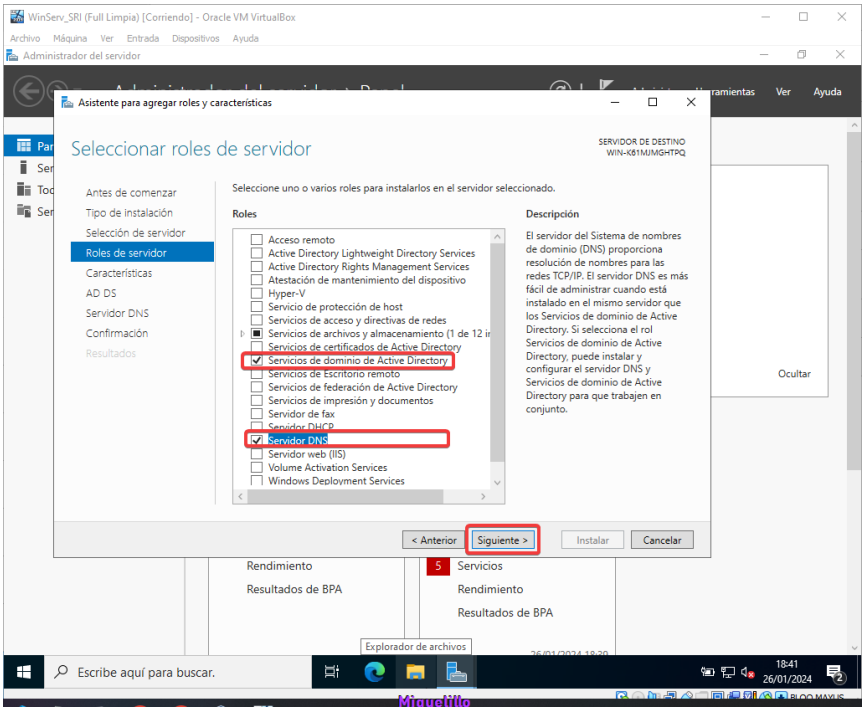
Índice:

Ejercicio 1

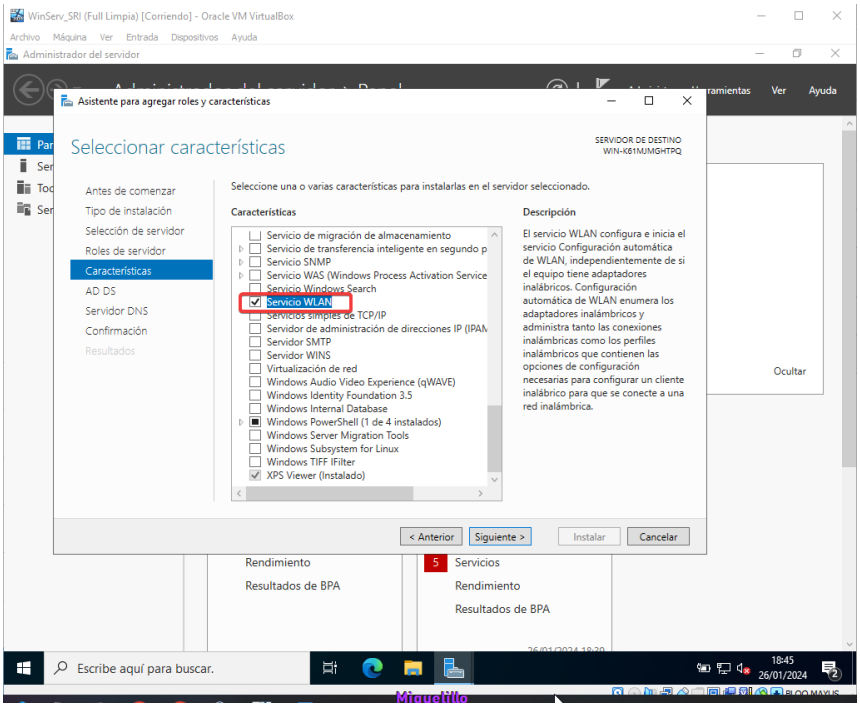
a) Configurar Windows 2008/2012 Server como servidor RADIUS

Solución:

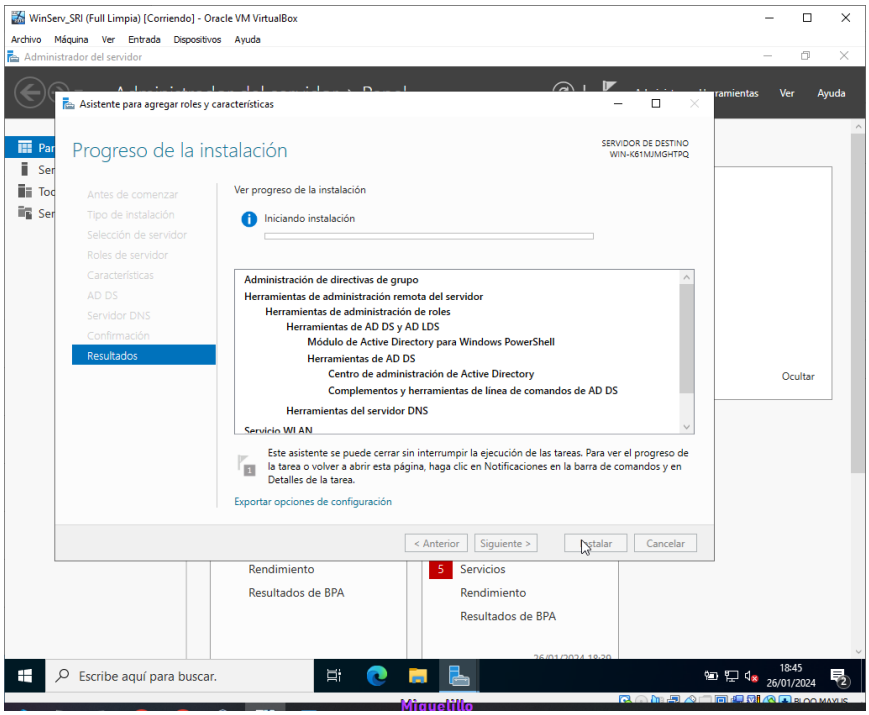
Vamos a **Administrar→ Agregar Roles y Características → Instalamos Active Directory y DNS**



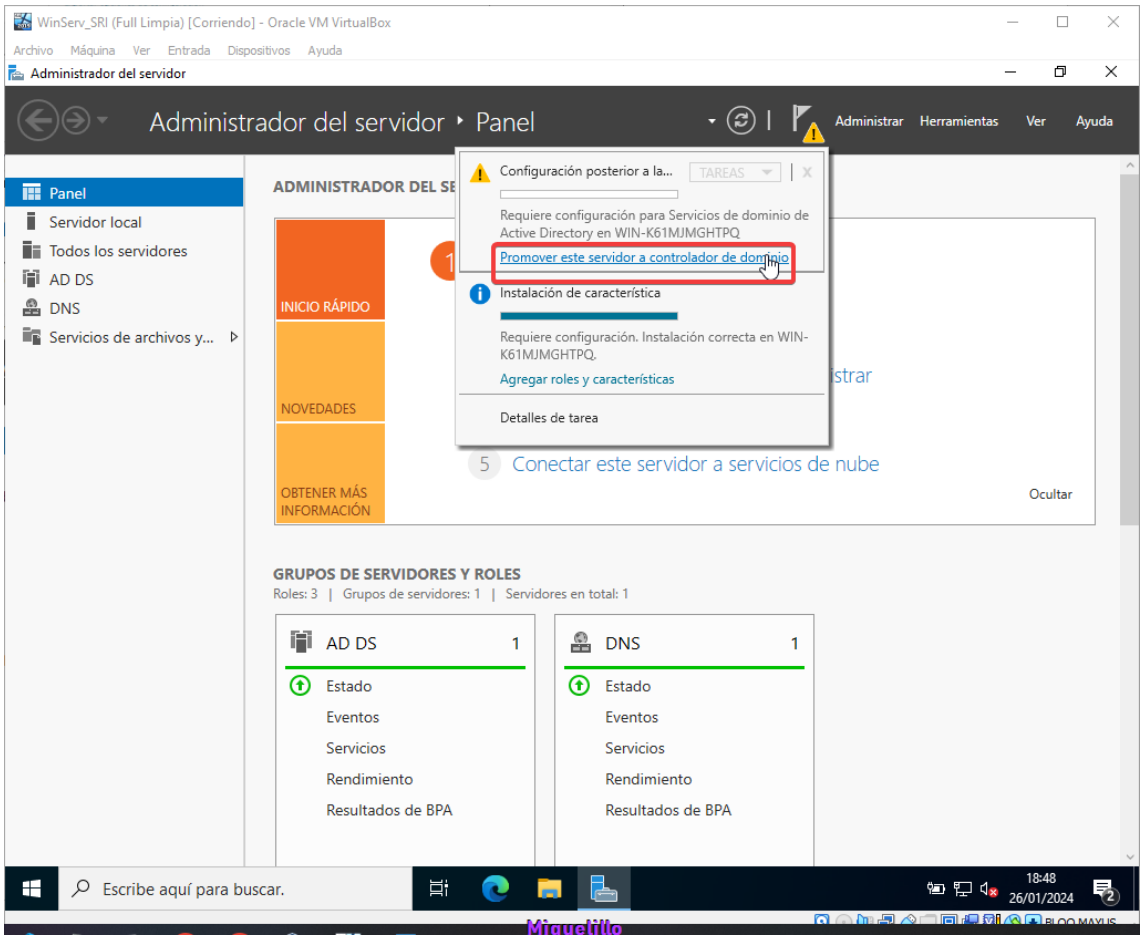
En Funcionalidades ponemos **Servicio WLAN**



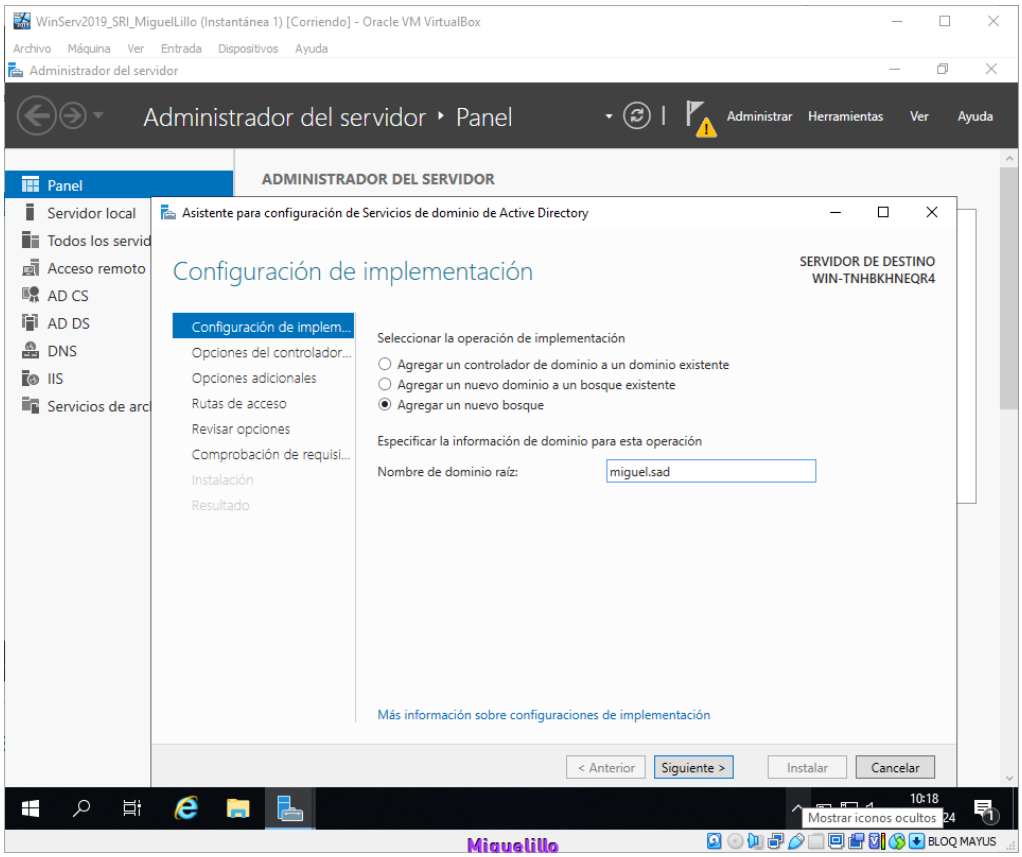
Esperamos que se instale la característica



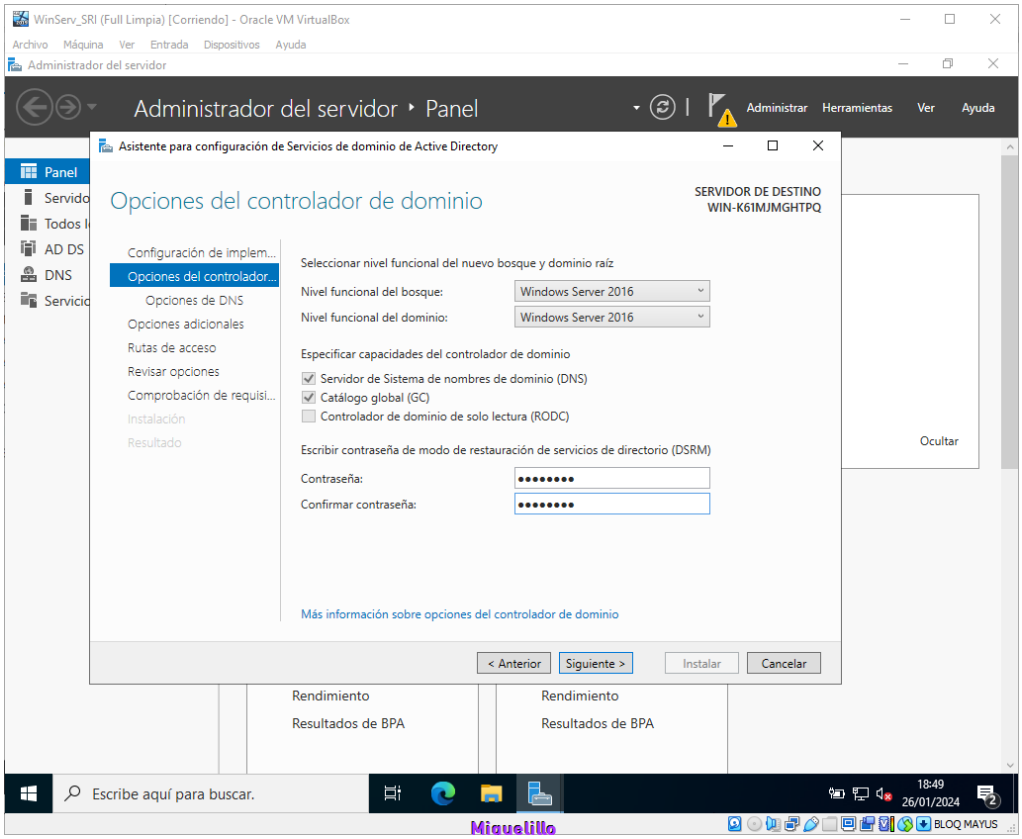
Configuramos Active Directory



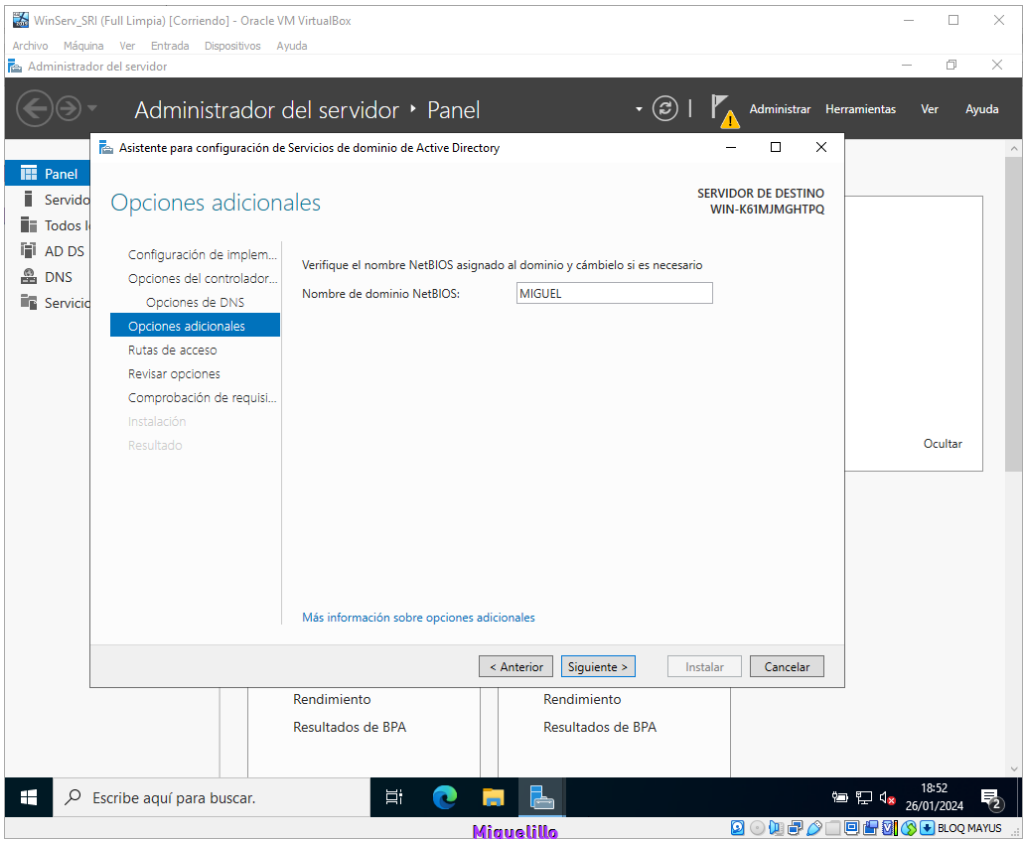
Ponemos el nombre del dominio



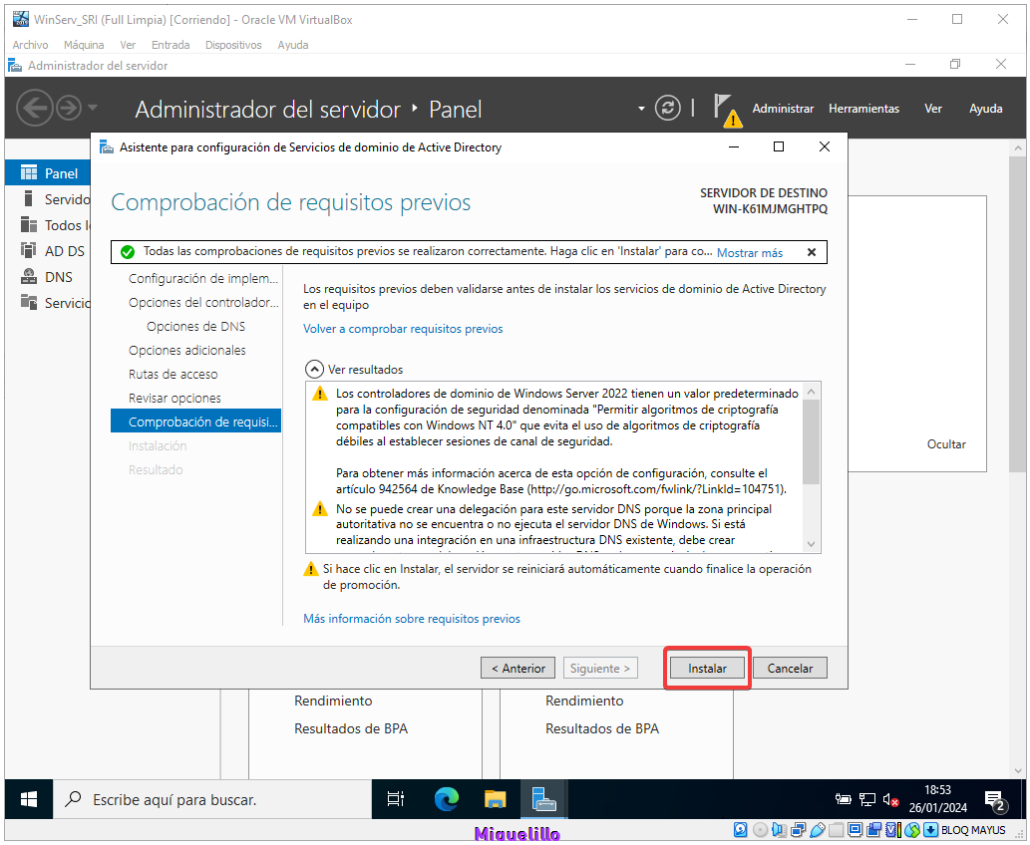
Configuramos la contraseña



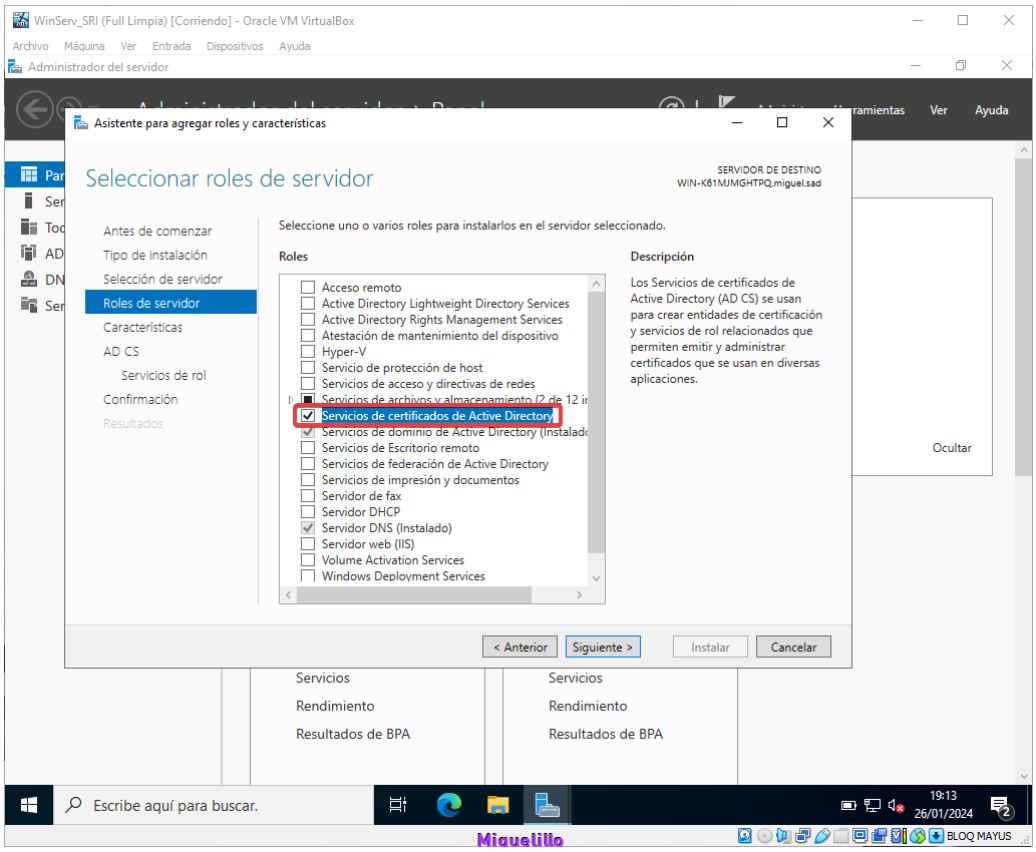
Configuramos l nombre NETBIOS

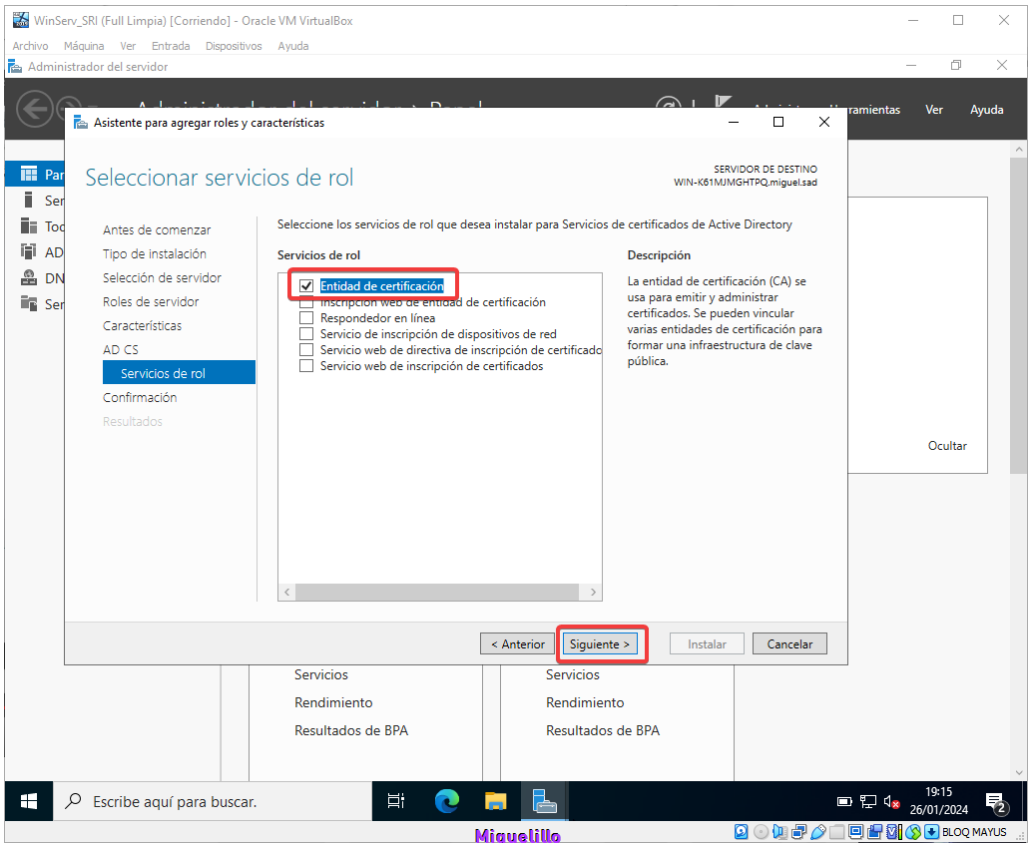


Clicamos en **Instalar**

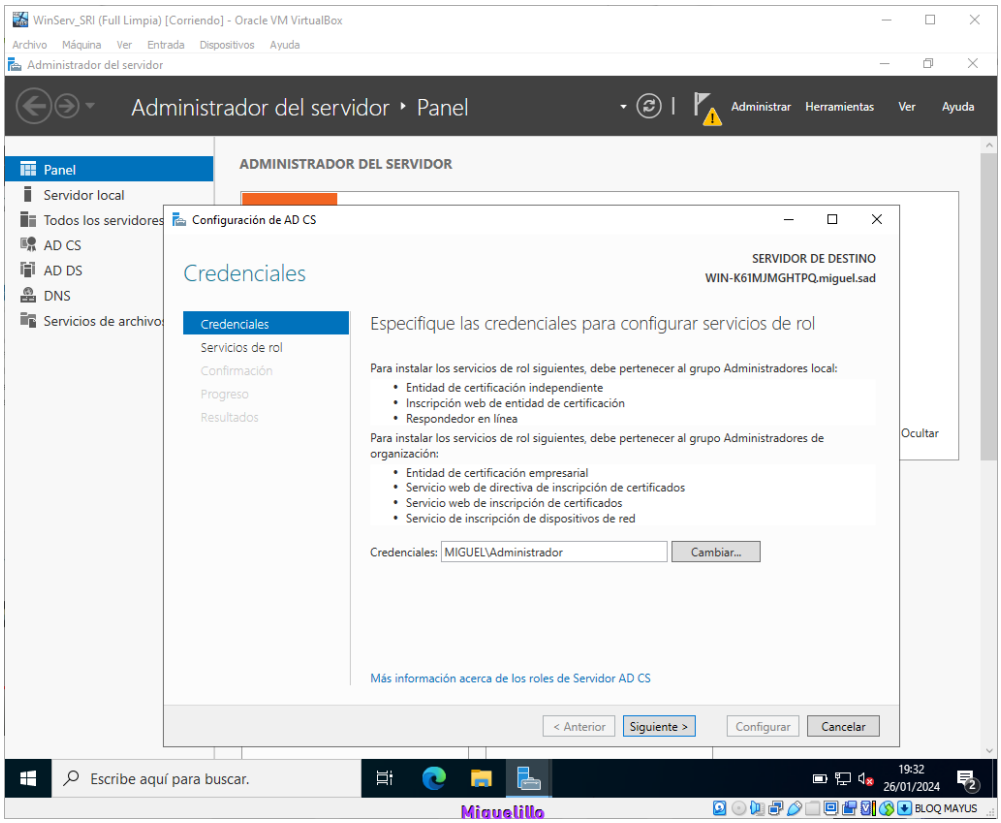


Instalamos los servidores

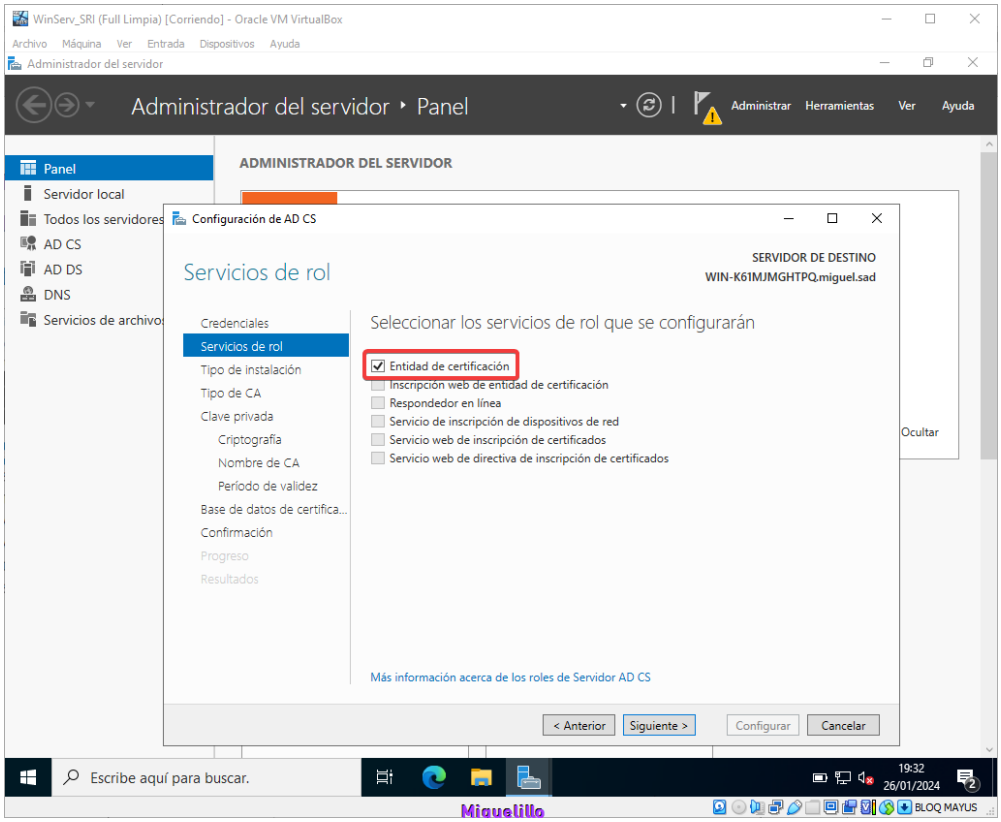




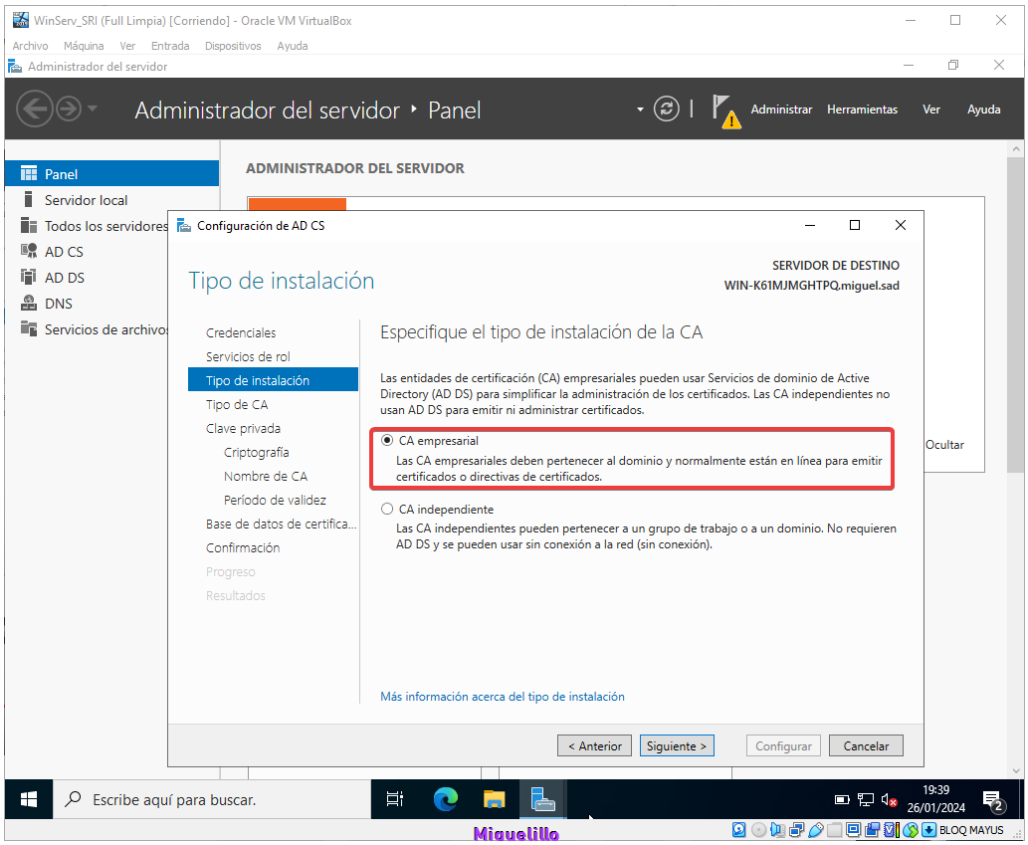
Instalamos la entidad certificadora

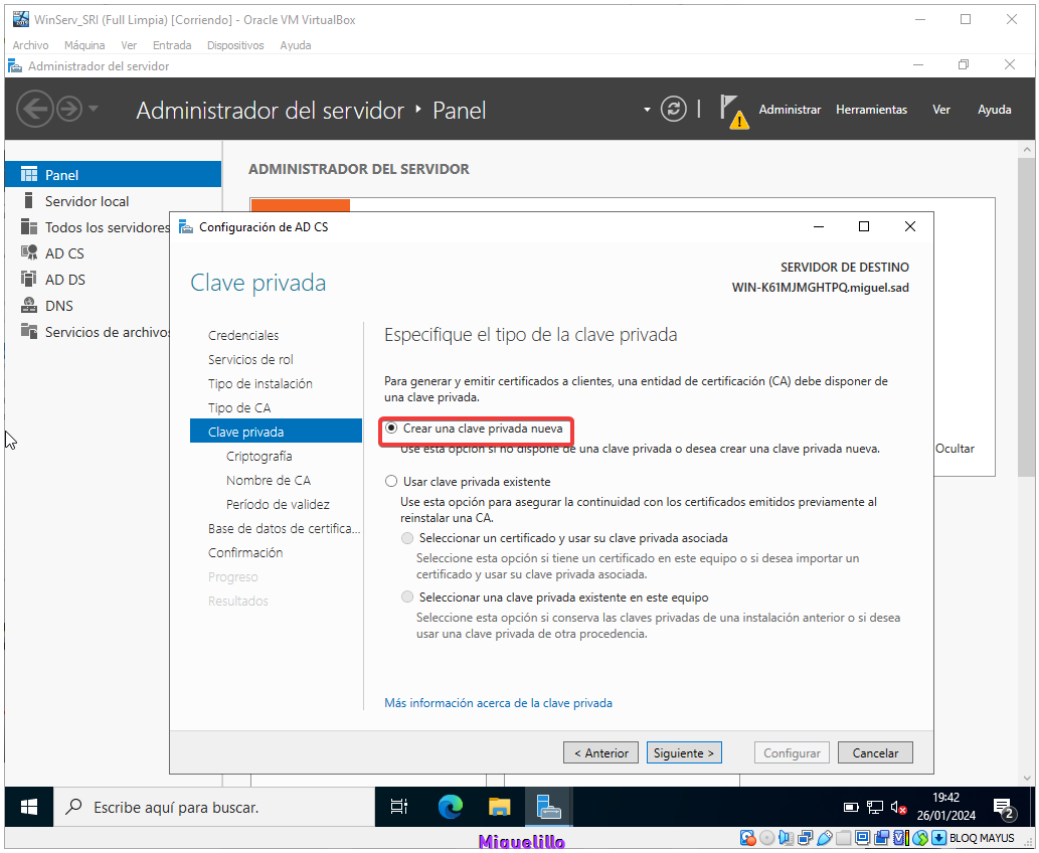


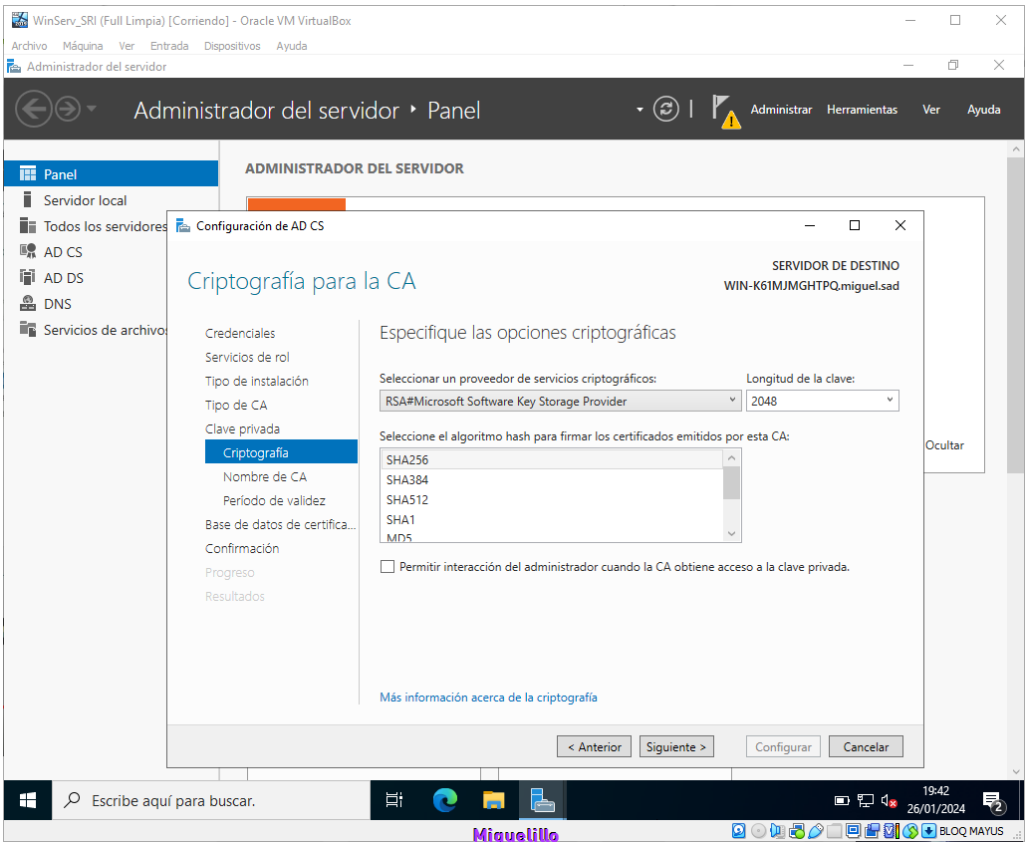
Seleccionamos los servicios de rol que queremos configurar **Entidad de certificación**

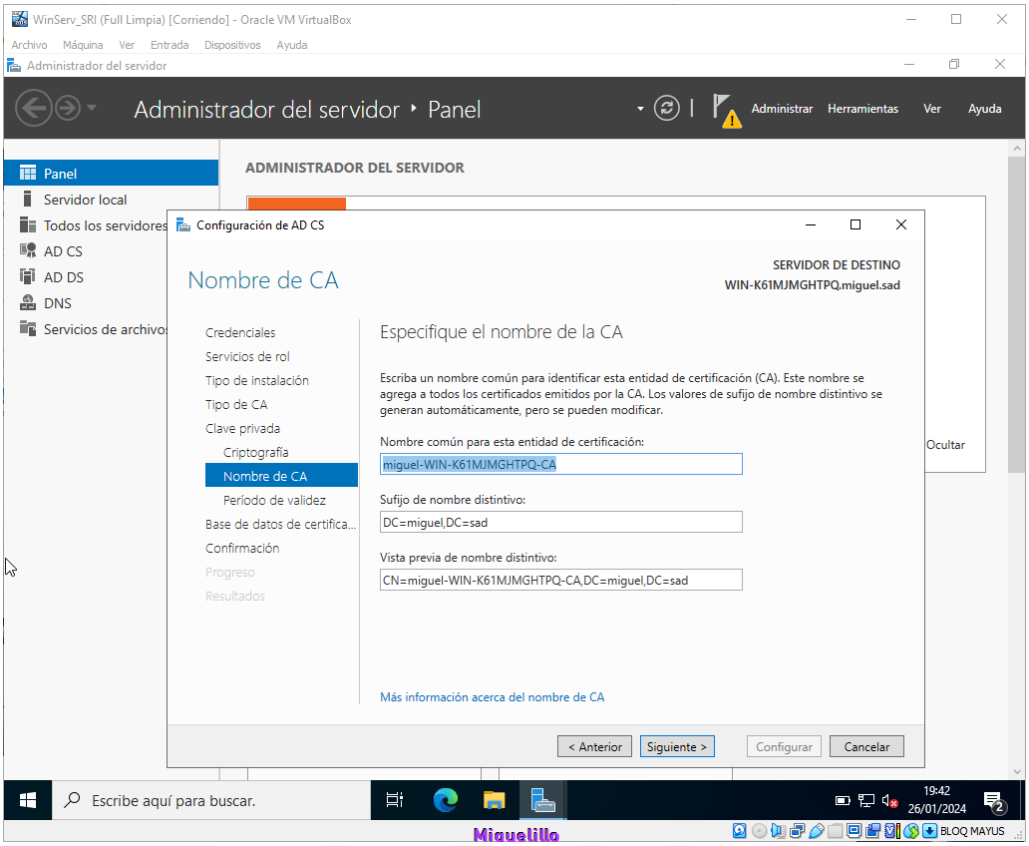


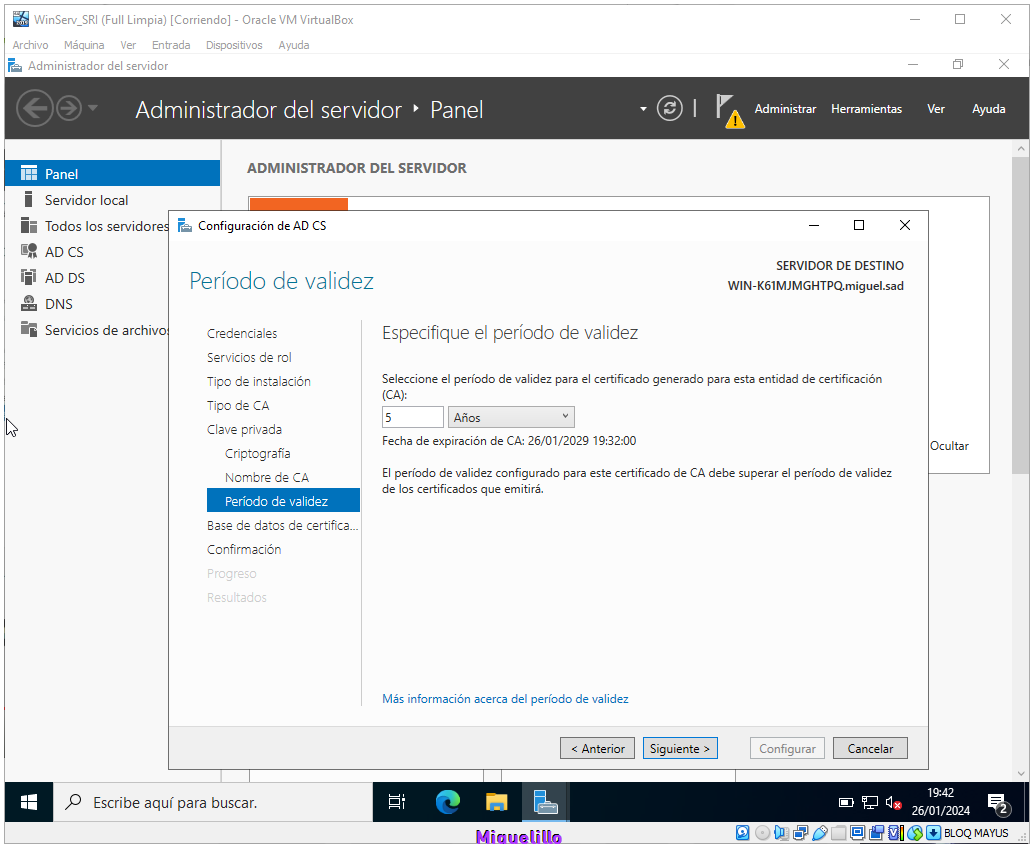
Seleccionamos **CA empresarial**

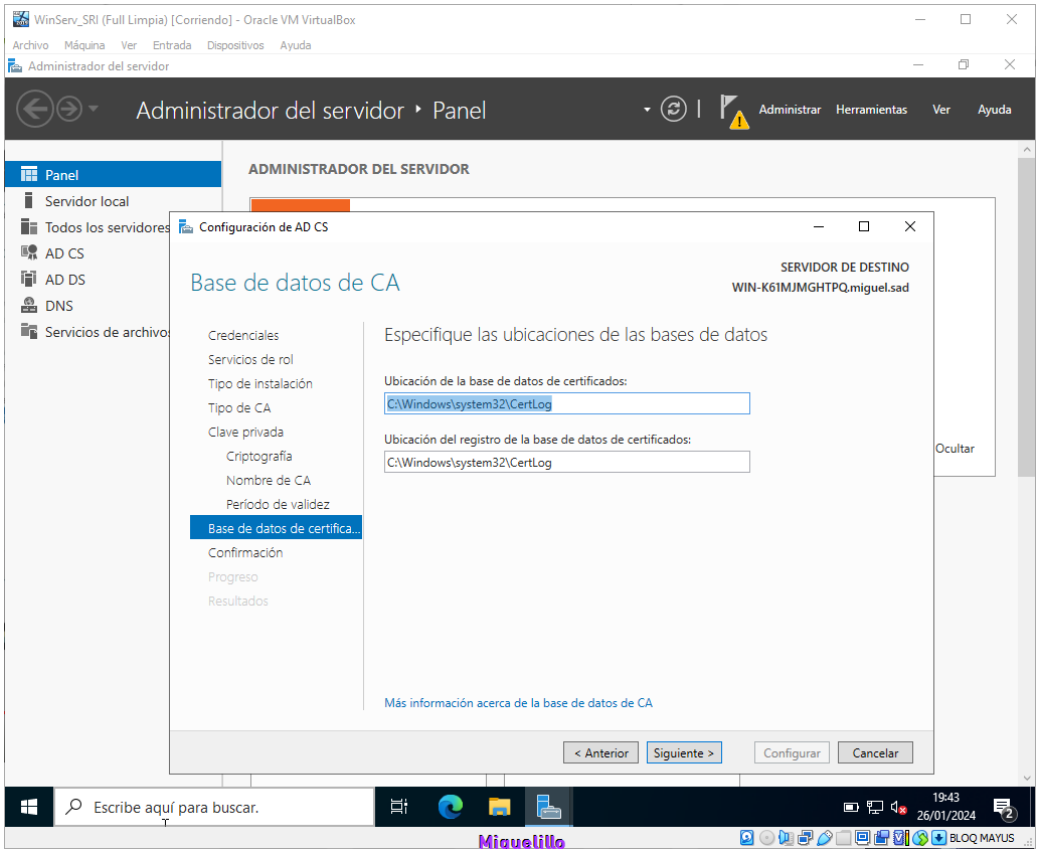


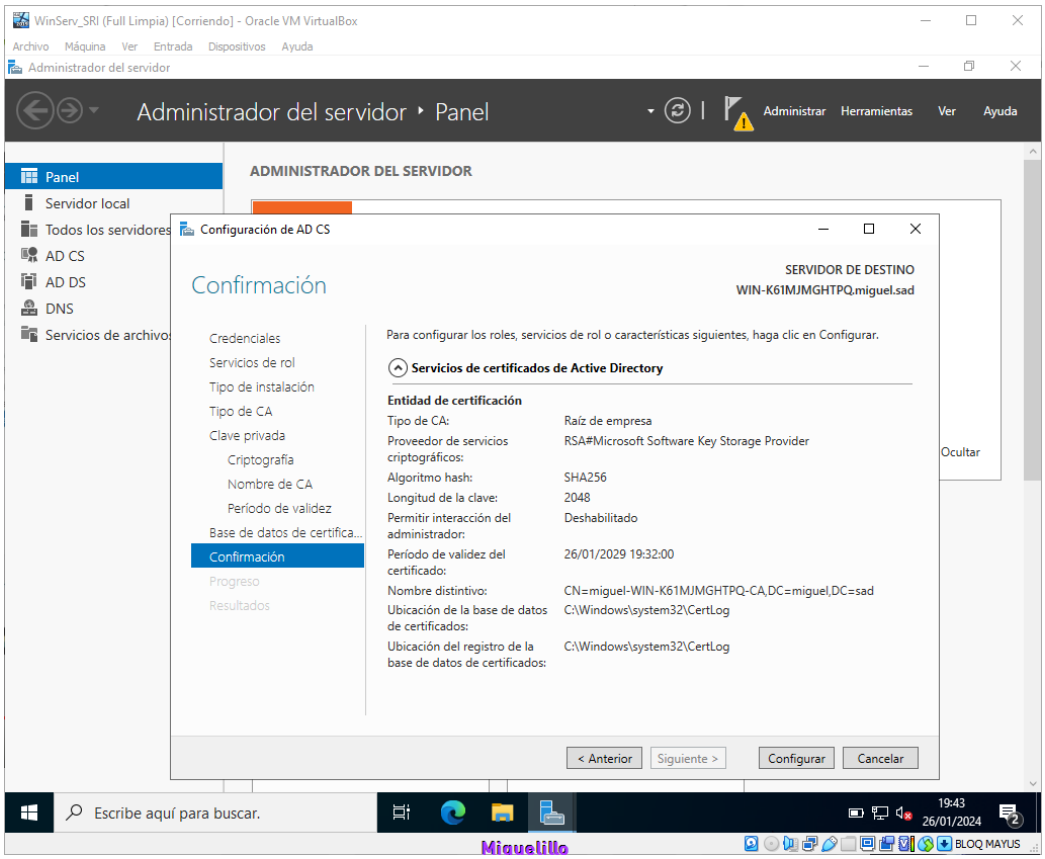



WinServ_SRI (Full Limpia) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador del servidor
Administrador del servidor ‣ Panel
Administrar Herramientas Ver Ayuda
Panel
Servidor local
Todos los servidores
AD CS
AD DS
DNS
Servicios de archivo
ADMINISTRADOR DEL SERVIDOR
Ocultar
Configuración de AD CS
Criptografía para la CA
SERVIDOR DE DESTINO
WIN-K61MJMGHTPQ.miguel.sad
Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados
Especifique las opciones criptográficas
Seleccionar un proveedor de servicios criptográficos:
RSA#Microsoft Software Key Storage Provider
Longitud de la clave:
2048
Seleccione el algoritmo hash para firmar los certificados emitidos por esta CA:
SHA256
SHA384
SHA512
SHA1
MD5
Permitir interacción del administrador cuando la CA obtiene acceso a la clave privada.
Más información acerca de la criptografía
< Anterior
Siguiente >
Configurar
Cancelar
Escribe aquí para buscar.
19:42
26/01/2024
Miguelillo
BLOQ MAYUS

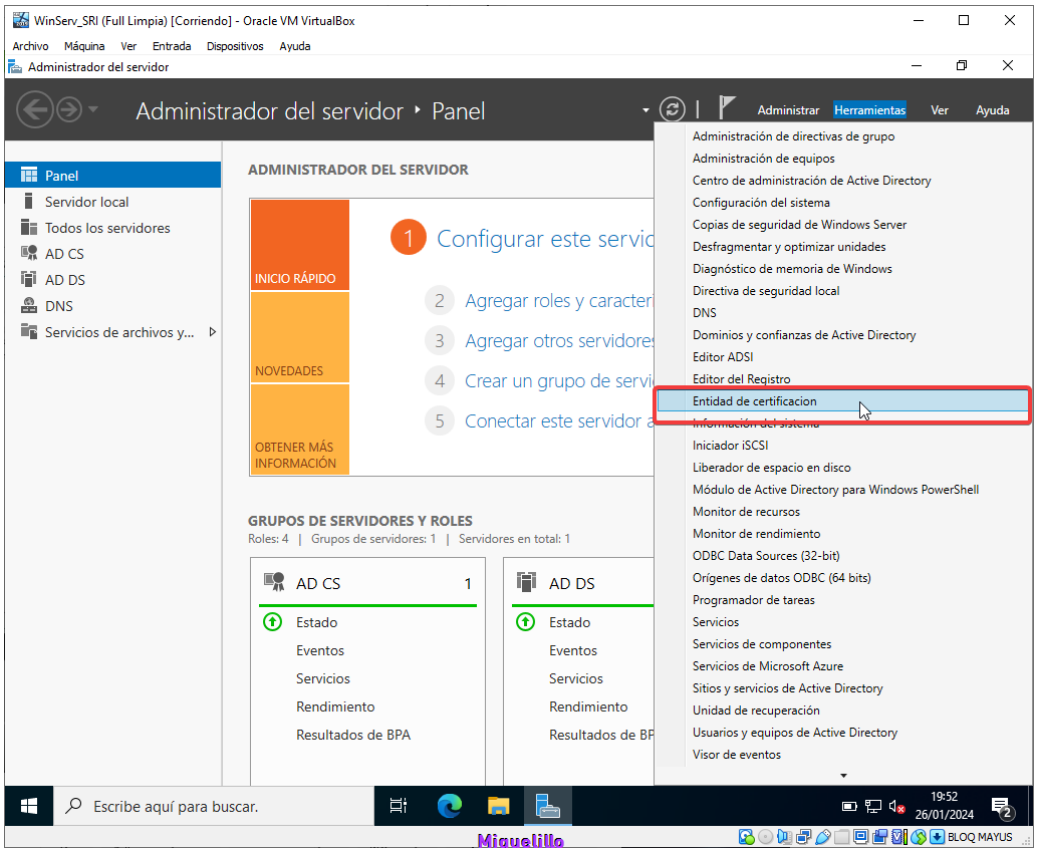

WinServ_SRI (Full Limpia) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador del servidor
Administrador del servidor ‣ Panel
Administrar Herramientas Ver Ayuda
Panel
Servidor local
Todos los servidores
AD CS
AD DS
DNS
Servicios de archivo
ADMINISTRADOR DEL SERVIDOR
Ocultar
Configuración de AD CS
Nombre de CA
SERVIDOR DE DESTINO
WIN-K61MJMGHTPQ.miguel.sad
Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados
Especifique el nombre de la CA
Escriba un nombre común para identificar esta entidad de certificación (CA). Este nombre se agrega a todos los certificados emitidos por la CA. Los valores de sufijo de nombre distintivo se generan automáticamente, pero se pueden modificar.
Nombre común para esta entidad de certificación:
miguel-WIN-K61MJMGHTPQ-CA
Sufijo de nombre distintivo:
DC=miguel,DC=sad
Vista previa de nombre distintivo:
CN=miguel-WIN-K61MJMGHTPQ-CA,DC=miguel,DC=sad
Más información acerca del nombre de CA
< Anterior
Siguiente >
Configurar
Cancelar
Escribe aquí para buscar.
19:42
26/01/2024
Miguelillo
BLOQ MAYUS


WinServ_SRI (Full Limpia) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador del servidor
Administrador del servidor ‣ Panel
Administrar Herramientas Ver Ayuda
Panel
Servidor local
Todos los servidores
AD CS
AD DS
DNS
Servicios de archivo
ADMINISTRADOR DEL SERVIDOR
Ocultar
Configuración de AD CS
Período de validez
SERVIDOR DE DESTINO
WIN-K61MJMGHTPQ.miguel.sad
Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados
Especifique el período de validez
Seleccione el período de validez para el certificado generado para esta entidad de certificación (CA):
5
Años
Fecha de expiración de CA: 26/01/2029 19:32:00
El período de validez configurado para este certificado de CA debe superar el período de validez de los certificados que emitirá.
Más información acerca del período de validez
< Anterior
Siguiente >
Configurar
Cancelar
Escribe aquí para buscar.
19:42
26/01/2024
Miguelillo
BLOQ MAYUS

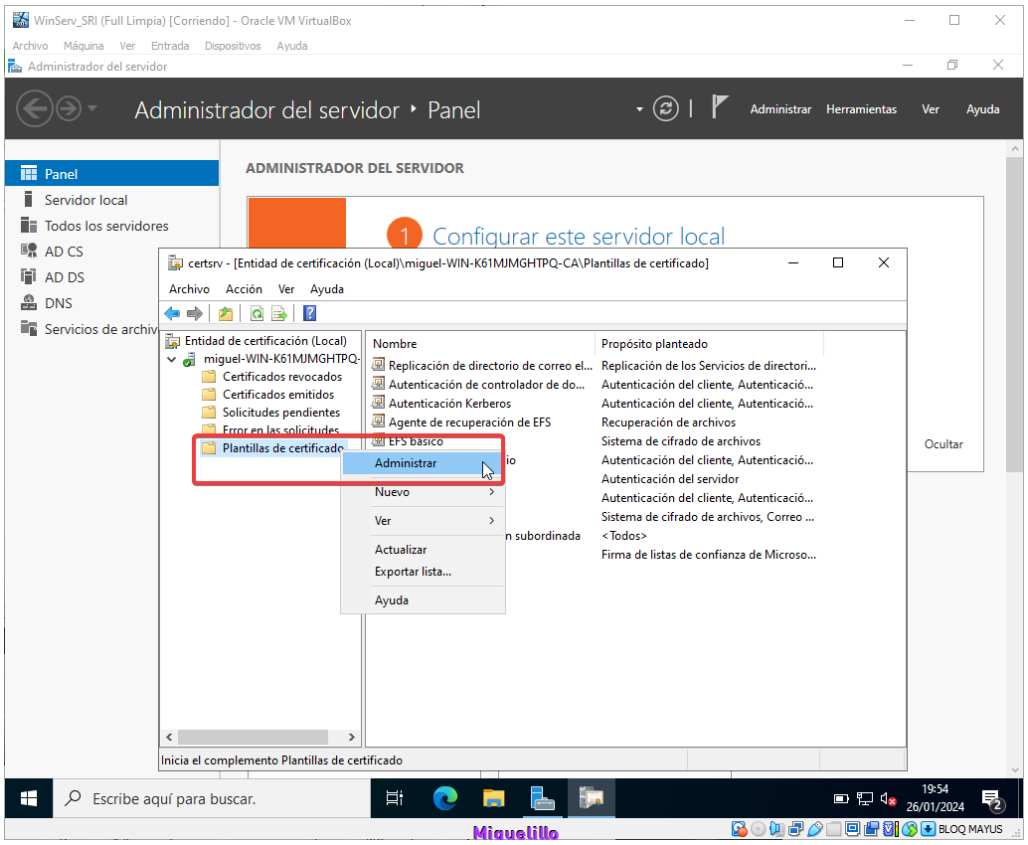

WinServ_SRI (Full Limpia) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Administrador del servidor
Administrador del servidor ‣ Panel
Administrar Herramientas Ver Ayuda
Panel
Servidor local
Todos los servidores
AD CS
AD DS
DNS
Servicios de archivo
ADMINISTRADOR DEL SERVIDOR
Ocultar
Configuración de AD CS
Base de datos de CA
SERVIDOR DE DESTINO
WIN-K61MJMGHTPQ.miguel.sad
Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados
Especifique las ubicaciones de las bases de datos
Ubicación de la base de datos de certificados:
C:\Windows\system32\CertLog
Ubicación del registro de la base de datos de certificados:
C:\Windows\system32\CertLog
Más información acerca de la base de datos de CA
< Anterior
Siguiente >
Configurar
Cancelar
Escribe aquí para buscar.
19:43
26/01/2024
Miguelillo
BLOQ MAYUS



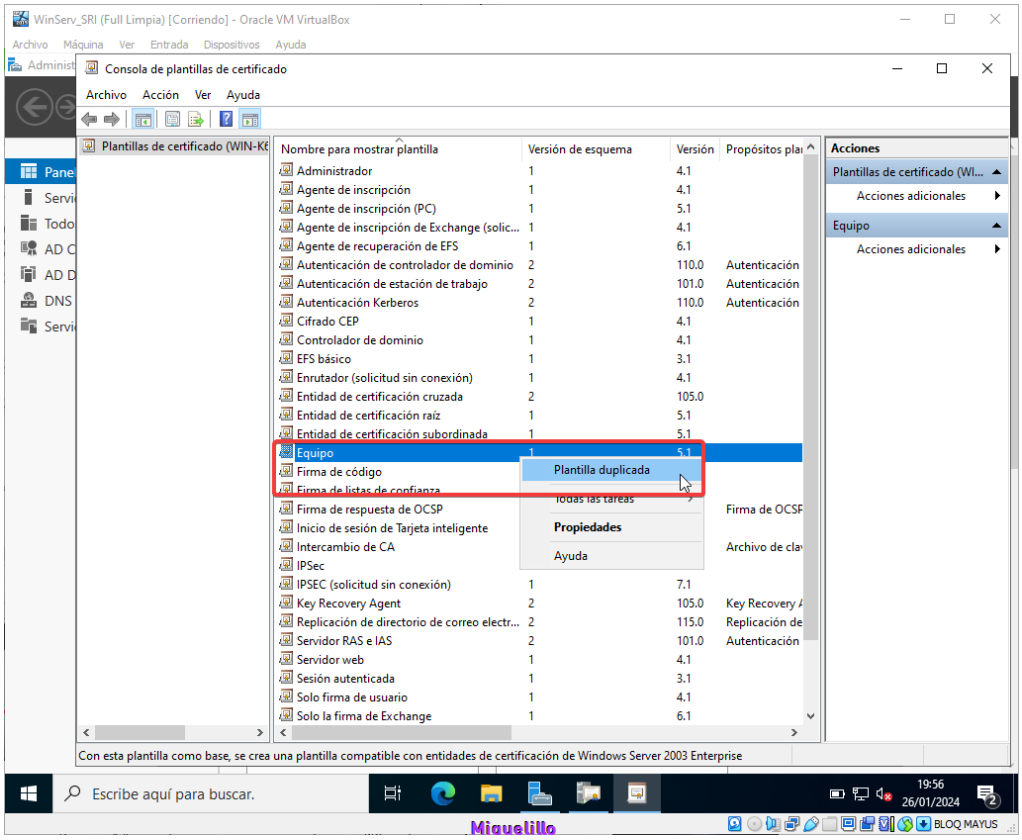
Seleccionamos **Entidad de certificación**



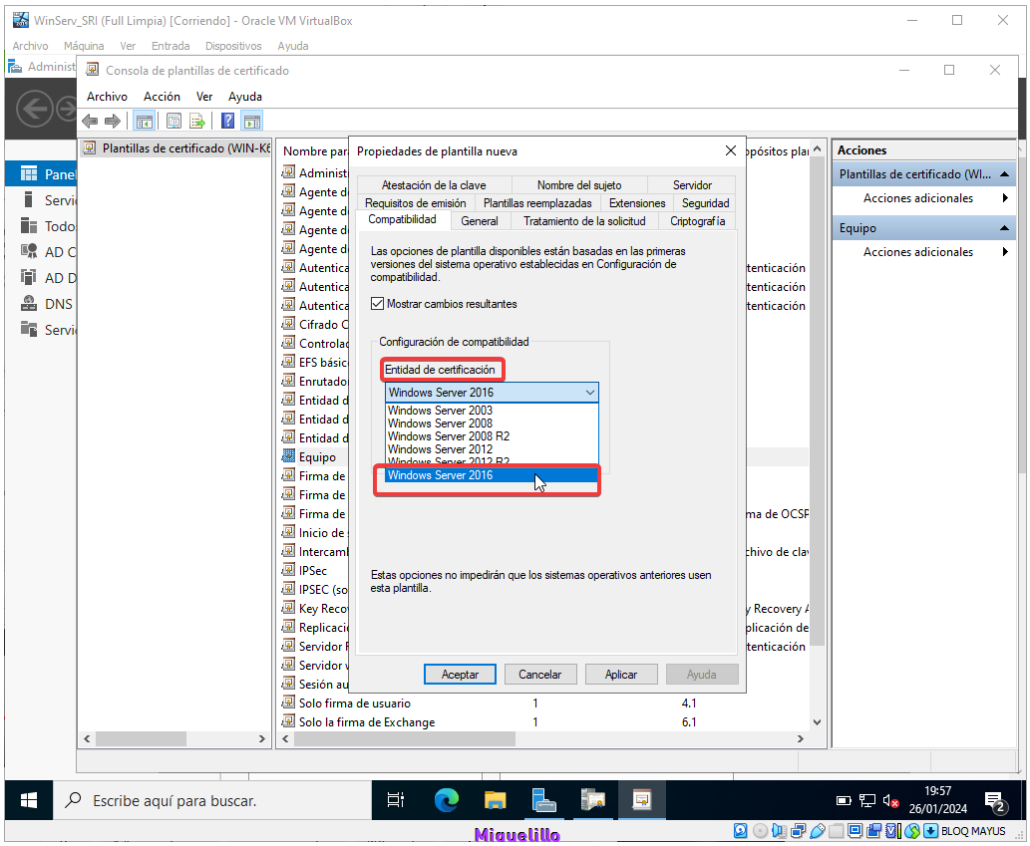
Clicamos en **Pantillas de certificado → Administrar**



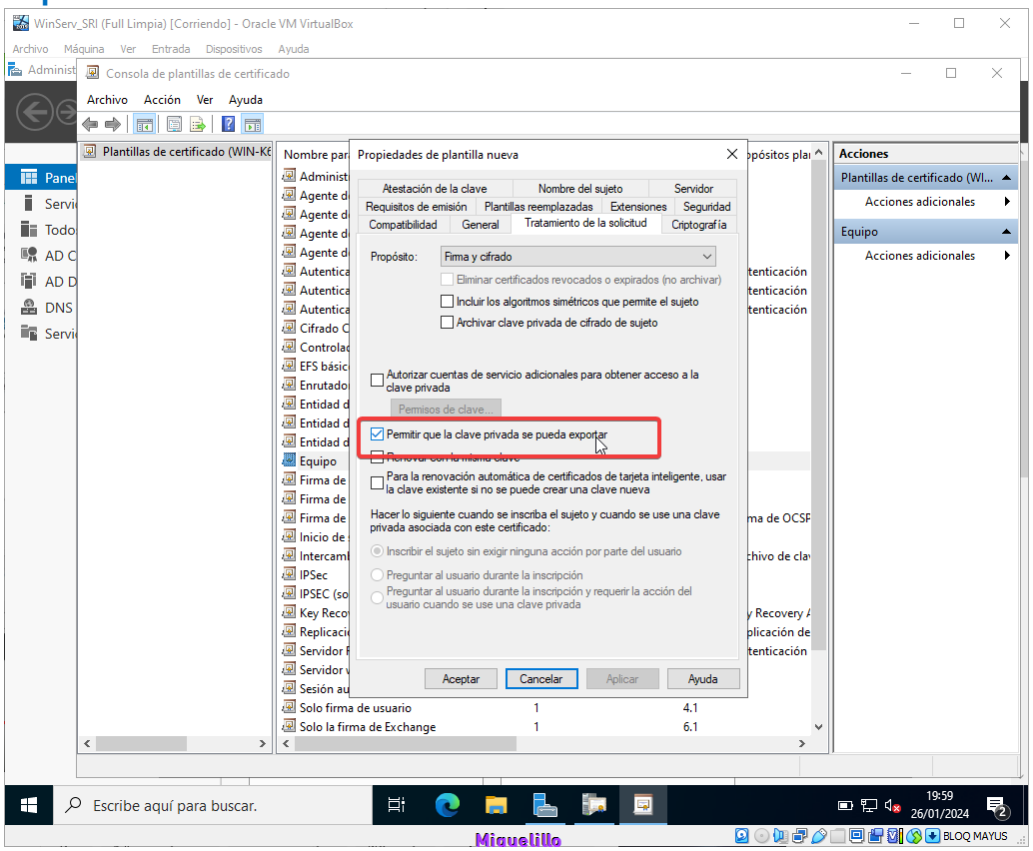
Vamos a **Equipo** y duplicamos la plantilla



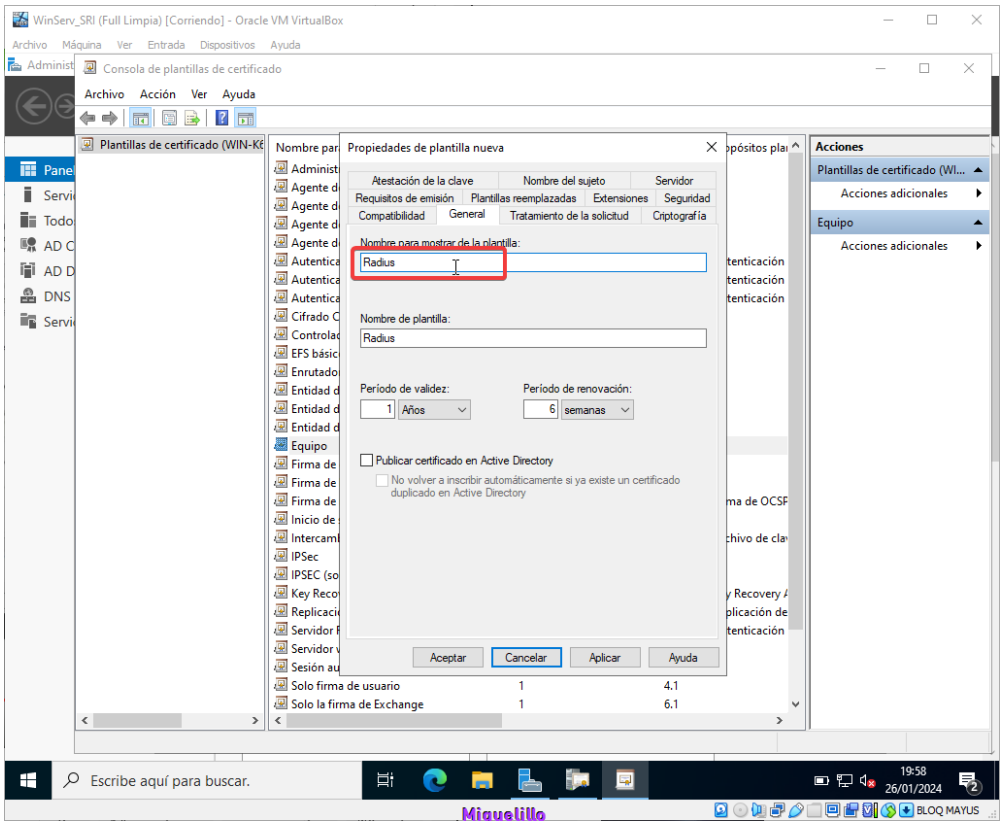
Vamos a **Compatibilidad** Seleccionamos **Windows Server 2016**



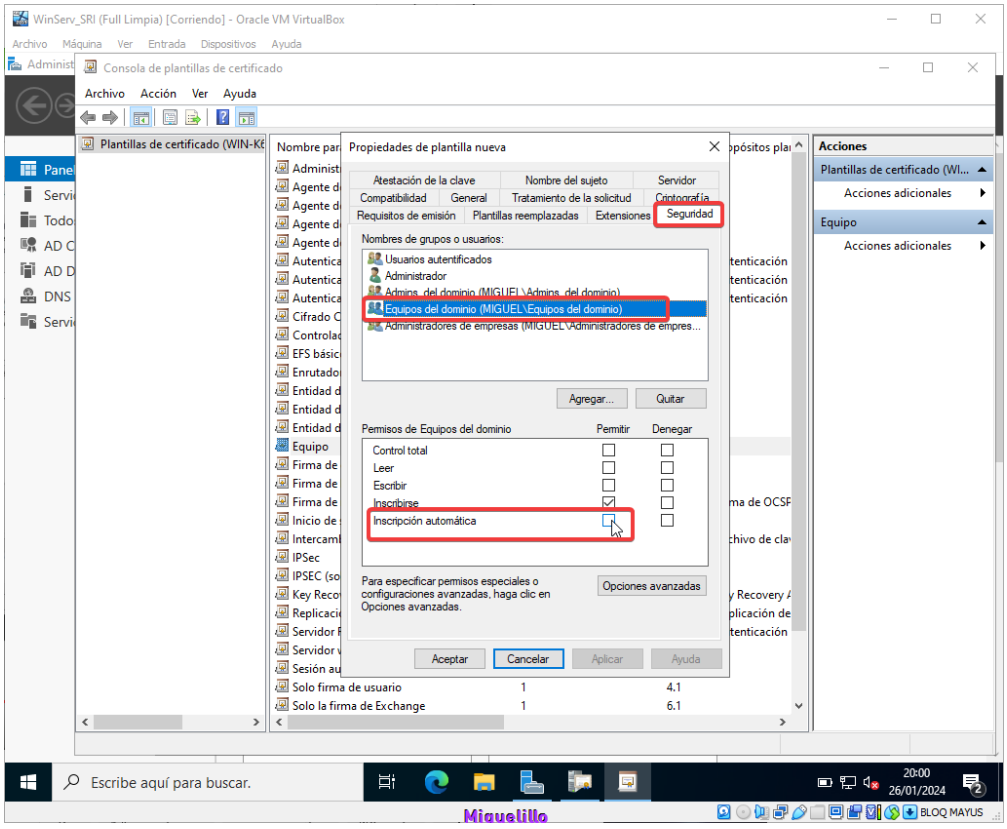
Vamos a **Tratamiento de solicitud Permitimos que la clave se pueda exportar**



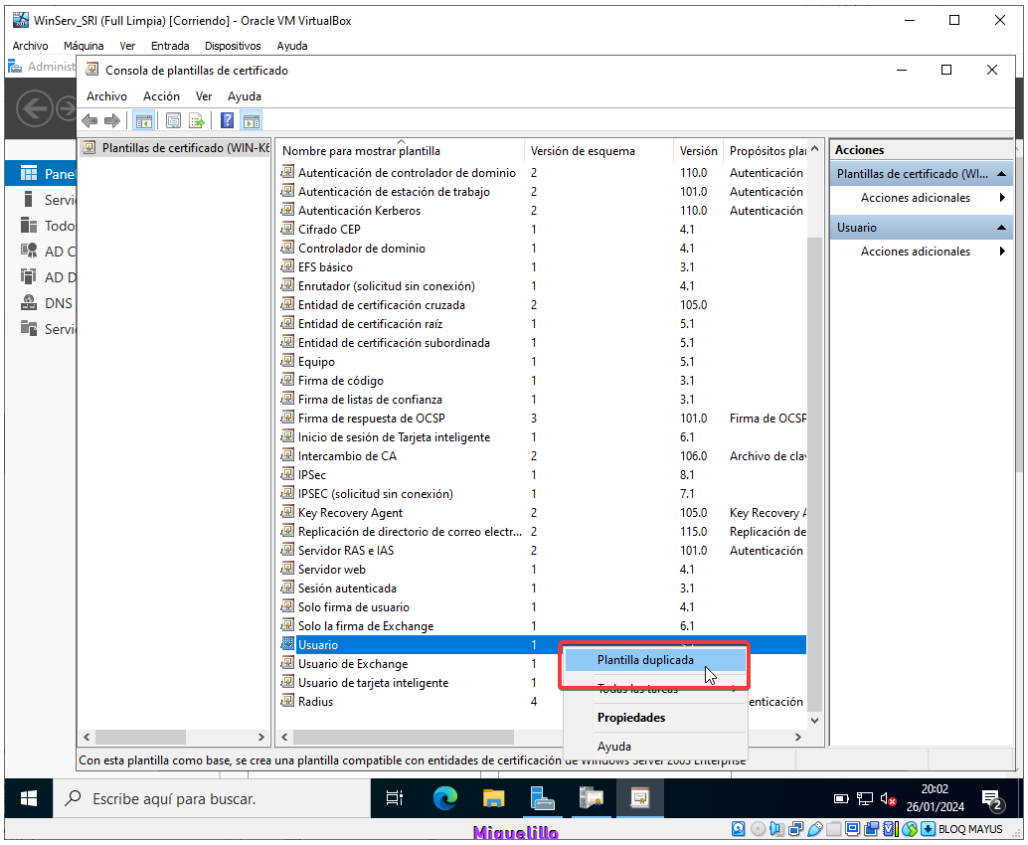
Vamos a **General** y le ponemos un **Nombre**



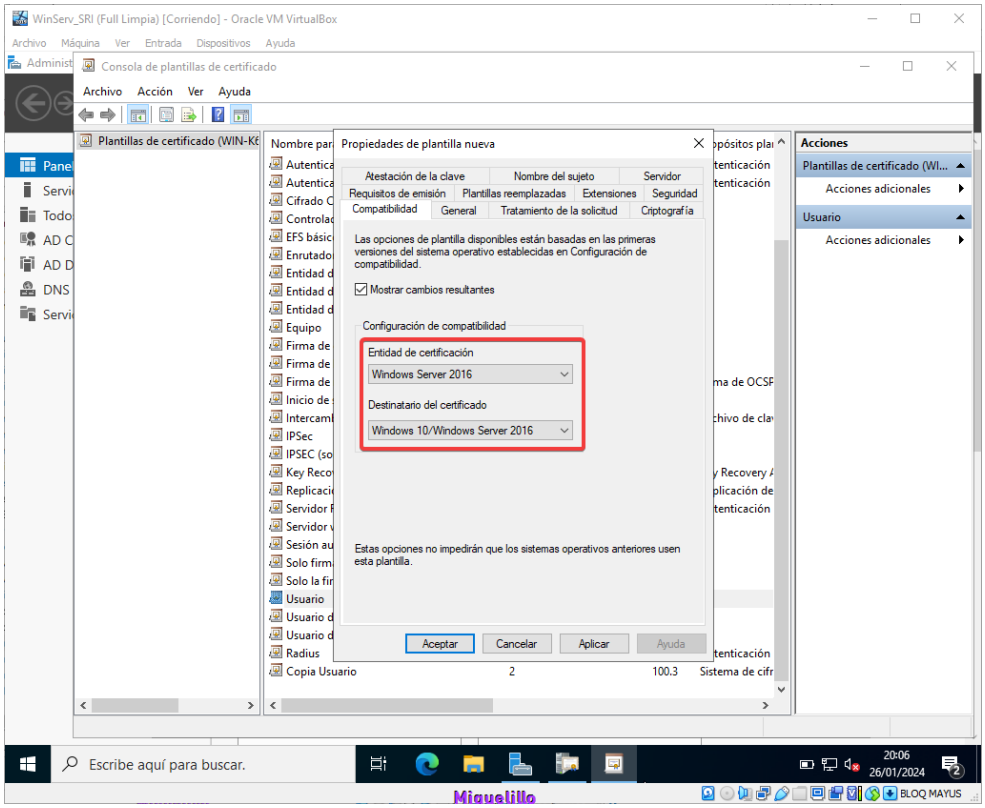
Vamos a **Seguridad** y le damos permisos a **Equipos del dominio**



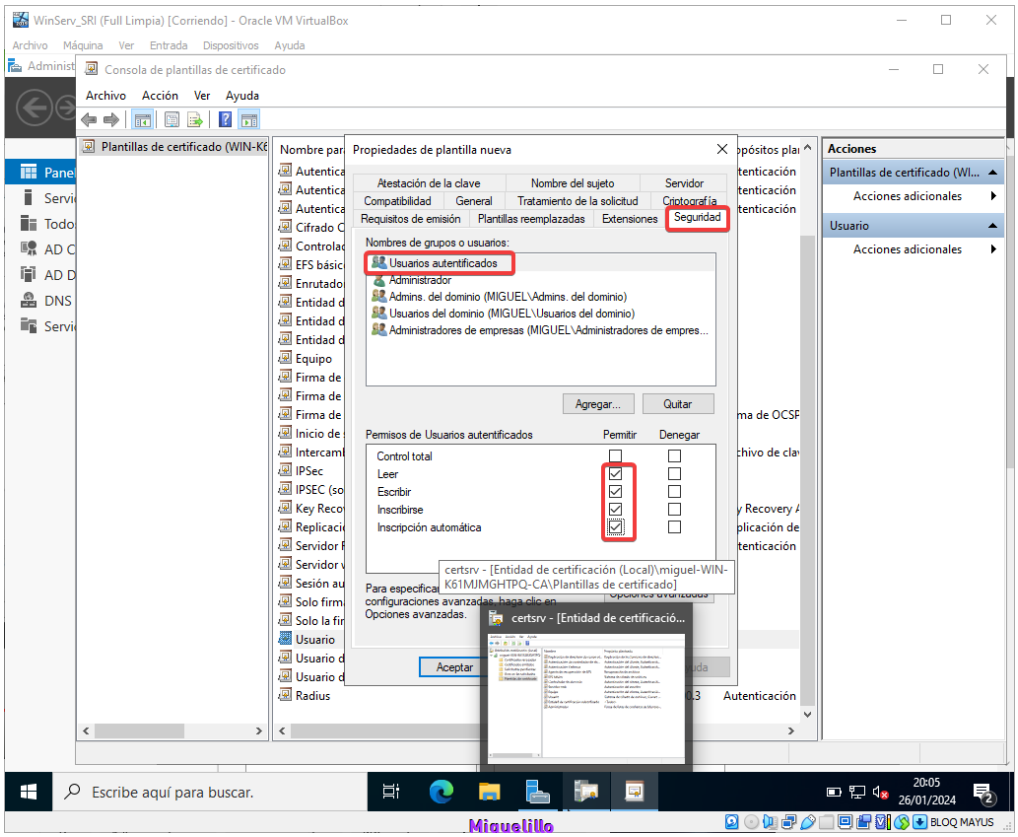
Duplicamos la plantilla de **Usuario**



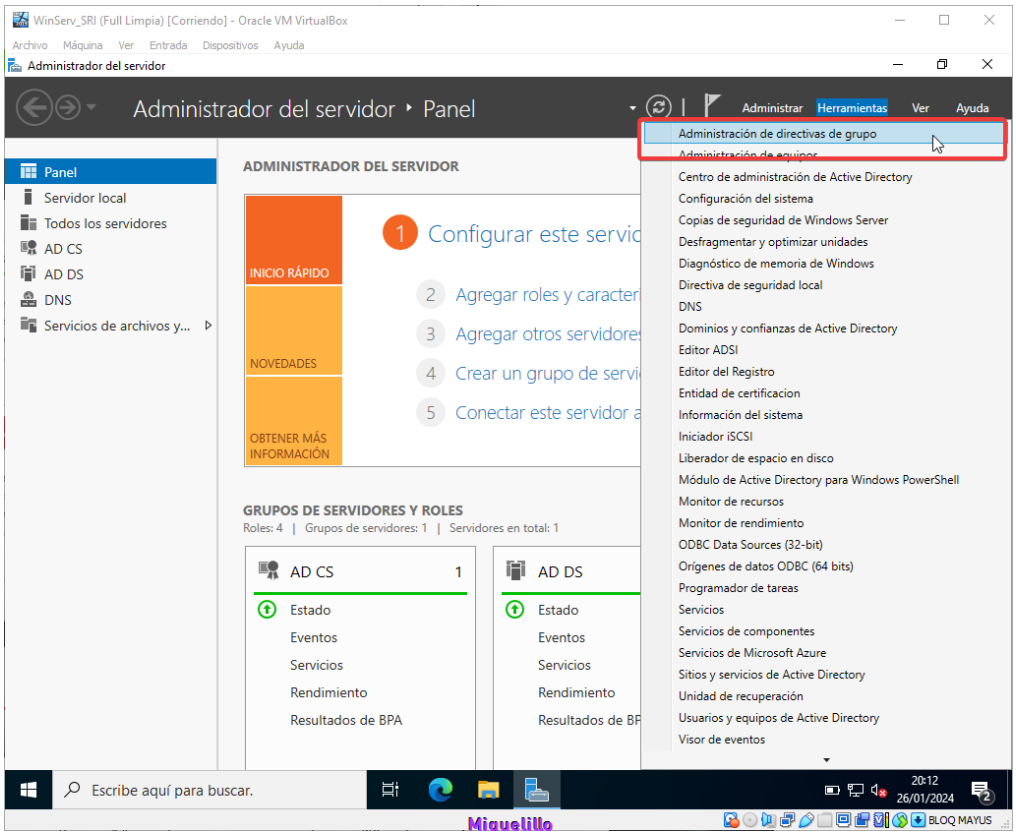
Seleccionamos **Windows Server 2016** como el anterior



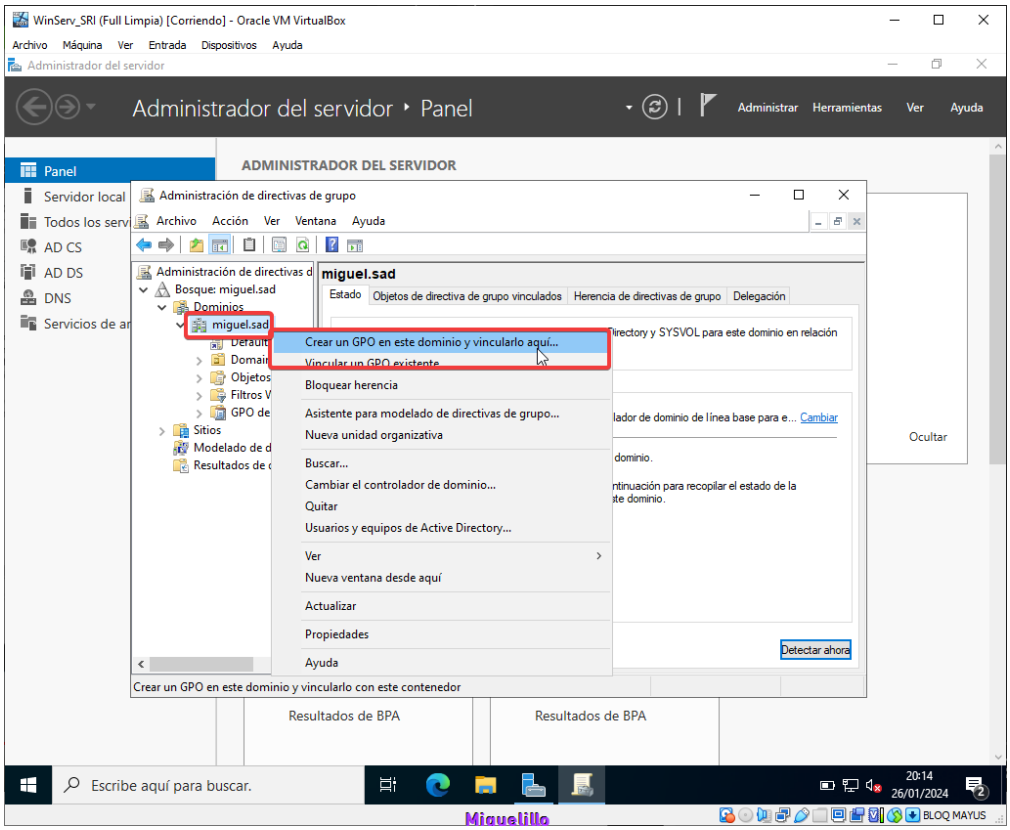
Vamos a **Seguridad** y damos permisos a **Usuarios autentificados**.



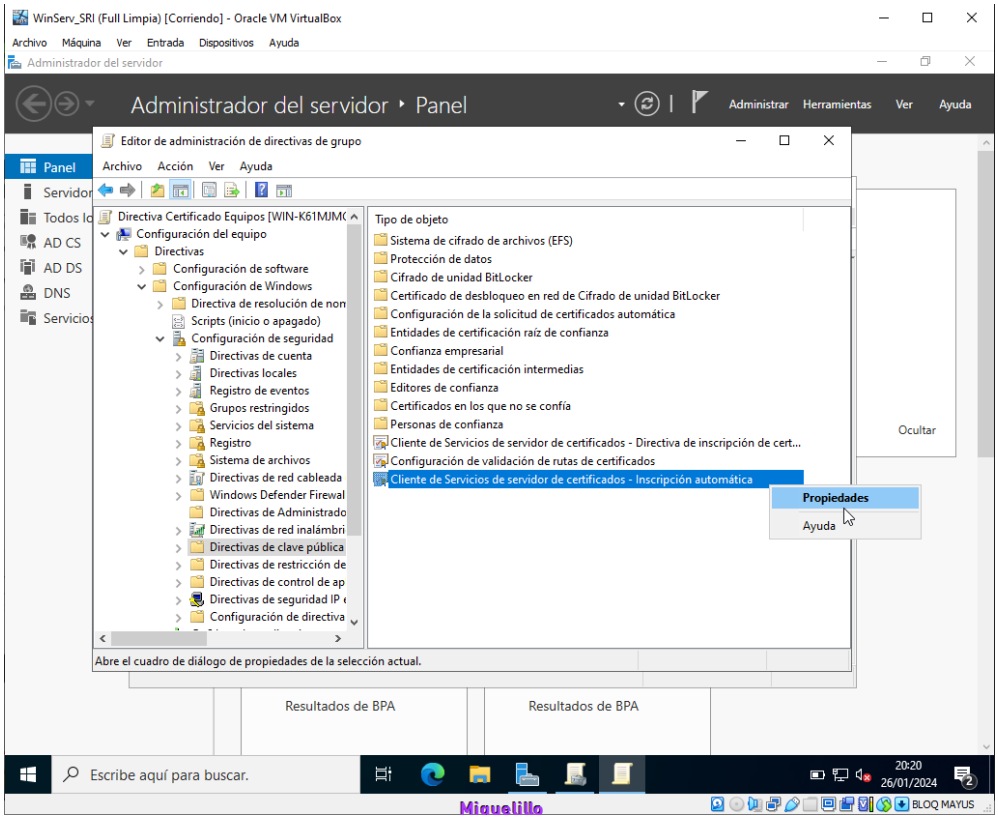
Vamos a **Herramientas → Administrar directivas de grupos**



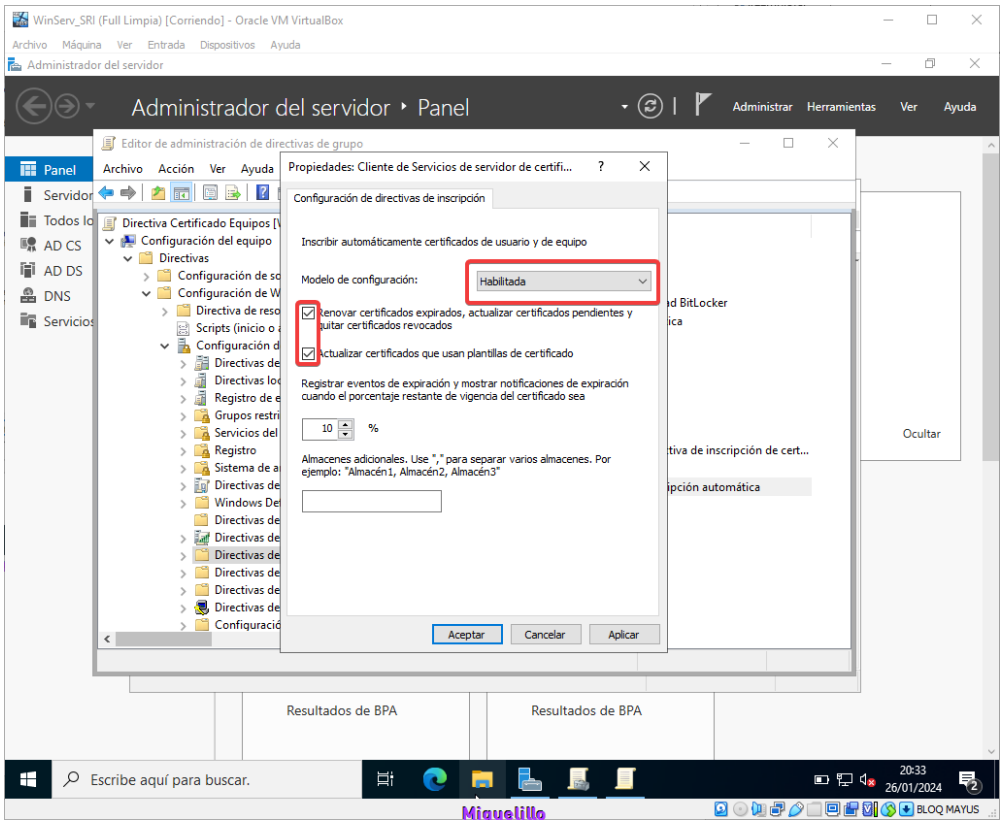
Creamos una **GPO** y le ponemos un nombre



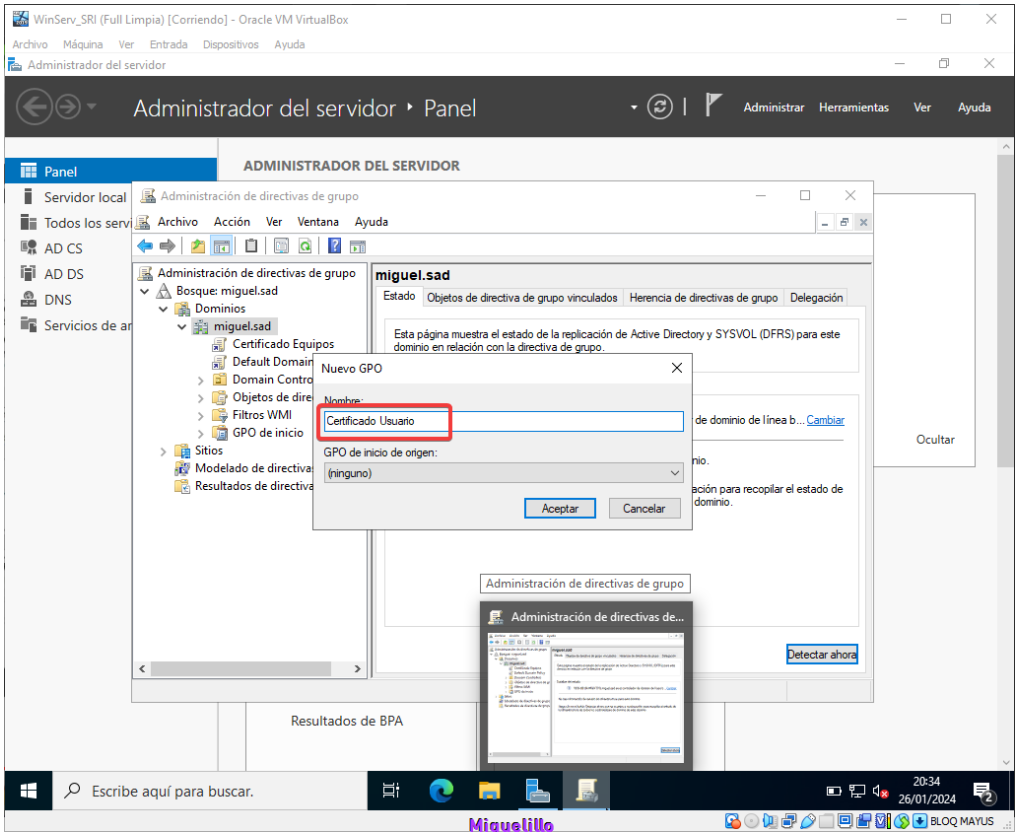
Editamos la GPO creada vemos las propiedades de Cliente de servicios de servidor de certificados



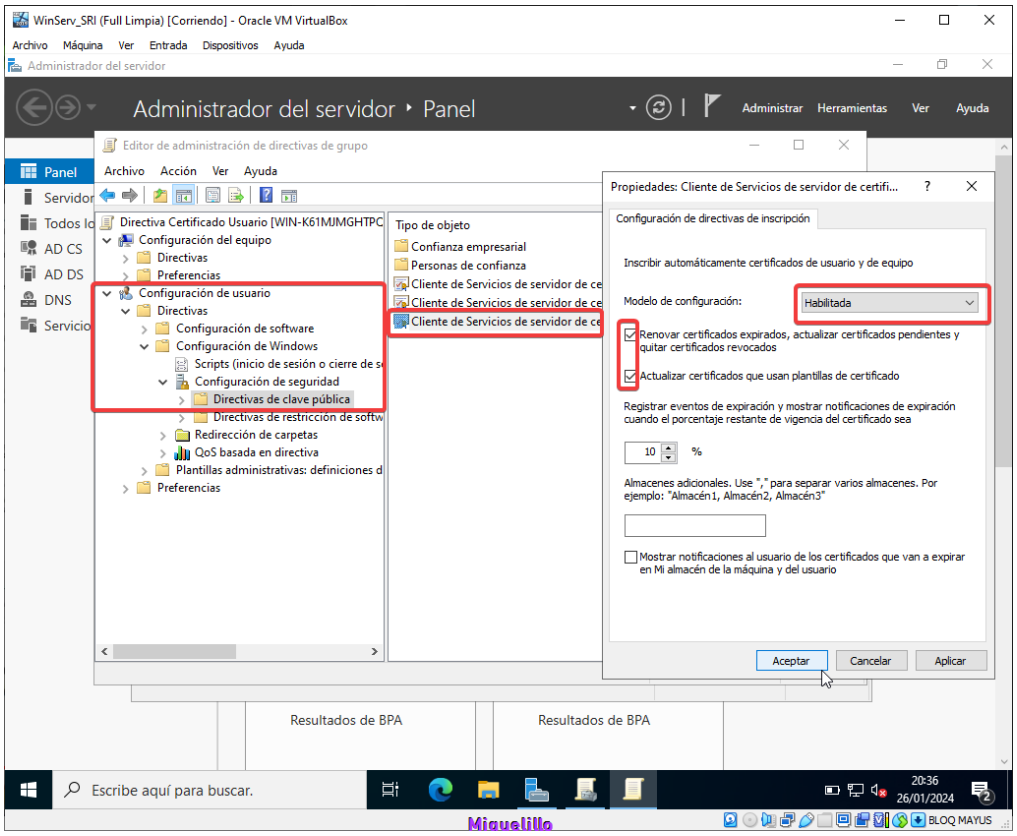
Habilitamos y marcamos los CheckBox



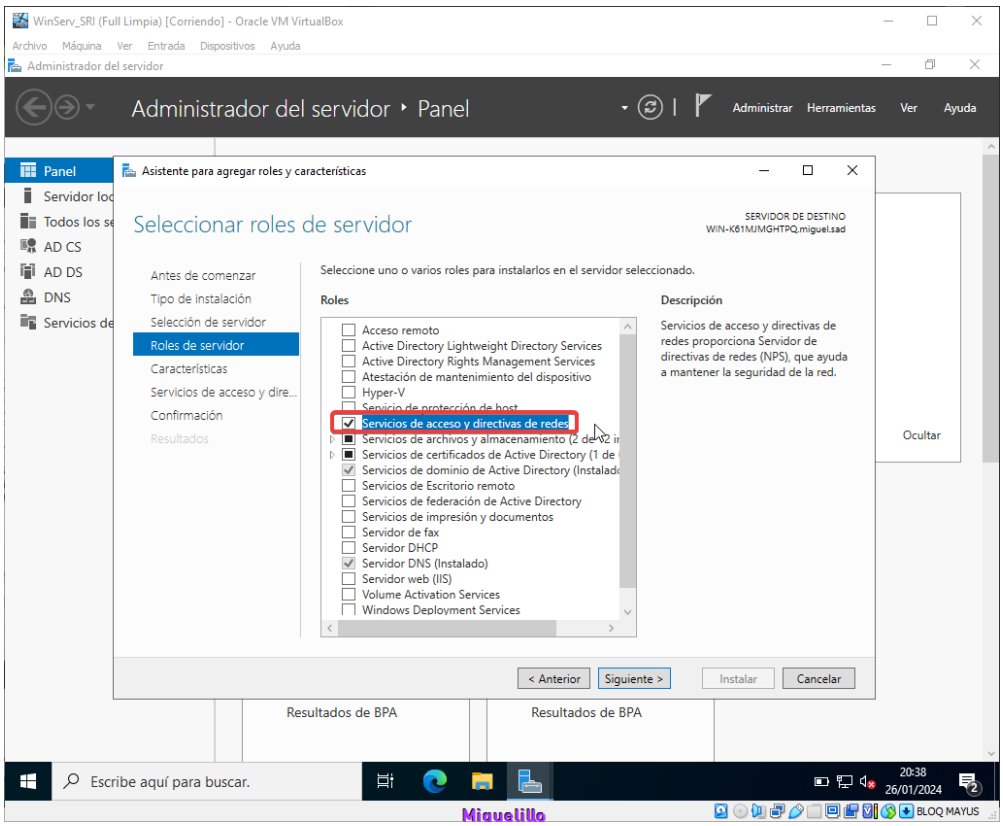
Creamos otra GPO para usuarios



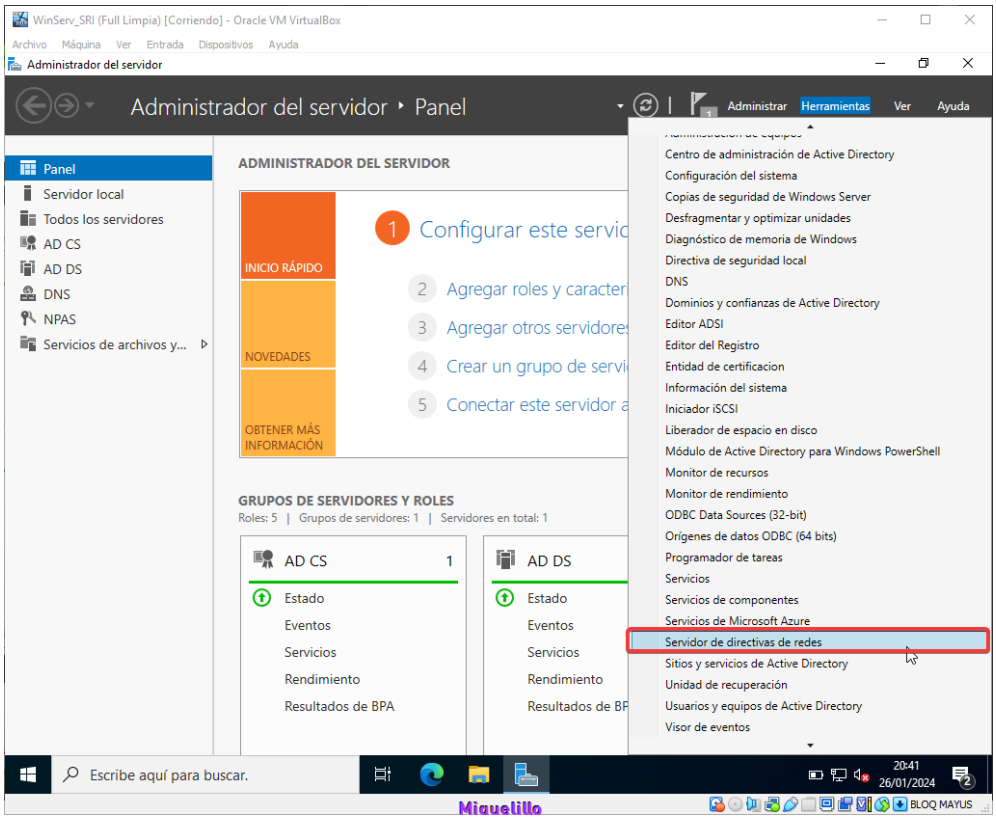
Repetimos como hemos hecho antes



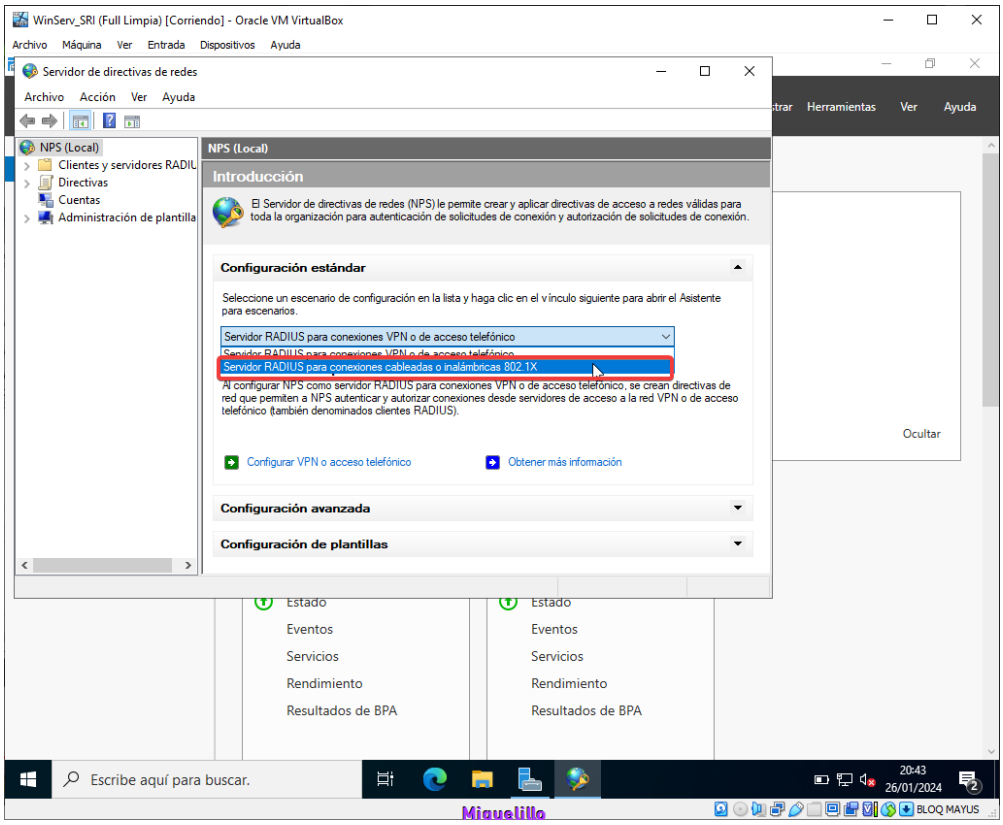
Agregamos un rol el de **Servicios de acceso y directivas de redes**



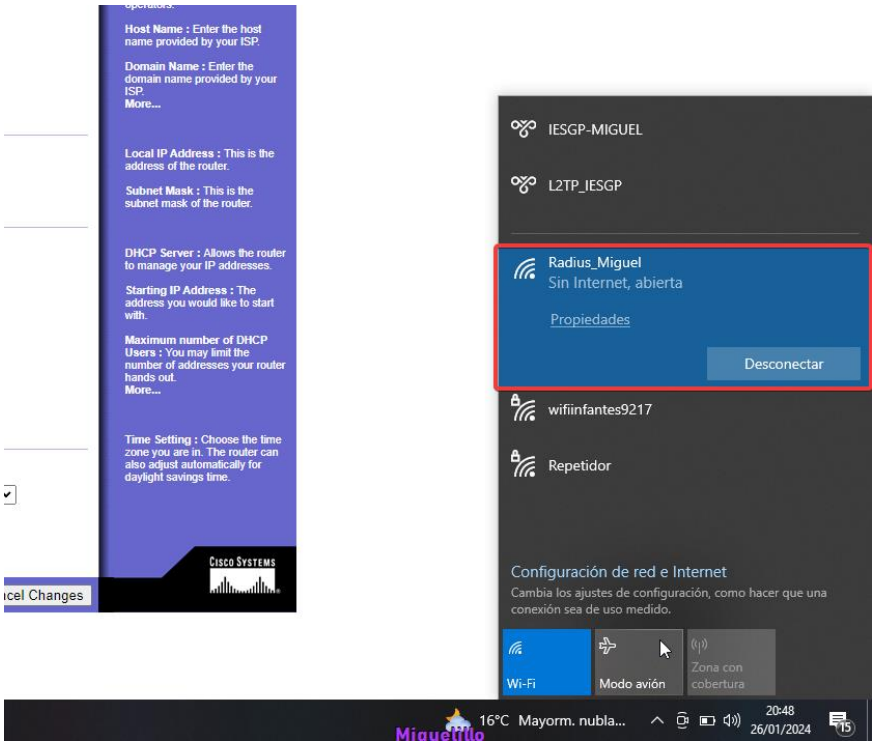
Vamos a **Herramientas→ Servidor de directivas de redes**



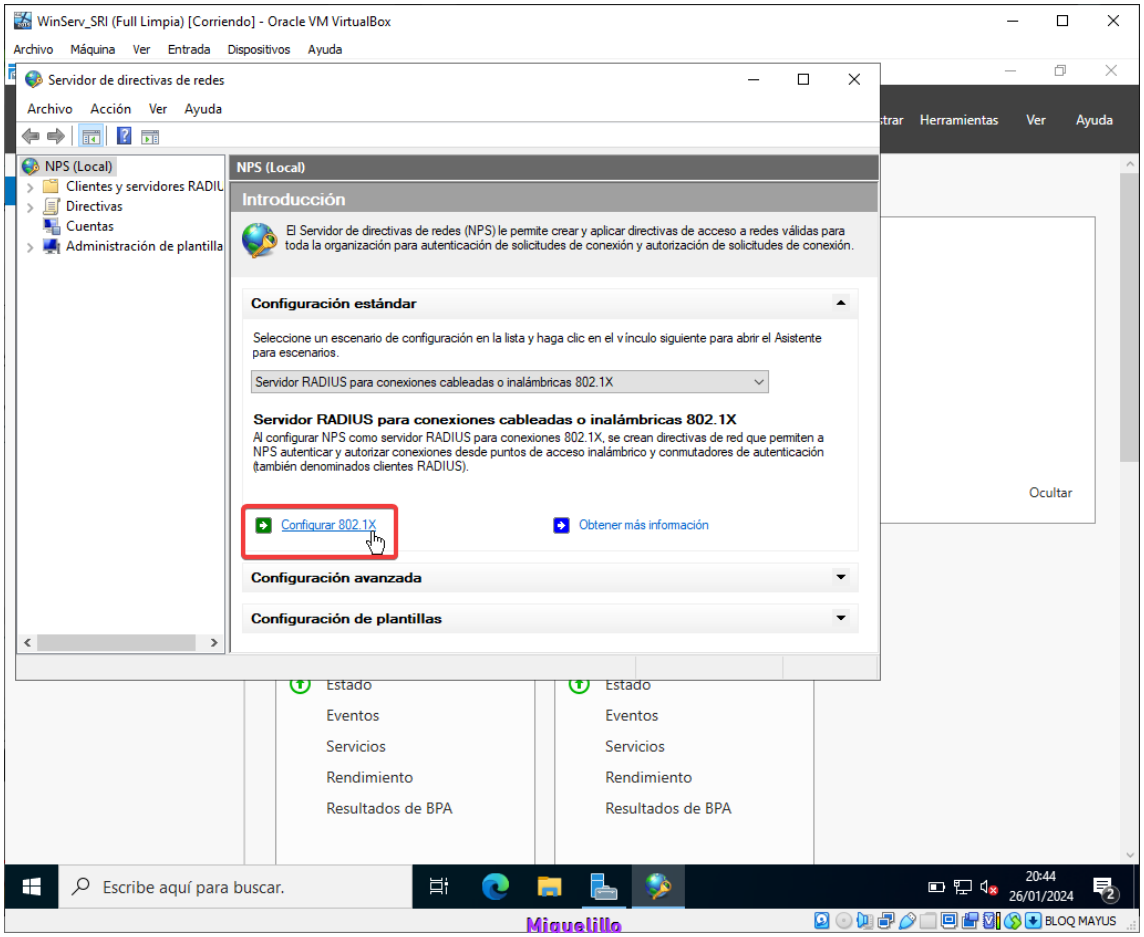
Seleccionamos **Servidor radius para conexiones cableadas o inalámbricas 802.1x**



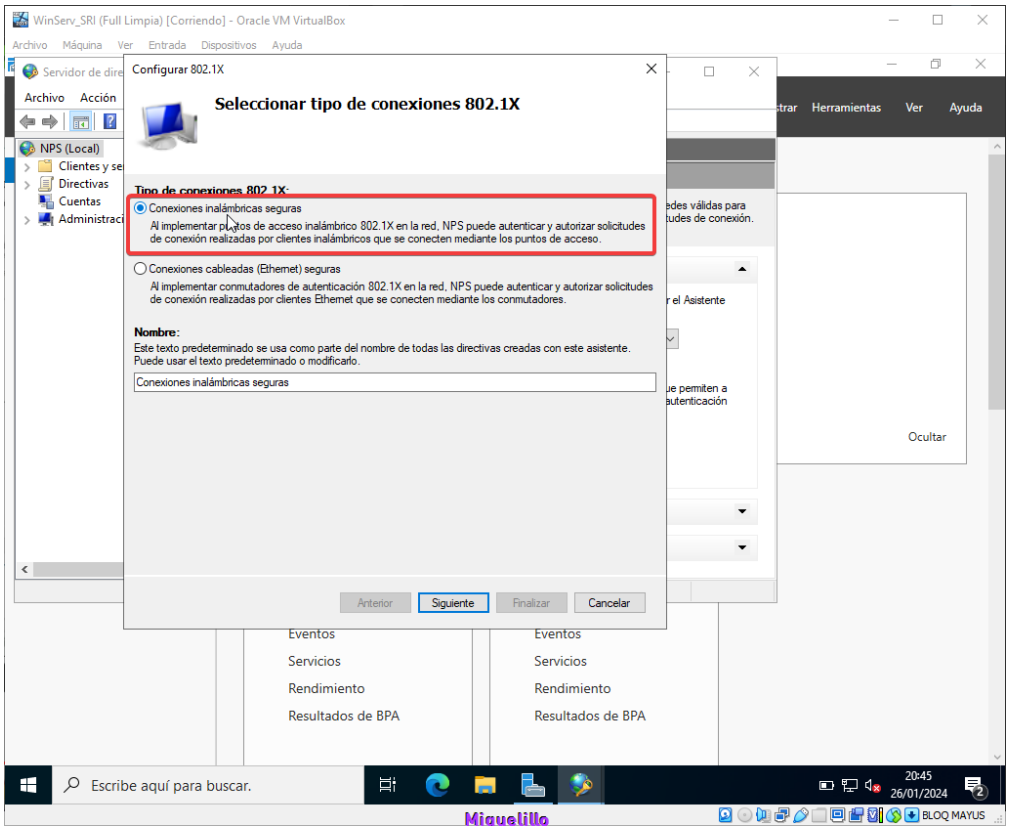
Nos conectamos al router del radius



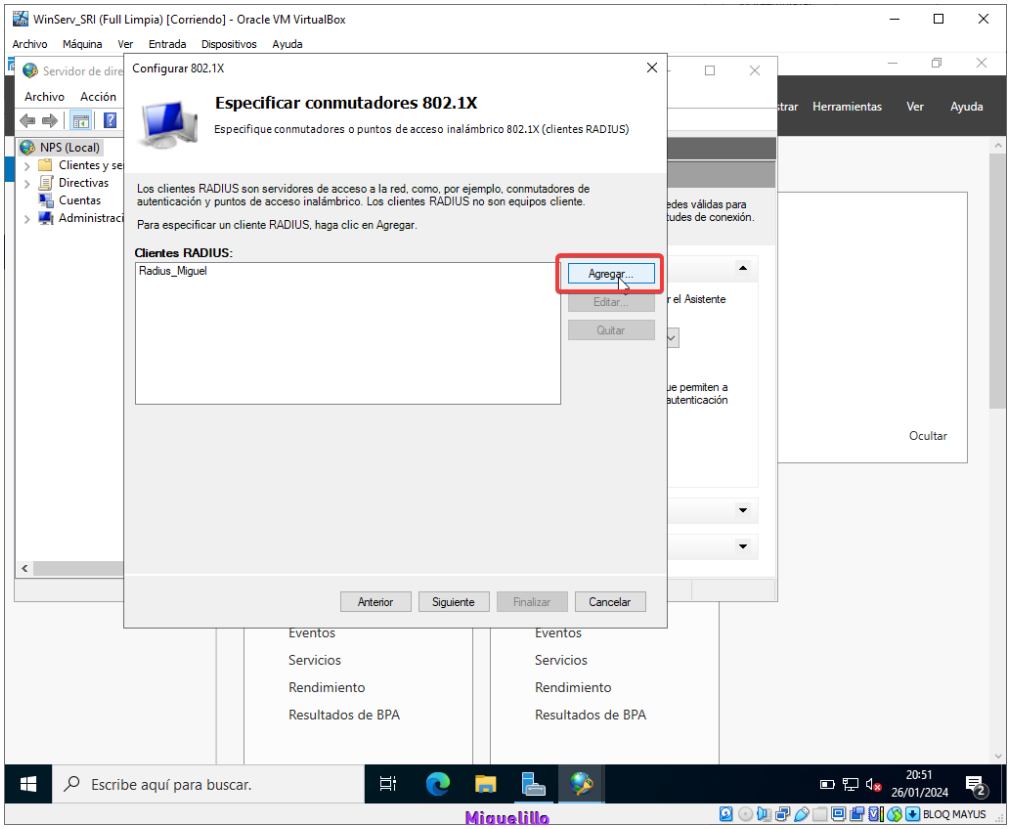
Clicamos en **Configurar 802.1x**



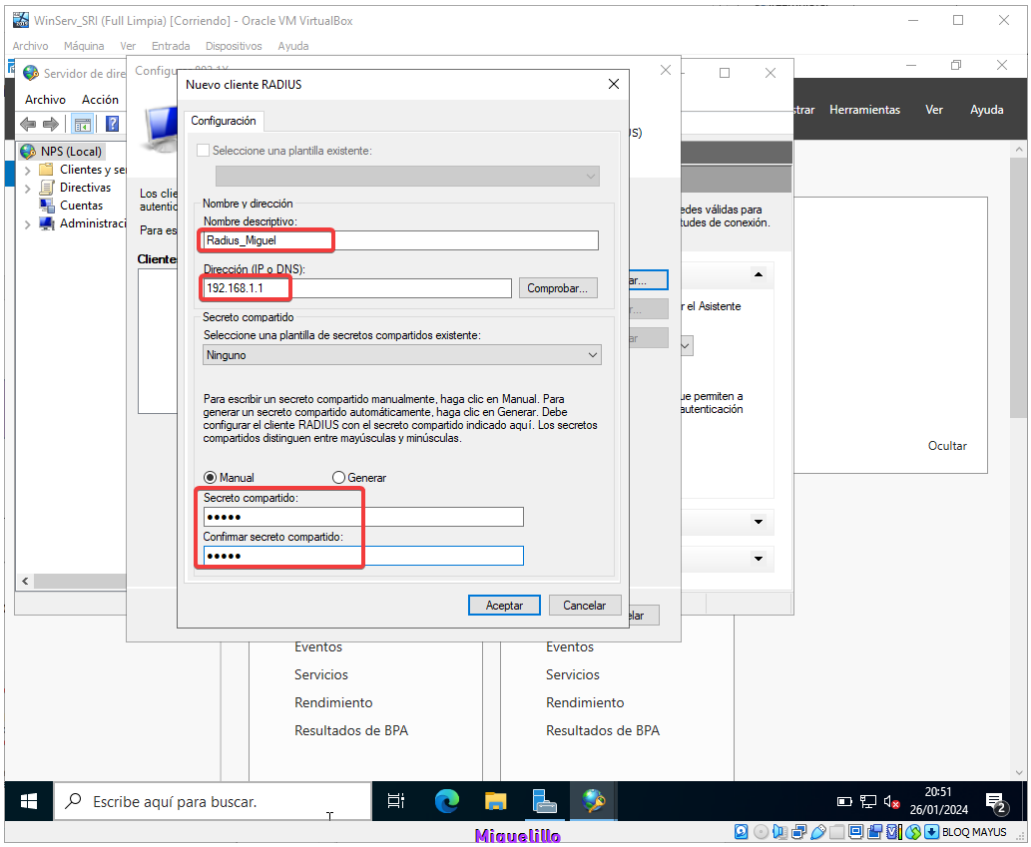
Clicamos en **Conexiones inalámbricas seguras**



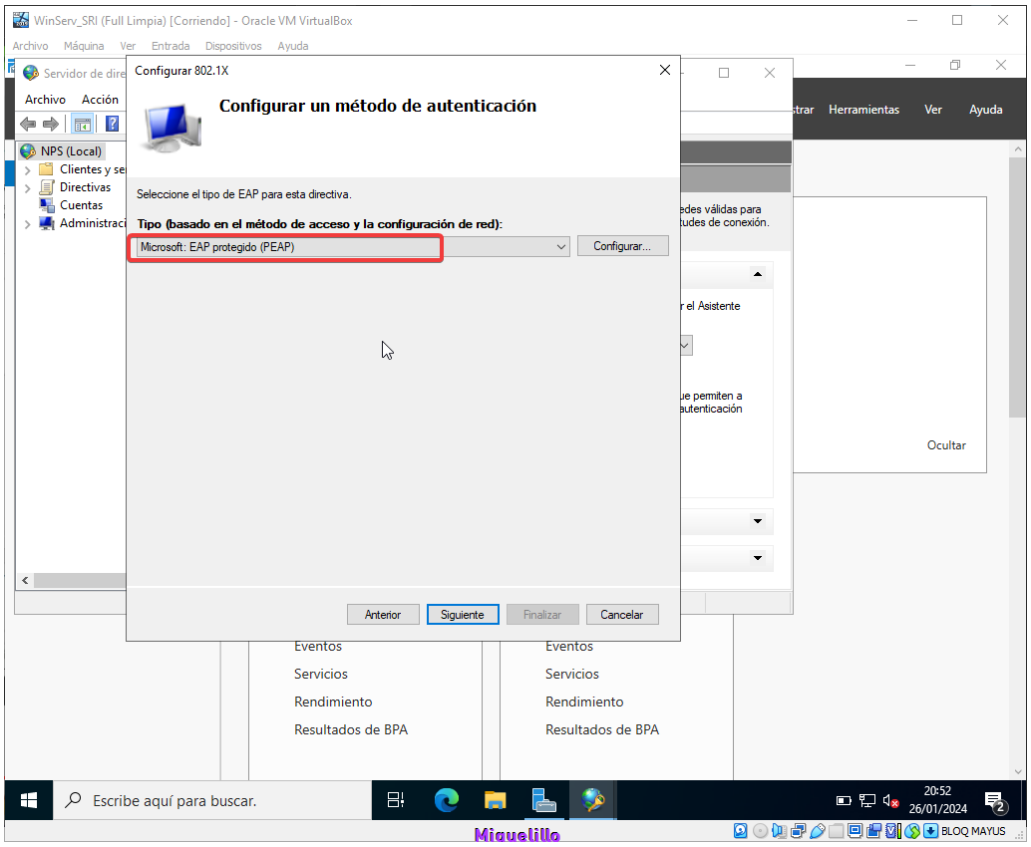
Clicamos en **Agregar…**



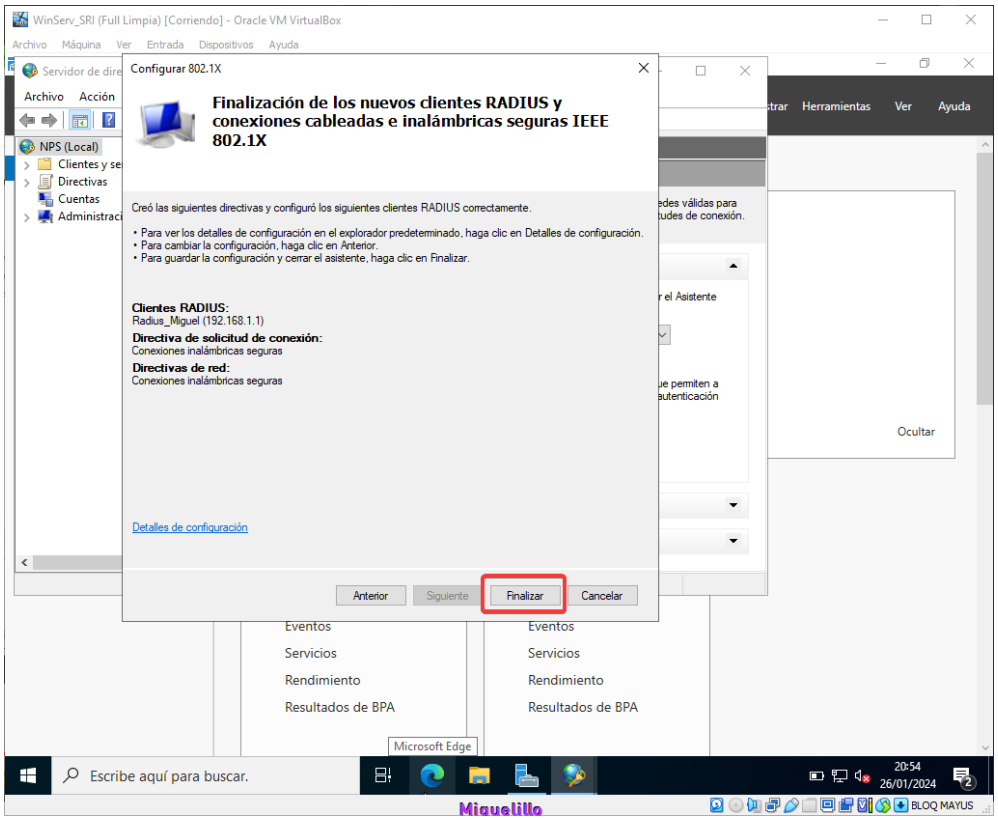
Configuramos los parámetros el **nombre** la **IP** y la **clave precompartida**



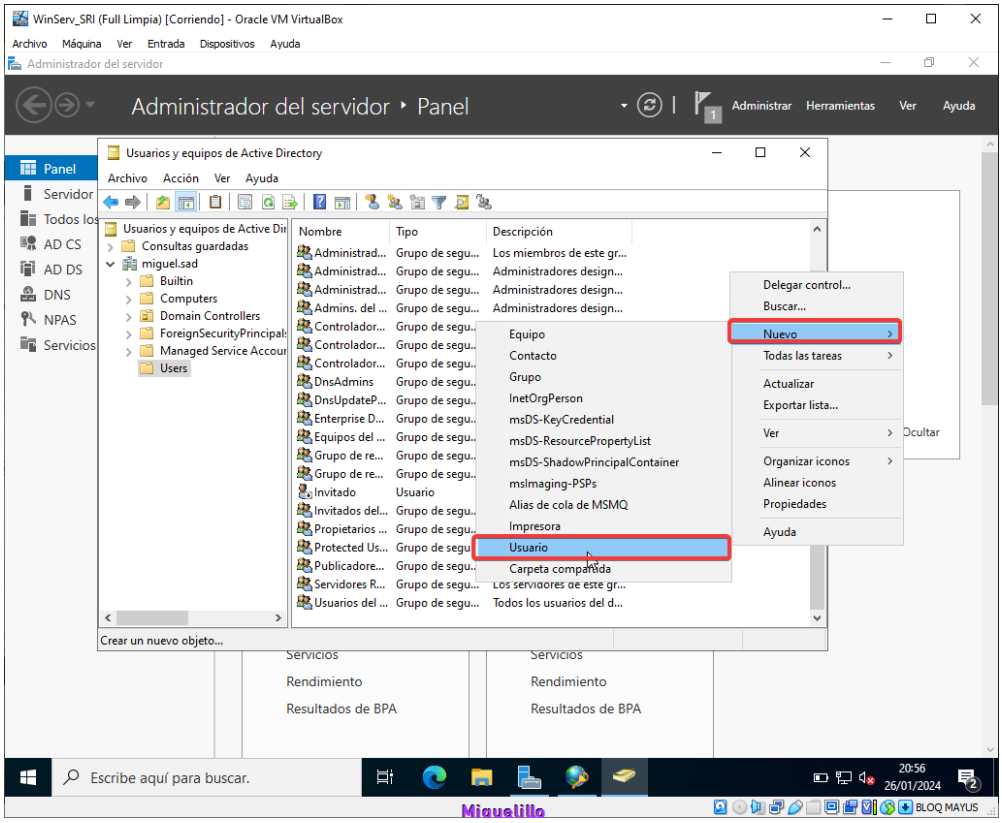
Seleccionamos el método de acceso



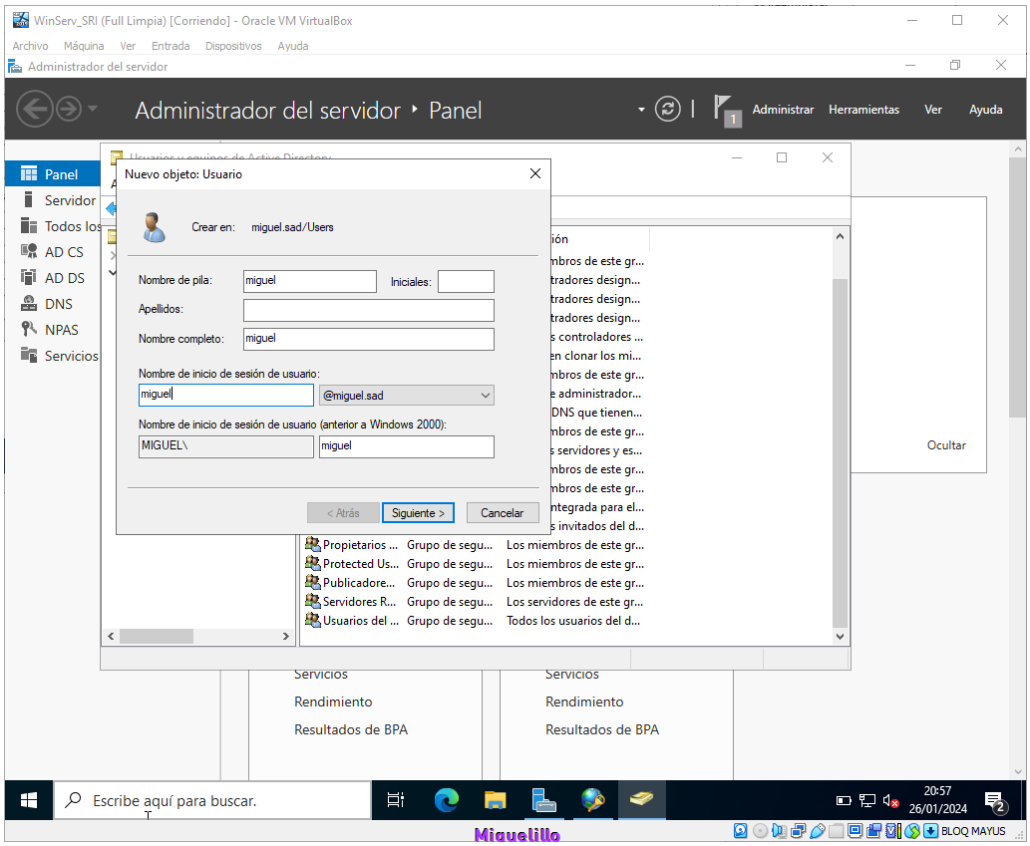
Clicamos en **Finalizar**



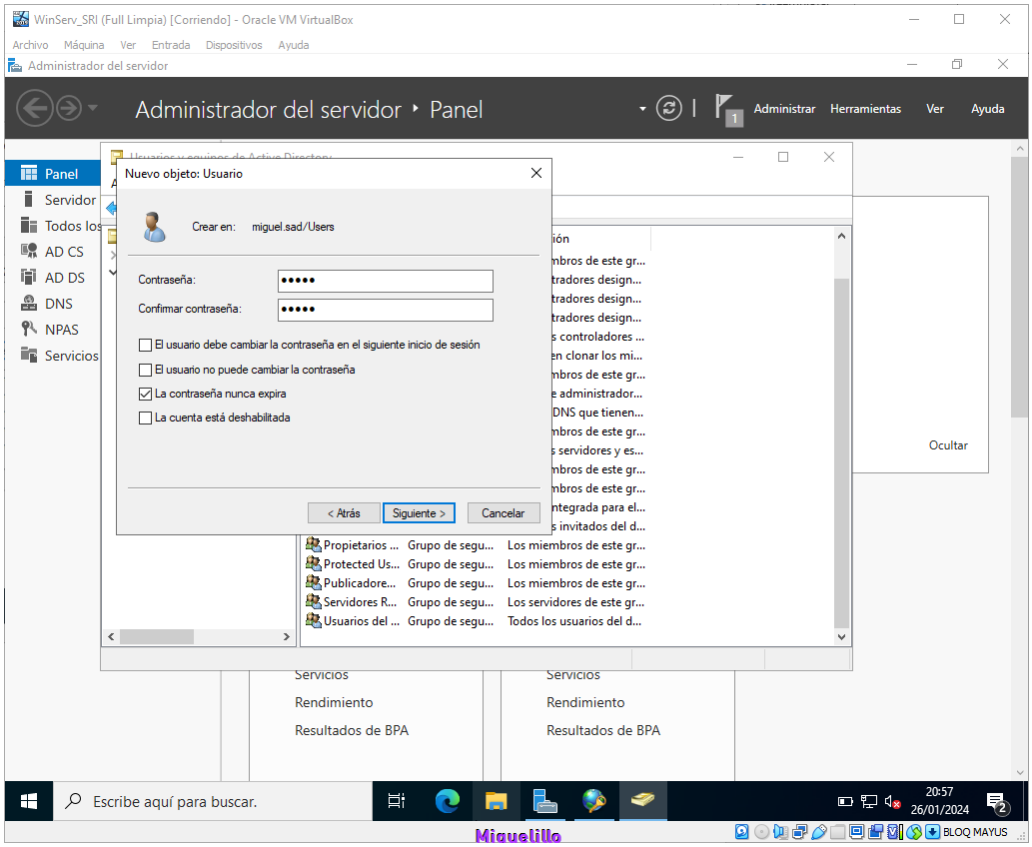
Vamos a **Usuarios y equipos de Active Directory** y creamos un usuario para autenticarnos en el radius



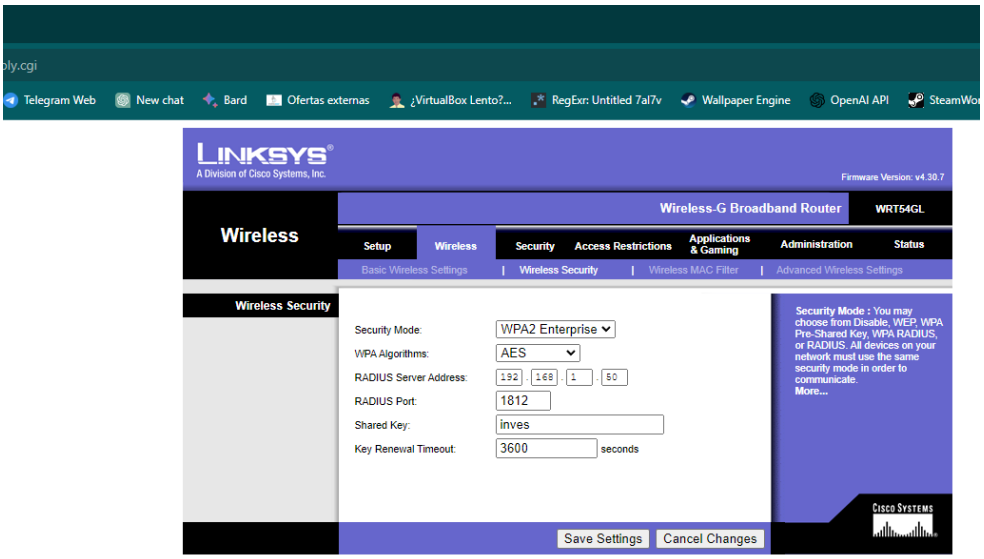
Introducimos el nombre



La contraseña



Ahora vamos al Router →**Wireless** → **Wireless Security** y lo configuramos seleccionando **WPA2 Enterprise, Algoritmo de autenticación AES** introduciendo la **IP** del servidor, el **puerto** para el Radius y la **clave precompartida**.



Miguelillo

Probamos a acceder desde un teléfono