
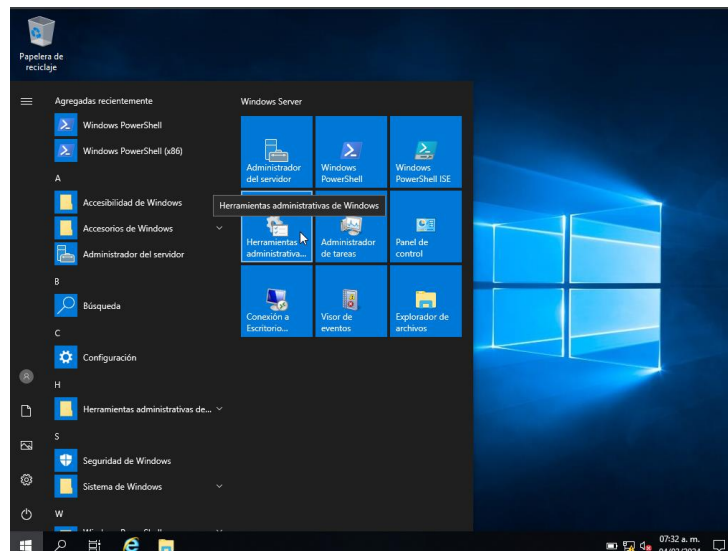
 GOBIERNO DEL ESTADO DE MÉXICO	<h1 style="text-align: center;">MANUAL DE PRÁCTICAS</h1> <p style="text-align: center;">FO-TESJI-11100-12</p>		 TECNOLÓGICO DE ESTUDIOS SUPERIORES JILOTEPEC
NOMBRE DE LA PRÁCTICA:	Equipos específicos para usuarios específicos		No. 1
ASIGNATURA:	Fundamentos de telecomunicaciones	CARRERA: ISIC	Unidad: III
ALUMNOS:	<ul style="list-style-type: none"> Ana Edith Hernández Hernández Vanesa Hernández Martínez Jesús Navarrete Martínez 		

1- Competencias Específicas:

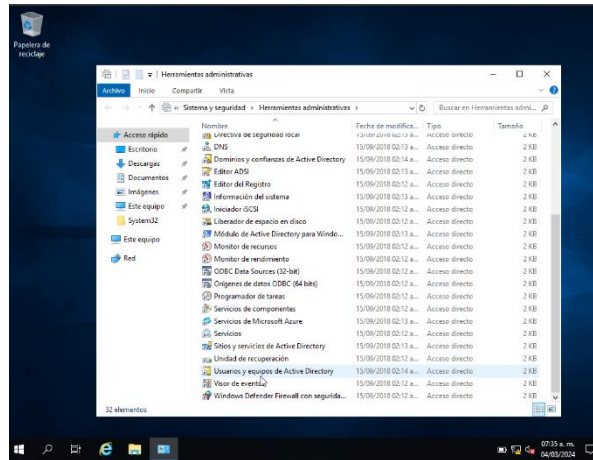
2- Desarrollo con: Laptops y cable ethernet

3- Desarrollo de la Practica:

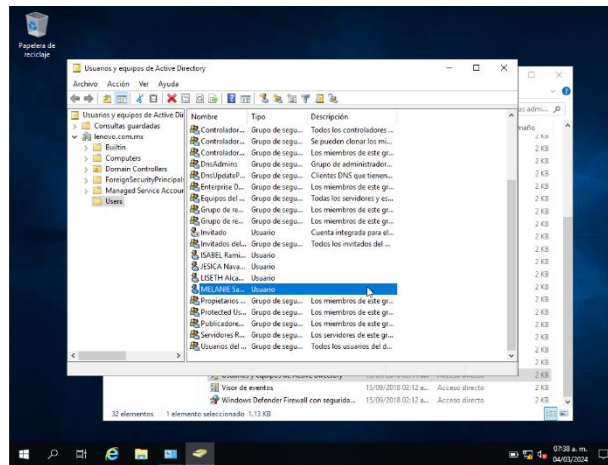
1. Iniciamos sesión en la máquina virtual donde tenemos instalado Windows 2019 Server, es decir en donde creamos nuestro dominio.
2. Entramos a las herramientas administrativas de Windows.



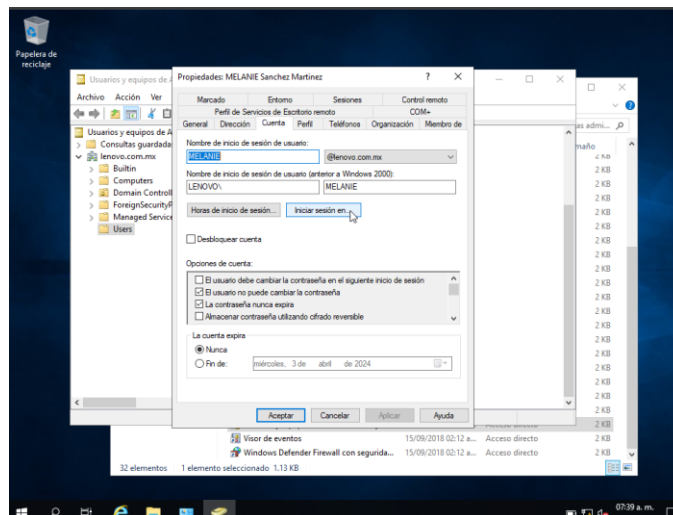
3. Entramos a los usuarios y equipos de Active Directory.



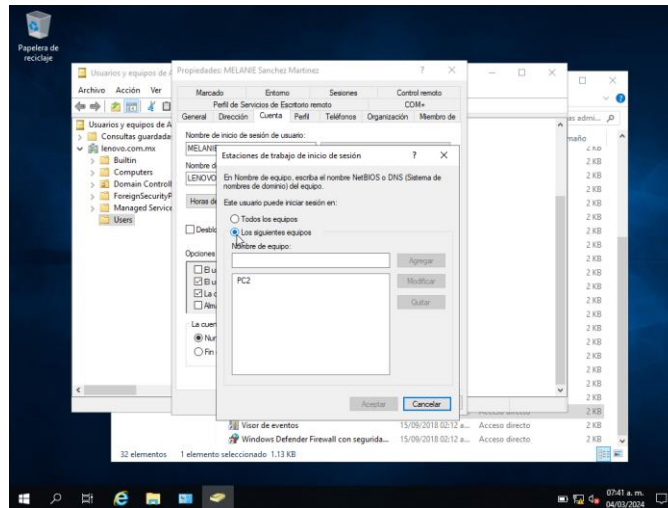
4. Seleccionamos el usuario al cual le vamos a asignar un equipo en específico para trabajar.



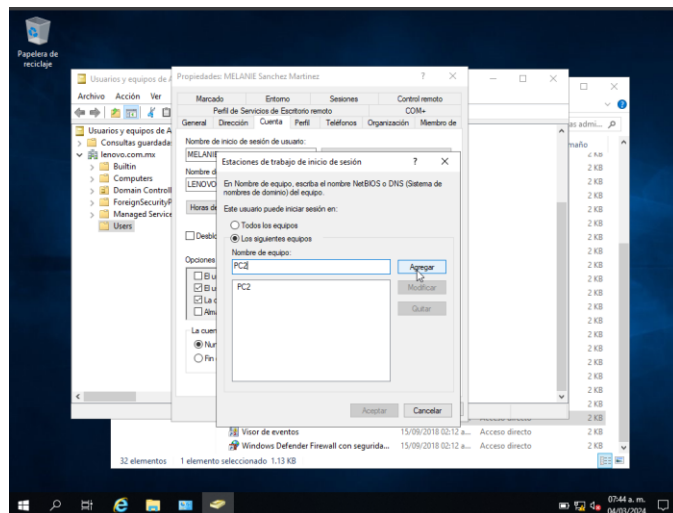
5. Entramos a la pestaña de cuenta y seleccionamos la opción de “iniciar sesión en”



6. En la sección de “el usuario puede iniciar sesión en”, seleccionamos la opción de “los siguientes equipos”.

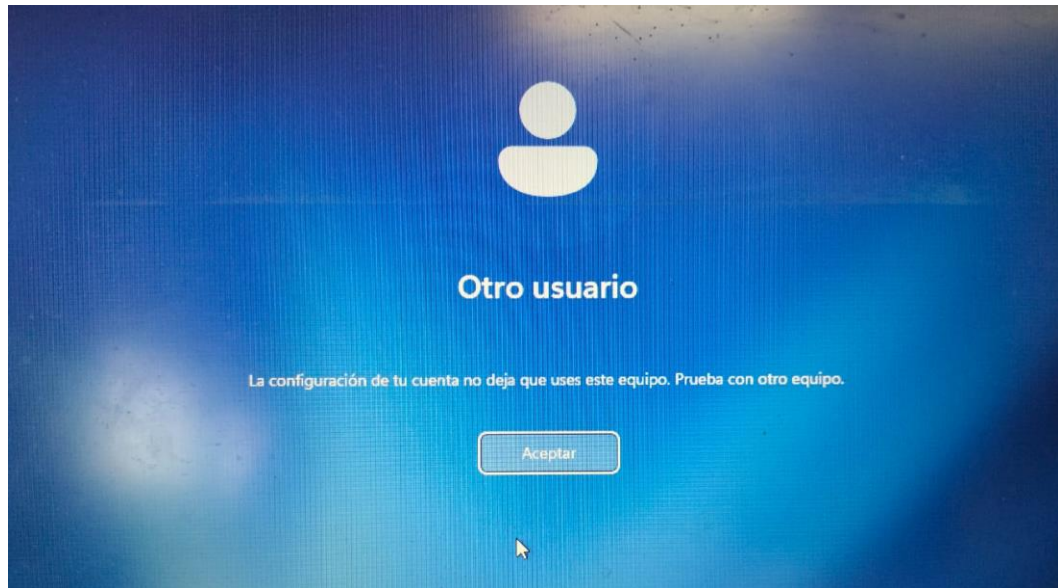


7. Escribimos el nombre del equipo en el cual va a tener acceso único para desarrollar sus actividades dicho usuario.



8. Damos clic en agregar, aplicar y aceptar para guardar los cambios realizados.

Nota: Si un usuario quiere ingresar en un equipo que no se le fue asignado, aparecerá el siguiente mensaje:



Conclusiones:

La asignación de equipos de trabajo específicos a cada cliente utilizando un dominio proporciona una solución eficiente y segura para la gestión de recursos en entornos de red. Al implementar esta práctica, no solo garantizamos la optimización de los recursos disponibles, sino también fortalecemos la seguridad al evitar el acceso no autorizado a máquinas asignadas. El mensaje de error generado cuando un usuario intenta iniciar sesión en una máquina no asignada sirve como un mecanismo de protección adicional, reforzando la integridad del sistema y la confidencialidad de los datos. En resumen, esta estrategia contribuye significativamente a la organización y protección de la infraestructura, asegurando un entorno operativo eficiente y seguro para todos los usuarios.