

● Día 6: Configuración Avanzada de Windows Server



Abraham Caamaño Martínez

13-06-2025

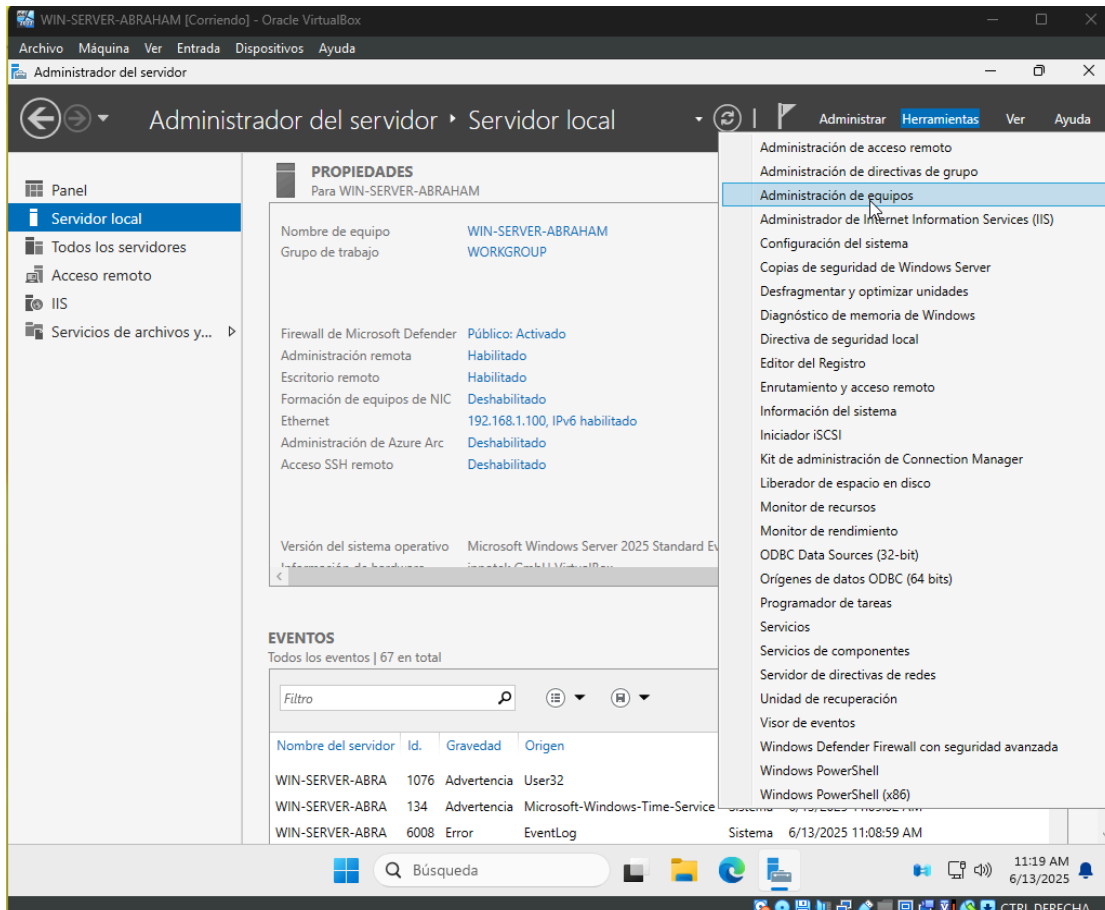
💡 Ejercicio práctico con impacto en la empresa

-Fase 2: Gestión de usuarios y permisos:

Para crear tres usuarios estándar con diferentes permisos:

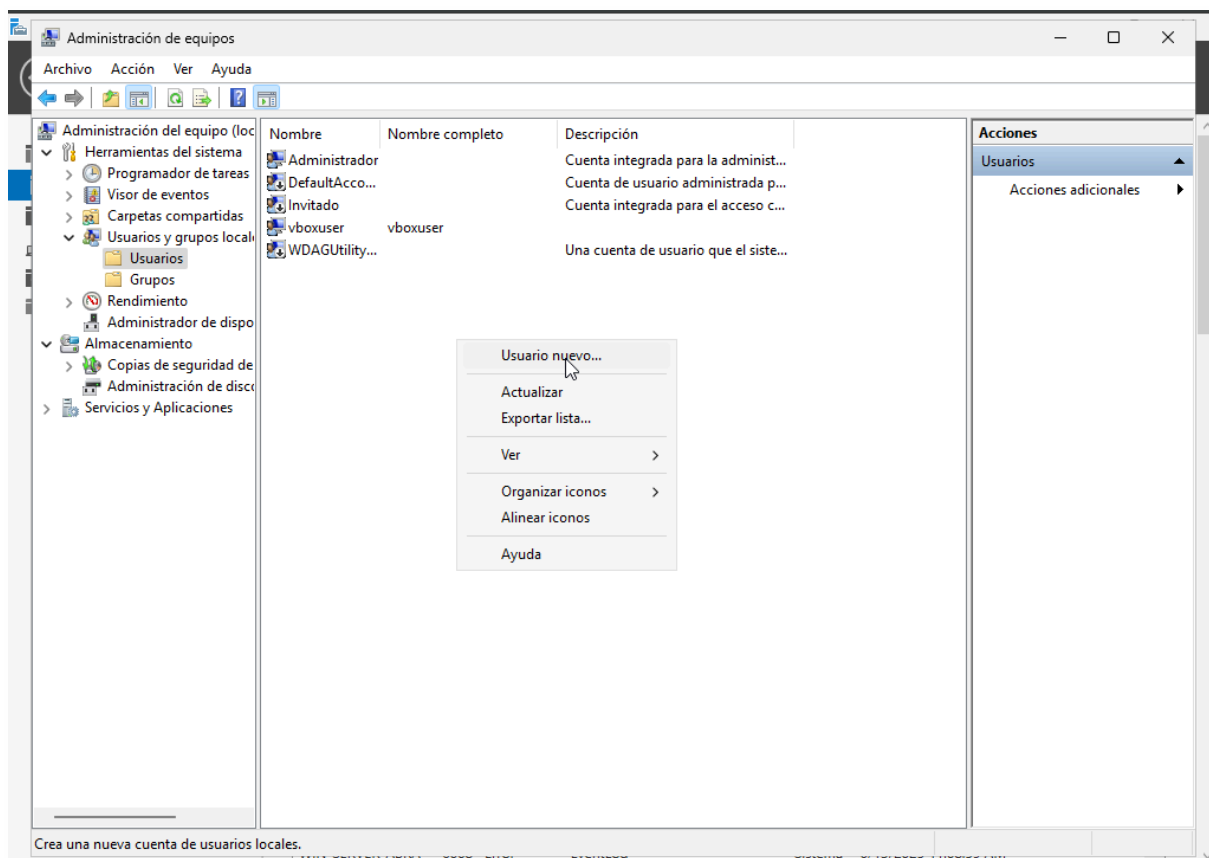
1.En el servidor, abrimos el Administrador del Servidor.

2.Vamos a Herramientas > Administración de equipos.

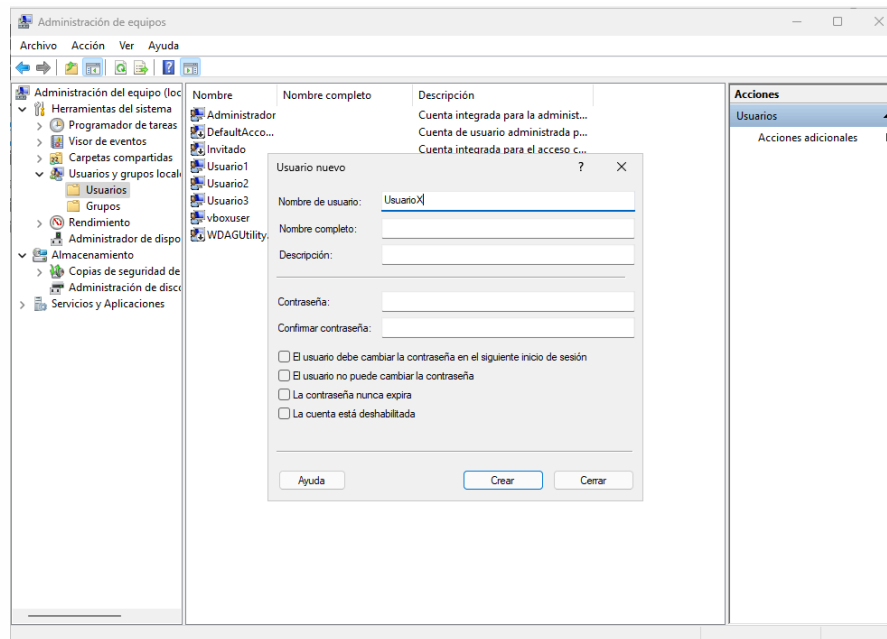


3.En el panel izquierdo, navegamos a Usuarios y grupos locales > Usuarios.

4.Hacemos clic derecho en un espacio vacío en el panel central y seleccionamos Usuario nuevo....



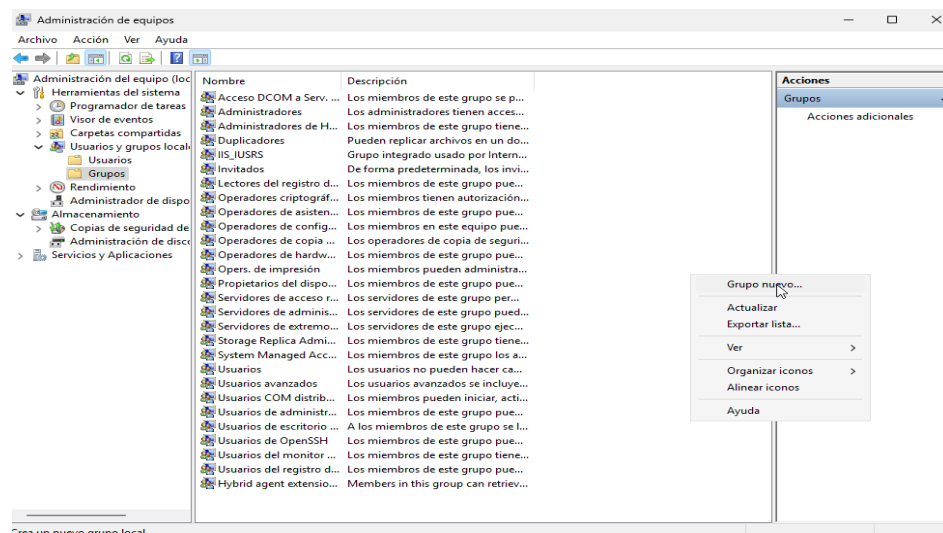
5.Creamos los usuarios (desmarcamos "El usuario debe cambiar la contraseña en el siguiente inicio de sesión" para facilitar las pruebas)



6. Hacemos clic en Crear por cada usuario y luego en Cerrar

Configurar Grupos de Seguridad para la Administración del Servidor

1. En la misma ventana de Administración de equipos, vamos a Usuarios y grupos locales > Grupos.
2. Hacemos clic derecho en un espacio vacío y seleccionamos Grupo nuevo....



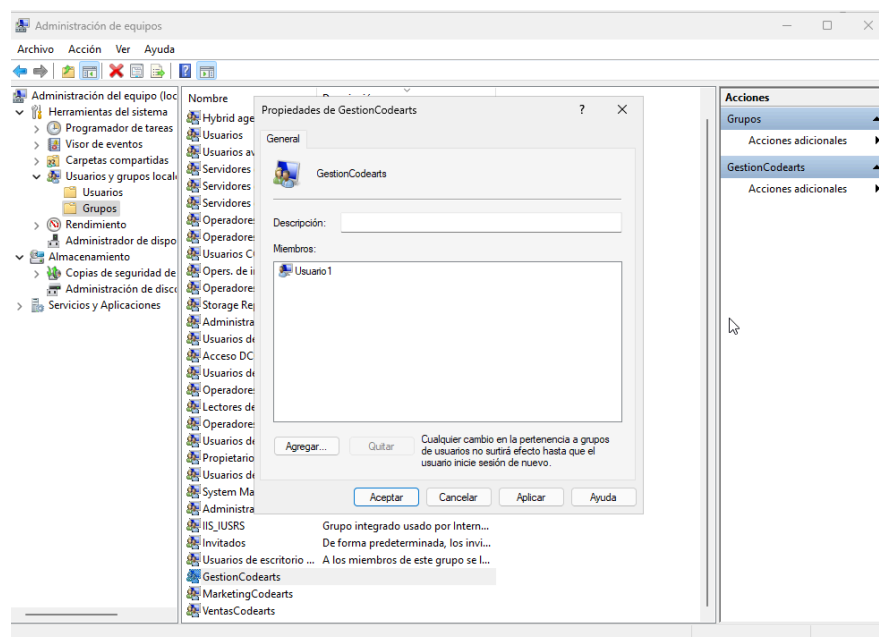
3. Creamos los siguientes grupos por ejemplo:

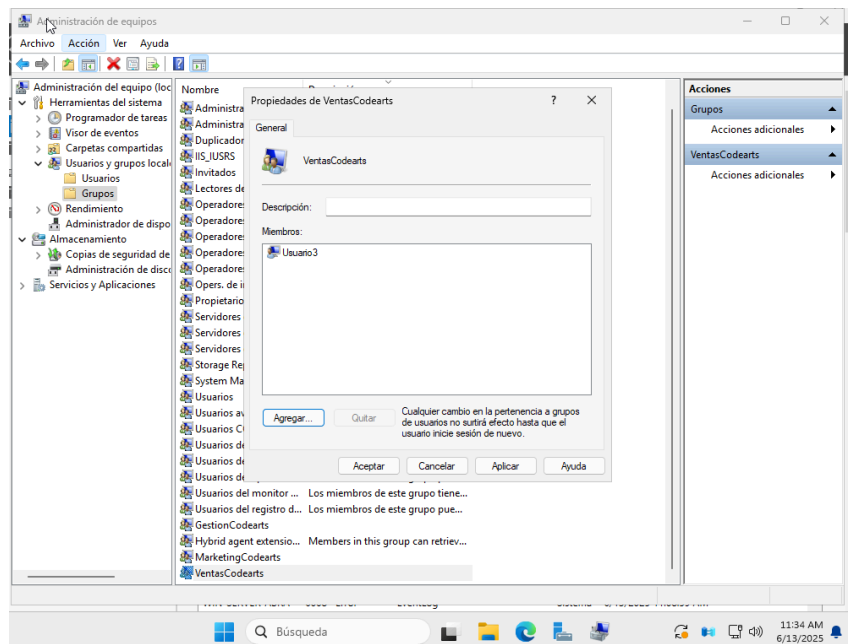
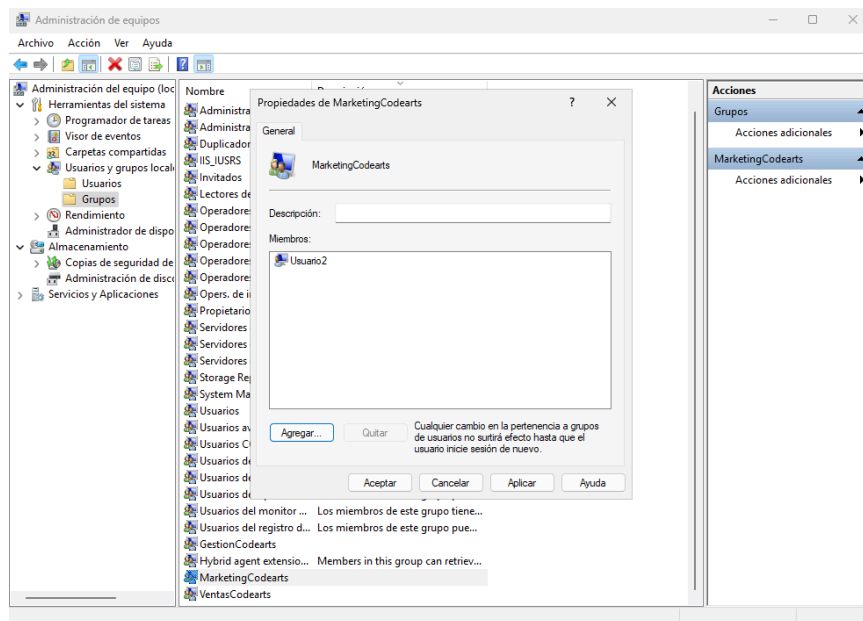
- MarketingCodearts
- GestiónCodearts
- VentasCodearts

4. Hacemos clic en Crear por cada grupo y luego en Cerrar.

5. Ahora, añadimos a los usuarios a sus respectivos grupos:

- Doble clic en el grupo GestionCodearts, clic en Agregar... y añadimos a Usuario1.
- Doble clic en el grupo MarketingCodearts, clic en Agregar... y añadimos a Usuario2.
- Doble clic en el grupo VentasCodearts, clic en Agregar... y añadimos a Usuario3.

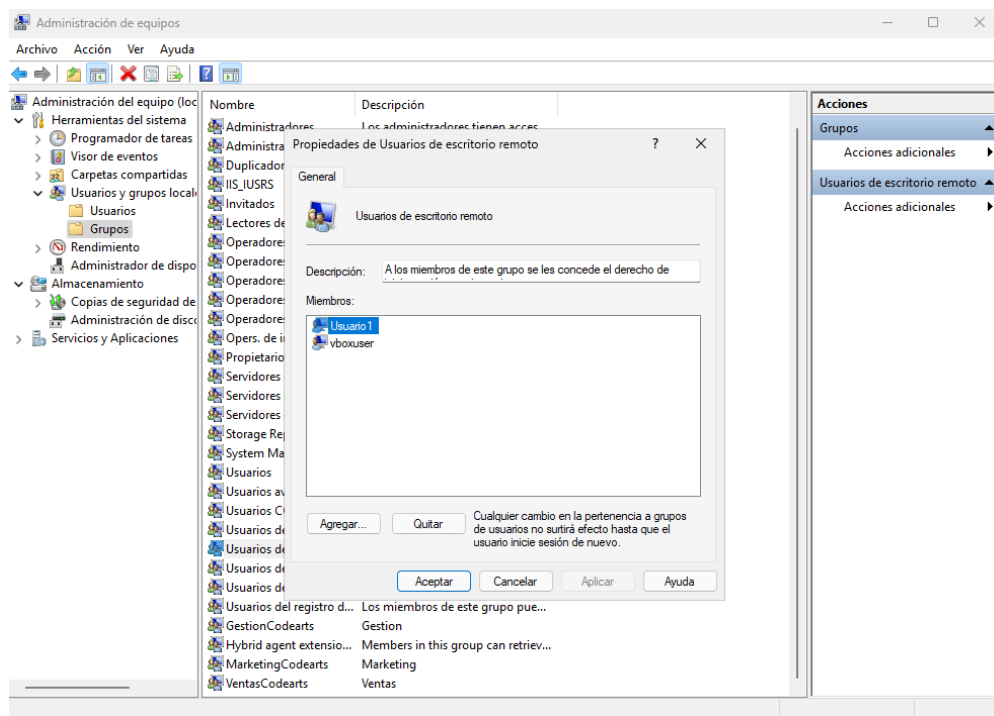




Para que los usuarios del grupo GestionCodearts puedan administrar el servidor si es necesario, vamos a darles acceso a Escritorio Remoto:

- Doble clic en el grupo "Usuarios de Escritorio remoto".
- Clic en Agregar... y añadimos el grupo GestionCodearts. Esto permitirá que Usuario1 (y futuros miembros de ese grupo) puedan conectarse por RDP.

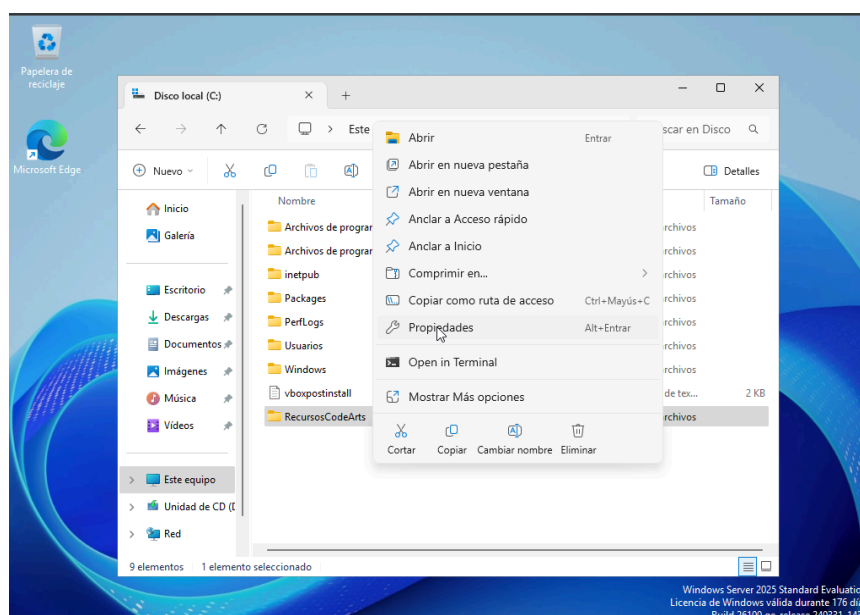
En mi caso no me aparecen los grupos que he creado a la hora de agregarlos al grupo de Usuarios de Escritorio remoto por lo que añadiré solo al usuario.



Aplicar Permisos en Carpetas Compartidas

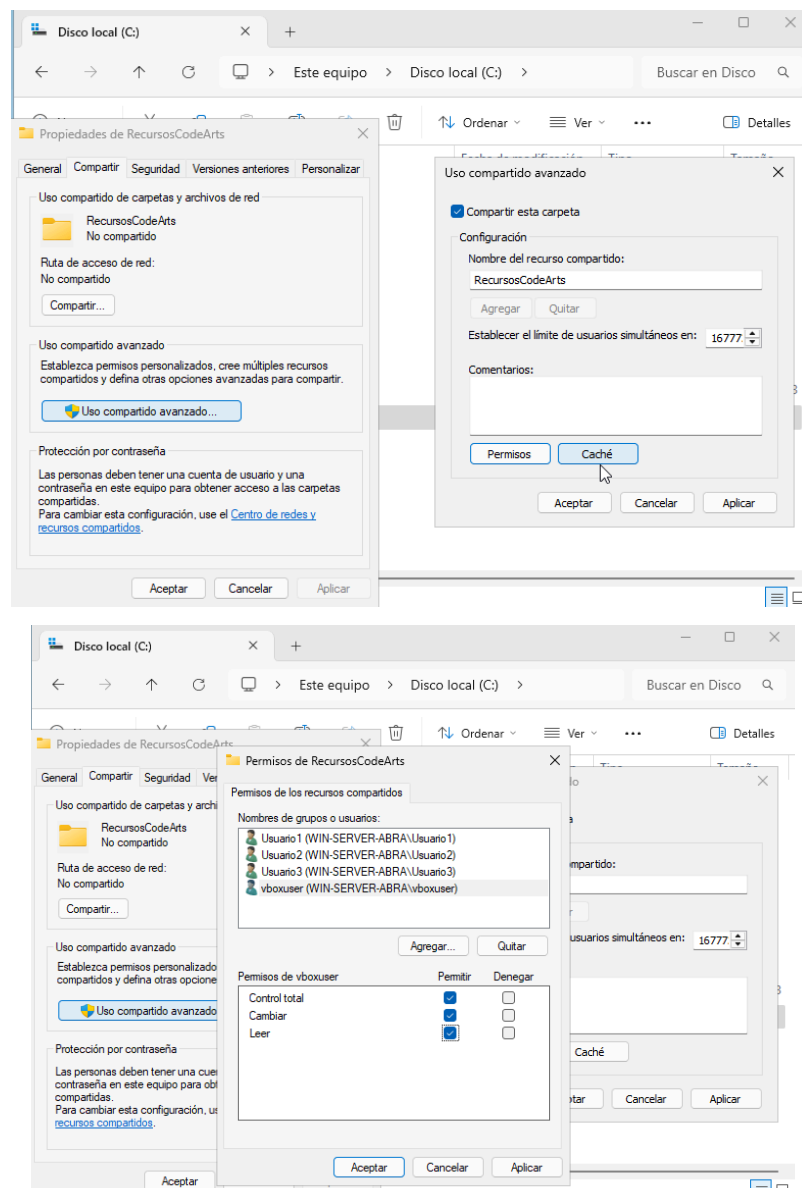
Vamos a crear una carpeta compartida y controlar quién puede acceder a ella.

Crearemos una carpeta en el disco C: llamada RecursosCodearts.



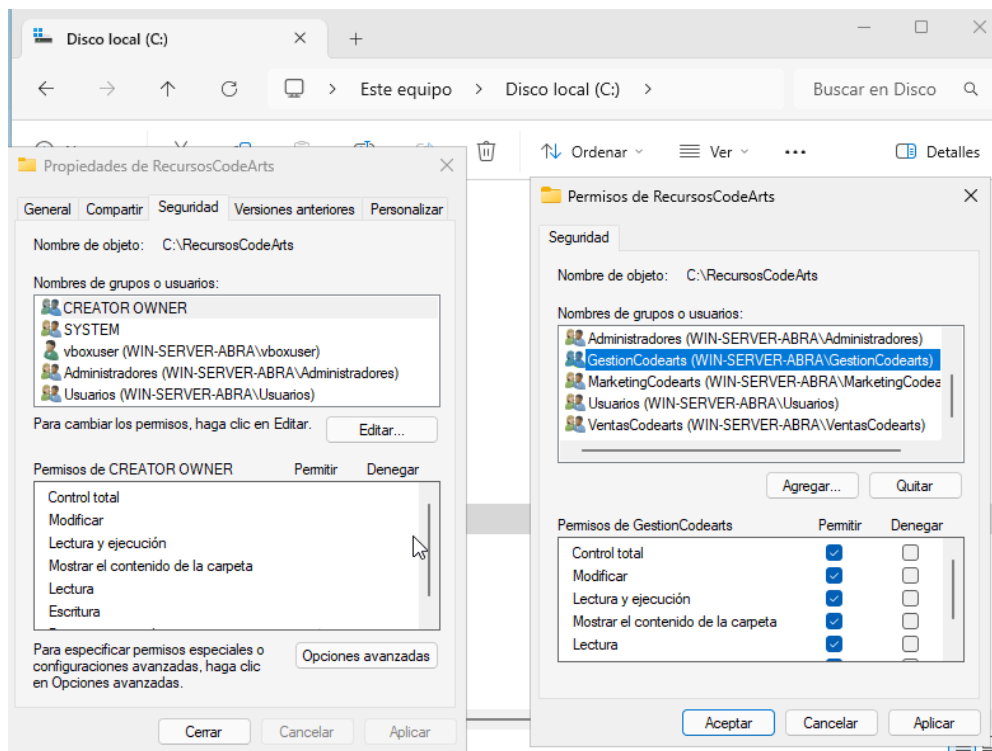
Configurar compartición:

- Hacemos clic derecho en la carpeta RecursosCodearts y selecciona Propiedades.
- Vamos a la pestaña Compartir y hacemos clic en "Uso compartido avanzado...".
- Marcamos "Compartir esta carpeta".
- Hacemos clic en Permisos. Quitamos "Todos" y agregamos los grupos que creamos anteriormente.
- Para cada grupo, definimos los permisos de compartición que queramos
- Haz clic en Aceptar en todas las ventanas hasta cerrar las propiedades de compartición.



Configurar permisos NTFS

1. En la misma ventana de Propiedades de la carpeta RecursosCodearts, vamos a la pestaña Seguridad.
2. Clic en Editar
3. Clic en Agregar y añadimos los grupos GestionCodearts, MarketingCodearts y VentasCodearts.
4. Para cada grupo, le ponemos los permisos que deseemos.
5. Haz clic en Aceptar.



Revisar el Estado del Servidor y Monitorear Eventos del Sistema

Para monitorear nuestro servidor, debemos seleccionar nuestro servidor en el Administrador, podremos ver los siguientes elementos:

ROLES Y CARACTERÍSTICAS

Todos los roles y características | 43 en total

TAREAS

Filtro			
Nombre del servidor	Nombre	Tipo	Ruta de acceso
WIN-SERVER-ABRA	Servidor web (IIS)	Rol	Servidor web (IIS)
WIN-SERVER-ABRA	Kit de administración de Connection Manager RAS (CMAK)	Característica	Kit de administración de Conne
WIN-SERVER-ABRA	Herramientas de administración remota del servidor	Característica	Herramientas de administración
WIN-SERVER-ABRA	Herramientas de administración de roles	Característica	Herramientas de administración
WIN-SERVER-ABRA	Herramientas de administración de acceso remoto	Característica	Herramientas de administración
WIN-SERVER-ABRA	Módulo de acceso remoto para Windows PowerShell	Característica	Herramientas de administración

EVENTOS

Todos los eventos | 2 en total

TAREAS

Filtro					
Nombre del servidor	Id.	Gravedad	Origen	Registro	Fecha y hora
WIN-SERVER-ABRA	6008	Error	EventLog	Sistema	6/16/2025 11:05:53 AM
WIN-SERVER-ABRA	41	Critico	Microsoft-Windows-Kernel-Power	Sistema	6/16/2025 11:05:49 AM
El cierre anterior del sistema a las 12:28:54 PM del 6/13/2025 resultó inesperado.					

SERVICIOS

Todos los servicios | 246 en total

TAREAS

Filtro			
Nombre del servidor	Nombre para mostrar	Nombre de servicio	Esta
WIN-SERVER-ABRA	LxpSvc	LxpSvc	Dete
WIN-SERVER-ABRA	Cliente DHCP	Dhcp	En ej
WIN-SERVER-ABRA	Servicio orquestador de actualizaciones	UsoSvc	En ej
WIN-SERVER-ABRA	Host del servicio de diagnóstico	WdiServiceHost	Dete
WIN-SERVER-ABRA	Administrador de pagos y NFC/SE	SEMgrSvc	Dete
WIN-SERVER-ABRA	Agente de conexión de red	NcbService	En ej

RENDIMIENTO

Todos los resultados | 1 en total | Últimas 24 horas

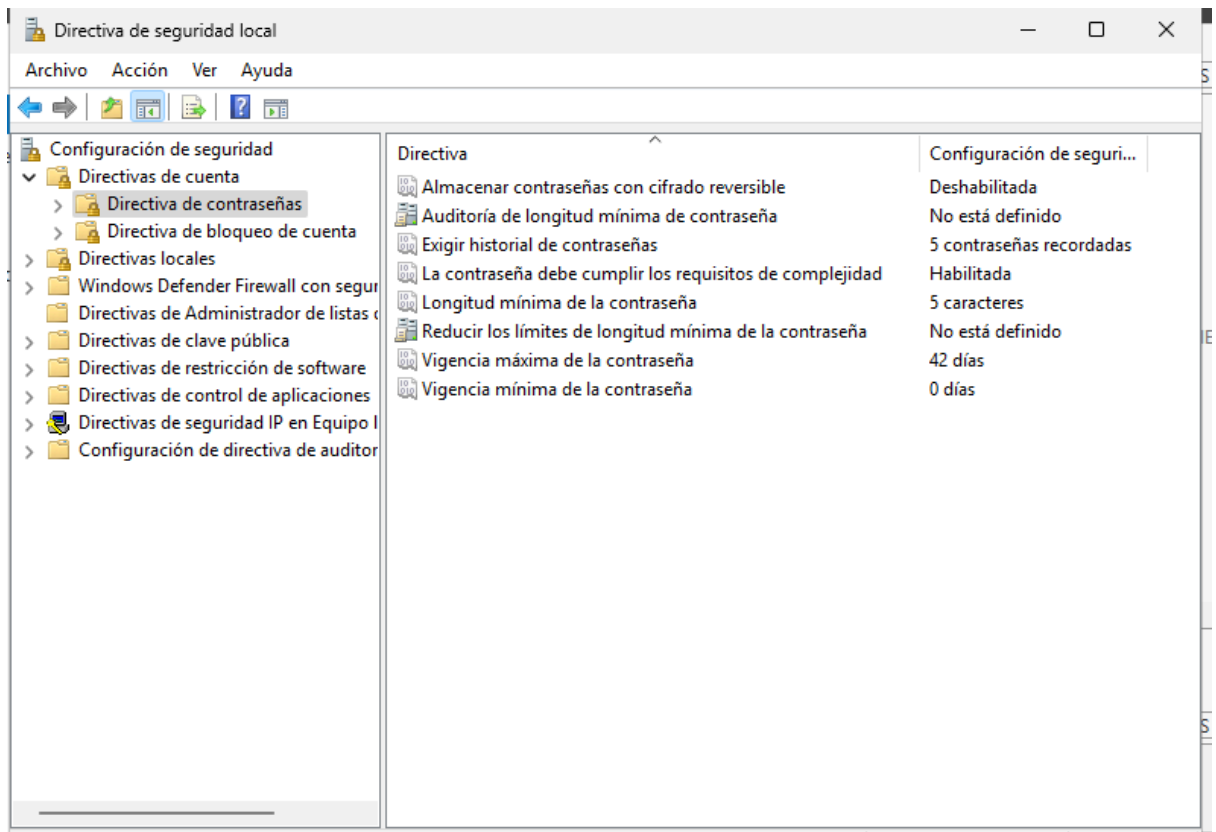
TAREAS

Uso de CPU					
12 pm 2 pm 4 pm 6 pm 8 pm 10 pm 12 am 2 am 4 am 6 am 8 am 10 am					
Memoria disponible					
Filtro					
Nombre del servidor	Estado del contador	Número de alertas de CPU	Número de alertas de memoria	Primera repetición	Última rep
WIN-SERVER-ABRA	Desactivado	-	-	-	-

Implementar Políticas de Seguridad para Accesos Remotos

Desde Herramientas-Directiva de seguridad local.
Navegamos a Directivas de cuenta-Directiva de contraseñas:

1. Marcamos "Exigir el historial de contraseñas" poniendo 5 por ejemplo.
2. "La contraseña debe cumplir los requisitos de complejidad" lo habilitamos.
3. "Longitud mínima de la contraseña": lo ponemos en 5 por ejemplo.



Navega a Directivas de cuenta > Directiva de bloqueo de cuenta:

"Umbral de bloqueo de cuenta": Lo ponemos en 3 intentos fallidos.

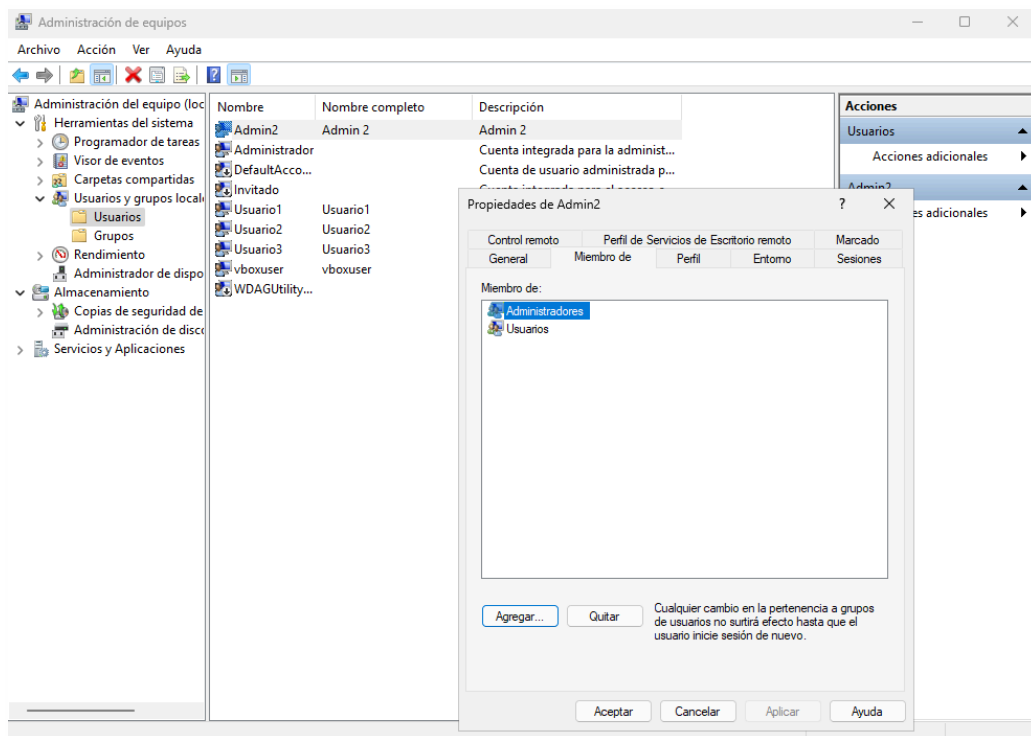


Fases del reto

Fase 1: Preparación del entorno y consola administrativa

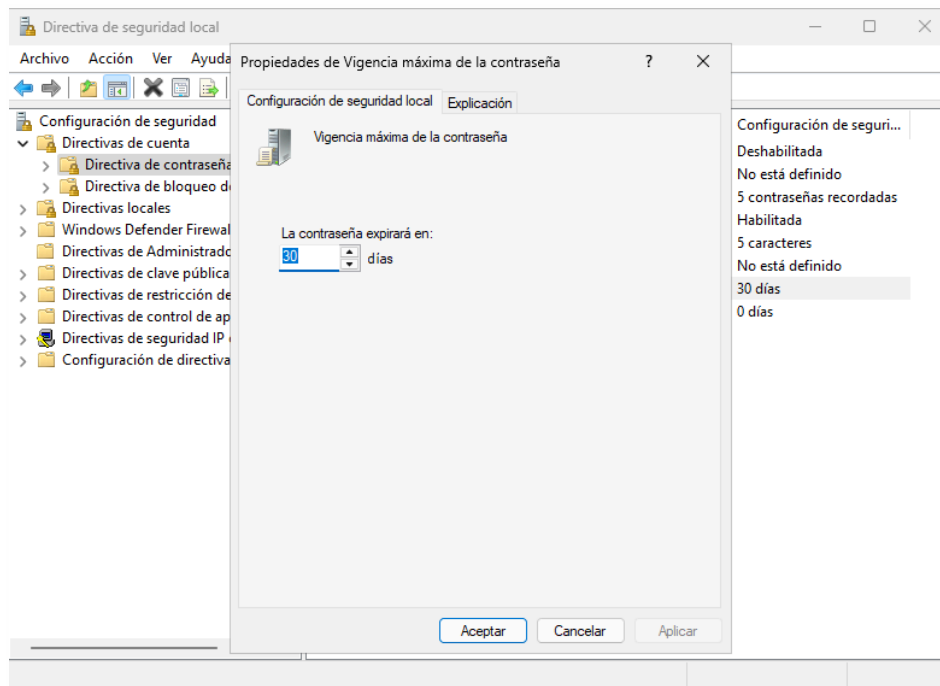
Crear un usuario administrador secundario con una contraseña compleja:

He creado el usuario Admin2 el cual es un administrador secundario.



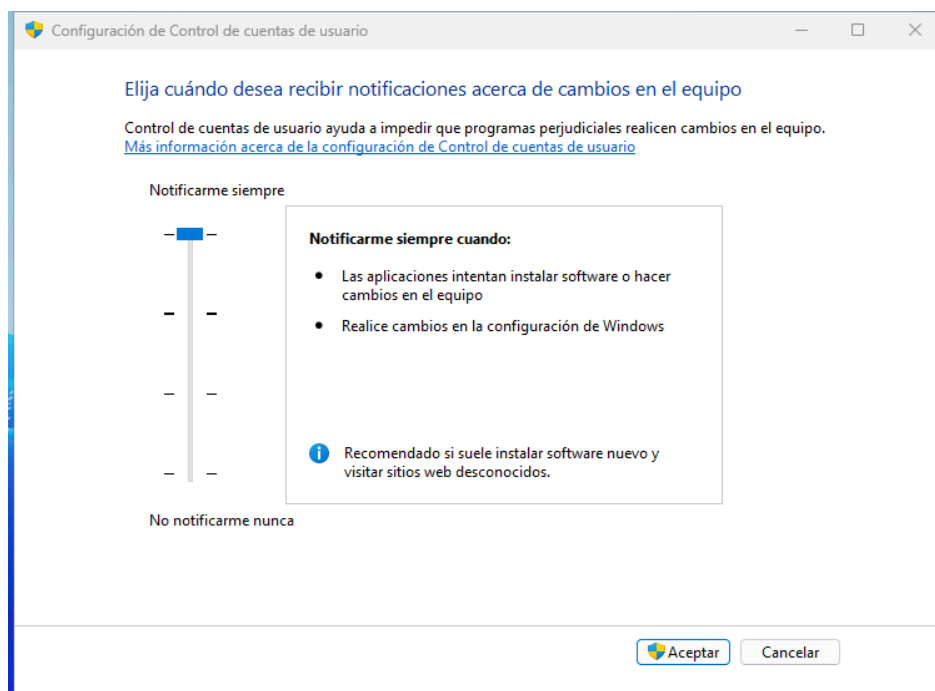
Configurar una directiva de seguridad local para que las contraseñas caduquen cada 30 días.

He cambiado la vigencia maxima de la contraseña a 30 dias en Herramientas-Directiva de seguridad local y luego en la carpeta Directivas de cuenta-Directivas de contraseñas.



Cambiar la configuración del Control de Cuentas de Usuario (UAC) para mayor control de privilegios.

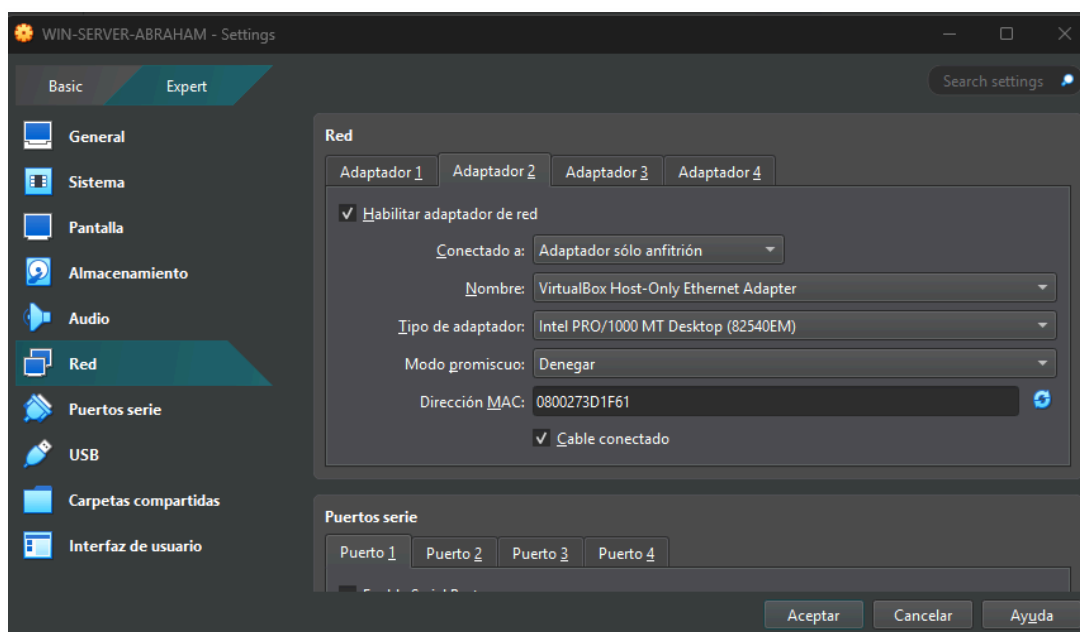
Cambié las notificaciones a siempre, para mayor control.



Fase 2: Ajustes de red y servicios

Establecer dos tarjetas de red en la máquina virtual: una para conexión interna, otra para externa.

He añadido otro adaptador de red tipo Solo Host.



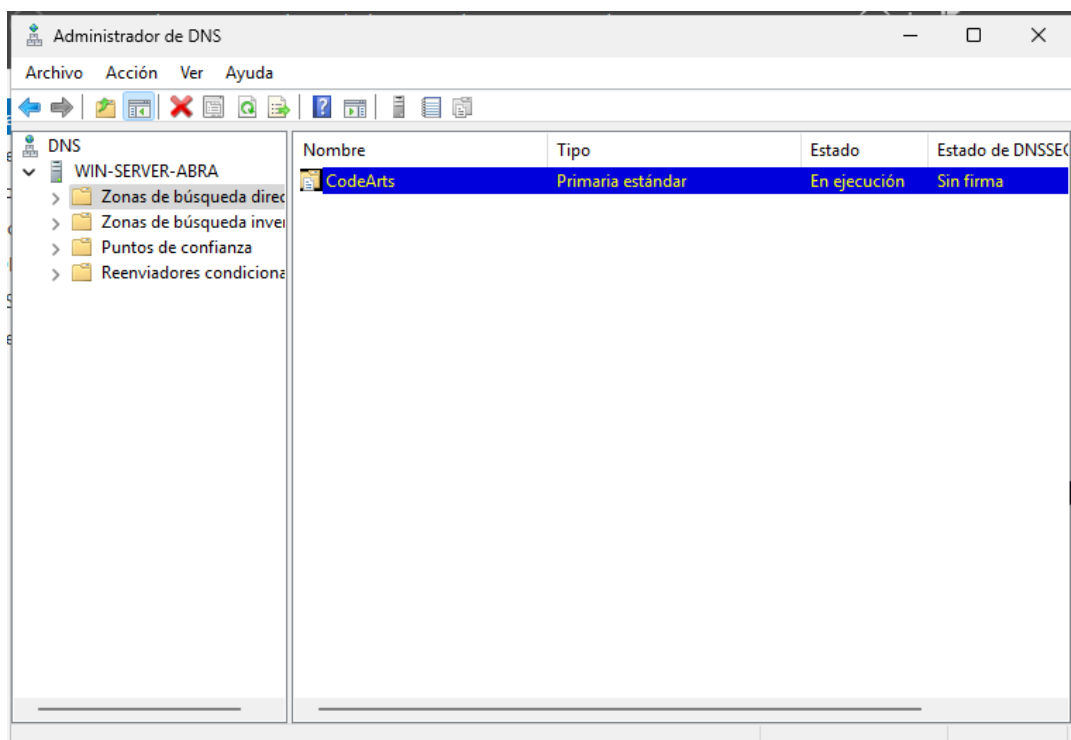
Configurar rutas estáticas en la tabla de red para simular un entorno más complejo.

Con el comando que he puesto en la siguiente imagen, básicamente le hemos dicho al sistema que cualquier paquete que vaya a la red 172.16.0.0 con máscara 255.255.255.0, lo envíe a través de la dirección 192.168.1.100, que es nuestro router.

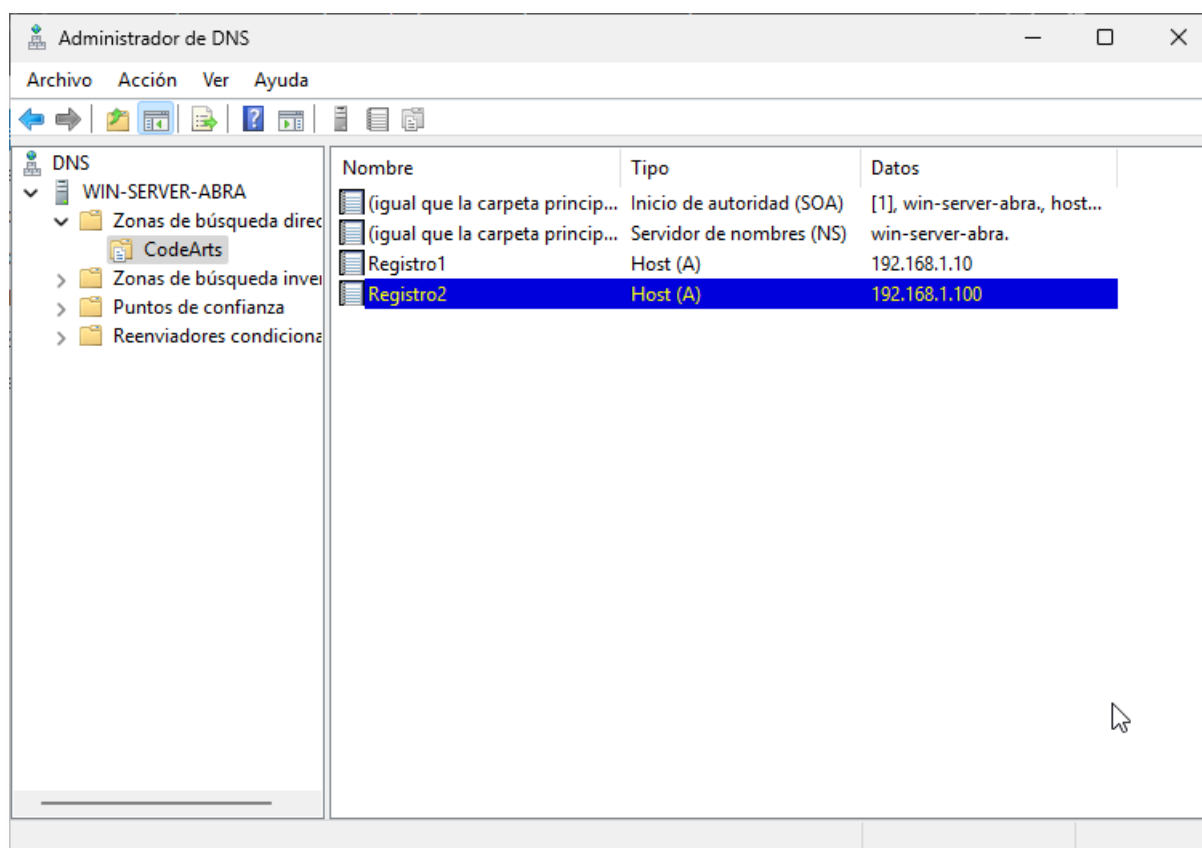
```
Administrador: Command Prompt
C:\Windows\System32>route ADD 172.16.0.0 MASK 255.255.255.0 192.168.1.100
Correcto
C:\Windows\System32>
```

Crear y activar un servidor DNS local, añadiendo una zona directa con al menos 2 registros

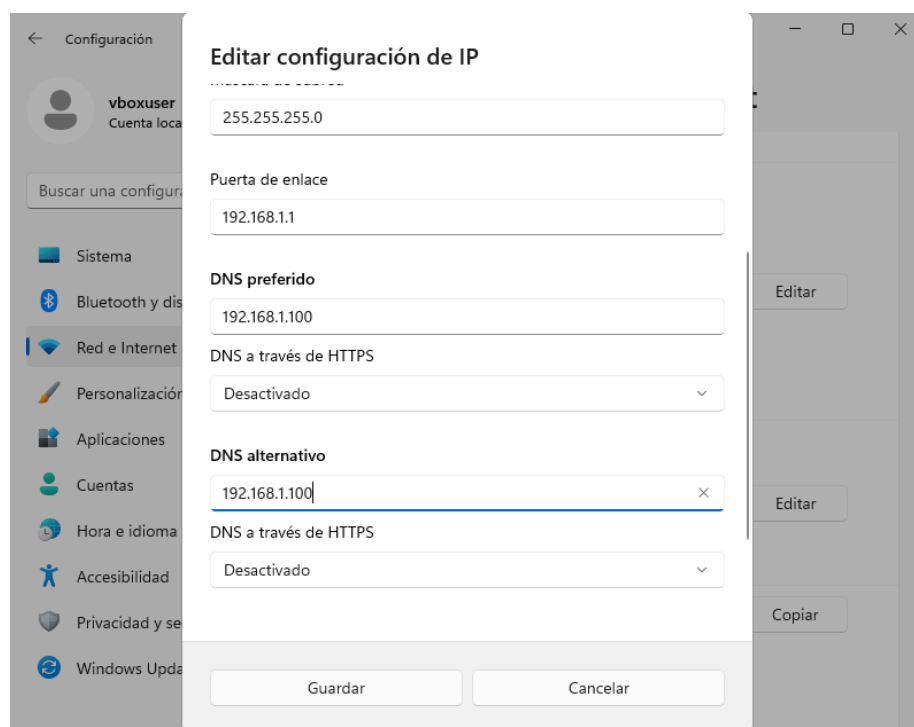
He instalado el rol DNS y he creado una zona primaria llamada CodeArts:



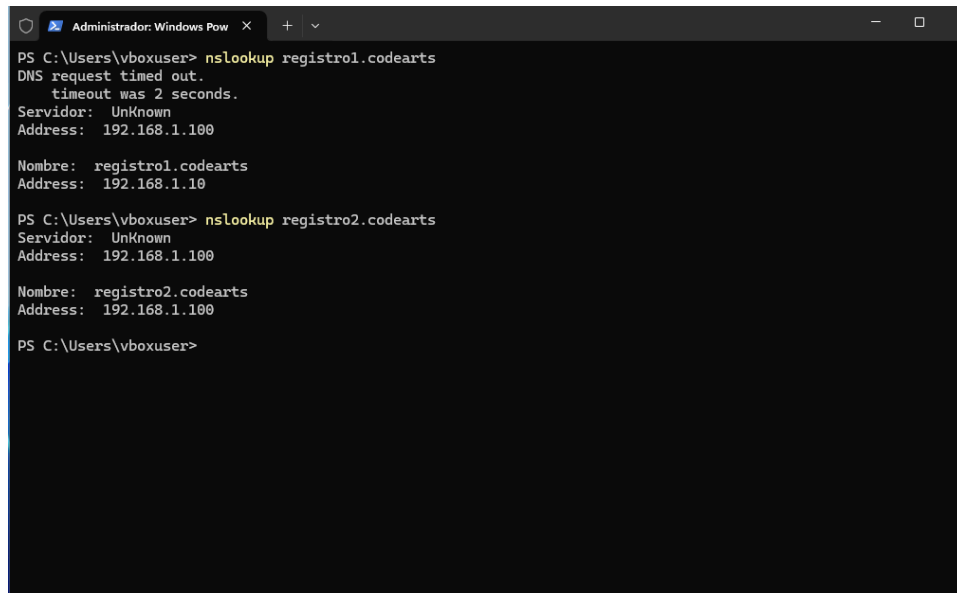
He creado 2 zonas directas, una para mi servidor y otra para otro dispositivo ficticio, con un registro cada una.



Añadimos las DNS a nuestro adaptador de red:



Y probamos que funciona:



```
PS C:\Users\vboxuser> nslookup registro1.codearts
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  192.168.1.100

Nombre:   registro1.codearts
Address:  192.168.1.10

PS C:\Users\vboxuser> nslookup registro2.codearts
Servidor:  UnKnown
Address:  192.168.1.100

Nombre:   registro2.codearts
Address:  192.168.1.100

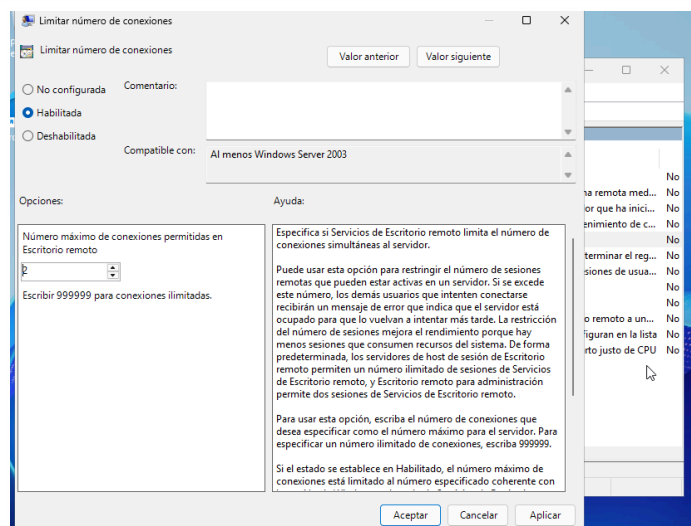
PS C:\Users\vboxuser>
```

Como nos devuelve las IP correctas significa que funciona perfectamente.

Fase 3: Personalización del entorno de trabajo del servidor

Habilitar el Escritorio Remoto y limitar el número de sesiones a 2.

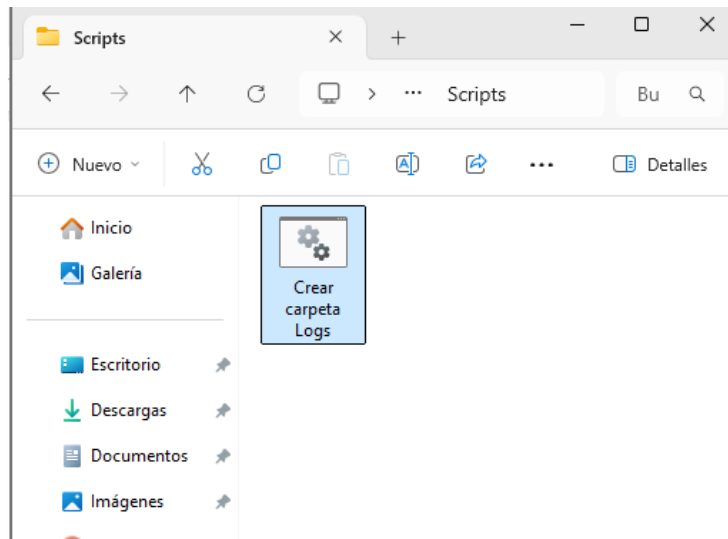
En la ruta: Configuración del equipo - Plantillas administrativas - Componentes de Windows - Servicios de Escritorio remoto - Host de sesión de Escritorio remoto - Conexiones he cambiado el número máximo de conexiones a 2.



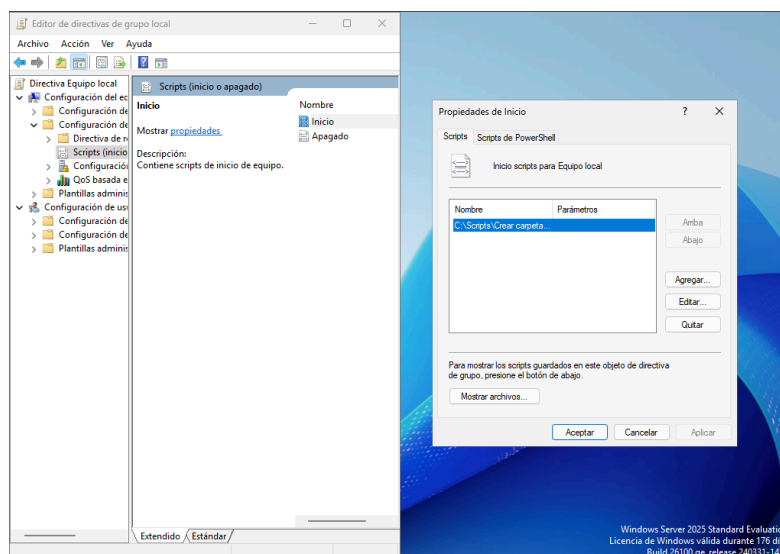
Personalizar el inicio del sistema añadiendo un script que cree automáticamente una carpeta de logs en C:\Logs.

He creado un archivo .bat desde el bloc de notas con el siguiente comando:

```
IF NOT EXIST C:\Logs MKDIR C:\Logs
```



Luego lo he añadido a los scripts de inicio desde el editor de directivas.

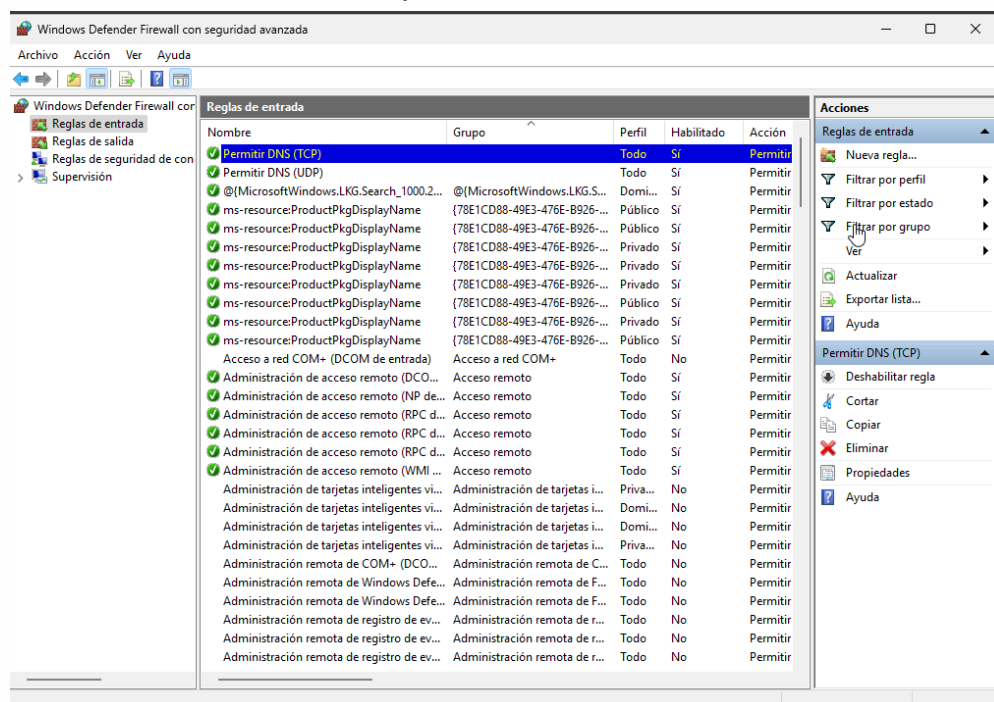


Configurar el firewall para que sólo permita el tráfico RDP y DNS.

La regla para permitir el tráfico RDP ya está creada:

✓	Multiplexor de equilibrador de carga de s...	Equilibrador de carga de sof...	Todo	No	Permitir
✓	Escritorio remoto - instantánea (TCP de e...	Escritorio remoto	Todo	Sí	Permitir
✓	Escritorio remoto - Modo usuario (TCP d...	Escritorio remoto	Todo	Sí	Permitir
✓	Escritorio remoto - Modo usuario (UDP d...	Escritorio remoto	Todo	Sí	Permitir

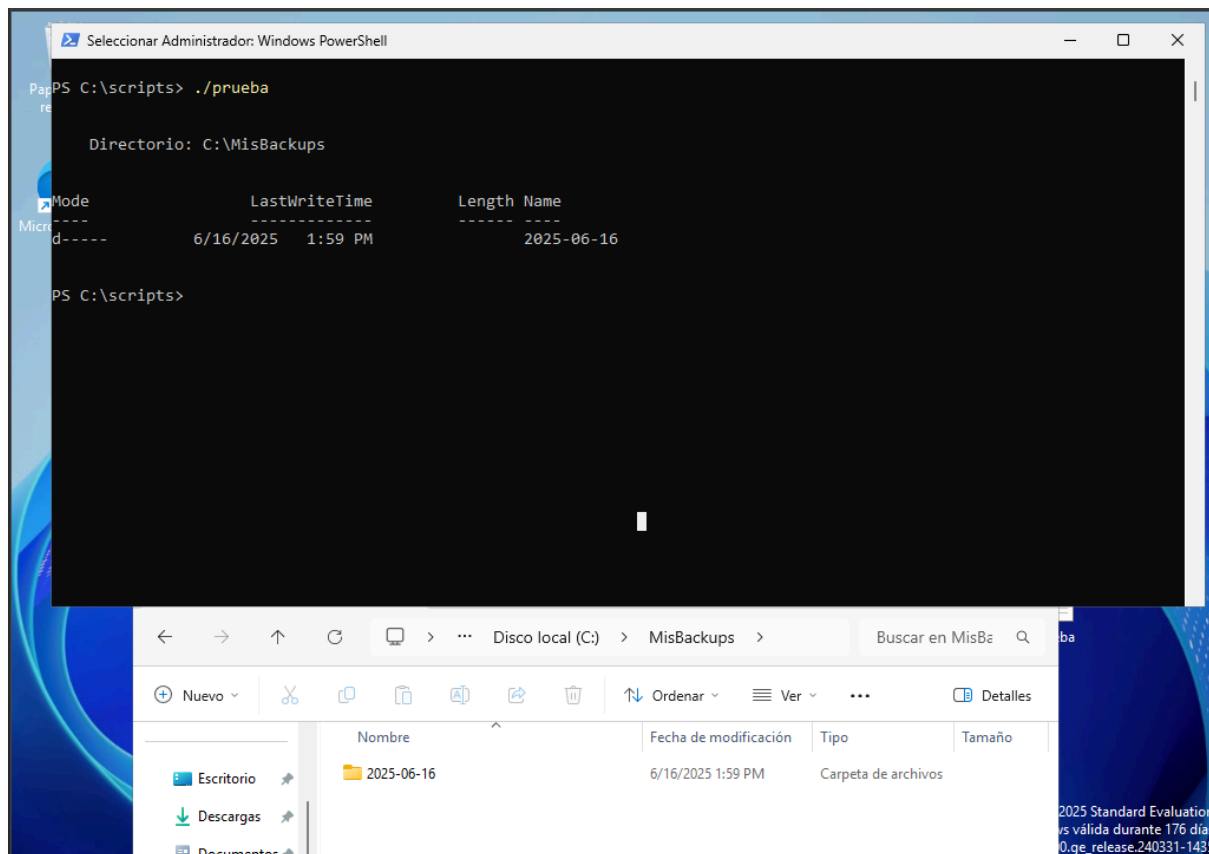
Por lo que si que creare las reglas para permitir conexiones TCP y UDP para la DNS:



Fase 4: Automatización básica

Crear un script en PowerShell

He creado un script en un bloc de notas y lo he guardado como .ps1 para abrirlo con PowerShell. Como podemos ver en la imagen, funciona perfectamente ejecutandolo desde PowerShell como administrador.



```
$DestinoHoy = "C:\MisBackups\$((Get-Date -Format 'yyyy-MM-dd'))"
New-Item -Path $DestinoHoy -ItemType Directory -Force -ErrorAction
SilentlyContinue
```

```
$LogFile = "$DestinoHoy\resultado_copia.txt"
```

```
try {
Copy-Item -Path "$env:USERPROFILE\Desktop\*" -Destination
$DestinoHoy -Recurse -Force -ErrorAction Stop
"Resultado: COPIA CORRECTA." | Out-File -FilePath $LogFile
}
catch {
"Resultado: ERROR." | Out-File -FilePath $LogFile
"Detalle: $($_.Exception.Message)" | Out-File -FilePath $LogFile
-Append
}
```