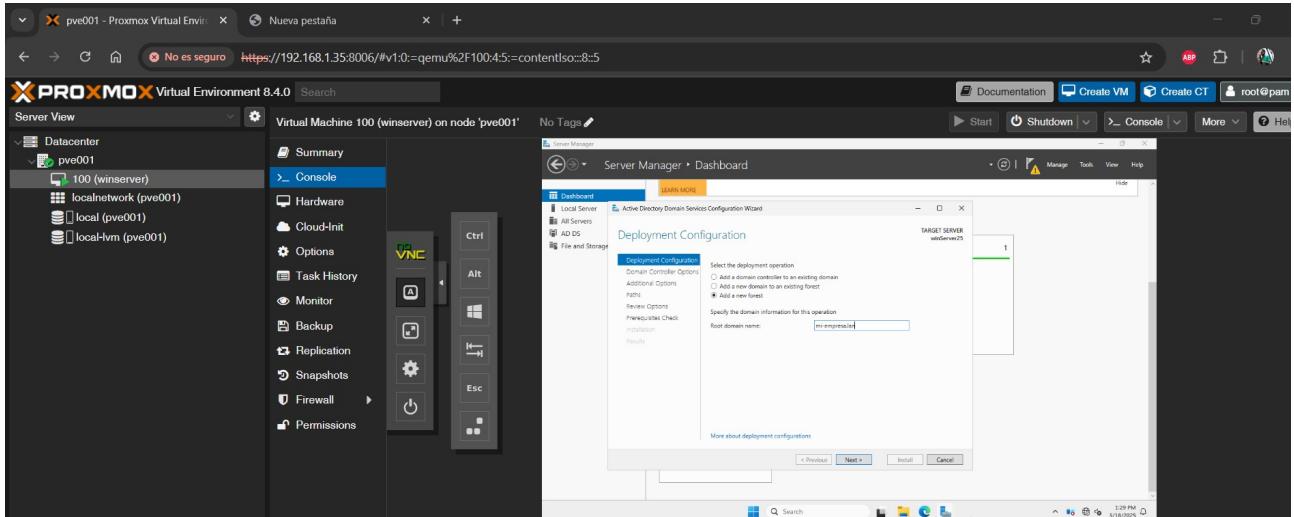


A5.2. Promoción del servidor a controlador de dominio y creación del bosque de dominio

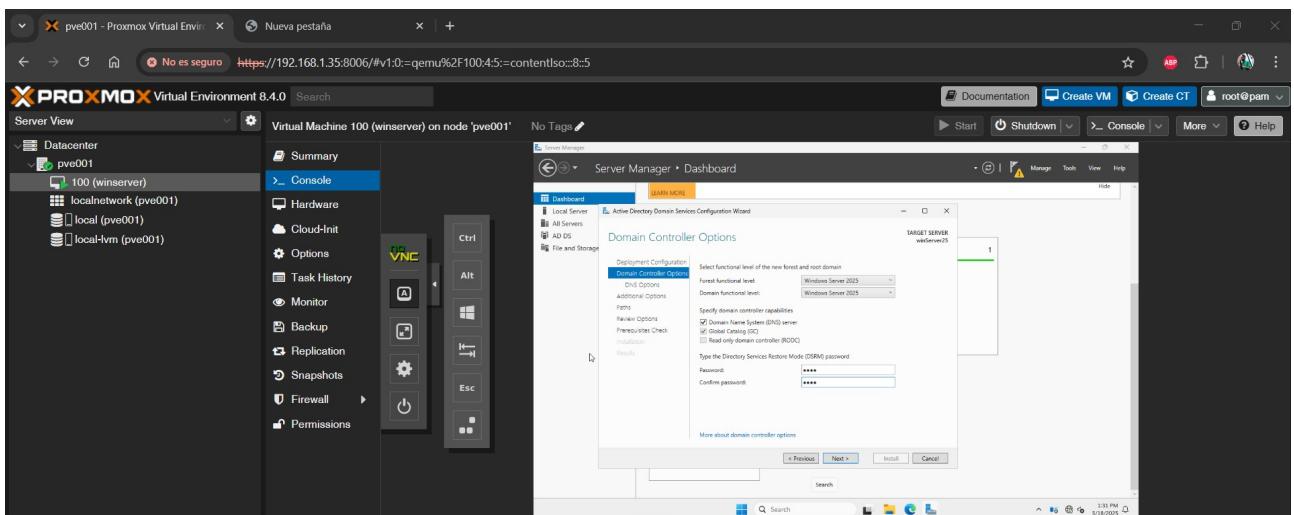
Ir al triángulo amarillo de las notificaciones y hacer clic en “*Promote this server to a Domain controller*” y seguir el asistente que se abre.



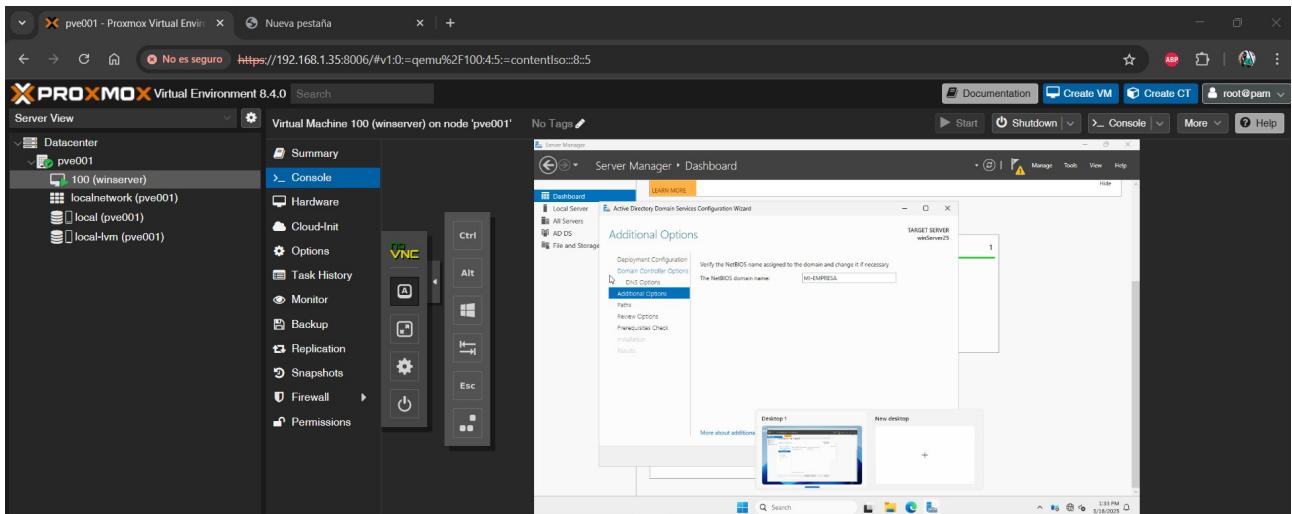
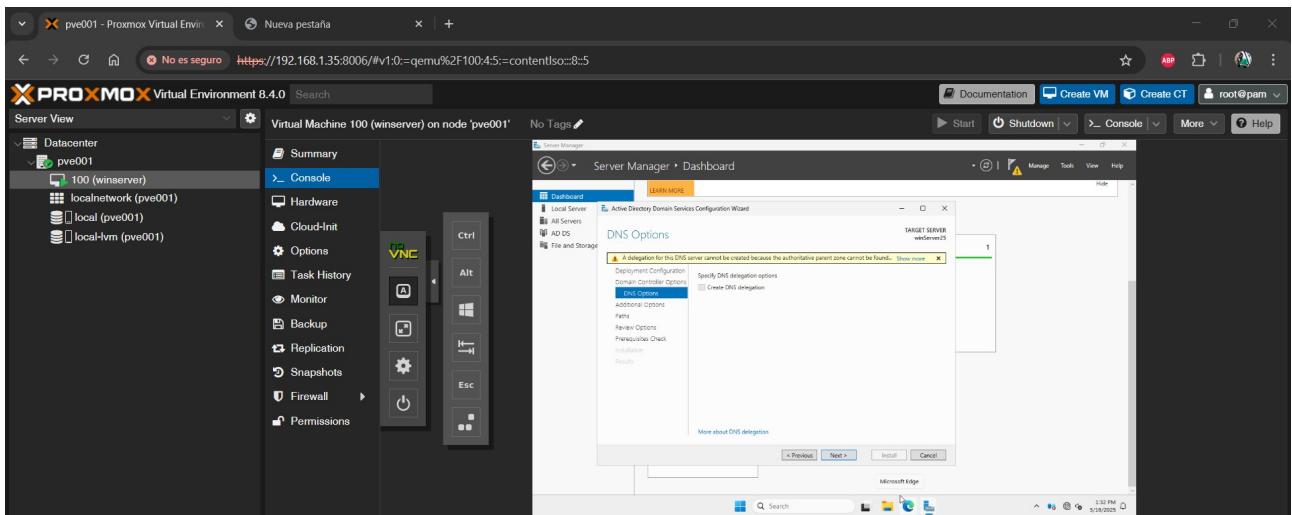
Añadir un nuevo bosque e introducir el nombre de dominio (**mi-empresa.lan**)

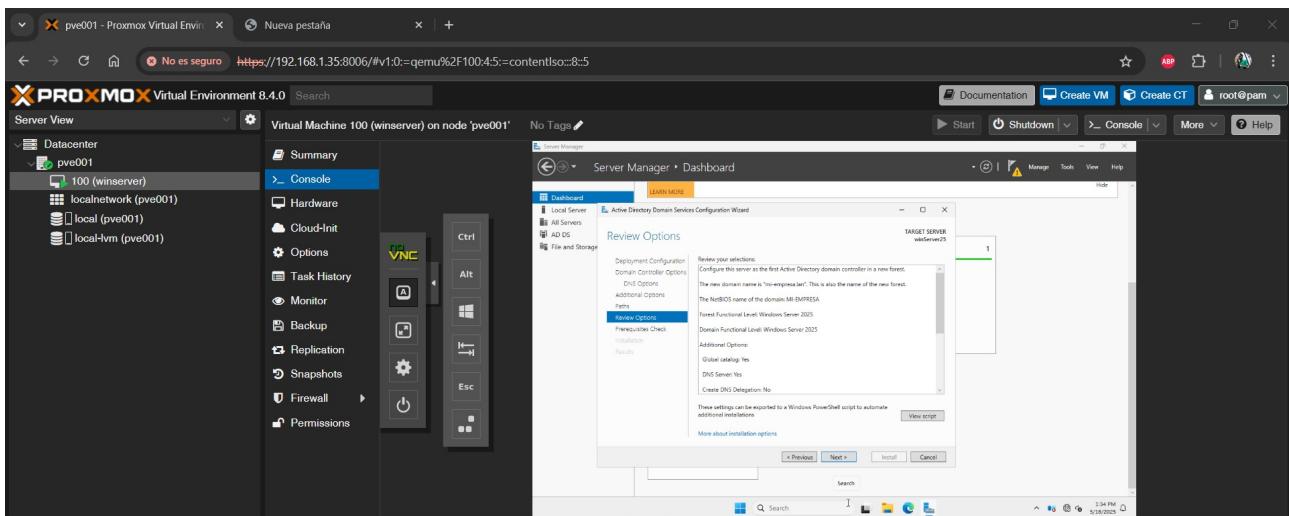
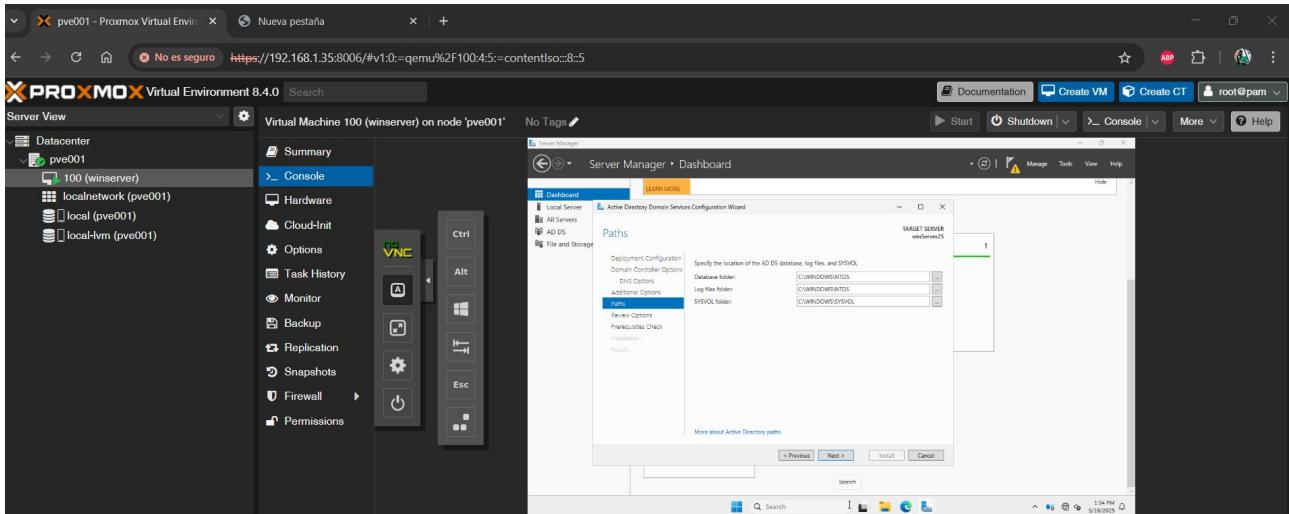


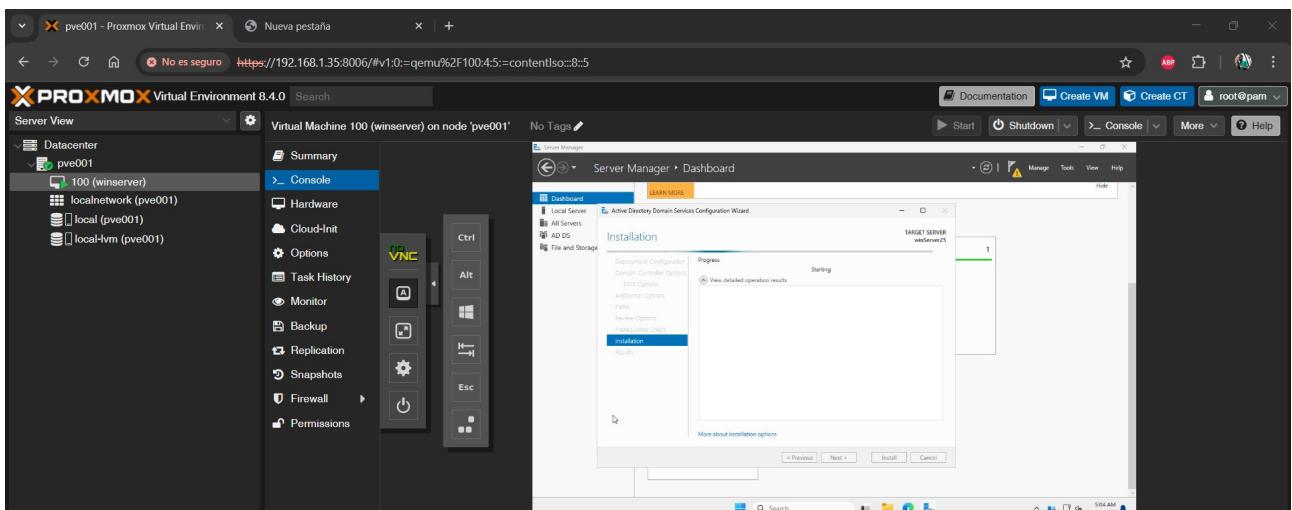
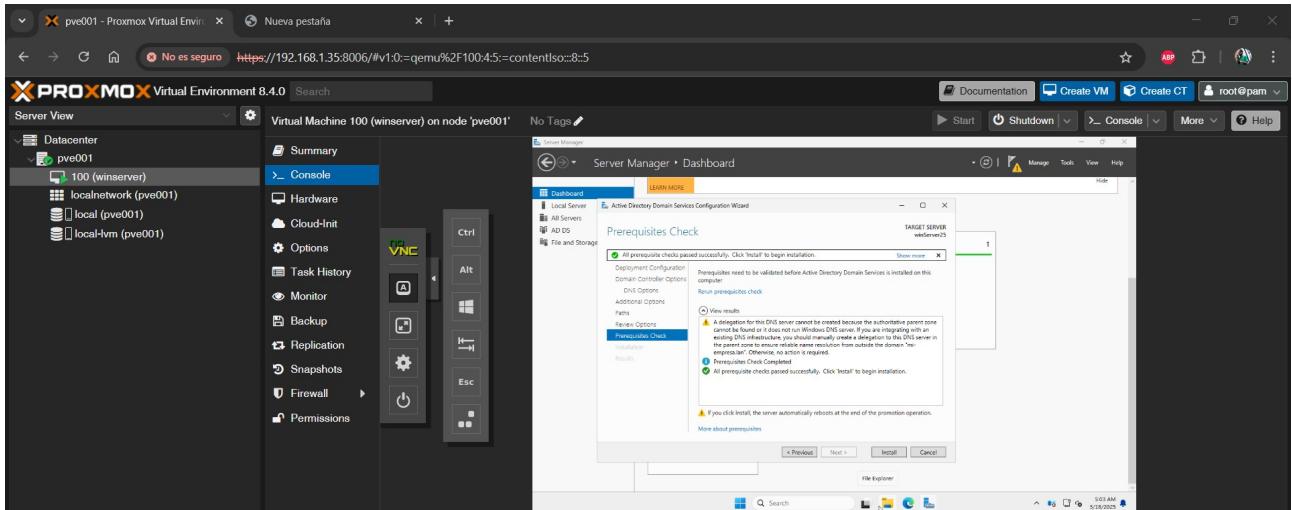
Introducir una contraseña válida



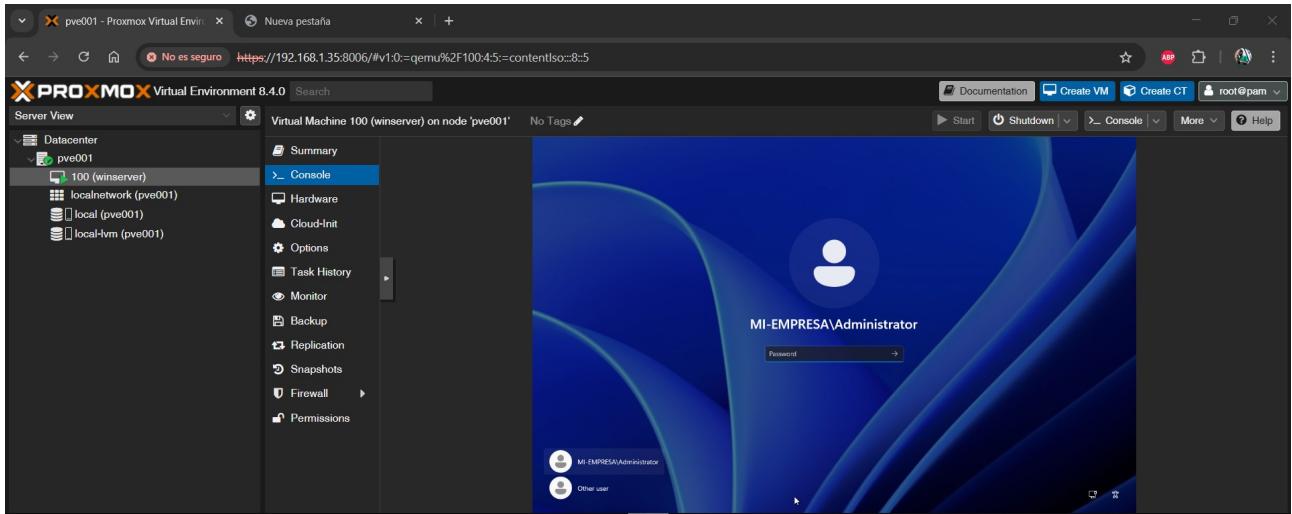
No crear zona dns y seguir hacia delante el asistente.



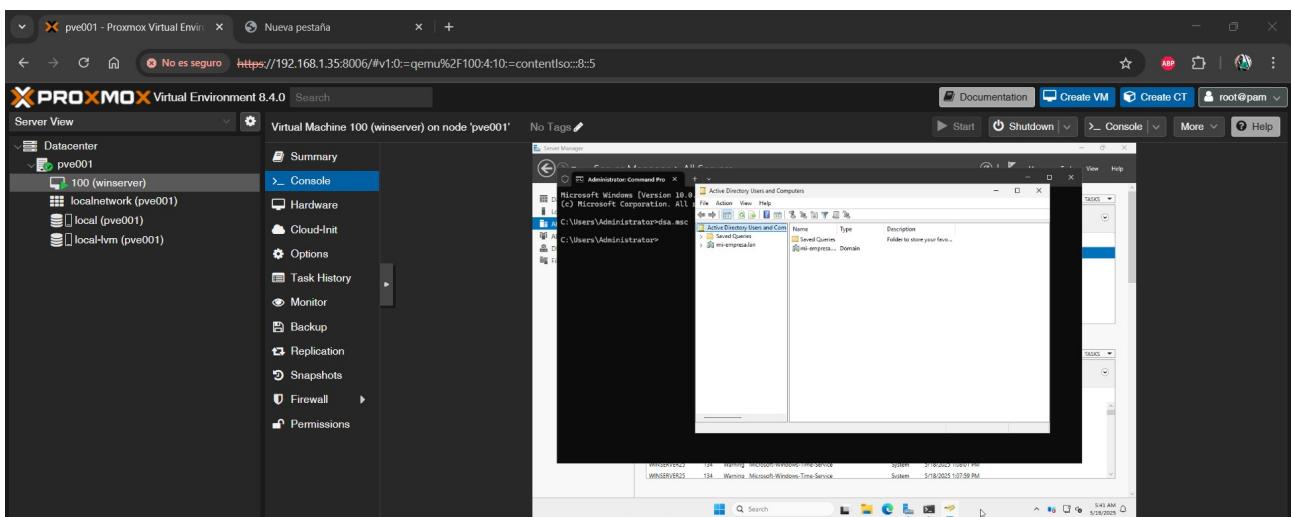




Después de instalar se reinicia y ya está activa la configuración realizada de AD DS y el dominio.



Como se puede comprobar el dominio está activo



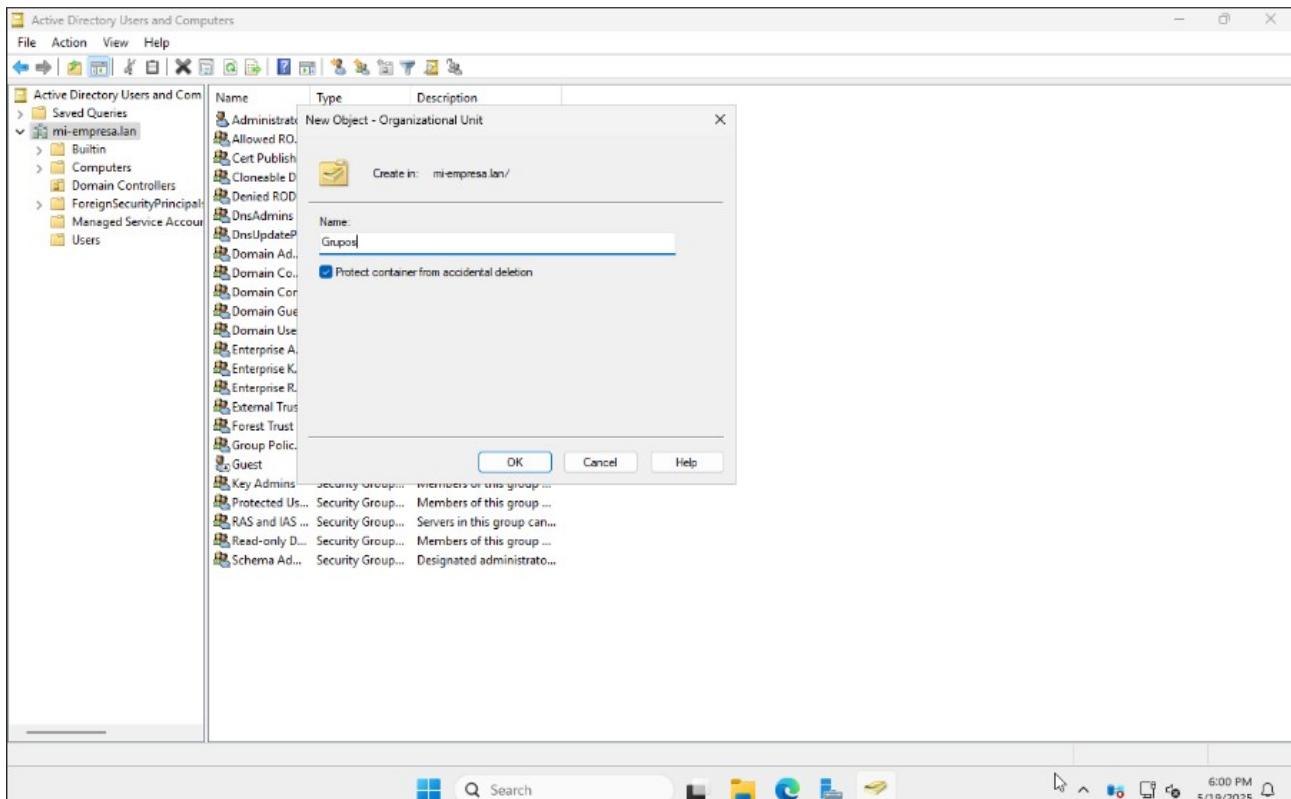
Anexo 6 - Creación de usuarios, grupos y Unidades Organizativas

Una vez instalado el rol AD DS y promovido el servidor a controlador de dominio (*mi-empresa.lan*), se procede a crear los usuarios y grupos de seguridad, así como a unir la estación cliente Windows 11 (VDI) al dominio.

En este proyecto se verificó el funcionamiento de los usuarios directamente desde la máquina cliente antes de crear la estructura de Unidades Organizativas, con la intención de mantener un enfoque progresivo y práctico de desarrollo.

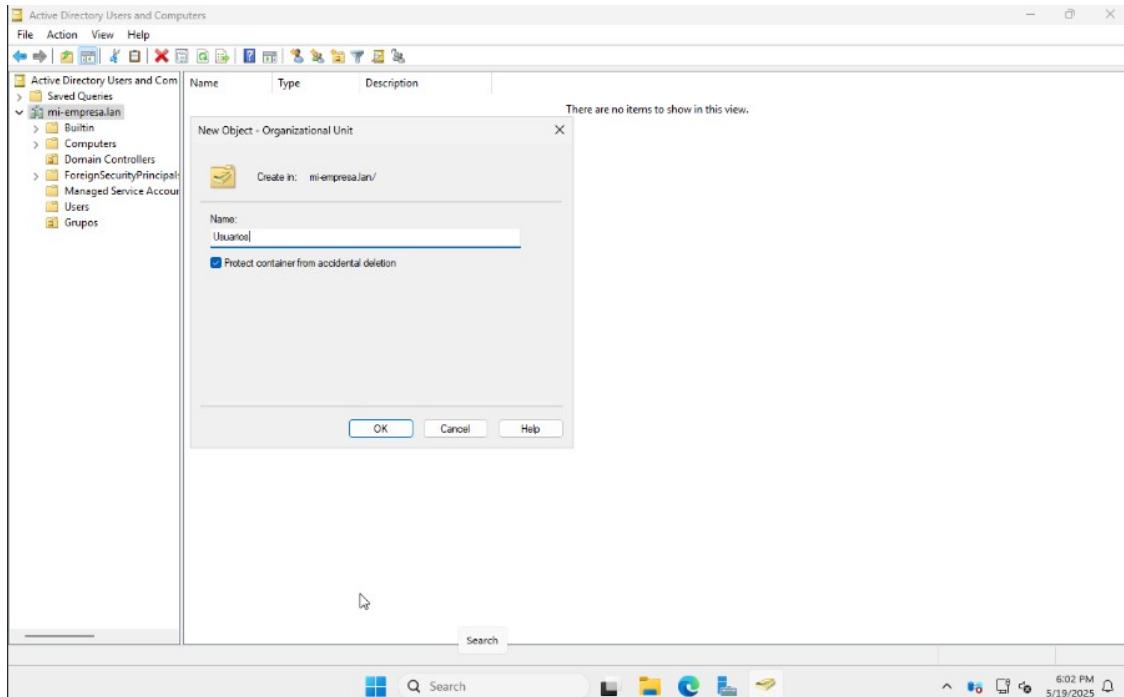
A6.1. Creación de Unidades Organizativas (UO)

Abrir un terminal cmd como administrador y abrir *Active Directory Users and Computers* ejecutando **dsa.msc**, hacer clic derecho en el dominio (*mi-empresa.lan*) > “**New Organization Unit**” y crear la Unidad Organizativa “**Grupos**”. Ésta se usará como contenedor para otras unidades organizativas (empleados y admins).



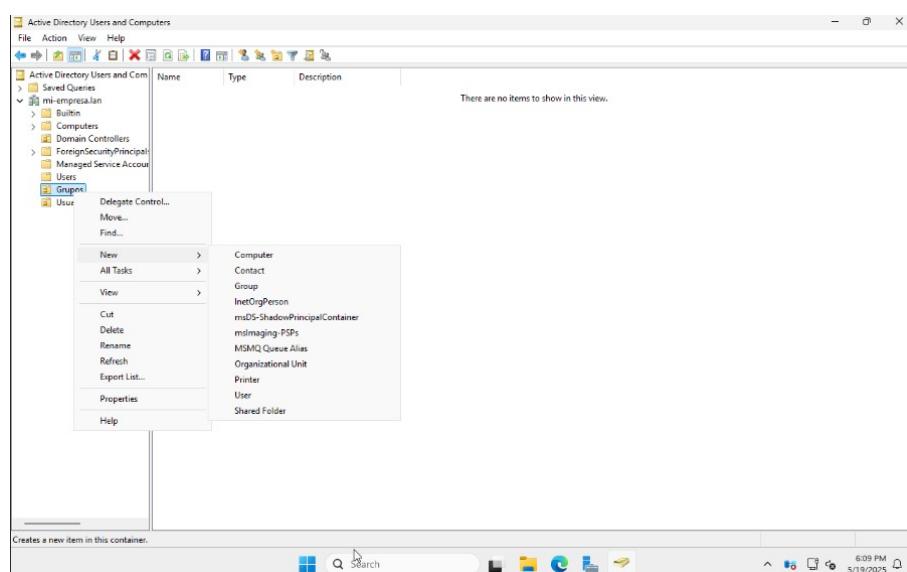
Crear de igual manera como hijo del dominio una Unidad Organizativa llamada **Usuarios** que contendrá los usuarios del dominio.

Una vez creadas las unidades organizativas para grupos y usuarios, dentro de grupos crear **dos**

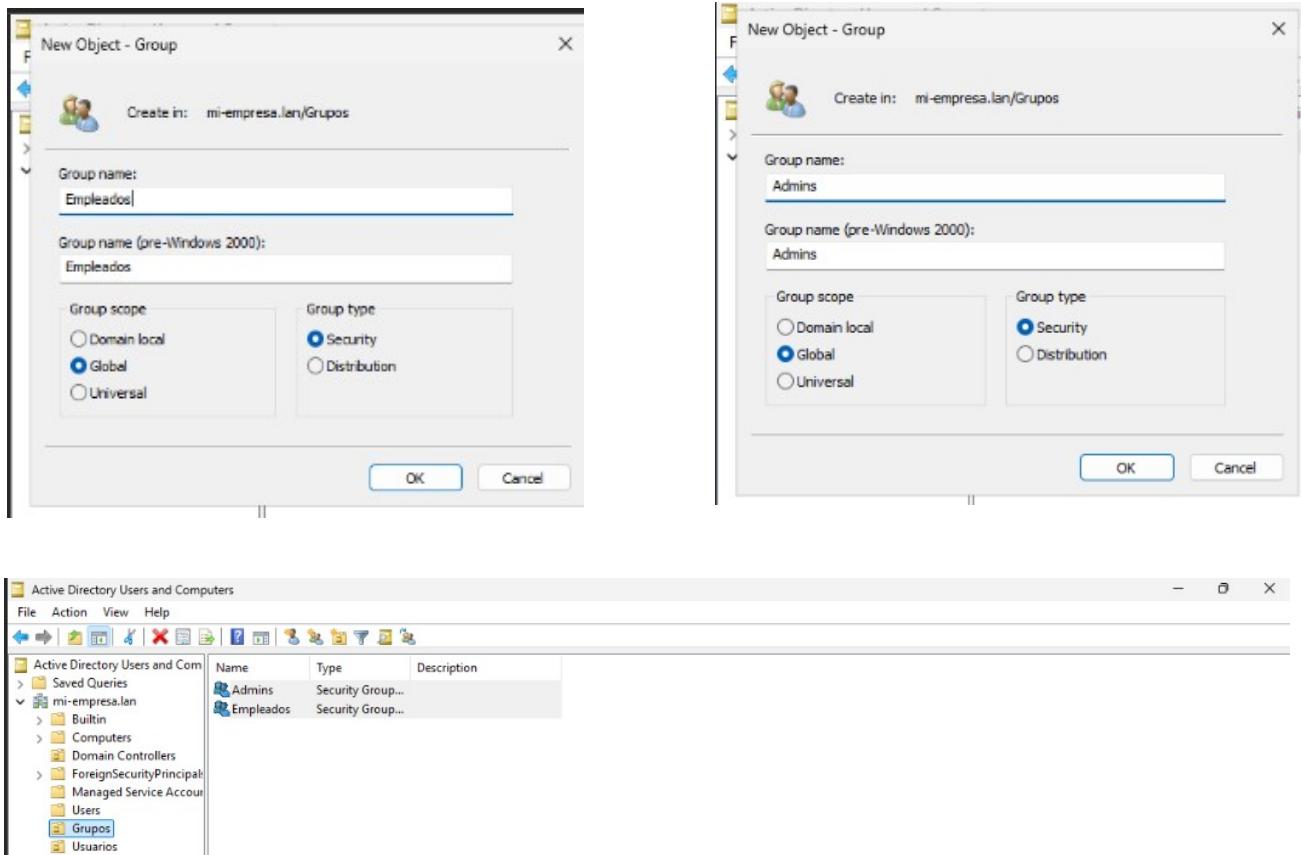


nuevos **grupos**. Uno para *empleados* (empleados genérico, que serán los usuarios que sólo tendrán acceso a la vdi configurada para ellos) y para *administradores del sistema (admins)*.

Para ello hacer clic derecho en la unidad organizativa creada anteriormente, **Grupos** > New > Group.



Crear de esta manera un grupo para todos los empleados (**Empleados**) y otro destinado para los administradores de sistemas (**Admins**) (al que posteriormente se le asignará también el acceso a todas las VDI).



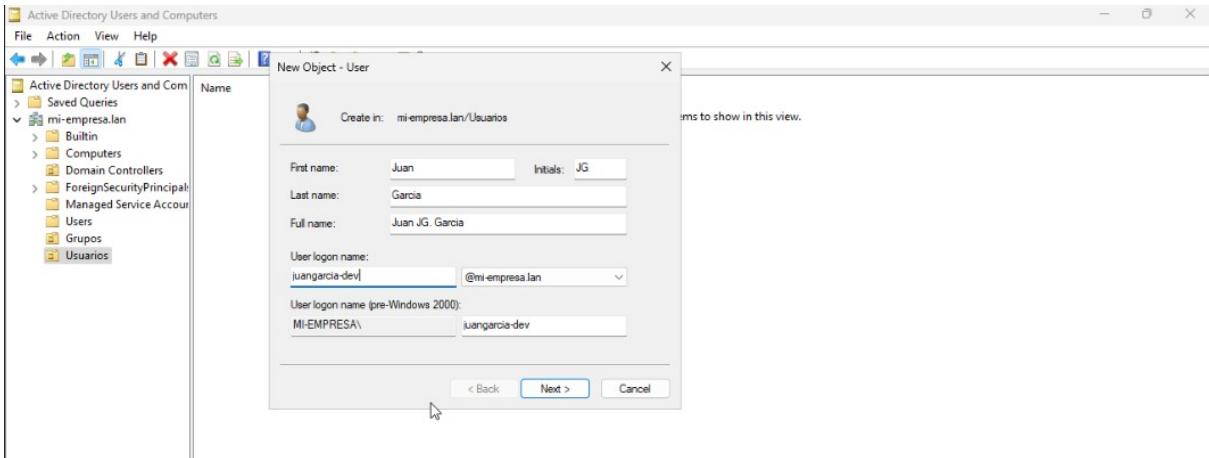
***Nota:** También habría que crear una unidad organizativa para los equipos del dominio (las vdi destinadas a escritorio remoto), pero ser realizará más adelante de la misma forma y se explicará cómo unir la VDI al dominio.*

A6.2. Creación de Usuarios

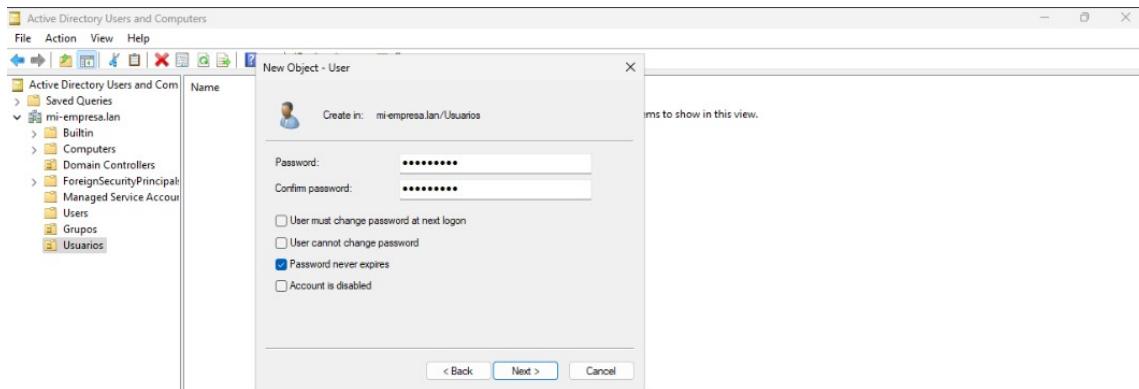
Para la simulación de este proyecto se crearon 3 usuarios, todos empleados. Uno será destinado a la máquina. Otro simula el resto de usuarios que no tendrán acceso. Y el tercero pertenecerá al grupo Admins que también tendrá acceso a la máquina.

Los usuarios se crearán en la unidad organizativa anteriormente creada **Usuarios**. Para ello hacer clic derecho en **Usuarios** > **New** > **User**

Introducir la información necesaria para el usuario y su login (**User logon name**)



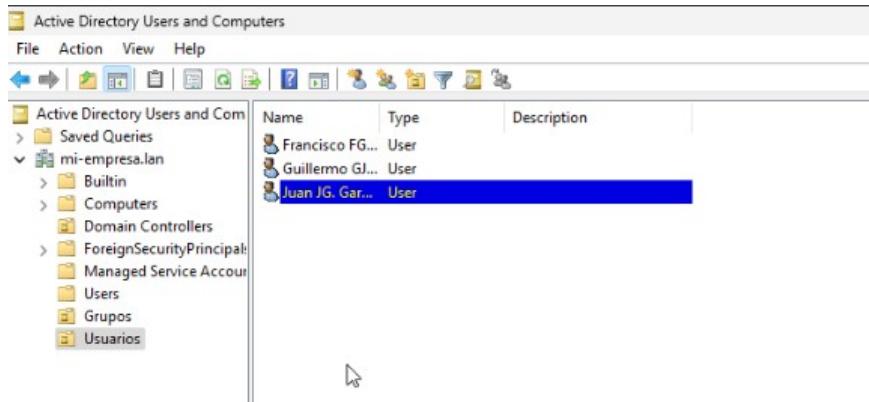
Configurar una contraseña y cuando queremos que expire la contraseña del usuario.



Y con esto ya estaría creado un usuario.

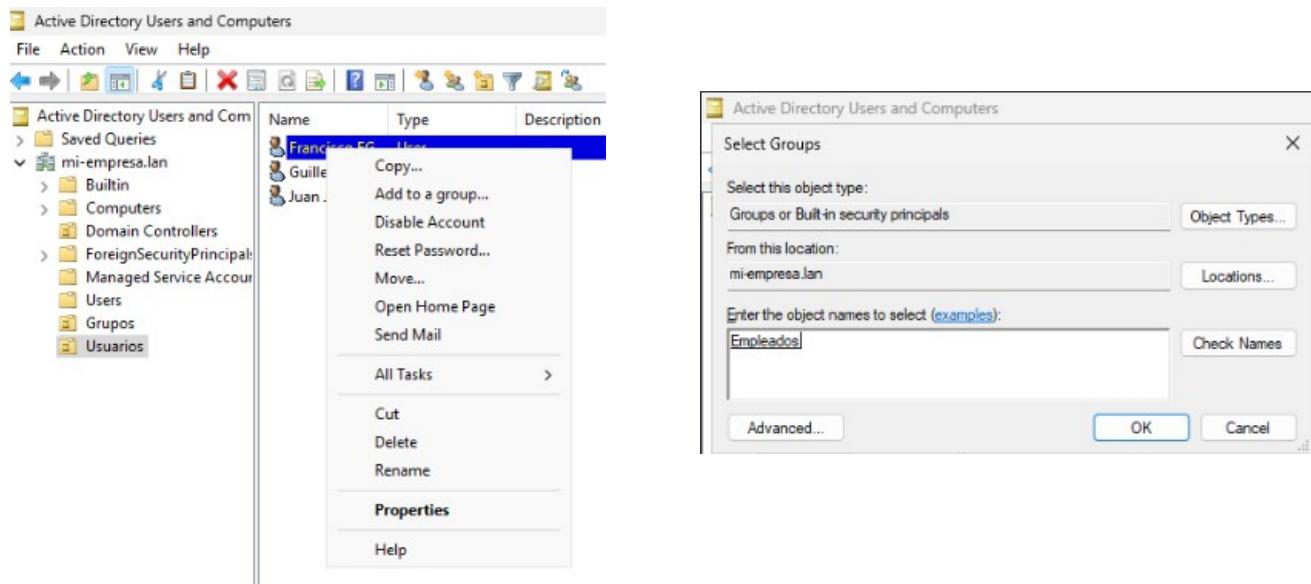
Nota: Para esta simulación he marcado la opción para que nunca expire la contraseña por facilidad, pero se recomienda la opción **User must change password at next login** por conservar la privacidad de los usuarios y que puedan elegir ellos la clave.

Ahora debemos realizar el mismo proceso para crear los dos usuarios restantes.

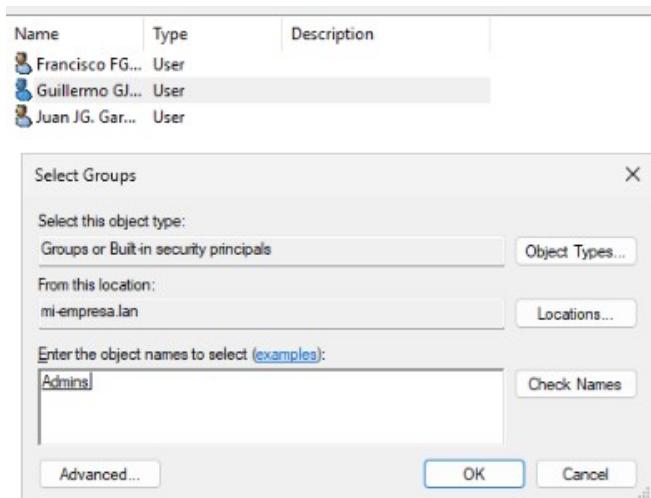


A6.3. Asignación de usuarios a grupos

Para añadir usuarios a un grupo, debemos entrar donde se encuentra el objeto usuario en cuestión, hacer click derecho sobre el usuario > add to a group, buscar el nombre del grupo (escribir y dar en “Check Names”).



Añadir igualmente al usuario Juan al grupo **Empleados**. Y a Guillermo, añadirlo al grupo Empleados y también al grupo de Admins para un futuro administrar los accesos de los usuarios administradores juntos).



Asignaciones realizadas:

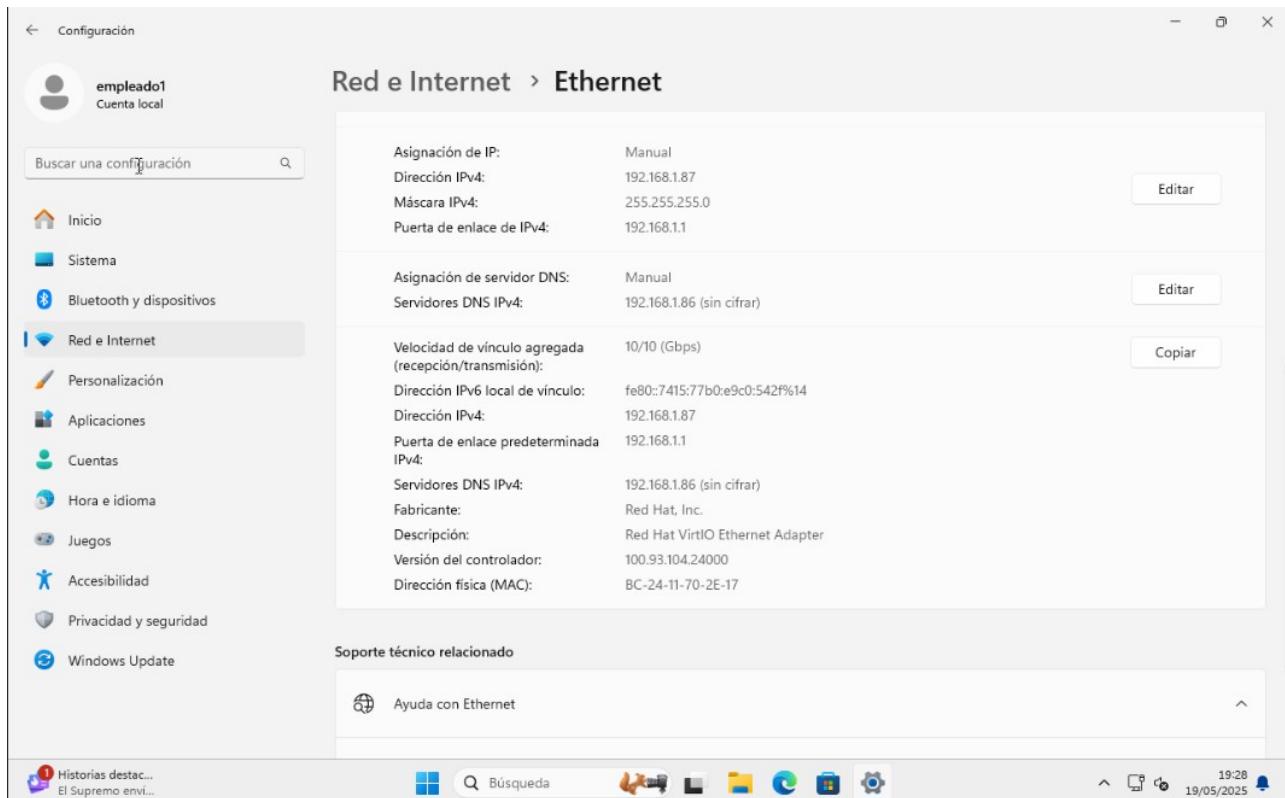
- Juan García → grupo Empleados
- Francisco Gutiérrez → grupo Empleados
- Guillermo De la Torre → grupo Empleados + Admins

Esta doble pertenencia permite aplicar permisos comunes a todos los usuarios, y privilegios especiales a administradores.

A6.4. Unión de la máquina Windows 11 al dominio

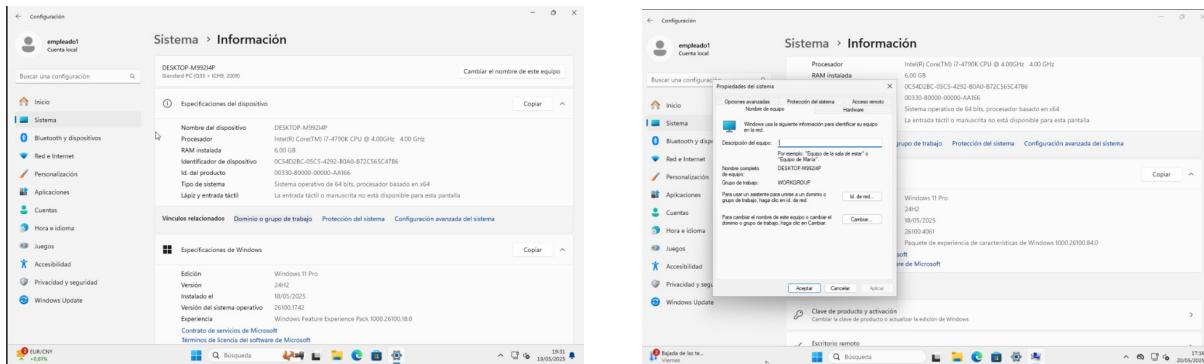
Antes de poder utilizar los usuarios creados, se procedió a unir la máquina cliente al dominio siguiendo estos pasos:

Asignar al cliente como DNS principal la dirección IP del servidor AD (en mi caso **192.168.1.87**)

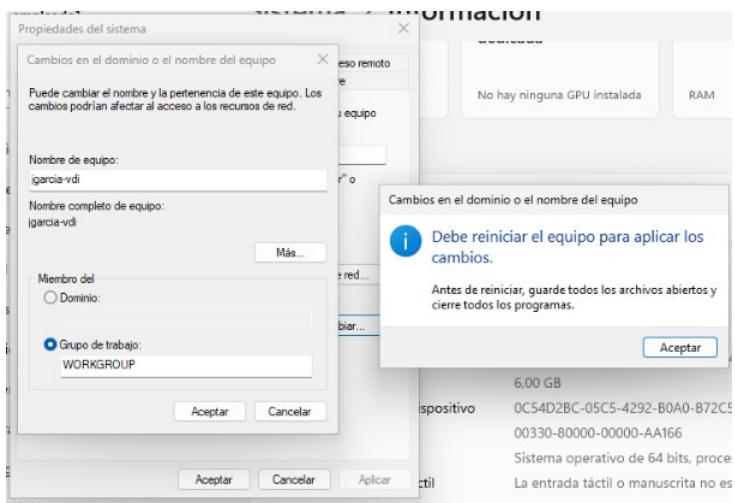


Una vez unido el equipo al dominio, se procede a asignarle un nombre identificativo y coherente con la infraestructura, para facilitar su gestión desde Active Directory.

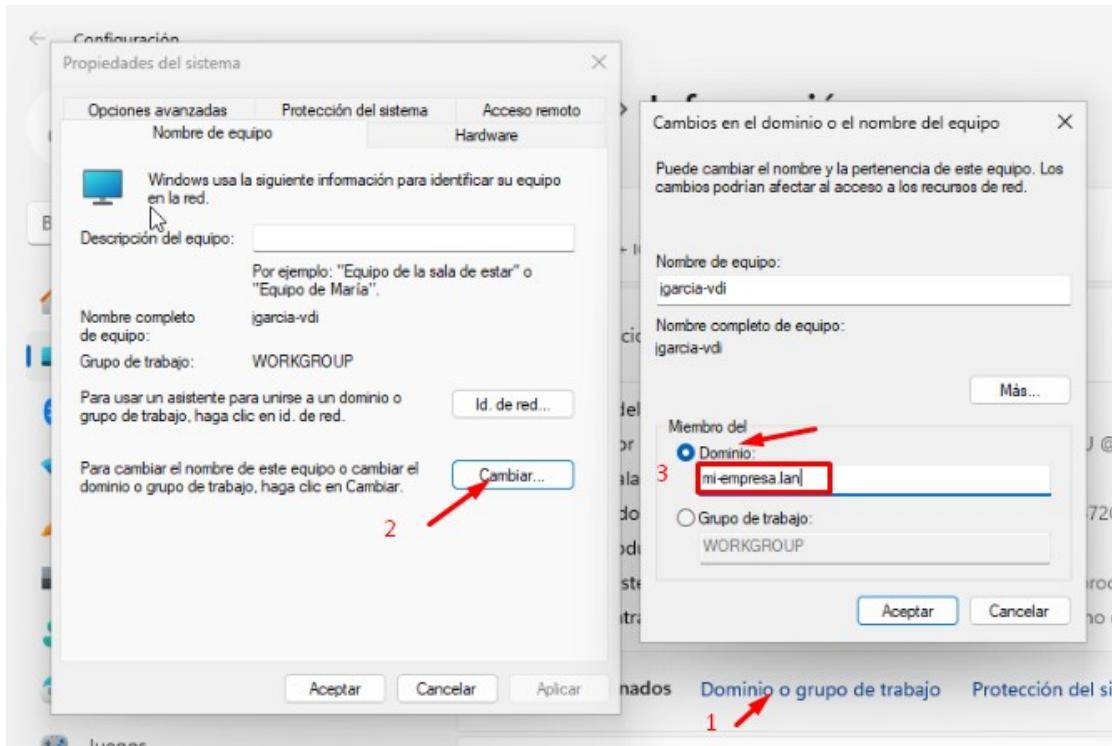
Para ello, se accede a: **Configuración > Sistema > Información del sistema** y se selecciona la opción “**Dominio o grupo de trabajo**”, lo que permite modificar el nombre del host antes de reiniciar si es necesario.



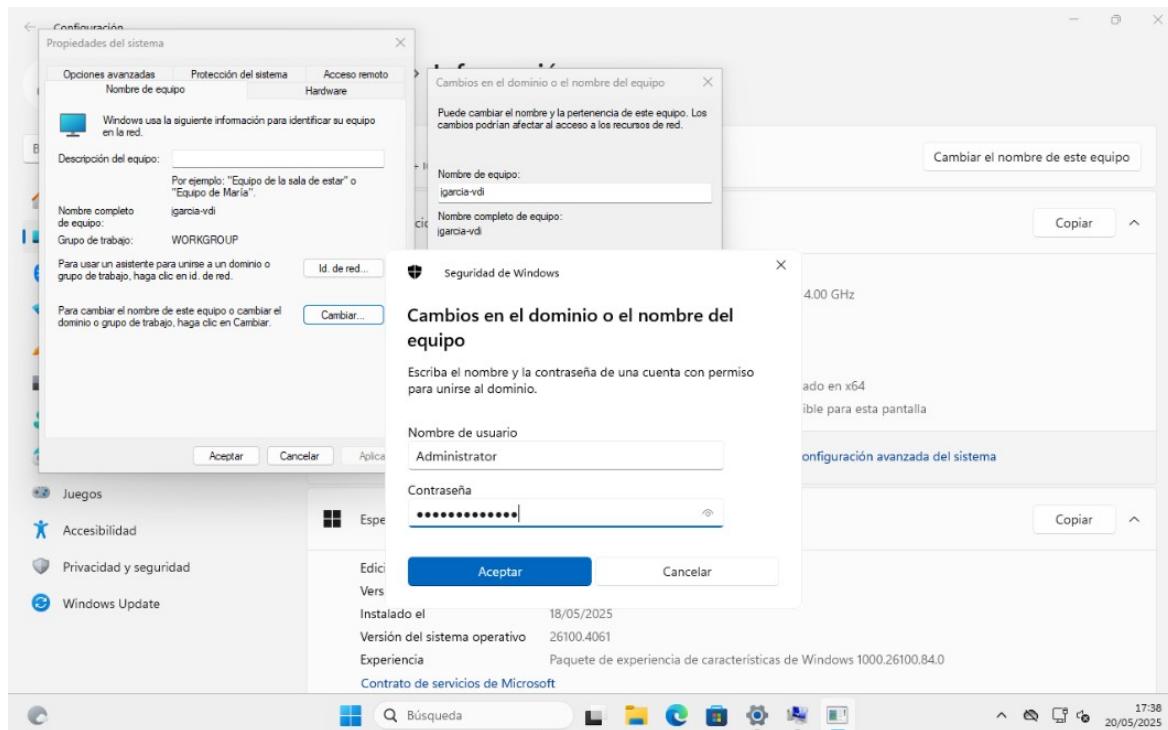
Hacer clic en "Cambiar" y asignarle el nuevo nombre, por ejemplo, vdi-juangarcia, y reiniciar para que aplique los cambios.



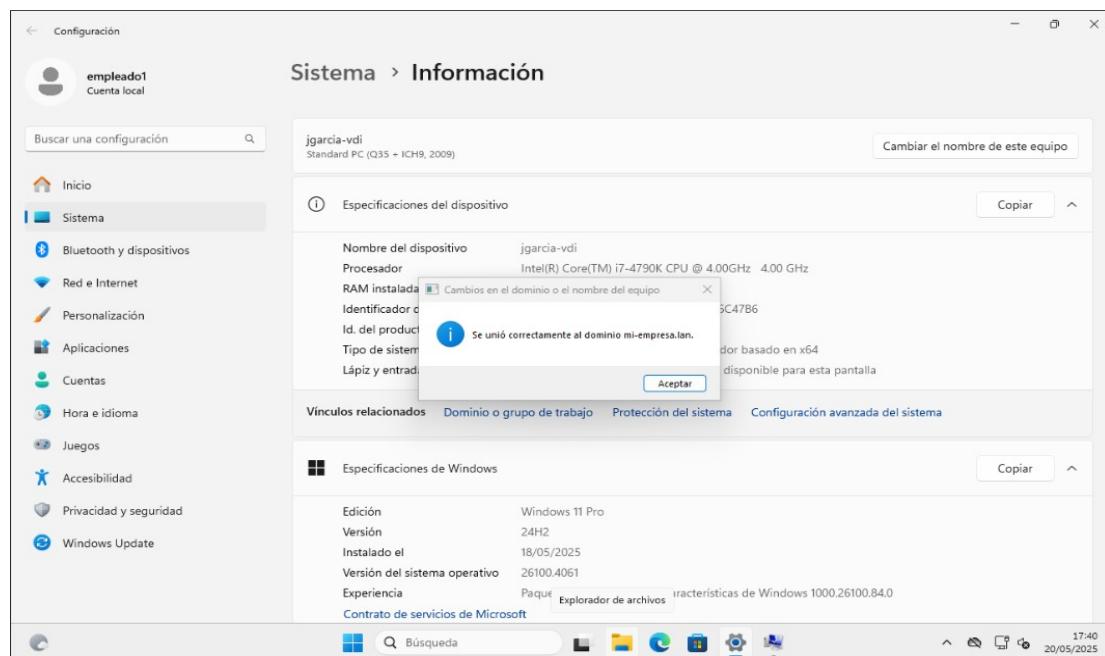
Cuando reinicie, acceder de nuevo a “Dominio o grupo de trabajo” y para proceder a unir el equipo al dominio.



Aparece una ventana emergente pidiendo credenciales donde hay que poner un usuario válido del dominio (por ejemplo, el usuario **Administrator** que se creó al instalar Windows Server)

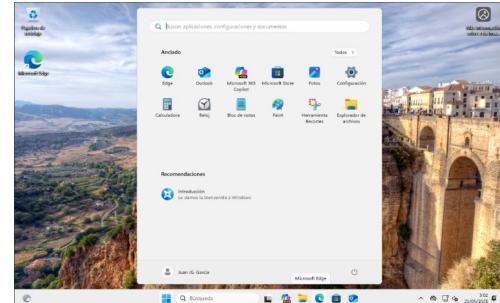
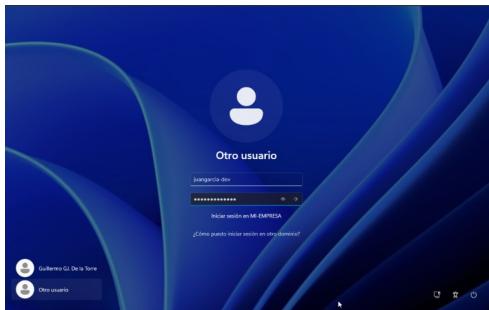


Aparece un mensaje de que se unió al dominio correctamente y posteriormente pide reiniciar el equipo para aplicar cambios al igual que antes.

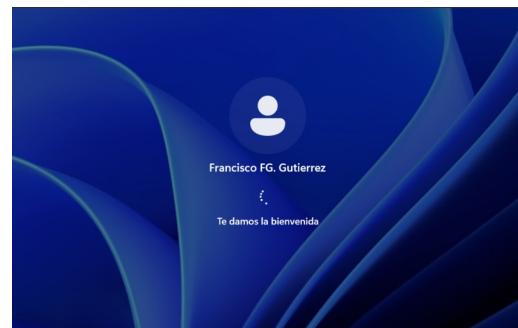
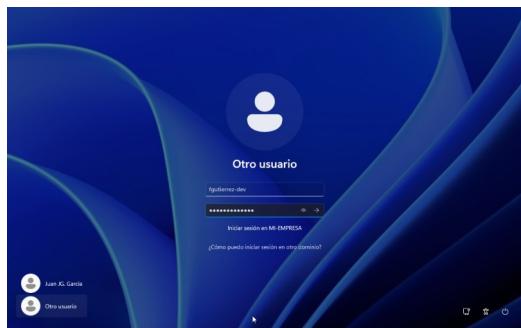


Si todo se ha configurado correctamente, al reiniciar la MV, en la pantalla para iniciar sesión podemos dar en la opción **Otro usuario** y acceder con un usuario del dominio.

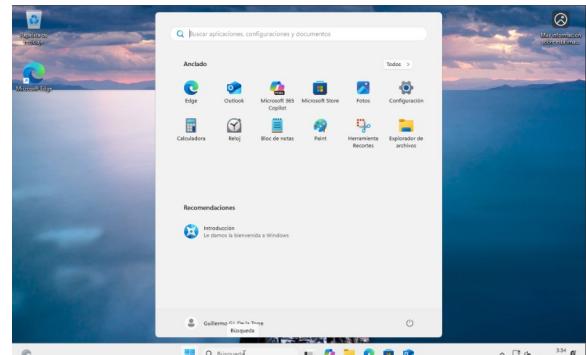
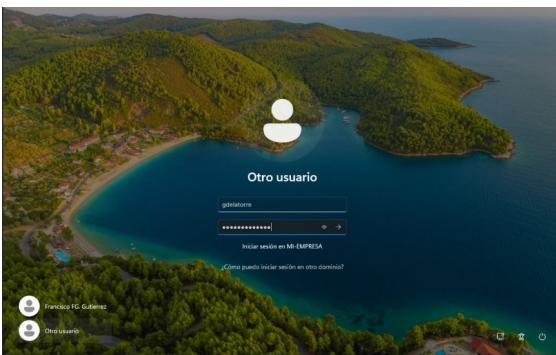
Usuario Juan García



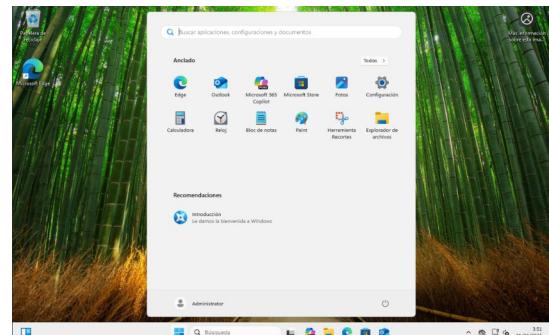
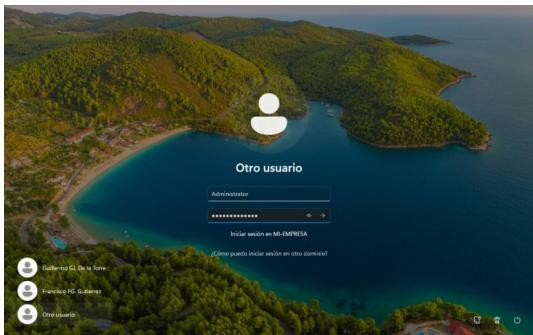
Usuario Francisco Gutiérrez



Usuario Guillermo De la Torre



Usuario Administrator.



Anexo 7 – Configuración y validación del acceso remoto mediante Escritorio Remoto RDP

Este anexo documenta la configuración y validación del acceso remoto a través de Escritorio Remoto (RDP) en las máquinas cliente del dominio.

Se detallan los pasos realizados para estructurar correctamente las Unidades Organizativas (UO), aplicar las Directivas de Grupo (GPO) que permiten el acceso remoto solo a usuarios y grupos autorizados, y validar ese acceso mediante pruebas reales.

A7.1. Organización de equipos en Unidades Organizativas

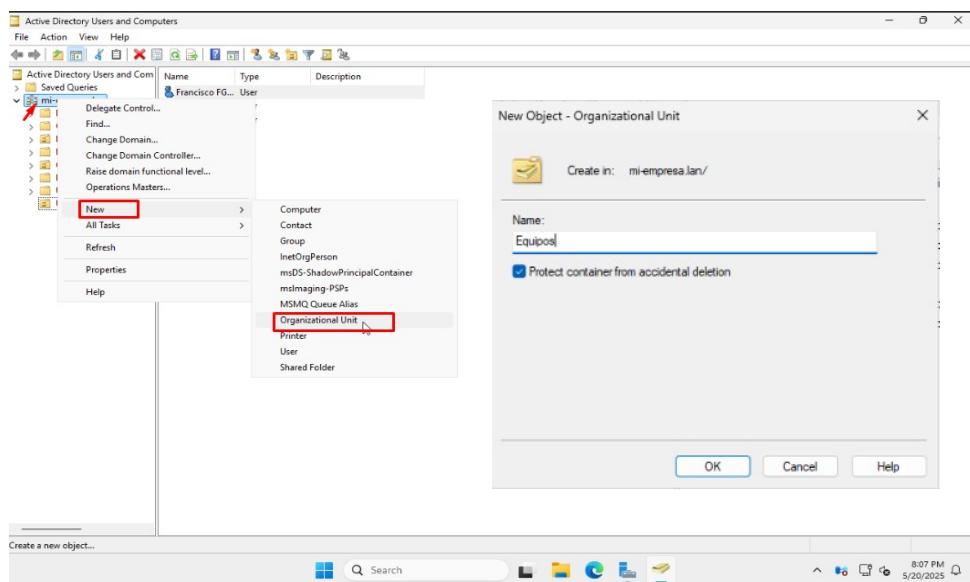
Para facilitar la administración de políticas específicas por máquina, se organizó la infraestructura de equipos dentro de Unidades Organizativas (UO) en Active Directory.

En este caso, se creó una UO exclusiva para las VDIs, permitiendo aplicar directivas diferenciadas respecto a otros dispositivos del dominio.

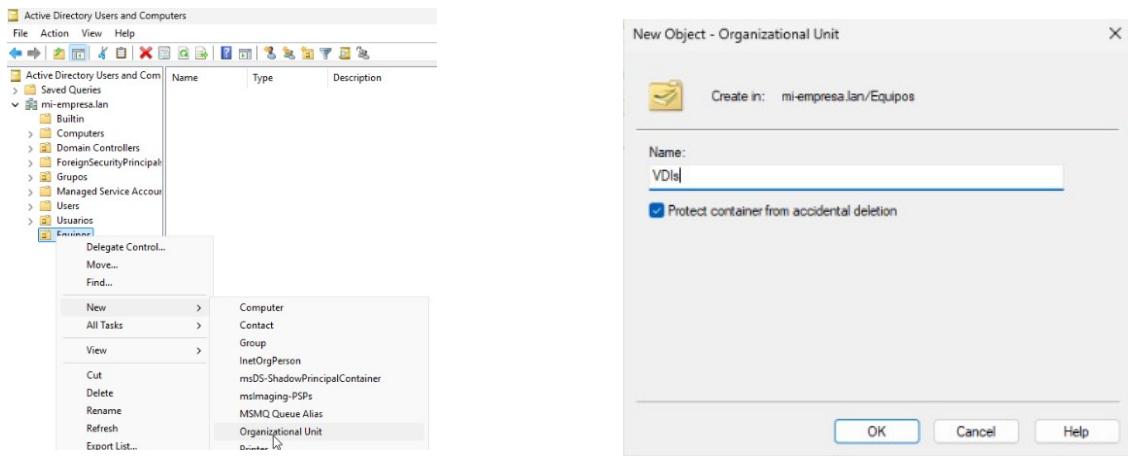
A7.1.1. Creación de UO para el equipo VDI en cuestión

Para simular algo más una estructura empresarial, se ha creado otra UO destinada a contener todos los equipos del dominio llamada **Equipos** la cual contendrá todos los equipos del dominio, entre ellos la UO contenedora **VDIs**

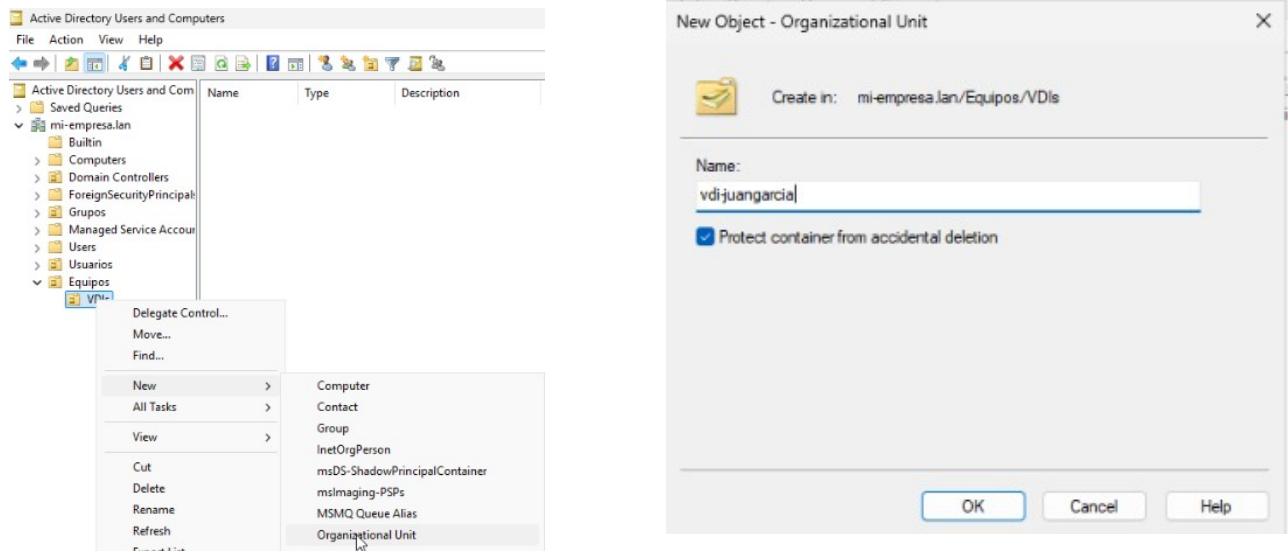
Comenzamos creando la UO **Equipos**. Para ello, abrir un cmd y ejecutar **dsa.msc** (“*Usuarios y equipos de Active Directory*”), clic derecho sobre el dominio > Nueva Unidad Organizativa y configuramos su nombre.



Ahora para crear la UO **VDIs**, repetir la acción anterior, pero en lugar de hacer clic derecho en el dominio, hacemos clic derecho en la UO **Equipos**.



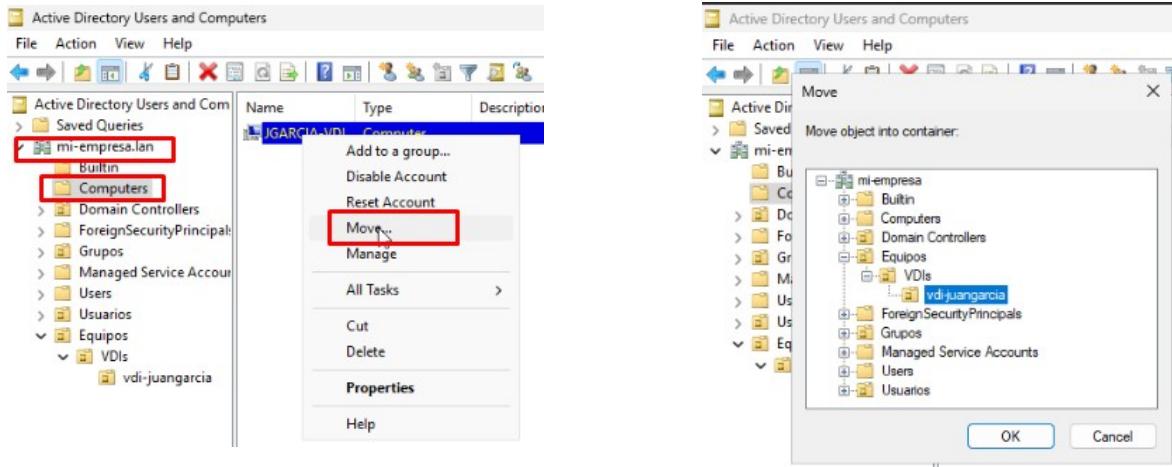
Es dentro de esta unidad **VDIs** donde se deben crear las UOs para todos las máquinas virtuales destinadas a equipos remotos de cada usuario. En este caso la máquina destinada al usuario *Juan García*. El procedimiento para crear las UOs es análogo a los anteriores.



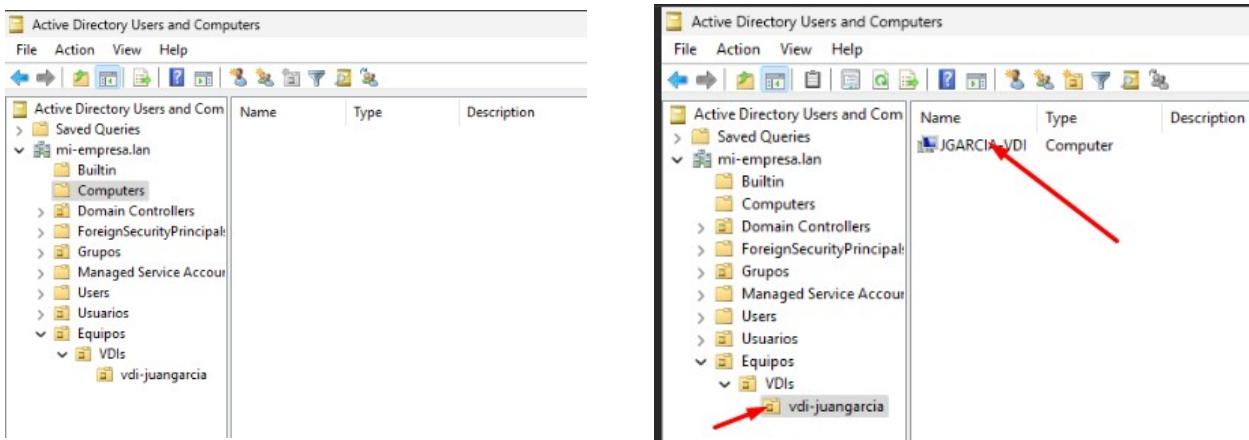
A7.1.2. Añadir un el equipo VDI a su UO

Ahora nos vamos a la unidad por defecto donde se añaden los equipos y vemos que nos aparece la VDI en cuestión.

Para añadirla a una UO específica hacer clic derecho en el equipo > “Mover...”. Esto abrirá una ventana donde debemos seleccionar la UO que creamos anteriormente destinada a este equipo en cuestión, la seleccionamos y damos a “OK”.



Al realizar esto, el equipo desaparece de la UO por defecto **Computers**, y al navegar por el dominio vemos que se a añadido a su UO correspondiente.

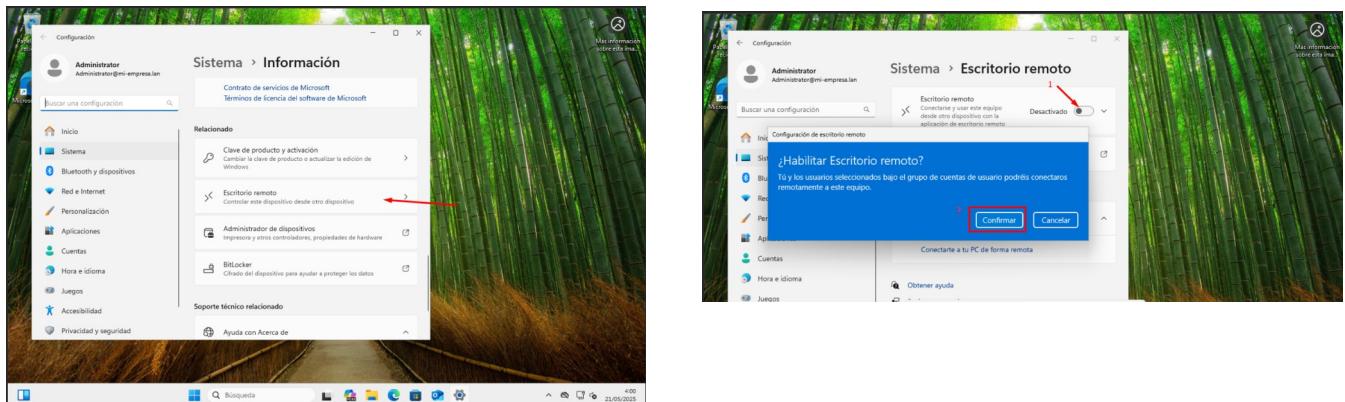


A7.2. Configuración del acceso a Escritorio Remoto en la VDI

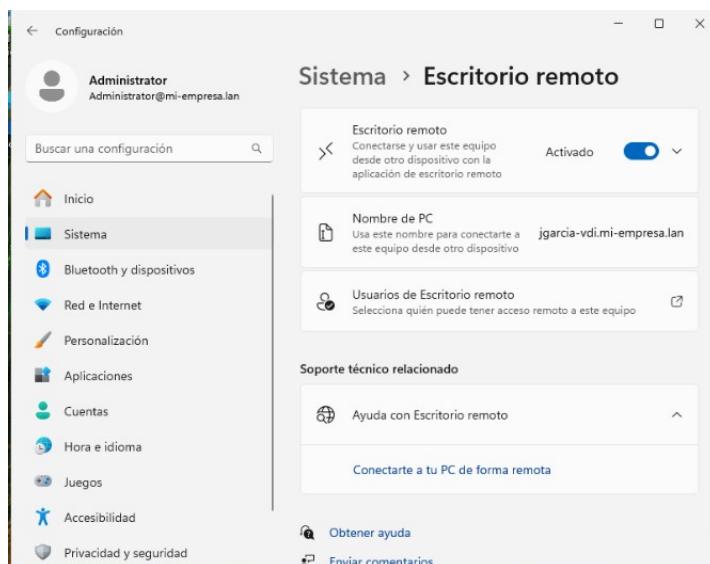
A7.2.1. Habilitar el Escritorio Remoto

Para permitir conexiones remotas a la máquina vdi-juangarcia, se debe activar manualmente la función de Escritorio Remoto.

Acceder a: Configuración > Sistema > Escritorio remoto y Activar la opción “Escritorio remoto” moviendo el interruptor a "Activado".



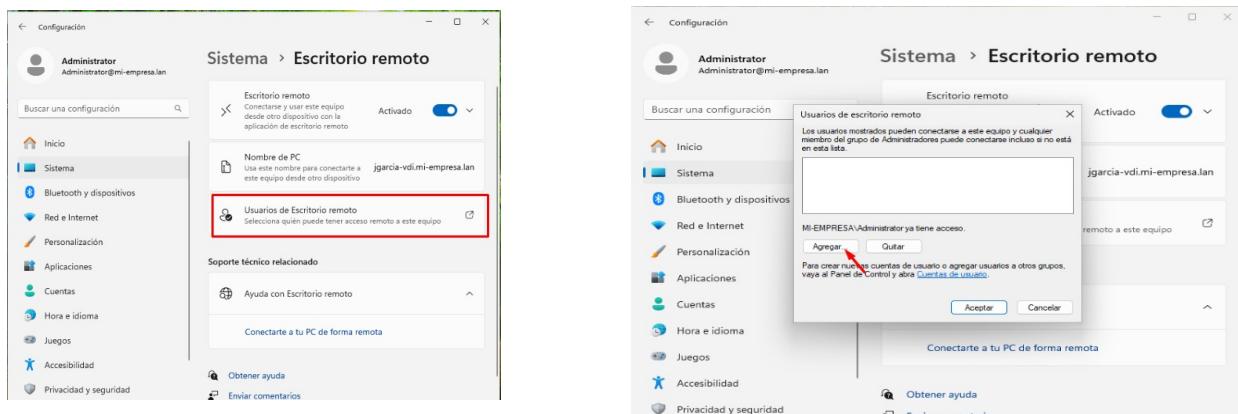
Al confirmar los cambios, en la parte inferior de la sección aparecerá el nombre completo del equipo, incluyendo el dominio al que pertenece (por ejemplo, vdi-juangarcia.mi-empresa.lan).



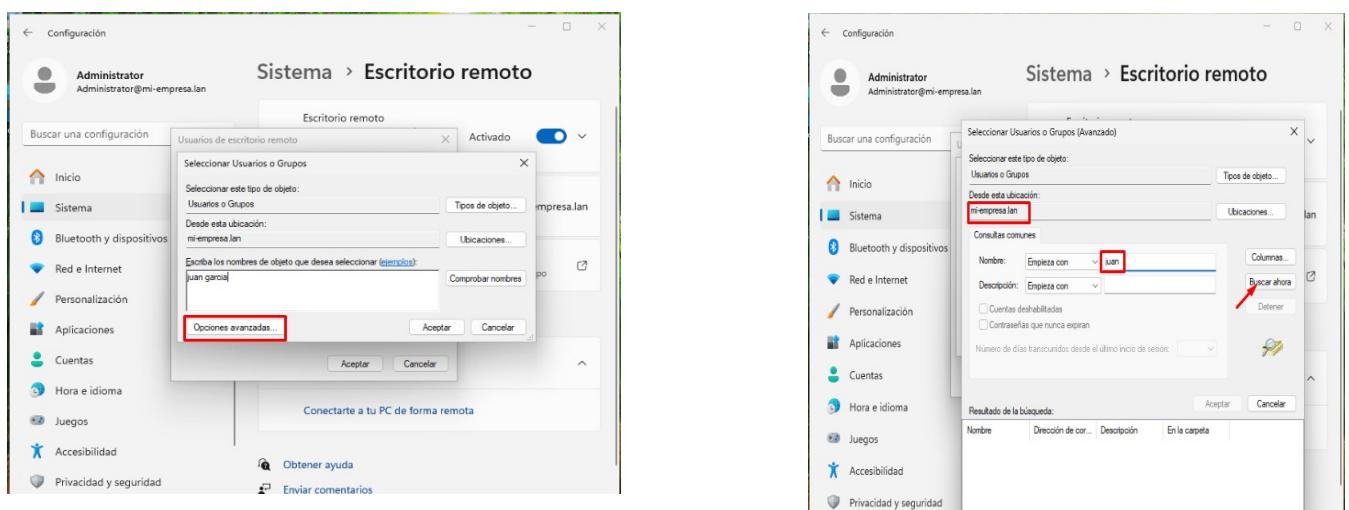
A7.2.2. Configuración de usuario autorizado

Una vez activado el servicio, es necesario definir qué usuarios o grupos del dominio tienen permiso para conectarse mediante RDP.

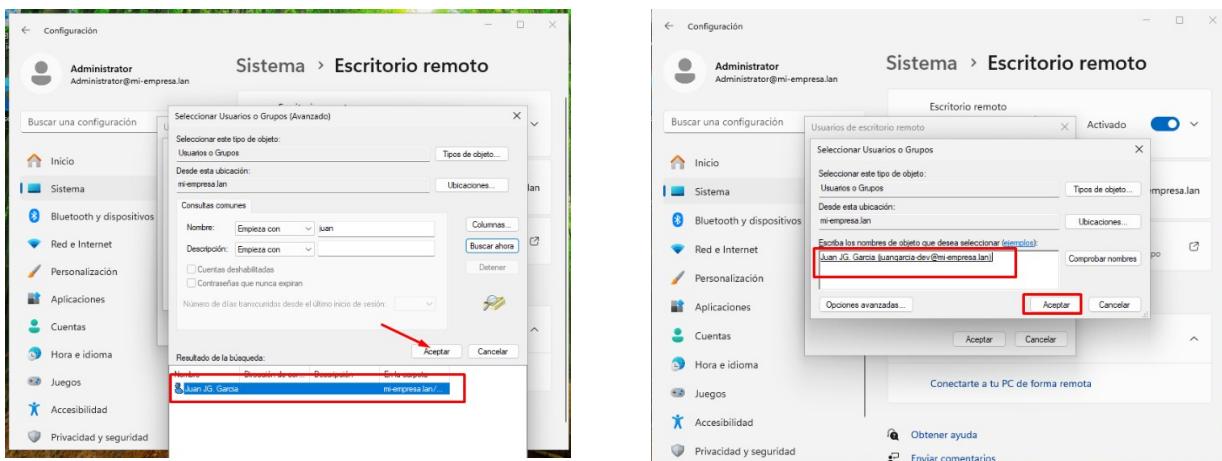
Dentro de la misma ventana, hacer clic en: “**Usuarios de Escritorio remoto**” > “**Agregar**” en la nueva ventana emergente.



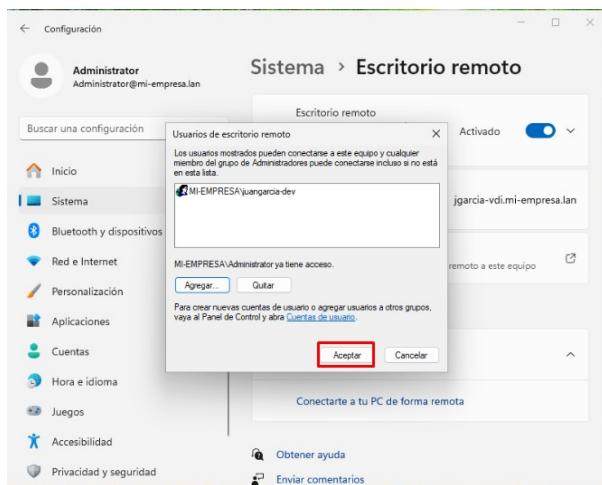
Se abre donde debemos pulsar en: “**Opciones avanzadas**” Confirmar que en “Ubicación” aparece seleccionado el dominio (en este caso, mi-empresa.lan), y realizar la búsqueda del usuario



Seleccionar el usuario deseado (por ejemplo, juan garcia) de la lista y pulsar: “Aceptar”



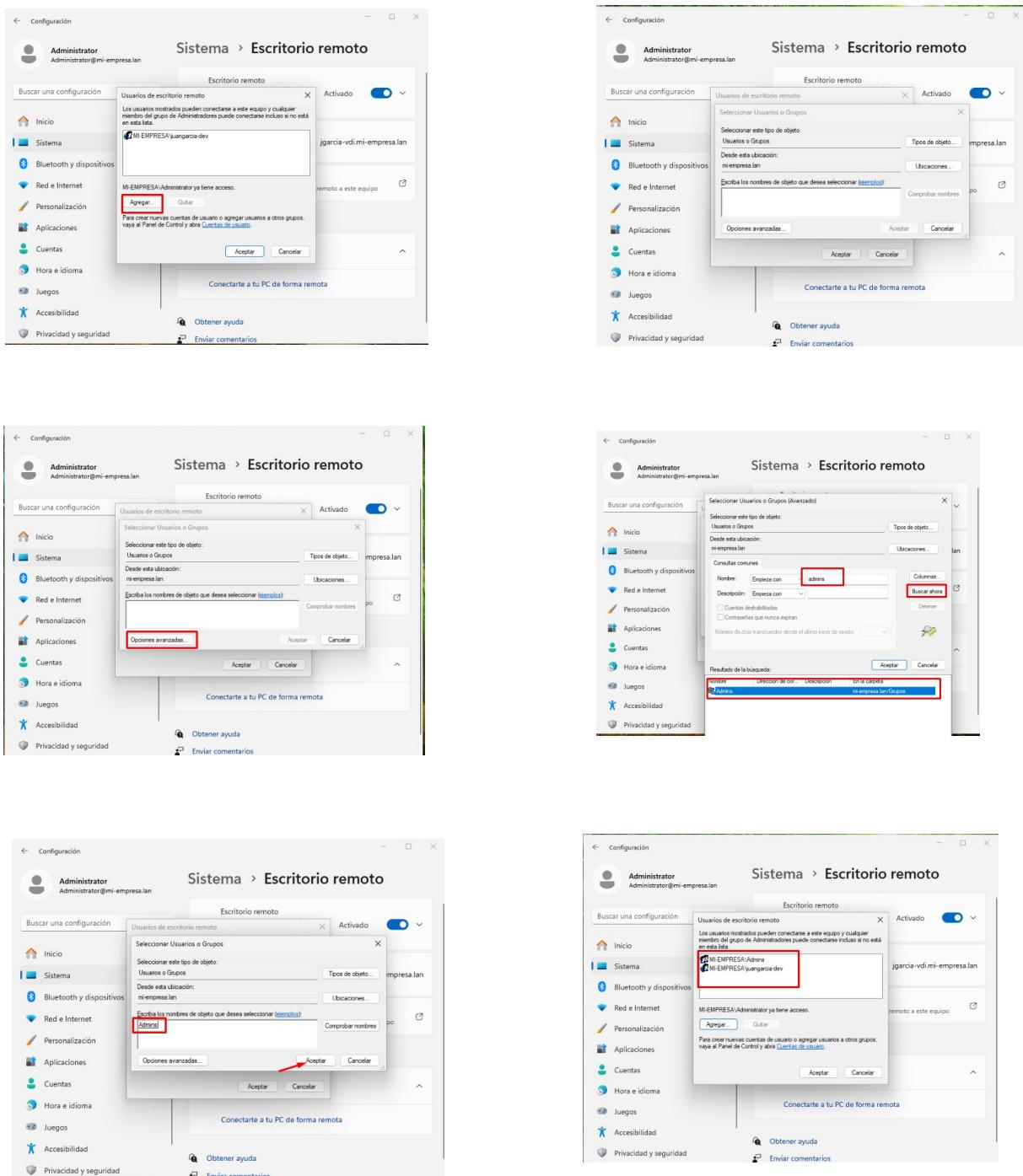
Con esto, Juan García queda autorizado para conectarse remotamente a la VDI mediante RDP.



A7.2.3. Añadir el grupo *Admins* como usuarios permitidos por RDP

Se permite exactamente el mismo procedimiento anterior, esta vez para añadir el grupo de seguridad ***Admins***

- 1- Volver a: “**Usuarios de Escritorio remoto**” > “**Agregar**”
- 2- Seleccionar “**Opciones avanzadas**” y pulsar “**Buscar ahora**”
- 3- Seleccionar el grupo **Admins** de la lista de resultados
- 4- Confirmar con “**Aceptar**” dos veces



De esta forma, cualquier usuario perteneciente al grupo Admins tendrá acceso habilitado por Escritorio Remoto a esta VDI.

A7.3. Aplicación de GPO específica para acceso RDP

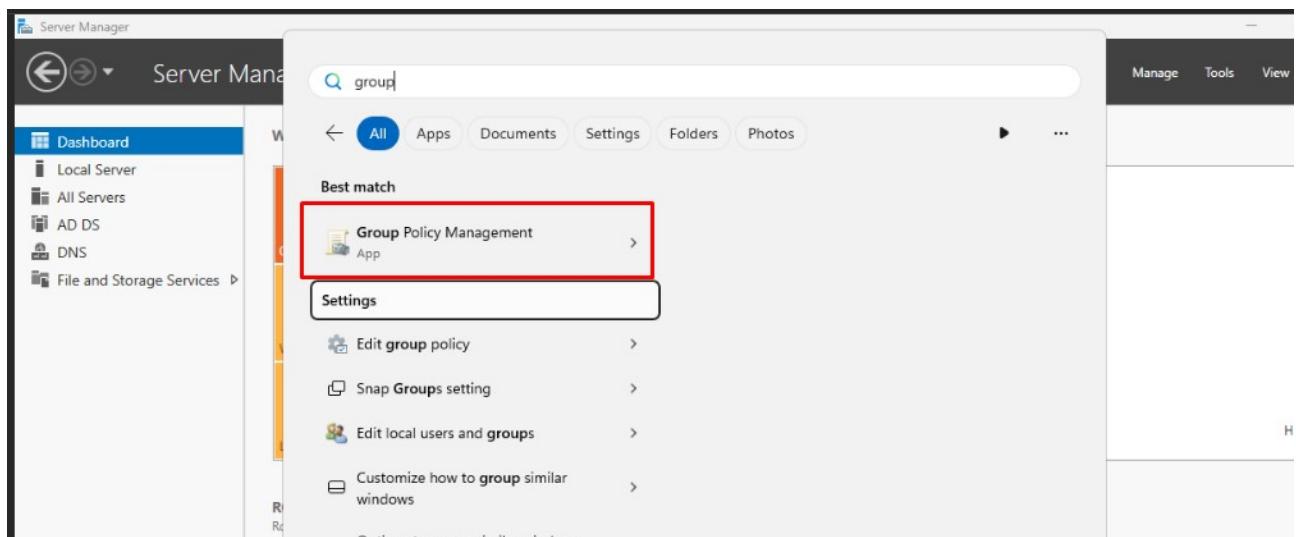
Con la máquina VDI ya integrada en el dominio y organizada dentro de su propia Unidad Organizativa (VDIs), se procede a aplicar una Directiva de Grupo (GPO) destinada a controlar qué usuarios o grupos del dominio tienen permiso para conectarse por Escritorio Remoto (RDP) a dicha máquina.

Esta GPO se crea y gestiona desde el servidor mediante la consola de Group Policy Management, y se vincula directamente a la UO correspondiente para que solo afecte a las máquinas allí contenidas.

Acceso a la consola de administración de GPO

Para comenzar, se accede a la herramienta Group Policy Management desde el menú de inicio de Windows Server.

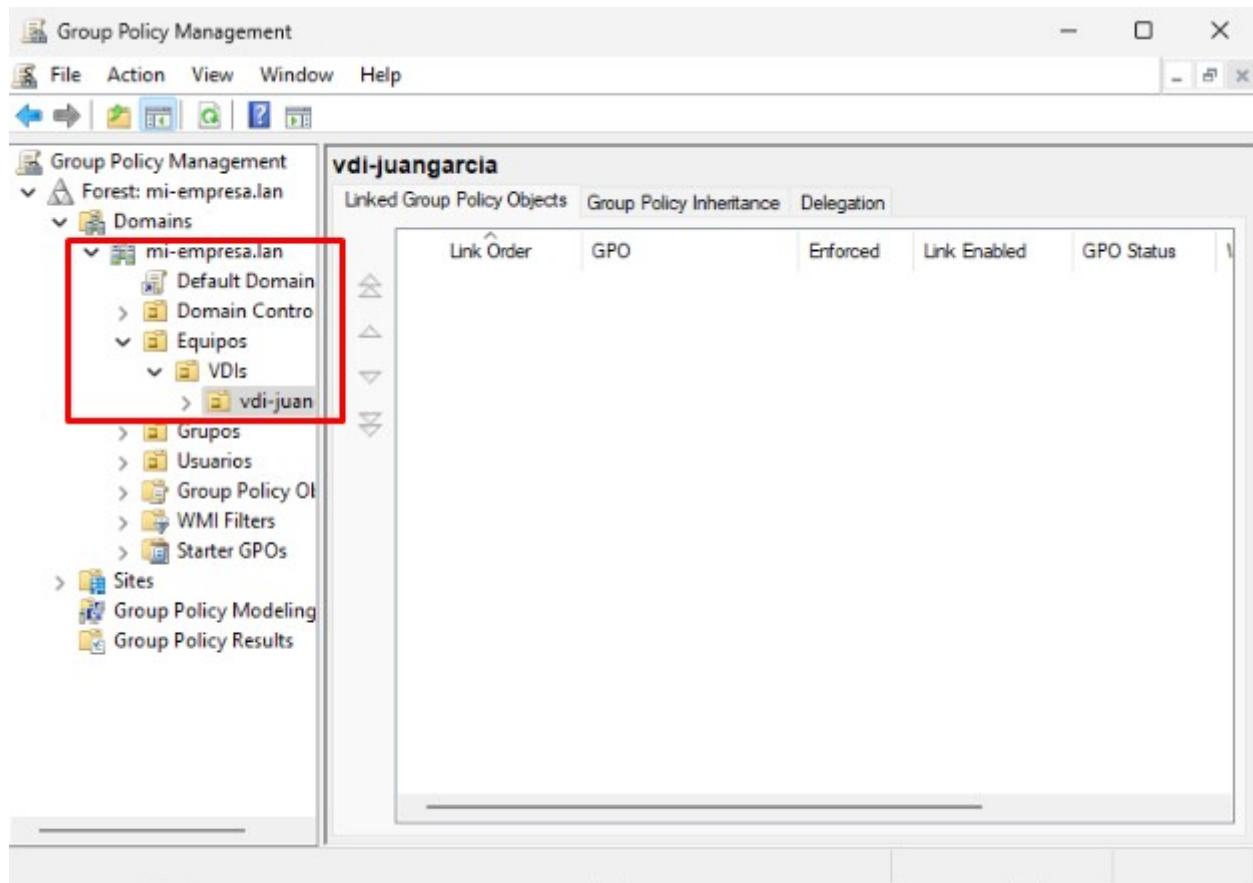
Para ello, se escribe group en el buscador y se selecciona la opción “Group Policy Management”, que permite crear, editar y aplicar directivas sobre contenedores de Active Directory.



Una vez abierta la consola de Group Policy Management, se expande la jerarquía del dominio para localizar la Unidad Organizativa donde se encuentra la máquina a la que se aplicará la directiva.

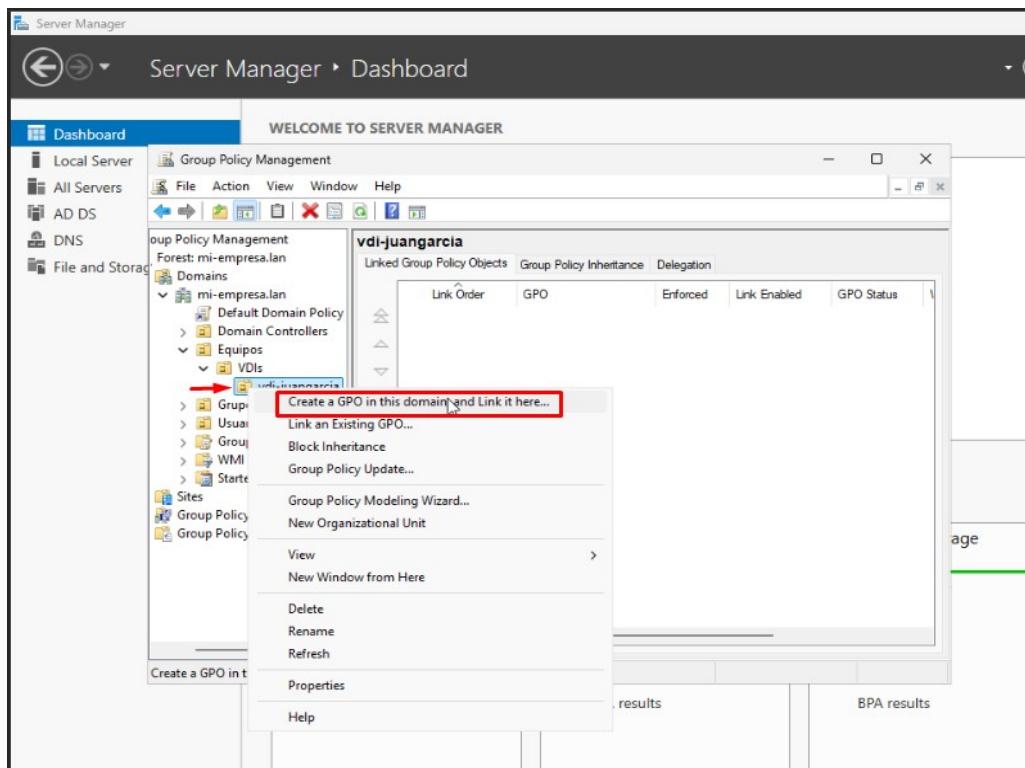
La ruta a seguir es: mi-empresa.lan > Equipos > VDIs > vdi-juangarcia

En este punto, todavía no hay ninguna GPO vinculada a esta UO, lo que permite aplicar una directiva específica sin interferencias de políticas heredadas.

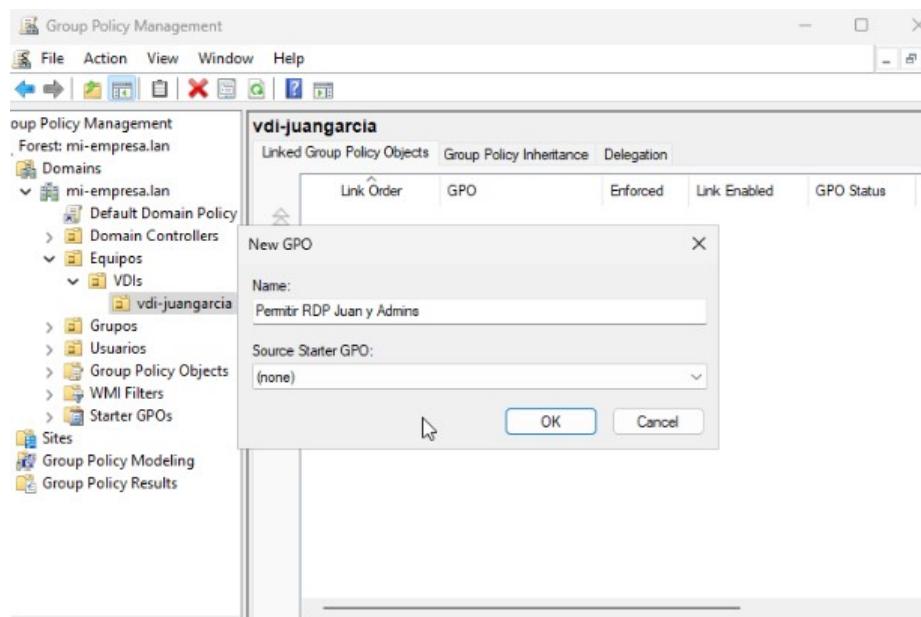


Una vez localizada la UO *vdi-juangarcia*, se procede a crear y vincular una nueva GPO específica para controlar el acceso remoto RDP a dicha máquina.

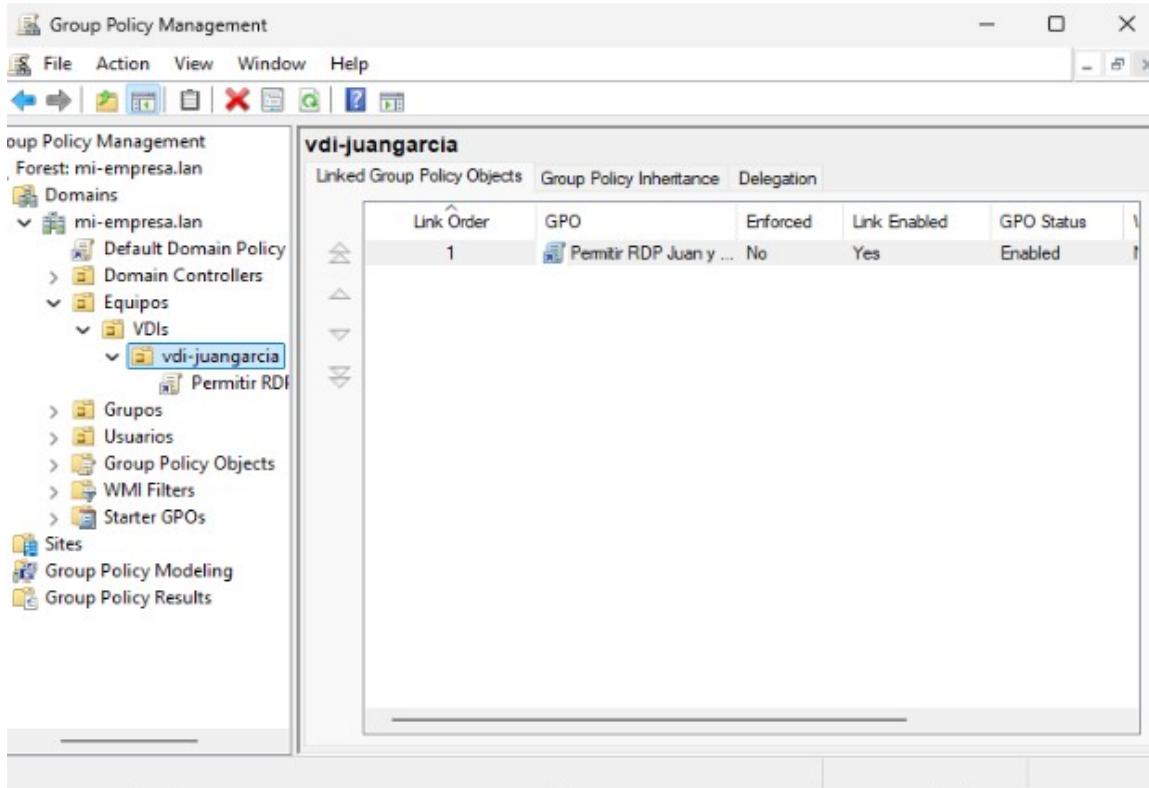
Hacer clic derecho sobre la unidad organizativa *vdi-juangarcia* y seleccionar la opción “**Create a GPO in this domain, and Link it here...**”



En la ventana emergente, introducir el nombre identificativo: ***Permitir RDP Juan y Admins.***. Pulsar ***OK*** para confirmar.

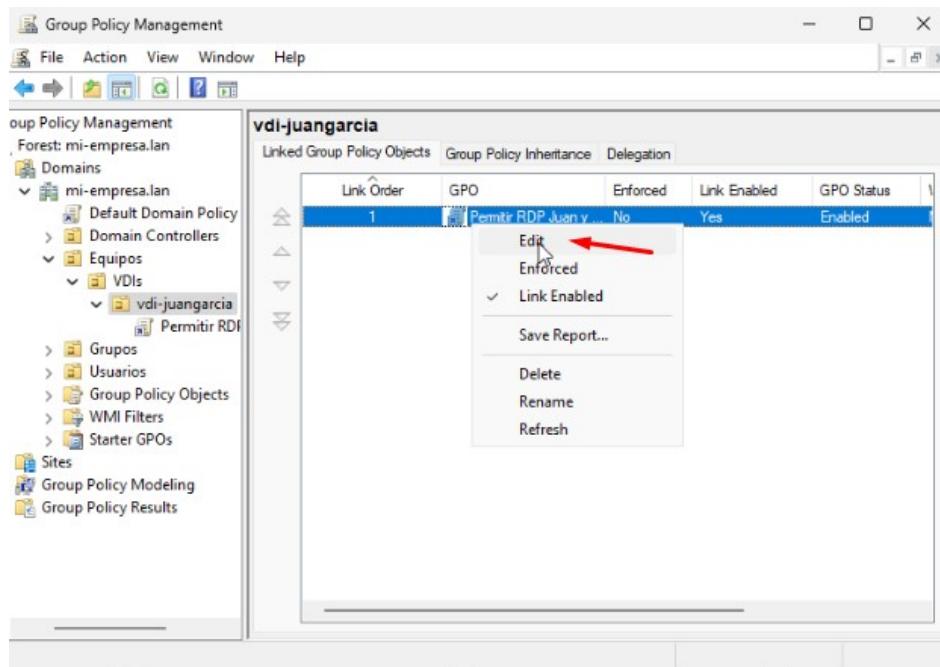


Con este paso, la nueva GPO queda automáticamente vinculada a la UO seleccionada, y aparece listada en la vista de políticas aplicadas, lista para su edición.



Una vez creada y vinculada la GPO Permitir RDP Juan y Admins a la unidad organizativa vdi-juangarcia, se procede a editarla para asignar explícitamente qué usuarios o grupos están autorizados a iniciar sesión mediante Escritorio Remoto.

Clic derecho sobre la GPO Permitir RDP Juan y Admins Seleccionar la opción **Edit**



En la ventana del editor de políticas, navegar por la siguiente ruta:

Configuración del equipo

|__ Policies

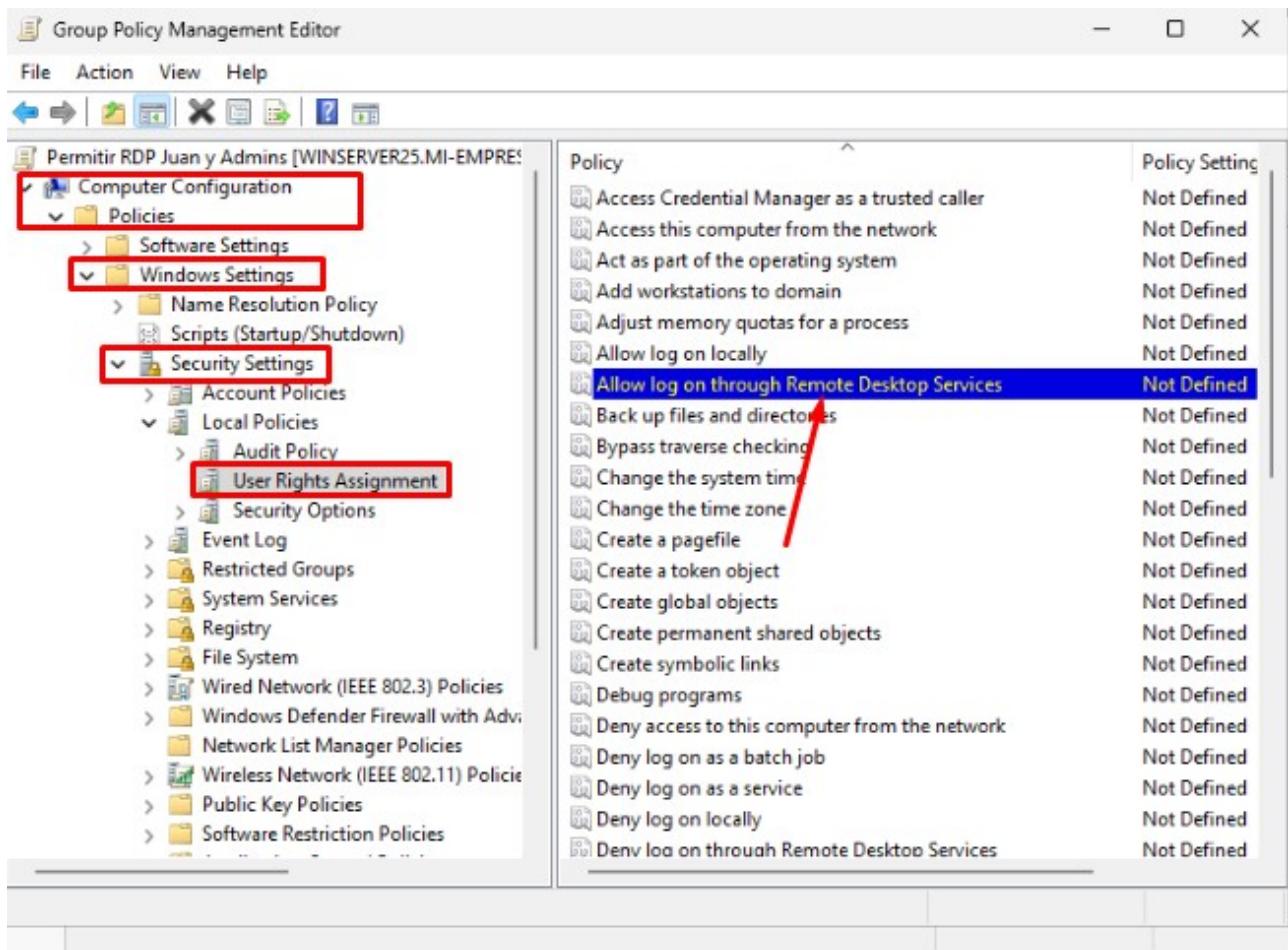
 |__ Configuración de Windows

 |__ Configuración de seguridad

 |__ Directivas locales

 |__ Asignación de derechos de usuario

 |__ Permitir el inicio de sesión a través de Servicios de Escritorio remoto

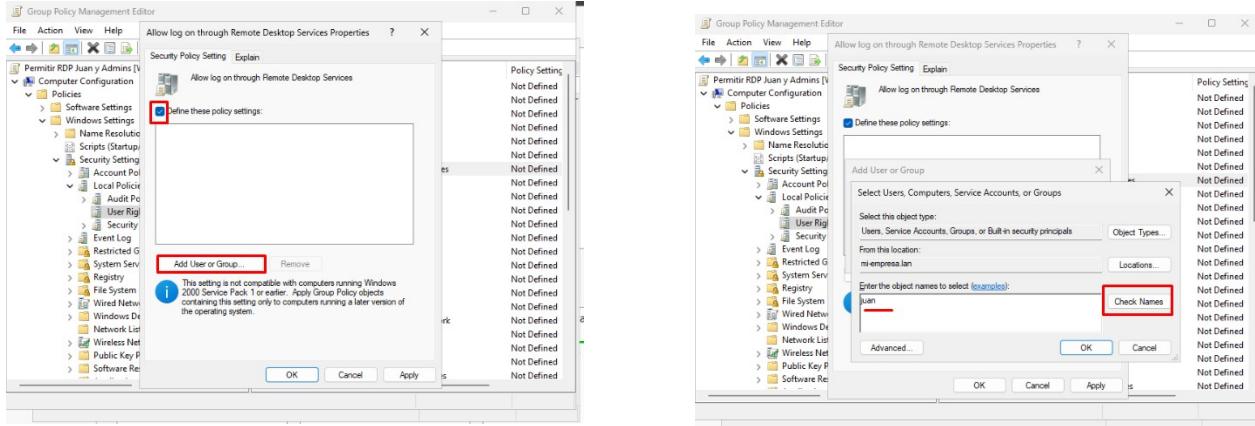


Esta directiva permite definir exactamente qué identidades del dominio (usuarios o grupos) están autorizadas a conectarse por RDP a las máquinas afectadas por esta GPO.

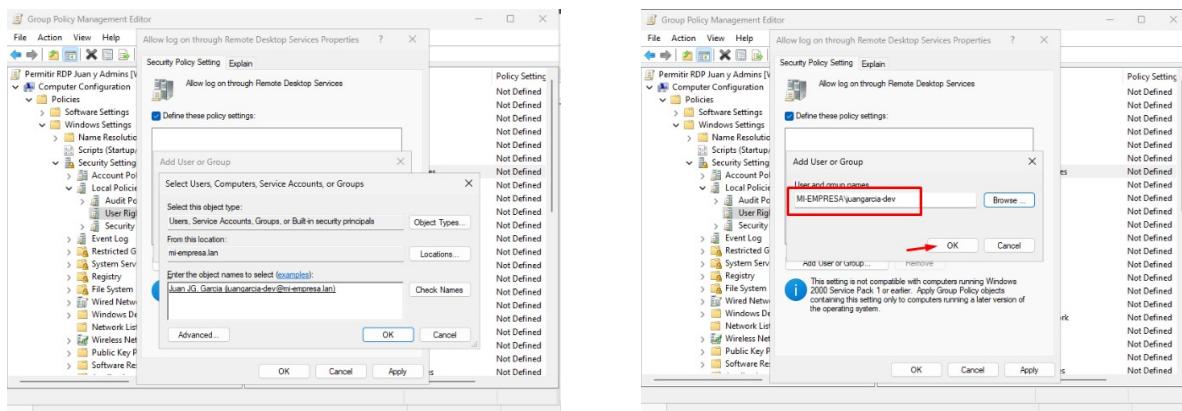
Esta política define explícitamente **quién tiene permitido iniciar sesión de forma remota (RDP)** en los equipos a los que se aplique esta GPO. En este caso, la directiva afecta únicamente a la máquina *vdi-juangarcia*

En el editor de políticas, hacer doble clic sobre: "**Allow log on through Remote Desktop Services**", marcar la opción: "**Define these policy settings**" y pulsar el botón: Add User or Group...

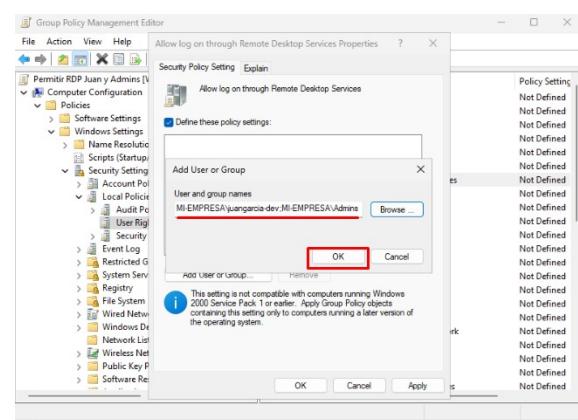
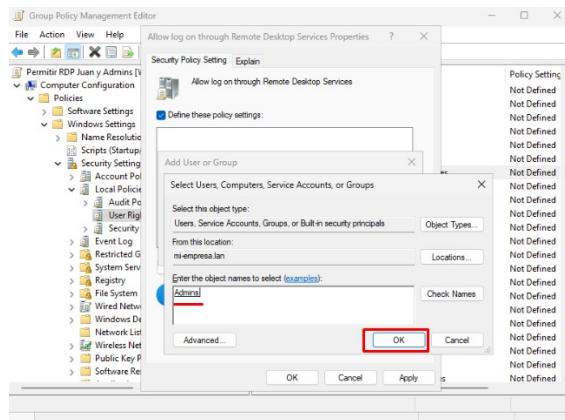
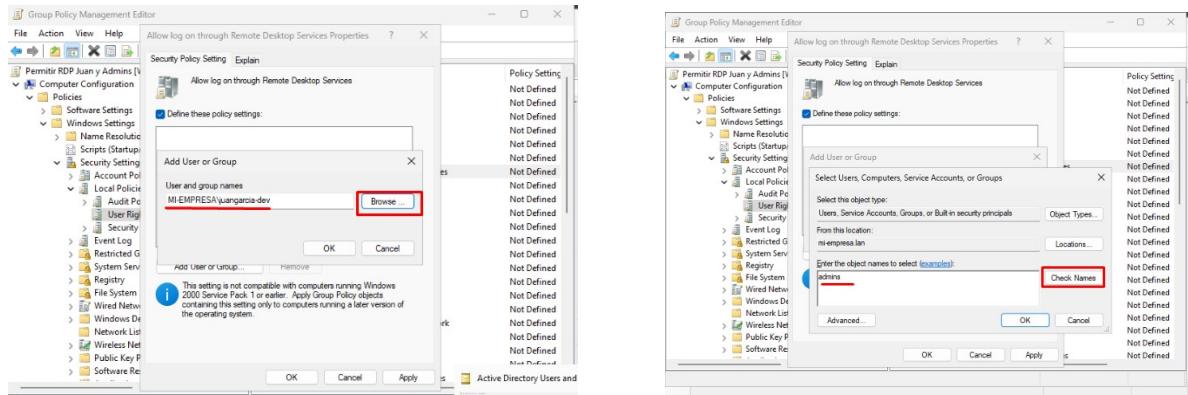
En la ventana emergente: Confirmar que la ubicación es el dominio: mi-empresa.lan En el campo de nombre, escribir: juan Pulsar Check Names para validar.



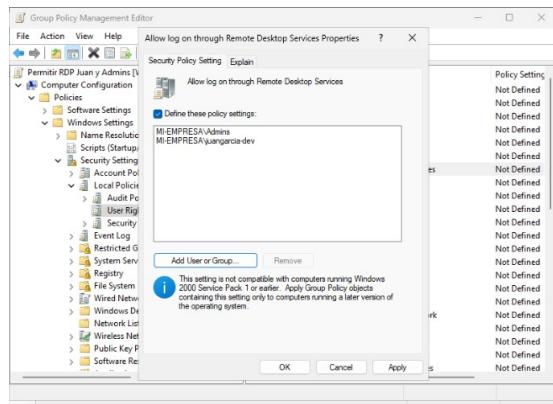
El sistema completa automáticamente el nombre como: *Juan JG. García (juangarcia-dev@mi-empresa.lan)*. Pulsar OK una vez se auto complete en nombre de usuario y pulsar OK igualmente en la ventana de **Security Policy Settings**.



Repetir el mismo proceso para añadir el grupo: Admins



Tras verificar ambos elementos en la lista (el usuario y el grupo admins, pulsar OK y luego Apply en la ventana principal.



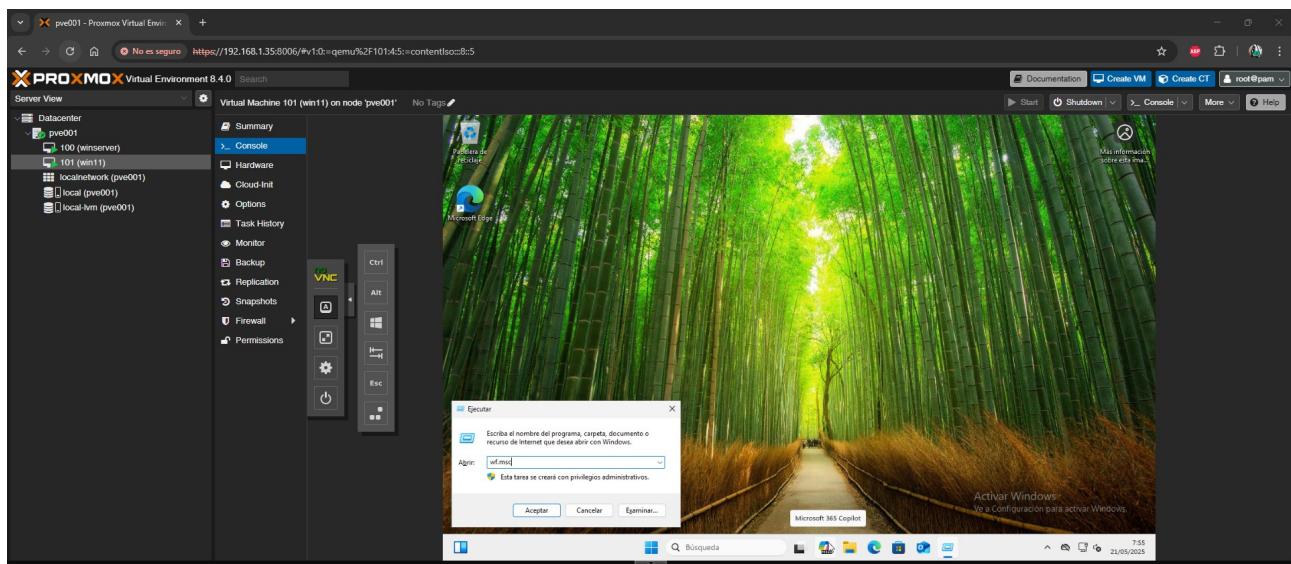
Con esto quedaría configurado el acceso al usuario destinado para la vdi y los usuarios del grupo de admins

Verificación local en la VDI: habilitación de la regla de Firewall para RDP

Aunque el control de acceso RDP se gestiona a través de GPO desde el servidor, es importante verificar que en la máquina cliente (VDI con Windows 11) las reglas del firewall no bloquean las conexiones entrantes.

Este paso garantiza que, una vez aplicadas las directivas, el tráfico RDP pueda pasar correctamente.

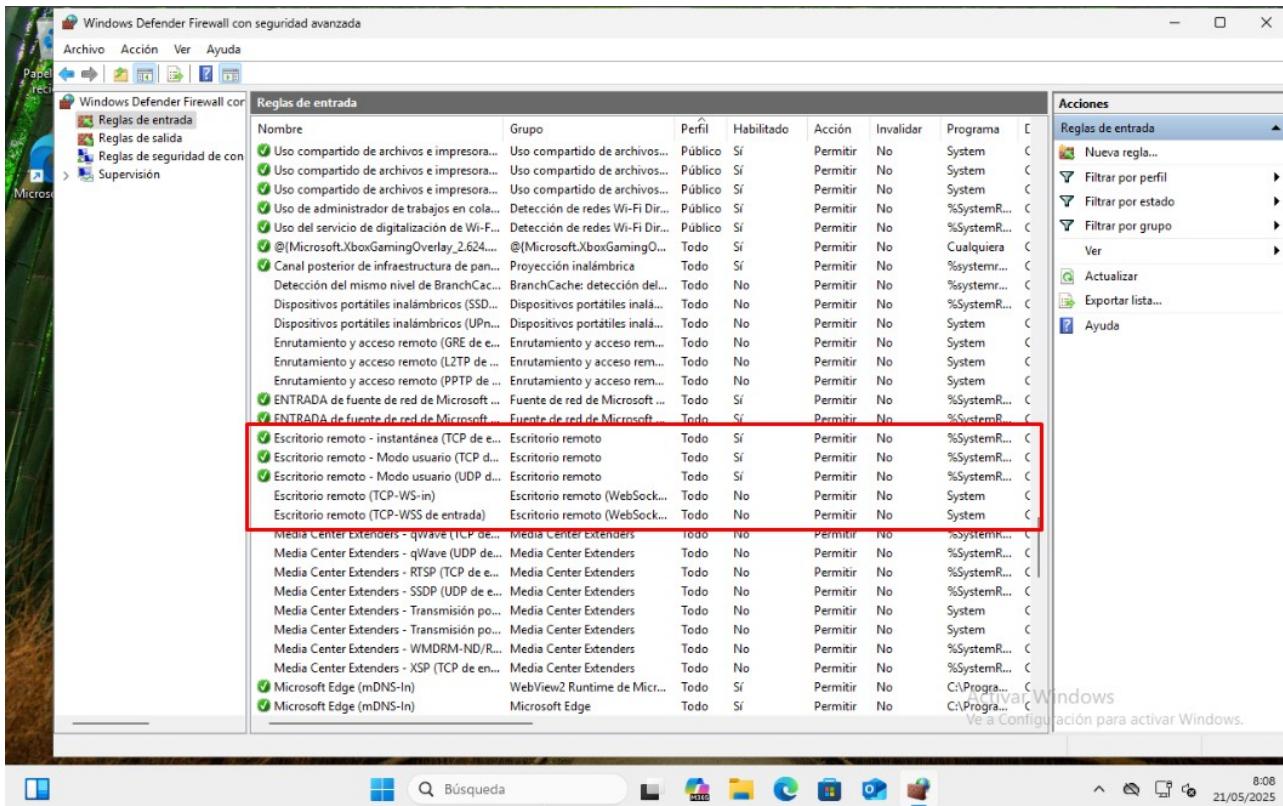
Iniciar sesión en vdi-juangarcia con una cuenta con permisos de administrador (por ejemplo, Administrator). Abrir la ventana “Ejecutar” con Windows + R y escribir: **wf.msc** Pulsar Aceptar para abrir el Firewall de Windows con seguridad avanzada.



En el panel izquierdo, seleccionar: “**Reglas de entrada**”. Localizar las siguientes reglas:

- Escritorio remoto - Modo usuario (TCP-In)
- Escritorio remoto - Modo usuario (UDP-In)
- Escritorio remoto - instantánea (TCP de entrada)

Comprobar que la columna **Habilitado** muestre “Sí”, la **acción** sea **Permitir**, que el perfil sea correcto (por ejemplo, Todo o Privado según tu red)



Si alguna de las reglas aparece deshabilitada, hacer clic derecho sobre ella y seleccionar “Habilitar regla”.

Esta verificación garantiza que el firewall local no bloquee las conexiones RDP, permitiendo que las políticas del dominio surtan efecto correctamente.

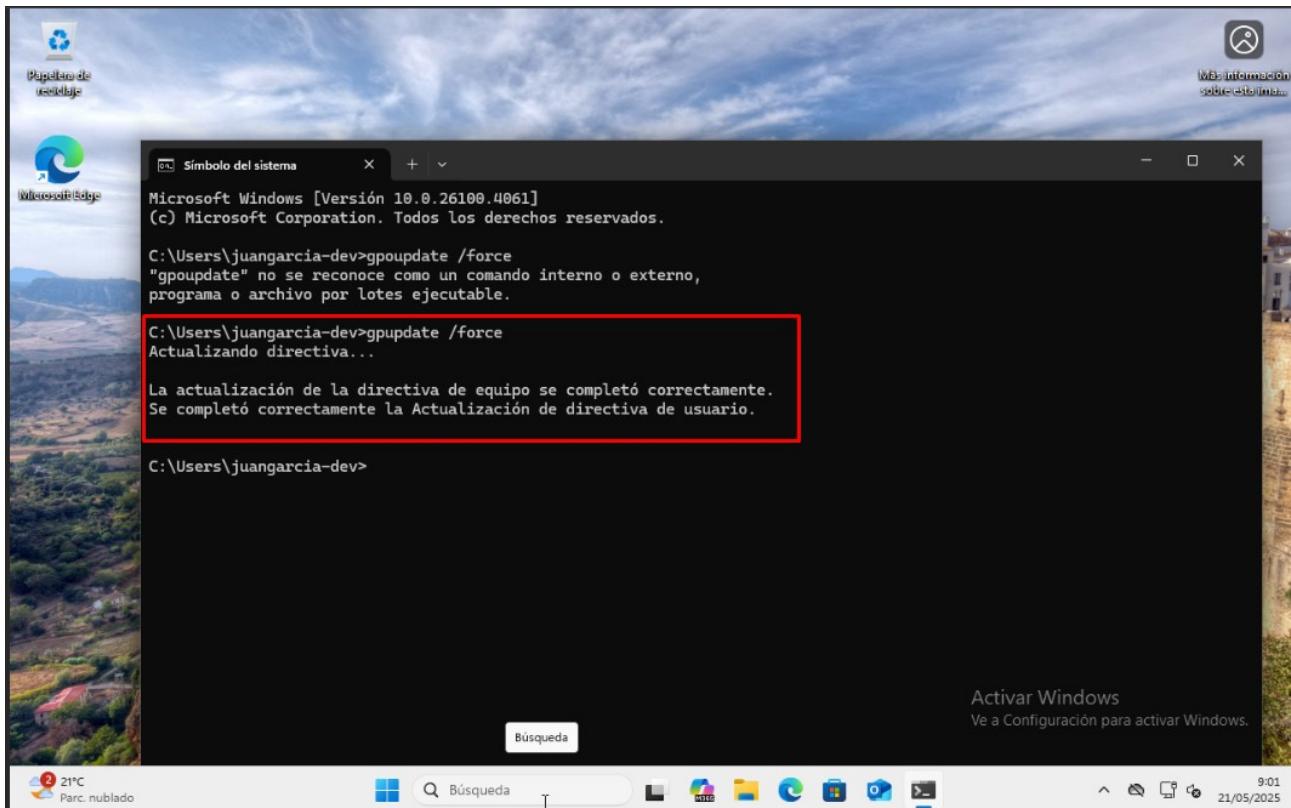
A7.4. Validación del acceso remoto con usuarios del dominio

Con la GPO aplicada, el firewall verificado y el Escritorio Remoto activado, se realizaron pruebas funcionales para confirmar que solo los usuarios autorizados pueden iniciar sesión de forma remota en la máquina *vdi-juangarcia*.

Al haber considerado la red doméstica como la red empresarial, para la realización de las pruebas de conectividad basta con usar un equipo conectado a la red (en mi caso un pc portátil).

Antes de realizar las pruebas, se forzó la aplicación inmediata de las políticas de grupo desde la VDI ejecutando el siguiente comando:

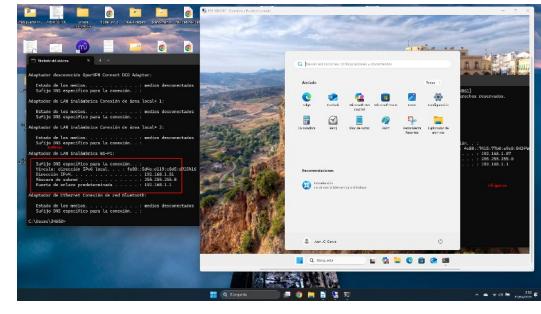
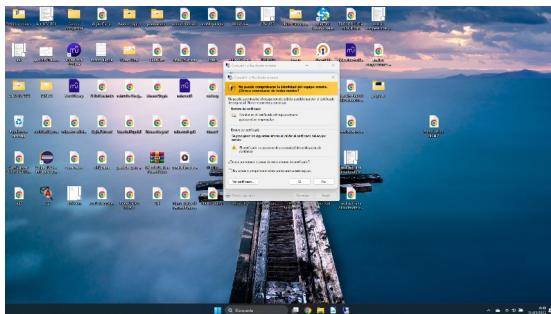
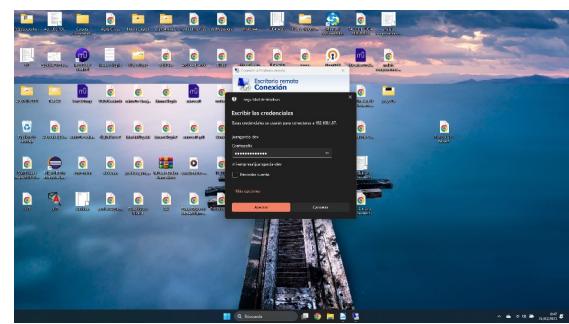
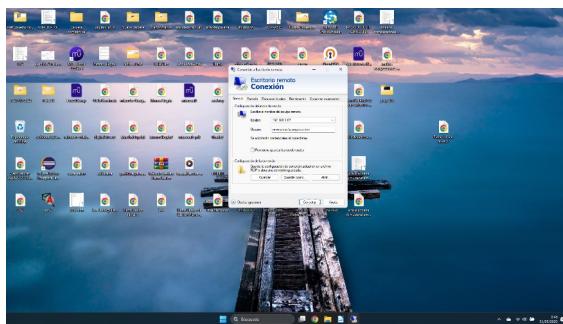
```
gpupdate /force
```



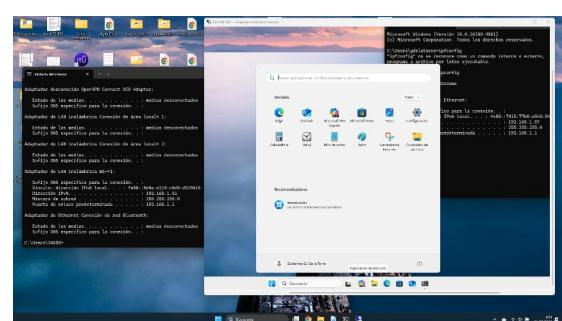
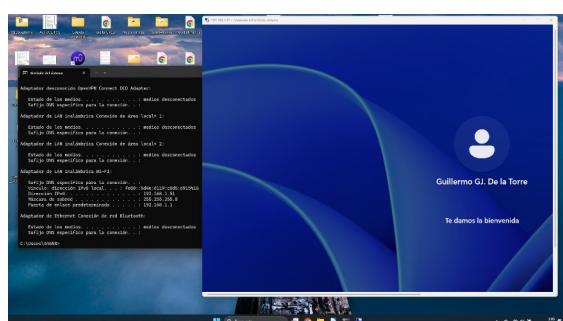
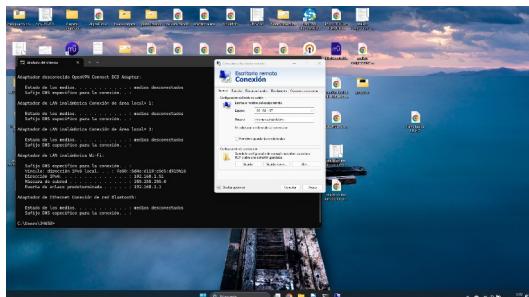
Esto asegura que la GPO recién aplicada surta efecto sin necesidad de esperar al ciclo automático de actualización. Hecho esto, se procedió a reiniciar la vdi.

Pruebas de acceso permitido

Usuario propietario: Juan García

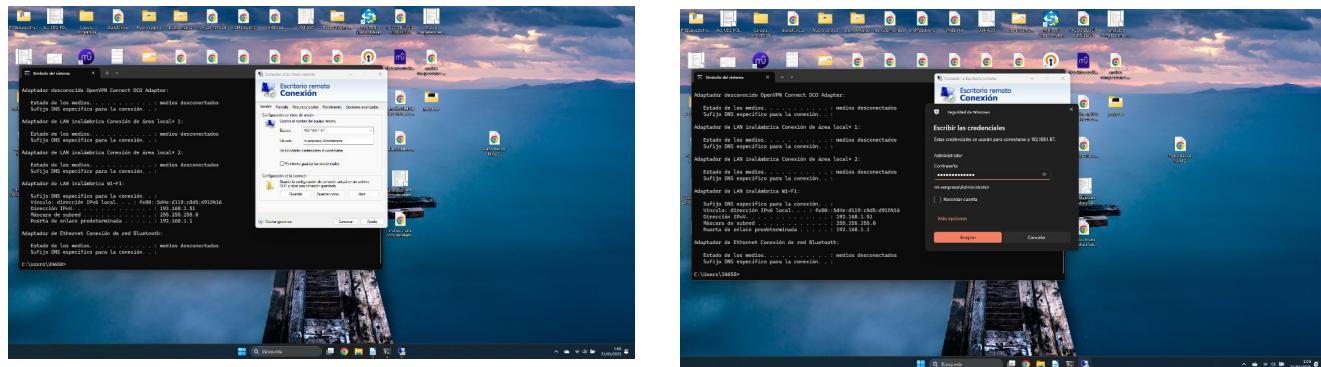


Usuario del grupo Admins: Guillermo De la Torre



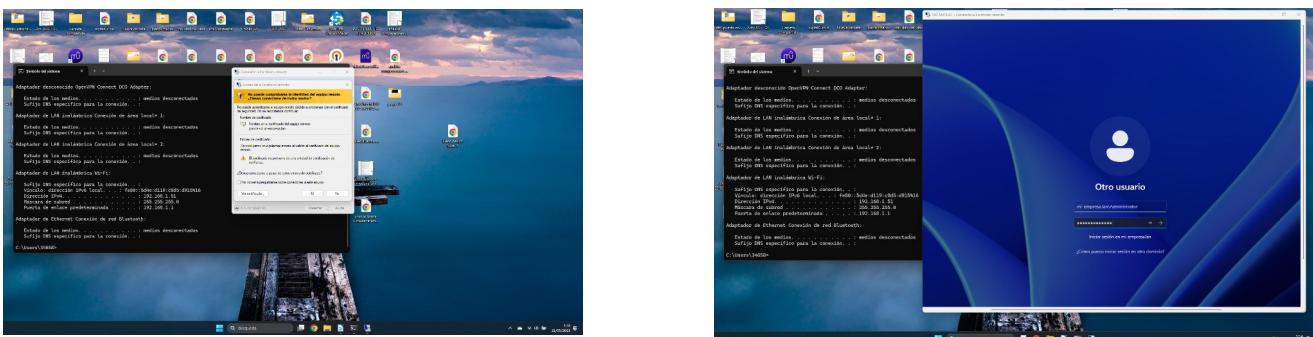
Pruebas de acceso denegado

Usuario Administrator

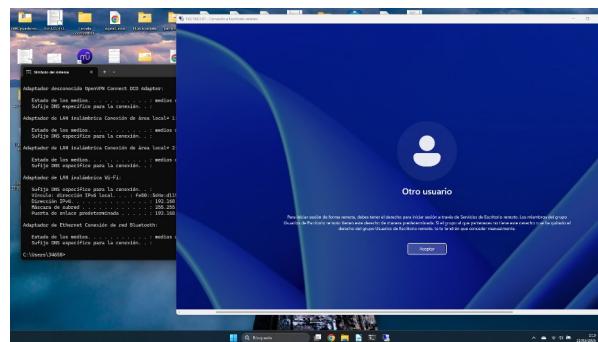


El usuario **Administrator**, que corresponde al controlador de dominio (Windows Server), sí **dispone por defecto de permisos** para realizar conexiones **RDP**.

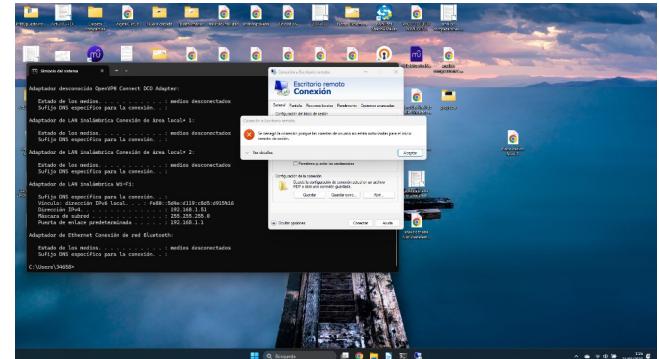
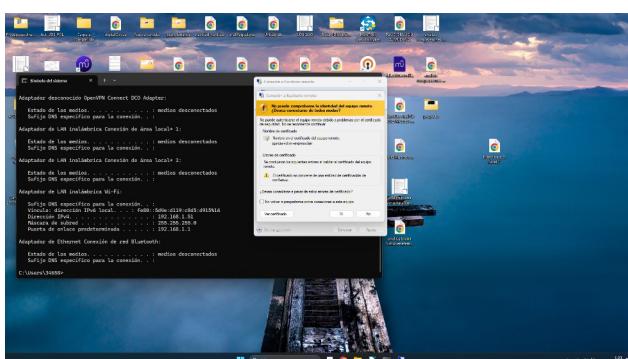
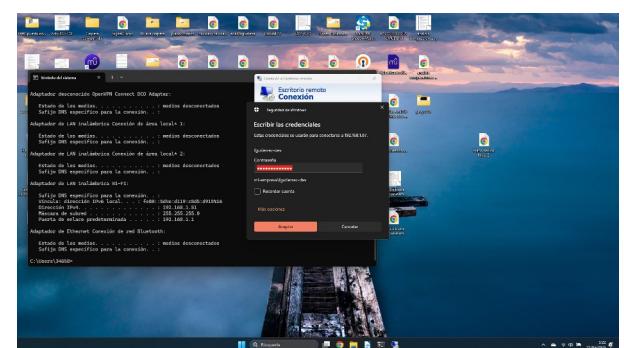
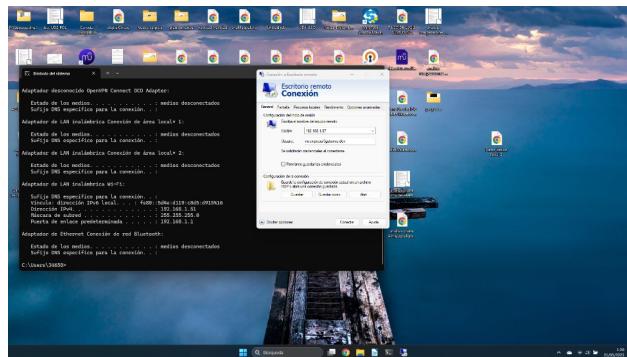
Sin embargo, al **configurar localmente** en la VDI el **acceso** remoto para que esté limitado únicamente al **usuario propietario** (Juan García) y al grupo **Admins**, esta restricción local **impide el acceso al propio Administrator**, ya que no fue incluido explícitamente en esa configuración.



En consecuencia, al intentar iniciar sesión en la VDI mediante RDP con Administrator, el sistema deniega el acceso, dando prioridad a la configuración local más restrictiva.



Usuario Frrancisco Gutierrez



El intento falló, mostrando el siguiente mensaje:

“Se denegó la conexión porque las cuentas de usuario no están autorizadas para el inicio remoto de sesión.”

A la izquierda de la captura, se muestra el resultado del comando ipconfig, confirmando que la máquina cliente se encuentra correctamente conectada a la red (192.168.1.51), lo que descarta problemas de conectividad y reafirma que la denegación se debe exclusivamente a la política aplicada.

Esta prueba demuestra que la GPO configurada cumple correctamente su función al bloquear el acceso a usuarios no autorizados, en este caso Francisco Gutiérrez.

Anexo 8 – Acceso remoto seguro mediante VPN y DNS dinámico (No-IP)

A8.1. Actualización y preparación del sistema OPNsense

Desde la interfaz web de OPNsense, se accedió al menú: **System > Firmware > Status**. Allí se verificó la versión instalada (25.1) y la fecha del último chequeo de actualizaciones.

The screenshot shows the OPNsense Firmware Status page. The left sidebar is expanded, showing the System menu with 'Firmware' selected. The main content area is titled 'System: Firmware' and displays the following information:

Type	opnsense
Version	25.1
Architecture	amd64
Commit	da994c043
Mirror	https://pkg.opnsense.org/FreeBSD:14:amd64/25.1
Repositories	OPNsense (Priority: 11)
Updated on	Tue Jan 28 07:48:20 UTC 2025
Checked on	Sun May 25 01:17:14 UTC 2025

At the bottom of the table, there are two buttons: 'Check for updates' (highlighted with a red box) and 'Run an audit'.

Se pulsó en “Check for updates” para obtener el listado de paquetes pendientes.

The screenshot shows the OPNsense Firmware Updates page. The left sidebar is expanded, showing the System menu with 'Updates' selected. The main content area is titled 'System: Firmware' and displays a table of package updates:

Package name	Current version	New version	Required action	Repository
base	25.1	25.1.6	upgrade	OPNsense
boost-libs	1.86.0_1	1.87.0_1	upgrade	OPNsense
ca_root_nss	3.104	3.108	upgrade	OPNsense
curl	8.11.1_1	8.13.0_2	upgrade	OPNsense
dhcpc6c	20241008	20250513	upgrade	OPNsense
dnsmasq	2.90.4_1	2.91.1	upgrade	OPNsense
easy-rsa	3.2.1_1,1	3.2.2,1	upgrade	OPNsense
expat	2.6.4	2.7.1	upgrade	OPNsense
glib	2.80.5_1,2	2.84.1_2,2	upgrade	OPNsense
hostapd	2.11_1	2.11_3	upgrade	OPNsense
icu	74.2_1,1	76.1,1	upgrade	OPNsense
indexinfo	0.3.1	0.3.1_1	upgrade	OPNsense
jansson	2.14	2.14.1	upgrade	OPNsense
jq	N/A	1.7.1	new	OPNsense
kea	2.6.1_2	2.6.2	upgrade	OPNsense
kernel	25.1	25.1.6	upgrade	OPNsense
krb5	1.21.3	1.21.3_1	upgrade	OPNsense
libcbor	0.11.0	0.12.0	upgrade	OPNsense
libedit	3.1.20240808,1	3.1.20250104,1	upgrade	OPNsense
libffi	3.4.6	3.4.8	upgrade	OPNsense
libidn2	2.3.7	2.3.8	upgrade	OPNsense
libinotify	N/A	20240724_1	new	OPNsense
libnghttp2	1.64.0	1.65.0	upgrade	OPNsense
libpsl	0.21.5_2	0.21.5_2	upgrade	OPNsense

Tras revisar el listado, se pulsó “Update” para iniciar la actualización del sistema.

The screenshot shows the OPNsense web interface under the 'Firmware' section. A list of packages is displayed with their current version, target version, and upgrade status. A prominent yellow dialog box titled 'Reboot required' states: 'The firewall will reboot directly after this firmware update.' It contains two buttons: 'OK' (highlighted with a red box) and 'Cancel'. Below the dialog, a message indicates 'There are 99 updates available, total download size is 320.2MB. This update requires a reboot.' The left sidebar shows various system management links like Reporting, Configuration, and Firewall.

Al finalizar la actualización, el sistema solicitó reinicio para aplicar los cambios.

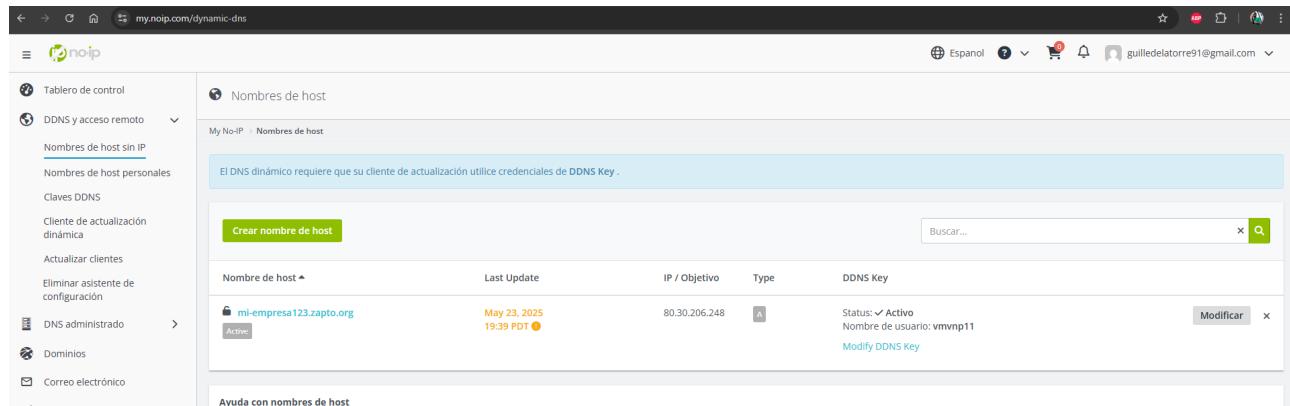
This screenshot shows the 'System: Firmware' page after the update was completed. A large message box says 'Your device is rebooting' and 'The upgrade has finished and your device is being rebooted at the moment, please wait...'. Below this, a terminal window displays the upgrade logs, which include commands like 'rm -rf /var/cache/pkg/*', file deletions, and kernel installations. The logs end with 'Please reboot. ***REBOOT***'. At the bottom, a note says 'Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.'

A8.2. Configuración de DNS dinámico con No-IP

Para poder acceder remotamente al servidor VPN desde redes externas, era necesario contar con un dominio que apuntase a la IP pública del router, incluso cuando esta cambiase. Para ello, se utilizó el servicio No-IP, una solución gratuita y ampliamente usada para DNS dinámico (DDNS).

Este servicio permite registrar un subdominio que se actualiza automáticamente con la IP pública actual del equipo o red donde esté configurado. En este proyecto, se integrará con ddclient en OPNsense para mantener el registro actualizado y permitir así que los clientes VPN se conecten mediante un nombre de dominio en lugar de una IP cambiante.

Desde el portal de administración de No-IP se creó el host: ***mi-empresa123.zapto.org***

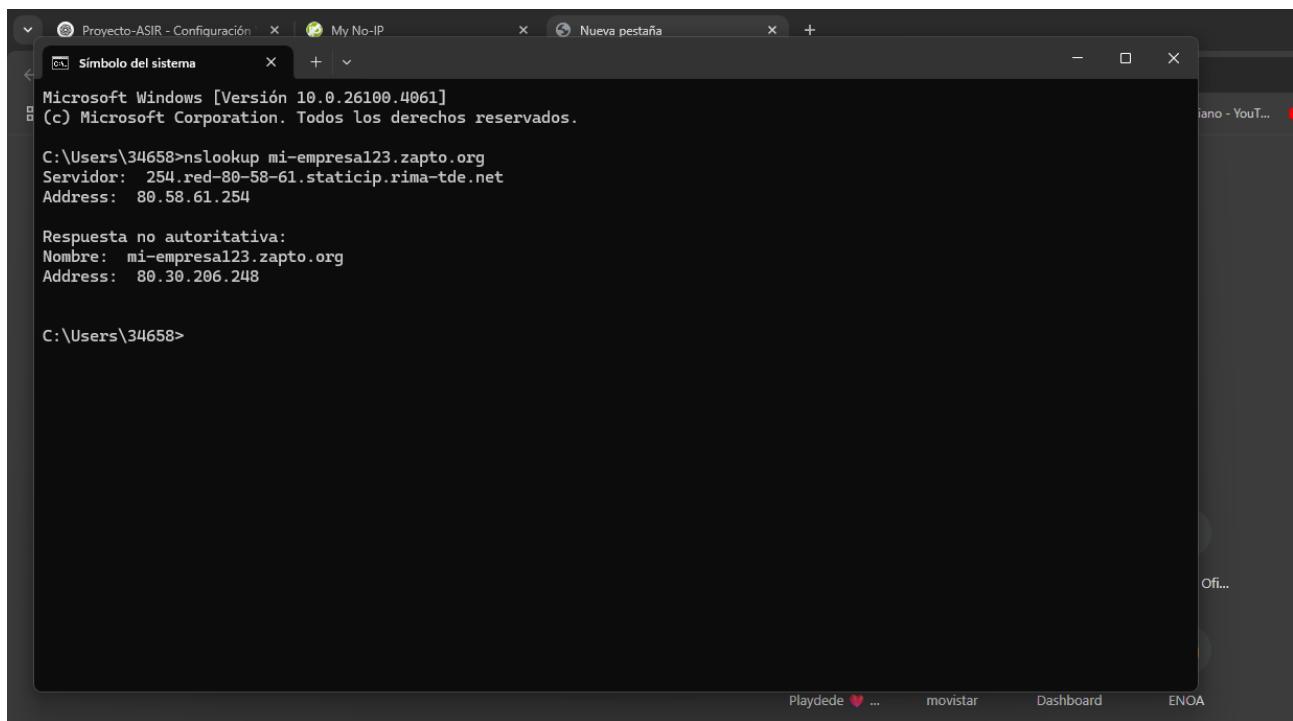


The screenshot shows the No-IP web interface at my.no-ip.com/dynamic-dns. The left sidebar has a tree view with 'Nombres de host sin IP' selected. The main area is titled 'Nombres de host' and shows a table with one row:

Nombre de host *	Last Update	IP / Objetivo	Type	DDNS Key
mi-empresa123.zapto.org <small>Active</small>	May 23, 2025 19:39 PDT	80.30.206.248		Status: ✓ Activo Nombre de usuario: vmvnp11 Modificar x

Este subdominio queda asociado a la IP pública actual y se mantendrá actualizado mediante el cliente ddclient. El estado figura como Activo, con la última actualización automática correctamente registrada.

Para comprobar el funcionamiento del DDNS, se ejecutó un nslookup desde un cliente externo al dominio. Como se observa, el dominio mi-empresa123.zapto.org se resuelve correctamente a la IP pública 80.30.206.248, demostrando que el servicio de DNS dinámico está funcionando y apuntando a la red correcta.



```
Microsoft Windows [Versión 10.0.26100.4061]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\34658>nslookup mi-empresa123.zapto.org
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

Respuesta no autoritativa:
Nombre: mi-empresa123.zapto.org
Address: 80.30.206.248

C:\Users\34658>
```

A8.3. Configuración del servidor OpenVPN en OPNsense

Una vez configurado el servicio de DNS dinámico para identificar la red desde el exterior, el siguiente paso fue crear y configurar un servidor OpenVPN en OPNsense. Esto permite a los usuarios autorizados establecer una conexión segura y cifrada con la red interna desde cualquier ubicación.

La configuración se realizó íntegramente desde la interfaz web de OPNsense, utilizando el asistente incluido, y se dividió en las siguientes fases:

A8.3.1. Creación de la Autoridad Certificadora (CA)

Antes de poner en marcha el servidor OpenVPN, es necesario generar una Autoridad Certificadora (CA) interna, que será la encargada de emitir y firmar los certificados tanto del servidor como de los clientes. Esto garantiza una autenticación segura entre ambas partes.

Acceder al menú: **System > Trust > Authorities** y pulsar el botón “+ Add” para crear una nueva CA.

The screenshot shows the OPNsense web interface. The left sidebar has a tree structure with several collapsed categories like 'Reporting', 'Access', 'Configuration', etc., and some expanded sections like 'System' and 'Trust'. Under 'Trust', the 'Authorities' section is highlighted with a red box. The main content area is titled 'System: Trust: Authorities' and contains a table header for 'Certificates' with columns: Description, Issuer, Name, Usages, Valid from, Valid to, and Commands. Below the header, it says 'No results found!' and shows a small icon of a certificate. At the bottom right of the table area, it says 'Showing 0 to 0 of 0 entries'.

En el formulario de creación de una CA. Los siguientes campos son clave:

Method: Create an internal Certificate Authority

Descriptive name: CA-VPN

Key type: RSA-2048

Digest Algorithm: SHA256

Lifetime (days): 825

Common Name: Certificadora VPN

The screenshot shows the 'Edit Certificate' dialog box. The 'Method' dropdown is set to 'Create an internal Certificate Authority'. The 'Description' field contains 'CA-VPN'. Under the 'Key' section, 'Key type' is 'RSA-2048' and 'Digest Algorithm' is 'SHA256'. The 'Issuer' dropdown is empty. The 'Lifetime (days)' is set to 825. In the 'General' section, the organization details are filled: Country Code (Netherlands), State or Province (SPAIN), City (ECija), Organization (IES LUIS VELEZ DE GUEVARA), Organizational Unit (INFORMATICA), Email Address (guillelatorre91@gmail.com), and Common Name (Certificadora VPN). There is also an empty 'OCSP uri' field. At the bottom right are 'Cancel' and 'Save' buttons.

A8.3.2. Creación del certificado del servidor VPN

Una vez creada la Autoridad Certificadora (CA), se procedió a generar el certificado específico para el servidor OpenVPN, que le permitirá identificarse ante los clientes de forma segura. Acceder a:

System > Trust > Certificates y pulsar el botón “+ Add / Sign” para añadir un nuevo certificado.

Configurar los siguientes parámetros en el formulario:

Method: Create an internal certificate

Description: cert-server-VPN

Certificate authority: CA-VPN (la creada en el paso anterior)

Type: Server Certificate

Key type: RSA-2048

Digest Algorithm: SHA256

Lifetime: 397 días

Edit Certificate

Method: Reissue and replace certificate (does not restart service)

Description: cert-server-VPN

Key

Type: Server Certificate

Key type: RSA-2048

Digest Algorithm: SHA256

Issuer: CA-VPN

Lifetime (days): 397

General

Country Code: Netherlands

State or Province: SPAIN

City: ECIJA

Organization: IES LUIS VELEZ DE GUEVARA

Organizational Unit: INFORMATICA

Email Address: guillelodelatorre91@gmail.com

Common Name: (empty)

OCSP uri: (empty)

Cancel **Save**

Pulsar **Save** para finalizar.

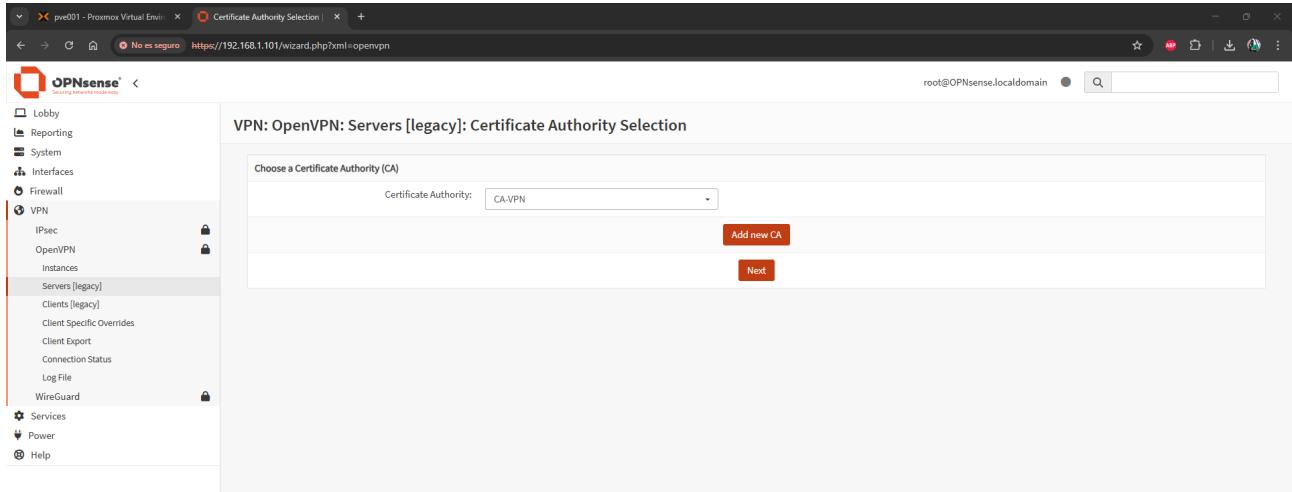
A8.3.3. Configuración del servidor OpenVPN usando el asistente (Wizard)

Para facilitar la configuración, se utilizó el asistente incluido en OPNsense para desplegar el servidor OpenVPN de forma guiada y rápida. Este método permite crear todos los elementos necesarios en una sola secuencia: certificado, servidor, reglas de firewall y rutas.

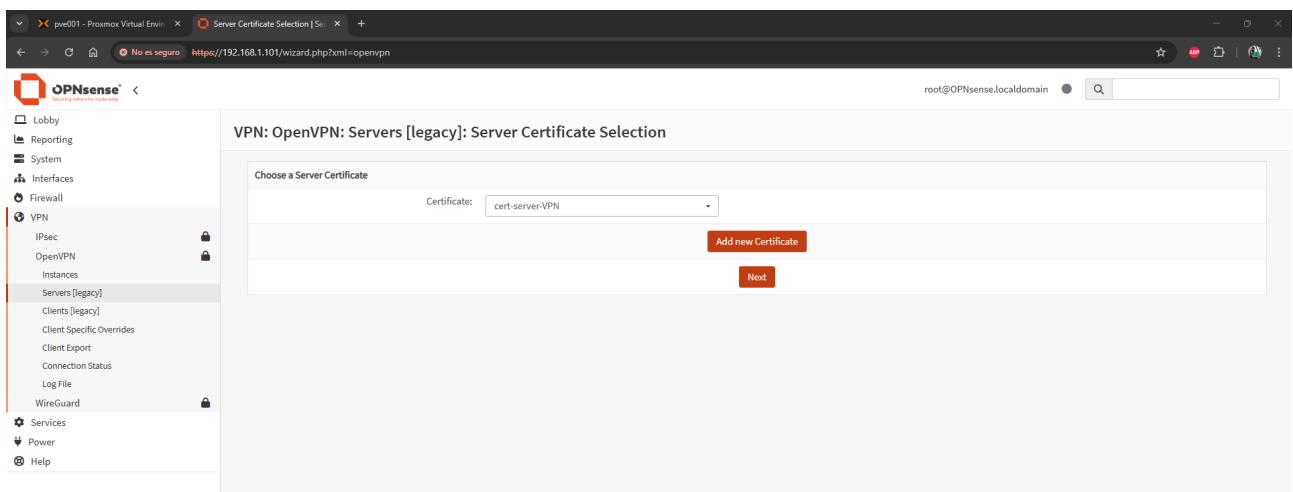
Acceder al asistente desde **VPN > OpenVPN > Servers** y hacer clic en el ícono de la barita

Tipo de autenticación: **Local user Access**

Seleccionar la CA creada anteriormente.



Seleccionar el certificado de servidor creado.



En la siguiente pantalla, aparece el formulario del asistente. Este incluye numerosos parámetros. A continuación se describen los más importantes:

Sección: General OpenVPN Server Information

- **Interface:** *any*. Permite que el servidor escuche conexiones entrantes en todas las interfaces disponibles. En entornos reales se suele limitar a WAN.

- **Protocol:** *UDP*. Protocolo recomendado para conexiones VPN por ser más rápido y eficiente que TCP en la mayoría de escenarios.

- **Local Port:** *1194*. Puerto por defecto de OpenVPN, puede cambiarse si se desea evitar bloqueos o filtrado de ISP.

Description: *lab-teletrabajo*. Nombre identificativo para distinguir esta instancia VPN de otras posibles.

Sección: Cryptographic Settings

TLS Authentication: *marcada*. Añade una capa de autenticación basada en clave compartida.

TLS Key: *generada automáticamente*. Permite proteger el canal de control OpenVPN y evitar conexiones no autorizadas.

Encryption Algorithm (fallback): AES-256-CBC. Estándar fuerte de cifrado simétrico, ampliamente soportado por clientes.

Auth Digest Algorithm: *SHA1*. Se usa para autenticar paquetes. Aunque existen opciones más modernas, sigue siendo funcional en muchos contextos.

Sección: Tunnel Settings

IPv4 Tunnel Network: *10.8.0.0/24*. Subred virtual que se asignará a los clientes VPN. No debe solaparse con redes internas.

IPv4 Local Network: *192.168.1.0/24*. Red LAN real a la que se desea dar acceso remoto. Permite acceder a las VDIs y servicios internos.

Sección: Client Settings

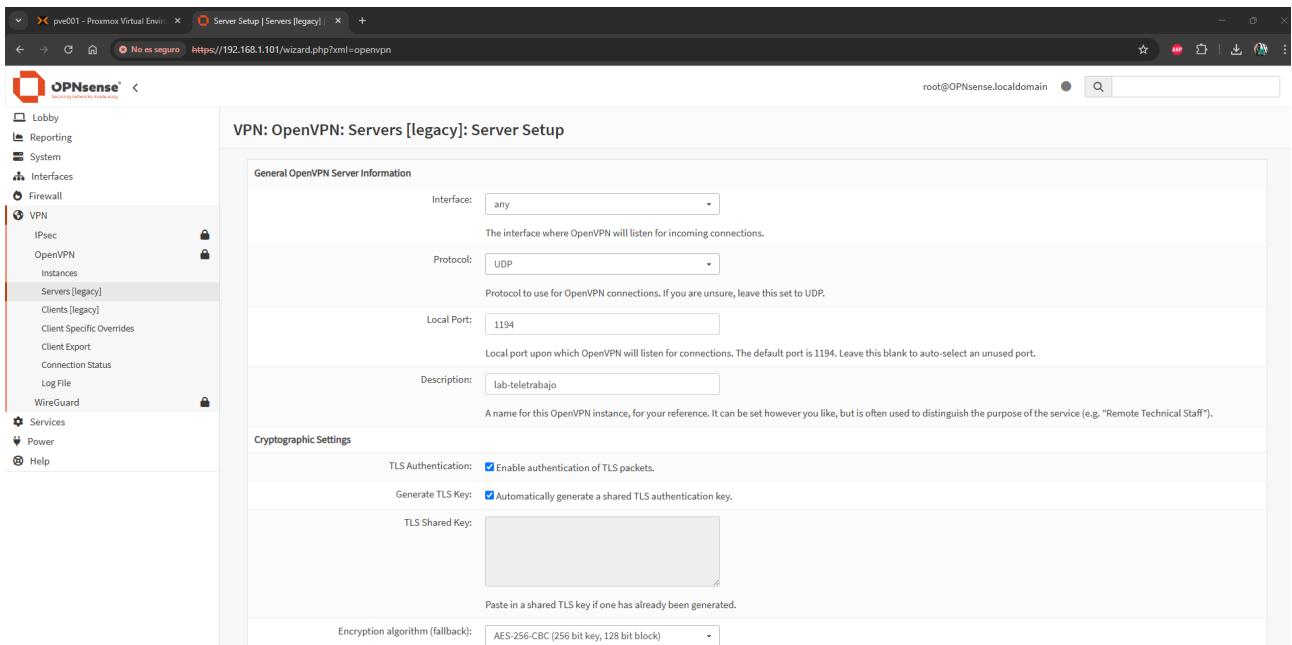
Inter-Client Communication: *marcada*. Permite que los clientes conectados a la VPN puedan comunicarse entre sí (útil en entornos colaborativos o pruebas).

Dynamic IP: *marcada*. Asegura que los clientes puedan reconectarse sin conflictos si cambia su IP local.

DNS Server 1: 8.8.8.8. Servidor DNS público de Google. Se enviará a los clientes para resolución de nombres.

DNS Default Domain: 1.1.1.1

Esta configuración permite establecer una conexión VPN básica, segura y funcional para acceder a la infraestructura interna de la red del proyecto desde cualquier ubicación remota.



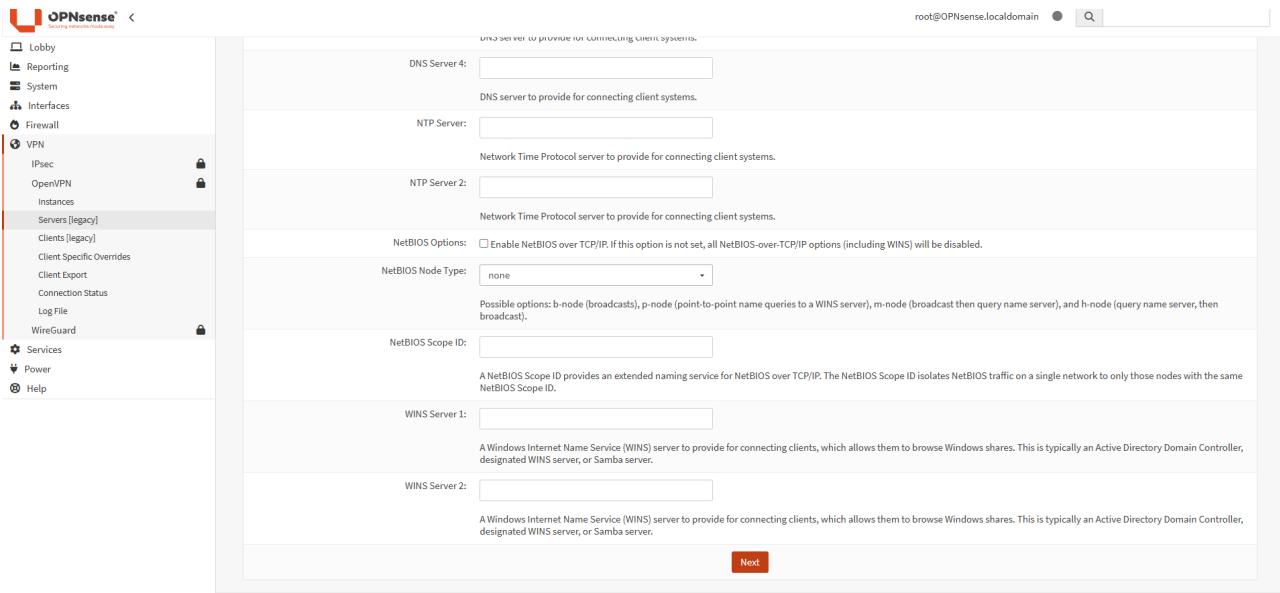
The screenshot shows the OPNsense web interface under the 'VPN' section. On the left sidebar, 'OpenVPN Instances' is selected. The main panel displays 'Tunnel Settings' for a specific tunnel. Key configuration options include:

- Encryption algorithm (fallback):** AES-256-CBC (256 bit key, 128 bit block)
- Auth Digest Algorithm:** SHA1 (160-bit)
- IPv4 Tunnel Network:** 10.8.0.0/24
- IPv6 Tunnel Network:** (empty field)
- Redirect Gateway:** (checkbox) Force all client generated traffic through the tunnel.
- IPv4 Local Network:** 192.168.1.0/24
- IPv6 Local Network:** (empty field)
- IPv4 Remote Network:** (empty field)

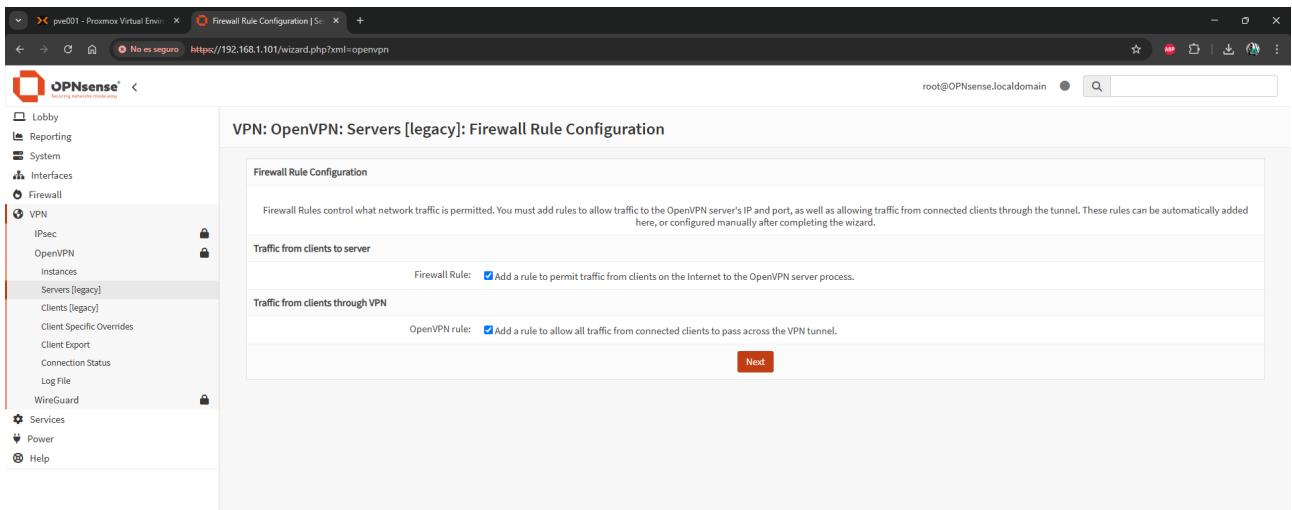
Each field includes descriptive text explaining its purpose and usage.

The screenshot shows the OPNsense web interface under the 'VPN' section. On the left sidebar, 'OpenVPN Instances' is selected. The main panel displays 'Client Settings' for an OpenVPN instance. Key configuration options include:

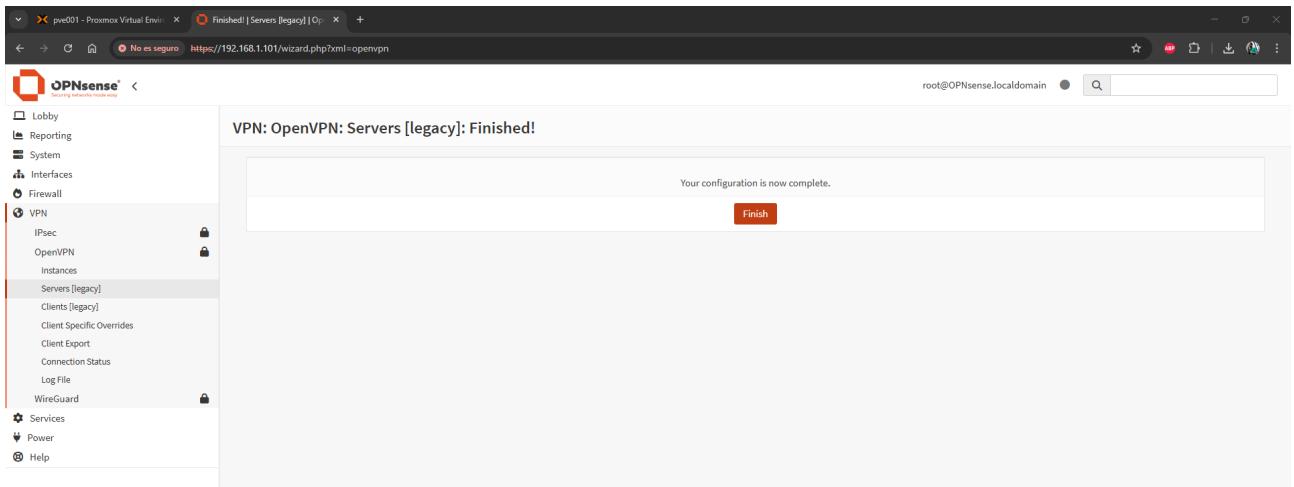
- IPv4 Remote Network:** (empty field)
- IPv6 Remote Network:** (empty field)
- Concurrent Connections:** (empty field)
- Compression:** No Preference
- Type-of-Service:** (checkbox) Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
- Inter-Client Communication:** (checkbox) Allow communication between clients connected to this server.
- Duplicate Connections:** (checkbox) Allow multiple concurrent connections from clients using the same Common Name. This is not generally recommended, but may be needed for some scenarios.
- Client Settings** section:
 - Dynamic IP:** (checkbox) Allow connected clients to retain their connections if their IP address changes.
 - DNS Default Domain:** 1.1.1.1
 - DNS Server 1:** 8.8.8.8



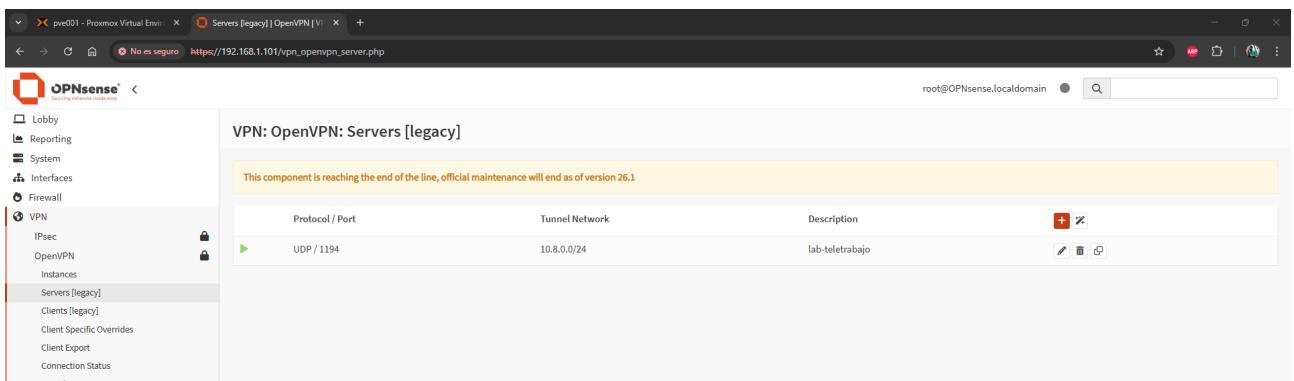
Tras completar la configuración de parámetros y redes del servidor OpenVPN, el asistente ofrece la posibilidad de **crear automáticamente las reglas** necesarias para que funcione correctamente (seleccionar ambas casillas)..



Al seleccionar estas opciones, se garantiza el flujo de datos hacia la red interna y el correcto establecimiento de sesiones VPN. A continuación, dar en el botón de **Finish**.



Una vez finalizado el asistente se puede apreciar que se ha creado el servidor.



A8.3.4. Creación del usuario VPN local

Para permitir el acceso remoto a través de OpenVPN, es necesario crear al menos un usuario en el sistema OPNsense. Este usuario podrá ser autenticado mediante certificado y/o credenciales si así se configura en el servidor.

Para ello acceder al menú de usuarios **System > Access > Users** y hacer clic en el botón “+ Add” para abrir el formulario de creación de un nuevo usuario.

The screenshot shows the OPNsense web interface with the URL <https://192.168.1.101/ui/auth/user>. The left sidebar has a tree view with 'Access' selected. The main panel title is 'System: Access: Users'. It shows one user entry: 'root' (uid 2000) is part of the 'admins' group and is described as a 'System Administrator'. There are buttons for search, refresh, and other actions.

Rellenar el formulario para el usuario y guardar

The 'Edit User' dialog box is open. The 'Username' field contains 'Administrator'. Other fields include 'Password' (redacted), 'Full name' (administrador de dominio), 'E-mail' (redacted), 'Comment' (redacted), 'Preferred landing page' (redacted), 'Language' (Default), 'Login shell' (Default (none for all but root)), 'Expiration date' (redacted), and 'Group membership' (Nothing selected). At the bottom are 'Cancel' and 'Save' buttons.

Realizado esto, ya aparece el usuario creado en la lista.

System: Trust: Certificates

Certificates	In use	Description	Issuer	Purpose	Name	Valid from	Valid to	User client certificate	Commands
	<input type="checkbox"/>	Web GUI TLS certificate	self-signed	id-kp-serverAuth	/CN=OPNsense.localdomain/C=NL/ST=Zuid-Holland/L=...	May 25, 2025 3:03 AM	Jun 26, 2026 3:03 AM	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	Web GUI TLS certificate	self-signed	id-kp-serverAuth	/CN=OPNsense.localdomain/C=NL/ST=Zuid-Holland/L=...	May 25, 2025 3:09 AM	Jun 26, 2026 3:09 AM	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	cert-server-VPN	CA-VPN	id-kp-serverAuth	/C=NL/ST=SPAIN/L=ECUJA/O=IES LUIS VELEZ DE GUEVA...	May 25, 2025 7:46 AM	Jun 26, 2026 7:46 AM	<input type="checkbox"/>	
	<input checked="" type="checkbox"/>	user-Administrator	CA-VPN	id-kp-clientAuth	/C=NL/ST=SPAIN/L=ECUJA/O=IES LUIS VELEZ DE GUEVA...	May 25, 2025 8:00 AM	Jun 26, 2026 8:00 AM	<input type="checkbox"/>	

Showing 1 to 4 of 4 entries

Para que el usuario pueda autenticarse con OpenVPN, es necesario generarle un certificado digital firmado por la autoridad certificadora (CA) creada previamente. Este certificado se incluirá en el paquete .ovpn que usará el cliente para conectarse. Para ello se crea igual que el certificado de servidor, pero en el tipo se debe poner **User Certificate** y su **common name** debe coincidir con el del usuario.

The screenshot shows the OPNsense web interface under the 'System' > 'Trust' > 'Certificates' navigation path. The left sidebar has 'Certificates' selected. The main area displays a table of certificates:

In use	Description	Issuer	Purpose	Name	Valid from	Valid to	Commands
<input type="checkbox"/>	Web GUI TLS certificate	self-signed	id-kp-serverAuth	/CN=OPNsense.localdomain/C=NL/ST=Zuid-Holland/L=... May 25, 2025 3:03 AM	May 25, 2025 3:03 AM	Jun 26, 2026 3:03 AM	
<input type="checkbox"/>	Web GUI TLS certificate	self-signed	id-kp-serverAuth	/CN=OPNsense.localdomain/C=NL/ST=Zuid-Holland/L=... May 25, 2025 3:09 AM	May 25, 2025 3:09 AM	Jun 26, 2026 3:09 AM	
<input type="checkbox"/>	certificado del servidor	self-signed	id-kp-serverAuth	/C=ES/ST=SEVILLA/L=ECIJA/O=IES LUIS VELEZ DE GUEV... May 25, 2025 6:53 AM	May 25, 2025 6:53 AM	Jun 26, 2026 6:53 AM	

Page navigation buttons: < < 1 > >.

Message: Showing 1 to 3 of 3 entries.

Edit Certificate

User Name/Subject

Key

Type: Client Certificate
Key type: RSA-2048
Digest Algorithm: SHA256
Issuer: CA-VPN
Lifetime (days): 397

General

Country Code: Netherlands
State or Province: SPAIN
City: ECIJA
Organization: IES LUIS VELEZ DE GUEVARA
Organizational Unit:
Email Address: guillelodelatorre91@gmail.com
Common Name: Administrator
OCSP uri:

Alternative Names

Output (PEM format)

Cancel Save

Finaliza pulsando **Save** para guardar los cambios.

Al crear el certificado con el mismo nombre que el usuario se vincula el nuevo certificado generado automáticamente a ese usuario y se puede ver que está generado por la CA VPN creada anteriormente.

The screenshot shows the OPNsense web interface with the URL <https://192.168.1.101/ui/trust/cert>. The left sidebar is collapsed, and the main content area is titled 'System: Trust: Certificates'. A table lists four certificates:

In use	Description	Issuer	Purpose	Name	Valid from	Valid to	Commands
<input type="checkbox"/>	Web GUI TLS certificate	self-signed	id-lp-serverAuth	/CN=OPNsense.localdomain/C=NL/ST=Zuid-Holland/L=...	May 25, 2025 3:03 AM	Jun 26, 2026 3:03 AM	<i>(edit)</i> <i>(trash)</i> <i>(copy)</i> <i>(details)</i>
<input checked="" type="checkbox"/>	Web GUI TLS certificate	self-signed	id-lp-serverAuth	/CN=OPNsense.localdomain/C=NL/ST=Zuid-Holland/L=...	May 25, 2025 3:09 AM	Jun 26, 2026 3:09 AM	<i>(edit)</i> <i>(trash)</i> <i>(copy)</i> <i>(details)</i>
<input checked="" type="checkbox"/>	cert-server-VPN	CA-VPN	id-lp-serverAuth	/C=NL/ST=SPAIN/L=ECIJA/O=IES LUIS VELEZ DE GUEVA...	May 25, 2025 7:46 AM	Jun 26, 2026 7:46 AM	<i>(edit)</i> <i>(trash)</i> <i>(copy)</i> <i>(details)</i>
<input type="checkbox"/>	user-Administrator	CA-VPN	id-lp-clientAuth	/C=NL/ST=SPAIN/L=ECIJA/O=IES LUIS VELEZ DE GUEVA...	May 25, 2025 8:00 AM	Jun 26, 2026 8:00 AM	<i>(edit)</i> <i>(trash)</i> <i>(copy)</i> <i>(details)</i>

Showing 1 to 4 of 4 entries

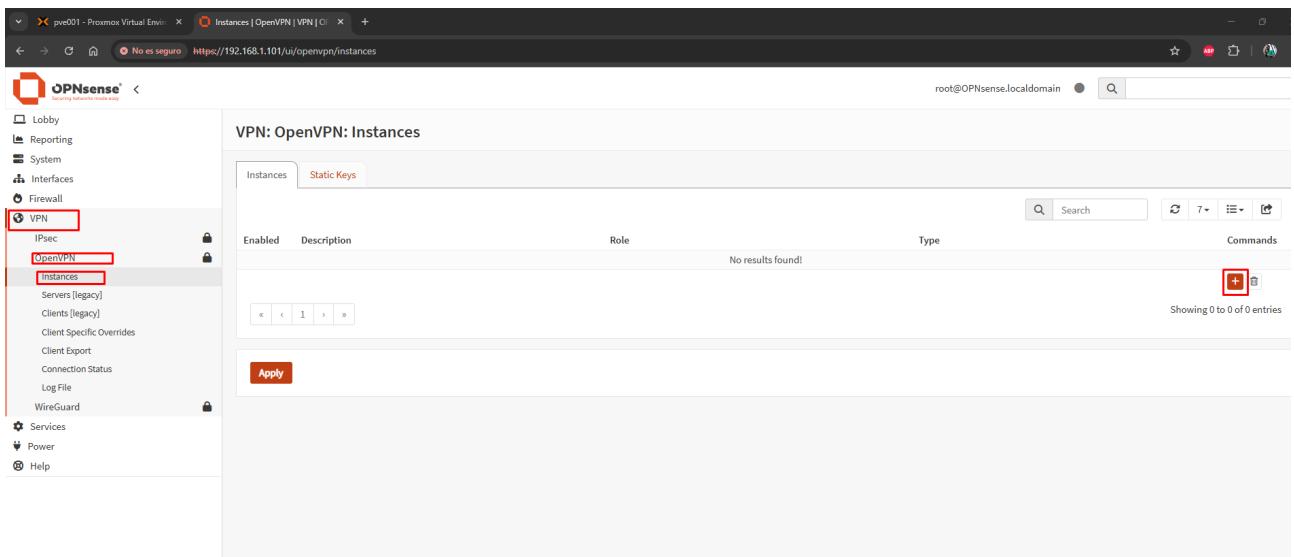
En caso de que no aparezca vinculado automáticamente ir a **System > Access > Users**, hacer clic en el icono del lápiz junto al usuario Administrador. En el campo Certificate, selecciona cert-Administrador.)

A8.3.5. Creación de la instancia del servidor OpenVPN

Una vez configurado el servidor OpenVPN a través del asistente, es necesario crear manualmente una instancia operativa que se asocie al servicio. Aunque el asistente configura correctamente las reglas del cortafuegos necesarias para el funcionamiento, no crea automáticamente la instancia del servidor, por lo que este paso es obligatorio para que la VPN funcione correctamente.

Para ello, se accede a la sección **VPN > OpenVPN > Instances**, donde se puede añadir una nueva instancia que actúe como servidor, definiendo los parámetros esenciales como el puerto, protocolo y certificado previamente configurado. Esta instancia es la que finalmente permitirá gestionar las conexiones remotas activas a través del túnel VPN.

Para crear una instancia ir a **VPN > OpenVPN > Instances**, vemos que no hay ninguna instancia relacionada con nuestro servidor VPN y proceder a añadir una nueva instancia pulsando en botón de añadir (+).



Aparecerá un formulario de configuración de la instancia. En este formulario debemos completar algunos campos clave:

Role: seleccionamos Server ya que esta instancia actuará como servidor VPN.

Description: se puede indicar un nombre descriptivo como por ejemplo instancia-lab-teletrabajo.

Protocol: dejamos UDP, que es el recomendado para conexiones OpenVPN.

Port number: utilizamos el puerto estándar 1194.

Type: dejamos TUN, que es el modo de túnel más común.

Server (IPv4): indicamos la IP del extremo del túnel, por ejemplo 10.8.0.1.

Topology: dejamos subnet.

Certificate: seleccionamos el certificado del servidor previamente creado, como cert-server-VPN.

Verify Client Certificate: lo dejamos en required para asegurar autenticación mediante certificados.

Edit Instance

advanced mode full help 

General Settings

Role	Server
Description	instancia-lab-teletrabajo
Enabled	<input checked="" type="checkbox"/>
Protocol	UDP
Port number	1194
Bind address	
Type	TUN
Server (IPv4)	10.8.0.1
Server (IPv6)	
Topology	subnet

Trust

Certificate	cert-server-VPN
Verify Remote Certificate	<input type="checkbox"/>
Certificate Revocation List	None
Verify Client Certificate	required

Cancel Save

Una vez llenado el formulario, hacemos clic en Save para guardar la configuración.

Tras ello, volveremos a la vista de instancias donde ya aparecerá la que acabamos de crear. Para que la instancia se active correctamente, es importante hacer clic en el botón Apply.

The screenshot shows the OPNsense web interface under the 'VPN' section, specifically the 'OpenVPN' tab. On the left sidebar, 'Instances' is selected. The main panel is titled 'VPN: OpenVPN: Instances' and shows a table with one entry:

Enabled	Description	Role	Type	Commands
<input checked="" type="checkbox"/>	instancia-lab-teletrabajo	Server	TUN	Edit Delete Static Keys

A red box highlights the 'Apply' button at the bottom of the table.

A8.3.6. Exportar perfil de conexión para el cliente OpenVPN

Una vez finalizada la configuración del servidor OpenVPN, el siguiente paso es generar el archivo de configuración que utilizarán los clientes para conectarse a la VPN.

Para ello, accedemos a: **VPN > OpenVPN > Client Export**. En la parte superior de la página nos aseguramos de seleccionar la instancia del servidor creada previamente, en este caso **lab-teletrabajo** en el desplegable **Remote Access Server**, en **Export type** elegir la opción **archive**, **Port :1194**.

The screenshot shows the OPNsense web interface under the 'VPN' section, specifically the 'Client Export' tab. The left sidebar shows 'Client Export' is selected. The main panel is titled 'VPN: OpenVPN: Client Export' and contains the following configuration fields:

- Remote Access Server:** lab-teletrabajo UDP:1194
- Export type:** Archive
- Hostname:** (empty input field)
- Port:** 1194
- Use random local port:**
- P12 Password/confirm:** (two empty input fields)
- Advanced Options:**
 - Validate server subject
 - Windows Certificate System Store
 - Disable password save
 - Enable static challenge (OTP)
 - Custom config

Below the configuration fields, there is a section for 'Accounts / certificates' which lists 'cert-server-VPN' and 'user-Administrator'. To the right of this section, there is a 'Linked user' section with an 'Administrator' entry.

Se recomienda dejar el resto de los valores por defecto, salvo que se desee personalizar el puerto, añadir contraseña al certificado o activar funciones adicionales como el almacenamiento de contraseña o configuración estática (OTP).

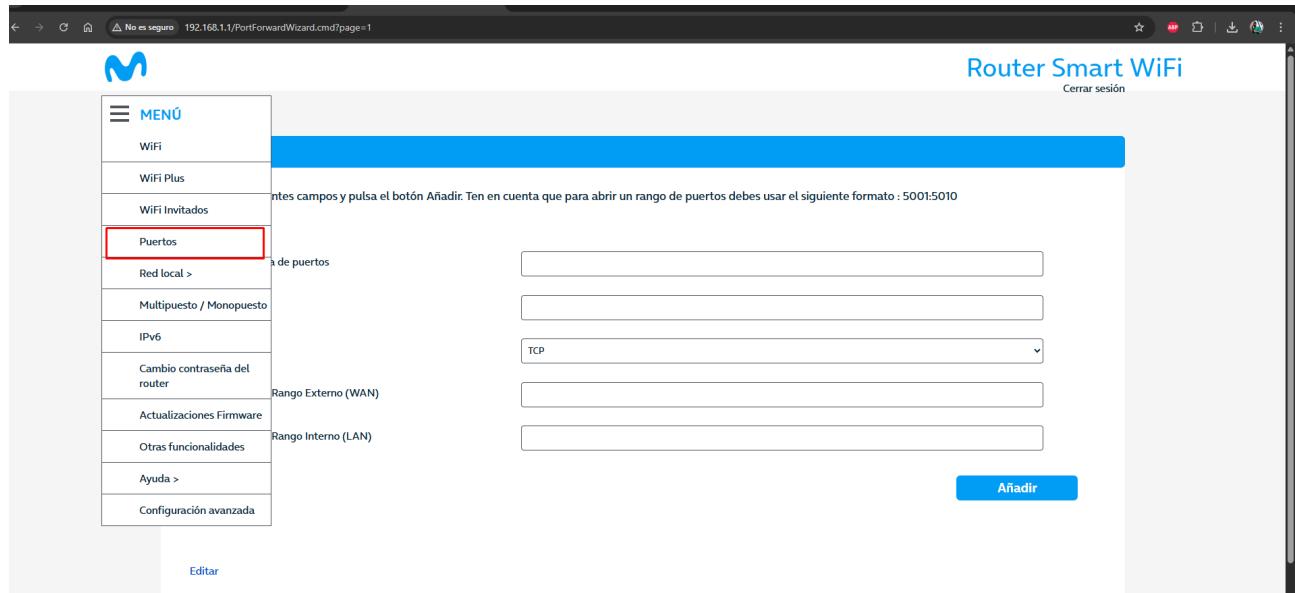
Al final del panel encontraremos el listado de usuarios con certificados válidos. En este ejemplo, buscamos al usuario Administrator y hacemos clic sobre el icono de la nube correspondiente a **user-Administrator** para descargar el archivo de configuración de perfil de conexión para el cliente OpenVPN.

A8.4. Redireccionamiento de puertos en el router de borde

Para permitir que las conexiones entrantes desde Internet lleguen correctamente al servidor VPN ubicado dentro de la red local, es necesario realizar un reenvío de puertos (port forwarding) en el router de borde, en este caso un router Movistar Smart WiFi.

Para ello acceder a la interfaz web del router abriendo un navegador e introduciendo la dirección <http://192.168.1.1>. Iniciar sesión con las credenciales de administración del router.

En el menú lateral izquierdo, selecciona Puertos.



Rellena el formulario con los siguientes datos y pulsa en **Añadir**.

Nombre de la regla: conexionVPN

Dirección IP: 192.168.1.101 (dirección local del servidor OPNsense)

Protocolo: UDP

Puerto externo (WAN): 1194

Puerto interno (LAN): 1194

The screenshot shows a web-based interface for managing port forwarding rules. At the top, there's a header bar with the title 'Puertos' (Ports). Below it, a message says: 'Rellena los siguientes campos y pulsa el botón Añadir. Ten en cuenta que para abrir un rango de puertos debes usar el siguiente formato : 5001:5010'. The main area contains several input fields and dropdown menus:

- 'Nombre regla de puertos': An empty text input field.
- 'Dirección IP': An empty text input field.
- 'Protocolo': A dropdown menu set to 'TCP'.
- 'Abrir Puerto/Rango Externo (WAN)': An empty text input field.
- 'Abrir Puerto/Rango Interno (LAN)': An empty text input field.

At the bottom right of this section is a blue 'Añadir' (Add) button. Below this section, there's a table titled 'Editar' (Edit) showing one existing rule:

Nombre	Protocolo	Puerto/Rango Externo	Puerto/Rango Interno	Dirección IP	Activar
conexionVPN	UDP	1194:1194	1194:1194	192.168.1.101	<input checked="" type="checkbox"/>

Below the table, it says '1/1'.

Asegurarse de que la **casilla de activación** esté marcada como **ON** en la tabla de reglas creadas.

A8.5. Prueba de conexión

Con la infraestructura de red, el servidor VPN y las reglas de cortafuegos correctamente configuradas, es el momento de validar todo el sistema con una prueba real. El objetivo de esta fase es comprobar que un usuario externo puede:

- Establecer conexión VPN con el servidor OPNsense desde fuera de la red local.
- Autenticarse correctamente con su certificado y credenciales de dominio.
- Acceder a su puesto de trabajo virtual (VDI) mediante Remote Desktop Protocol (RDP).

Estas pruebas son fundamentales para garantizar que la solución de acceso remoto está operativa y que cumple con los requisitos de seguridad y funcionalidad esperados.

Requisitos previos para realizar la prueba:

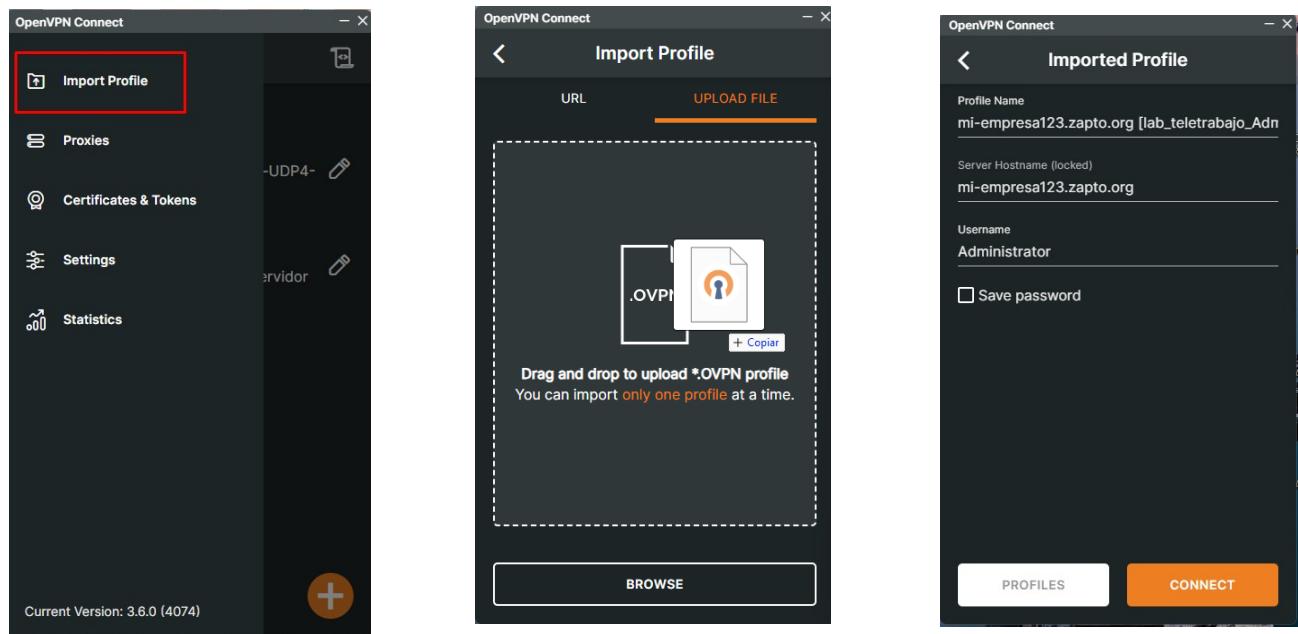
- **Archivo .ovpn exportado** y configurado en el cliente OpenVPN.
- **Redirección del puerto 1194 UDP** en el router correctamente activa.

- **Usuario** del dominio **habilitado** y con permisos para **iniciar sesión en su VDI** vía RDP.

- El equipo VDI encendido y accesible dentro de la red interna.

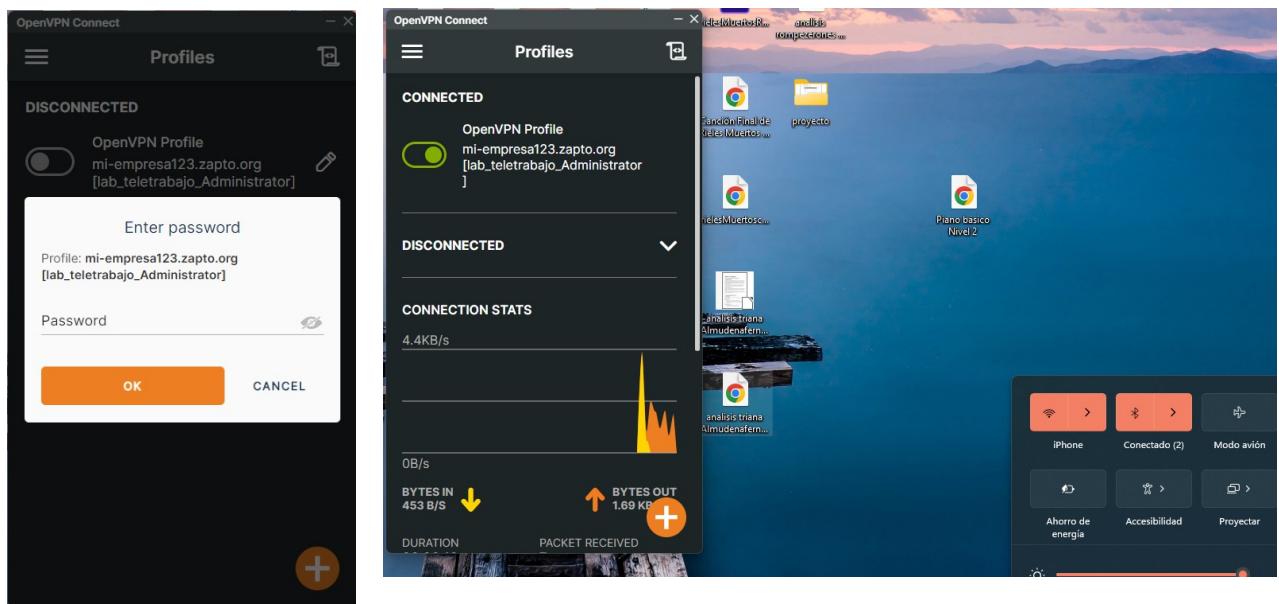
A8.5.1. Prueba de conexión VPN

Se abre la aplicación OpenVPN Connect y se selecciona la opción Import Profile. A continuación, se carga el archivo .ovpn exportado desde el servidor OPNsense, bien arrastrándolo o seleccionándolo manualmente. Una vez cargado el archivo, carga los datos de configuración de este y pulsar en **Connect**.



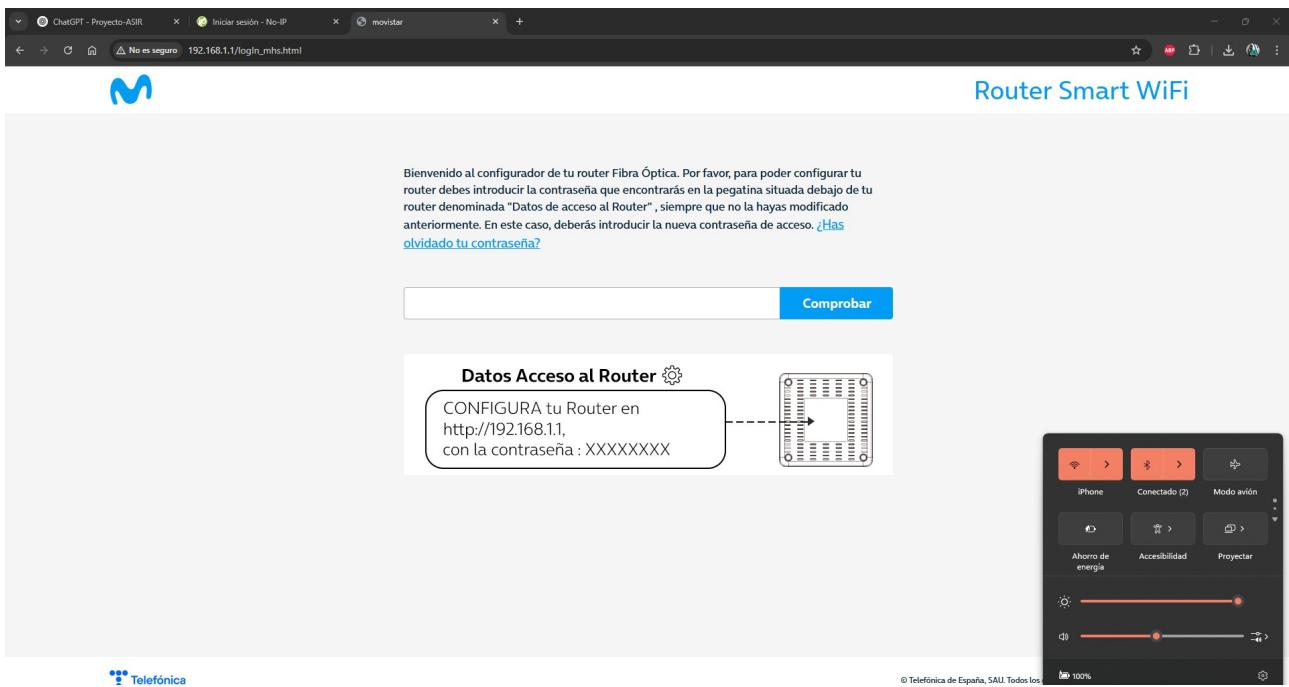
Nos solicita la contraseña del usuario (este es el **usuario creado en el servidor VPN OPNsense**).

Tras introducirla correctamente ya aparece el perfil de conexión en nuestro cliente VPN para dar en el interruptor y Activar la conexión VPN de ese perfil.



Como se puede apreciar en la captura anterior, el PC está conectado a la red compartida de mi teléfono móvil y se ha podido establecer la conexión VPN.

Esta prueba demuestra que el cliente ha podido alcanzar y autenticar contra el servidor VPN a través de Internet usando el nombre de dominio dinámico (mi-empresa123.zapto.org), lo cual valida que tanto el servicio No-IP como el enrutamiento NAT/port forwarding y la instancia OpenVPN están funcionando correctamente y podemos acceder a recursos de dentro de la red de la empresa como por ejemplo la Web de configuración del router.



A.8.5.2. Prueba de conexión a VDI con usuario autorizado.

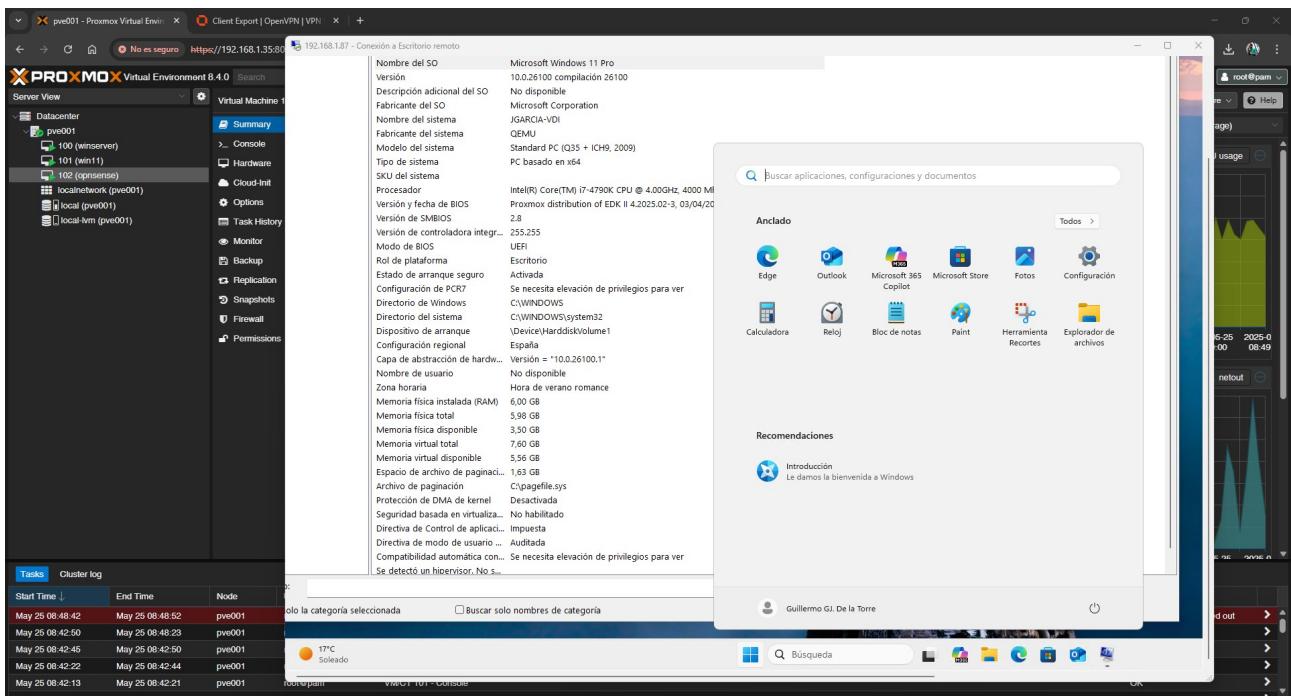
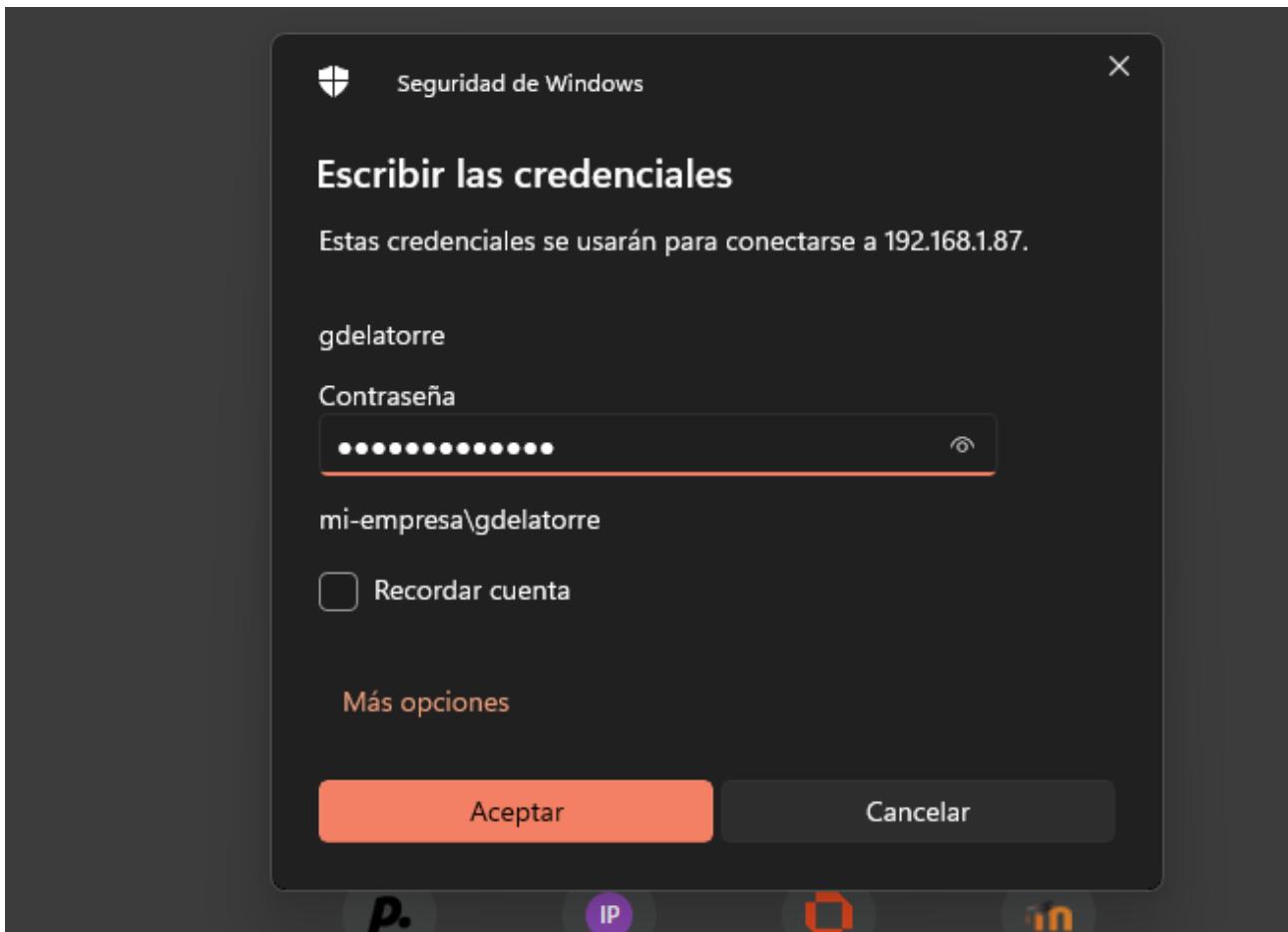
Una vez establecida la conexión VPN correctamente, se procede a comprobar que un usuario del dominio con permisos de acceso puede iniciar sesión en su escritorio virtual remoto (VDI). Para esta prueba, se ha utilizado el usuario del dominio gdelatorre, perteneciente al grupo admins, tal y como se definió en las pruebas previas de acceso local mediante GPO.

Desde el equipo remoto, y tras importar y activar el perfil .ovpn, se ha accedido por Escritorio Remoto (RDP) a la IP interna asignada a la VDI (en este caso, 192.168.1.87), introduciendo las credenciales de dominio correspondientes.

Como se observa en la siguiente captura, el acceso se ha realizado correctamente, permitiendo así validar que:

- La comunicación entre cliente y servidor VPN es funcional.
- La política de acceso definida por GPO está operativa también a través del túnel VPN.

El usuario remoto puede utilizar su escritorio virtual de forma transparente como si estuviese dentro de la red local de la empresa.



A.8.5.3. Conclusión de las pruebas

Tras realizar las pruebas de conexión VPN desde una red externa, y posteriormente el acceso remoto a la máquina virtual Windows 11 del entorno VDI, se confirma que toda la infraestructura configurada funciona correctamente.

El perfil del usuario Administrator, generado y exportado desde OPNsense, ha sido importado sin problemas en el cliente OpenVPN Connect, estableciendo la conexión contra el servidor remoto mediante el dominio configurado en No-IP y la redirección de puertos del router de borde.

Posteriormente, se ha accedido vía RDP a la máquina virtual con un usuario del dominio autorizado, demostrando que las políticas de acceso establecidas en el servidor y aplicadas vía GPO se cumplen también en un escenario remoto a través de la VPN.

Todo ello valida que la infraestructura VPN está operativa, ofrece acceso seguro a los recursos internos, y respeta las políticas de seguridad definidas en el dominio.