Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

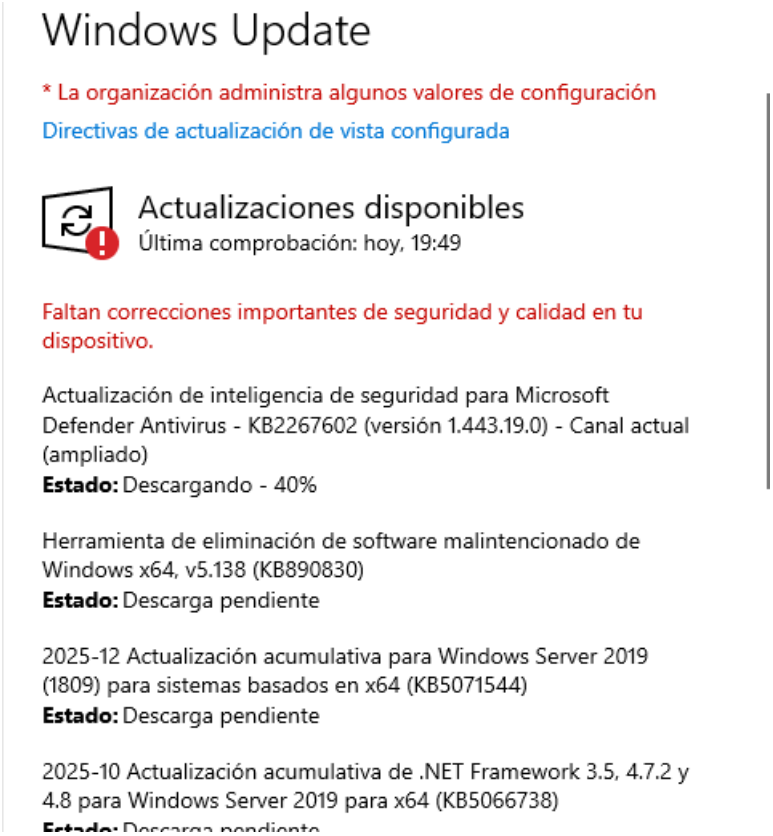
Bastionado active directory

Héctor Ramírez López.

Índice

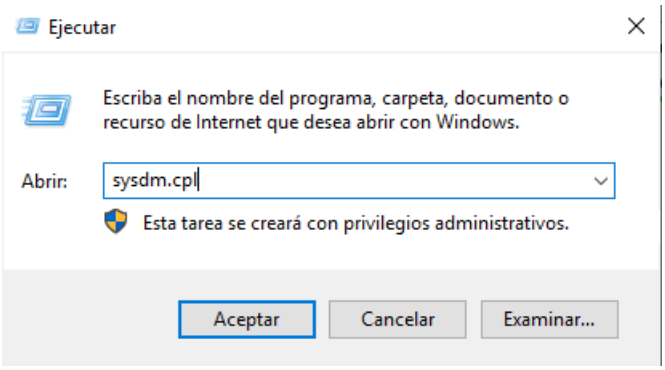
1.Introducción

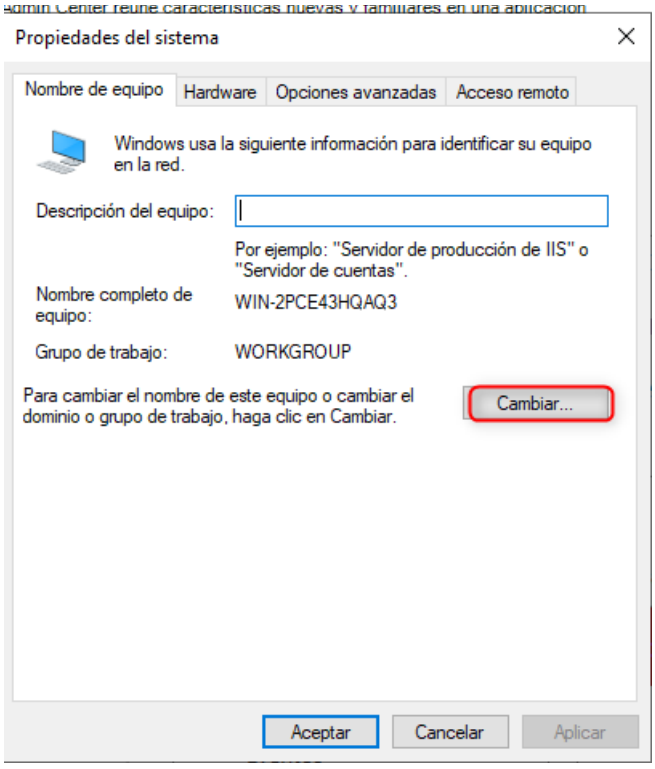
Antes de promover el servidor a Controlador de Dominio debemos de actualizar el equipo desde windows update para aplicar los últimos parches de seguridad.

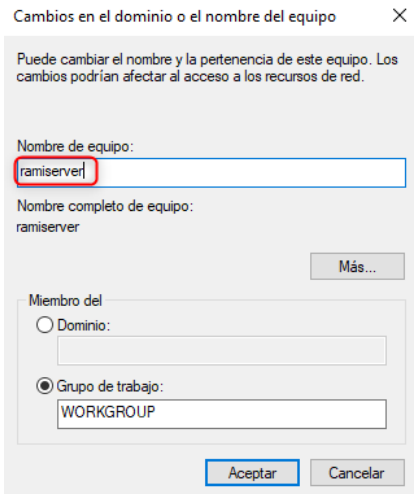


Lo siguiente sera cambiar el nombre del equipo y establecer un ip estática.

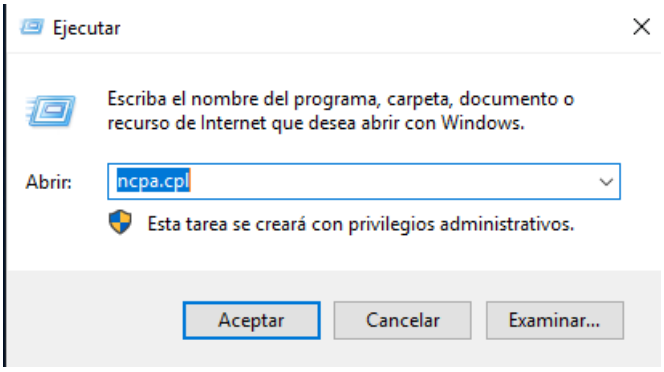
Para cambiar el nombre abriremos ejecutar y escribimos el siguiente comando, le damos a cambiar y ponemos el nombre que queramos.



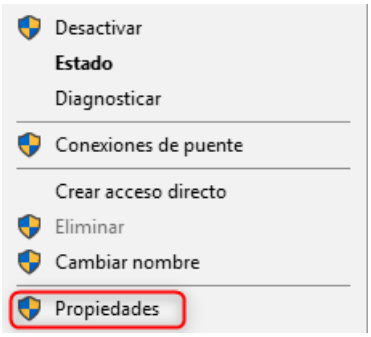




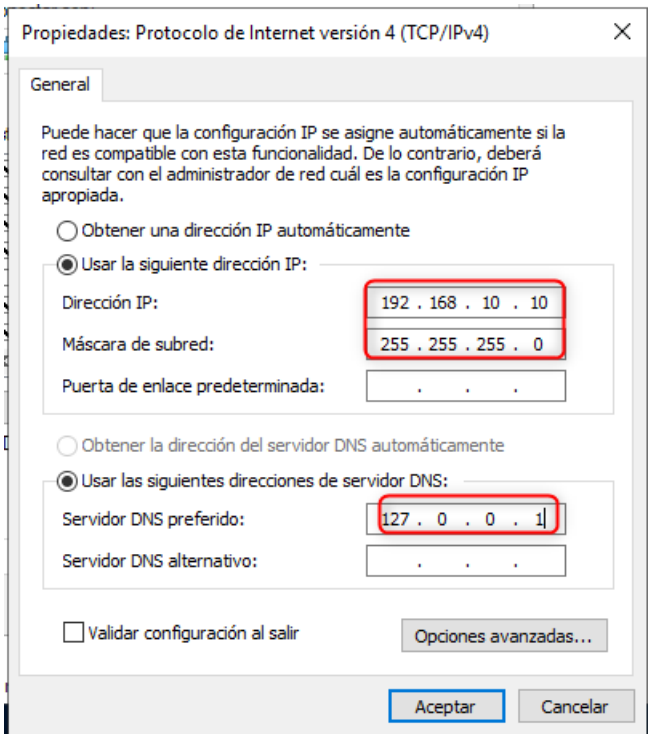
Para establecer una ip estática abrimos ejecutar y ponemos el siguiente comando.



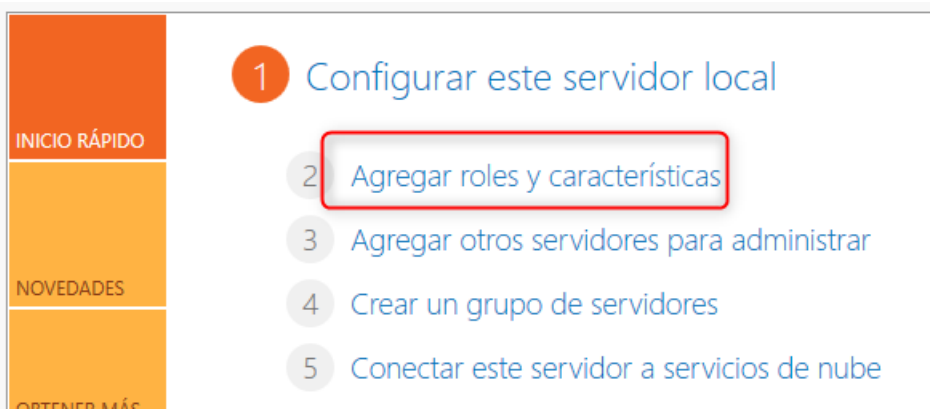
Le daremos clic derecho en el adaptador de red y nos iremos a propiedades.

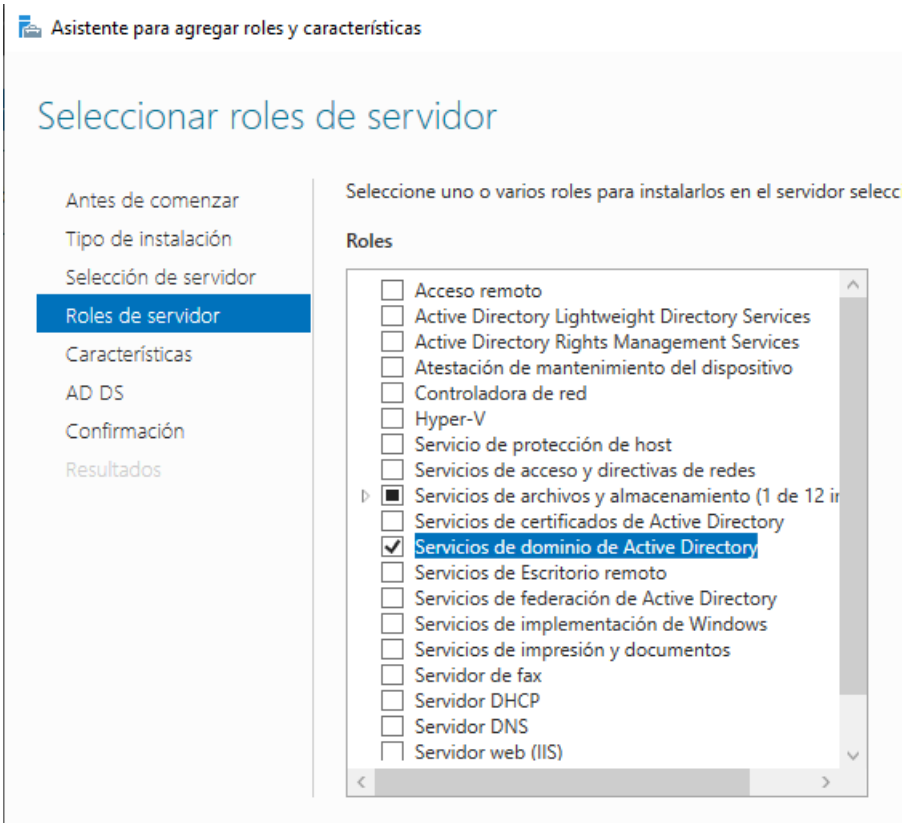


Pondremos la siguiente dirección ip mascara de red y dns.

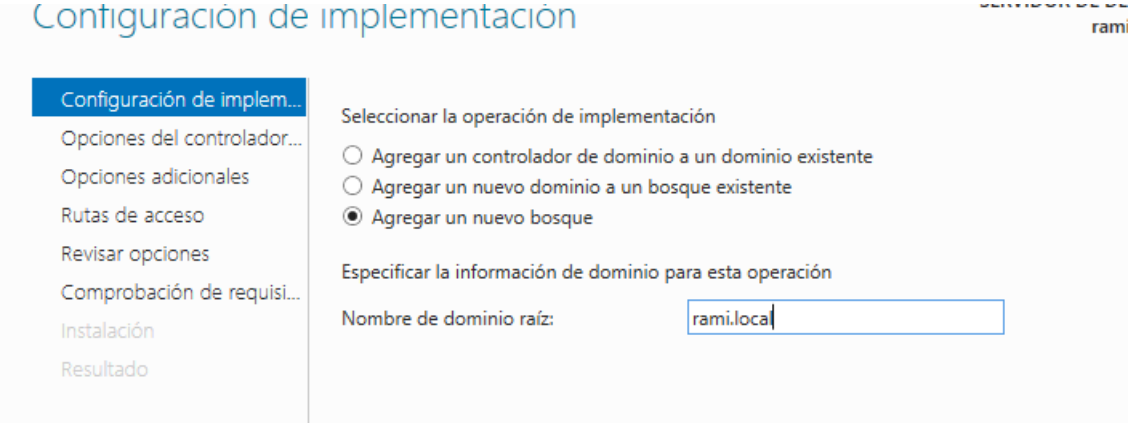


Ahora ya podremos promover el servidor a controlador de dominio abrimos el administrador del servidor y agregar roles y características, seleccionamos servicios de dominio y active directory.

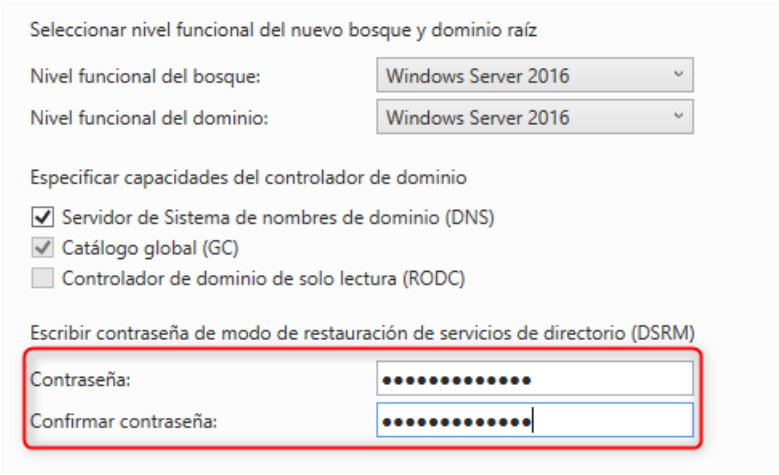



Asistente para agregar roles y características
Seleccionar roles de servidor
Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
AD DS
Confirmación
Resultados
Seleccione uno o varios roles para instalarlos en el servidor selecc
Roles
Acceso remoto
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Atestación de mantenimiento del dispositivo
Controladora de red
Hyper-V
Servicio de protección de host
Servicios de acceso y directivas de redes
Servicios de archivos y almacenamiento (1 de 12 i
Servicios de certificados de Active Directory
Servicios de dominio de Active Directory
Servicios de Escritorio remoto
Servicios de federación de Active Directory
Servicios de implementación de Windows
Servicios de impresión y documentos
Servidor de fax
Servidor DHCP
Servidor DNS
Servidor web (IIS)

Agregamos un nuevo bosque con el nombre que queramos para nuestro active directory.

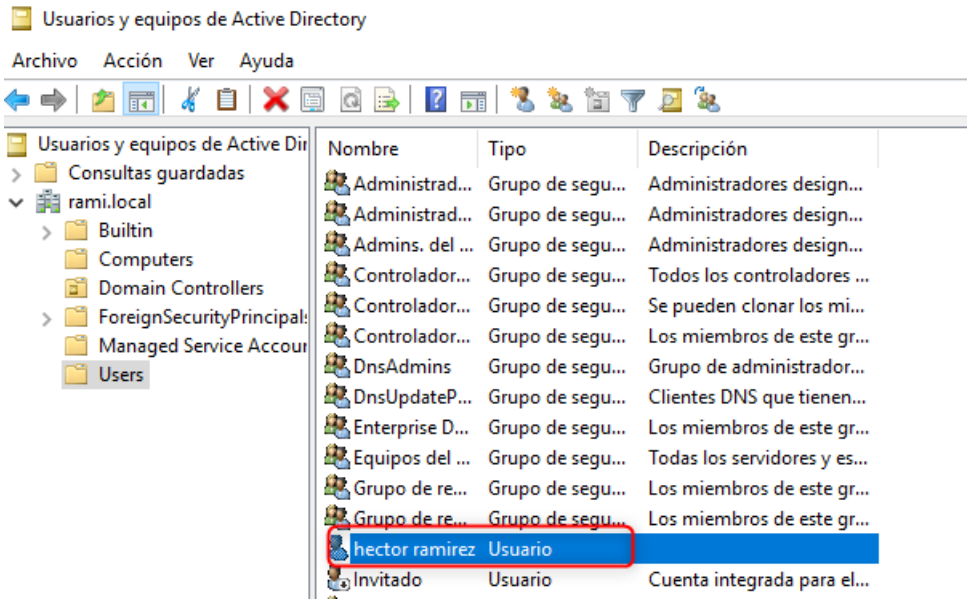


Nos pedira una contraseña para poder restaurar el directorio en caso de que haya problemas.

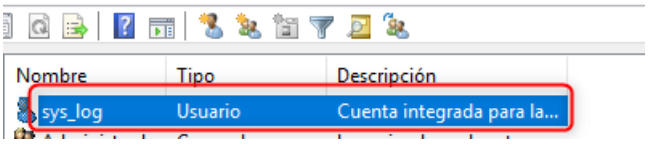


2. Bastionado de Identidades

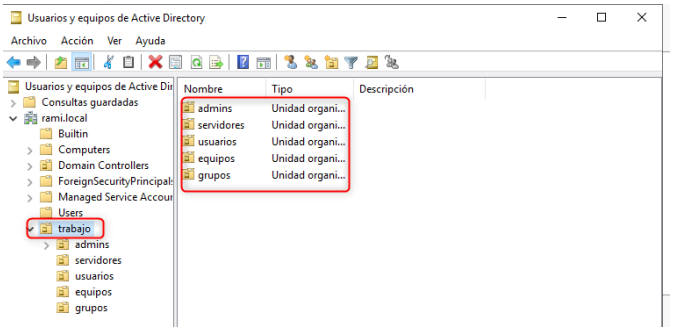
No se debería trabajar con el usuario admin por defecto, vamos a crear uno nuevo para ello abrimos usuario y equipo de active directory creamos el usuario en la ou users.



Renombraremos la cuenta de admin que venía por defecto.

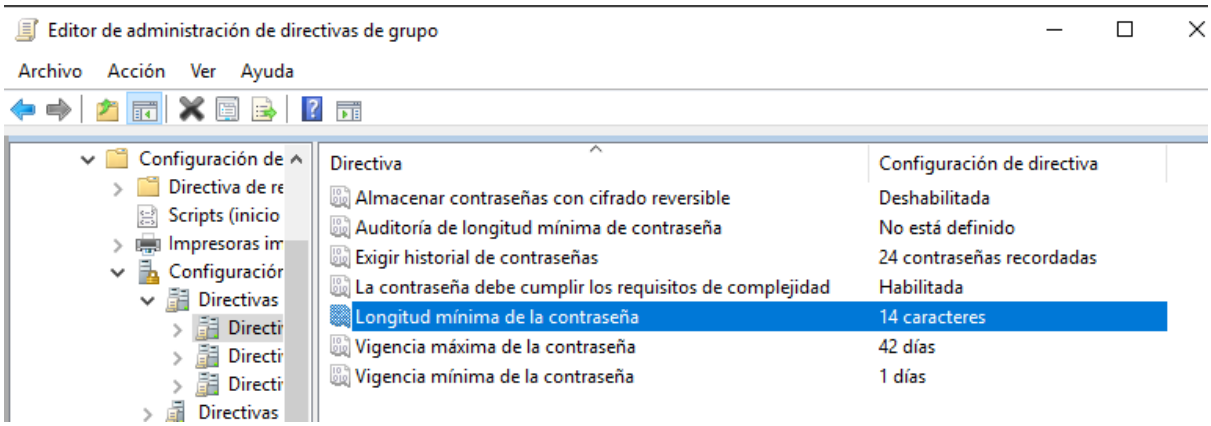


Vamos a crear una OU llamada trabajo y dentro vamos a crear las ous admins servidores, equipos, usuarios y grupos.

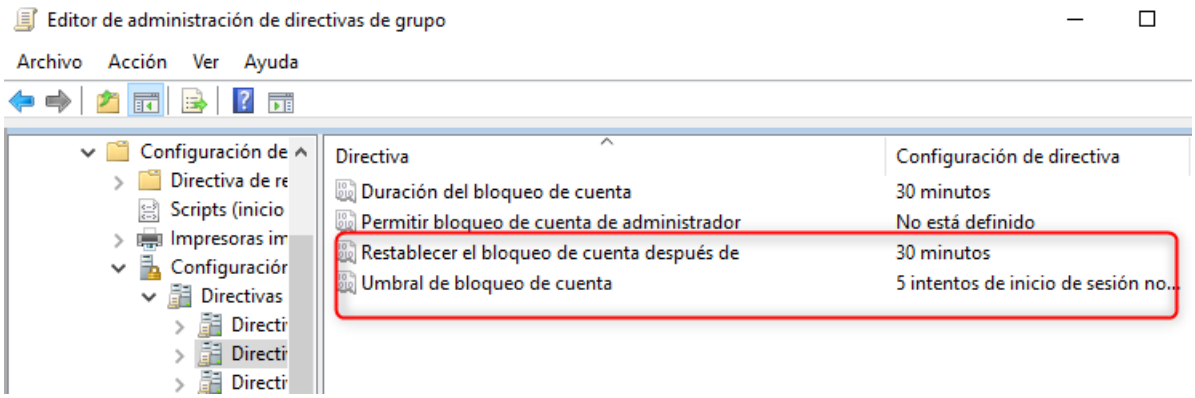


3. Políticas de grupo

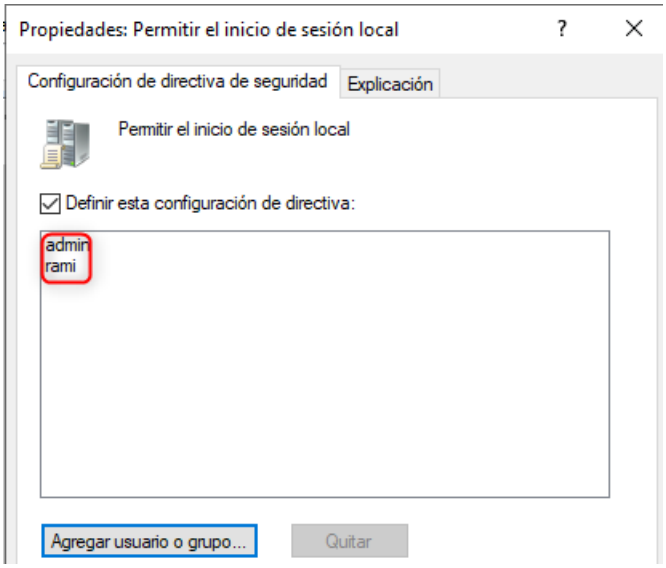
Ahora vamos a crear políticas de grupo para ello abrimos ejecutar y escribimos gpmc.msc. Y en directivas de contraseña pondremos longitud minima de contraseña 14 caracteres.



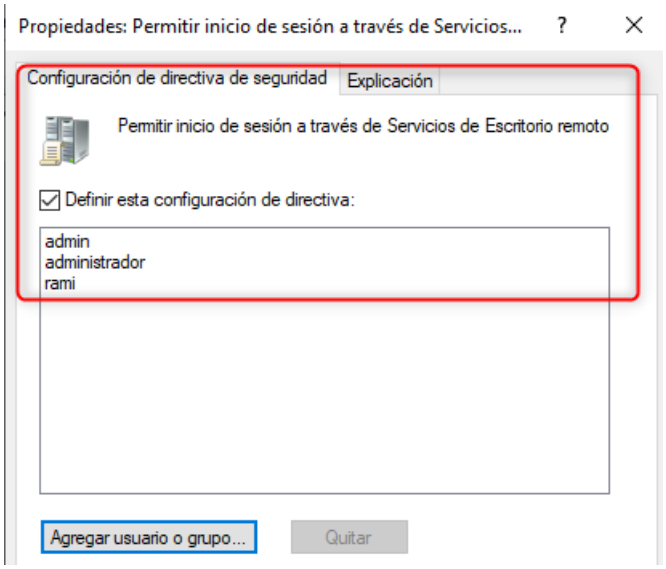
Ahora iremos a directivas de bloqueo de contraseñas y lo estableceremos en 5 intentos y que se reste el bloqueo despues de 30 minutos.



Ahora evitaremos que cualquier usuario inicie sesión en el servidor vamos a configuración del equipo, directivas, configuración de windows, configuración de seguridad, directivas locales y asignación de derechos de usuario. Ahi dentro nos vamos a permitir el inicio de sesion local y solo dejamos el usuario que sea administrador.

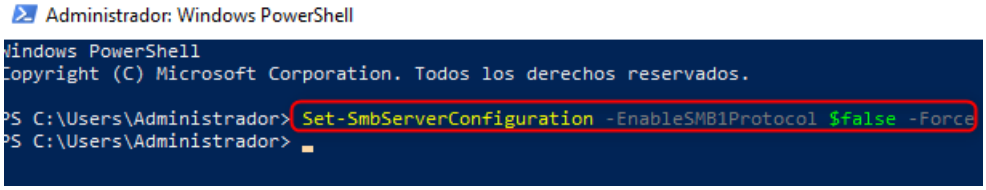


Y en permitir inicio de sesión por escritorio remoto aremos lo mismo.

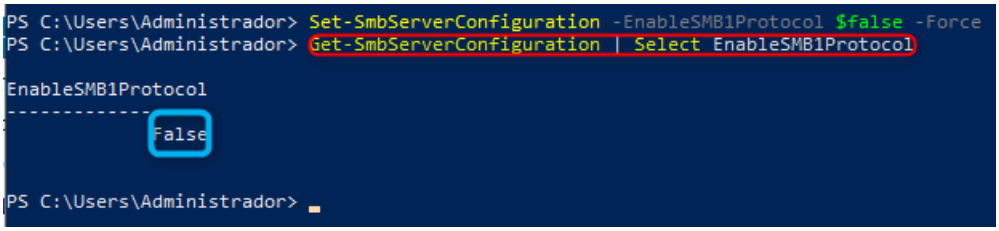


4. Deshabilitar SMB1

Para deshabilitar SMB1 abrimos PowerShell y ejecutamos el siguiente comando.

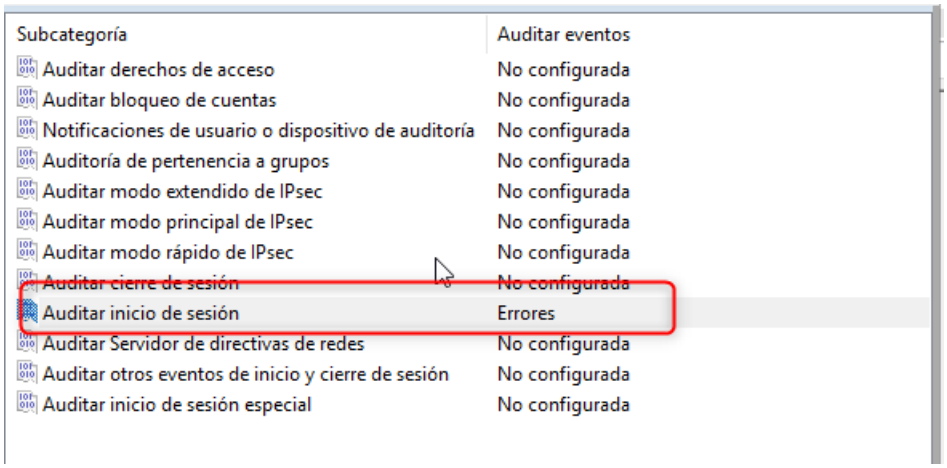


Para comprobar que ya no está activo ejecutaremos el siguiente comando y debería devolver false.



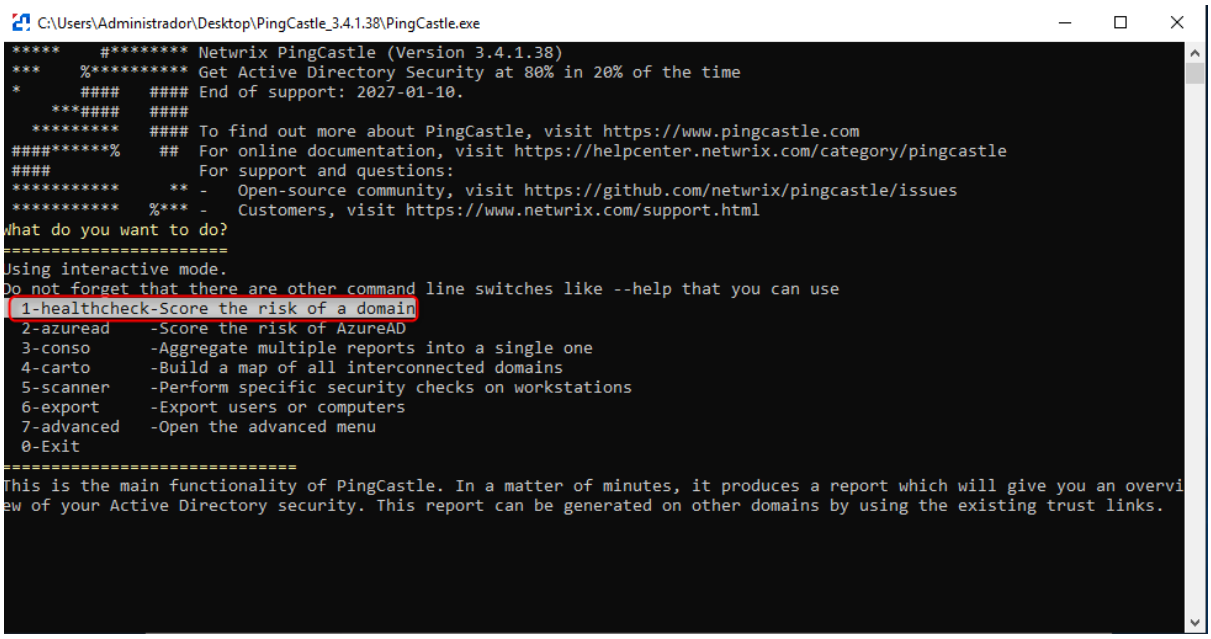
5. Auditoria

Primero activaremos la auditoria avanzada en la gpo de controladores de dominio y en inicio y cierre de sesión habilitamos inicio de sesión asi registraremos los intentos de intrusión.

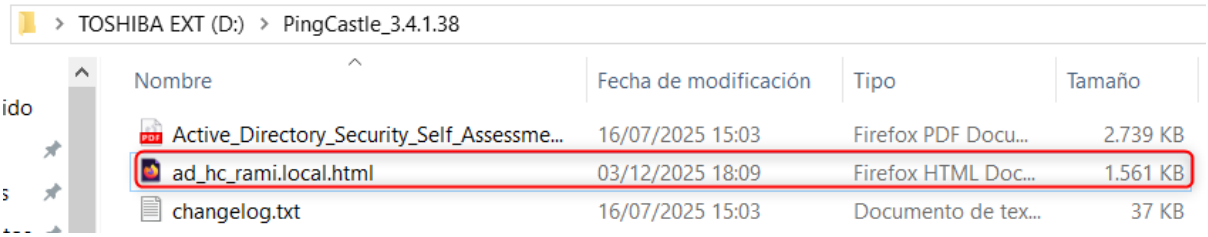


Por último instalaremos pingcastle y nos escaneara nuestro active directory y nos dira como es de seguro y que podemos mejorar.

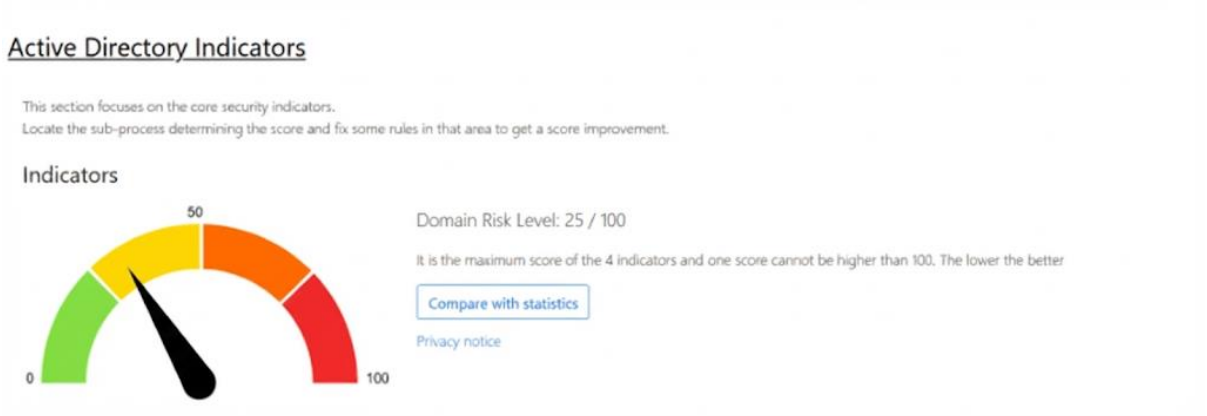
Una vez abierto seleccionamos la opción 1 healthcheck.



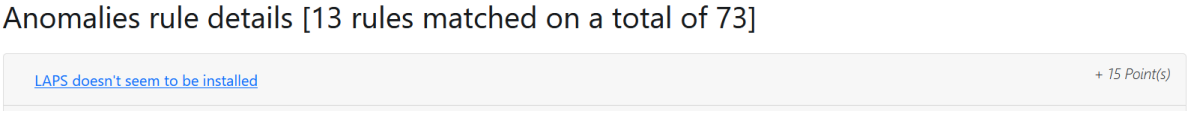
Una vez termine nos dejara un archivo html en la carpeta donde hallamos descargado la herramienta.



Al abrir ese archivo nos dará una puntuación y según vayamos corrigiendo cosas nos bajará la puntuación, lo mejor es cuanto más baja este.



Como podemos ver tenemos un 25 de 100 la idea es ir haciendo las cosas que no propone para bajar el riesgo a 0 o lo más cercano.



Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.12.11 10:40:24 +01'00'