

# FASE 2 PROYECTO ASIX2A **GRUP1**

Nicolas Gomariz, Albert Martínez

23/10/2025



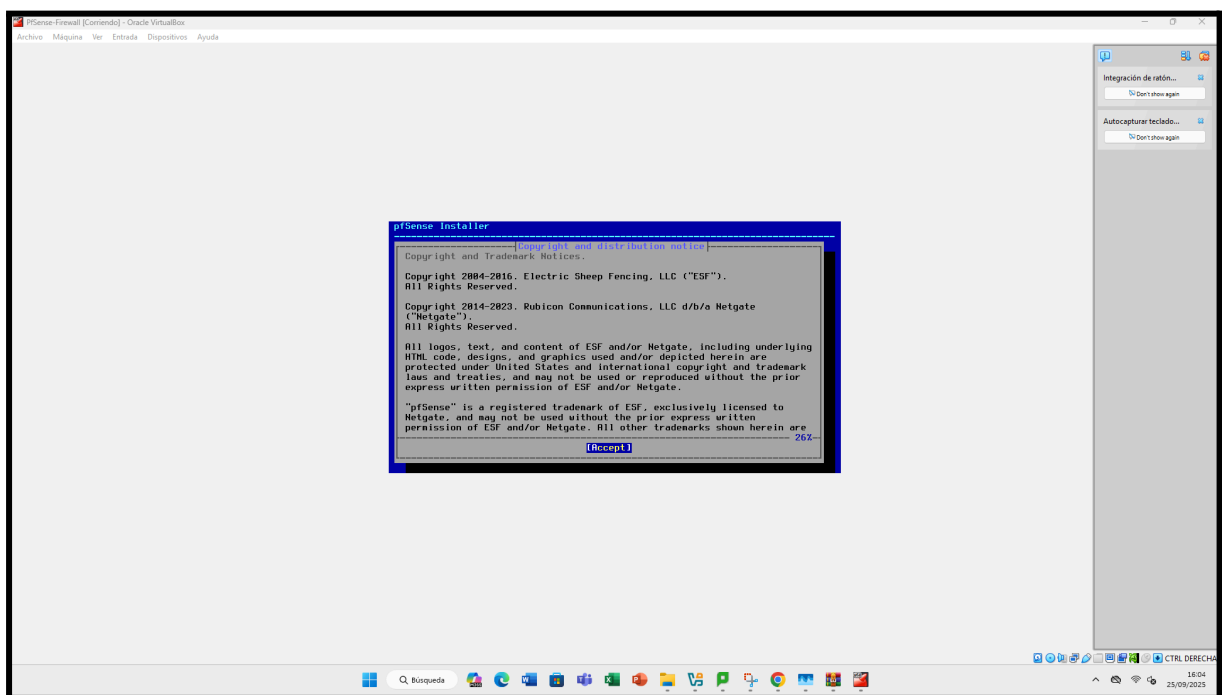
# INDEX

<b>Instalacio pFsense</b>	<b>3</b>
Comprobación de instalación de pfSense	10
<b>DHCP</b>	<b>10</b>
Demostración DHCP	12
<b>DNS</b>	<b>13</b>
Demostración DNS	16
<b>Active directory</b>	<b>16</b>
Demostracion DNS	19
<b>SMB</b>	<b>20</b>
Demostración SMB	27
<b>RDP</b>	<b>27</b>
Demostración RDP	28
<b>FTP</b>	<b>28</b>
Demostración FTP	33
<b>SSH</b>	<b>34</b>
Demostración SSH	35
<b>VPN</b>	<b>35</b>
Demostración VPN	39
<b>AD SG</b>	<b>39</b>
Demostración AD SG	39

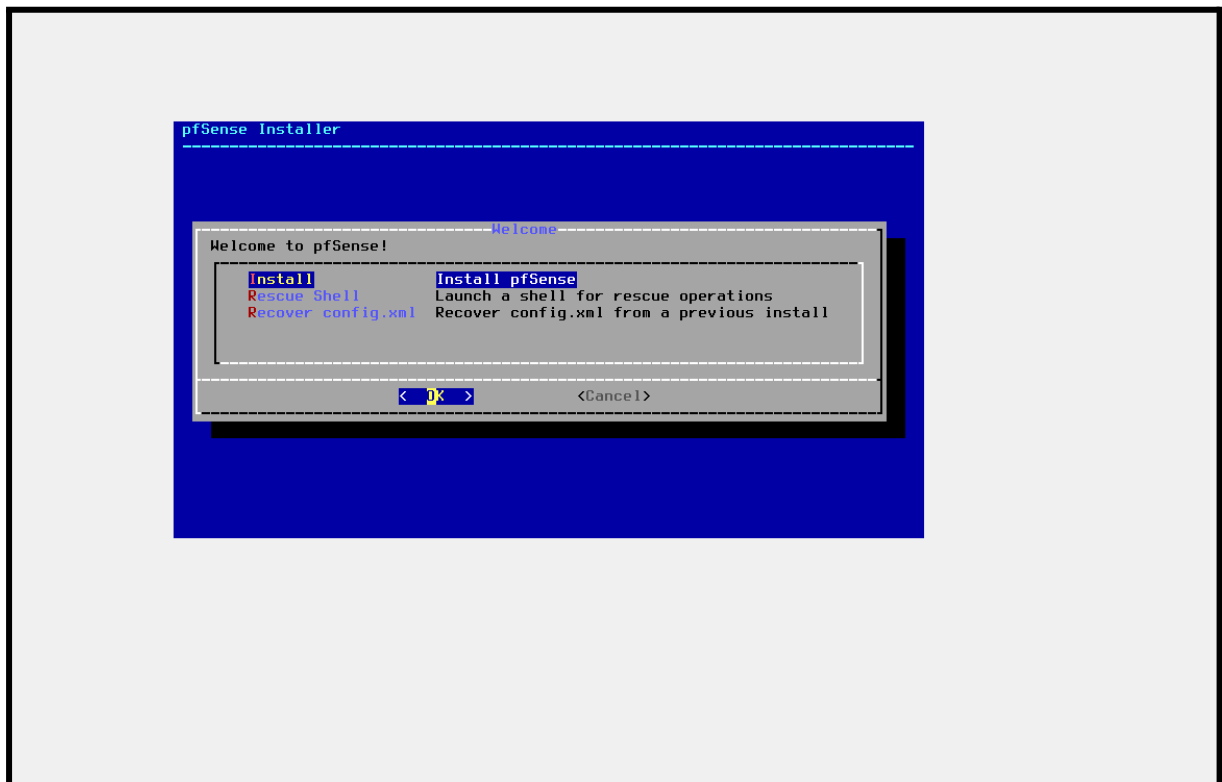


# Instalacio pFsense

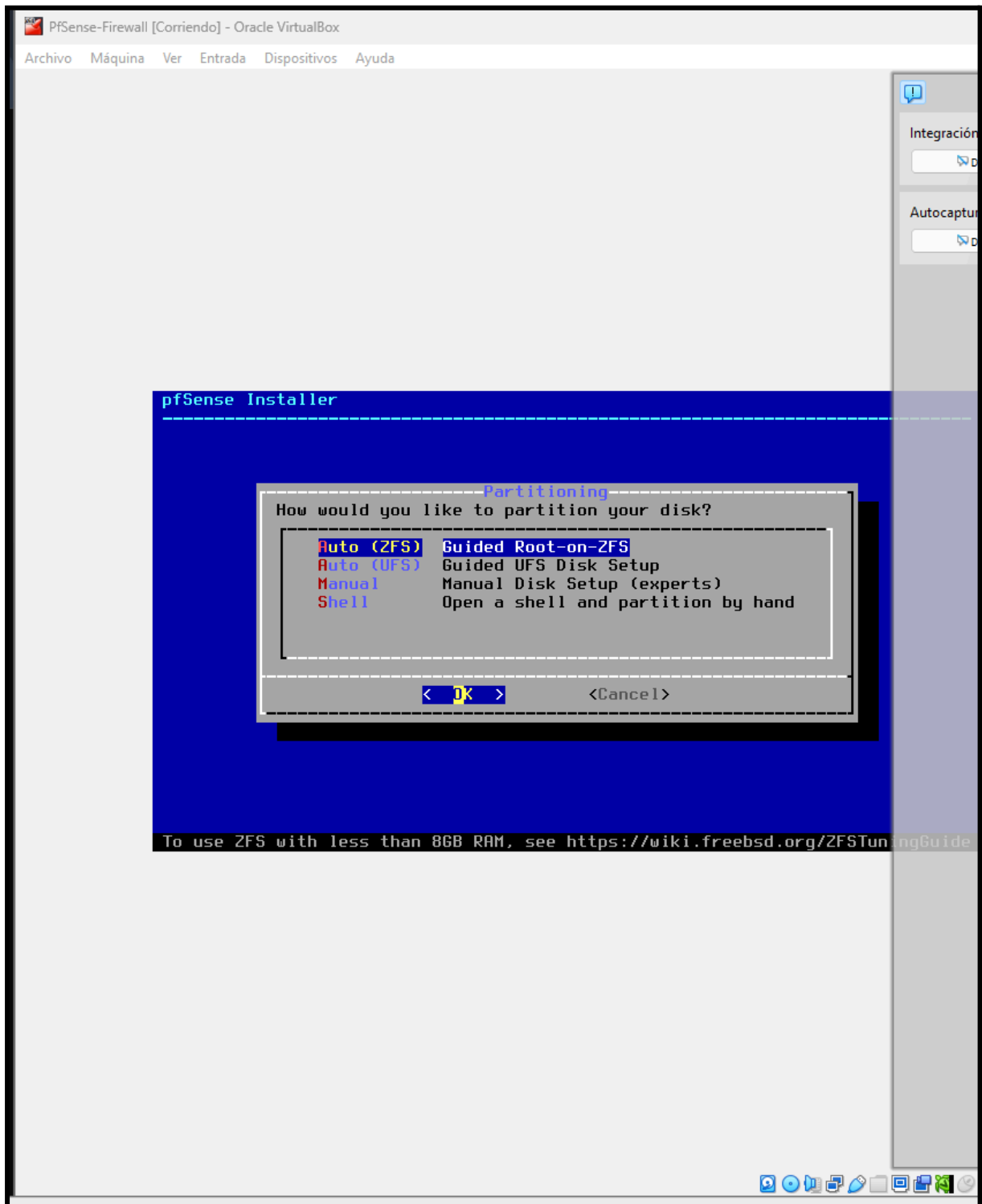
Inicio de la instalación y configuración básica de pfSense.



Confirmamos para iniciar el proceso de instalación.

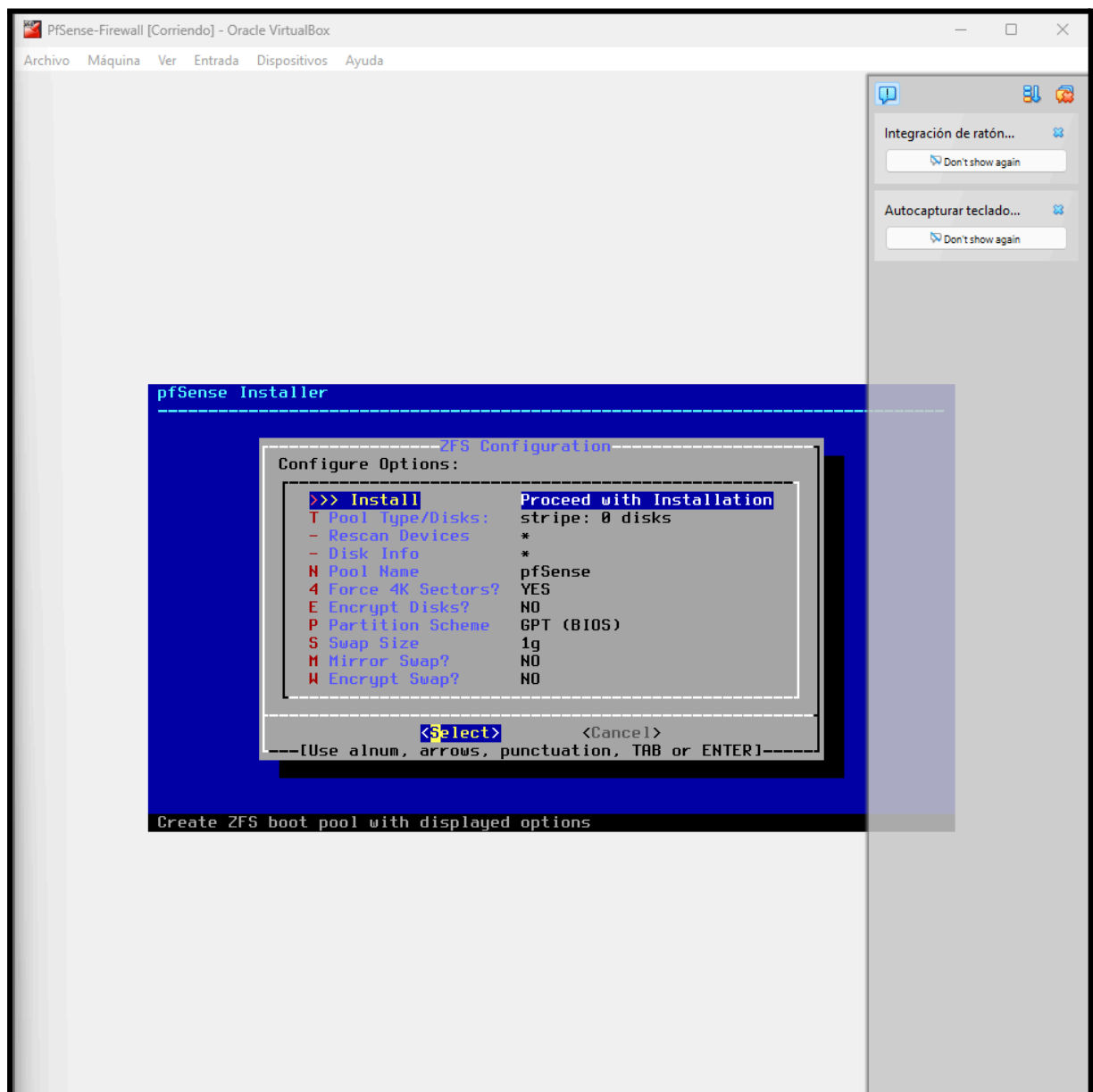


Selección de la unidad de disco para la instalación.



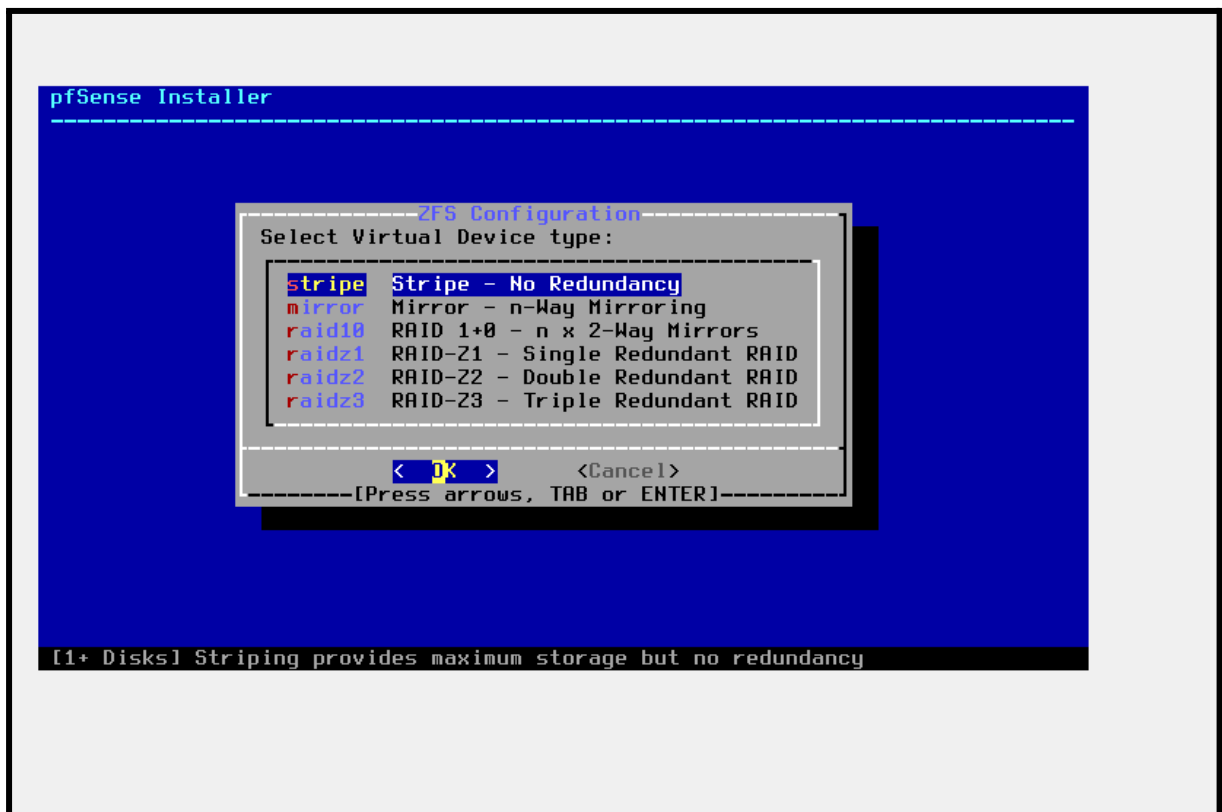


Confirmación e inicio de la instalación en el disco.

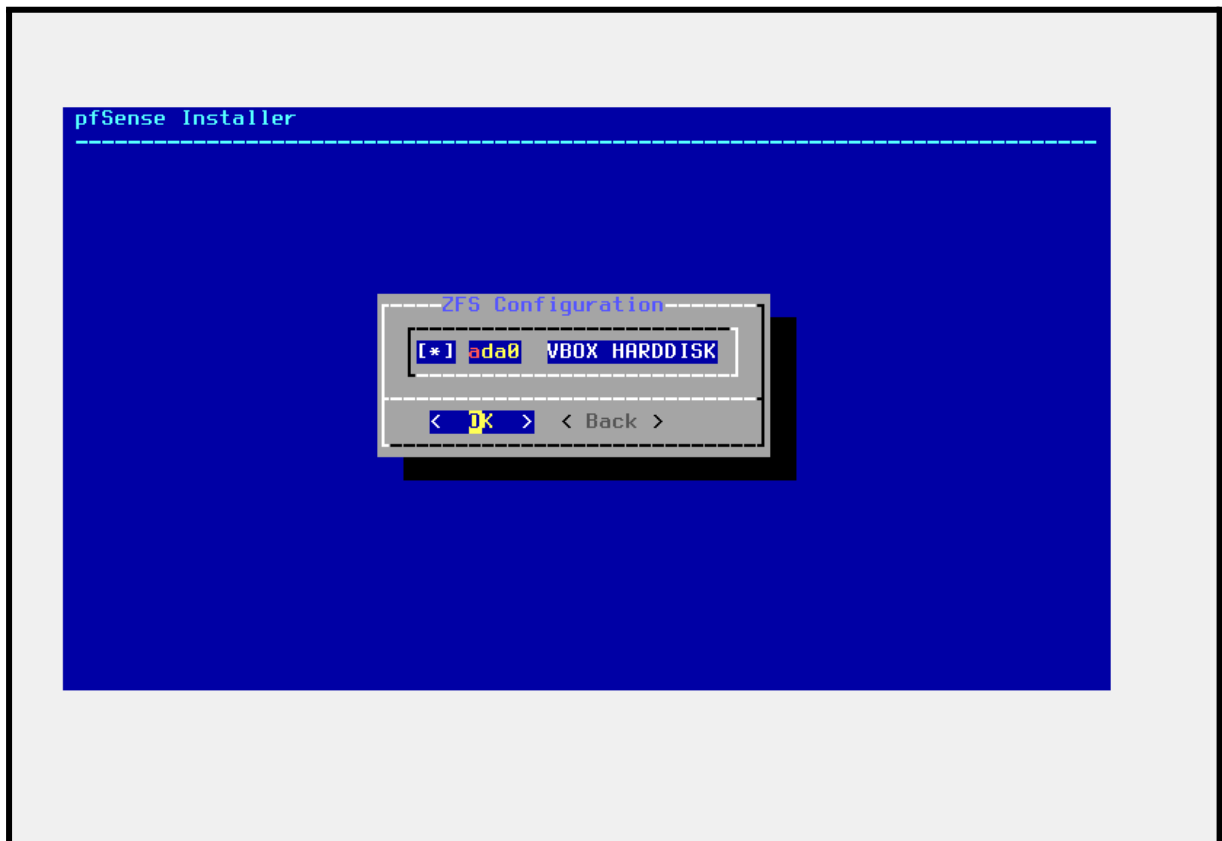




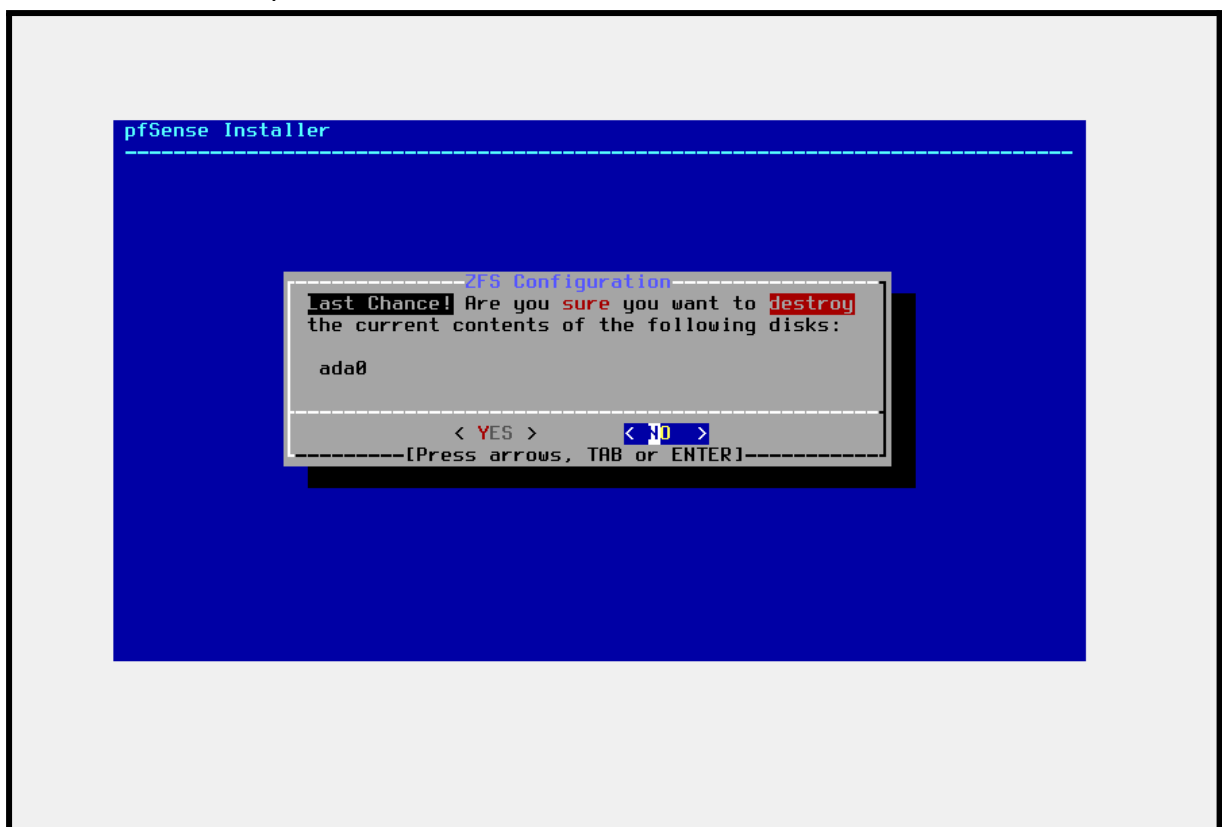
## Selección del dispositivo de instalación



## Selección del disco de destino para la instalación.



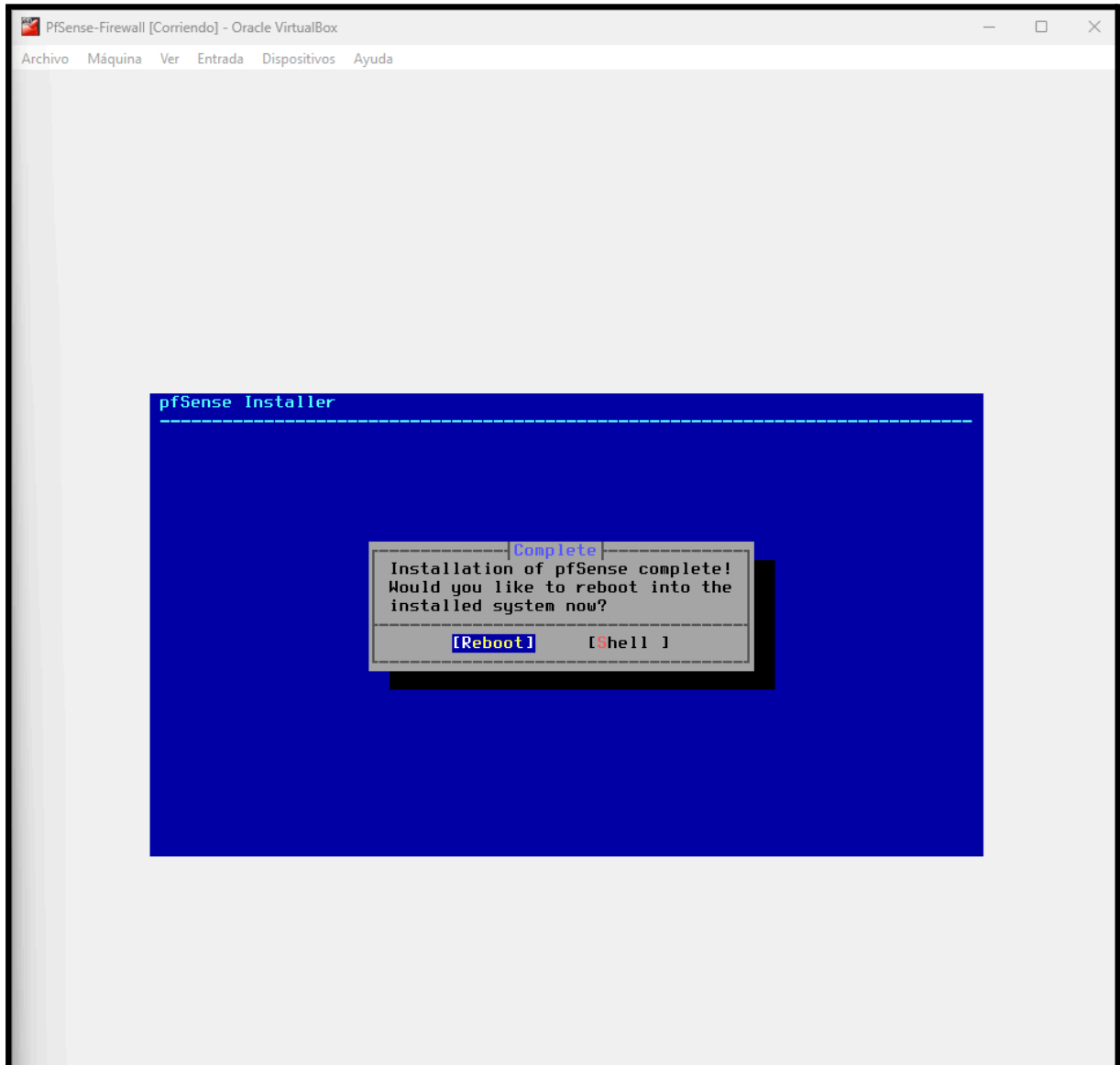
Nos da un aviso de que vamos a destruir el contenido del disco







Reinicio del sistema para completar la instalación.





Comprobación de instalación de pfSense

Instalación de pfSense completada exitosamente.

```
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: acdd558fd1d9c5dea10e

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
                v6/DHCP6: fd17:625c:f037:2:a00:27ff:fec2:e44c/
64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

DHCP



Metemos el rango de ips que queremos en nuestro DHCP

same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool	
<b>Subnet</b>	192.168.1.0/24
<b>Subnet Range</b>	192.168.1.1 - 192.168.1.254
<b>Address Pool Range</b>	<div><div>192.168.1.10</div><div>From</div><div>192.168.1.245</div><div>To</div></div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>
<b>Additional Pools</b>	<div><div>+ Add Address Pool</div><p>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</p></div>
Server Options	
<b>WINS Servers</b>	<div>WINS Server 1</div> <div>WINS Server 2</div>



## Demostración DHCP

Como vemos hemos configurado nuestro dhcp en la LAN

```
PfSense-Firewall (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Starting package OpenVPN Client Export Utility...done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (grup1NA.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: acdd558fd1d9c5dea10e

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on grup1NA ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.30.243.17/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
DMZ (opt1)    -> em2      -> v4: 192.168.4.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```



# DNS

Configuración de servidores DNS para la resolución de nombres.



### Server Options

**WINS Servers**

WINS Server 1

WINS Server 2

**DNS Servers**

192.168.1.1

8.8.8.8

DNS Server 3

DNS Server 4

### OMAPI

**OMAPI Port**

OMAPI Port

Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.

**OMAPI Key**

OMAPI Key

Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.

☐ Generate New Key  
Generate a new key based on the selected algorithm.

**Key Algorithm**

HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

### Other DHCP Options

**Gateway**

192.168.1.1

The default is to use the IP address of this firewall interface as the gateway. Specify an

Verificación del cambio de IP desde la consola (cmd).



```
Administrador: Símbolo del sistema
C:\>

:\Users\Administrador>IP A
IP" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

:\Users\Administrador>ip a
ip" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

:\Users\Administrador>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 3:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . : home.arpa
    Vínculo: dirección IPv6 local. . . : fe80::df5f:1333:1daf:6f24%16
    Dirección IPv4. . . . . : 192.168.1.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . : fe80::a00:27ff:fe5f:a0ac%16
```

Aquí creamos nuestro hostname para nuestro DNS y ponemos de nombre de hostname grup NA y ponemos los DNS de cloudflare. Esto se integrará a nuestro DHCP para cuando un dispositivo se integre en nuestra LAN le dé este DNS

System / General Setup

**System**

**Hostname**   
Name of the firewall host, without domain part.

**Domain**   
Domain name for the firewall.

Do not end the domain name with 'local' as the final part (Top Level Domain, TLD). The 'local' TLD is **widely used** by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

**DNS Server Settings**

**DNS Servers**

<input type="text" value="1.1.1.1"/> Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	<input type="text" value="grupNA"/> Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).
---	---

**Add DNS Server** [+ Add DNS Server](#)

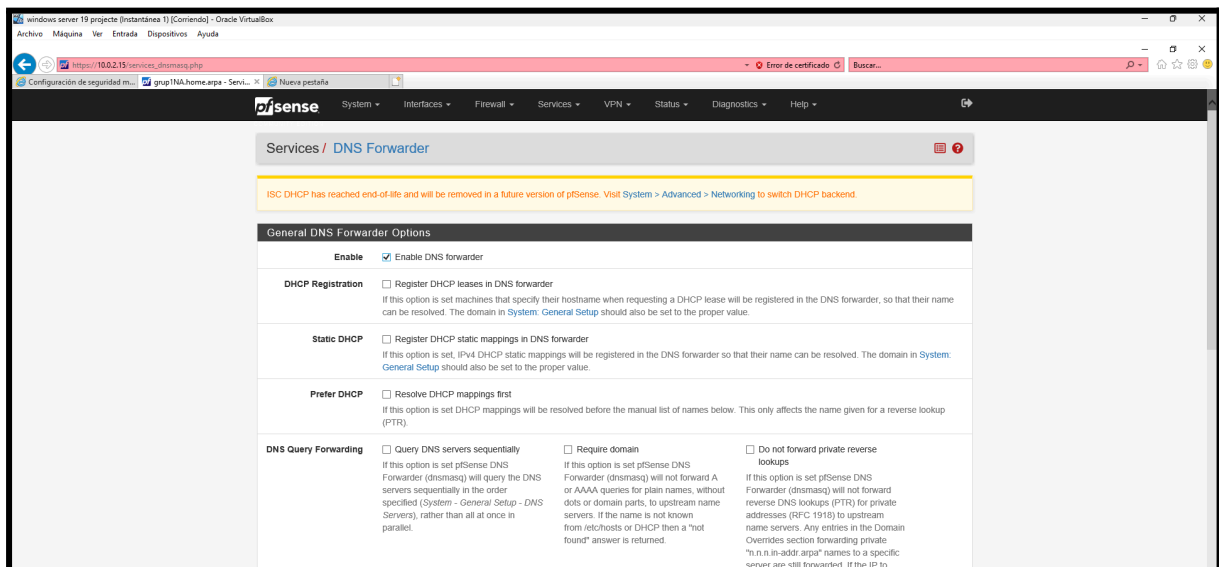
**DNS Server Override** ☒ Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server  
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

**DNS Resolution Behavior**   
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.



Configuramos el DNS con funciones de seguridad, incluyendo bloqueo de dominios maliciosos, encriptación DNS y registro de consultas para proteger y monitorear el tráfico de red.

Nos servirá para recibir las consultas DNS de nuestros dispositivos y reenviarlos a servidores DNS externos



## Demostración DNS

```
C:\Users\Administrador>nslookup
"nslookup" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Administrador>nslookup
Servidor predeterminado: grup1NA.home.arpa
Address: 192.168.1.1
```

## Active directory

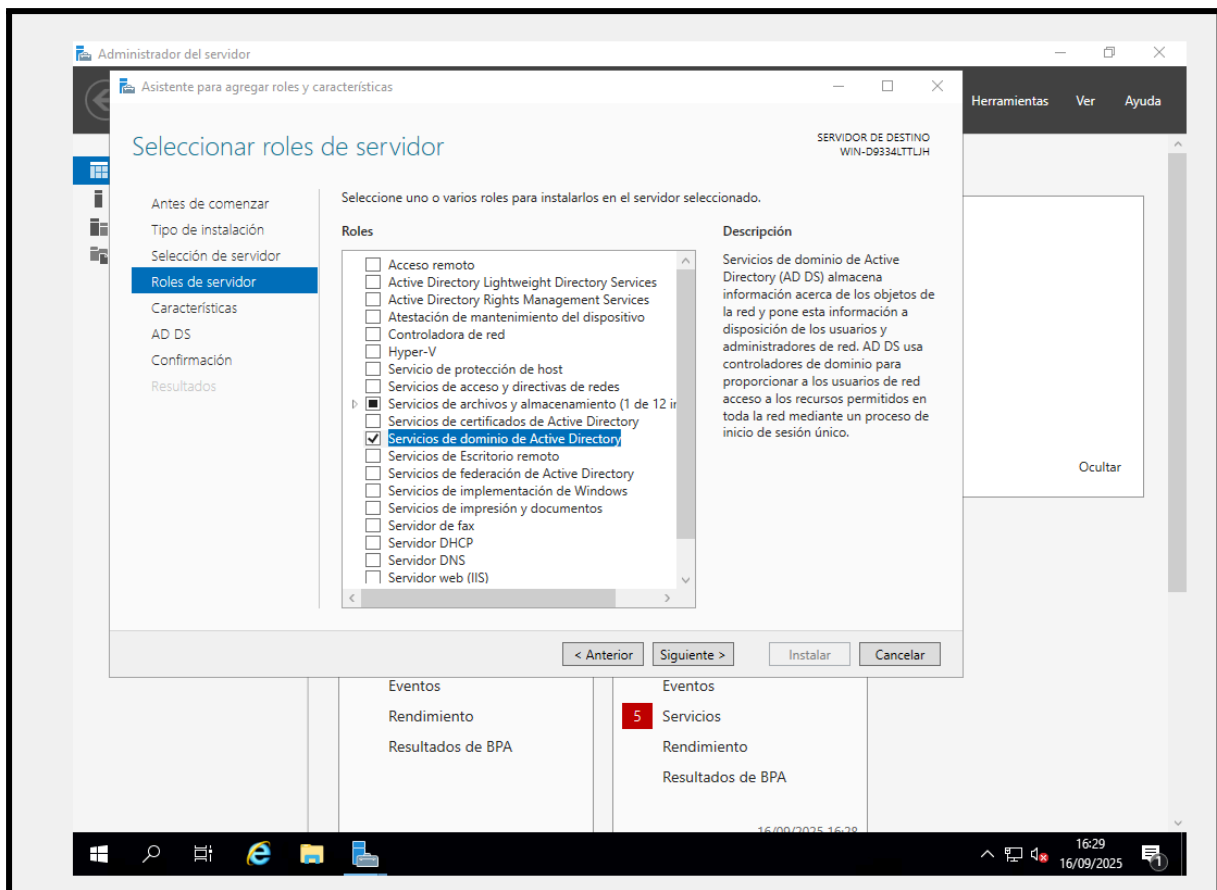
Desde el Administrador del Servidor:

- Abrimos el Administrador del Servidor desde el menú Inicio.
- Hicimos clic en "Agregar roles y características".



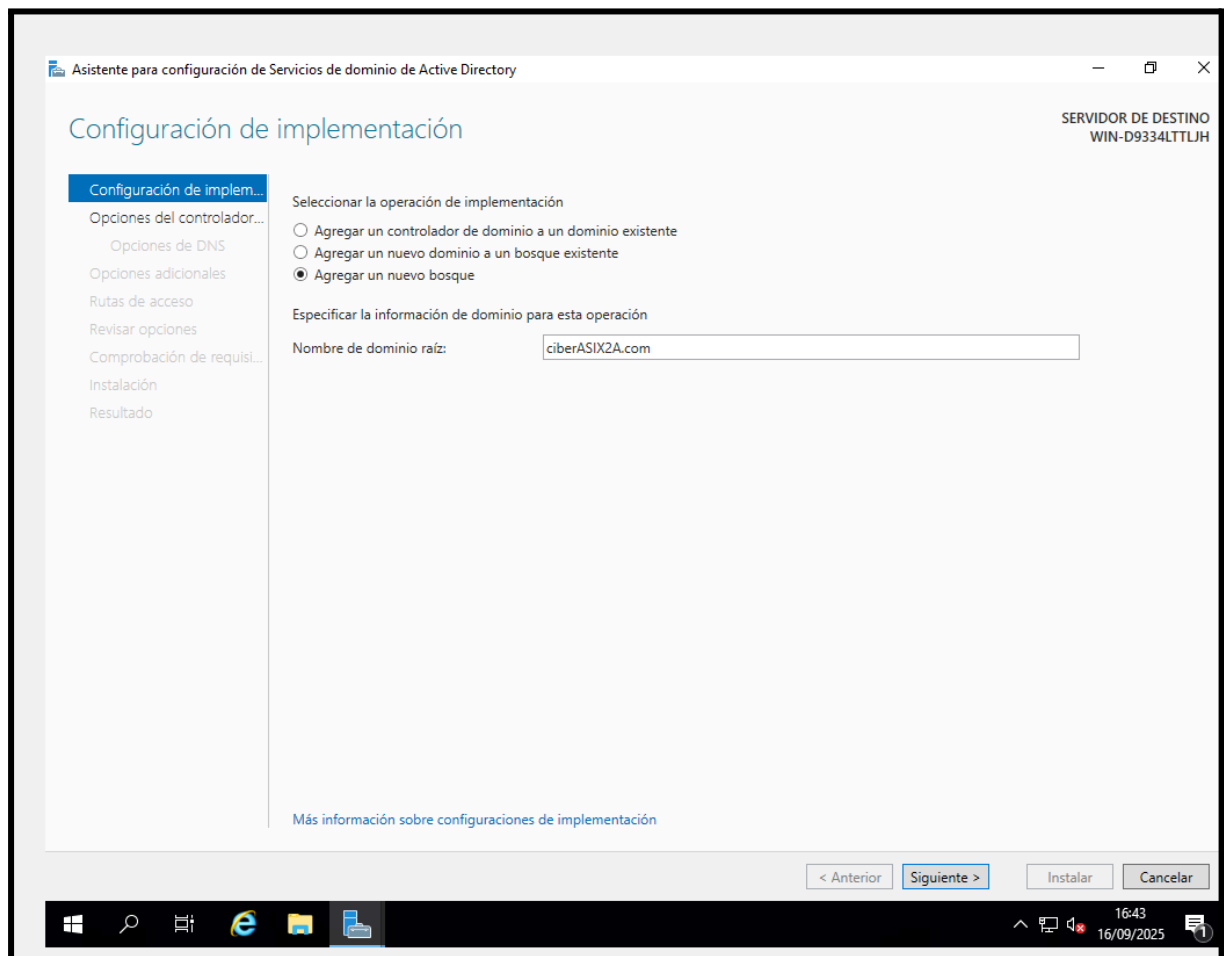


- En el asistente, seleccionamos la opción "Instalación basada en roles o características" y elegimos nuestro servidor destino.





En la configuración de implementación, seleccionamos "Agregar un nuevo bosque" y escribimos el nombre de dominio root: `ciberASIX.com`.





Establecimos una contraseña segura para el Modo de Restauración de Servicios de Directorio (DSRM). La anotamos en nuestro gestor de contraseñas seguro.

## Demostración DNS

Asistente para configuración de Servicios de dominio de Active Directory

OPCIONES DEL CONTROLADOR DE DOMINIO

SERVIDOR DE DESTINO  
WIN-D9334LTLJH

Configuración de implementación...  
**Opciones del controlador de dominio...**  
Opciones de DNS  
Opciones adicionales  
Rutas de acceso  
Revisar opciones  
Comprobación de requisitos...  
Instalación  
Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio

☒ Servidor de Sistema de nombres de dominio (DNS)  
☒ Catálogo global (GC)  
☐ Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña: .....

Confirmar contraseña: .....

Más información sobre opciones del controlador de dominio

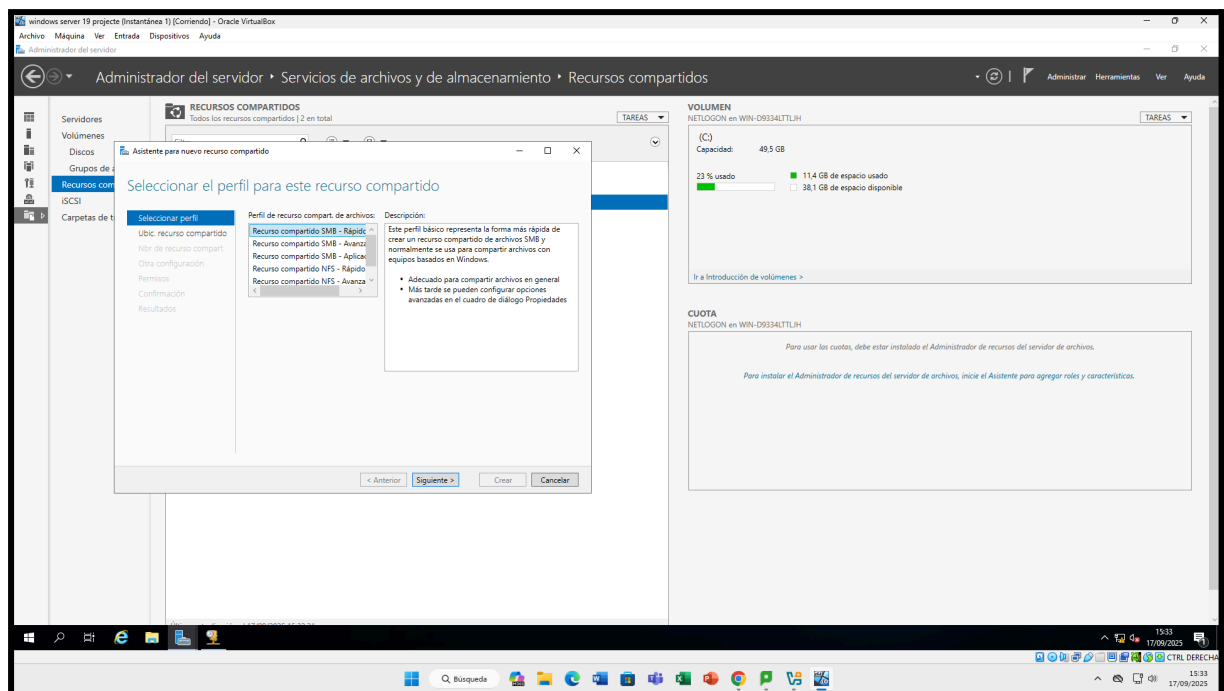
< Anterior Siguiente > Instalar Cancelar

16:44  
16/09/2025



# SMB

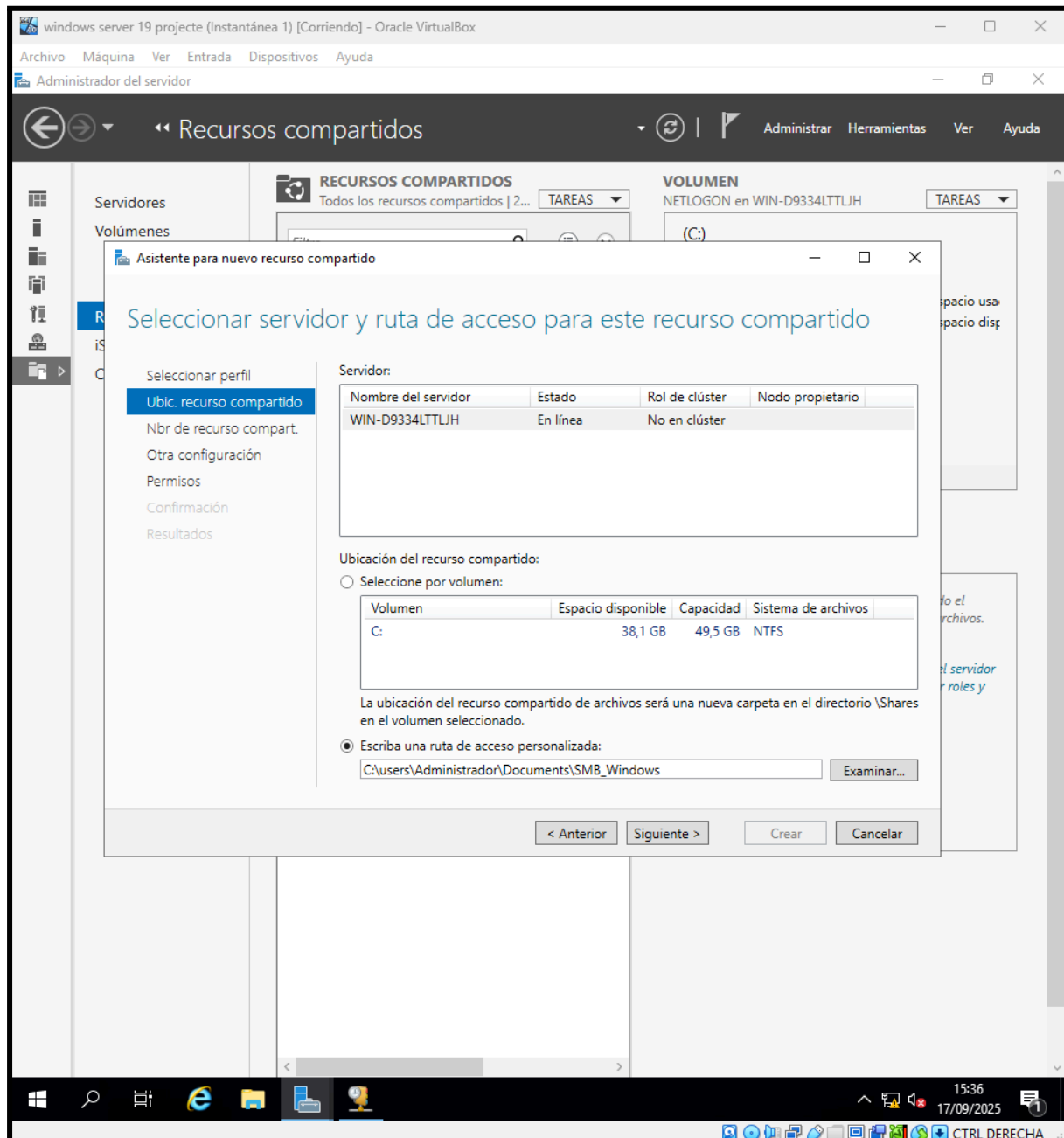
Creamos un recurso compartido con SMB





Seleccionamos nuestro servidor de la lista.

Especificamos la ruta de acceso a la carpeta



Y le añadimos los permisos necesarios



Windows Server 19 projecte (Instantánea 1) [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Administrador del servidor

Recursos compartidos

Administrar Herramientas Ver Ayuda

Servidores

Volumenes

RECURSOS COMPARTIDOS

Todos los recursos compartidos | 2... TAREAS

VOLUMEN

NETLOGON en WIN-D9334LTLJH TAREAS

(C:)

Asistente para nuevo recurso compartido

Especificar permisos para controlar el acceso

Seleccionar perfil

Ubic. recurso compartido

Nbr de recurso compart.

Otra configuración

Permisos

Confirmación

Resultados

Los permisos para obtener acceso a los archivos de un recurso compartido se establecen mediante una combinación de permisos de carpeta, permisos de recurso compartido y, opcionalmente, una directiva de acceso central.

Permisos de los recursos compartidos: Todos tienen control total

Permisos de carpeta:

Tipo	Entidad de seguridad	Acceso	Se aplica a
Permitir	CIBERASIX2\Administrador	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos

Personalizar permisos...

< Anterior Siguiente > Crear Cancelar

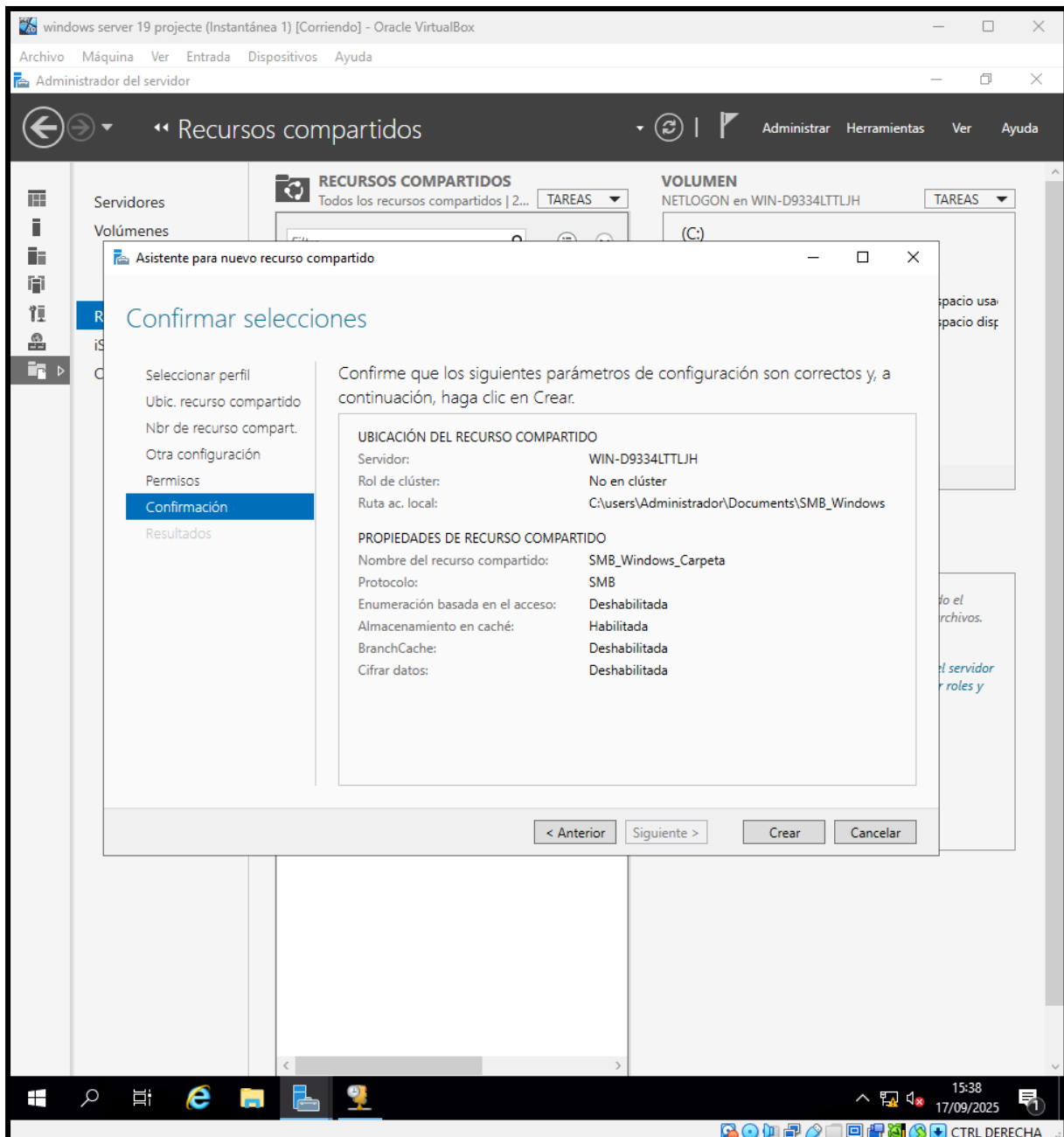
Administrador del servidor

Asistente para nuevo recurso c...

15:37 17/09/2025



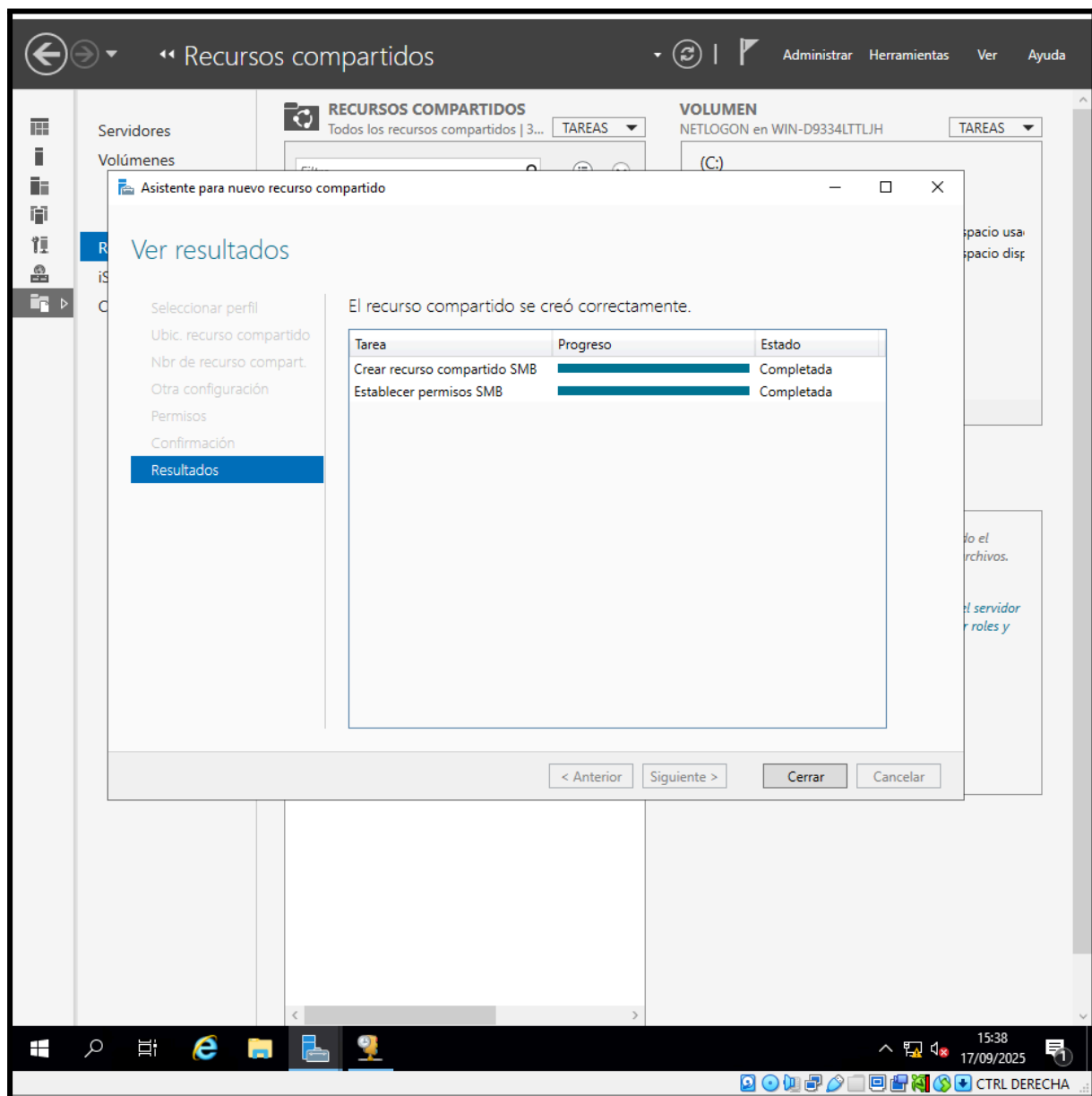
Confirmamos lo que hemos hecho anteriormente





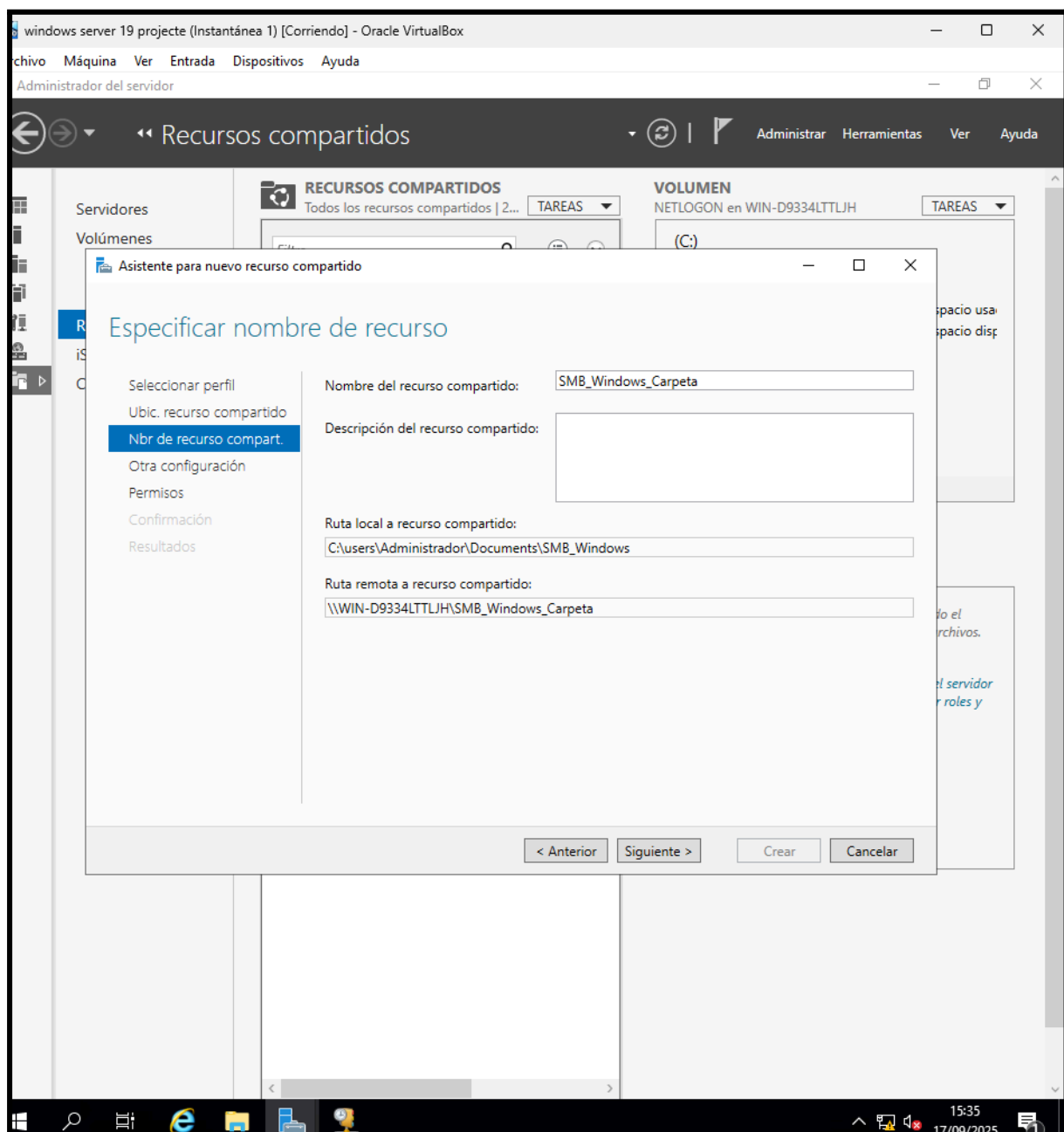


Y esperamos a que se creen los recursos





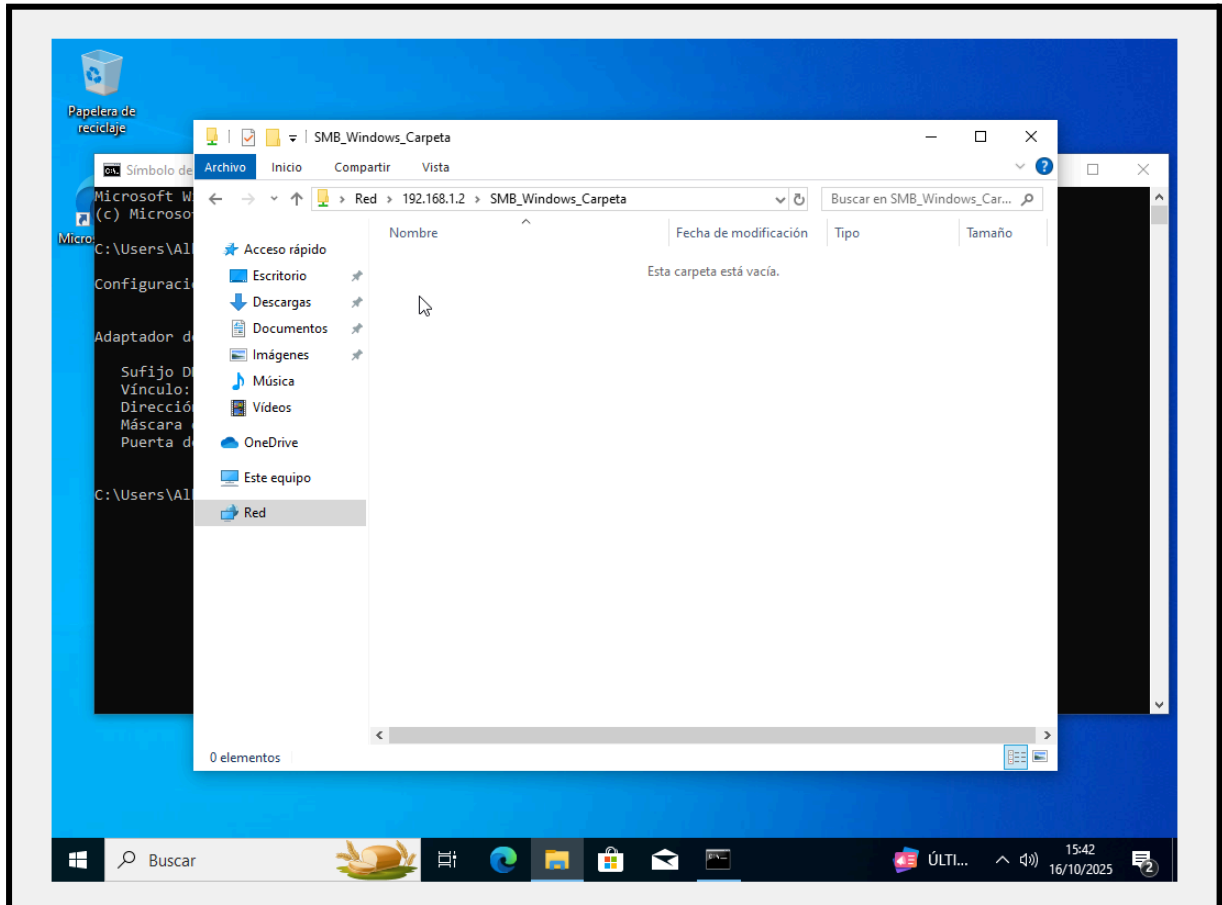
Le ponemos nombre al recurso





Comprobamos que se haya creado la carpeta compartida,

## Demostración SMB

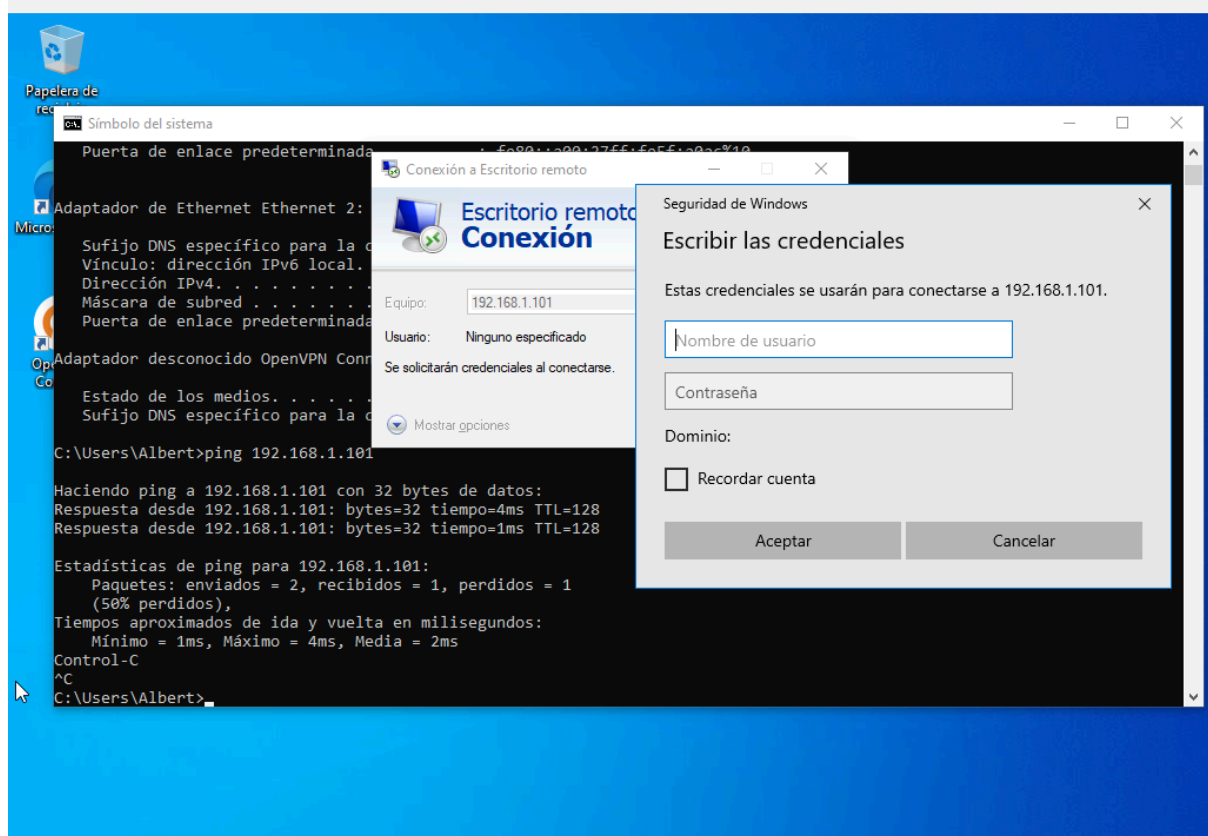


## RDP

Para hacer el escritorio remoto hemos usado el predeterminado de windows, en nuestro caso no usamos linux por lo tanto con el escritorio remoto de windows ya nos vale, podemos ver aqui nuestro ordenador cliente conectando a nuestra maquina servidor



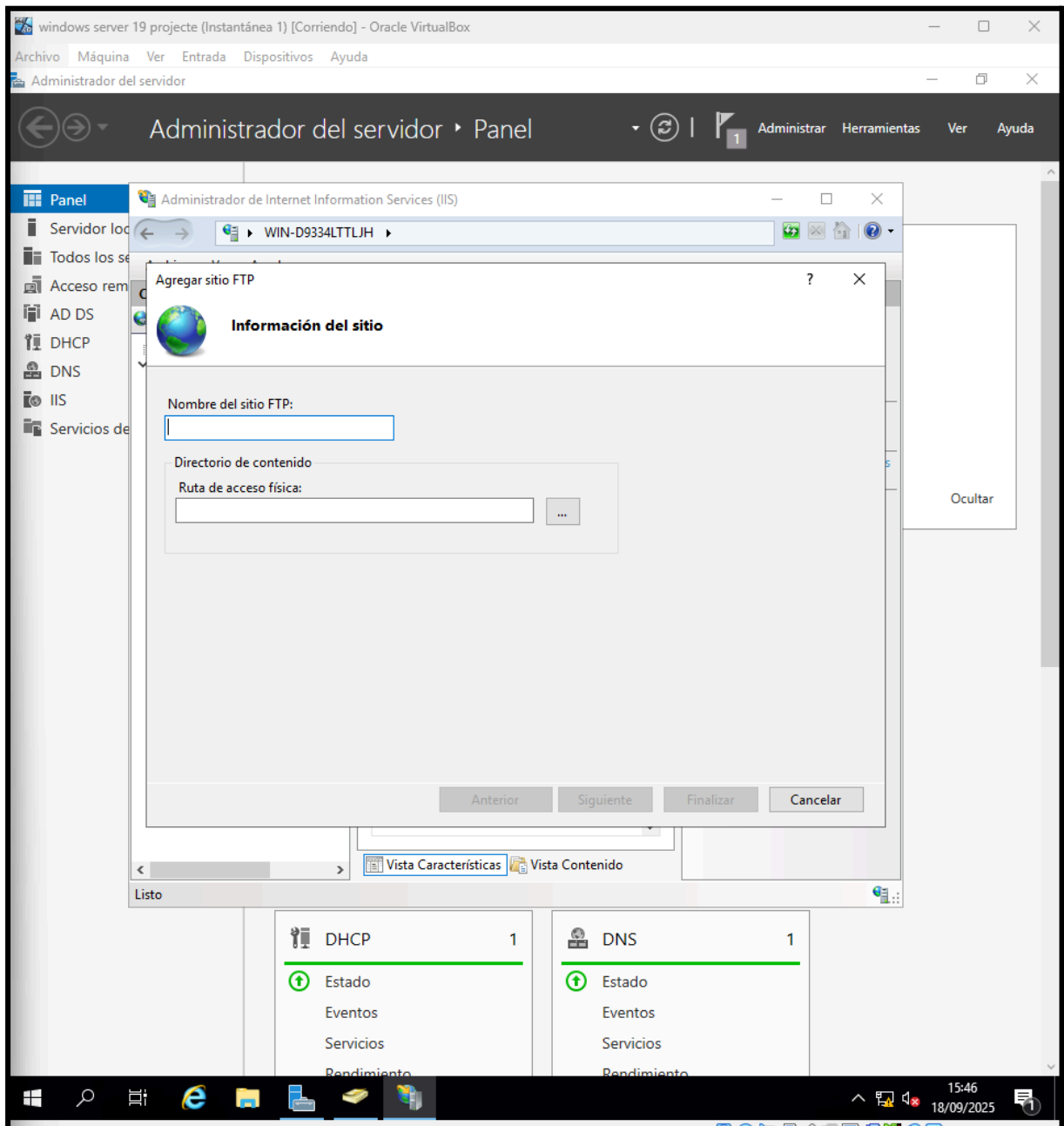
## Demostración RDP



## FTP

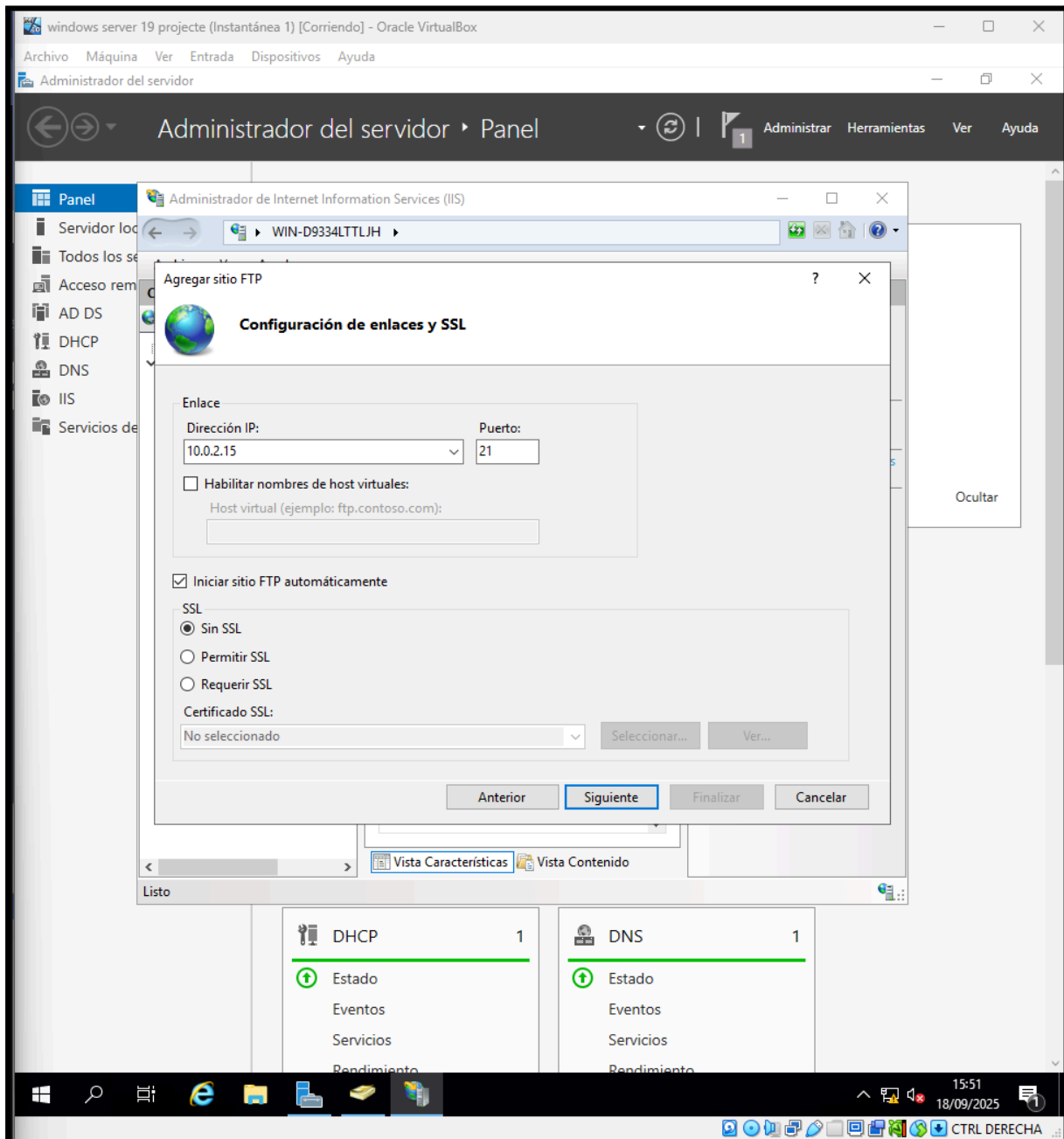
Al igual que con los roles anteriores, desde el Administrador del Servidor > Agregar roles y características, agregamos el servicio "Servidor FTP" bajo el rol de "Servicios de IIS"

Le ponemos nombre al sitio ftp





Panel de administración de servidor para configurar un sitio FTP, con opciones de dirección IP, host virtual y SSL.

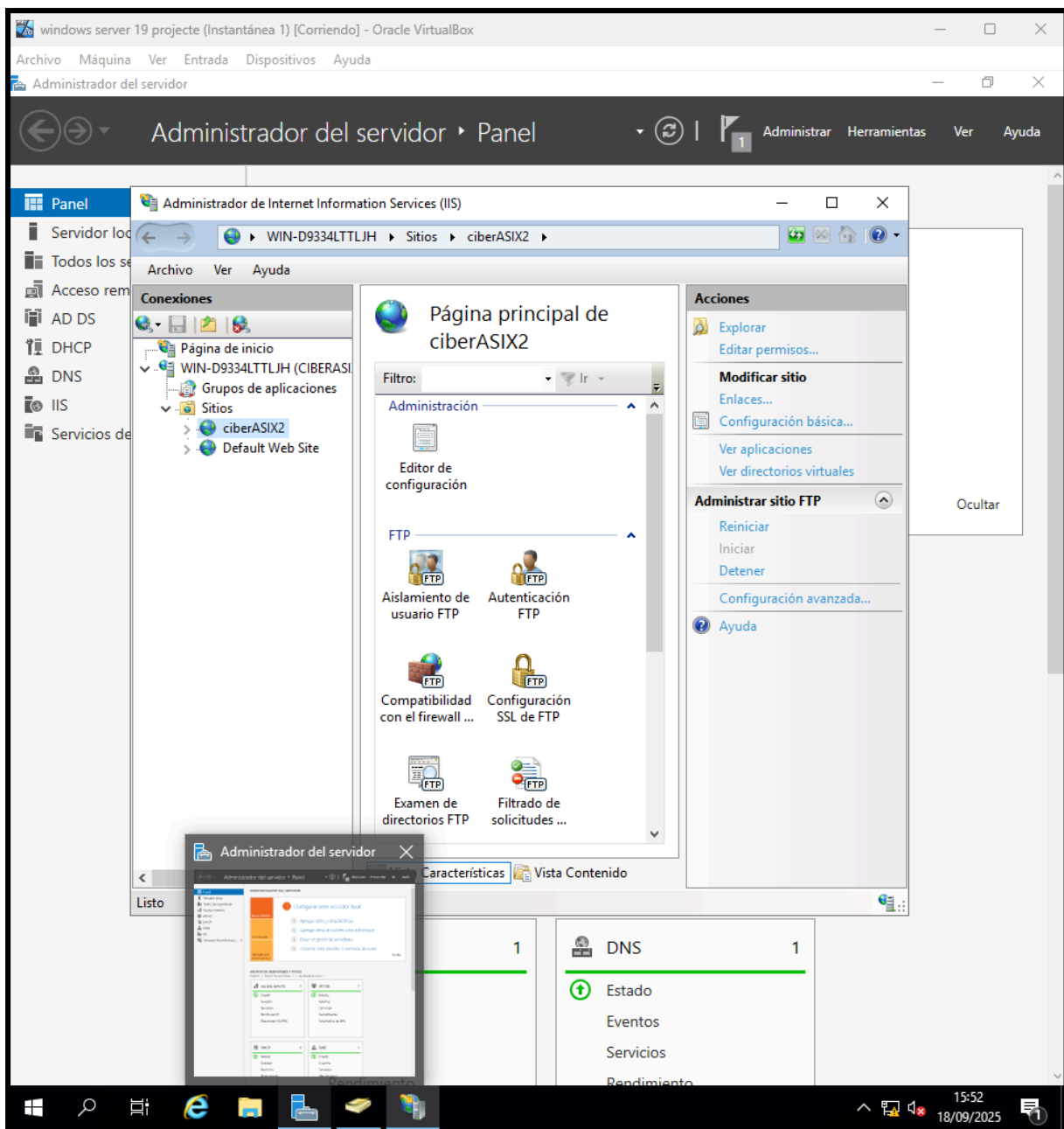


Conexión FTP establecida a 10.30.243.38. Servicio Microsoft FTP, con UTF8 habilitado. Esperando usuario.



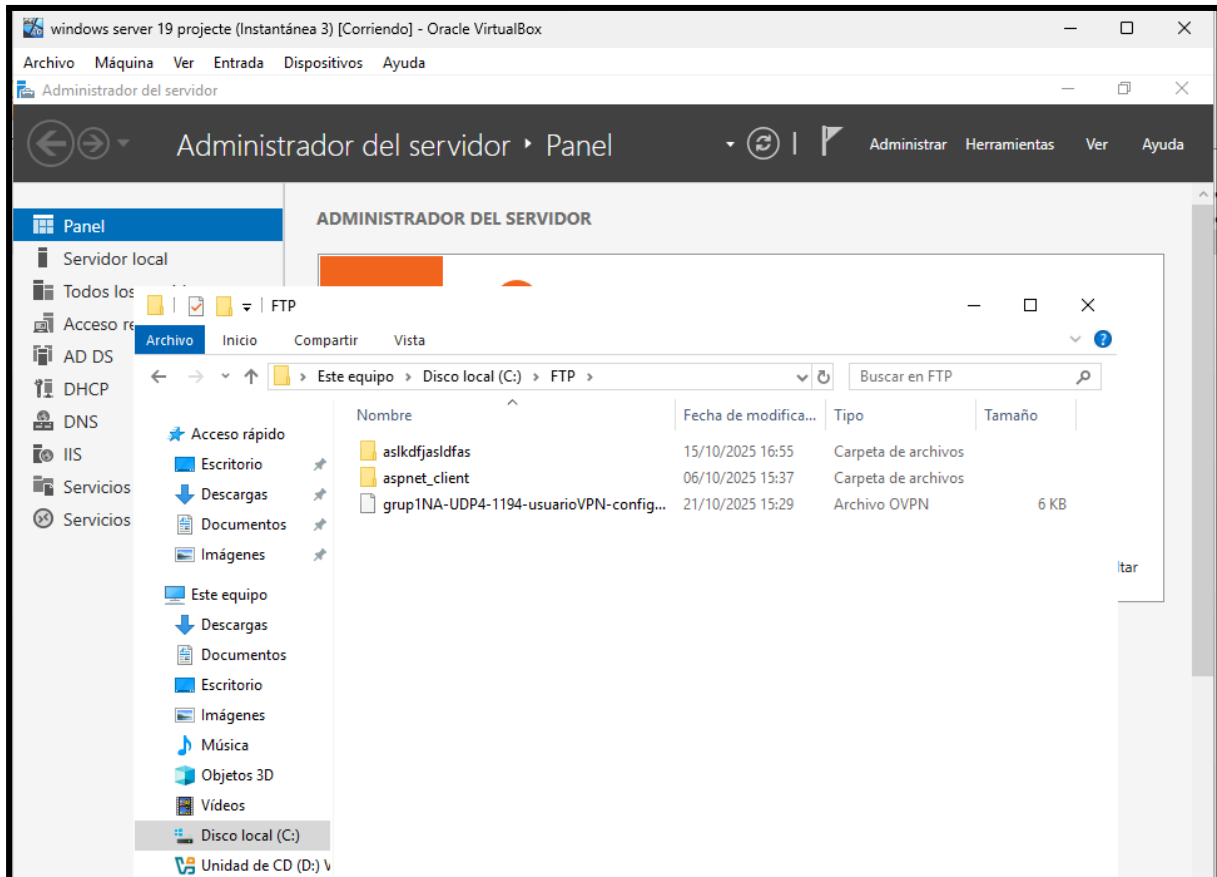
```
C:\Users\Administrador>ftp 10.30.243.38
Conectado a 10.30.243.38.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Usuario (10.30.243.38:(none)): _
```

Interfaz del Administrador de IIS mostrando el sitio FTP **ciberASIX2** y sus opciones de configuración y gestión.





Después de crear el sitio FTP hacemos una prueba en nuestra carpeta designada ponemos un archivo en nuestro caso el archivo cliente del openvpn para ver si funciona con nuestro cliente conectado a nuestro dominio

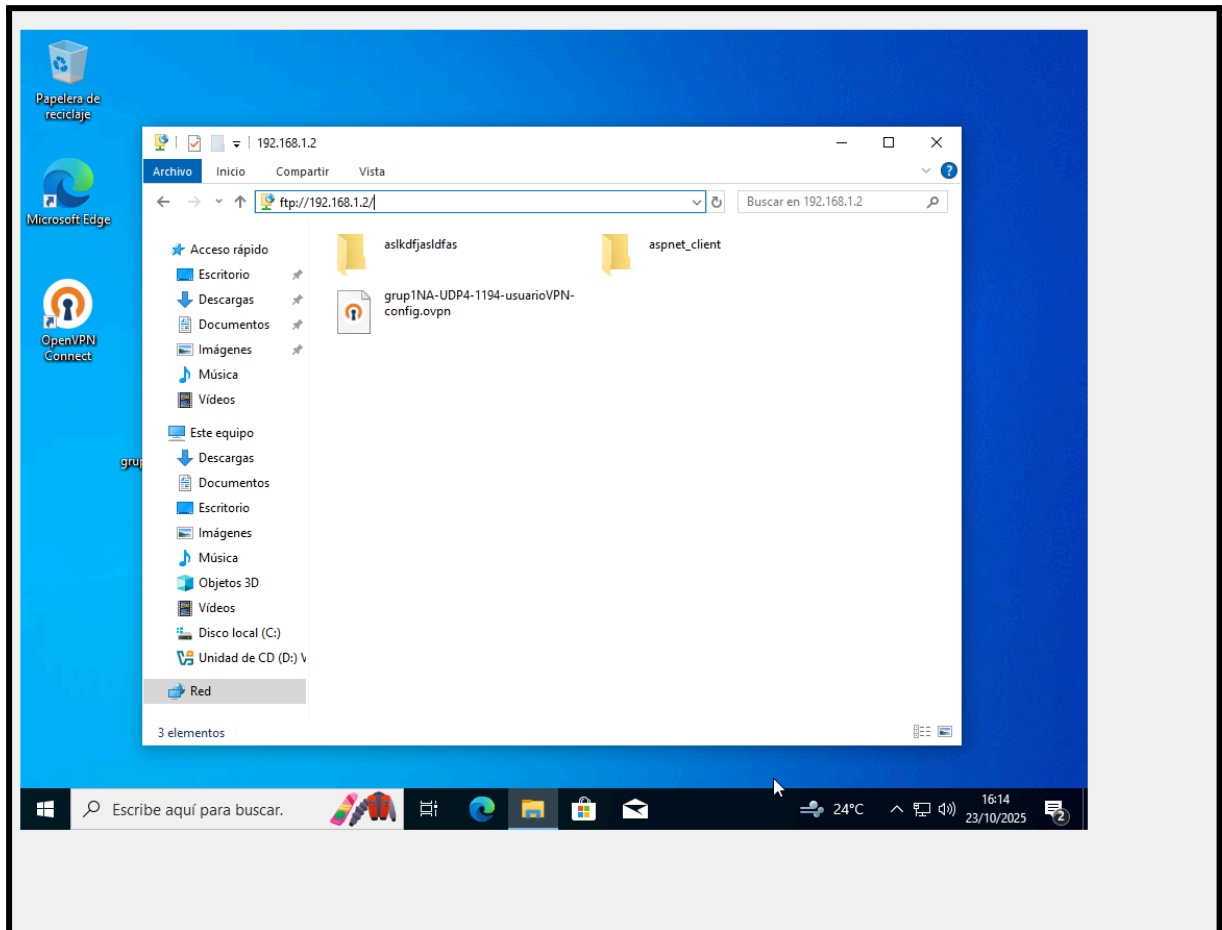






## Demostración FTP

Como vemos en nuestro windows 10 podemos ver que esta nuestro archivo, entramos a través de red/ y luego ponemos nuestra ip en nuestro caso ftp://192.168.1.2





# SSH

Abrimos Windows PowerShell como Administrador y instalamos el ssh

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> # Instalar OpenSSH Server
PS C:\Users\Administrador> Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

Path          :
Online        : True
RestartNeeded : False

PS C:\Users\Administrador>
PS C:\Users\Administrador> # Iniciar y configurar servicio
PS C:\Users\Administrador> Start-Service sshd
PS C:\Users\Administrador> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Users\Administrador>
PS C:\Users\Administrador> # Configurar firewall
PS C:\Users\Administrador> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction
inbound -Protocol TCP -Action Allow -LocalPort 22

Name          : sshd
DisplayName    : OpenSSH Server (sshd)
Description    :
DisplayGroup   :
Group          :
Enabled        : True
Profile        : Any
Platform       : {}
Direction     : Inbound
Action         : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner          :
PrimaryStatus  : OK
Status         : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

PS C:\Users\Administrador>
```

Comprobamos que el servicio ssh este en ejecución



SERVICIOS				
Resultados filtrados   2 de 232 totales				
SSH				
Nombre del servidor	Nombre para mostrar	Nombre de servicio	Estado	Tipo de inicio
WIN-D9334LTTLJH	OpenSSH Authentication Agent	ssh-agent	Detenido	Deshabilitado
WIN-D9334LTTLJH	OpenSSH SSH Server	sshd	En ejecución	Automático

## Demostración SSH

Después de hacer un comando ssh con la ip de nuestra máquina servidor podemos comprobar que el ssh funciona

## VPN

Implementamos un servidor VPN para acceso remoto seguro a la red interna



VPN / OpenVPN / Servers

Servers




Clients

Client Specific Overrides

Wizards

Client Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	<b>Mode:</b> Remote Access ( SSL/TLS + User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits		  

+ Add

aquí podemos ver nuestro certificado openvpn que se llama CA-OpenVPN

Cryptographic Settings

TLS Configuration

☒ Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

TLS Key

#  
# 2048 bit OpenVPN static key  
#  
-----BEGIN OpenVPN Static key V1-----

Paste the TLS key here.  
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode

TLS Authentication

In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction

Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority

CA-OpenVPN

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check

☐ Check client certificates with OCSP


Server certificate

Cert-OpenVPN (Server: Yes, CA: CA-OpenVPN, In Use)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length

2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. 

ECDH Curve

Use Default

Por aquí ponemos nuestro tunnel ip ponemos este rango de ip



Tunnel Settings

IPv4 Tunnel Network

10.0.8.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

192.168.1.1/24

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Aqui vemos como se crea el usuario vpn

Defined by

USER

Disabled

☐ This user cannot login

Username

usuarioVPN

Password

Password

Confirm Password

Full name

usaurioVPN

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings

☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

admins

Not member of

Member of

>> Move to "Member of" list

<< Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Effective Privileges

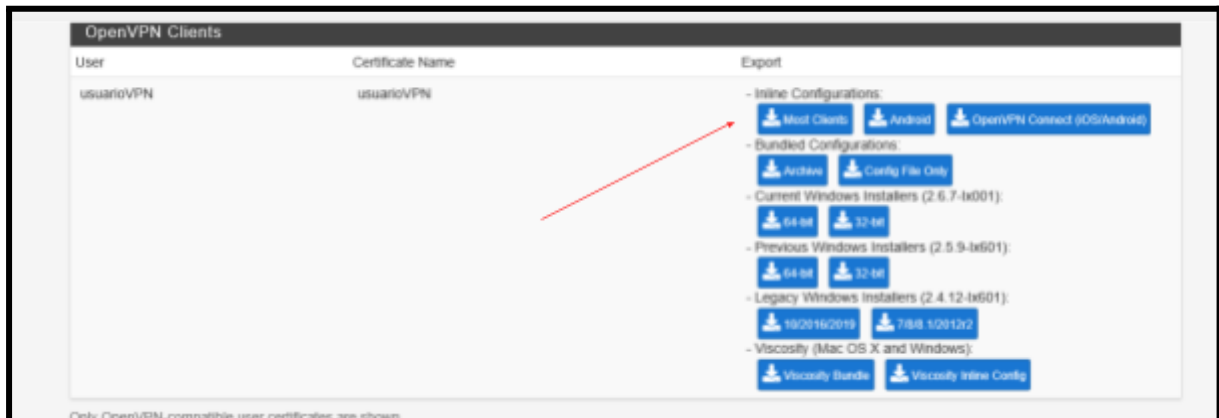
Inherited from	Name	Description	Action
			+ Add

User Certificates

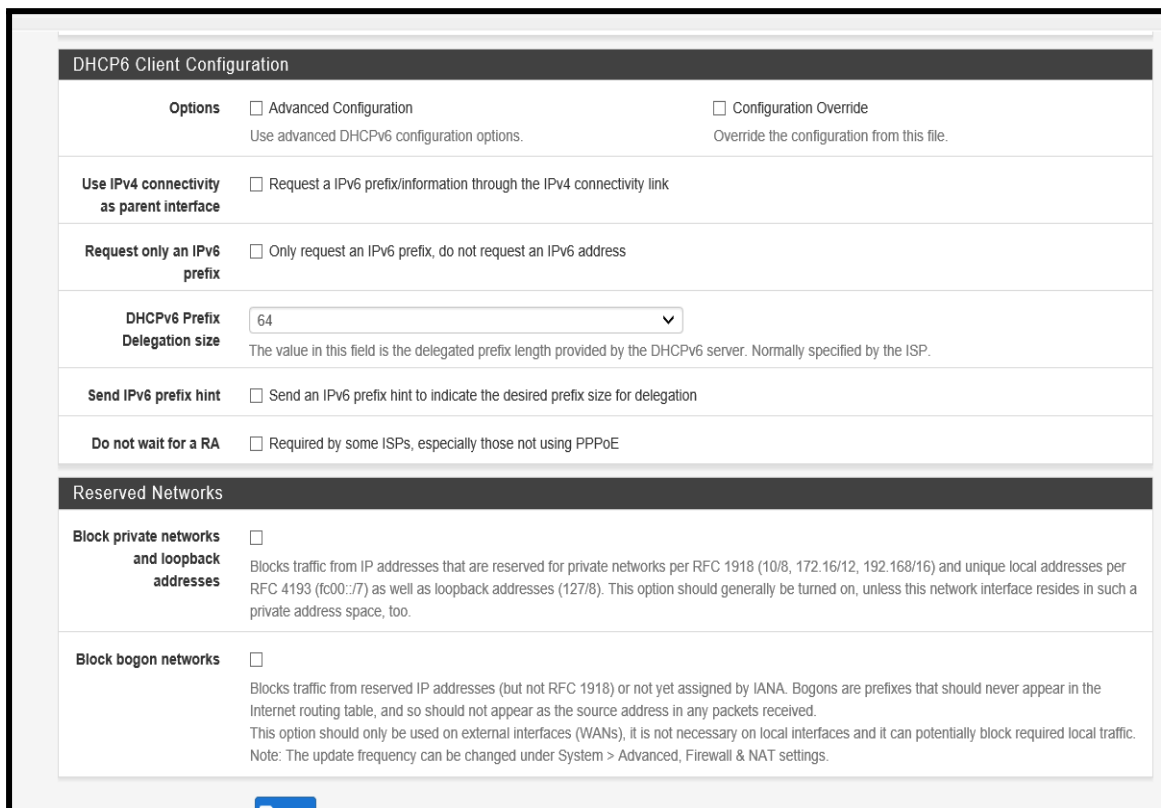
Name	CA	
usuarioVPN	CA-OpenVPN	🗑

+ Add

descargamos el cliente vpn



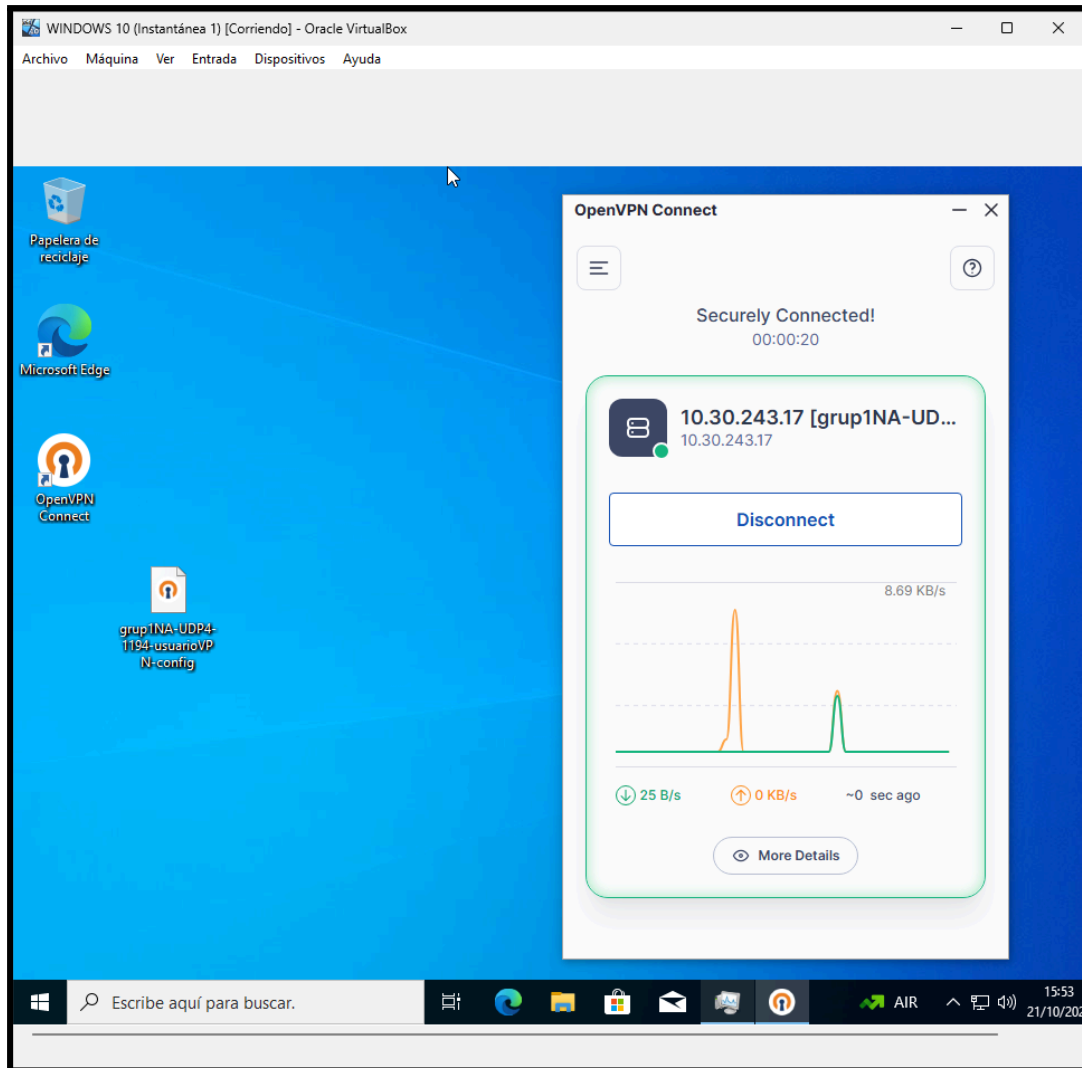
Quitamos una norma de firewall para que nos deje conectarnos desde una conexión privada



Desde el servidor nos pasamos el archivo del cliente vpn que hemos descargado desde el pfSense y a través del cliente vpn del windows 10 nos conectamos



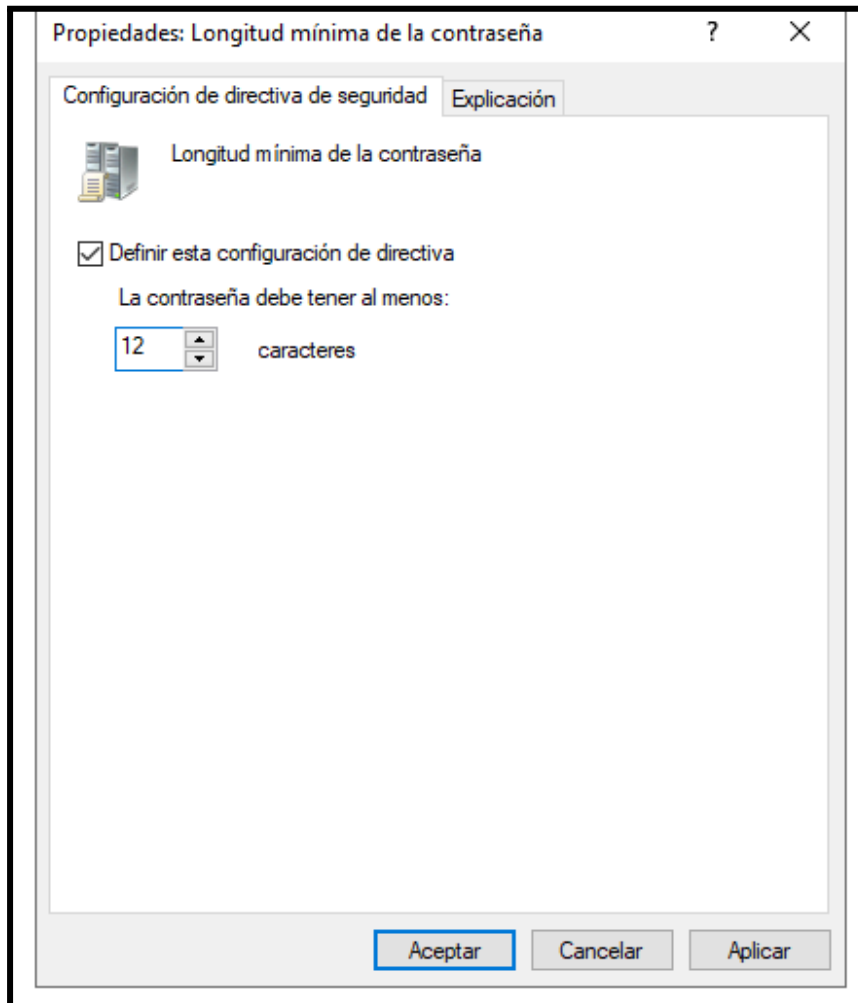
## Demostración VPN



## AD SG

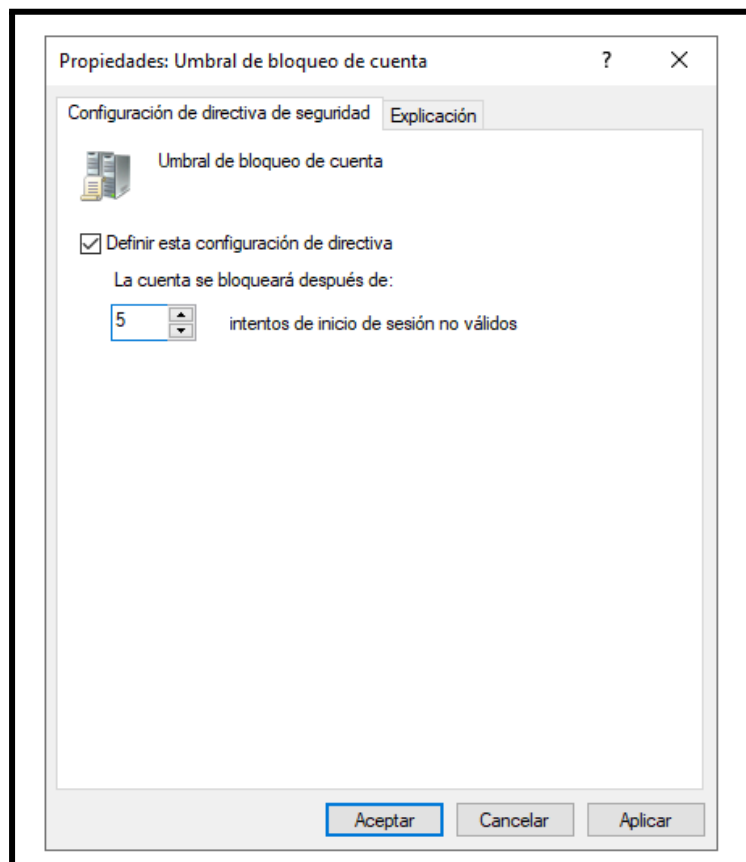
### Demostración AD SG

Parra nuestras políticas de seguridad pondremos de primera política una directiva que haga que los usuarios de nuestro dominio tengan una contraseña de mínimo 12 caracteres

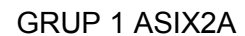


La siguiente es una política para poner 5 intentos de contraseña antes del bloque de inicio de sesión de windows hacemos esto para evitar ataques de fuerza bruta en nuestros pc clientes usando programas como hydra





La ultima ponemos actualizaciones automáticas en los fines de semana para así no molestar a nuestros trabajadores durante su horario laboral



The screenshot shows the 'Configuración' (Configuration) window for Windows updates. The window is divided into several sections:

- Privacidad de la aplicación:** This section is partially visible on the left.
- Configurar Actualizaciones automáticas:** This section contains three radio buttons: 'No configurada', 'Habilitada' (selected), and 'Deshabilitada'. A 'Comentario:' text box is next to it.
- Compatible con:** This section shows a list of operating systems: 'Windows XP Professional Service Pack 1 o, como mínimo, Windows 2000 Service Pack 3'. A note below it states: 'La opción 7 solo se admite en servidores que ejecuten Windows Server 2016'.
- Opciones:** This section is expanded, showing a list of update options. The selected option is 'Automáticamente y notificar instalación'. Below this, there are two dropdown menus: 'Actualización programada:' set to '6 - Todos los viernes' and 'Hora programada:' set to '17:00'.
- Ayuda:** This section provides detailed information about the selected update option. It explains that this configuration allows specifying when to download and install updates. It also mentions that users can choose to receive notifications before downloading and installing updates.

The 'Aceptar' (Accept) button is highlighted with a red box, indicating the final step in the configuration process.