

FASE 2 PROYECTO ASIX2A **GRUP1**

Nicolas Gomariz, Albert Martínez

23/10/2025



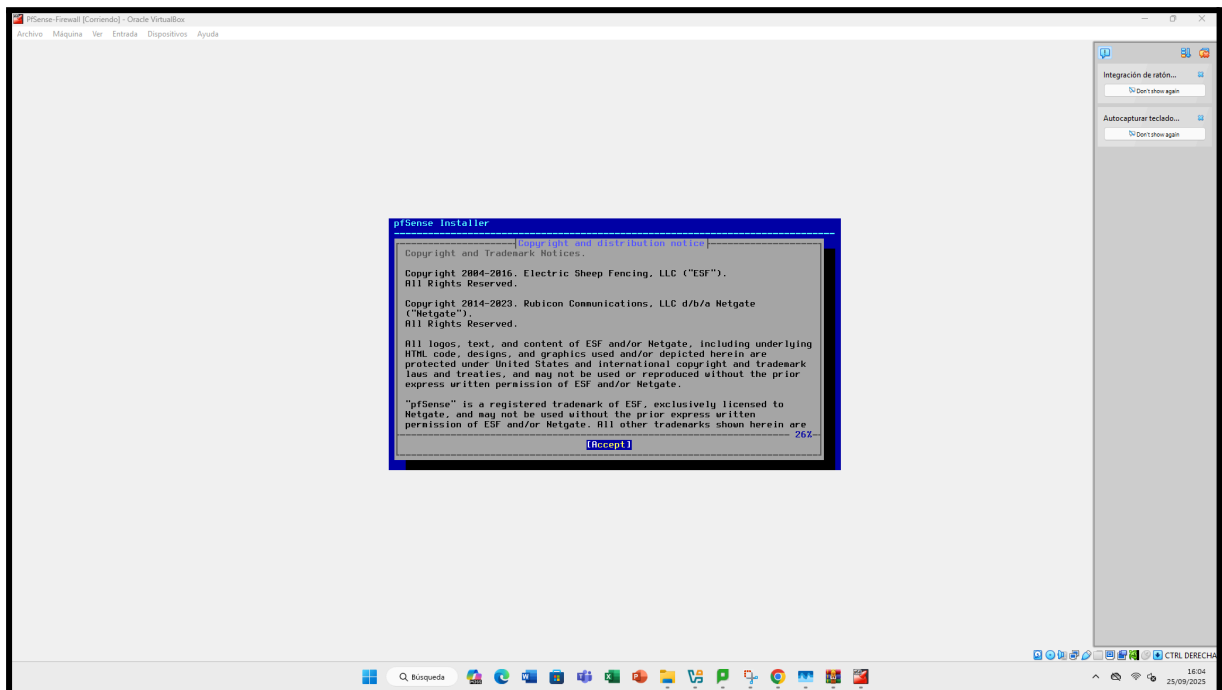
INDEX

Instalacio pFsense	3
DHCP	10
Demostrocio DHCP	11
DNS	13
Active directory	20
SMB	24
Demostración SMB	31
RDP	31
FTP	32
SSH	38
VPN	39
AD SG	43

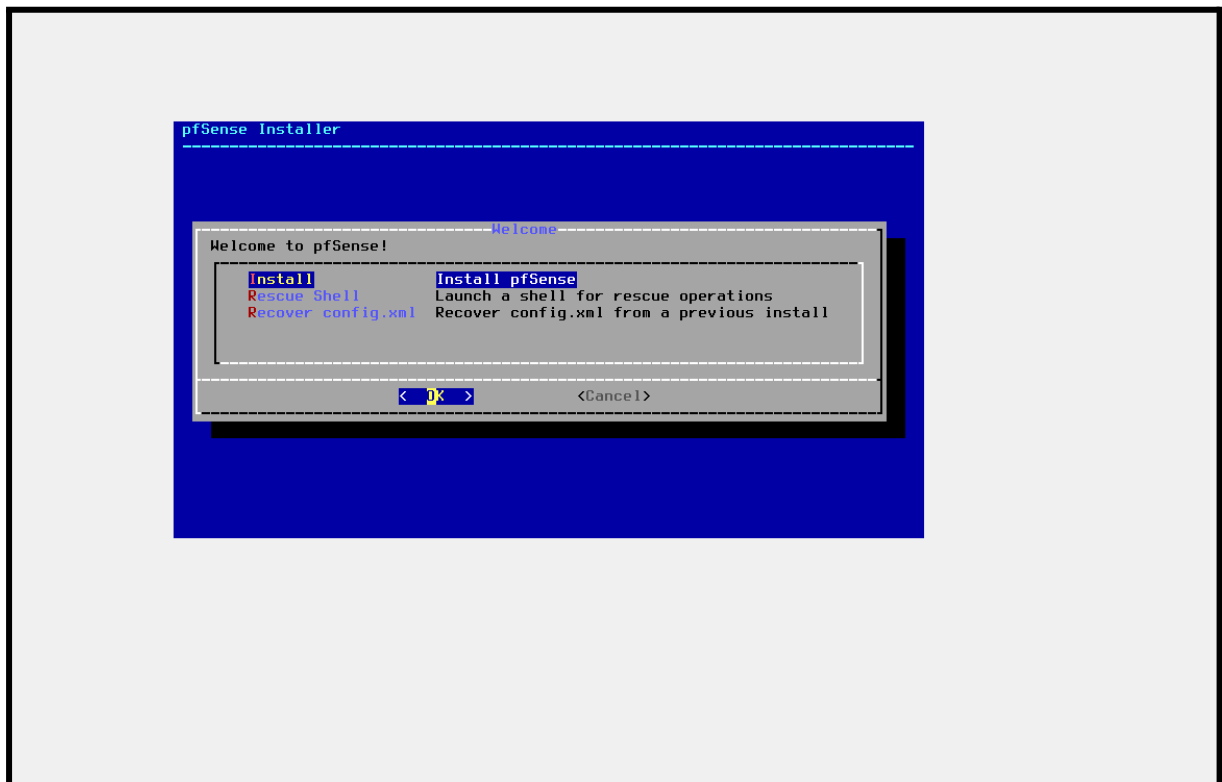


Instalacio pFsense

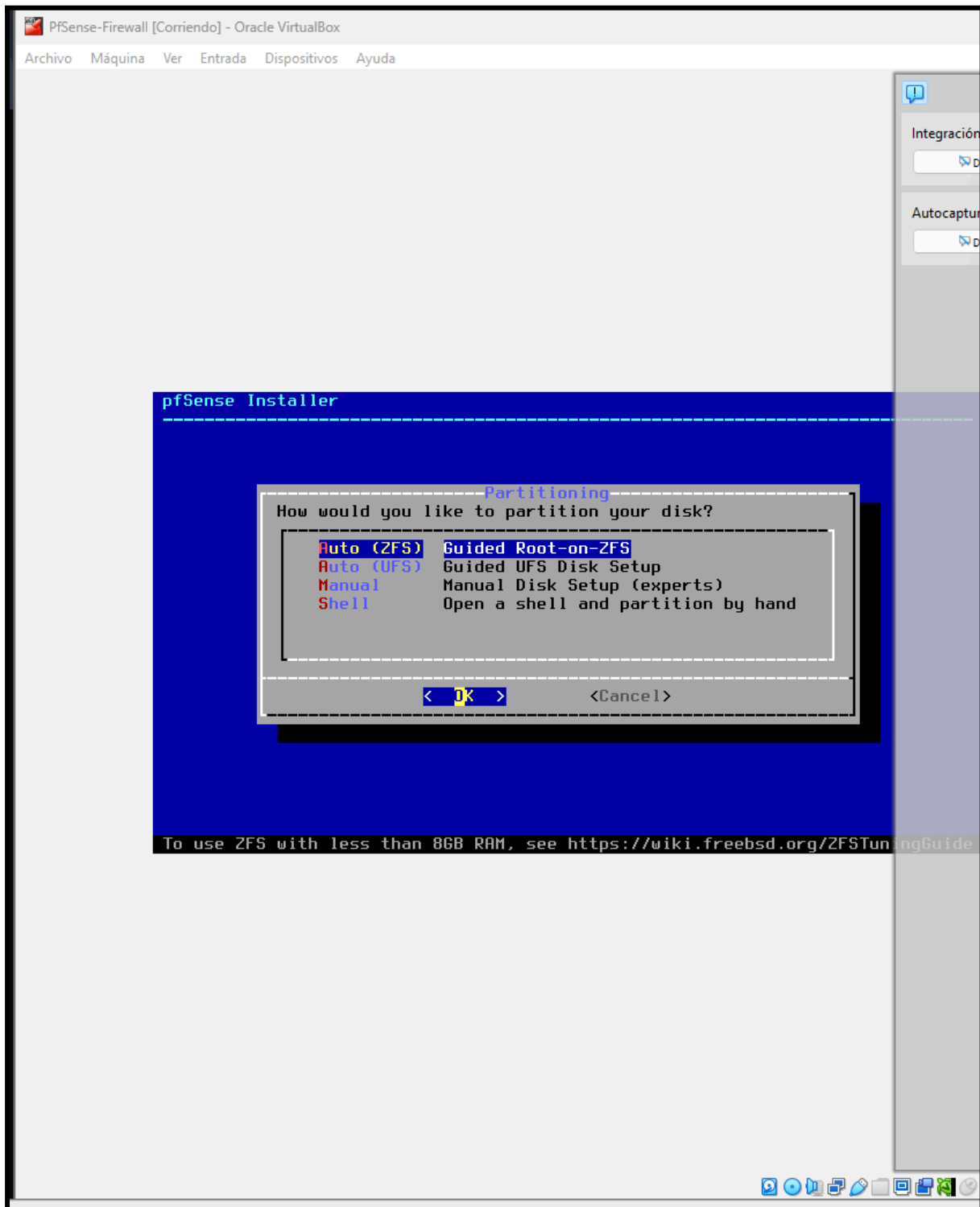
Inicio de la instalación y configuración básica de pfSense.



Confirmamos para iniciar el proceso de instalación.

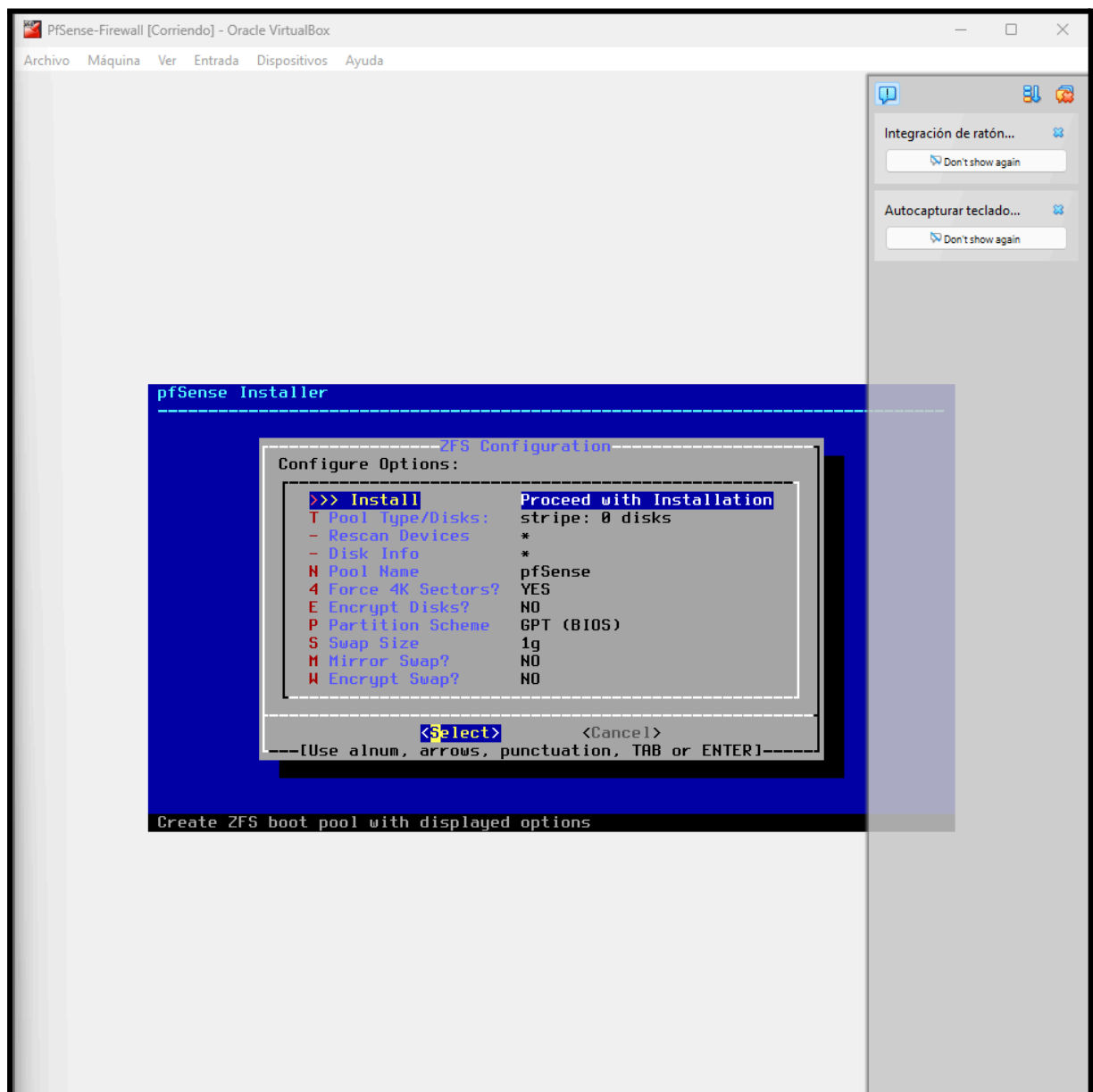


Selección de la unidad de disco para la instalación.



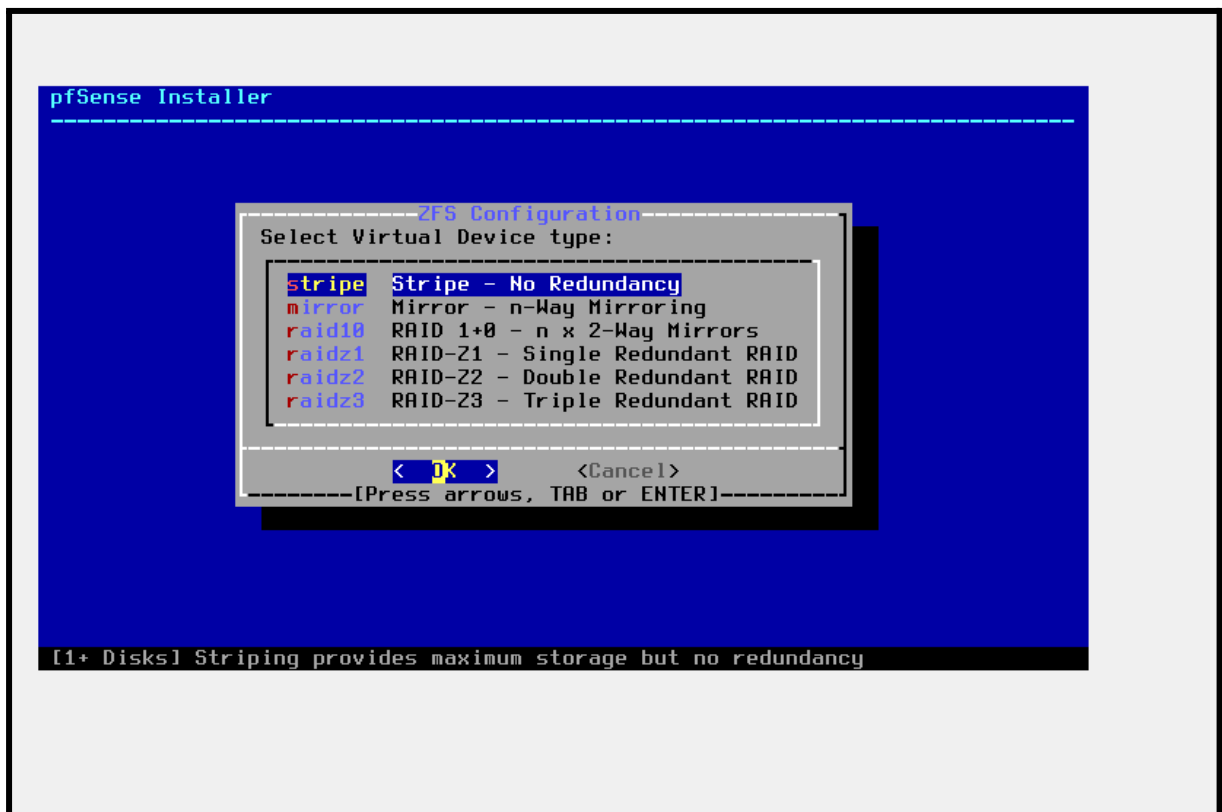


Confirmación e inicio de la instalación en el disco.

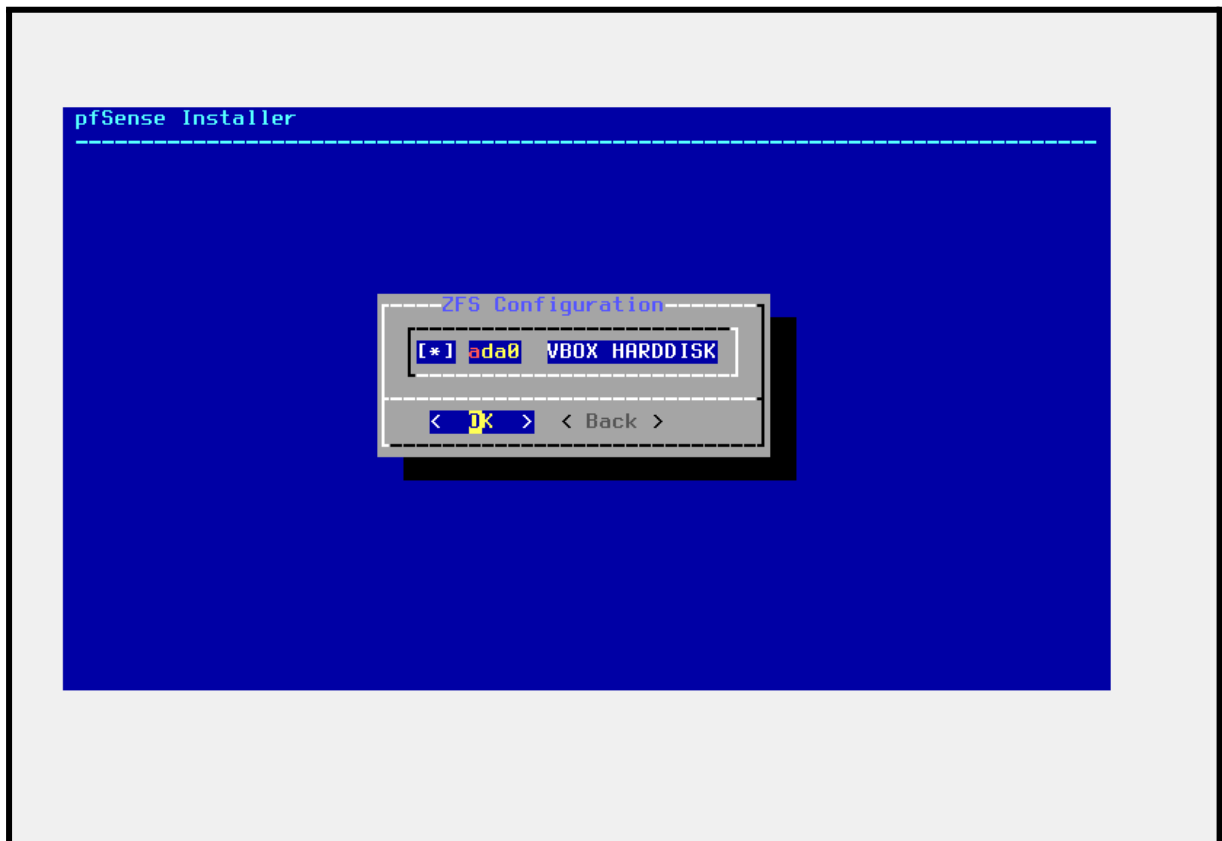




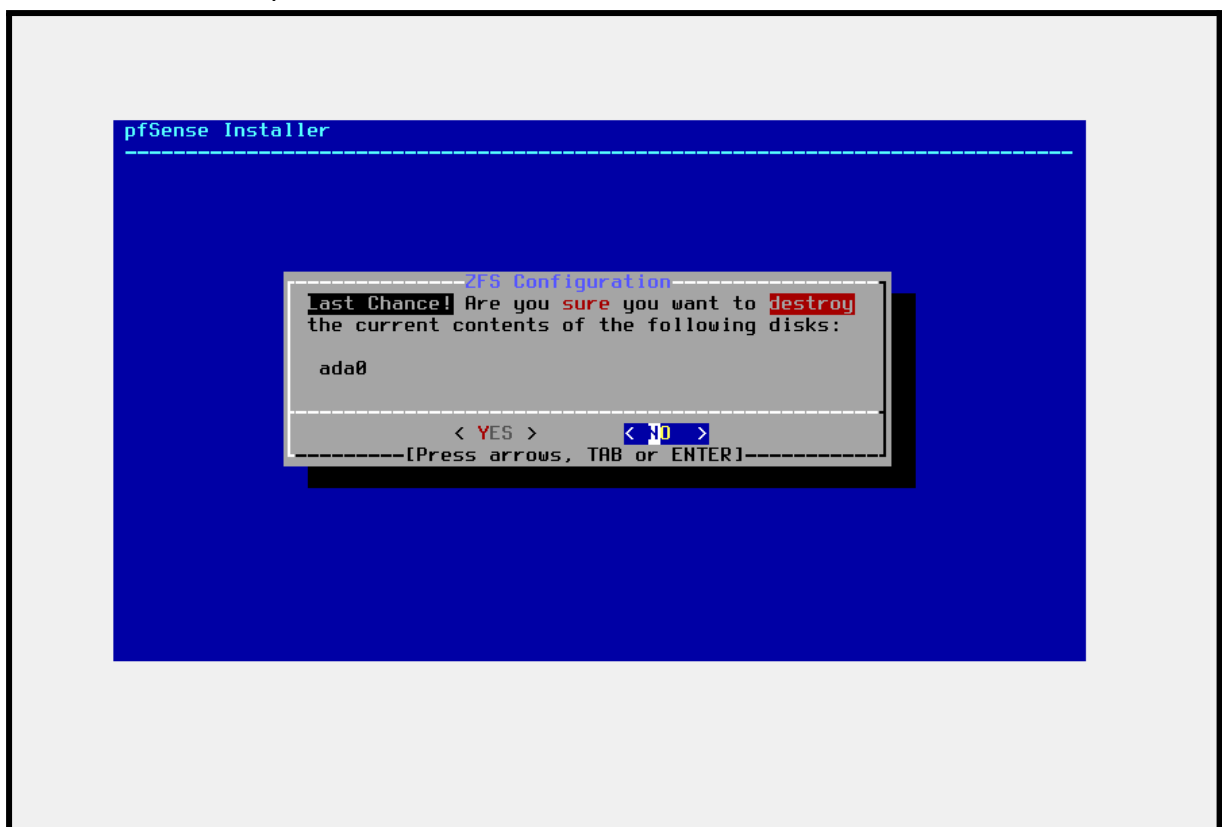
Selección del dispositivo de instalación



Selección del disco de destino para la instalación.

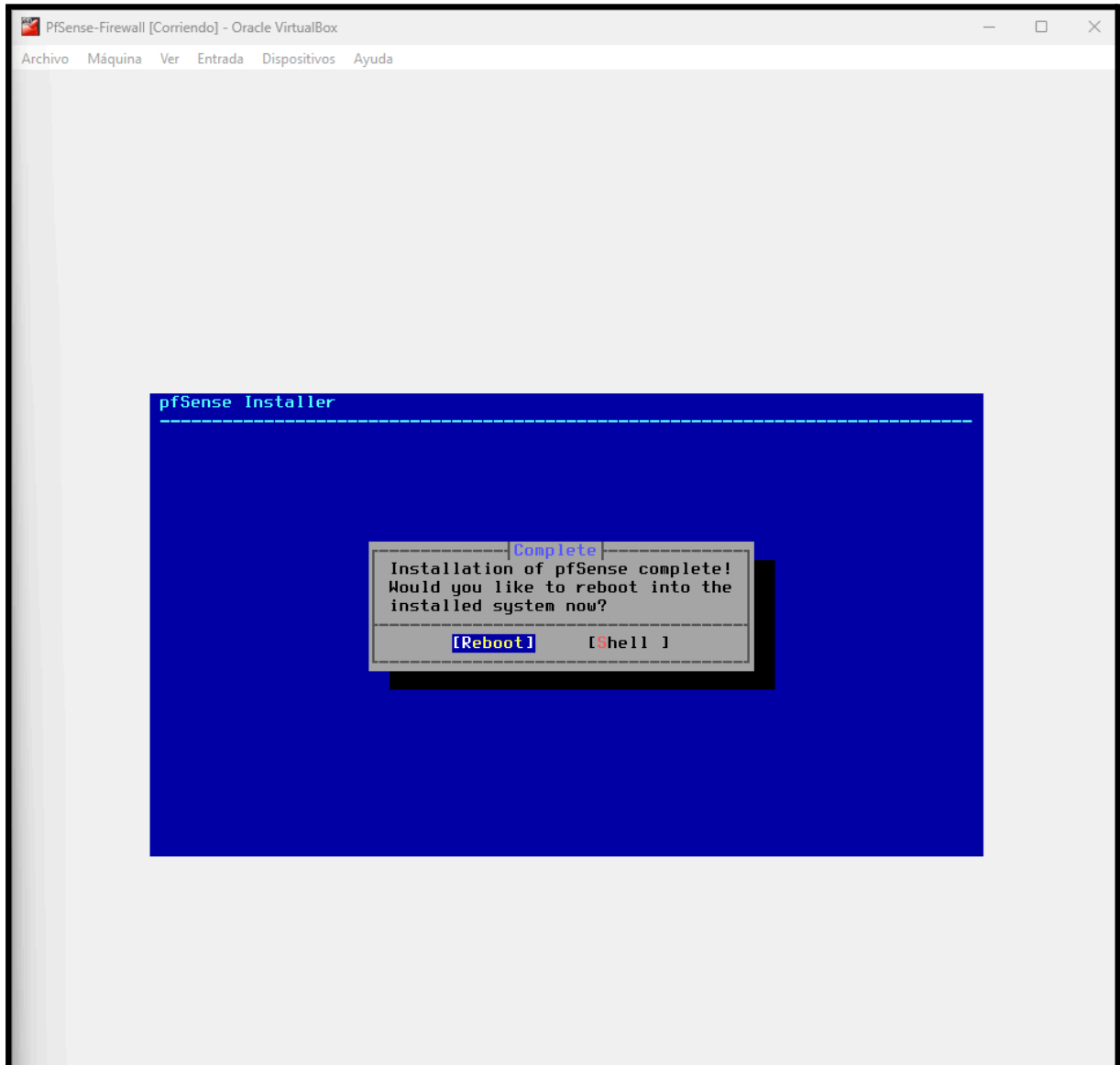


Nos da un aviso de que vamos a destruir el contenido del disco





Reinicio del sistema para completar la instalación.





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	
Subnet	192.168.1.0/24
Subnet Range	192.168.1.1 - 192.168.1.254
Address Pool Range	<div>192.168.1.10192.168.1.245</div> <div>FromTo</div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p>
Additional Pools	<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	
WINS Servers	<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. <input type="checkbox"/> 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).

```
CA Administrador: Símbolo del sistema
:\Users\Administrador>IP A
IP" no se reconoce como un comando interno o externo,
rograma o archivo por lotes ejecutable.

:\Users\Administrador>ip a
ip" no se reconoce como un comando interno o externo,
rograma 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
```



System / General Setup

System

Hostname grup1NA
Name of the firewall host, without domain part.

Domain home.arpa
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

Address: 1.1.1.1
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.

Hostname: grupNA
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, pSense 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 Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)
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

Windows Server 19 projecte (Instancia 1) [Comandos] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

https://10.0.2.15/services/dnsmasq.php

Configuración de seguridad m... grup1NA.home.arpa - Servi... Nueva pestaña

pfsense System Interfaces Firewall Services VPN Status Diagnostics Help

Services / DNS Forwarder

ISC DHCP has reached end-of-life and will be removed in a future version of pSense. Visit System > Advanced > Networking to switch DHCP backend.

General DNS Forwarder Options

Enable ☒ Enable DNS forwarder

DHCP Registration ☐ Register DHCP leases in DNS forwarder
If this option is set machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. The domain in System: General Setup should also be set to the proper value.

Static DHCP ☐ Register DHCP static mappings in DNS forwarder
If this option is set, IPv4 DHCP static mappings will be registered in the DNS forwarder so that their name can be resolved. The domain in System: General Setup should also be set to the proper value.

Prefer DHCP ☐ Resolve DHCP mappings first
If this option is set DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).

DNS Query Forwarding

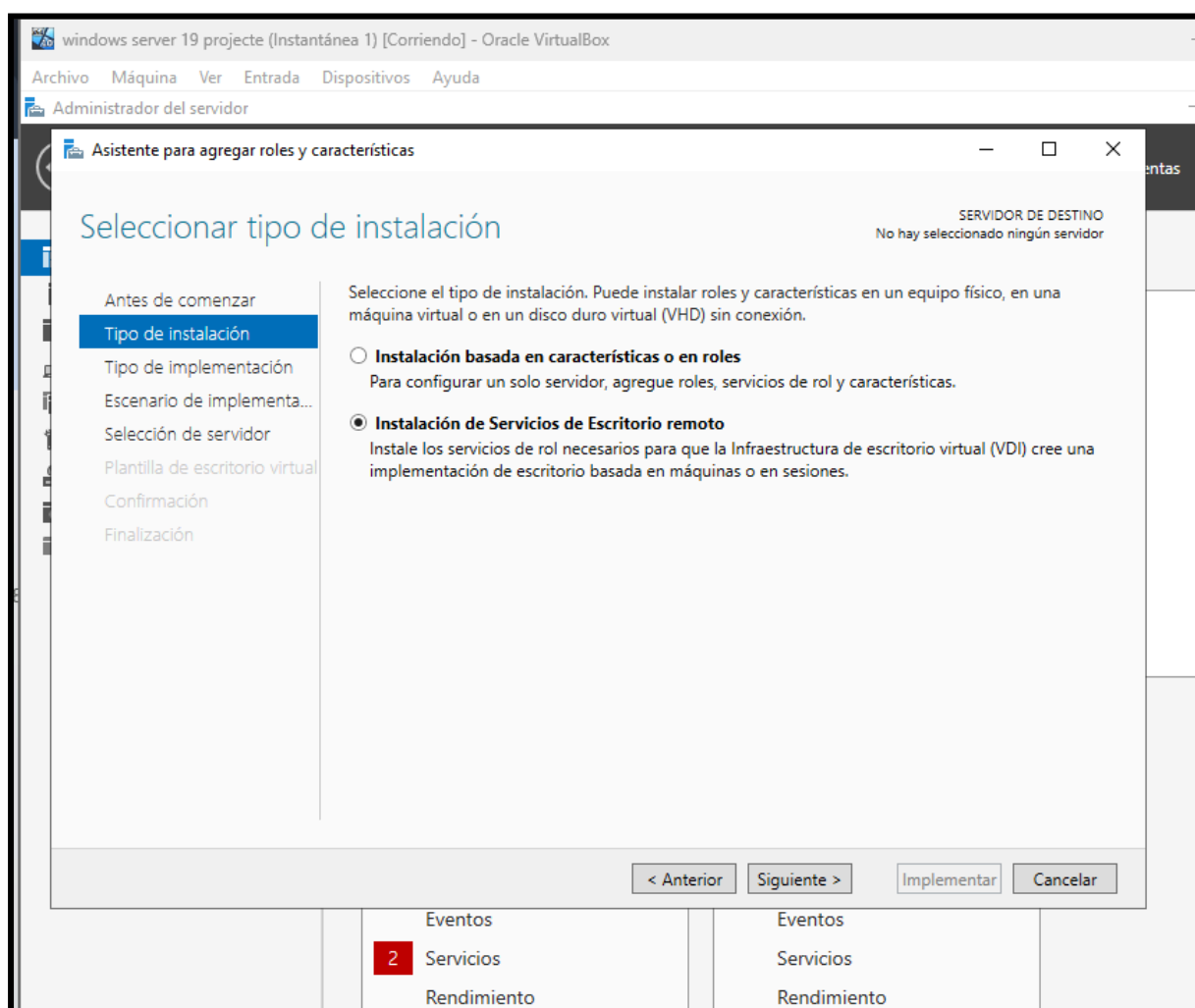
☐ Query DNS servers sequentially
If this option is set pSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers), rather than all at once in parallel.

☐ Require domain
If this option is set pSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.

☐ Do not forward private reverse lookups
If this option is set pSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private "n.n.n.in-addr.arpa" names to a specific server are still forwarded. If this ID is...

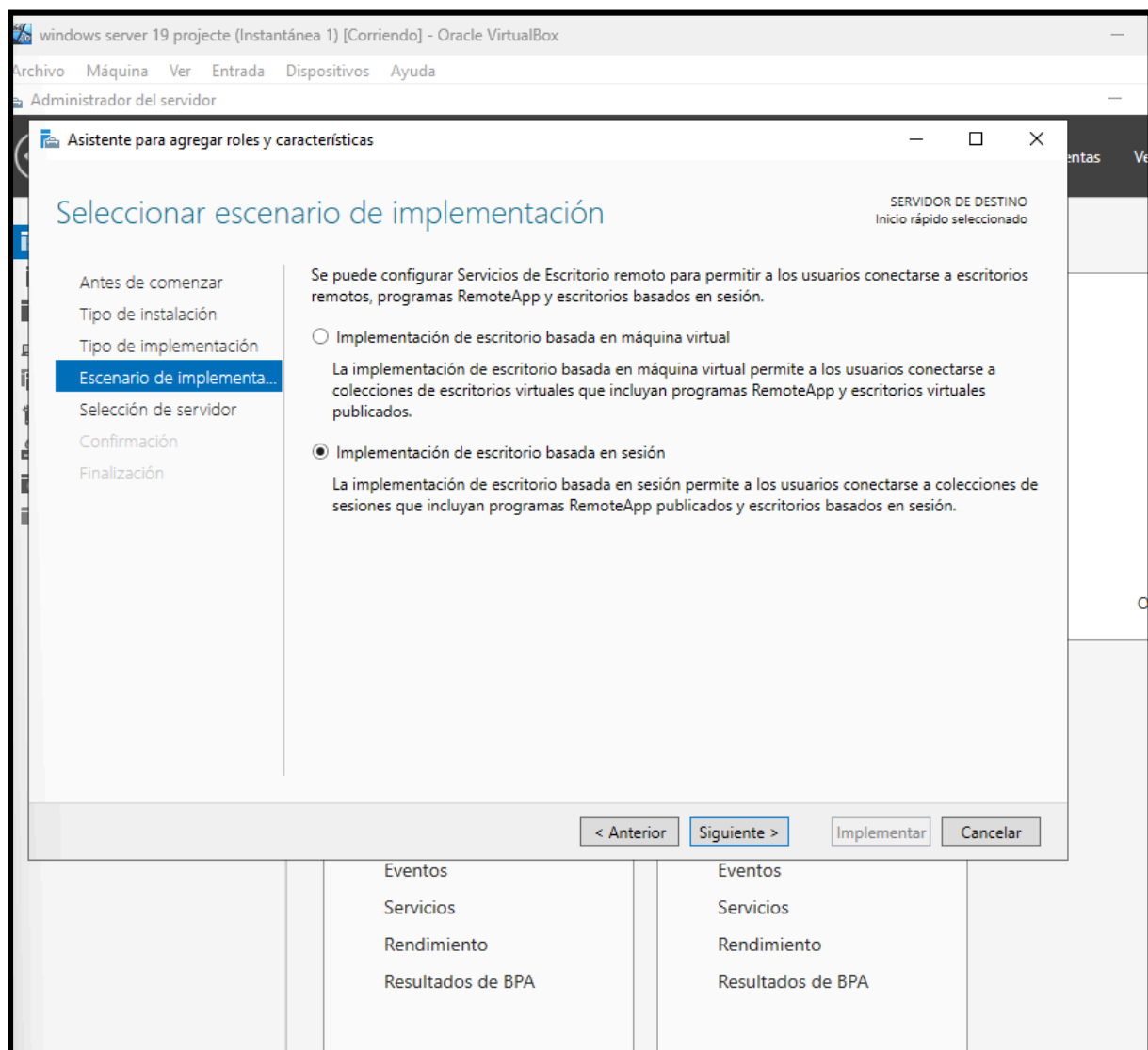


Instalación y configuración del servicio de Escritorio Remoto.



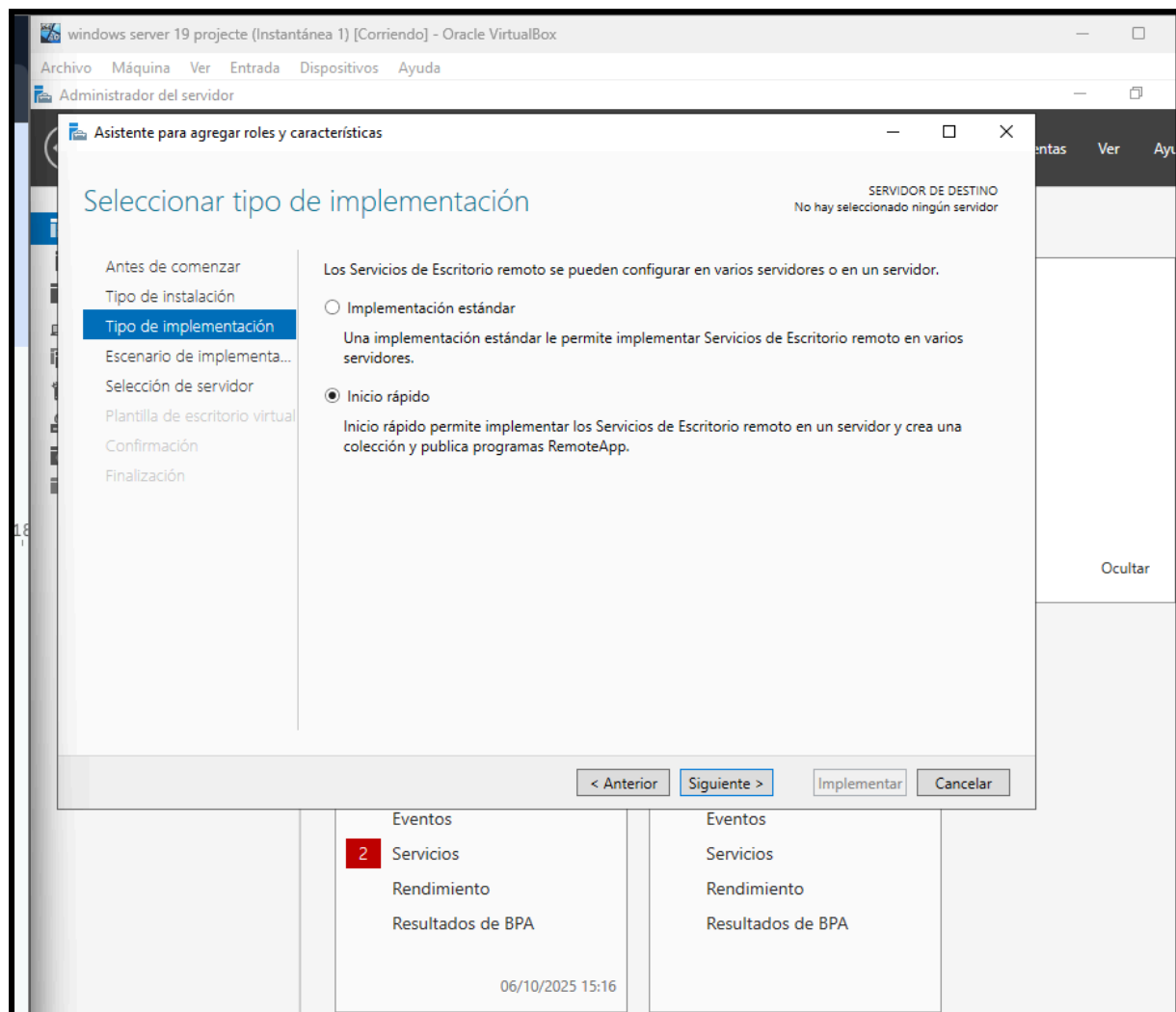


Selección del escenario de implementación para el servicio.



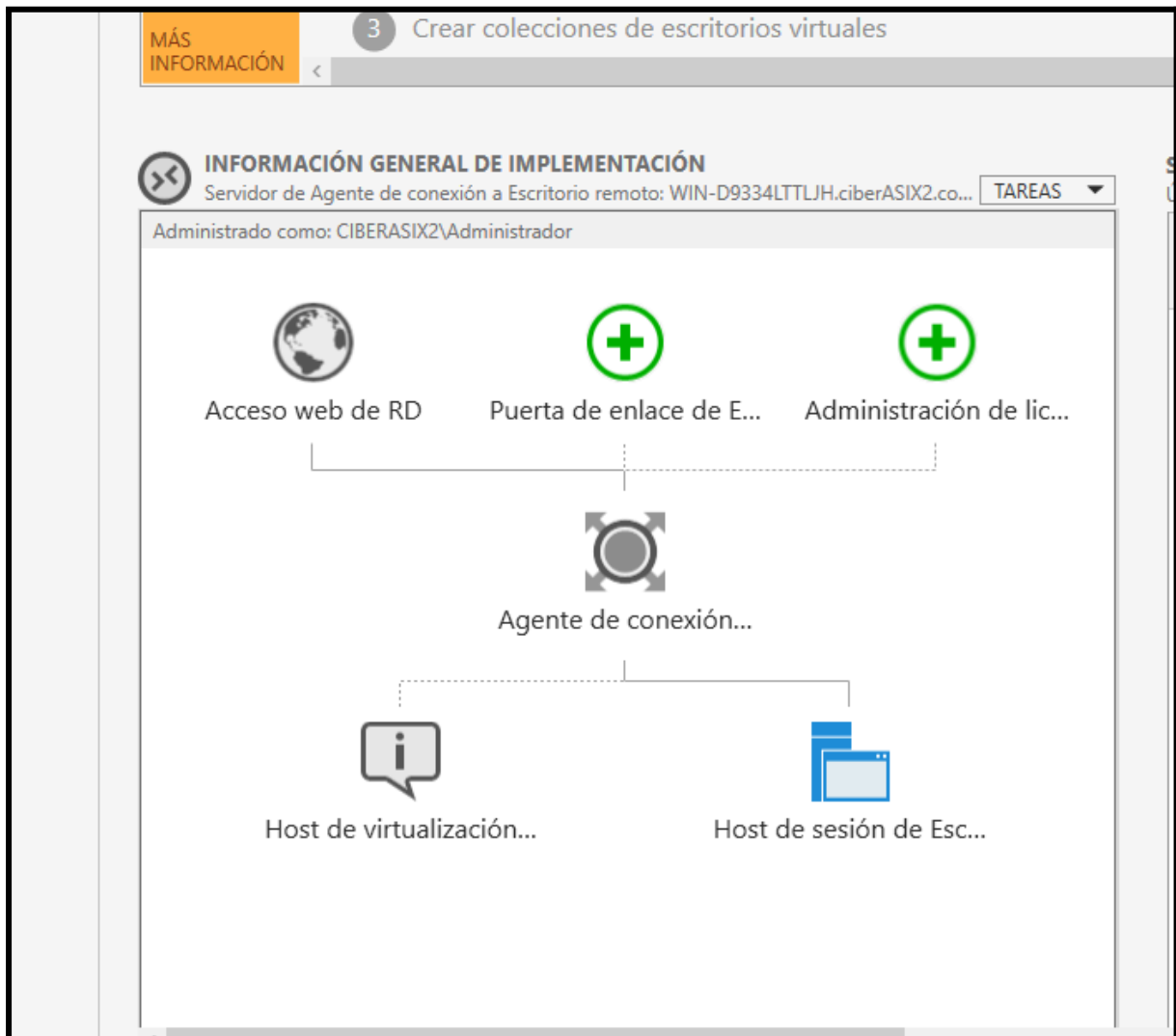


Selección del tipo de implementación requerido.





Verificamos la configuración en el panel de Escritorio Remoto.



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.



Administrador del servidor

Asistente para agregar roles y características

Selección de roles de servidor

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
AD DS
Confirmación
Resultados

Selección de roles de servidor

Seleccione uno o varios roles para instalarlos en el servidor seleccionado.

SERVIDOR DE DESTINO
WIN-D9334LTLJH

Roles	Descripción
<input type="checkbox"/> Acceso remoto	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Atestación de mantenimiento del dispositivo	
<input type="checkbox"/> Controladora de red	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Servicio de protección de host	
<input type="checkbox"/> Servicios de acceso y directivas de redes	
<input type="checkbox"/> Servicios de archivos y almacenamiento (1 de 12 roles)	
<input type="checkbox"/> Servicios de certificados de Active Directory	
<input checked="" type="checkbox"/> Servicios de dominio de Active Directory	Servicios de dominio de Active Directory (AD DS) almacena información acerca de los objetos de la red y pone esta información a disposición de los usuarios y administradores de red. AD DS usa controladores de dominio para proporcionar a los usuarios de red acceso a los recursos permitidos en toda la red mediante un proceso de inicio de sesión único.
<input type="checkbox"/> Servicios de Escritorio remoto	
<input type="checkbox"/> Servicios de federación de Active Directory	
<input type="checkbox"/> Servicios de implementación de Windows	
<input type="checkbox"/> Servicios de impresión y documentos	
<input type="checkbox"/> Servidor de fax	
<input type="checkbox"/> Servidor DHCP	
<input type="checkbox"/> Servidor DNS	
<input type="checkbox"/> Servidor web (IIS)	

< Anterior Siguiente > Instalar Cancelar

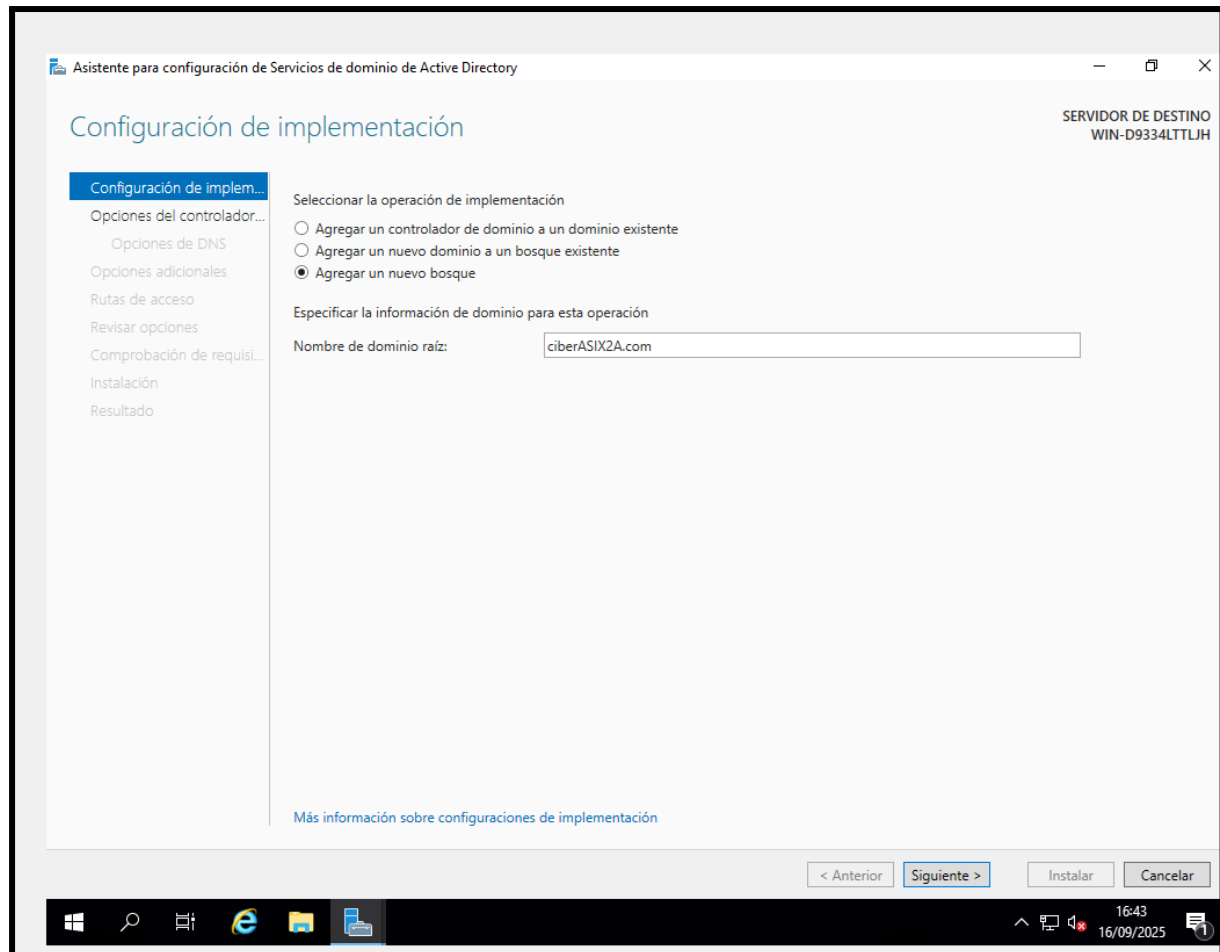
Eventos	Eventos
Rendimiento	5 Servicios
Resultados de BPA	Rendimiento
	Resultados de BPA

16/09/2025 16:28

16:29
16/09/2025



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.

Asistente para configuración de Servicios de dominio de Active Directory

SERVIDOR DE DESTINO
WIN-D9334LTLJH

Opciones del controlador de dominio

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](#)

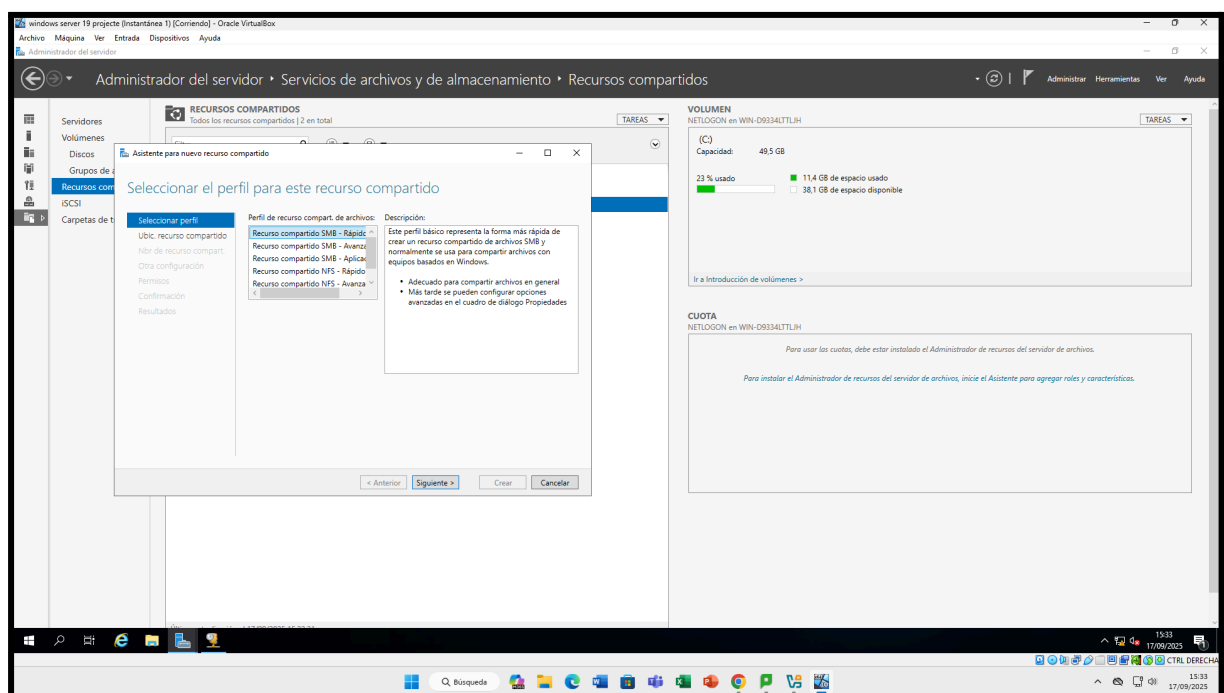
< Anterior Siguiente > Instalar Cancelar

16:44
16/09/2025



SMB

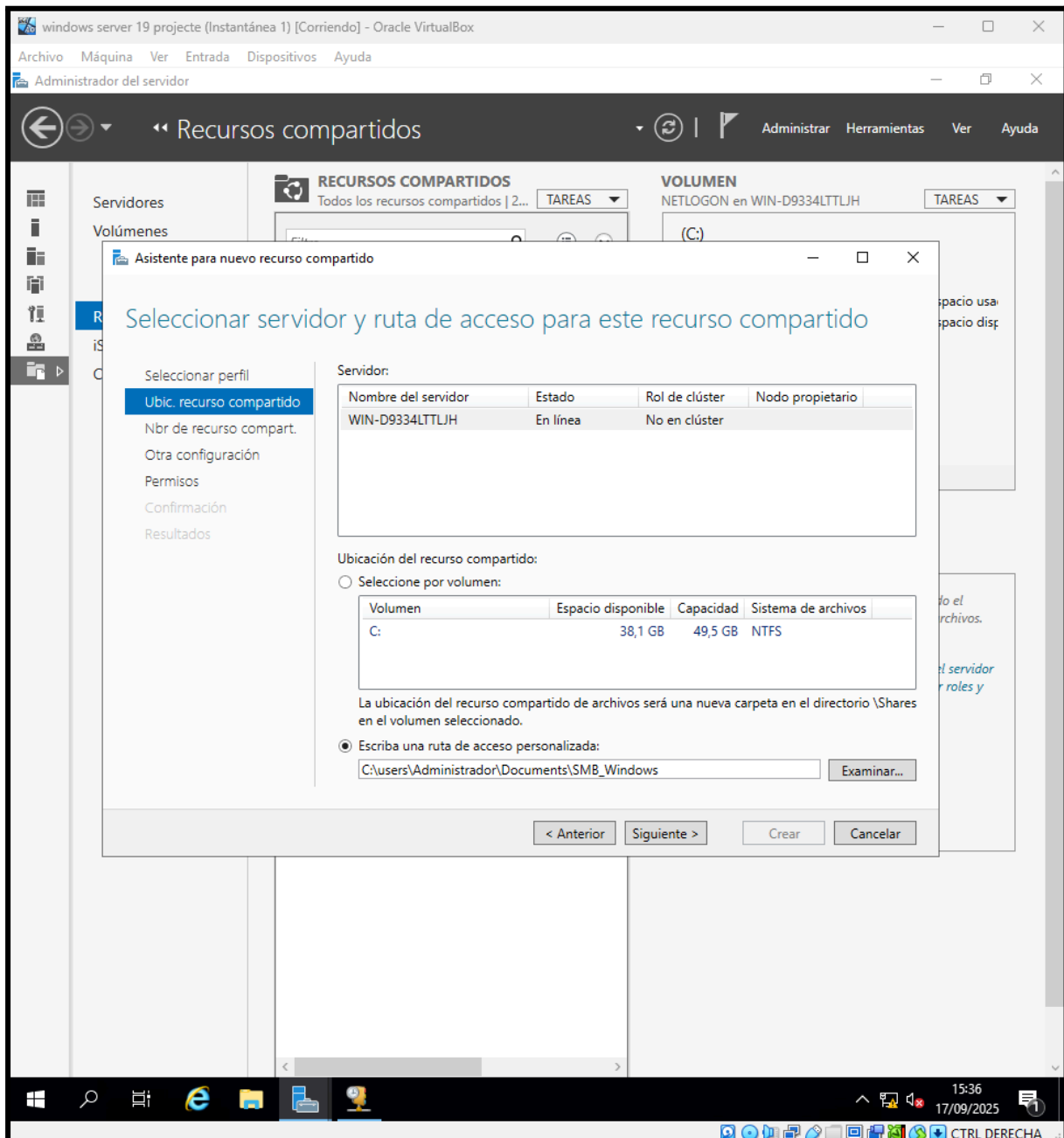
Creamos un recurso compartido con SMB





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

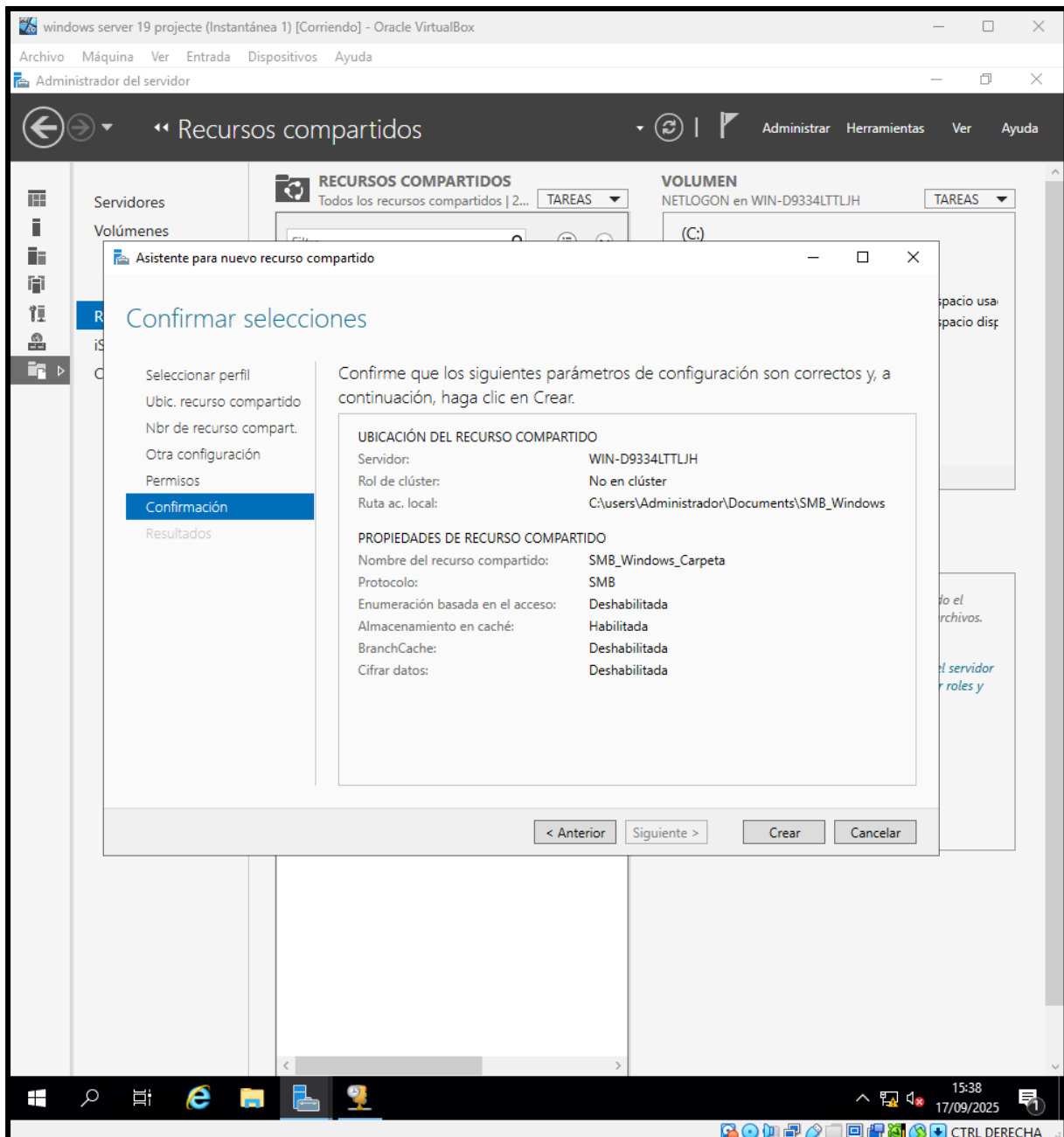
Administrador del servidor

Asistente para nuevo recurso c...

15:37 17/09/2025

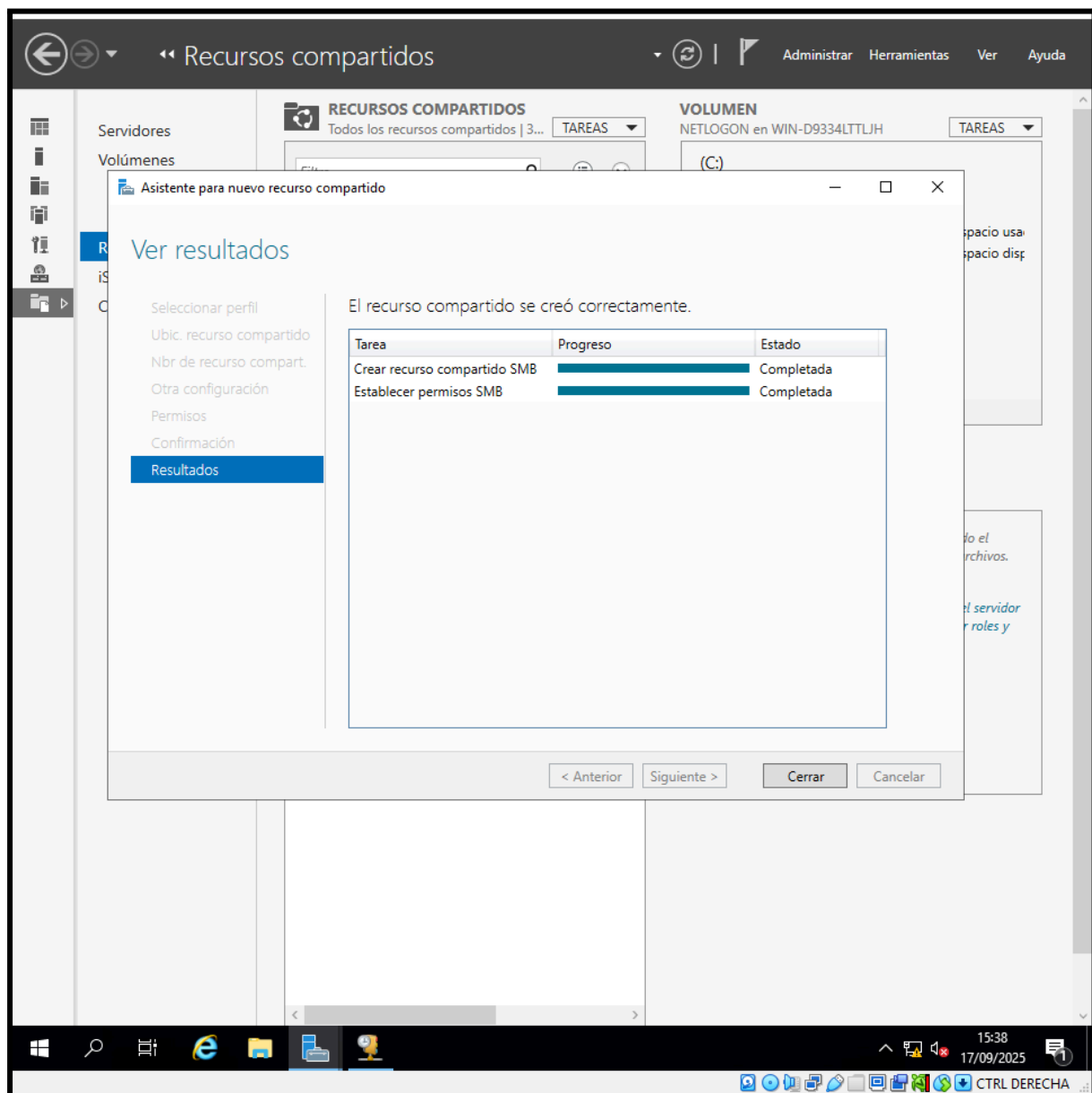


Confirmamos lo que hemos hecho anteriormente



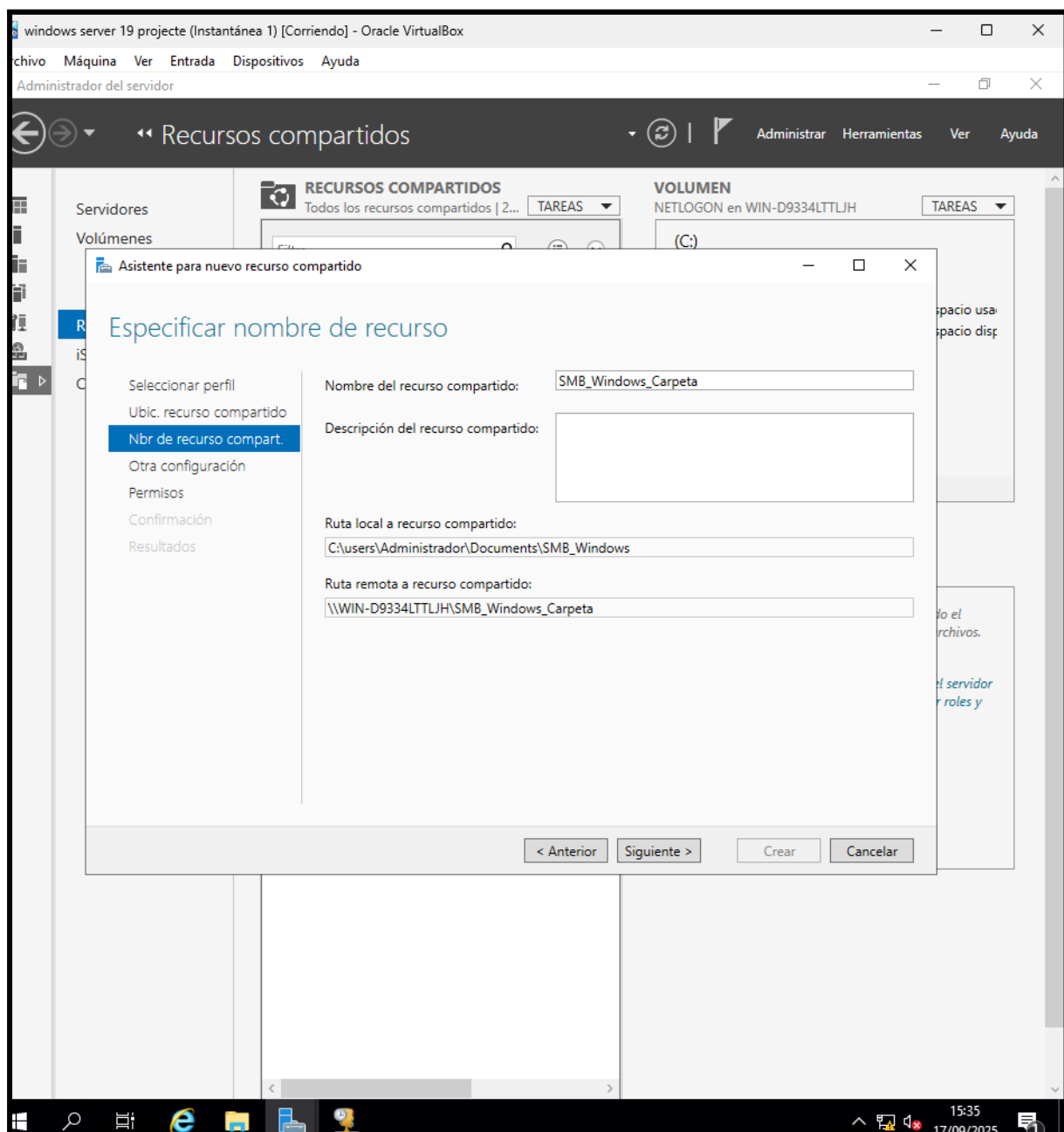


Y esperamos a que se creen los recursos





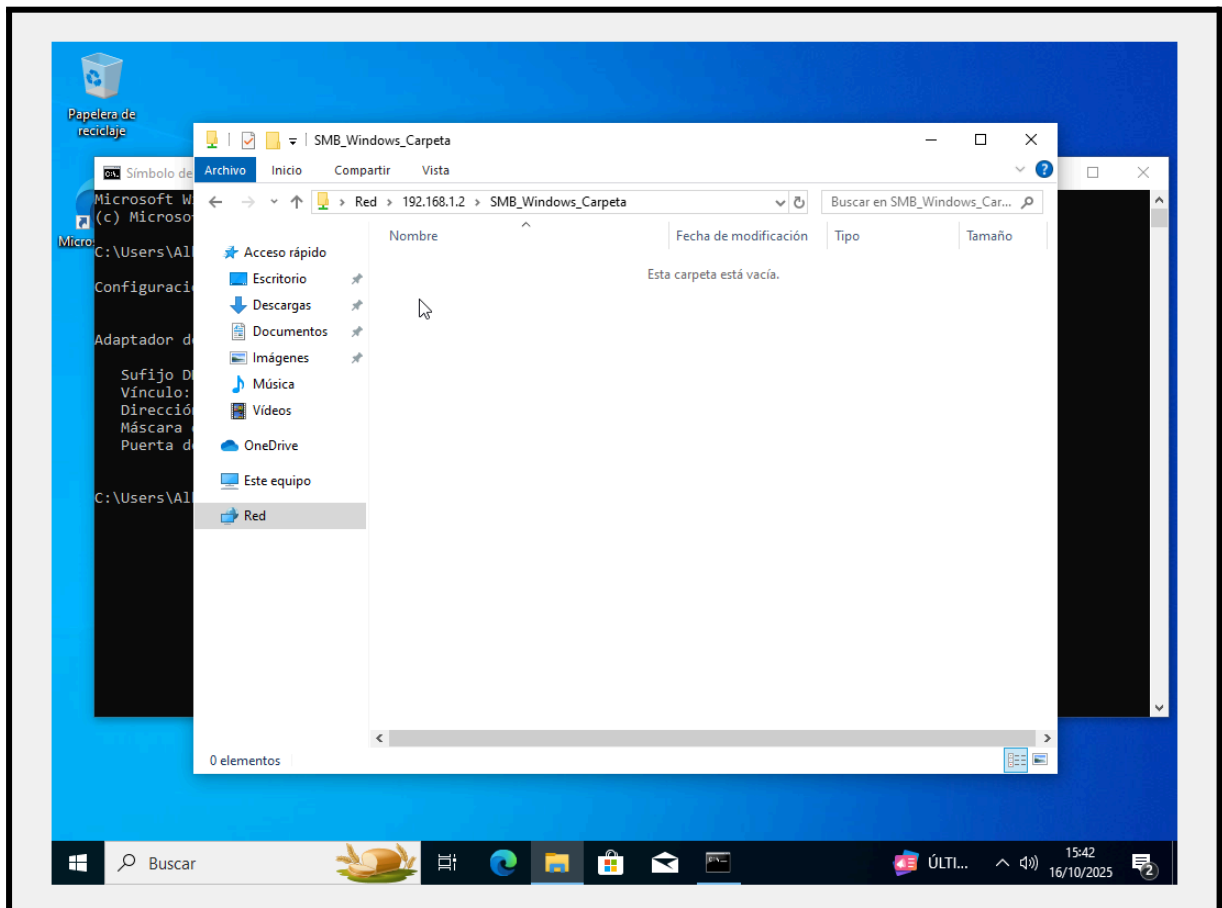
Le ponemos nombre al recurso





Comprobamos que se haya creado la carpeta compartida,

Demostración SMB



RDP

Habilitamos el acceso por escritorio remoto por RDP



PROPIEDADES
Para WIN-D9334LTLJH

Nombre de equipo: WIN-D9334LTLJH
Dominio: ciberASIX2.com

Últimas actualizaciones instaladas: Windows Update
Últimas actualizaciones buscadas: Windows Update

Firewall de Windows Defender: Privado: Activado
Administración remota: Habilitado
Escritorio remoto: Deshabilitado
Formación de equipos de NIC Ethernet: Deshabilitado
Dirección IPv4 asignada: Dirección IPv4 asignada

Propiedades del sistema

Nombre de equipo: Hardware: Opciones avanzadas: Acceso remoto

Asistencia remota

☐ Permitir conexiones de Asistencia remota a este equipo

Opciones avanzadas...

Escritorio remoto

Haga clic en una opción y especifique quién puede conectarse.

☐ No permitir las conexiones remotas a este equipo
☒ Permitir las conexiones remotas a este equipo
☒ Permitir solo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red (recomendado)

Ayúdame a elegir Seleccione usuarios...

Aceptar Cancelar Aplicar

EVENTOS
Todos los eventos | 42 en total

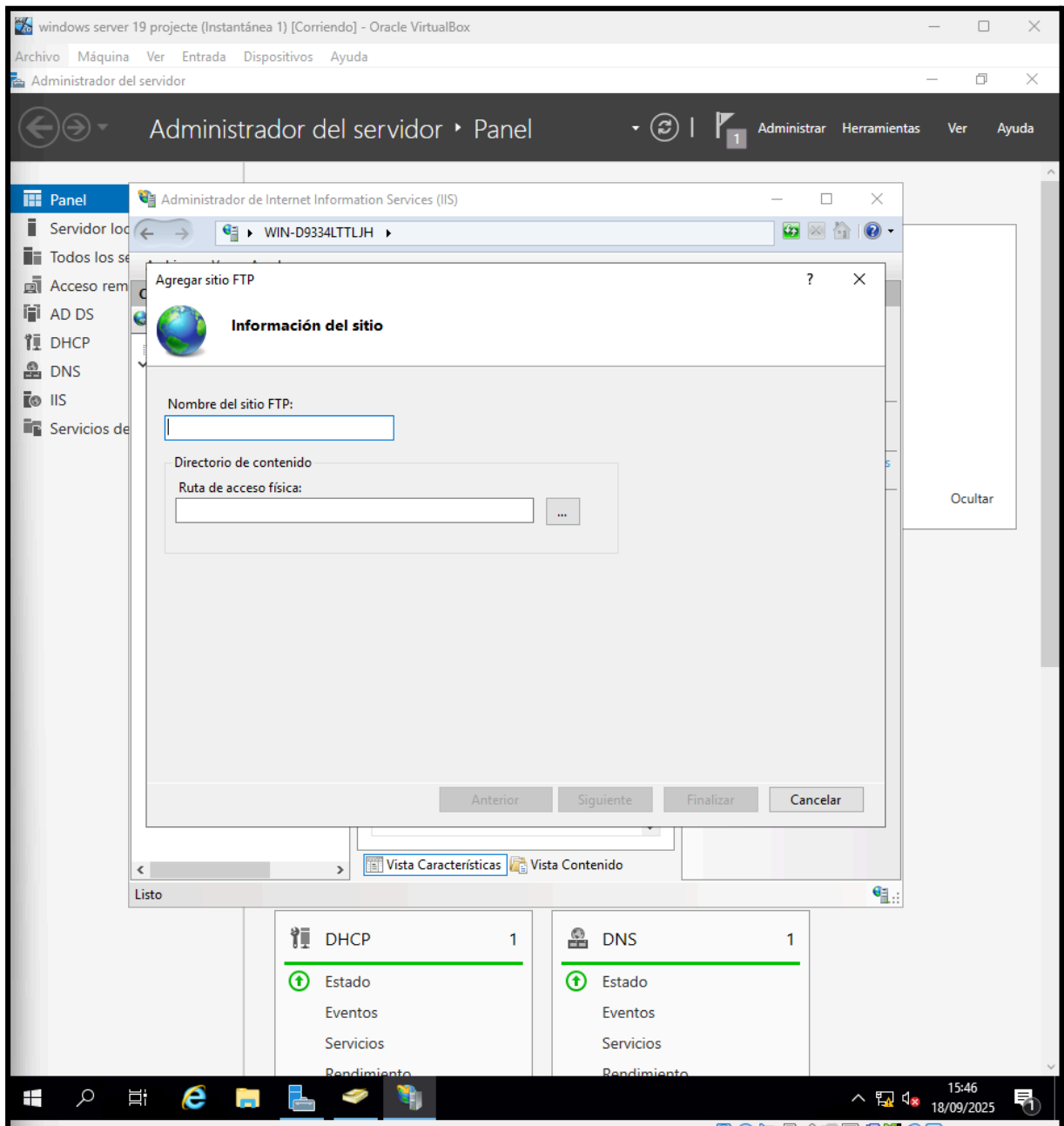
Nombre del servidor	Id.	Gravedad	Origen
WIN-D9334LTLJH	1076	Advertencia	User32
WIN-D9334LTLJH	1041	Error	Microsoft-Windows-DHCP-Server
WIN-D9334LTLJH	10020	Advertencia	Microsoft-Windows-DHCP-Server
WIN-D9334LTLJH	12	Advertencia	Microsoft-Windows-Time-Service
WIN-D9334LTLJH	10154	Advertencia	Microsoft-Windows-Windows Remote Management
WIN-D9334LTLJH	8193	Error	VSS

SERVICIOS
Todos los servicios | 215 en total

FTP

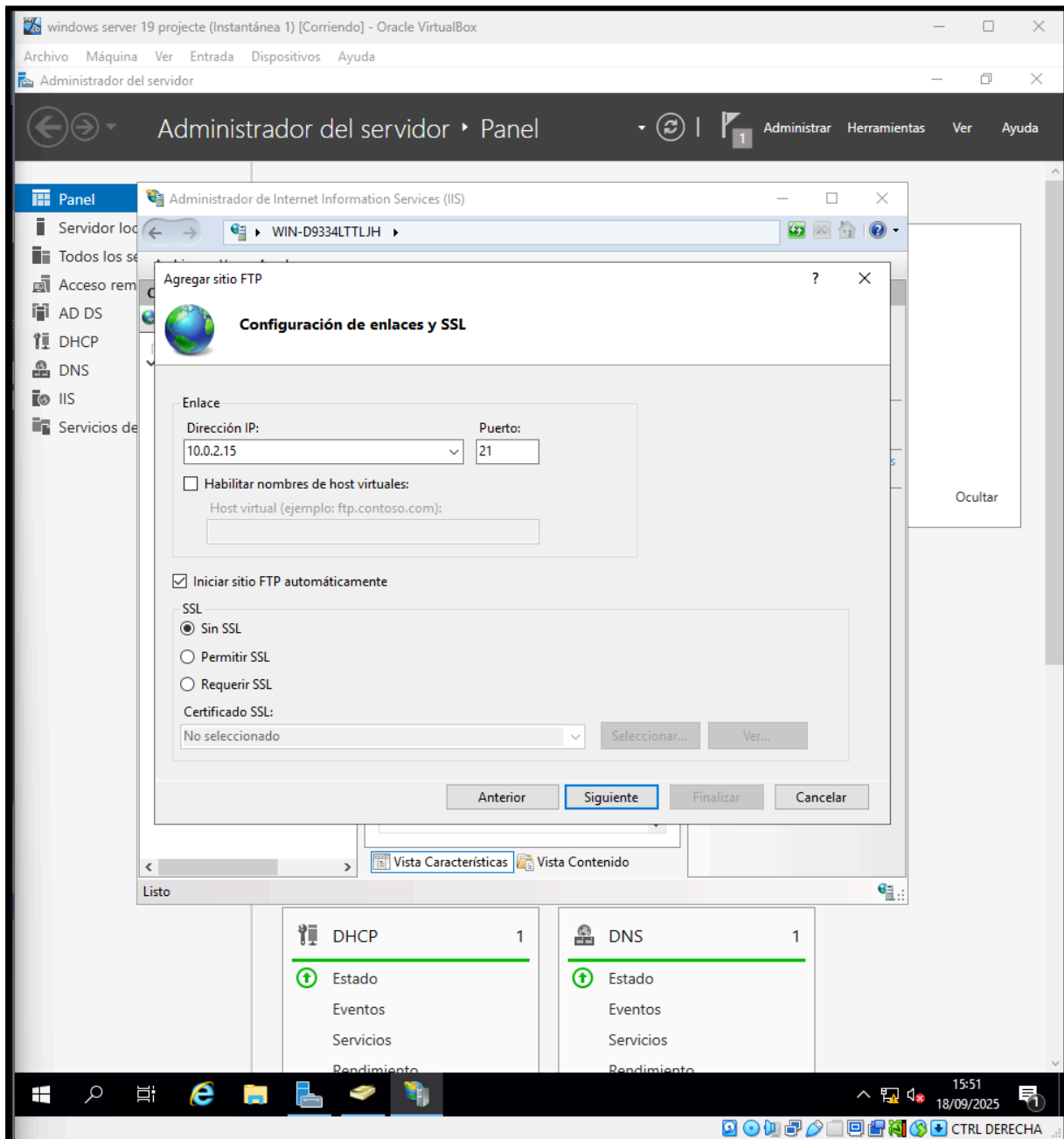
Al igual que con los roles anteriores, desde el Administrador del Servidor > Agregar roles y características, agregamos el servicio "Servidor FTP" bajo el rol de "Servicios de IIS"

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.

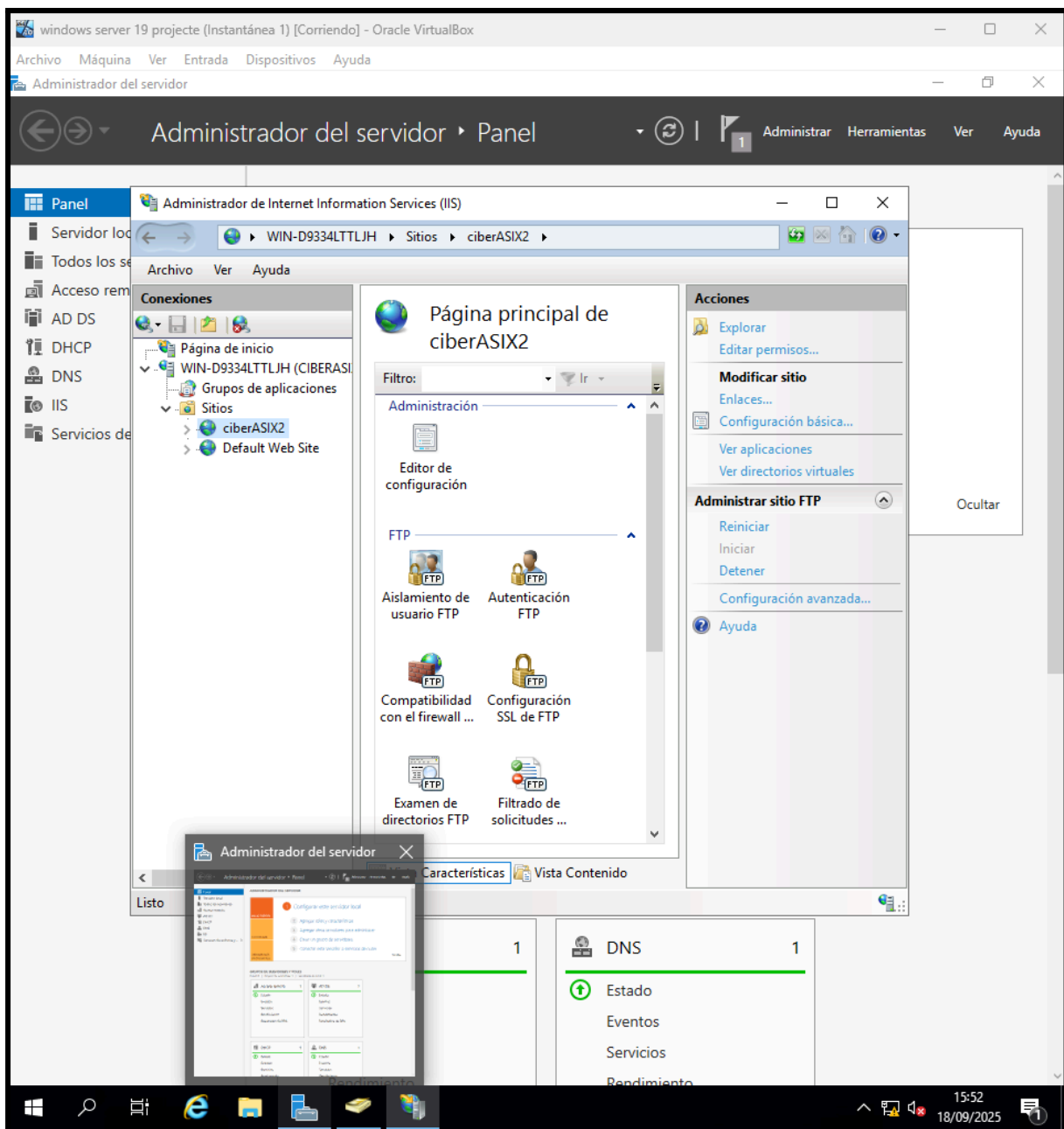


Conexión FTP establecida a 10.30.243.38. Servicio Microsoft FTP, con UTF8 habilitado. Esperando usuario.



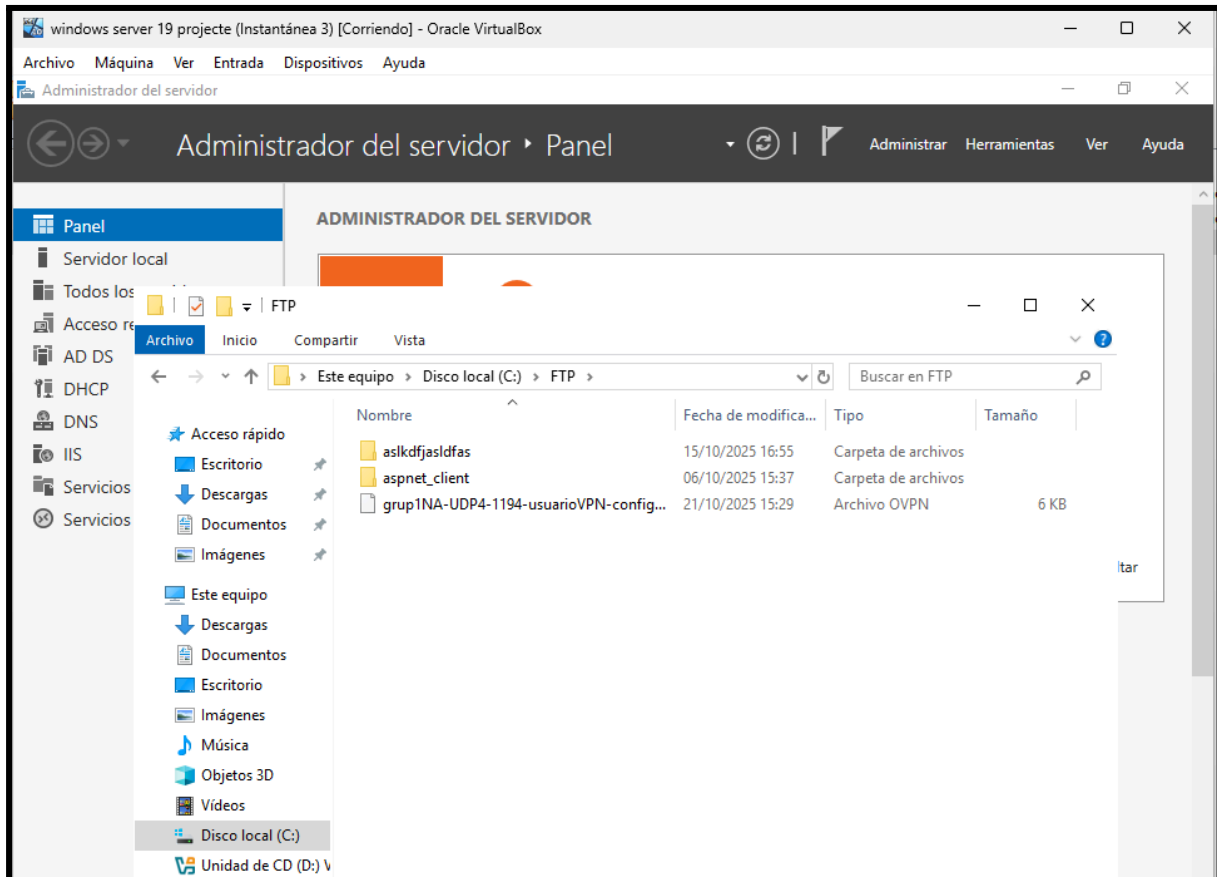
```
C:\Users\Administrador>ftp 10.30.243.38
Conectado a 10.30.243.38.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Usuario (10.30.243.38:(none)): _
```

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



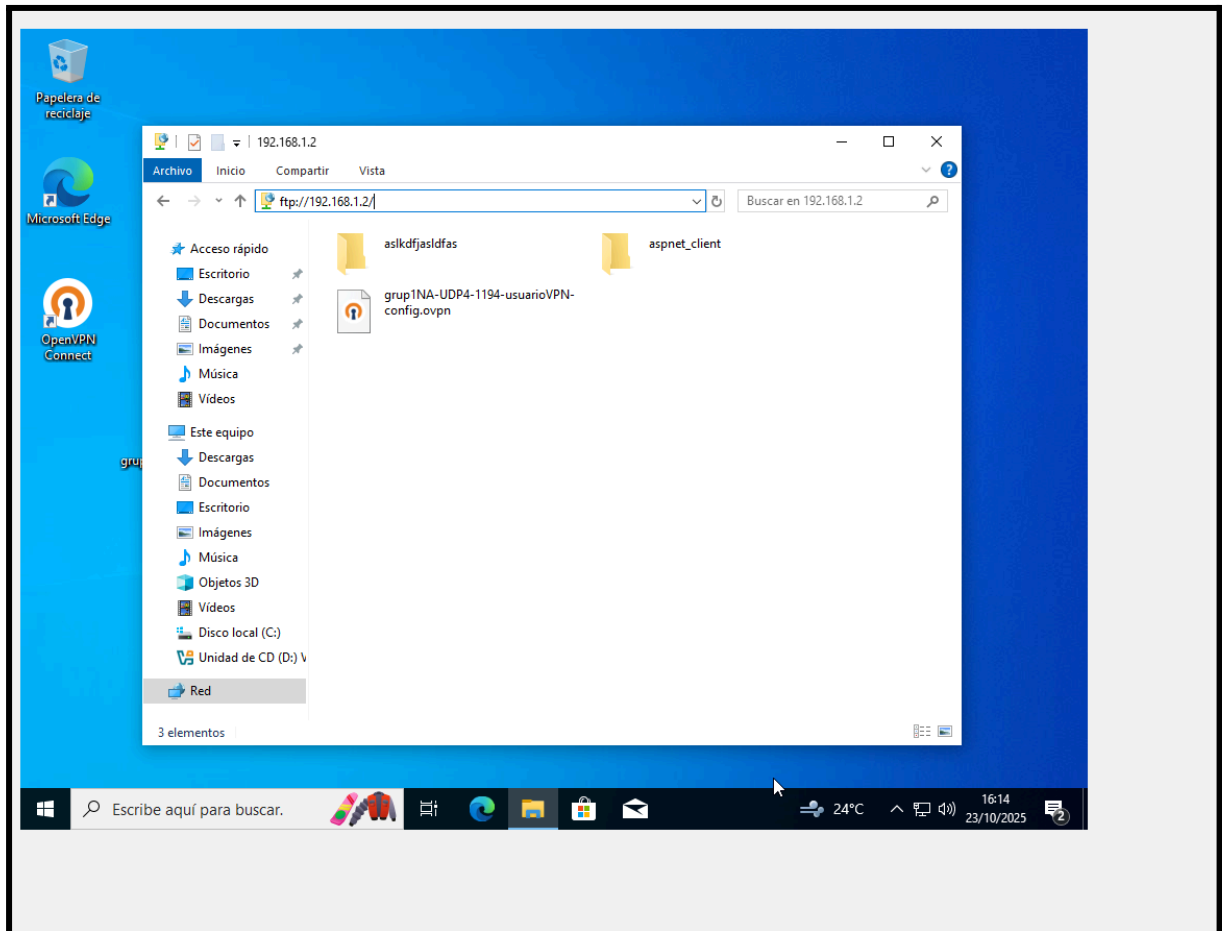


Después de crear el sitio FTP hacemos una prueba en nuestra carpeta designada ponemos un archivo en nuestro caso el archivo cliente del openvpn para ver si funciona con nuestro cliente conectado a nuestro dominio





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

Despues de hacer un comando ssh con la ip de nuestra maquina servidor podemos comprobar que el ssh funciona

```
Administrador: c:\windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.17763.3650]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.
ciberasix2\administrador@WIN-D9334LTTLJH C:\Users\Administrador>
```

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	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 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. 

ECDF 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

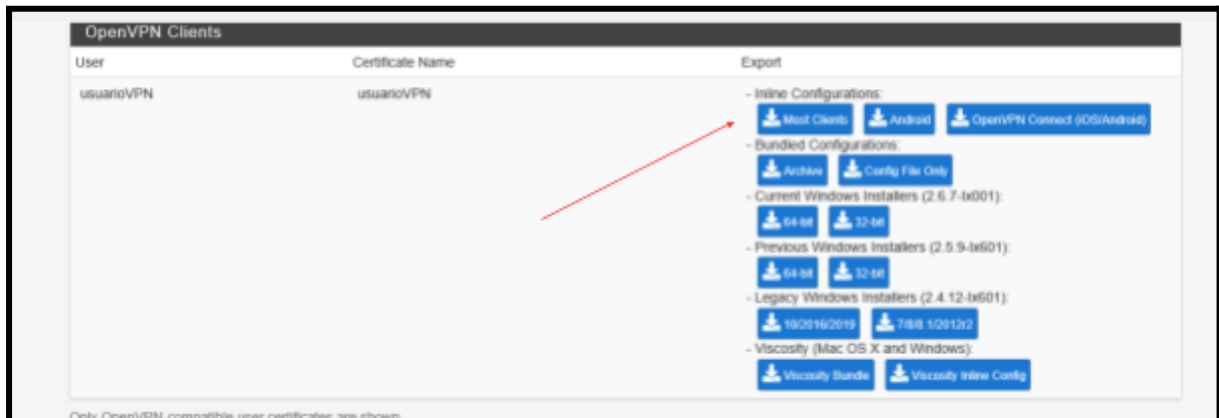
Inherited from	Name	Description	Action
			+ Add

User Certificates

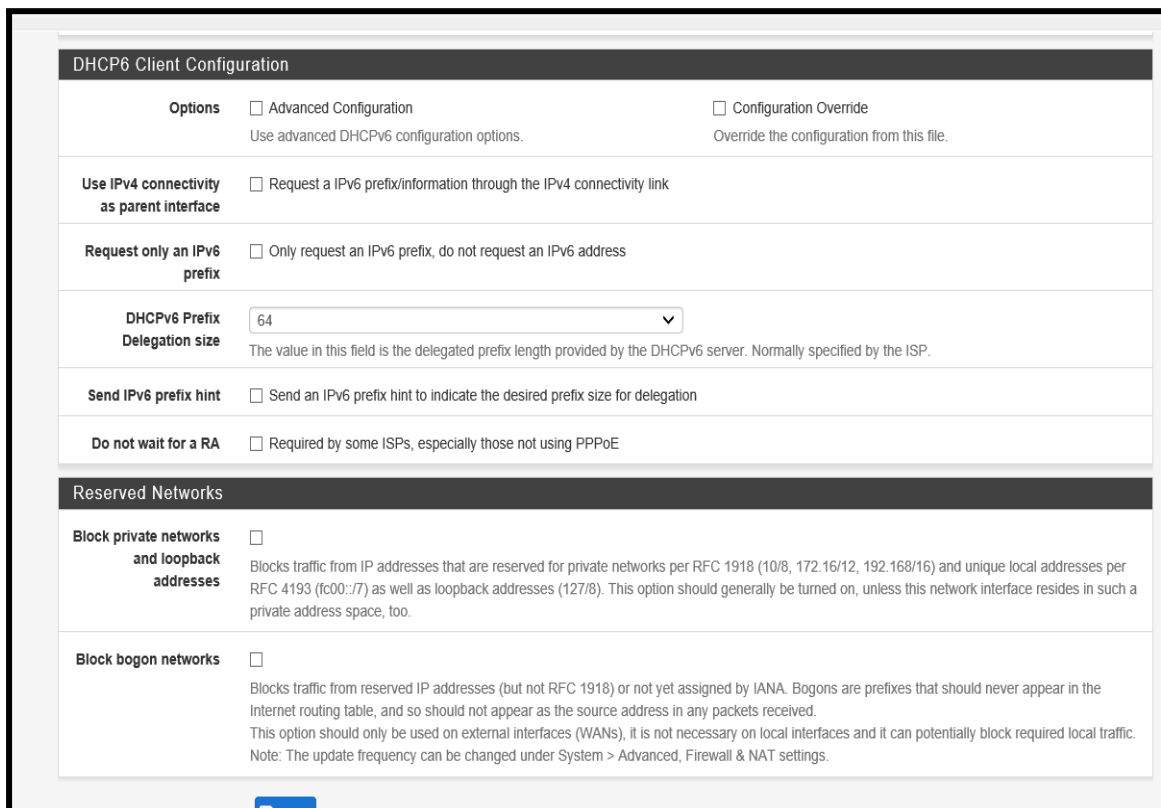
Name	CA	
usuarioVPN	CA-OpenVPN	🗑

+ Add

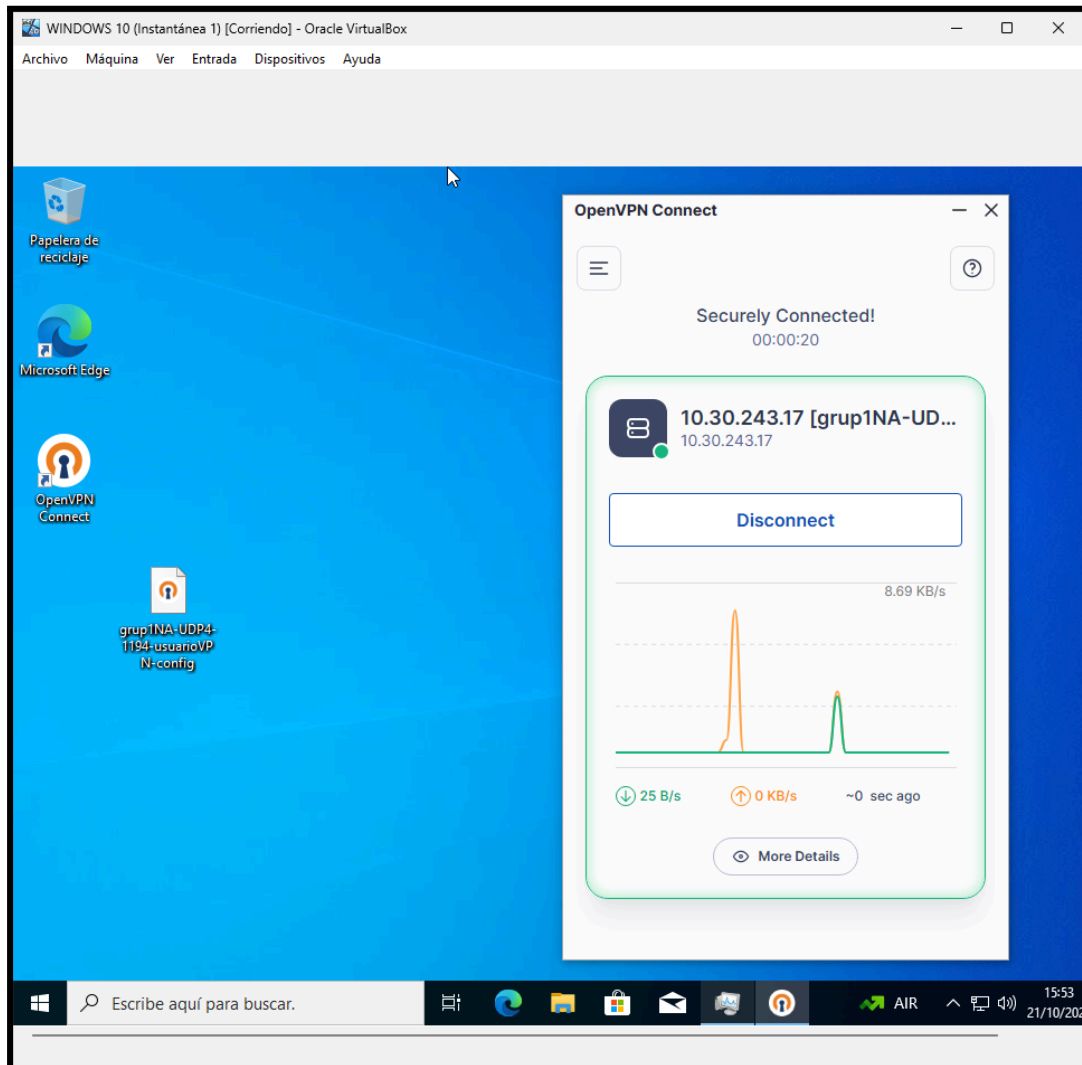
descargamos el cliente vpn



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

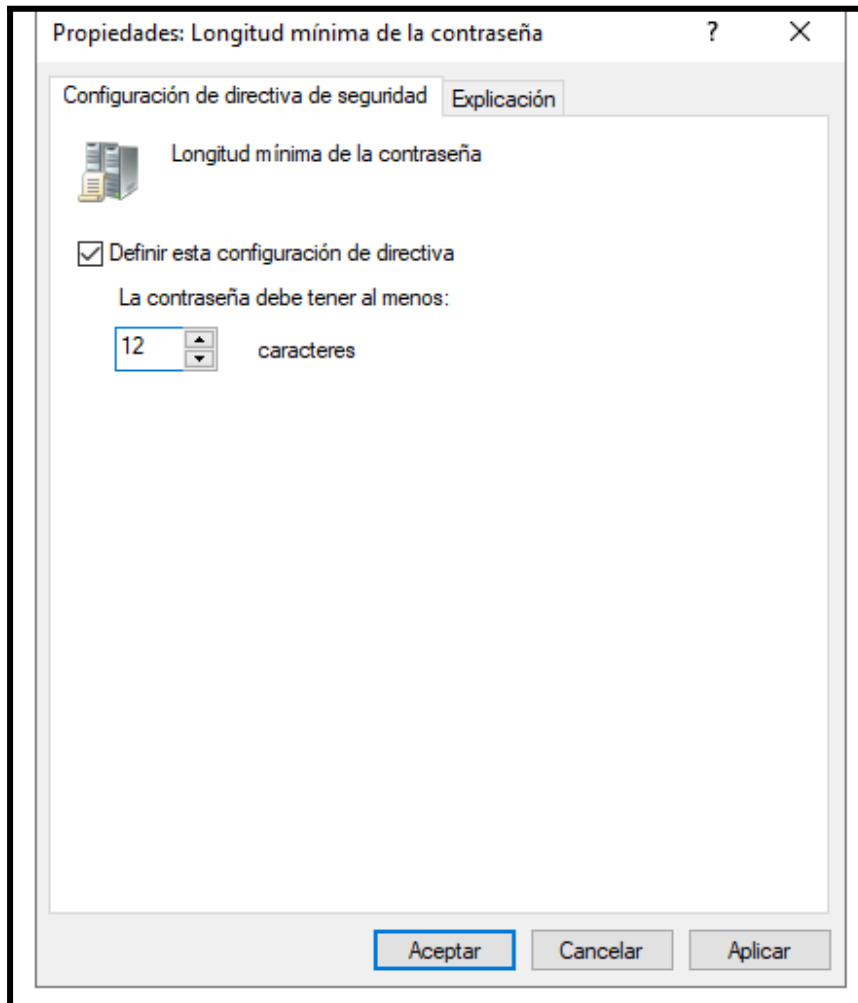


Desde el servidor nos pasamos el archivo del cliente vpn que hemos descargado desde el pfSense y a través del cliente vpn del windows 10 nos conectamos

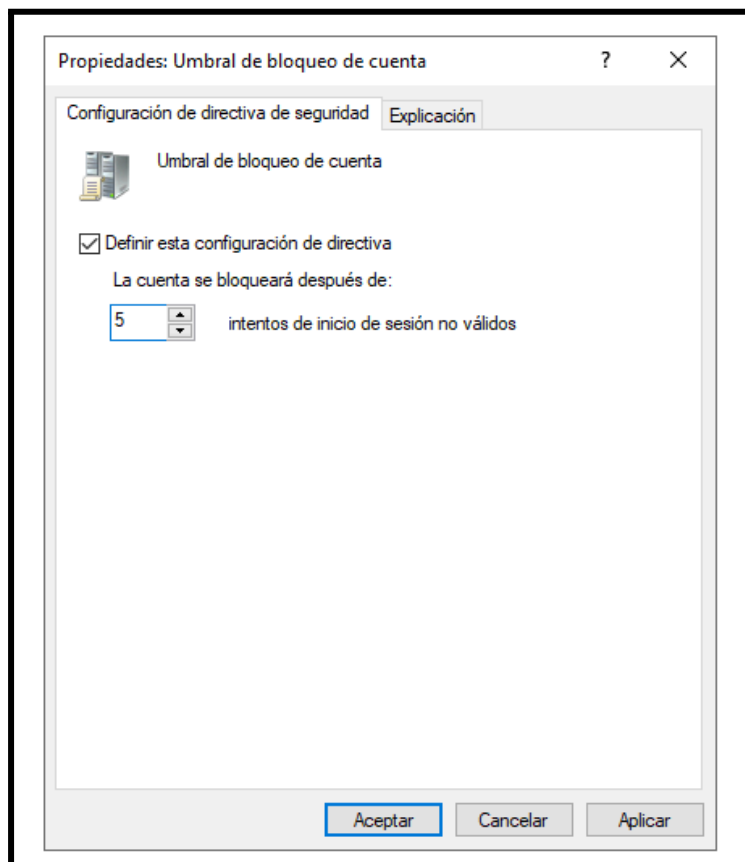


AD SG

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



Privacidad de la aplicación | **Configurar Actualizaciones** | Configuración

Configurar Actualizaciones automáticas

Valor anterior Valor siguiente

☐ No configurada Comentario:

☒ **Habilitada**

☐ Deshabilitada

Compatible con: Windows XP Professional Service Pack 1 o, como mínimo, Windows 2000 Service Pack 3
La opción 7 solo se admite en servidores que ejecuten Windows Server 2016

Opciones: Ayuda:

Actualización automática:

Automáticamente y notificar instalación

Opciones de configuración son necesarias y aplicables a la opción 4.

Intervalo de mantenimiento automático

Intervalo programado: 6 - Todos los viernes

Hora programada: 17:00

Opción 4 - Descargar automáticamente y programar la instalación el día de instalación programado y has especificado también tienes la opción de limitar la actualización a una hora, quincenal o mensual, con las opciones siguientes

Intervalo de actualización: Mensual

Intervalo de actualización: Mensual

Ayuda:

Especifica si este equipo recibirá actualizaciones de seguridad y otras descargas importantes a través del servicio de actualización automática de Windows.

Nota: Esta directiva no se aplica a Windows RT.

Esta configuración te permite especificar si se habilitan las actualizaciones automáticas en este equipo. Si se habilita el servicio, debes seleccionar una de las cuatro opciones que figuran en Configuración de directiva de grupo:

2 = Notificar antes de descargar e instalar cualquier actualización.

Quando Windows encuentre actualizaciones aplicables a este equipo, se notificará a los usuarios que hay actualizaciones listas para descargar. Los usuarios pueden descargar e instalar cualquier actualización disponible desde Windows Update.

3 = (valor predeterminado) Descargar las actualizaciones automáticamente y notificar cuando estén listas para instalarse.

Aceptar Cancelar Aplicar

Permitir actualizaciones firmadas procedentes de una ubicación...
Mostrar opciones para notificaciones de actualización