**Configuración Avanzada de Windows Server**

# Introducción.

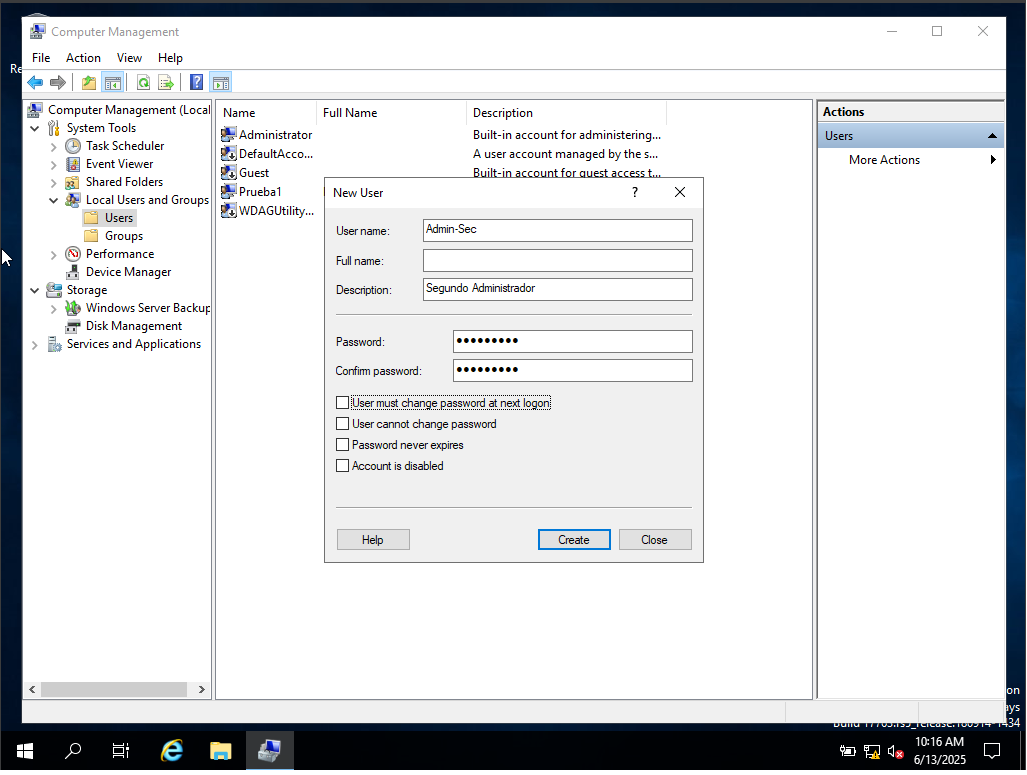
El objetivo principal es preparar una máquina con servicios básicos de red, políticas de seguridad y automatización mediante scripts.

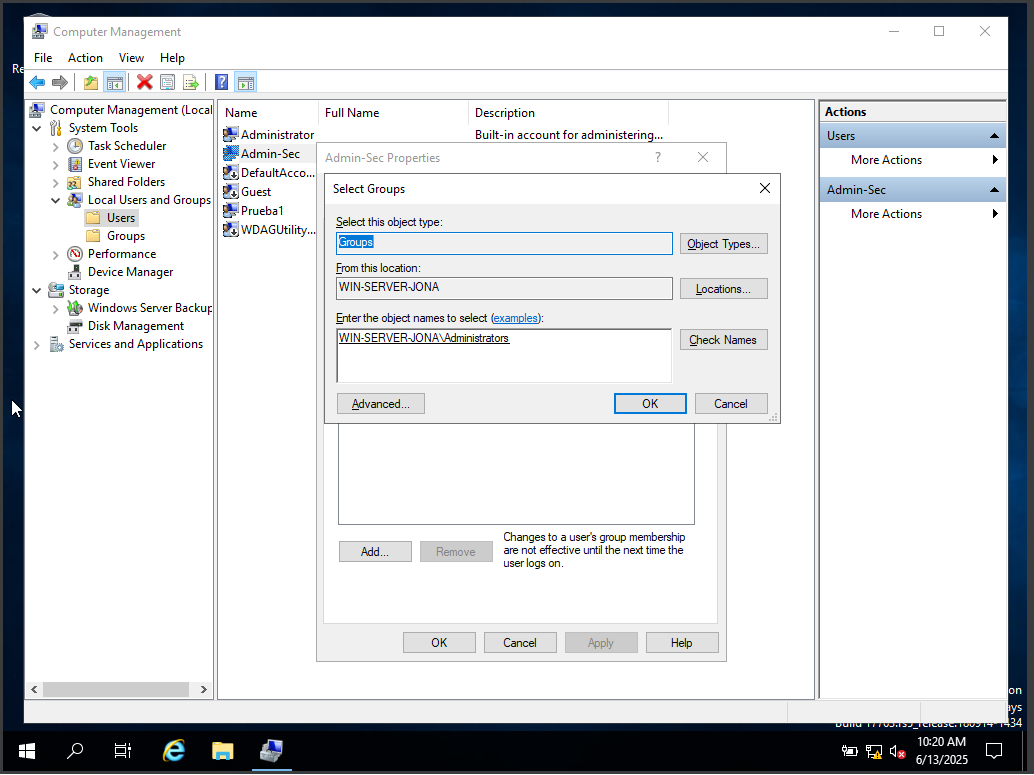
# Fase 1: Preparación del entorno y consola administrativa.

## Creación de un usuario administrador secundario.

En este primer punto vamos a realizar la creación de un segundo usuario administrativo, con una contraseña compleja para disponer de un usuario alternativo en caso de fallo o bloqueo del principal.

Ya sabemos crear usuarios, ahora tenemos que darle los privilegios de administrador para ello, nos iremos a propeties y daremos los permisos de administrador añadiendolo al grupo.



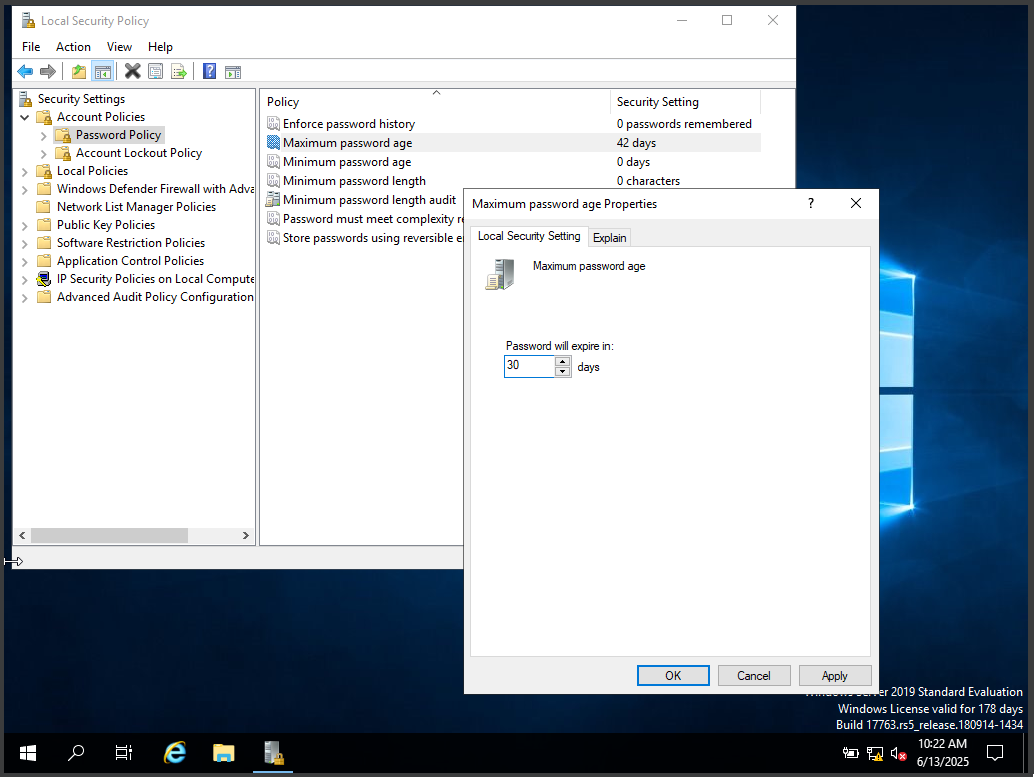


Ahora ya tenemos un segundo administrador para los problemas que podamos tener

## Configuración de directiva de caducidad de contraseñas.

Ahora queremos hacer cambios en la directiva de seguridad local y queremos que las contraseñas caduquen cada 30 días.

Para ello presionaremos la tecla de windows > run > y escribiremos secpol.msc, y nos dirigimos al apartado Account policies > Password policy y abriremos Maximum password age.



Ahora cada 30 días tendremos que renovar la contraseña.

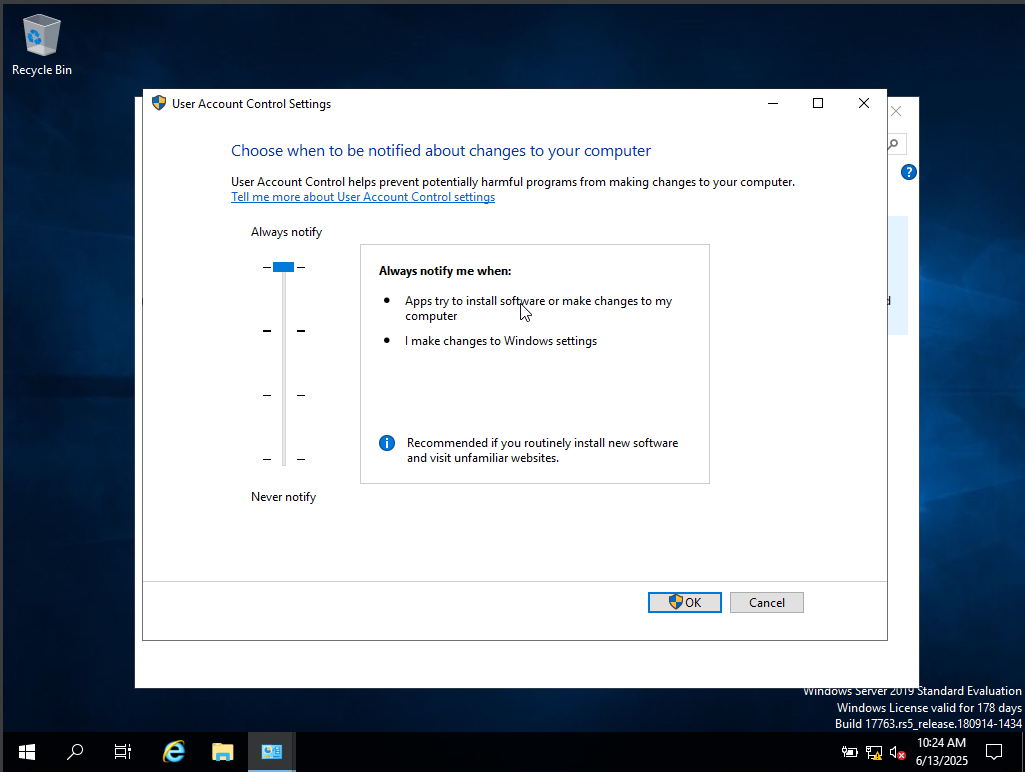
## Ajustes del Control de Cuentas de Usuario (UAC).

Vamos a modificar los valores del control de cuentas de usuario para mayor control de privilegios para tareas administrativas.

Para ello no vamos a Control Panel > User Accounts > Change user Account Control settings.

Seleccionamos el nivel alto.

Si queremos hacer un ajuste más fino podemos abrir secpol.msc desde run ir al apartado Local Policies > Security Options > User Account Control behavior for administrators in Admin Approval Mode y ahí puedes seleccionar “Prompt for consent on the secure desktop”



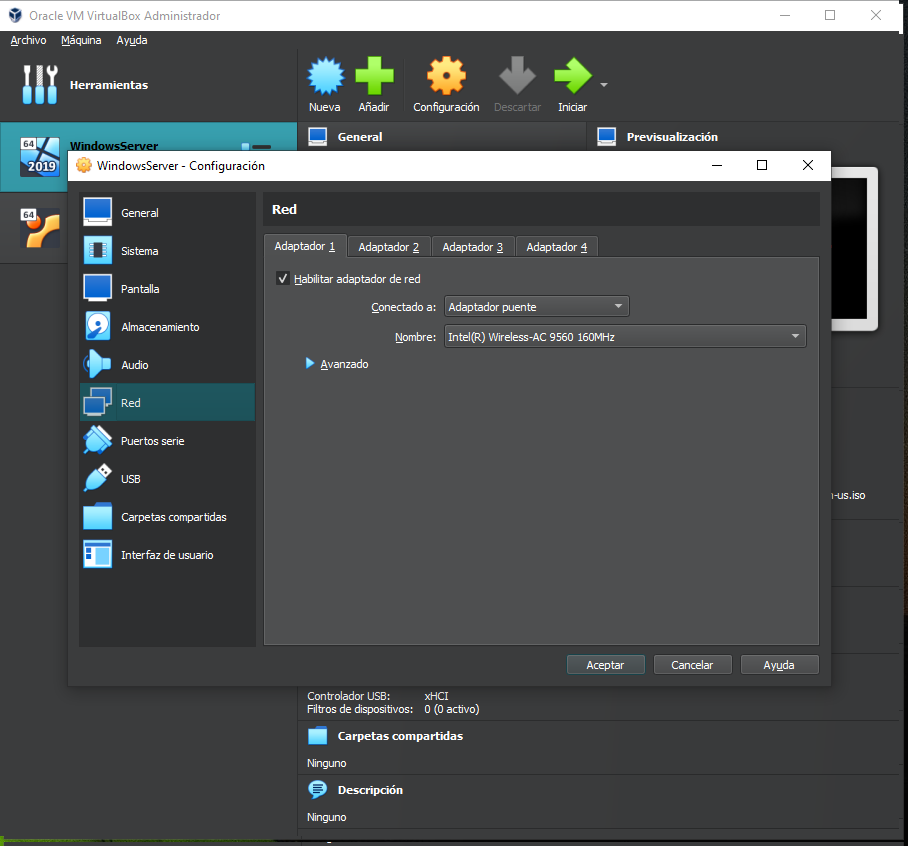
# Fase 2: Ajustes de red y servicios.

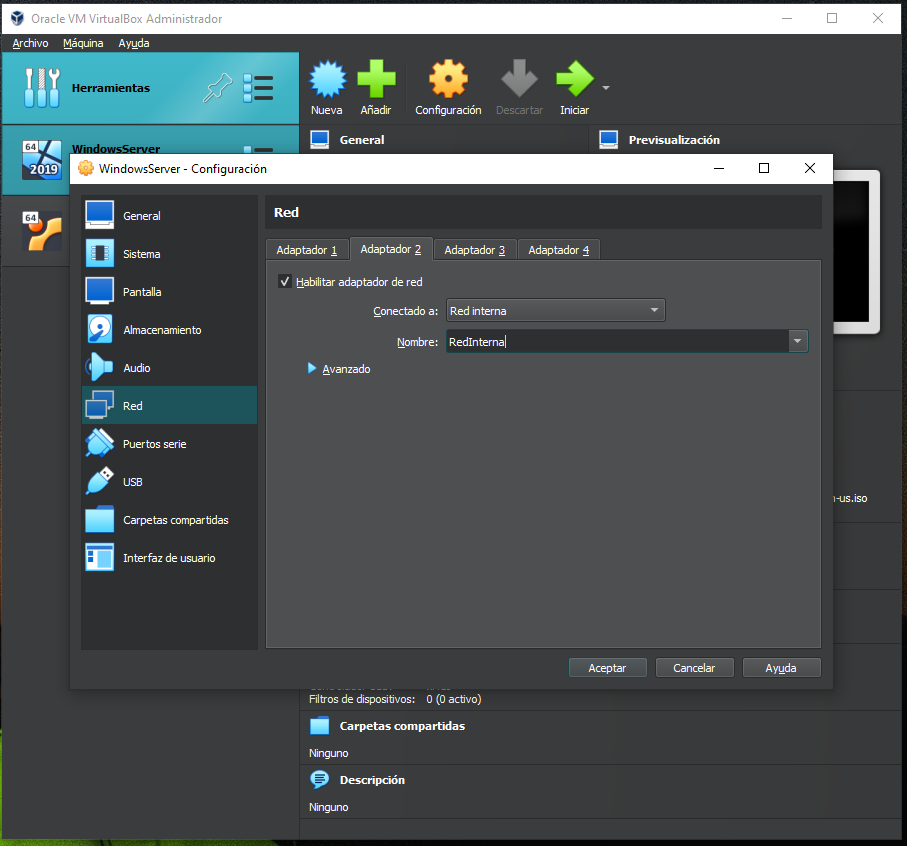
## Configuración de red con doble adaptador.

Vamos a configurar dos adaptadores de red:

* Una en modo **Bridge** (acceso a Internet desde la red física).
* Otra en modo **Interno** (para comunicación entre VMs).

En virtualbox nos iremos a la configuración de nuestra maquina al apartado Red y habilitaremos 2 adaptadores para poder configurarlos de la manera anteriormente dicha

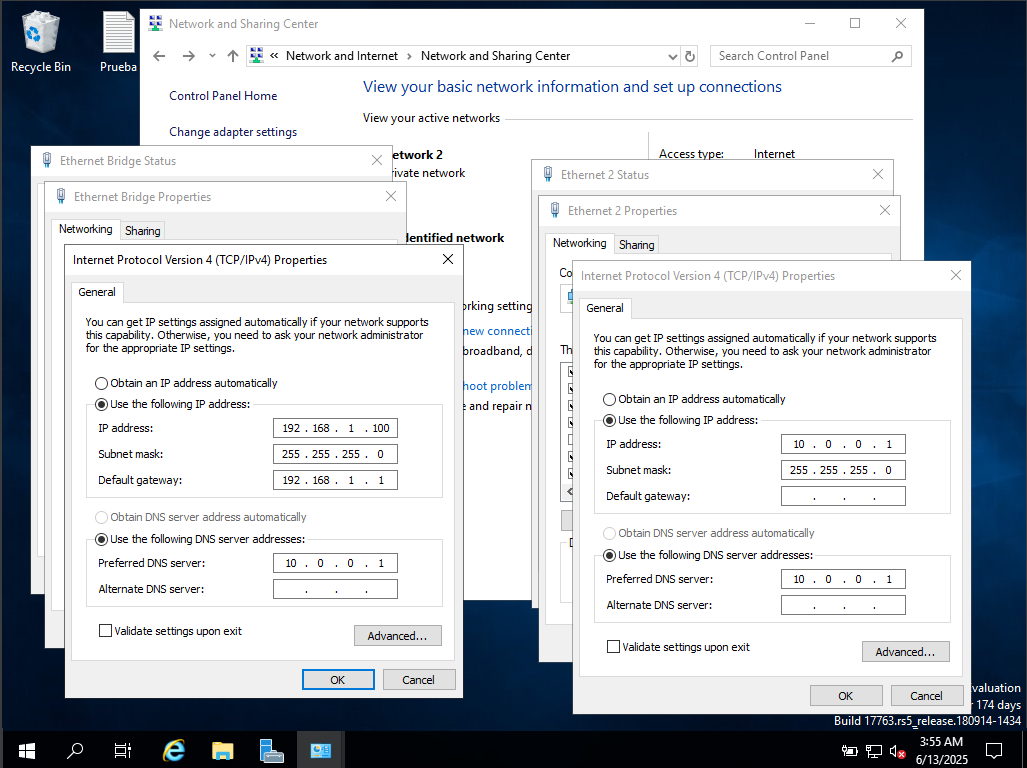


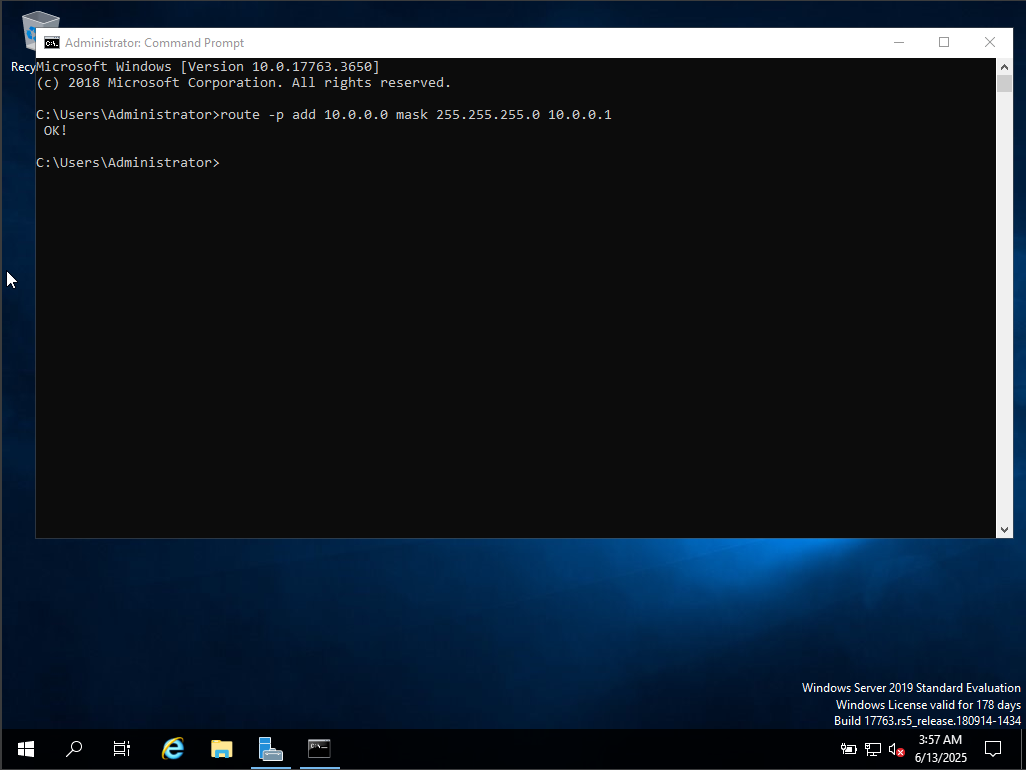


## Asignación de IP estática y Configuración de rutas estáticas.

Tendremos dos formas de realizarlo en las propiedades del adaptador de red o mediante comandos a través de la consola (cmd).

Nosotros lo hemos realizado mediante el adaptador de red iremos a sus propiedades y cambiaremos los dos adaptadores.





## Implementación de un servidor DNS local.

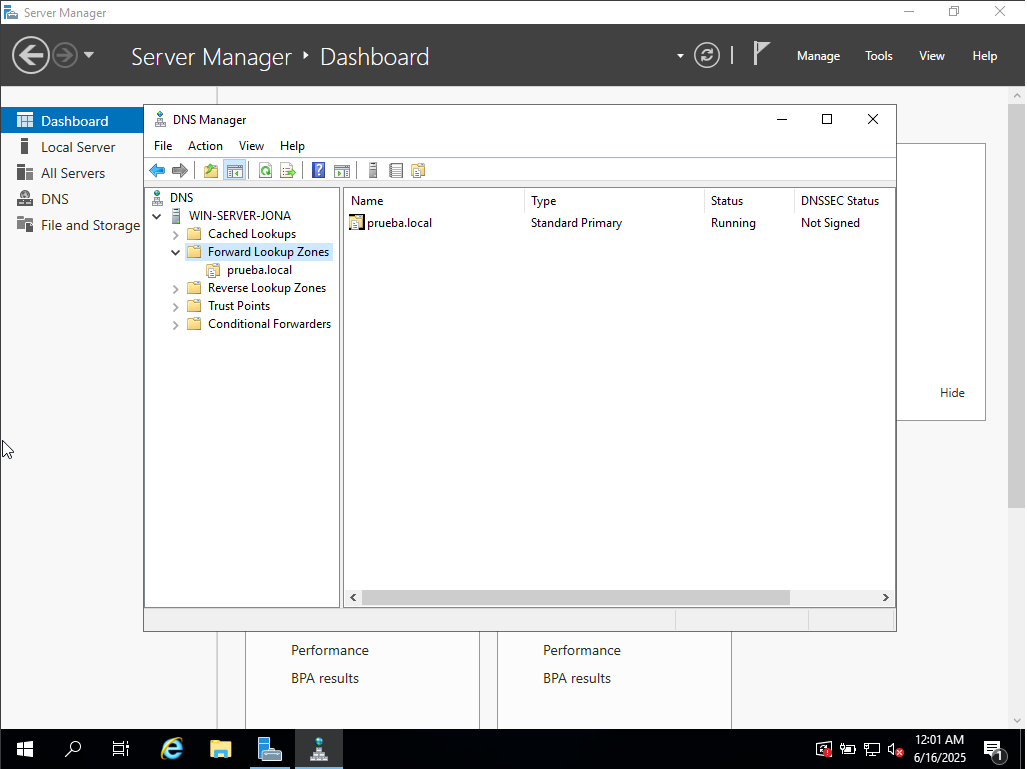
Lo primero es instalar y configurar el rol dns, no vamos a Server Manager > Manage > Add Roles and Features, instalamos el rol DNS server.

## 

Ahora vamos a crear una zona nueva para luego acto seguido crear los dos registros.

En Server Manager nos vamos al apartado de Tools > DNS.

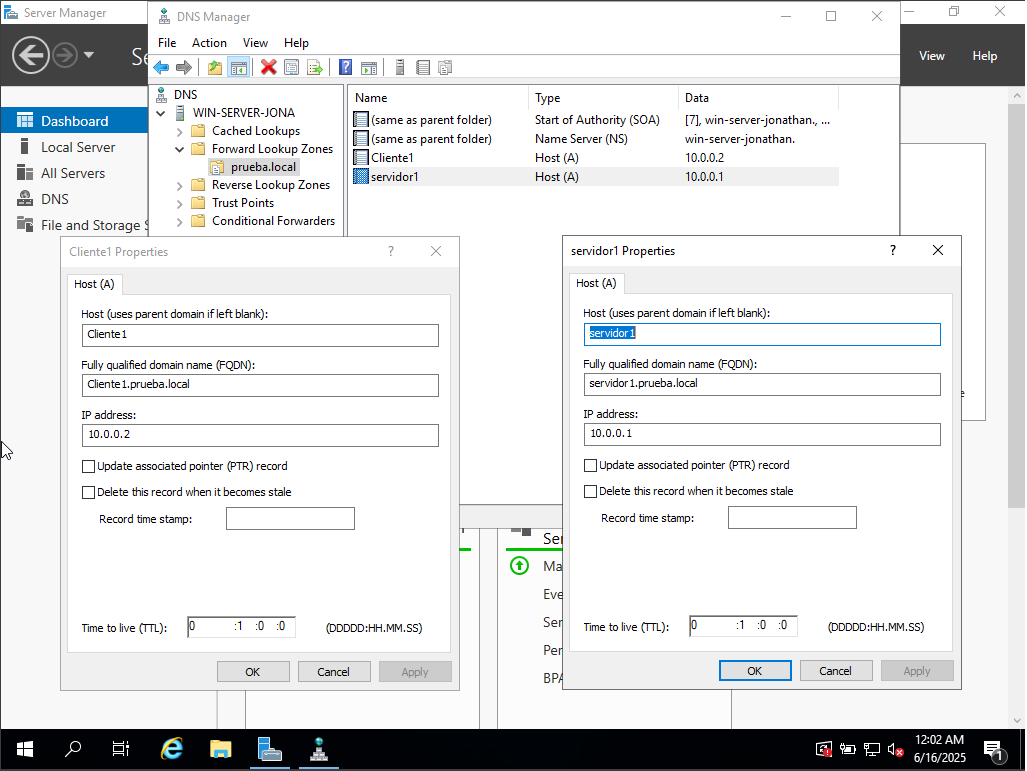
Botón derecho en Forward Lookup Zones > New Zone creamos una zona nueva “prueba.local”



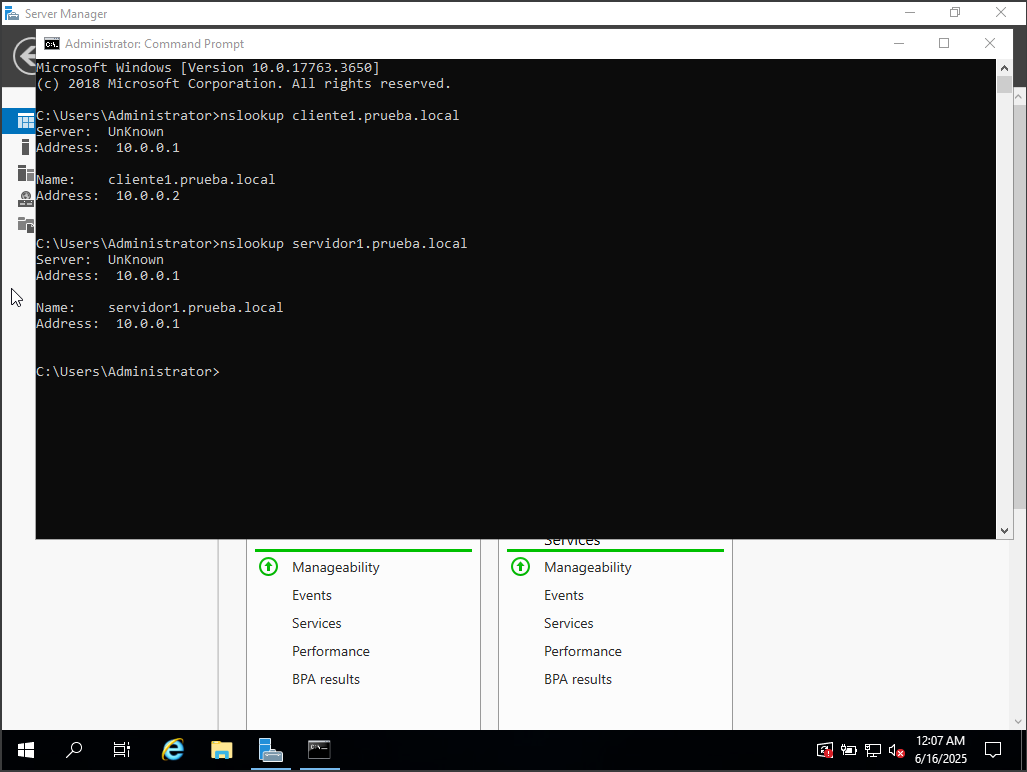
Dentro de esta zona “prueba.local” creamos dos registros

* **host 1:** cliente1
* **host 2:** servidor1

y añadiremos una ip.



Así ya tendremos nuestro servidor DNS operativo, y realizaremos una prueba en la consola de comandos con nslookup, para ver que todo funciona correctamente.



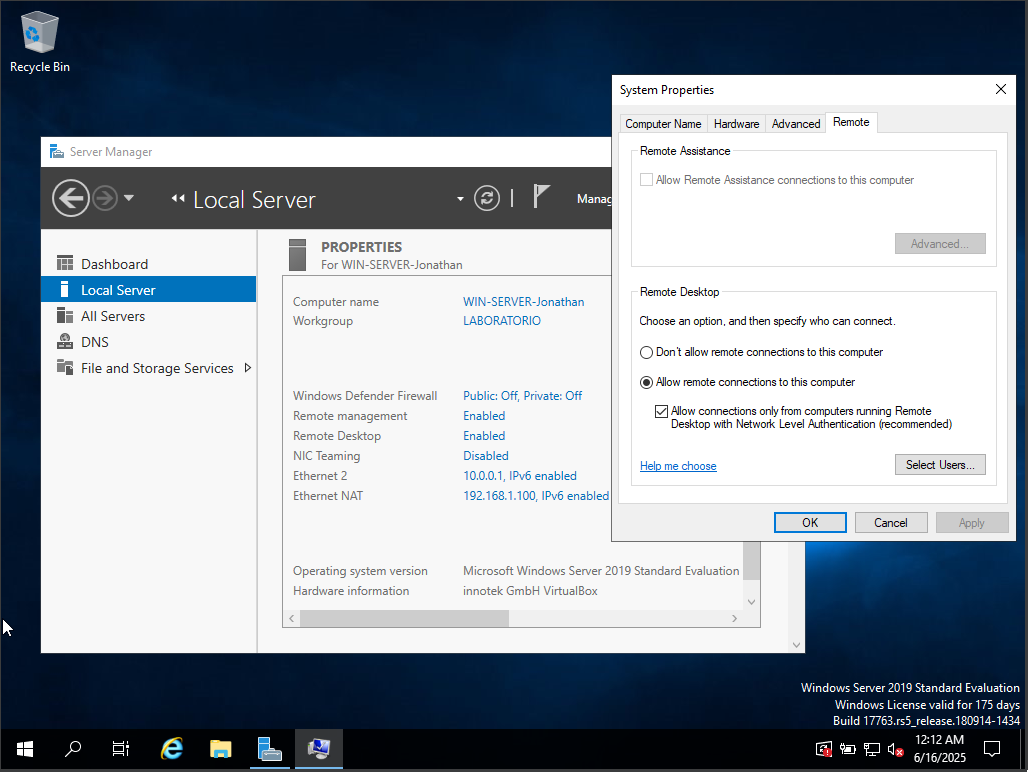
# Fase 3: Personalización del entorno de trabajo del servidor.

## Habilitación del Escritorio Remoto.

Vamos a habilitar el escritorio remoto, tecla Windows > Server Manager > Local Server.

Buscamos la opción Remote Desktop y lo cambiamos a Enabled.

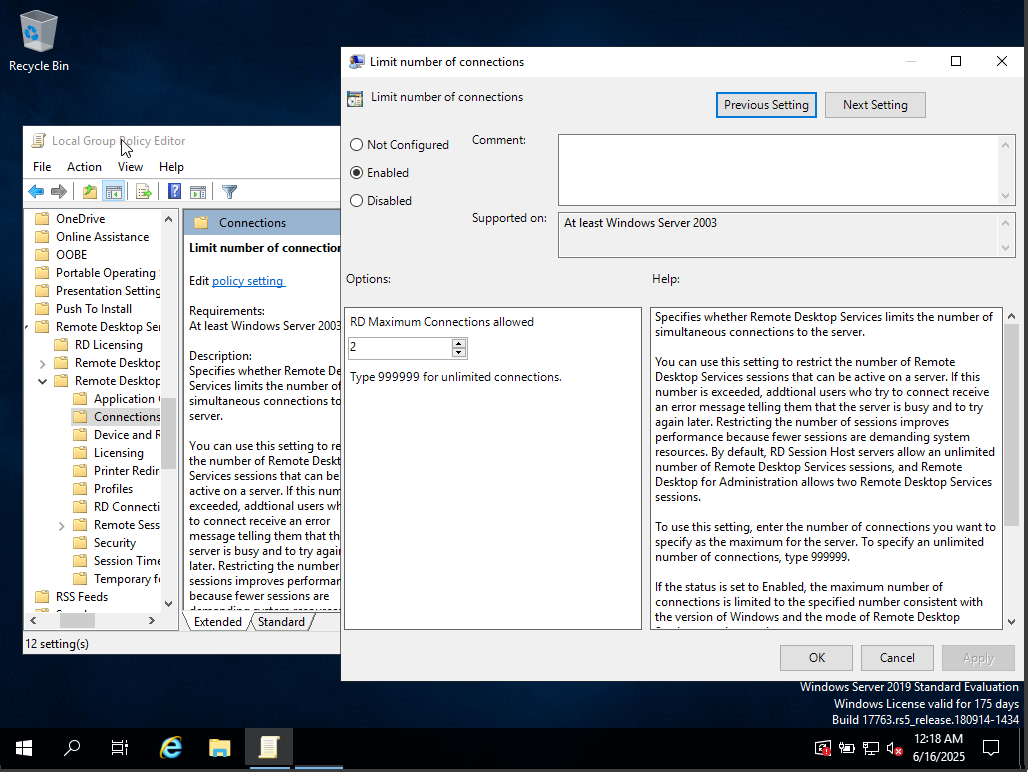
Si nos pregunta por el firewall, permite la excepción automáticamente.



Y vamos a limitar el número de sesiones a 2:

Abre el Editor de directivas de grupo local desde Windows > Run> gpedit.msc.

Nos dirigimos a Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections Activamos la opción Limit number of connections, ponemos el valor 2 aplicamos y aceptamos.

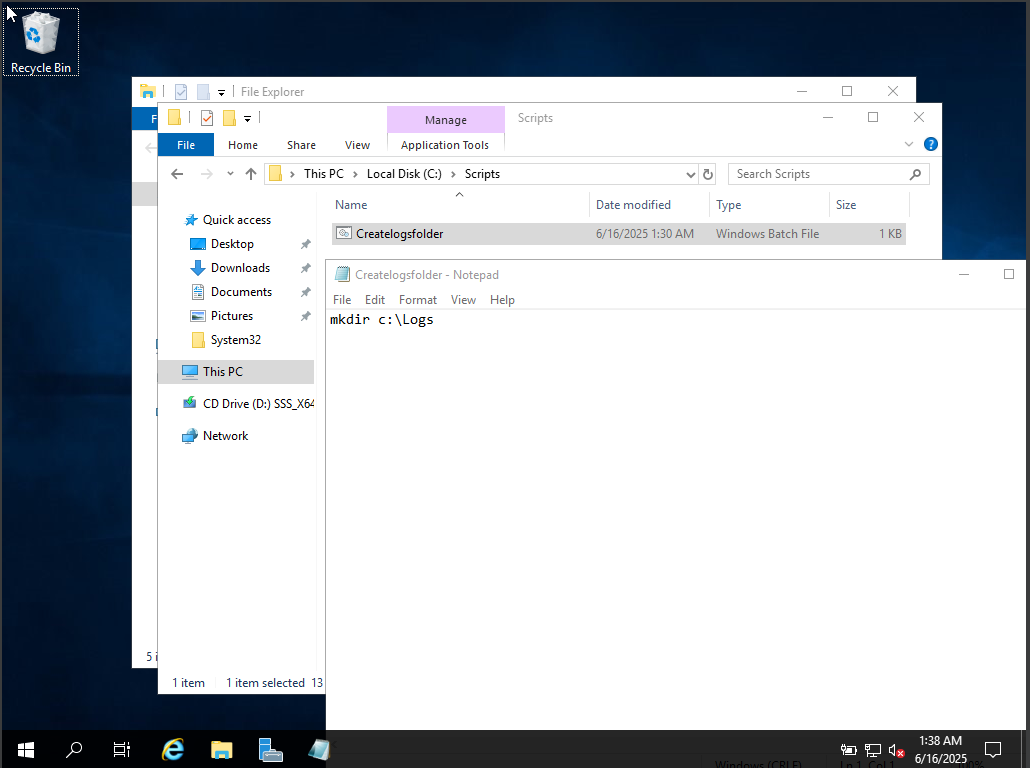


## Script de inicio para creación de logs.

Vamos a crear un script para que cree una carpeta de logs, abrimos el Bloc de notas y escribiremos

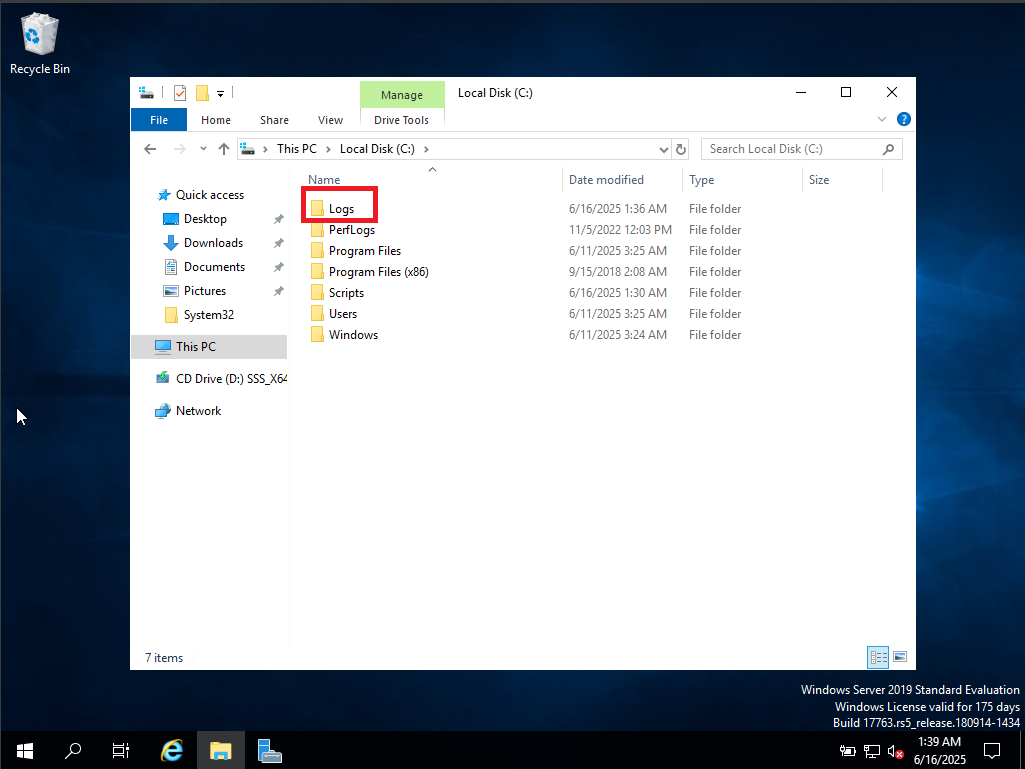
* **mkdir C:\Logs**

Y guardamos el archivo Createlogsfolder.bat con la extensión bat para que así sea ejecutable.



Ahora abrimos gpedit.msc como ya sabemos a través de Run, y nos dirigimos a Computer Configuration > Windows Settings > Scripts (Startup/Shutdown), hacemos doble clic en Startup y agregamos el script Createlogsfolder.bat.

Ahora cada vez que arranque el servidor, se asegurará que la carpeta existe.



## Configuración del firewall.

## Vamos a restringir el tráfico de red del servidor:

* Conexión entrantes por RDP (puerto 3389)
* Consultas DNS (puerto 53)

Vamos a abrir el Firewall de Windows defender, Control Panel > System and Security > Windows Defender Firewall > Advanced settings.

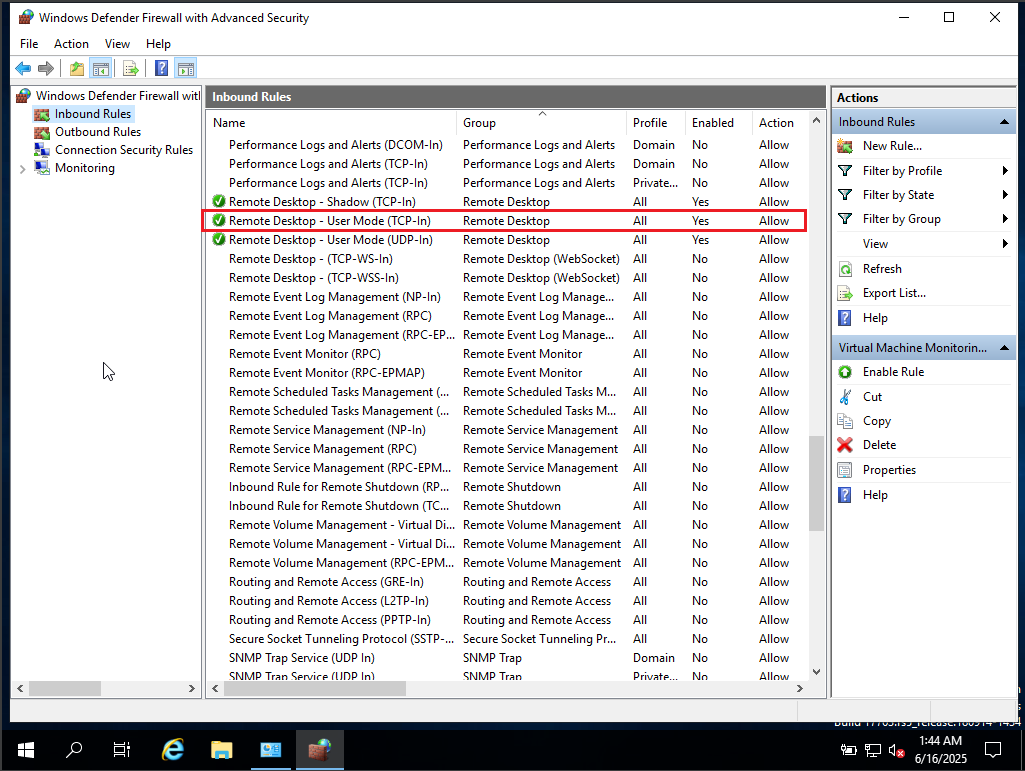
Vamos habilitar la regla:

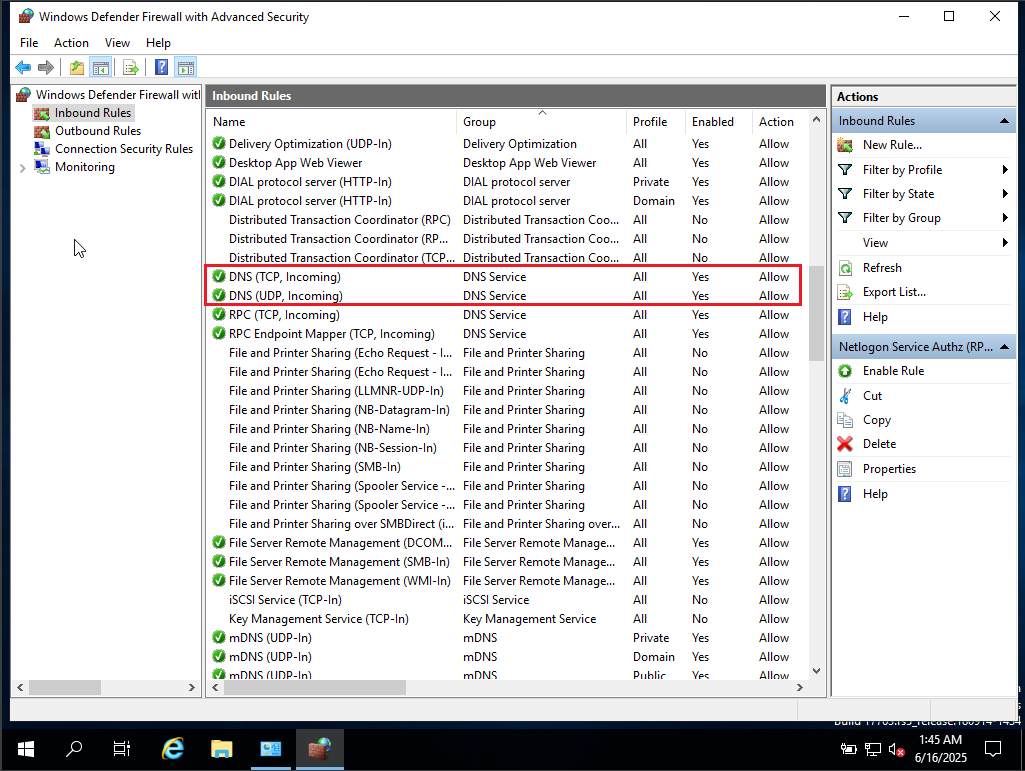
**➔ Permitir RDP:**

* Regla: **Remote Desktop - User Mode (TCP-In)**.
* Estado: **Enabled**.

#### **➔ Permitir DNS:**

* Regla: **DNS Server (UDP-In)** y **DNS Server (TCP-In)**.
* Estado: **Enabled**.





Listo, también podemos crear una regla de Outbound & Inbound que bloquee cualquier otra conexión no permitida.

# Fase 4: Automatización básica.

# Vamos a crear un script en PowerShell que realice las siguientes tareas:

* Crear una carpeta con la fecha actual.
* Copiar archivos del escritorio a esa carpeta.
* Generar un log en .txt con el resultado de la copia.

Abrimos el PowerShell y escribimos el código para que realice estas funciones y vamos a ir definiendo los puntos de cada comando.

**# Definir la ruta del escritorio del usuario actual**

$DesktopPath = [Environment]::GetFolderPath("Desktop")

**# Definir la ruta donde crear las carpetas de copia**

$BackupRoot = "C:\Backups"

**# Crear la carpeta de backups si no existe**

if (!(Test-Path $BackupRoot)) {

New-Item -ItemType Directory -Path $BackupRoot

}

**# Obtener la fecha actual en formato YYYY-MM-DD**

$Date = Get-Date -Format "yyyy-MM-dd"

**# Crear la carpeta con la fecha actual**

$BackupFolder = "$BackupRoot\$Date"

if (!(Test-Path $BackupFolder)) {

New-Item -ItemType Directory -Path $BackupFolder

}

**# Definir el archivo de log**

$LogFile = "$BackupFolder\backup\_log.txt"

**# Copiar los archivos del escritorio al backup**

try {

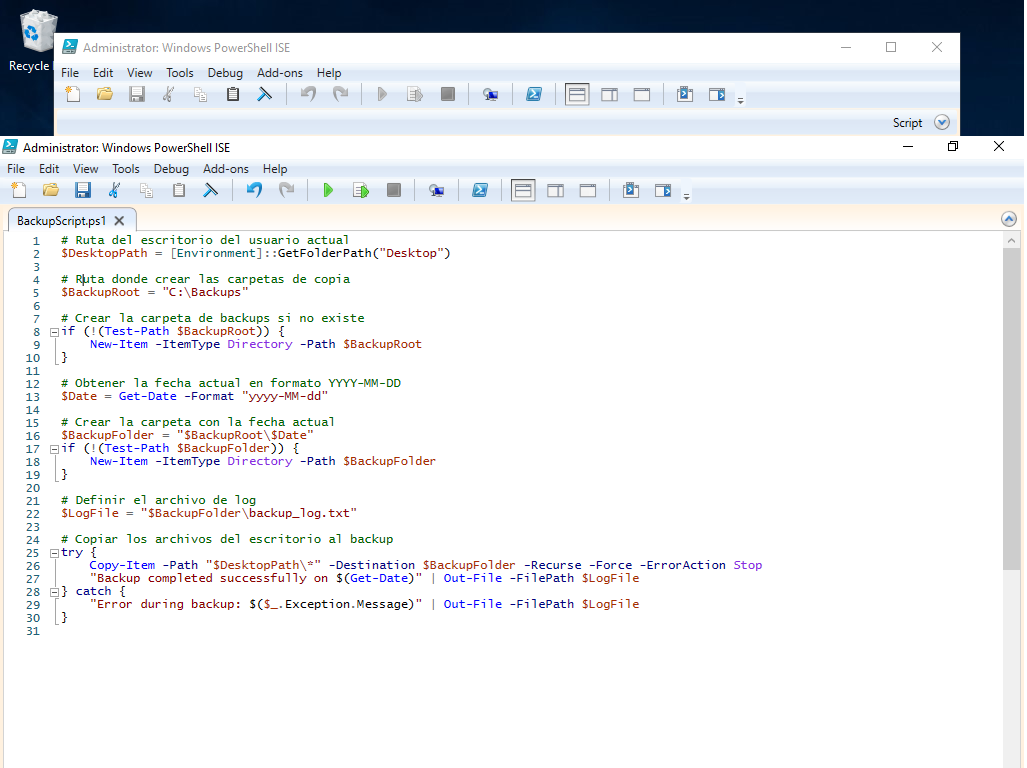
Copy-Item -Path "$DesktopPath\\*" -Destination $BackupFolder -Recurse -Force -ErrorAction Stop

"Backup completed successfully on $(Get-Date)" | Out-File -FilePath $LogFile

} catch {

"Error during backup: $($\_.Exception.Message)" | Out-File -FilePath $LogFile

}



Vamos a guardar definiendo la ruta c:\Scripts y le daremos el nombre de BackupScript.ps1

Ejecutamos el script y nos vamos a la carpeta Backups para ver que todo ha funcionado correctamente.

