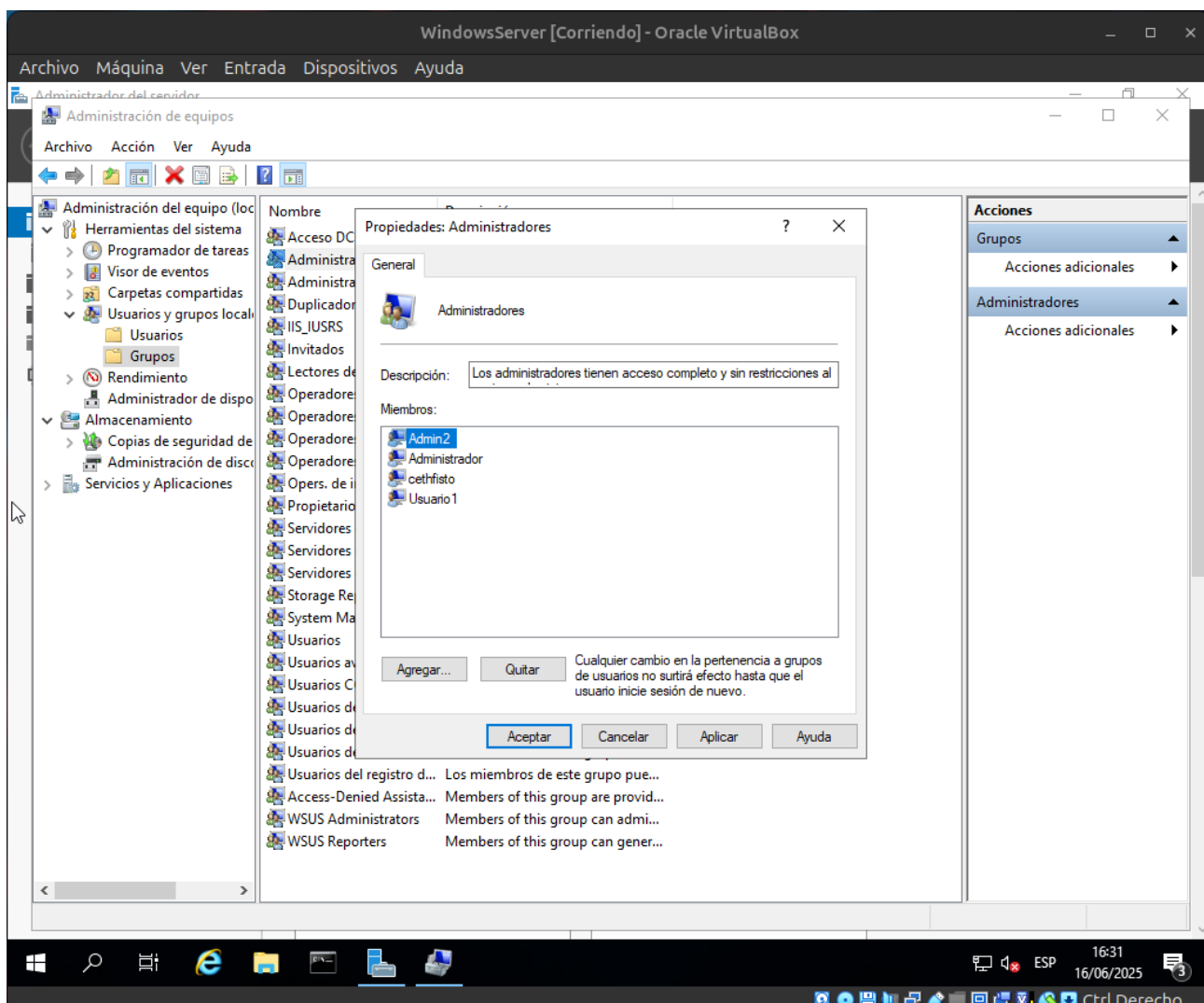


# Reto: Bloque 2 día 6

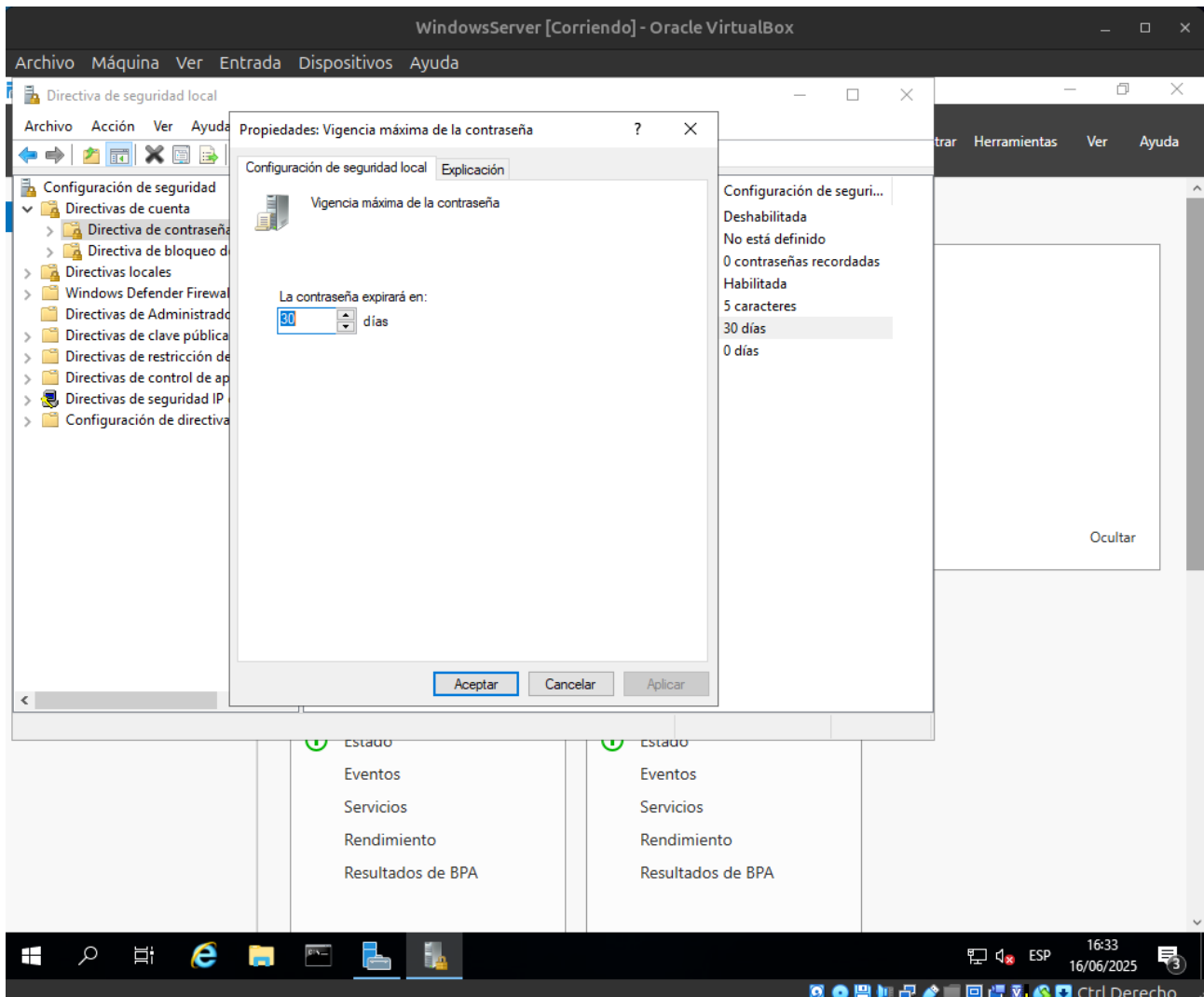
## Fase: 1

En esta primera fase del reto crearemos un administrador secundario, cambiaremos las políticas de las contraseñas para que caduquen en 30 días y el Control de Cuentas de Usuario (UAC).

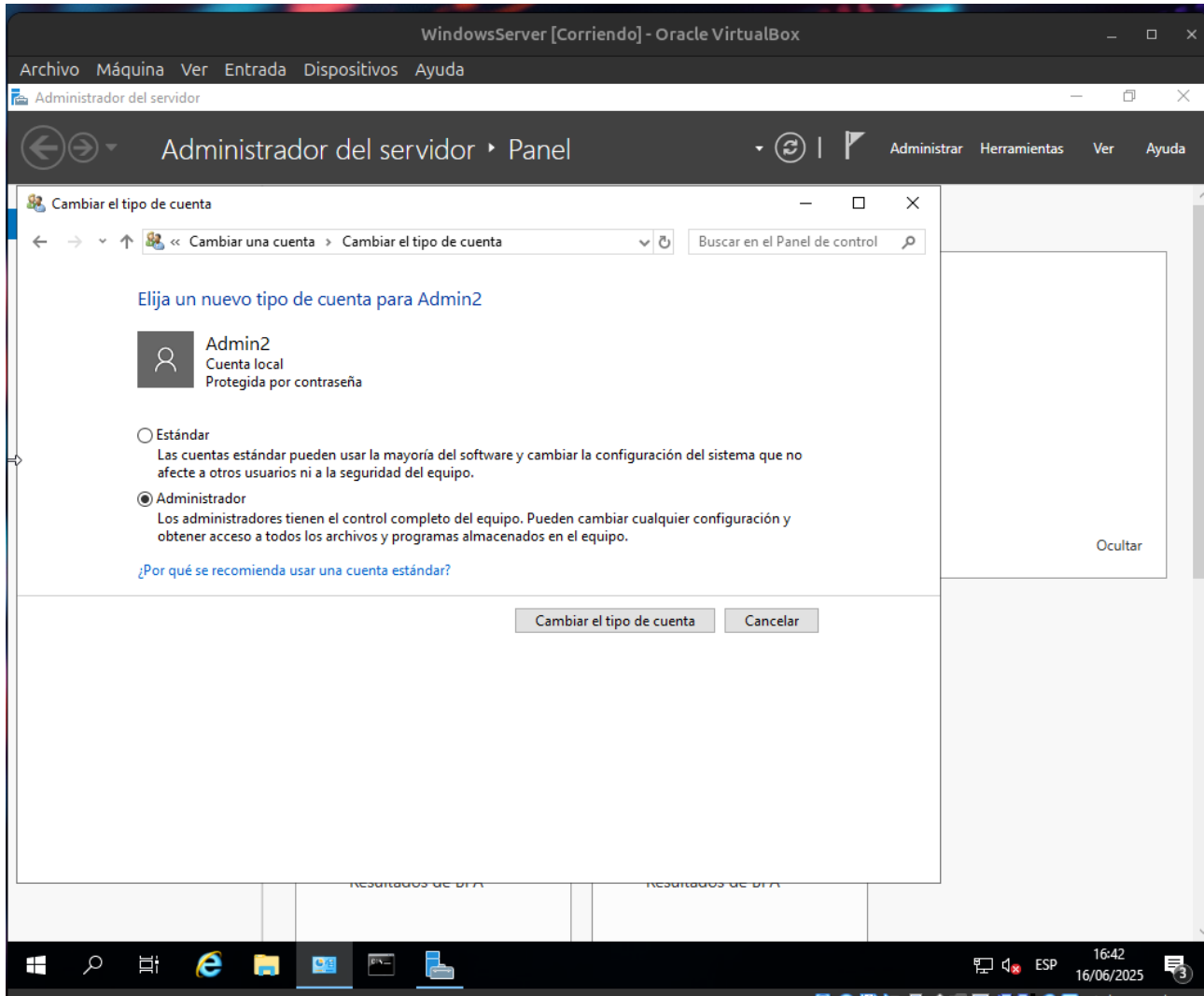
Para crear un Admin secundario, haremos los de siempre. Iremos a Herramienta y a Administración de Equipos. En Usuarios y grupos locales, crearemos el usuario y lo añadimos al grupo de Administradores. Llamaremos al usuario Admin2.



Para cambiar las políticas de contraseñas a la hora crear la contraseña, iremos a Herramientas, Directiva de seguridad local, Directiva de contraseñas. Ahí configuramos la política de contraseñas para que caduquen a los 30 días.



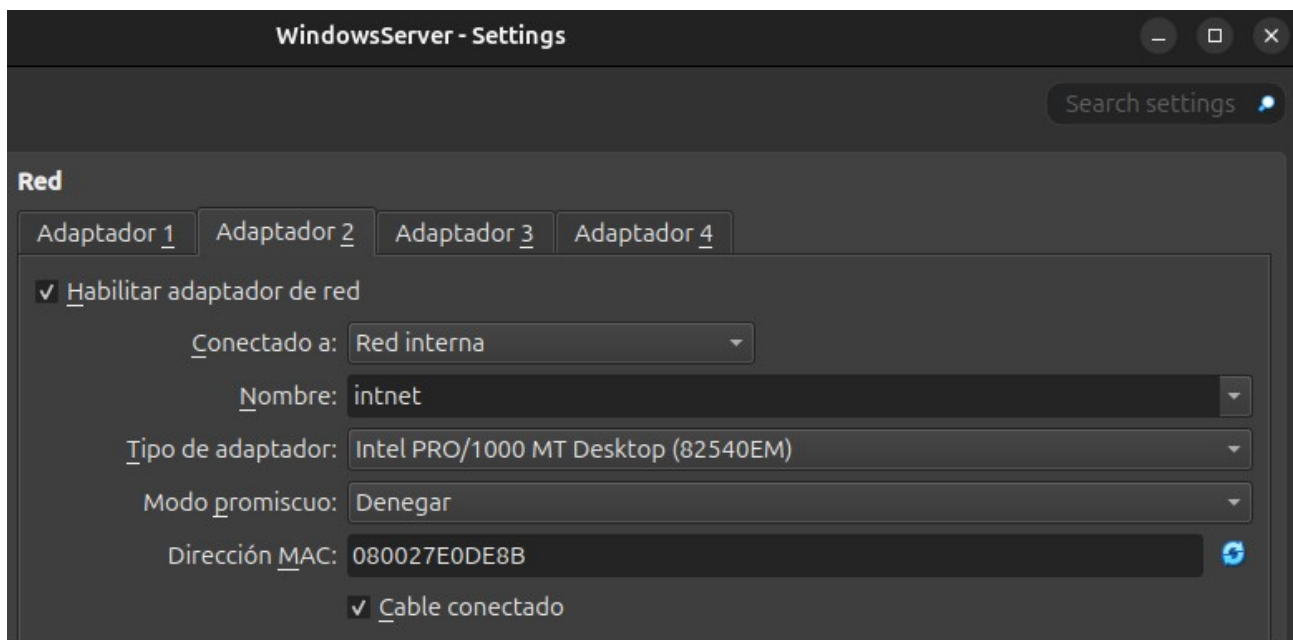
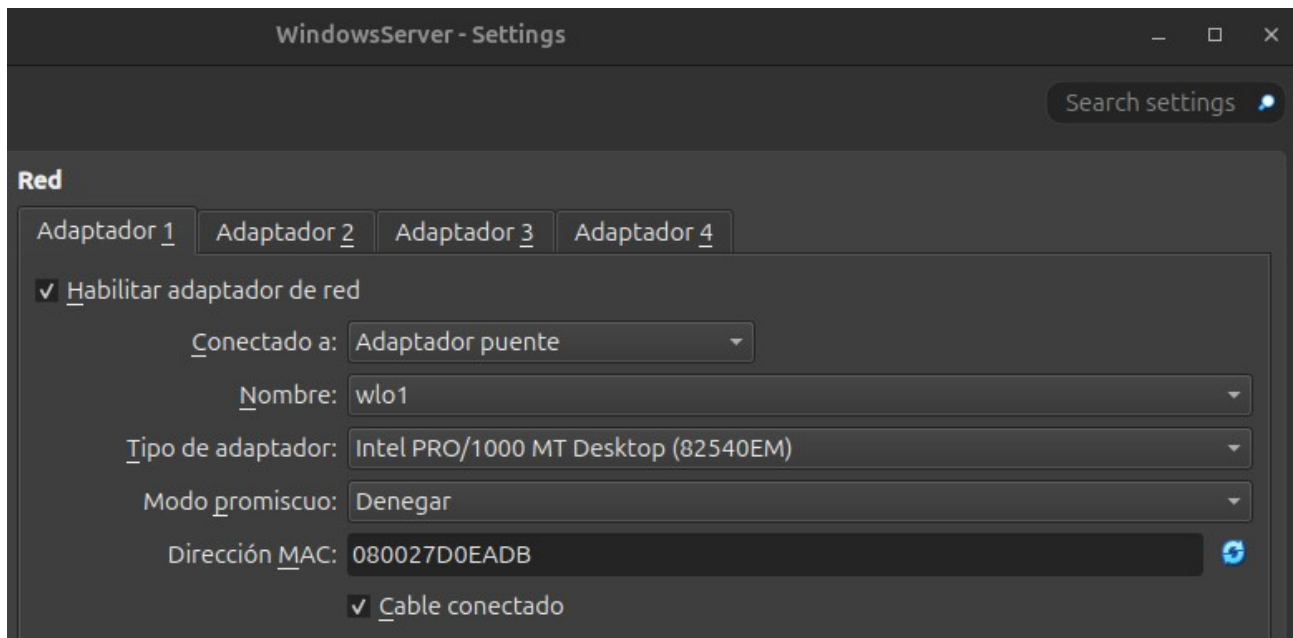
Para cambiar el UAC podemos hacerlo desde la Directiva de seguridad local o por el Panel de Control. Vamos a configurarlo usando el Panel de Control. Iremos a Panel de Control, Cuentas de usuario y Cambiar configuración de cuentas de usuario. Aquí podremos elegir que tipo de cuenta serán los usuarios, pueden ser Administradores o Estándar. Como queremos que Admin2 sea administrador, cambiaremos la opción.



## Fase: 2

En la segunda parte simularemos dos tarjetas de red interna y otra externa, configuraremos rutas estáticas en la red interna y crearemos y activaremos un DNS local.

Para configurar las tarjetas de red de la VM iremos a la configuración de la misma en Virtualbox. Ahí pondremos las dos tarjetas de red.



Para configurar las rutas estáticas de la red interna haremos varias cosas. Primero conocer cual es nuestra tarjeta de red, IP y la puerta de enlace. Recomendando tener una IP estática en la red interna también. Pondremos la IP 10.0.0.50.

Para empezar usaremos los comando ipconfig y route print para verificar que tenemos las IP estáticas y conocer la lista de interfaces. Una vez que conozcamos estos datos deberemos crear las rutas estáticas y permanentes con el comando route -p add, ya que las rutas se eliminan con cada reinicio. Por ejemplo si queremos que todo el tráfico de 10.0.0.0 pase por la red interna y el siguiente salto sea en 10.0.0.49 haremos: route -p add 10.0.0.0 mask 255.255.0.0 10.0.0.49 if 12. Y así sucesivamente hasta configurar las rutas estáticas en su totalidad.

```
Adaptador de Ethernet Red puente:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::72f7:ab79:387d:3904%11
Dirección IPv4. . . . . : 192.168.1.50
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . . : 192.168.1.1

Adaptador de Ethernet Intranet:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::771b:8ddf:6266:16f4%12
Dirección IPv4. . . . . : 10.0.0.50
Máscara de subred. . . . . : 255.255.0.0
Puerta de enlace predeterminada. . . . . :

C:\Users\Administrador>
```

Windows Server 2019 Standard Evaluation  
Licencia de Windows válida durante 177 días  
Build 17763.rs5\_release.180914-1434

17:11  
16/06/2025

Archivo Máquina Ver Entrada Dispositivos Ayuda

Papelera de reciclaje

Administrador: Símbolo del sistema

```
C:\Users\Administrador>route print

=====
Lista de interfaces
11...08 00 27 d0 ea db .....Intel(R) PRO/1000 MT Desktop Adapter
12...08 00 27 e0 de 8b .....Intel(R) PRO/1000 MT Desktop Adapter #2
1.....Software Loopback Interface 1
=====

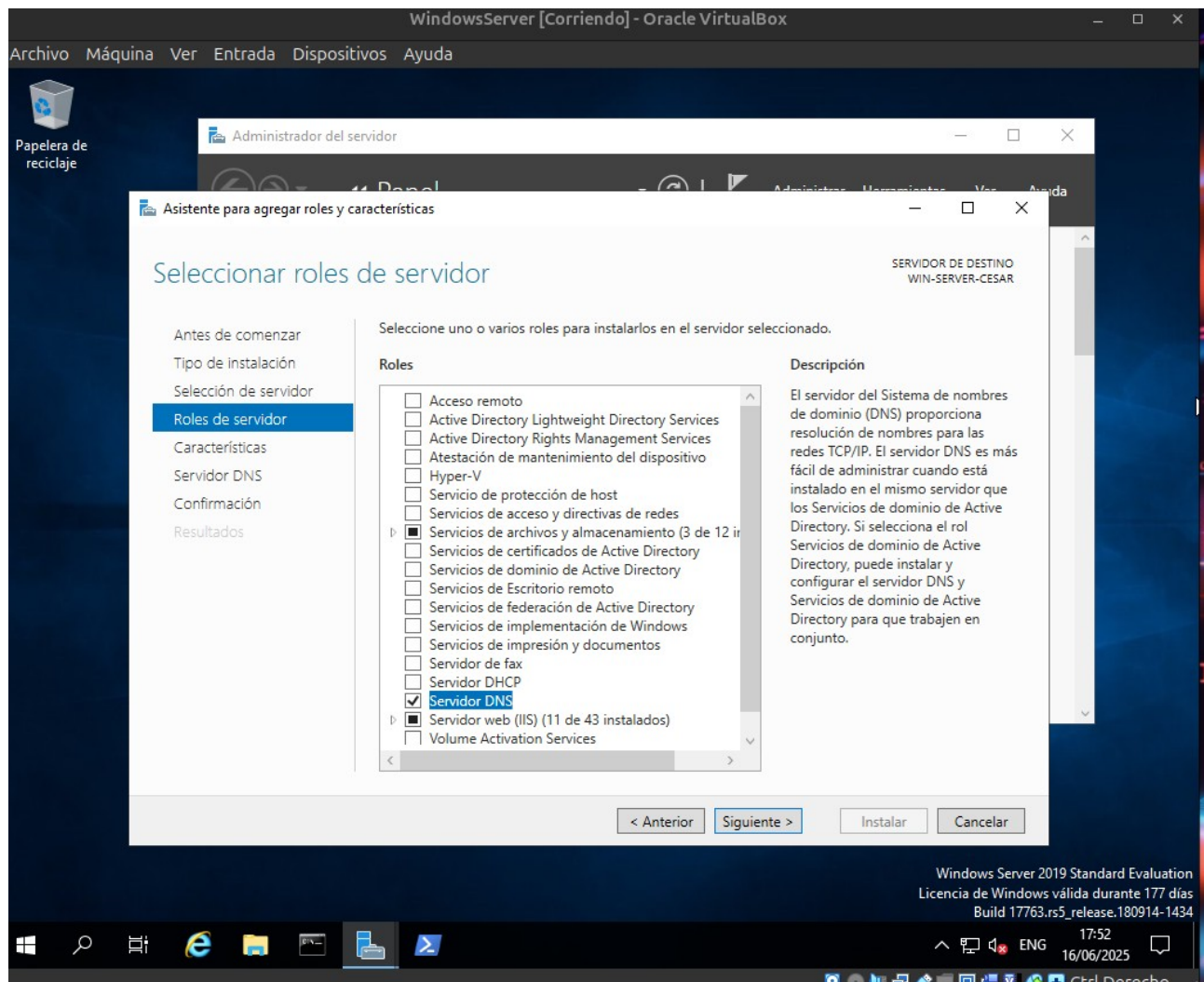
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
-----
0.0.0.0             0.0.0.0             192.168.1.1           192.168.1.50  281
10.0.0.0            255.255.0.0         En vínculo            10.0.0.50     281
10.0.0.50           255.255.255.255     En vínculo            10.0.0.50     281
10.0.255.255        255.255.255.255     En vínculo            10.0.0.50     281
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
192.168.1.0         255.255.255.0       En vínculo            192.168.1.50  281
192.168.1.50        255.255.255.255     En vínculo            192.168.1.50  281
192.168.1.255       255.255.255.255     En vínculo            192.168.1.50  281
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo            192.168.1.50  281
224.0.0.0           240.0.0.0           En vínculo            10.0.0.50     281
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
255.255.255.255     255.255.255.255     En vínculo            192.168.1.50  281
255.255.255.255     255.255.255.255     En vínculo            10.0.0.50     281
=====
```

Windows Server 2019 Standard Evaluation  
Licencia de Windows válida durante 177 días  
Build 17763.rs5\_release.180914-1434

17:46  
16/06/2025

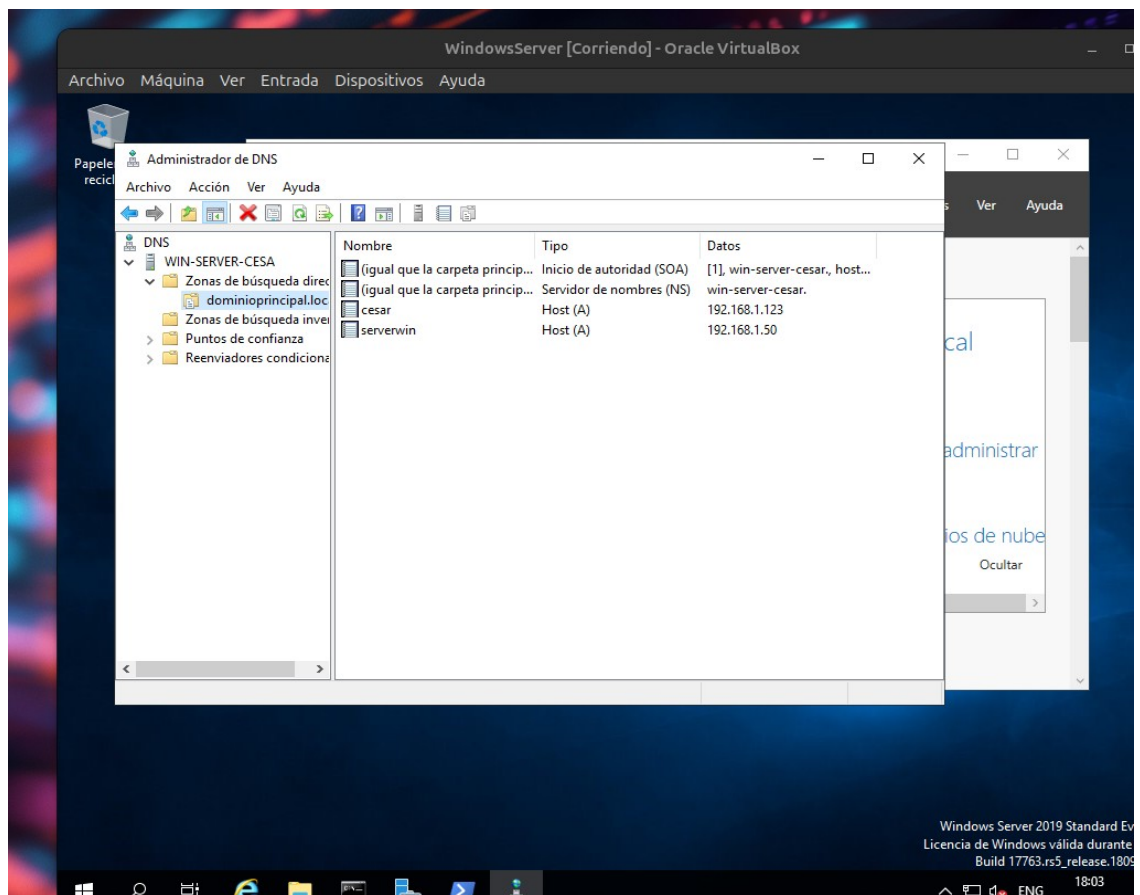
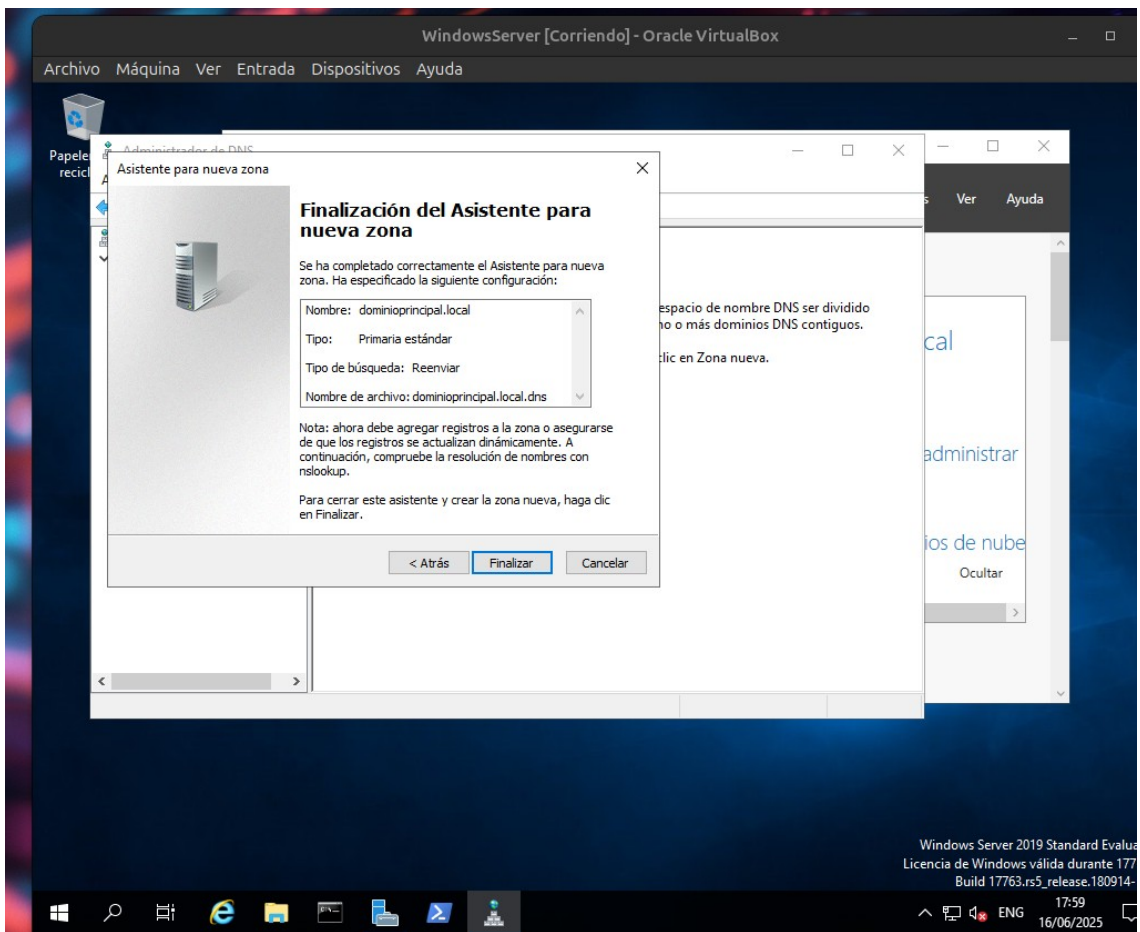
Ctrl Derecho

Para crear y activar un DNS local deberemos instalar el rol, para ello iremos a Agregar roles y características y hacemos el proceso de instalación.



Para hacer la configuración de la zona directa iremos a Herramientas y seleccionamos DNS. Una vez dentro vamos a Zonas de búsqueda directa y seleccionamos Nueva zona en el menú superior para iniciar el asistente al que llamaremos dominioprincipal.local. Y para añadir los registros, seleccionamos la zona creada y con clic derecho seleccionamos Nuevo host (A o AAAA) para añadir los equipos y su IP.

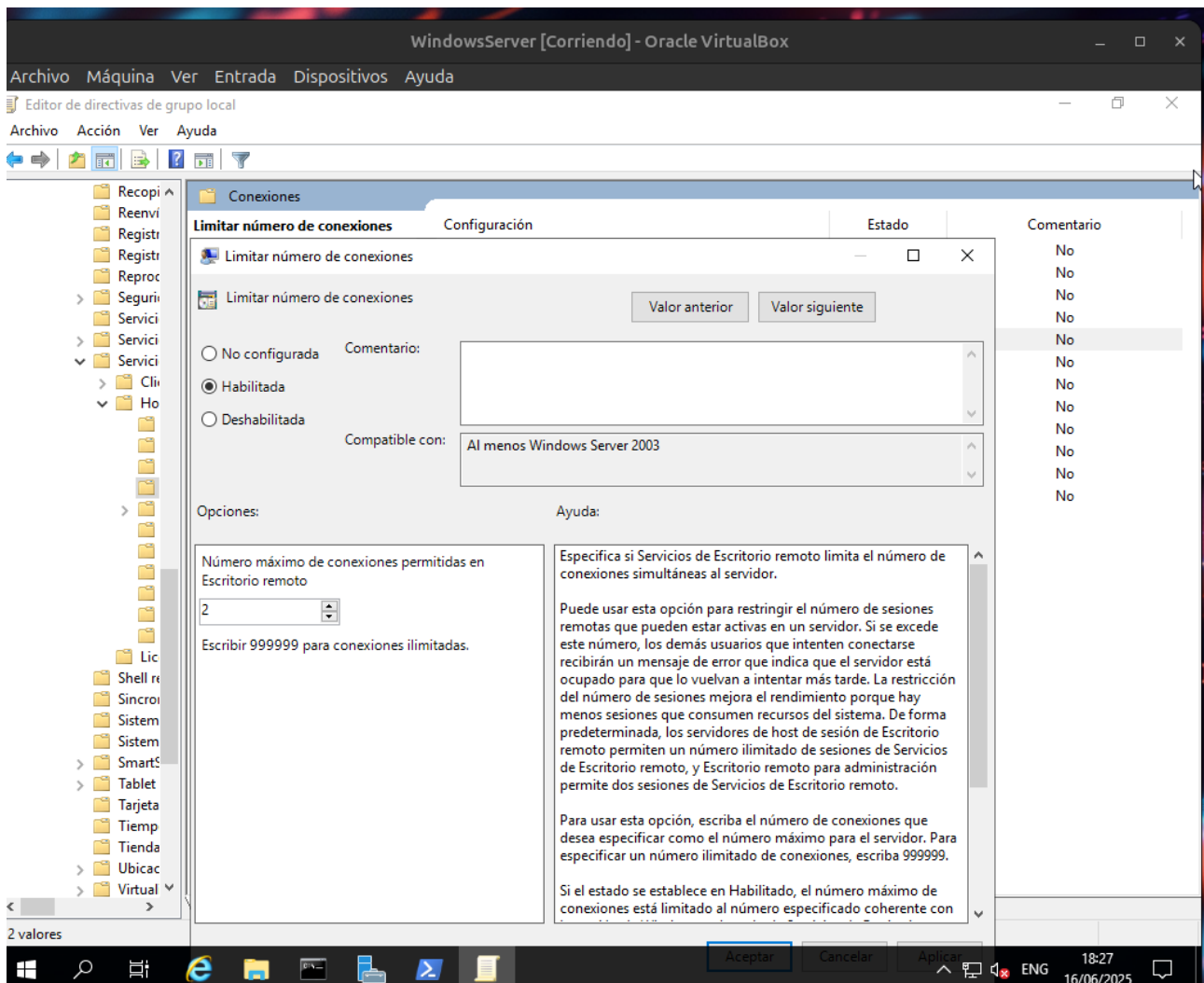




## Fase: 3

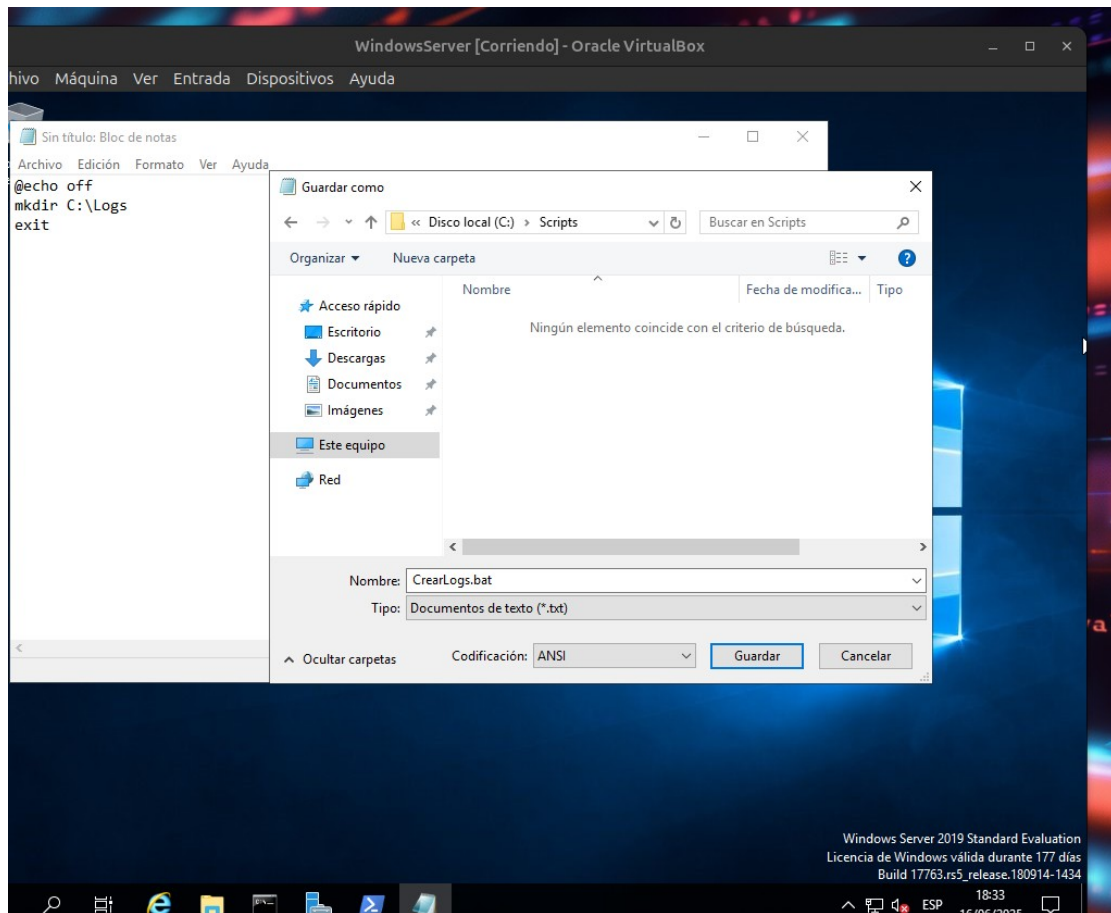
En esta fase habilitaremos en Escritorio Remoto a 2 sesiones, personalizaremos el inicio del sistema con un script en la carpeta Logs y configuraremos el Firewall para que solo permita el RDP y DNS.

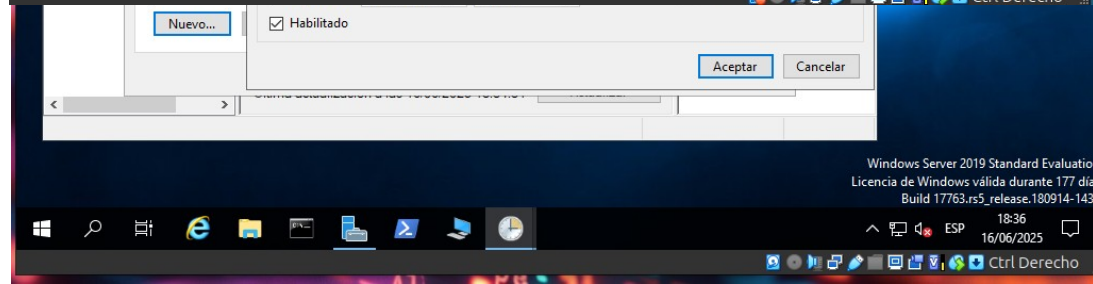
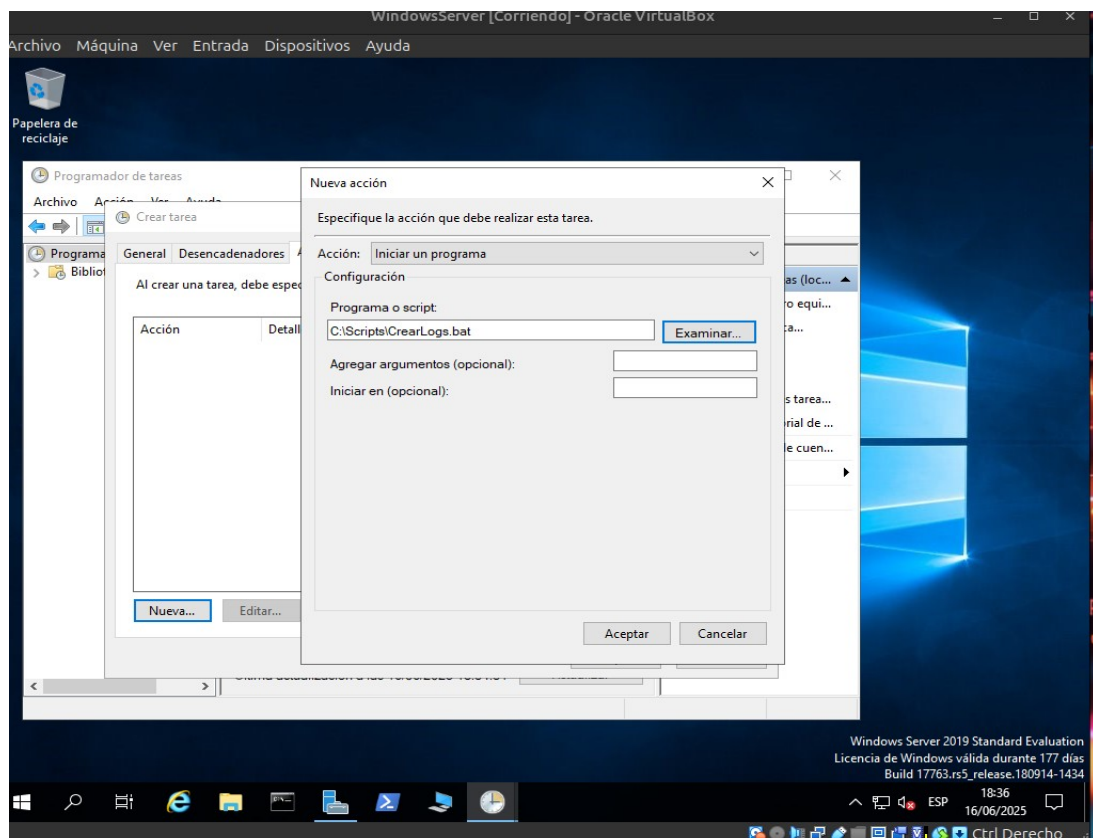
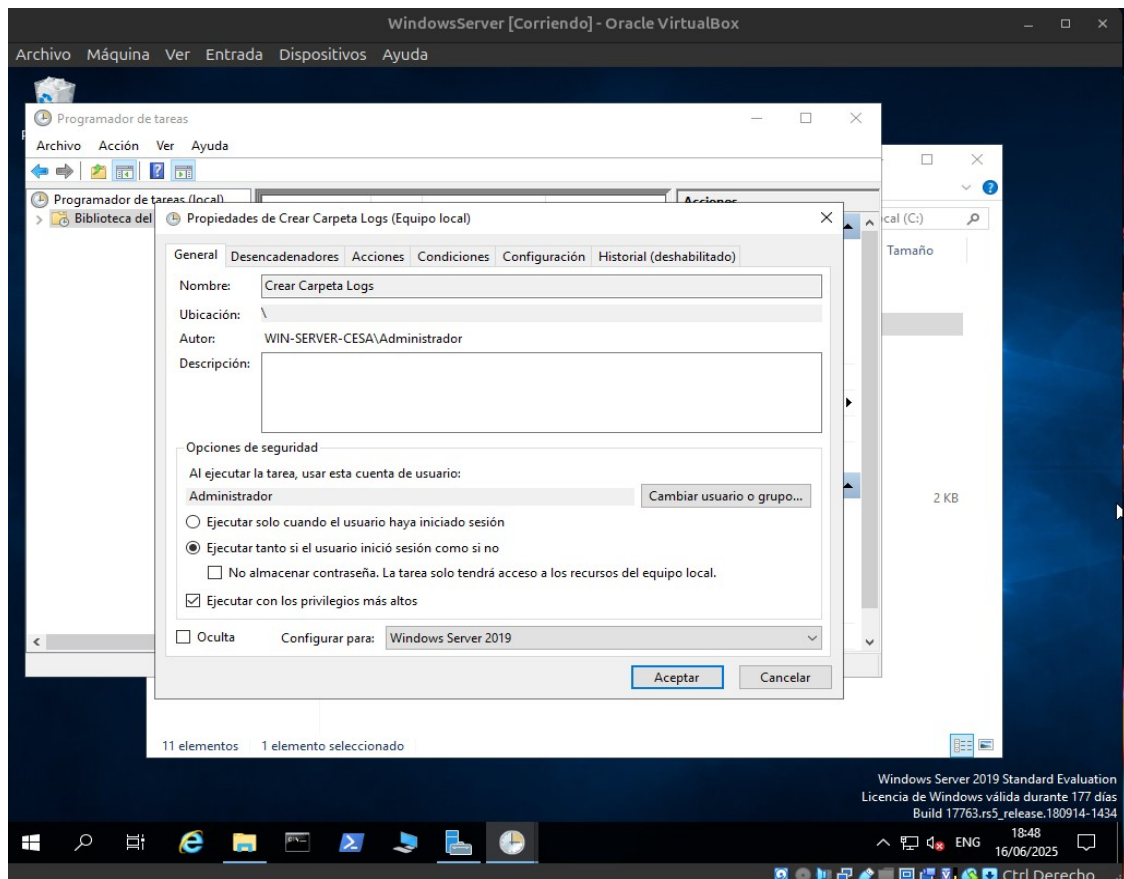
Para limitar el acceso remoto a dos sesiones, primero, deberemos activar el servicio. Ahora para limitar las sesiones, deberemos ir al Editor de directivas de grupo local, podemos acceder con la consola con el comando gpedit.msc. Una vez dentro iremos pasando por Configuración de equipo, Plantillas administrativas, Componentes de Windows, Servicios de Escritorio remoto hasta Conexiones. Dentro de conexiones seleccionamos Limitar número de conexiones y realizamos la configuración pertinente.

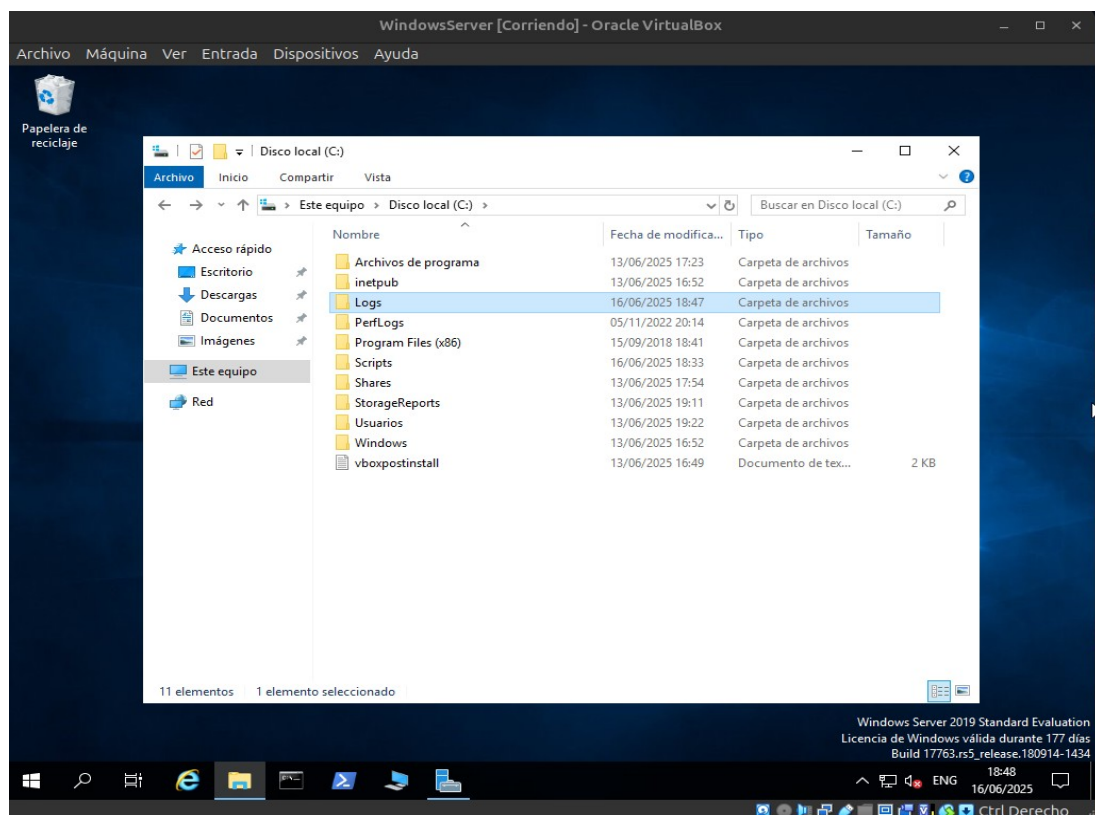




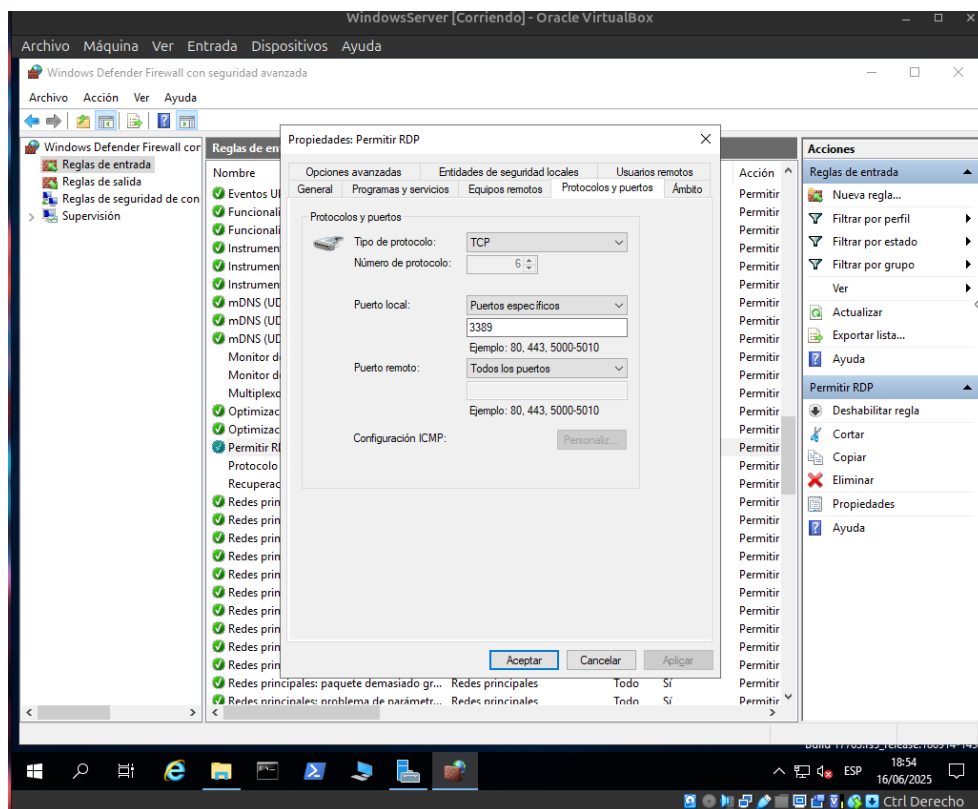
Ahora vamos a crear un script para crear una carpeta en el directorio [C:\Logs](#). Para poder usar el bloc de notas. Luego para automatizar el script iremos al Programador de tareas en el menú de Inicio, creamos, configuramos y activamos la tarea.

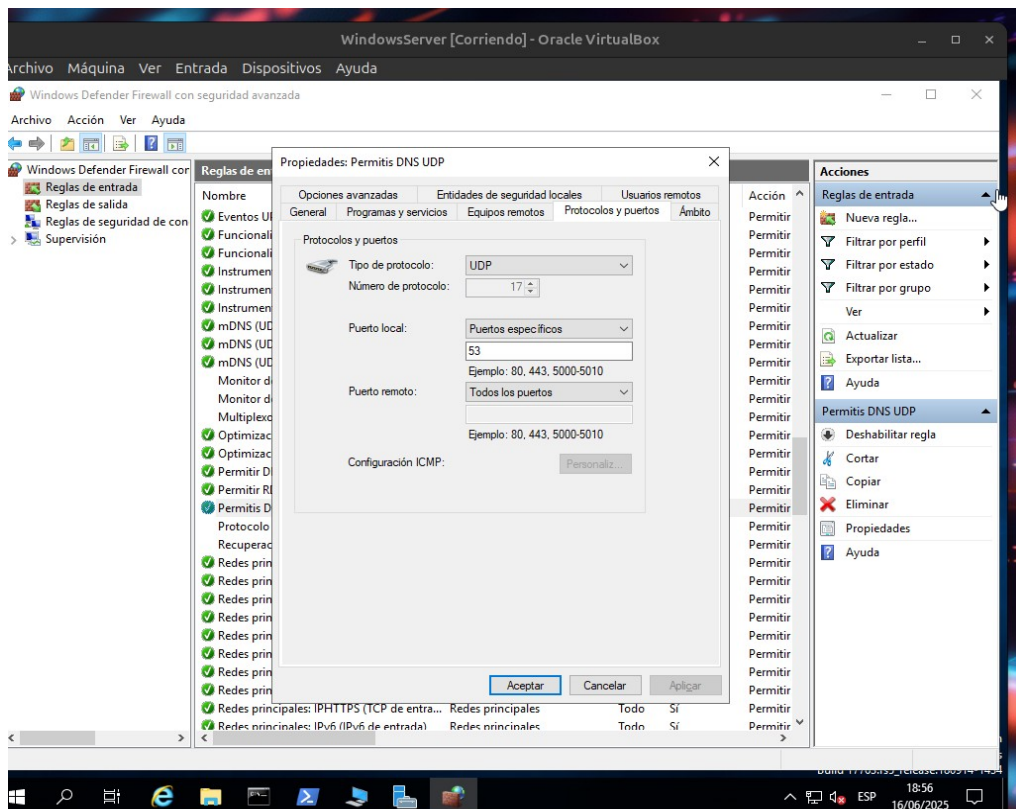
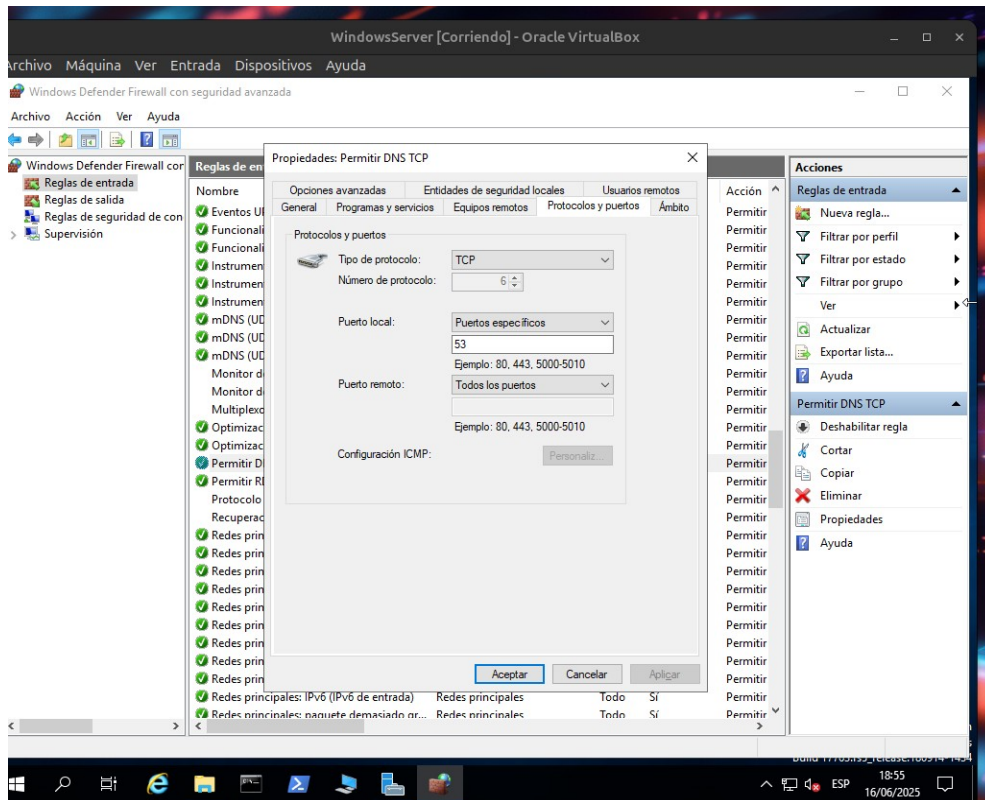






Por último configuramos el Firewall para que solo permita el RDP y DNS, para ello iremos al Windows Defender Firewall con seguridad avanzada. Iremos a reglas de entrada y creamos las reglas para el RDP y DNS. En el caso del DNS crearemos dos reglas una para el puerto TCP y otra para el puerto UDP.





## Fase: 4 y 5

Aquí, crearemos un script en PowerShell para crear una carpeta con la fecha actual, copie los archivos del escritorio de esa carpeta y genere un log en formato .txt con el resultado de la copia en el directorio creado previamente en [C:\Logs](#). Escribiremos las líneas de código para el script en PS y cuando lo tengamos lo guardamos y lo ejecutamos con PowerShell.

Por último dejaremos las configuraciones de red, directivas y añadiremos el código de script.

