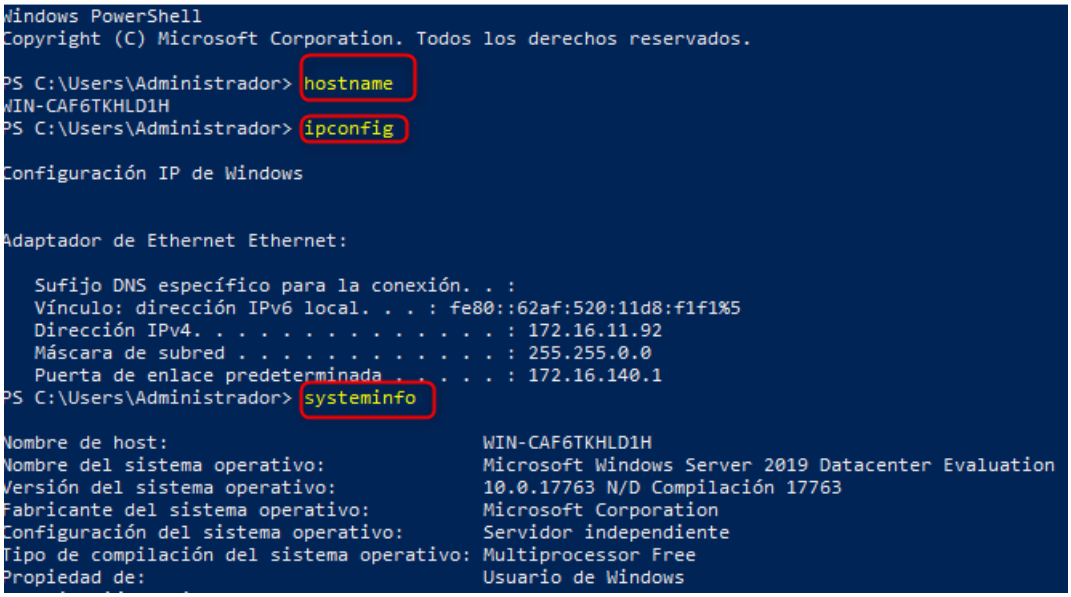
Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

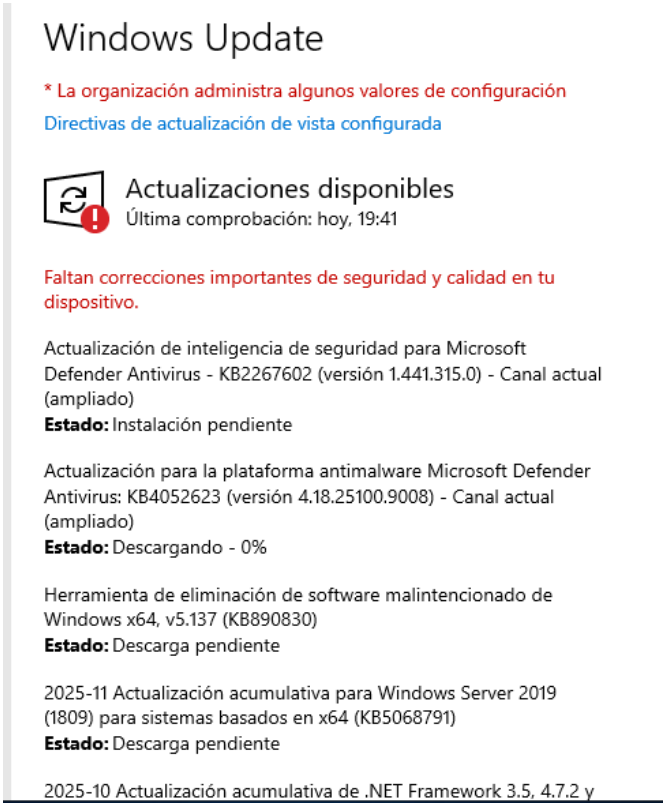
Bastionado de Windows server 2019

Héctor Ramírez López

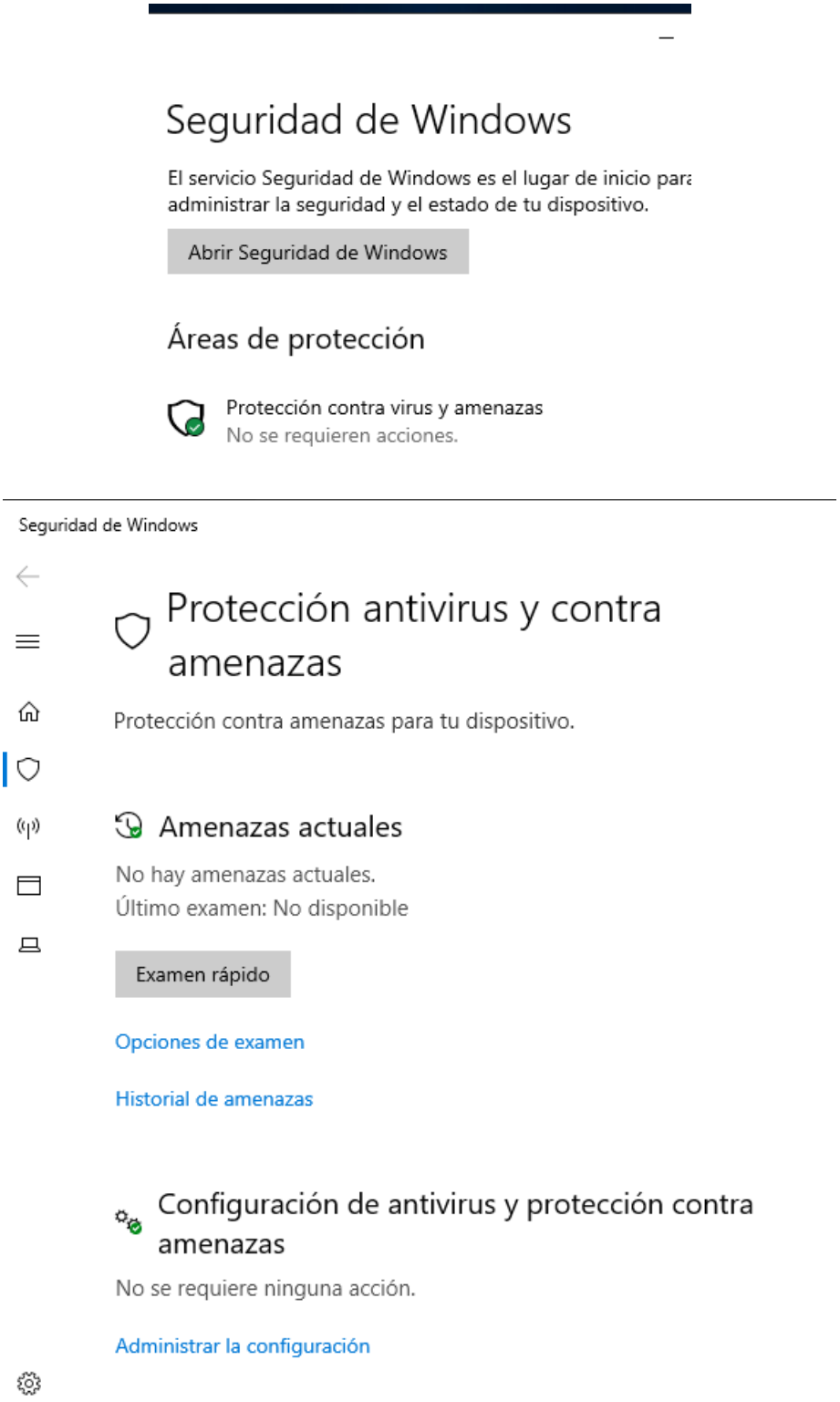
Una vez inciado el sistema lo primero que haremoos sera ejecutar una serie de comandos que son los siguientes: **hostname** para saber el nombre del equipo, **ipconfig** para ver la configuración de red y **systeminfo** para saber la versión que tenemos etc.



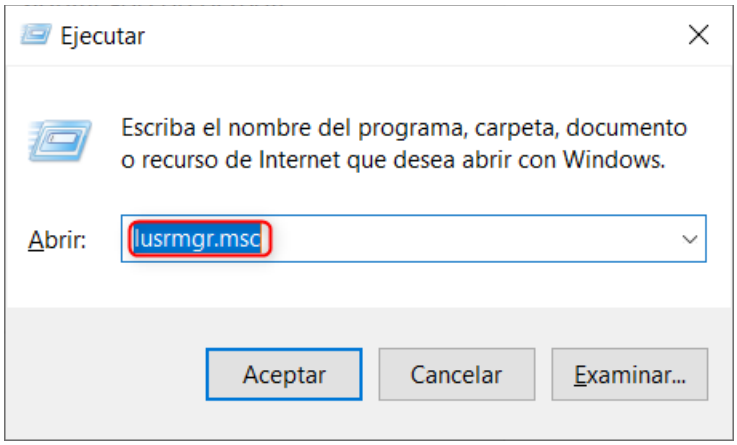
El siguiente paso es actualizar el equipo para ello abrimos Windows update, una vez actualizado nos pedirá reiniciar el equipo.



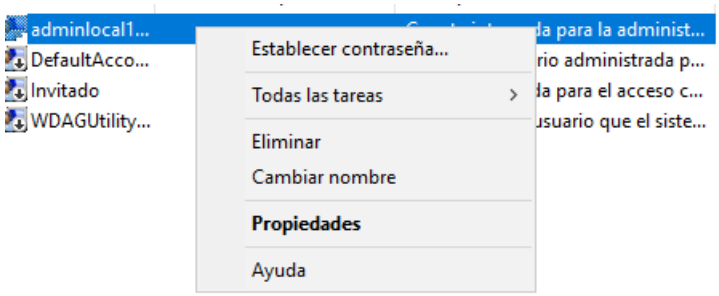
Tras reiniciar el equipo comprobaremos que el antivirus esta activo en este caso nos iremos a Windows defender, como podemos ver esta activado.



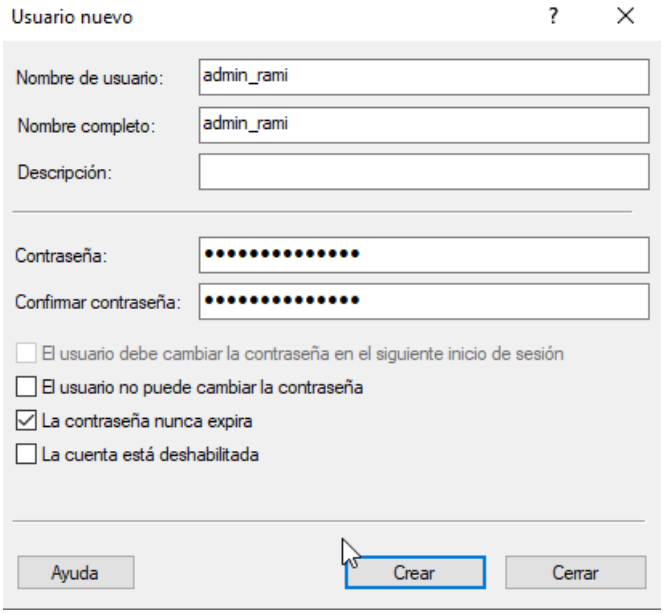
Ahora vamos a entrar en el apartado de cuentas y grupos locales de Windows para configurar el administrador, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **lusrmgr.msc.**



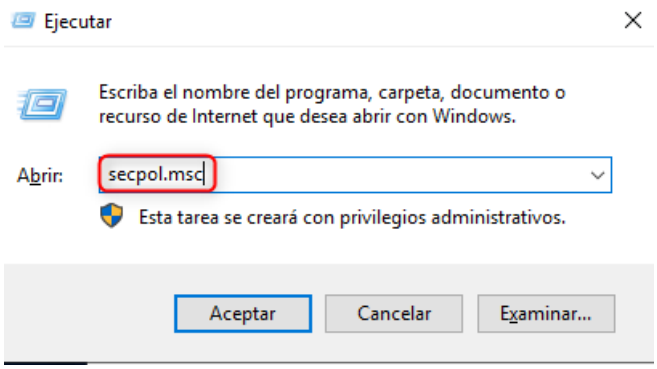
Una vez dentro nos iremos a renombrar el admin para que en caso de ataque al equipo no sea tan obvio conseguir el admin por ejemplo pondremos admin123, aunque en la mayoría de las empresas se suele deshabilitar ya que no cumple con el principio de mínimo privilegio ty crear otro usuario admin con otro nombre.



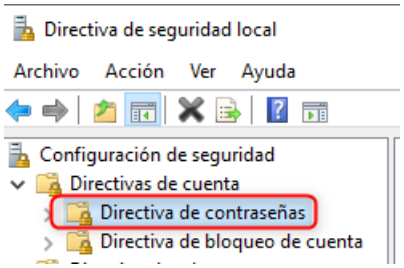
Aquí estaríamos creando otro usuario admin .



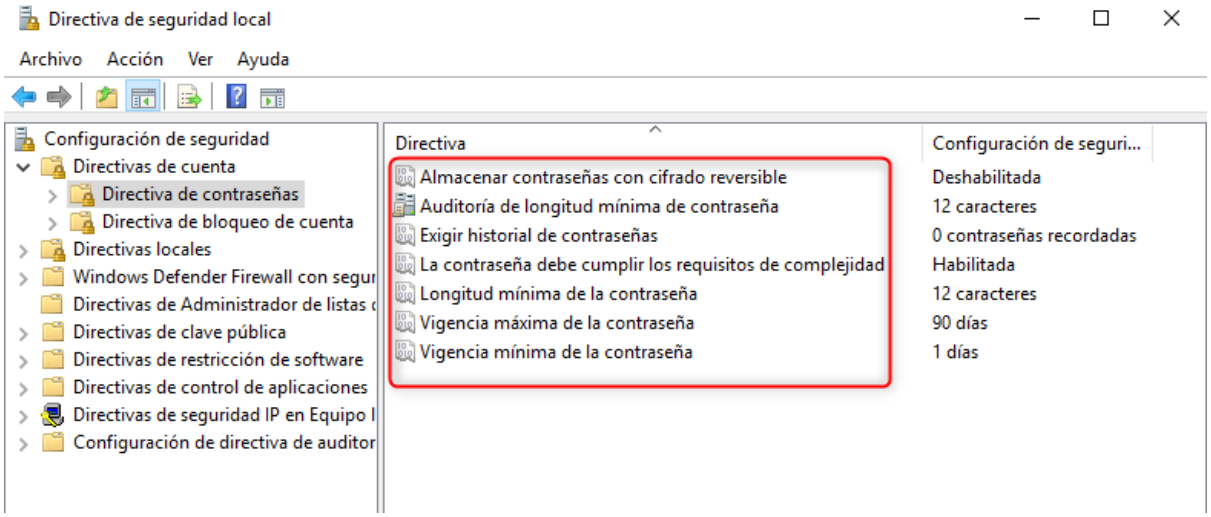
Lo siguiente a realizar es establecer una política de contraseñas, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **secpol.msc**.



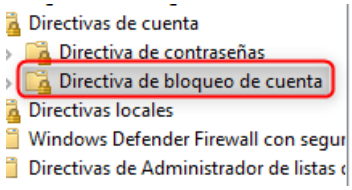
Una vez dentro nos iremos a directiva de contraseñas



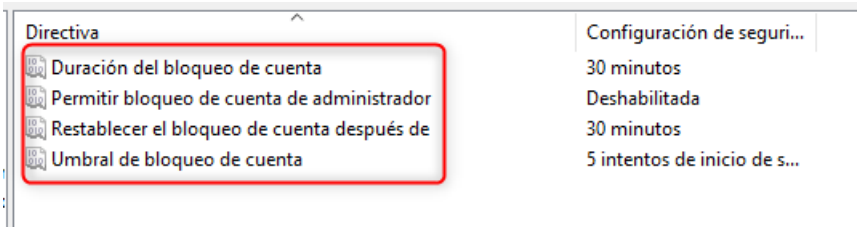
Los valores que nos aparecen aquí dentro los tendremos que dejar como en la imagen



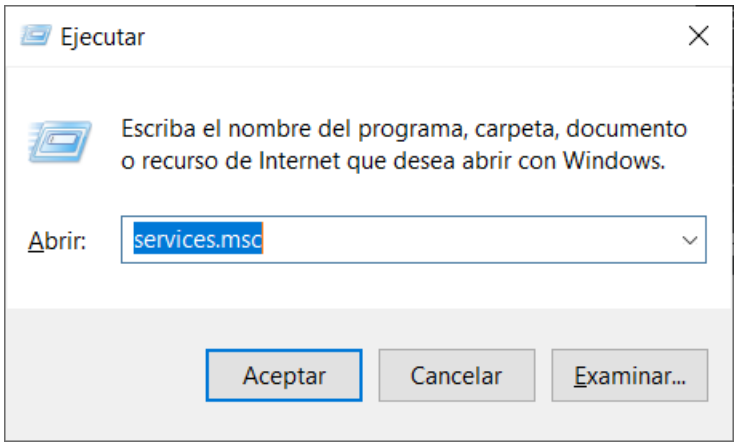
Después iremos a la parte de directiva de bloqueos de cuenta.



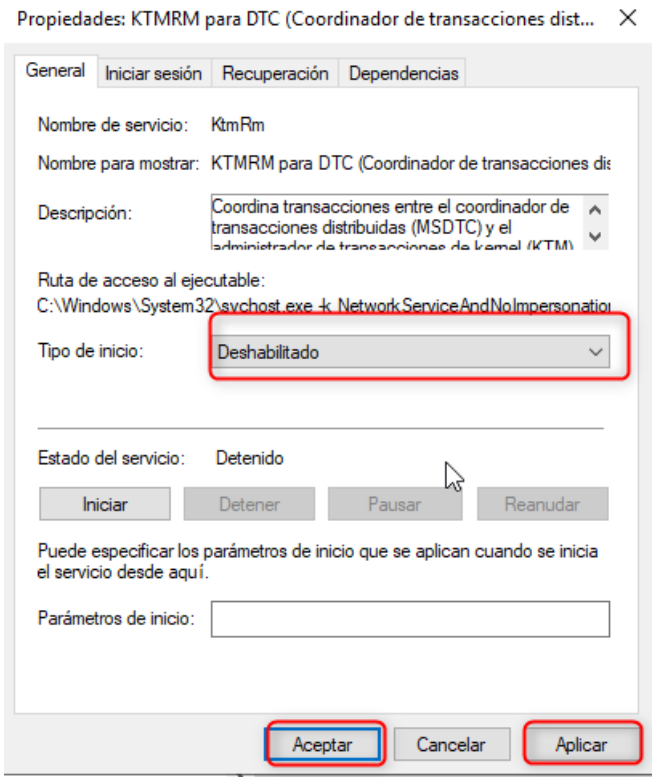
Y los campos marcados en rojo habría que ponerlos como se ve en la imagen.



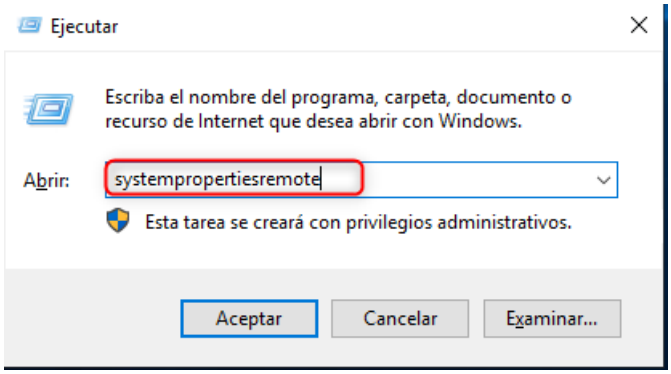
Una vez hecho esto no s iremos a deshabilitar servicios que no necesitemos, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **services.msc.**



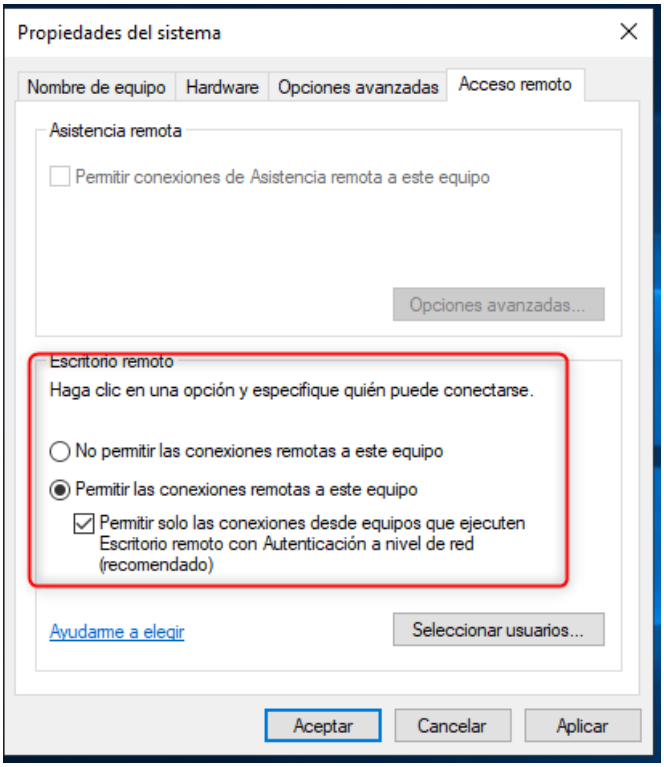
Nos saldrá una ventana con todos los servicios con doble click abrimos el que queramos deshabilitar y en inicio le ponemos la opción deshabilitada Y le daremos a aplicar y aceptar.



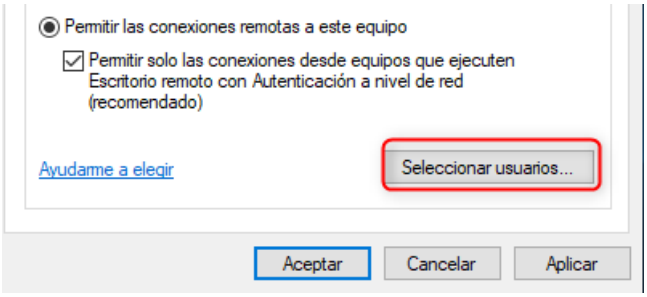
Ahora nos iremos a configurar el escritorio remoto, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **systempropertiesremote.**



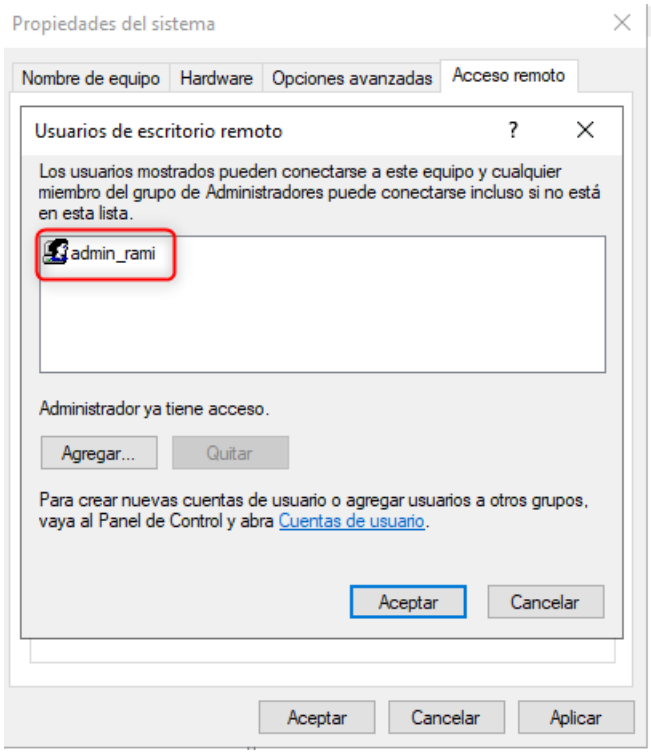
Se nos abrirá la ventana de la imagen aqui tendremos que seleccionar la casilla permitir las conexiones a este equipo y marcar la casilla escritorio remoto con autenticación de red.



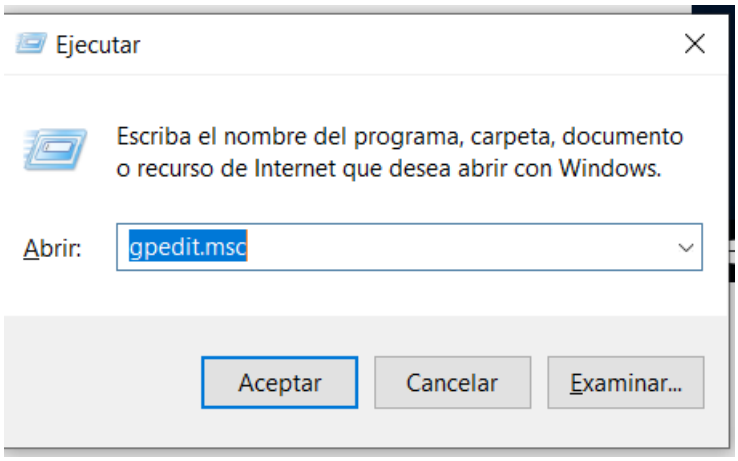
Despues nos iremos a la pestaña seleccionar usuarios.



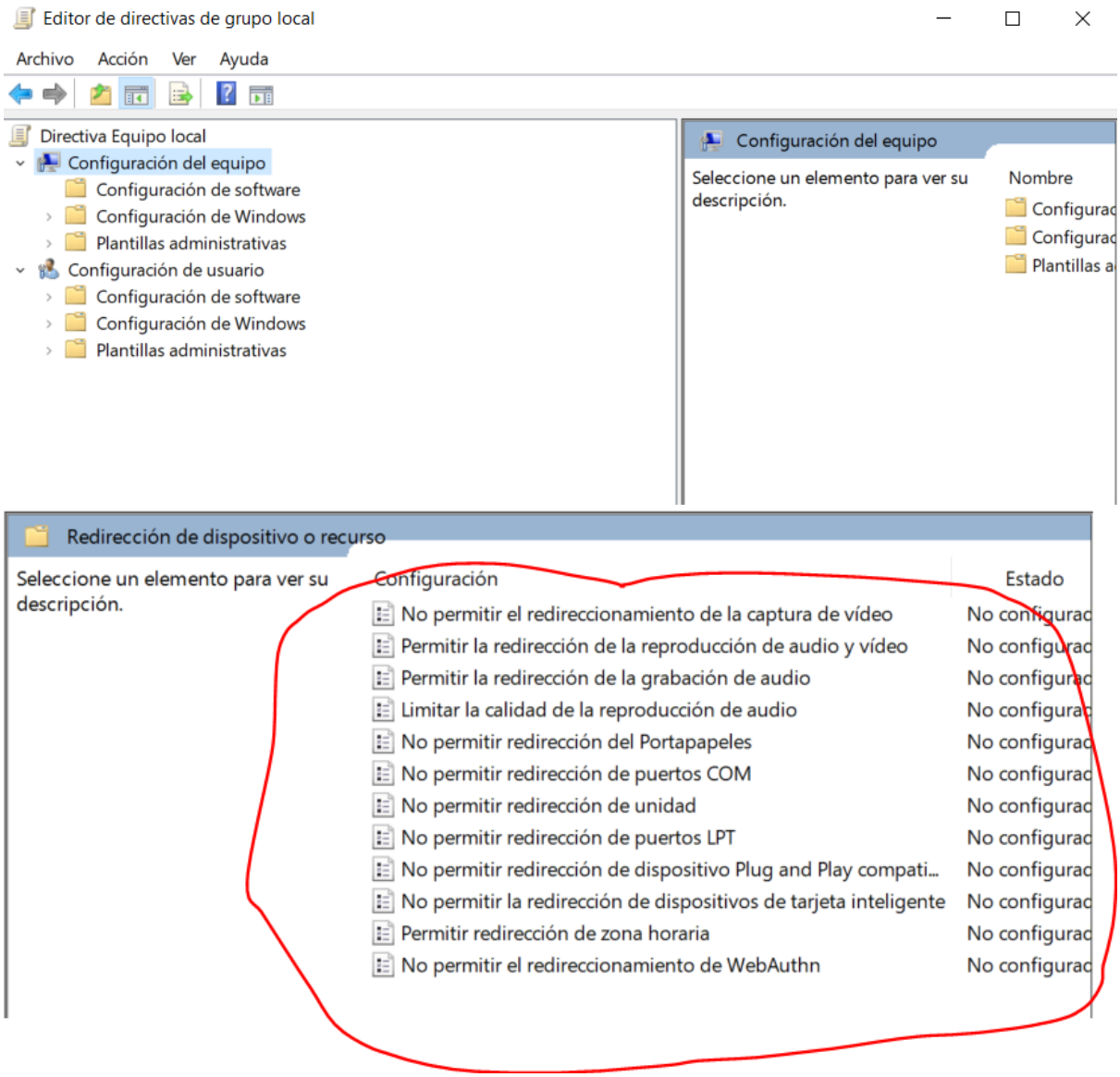
Pondremos el usuario con el que vamos a poder conectarnos



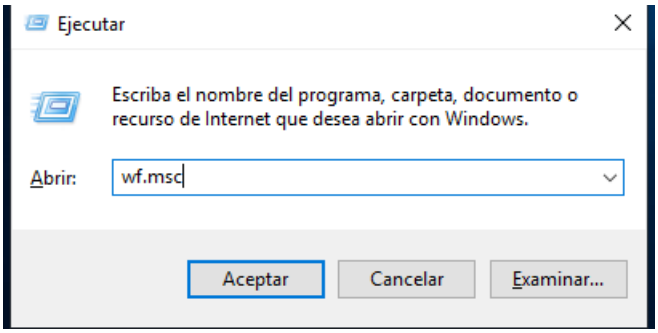
Una vez realizado el paso anterior nos iremos a configurar para evitar las redirecciones, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **gpedit.msc**



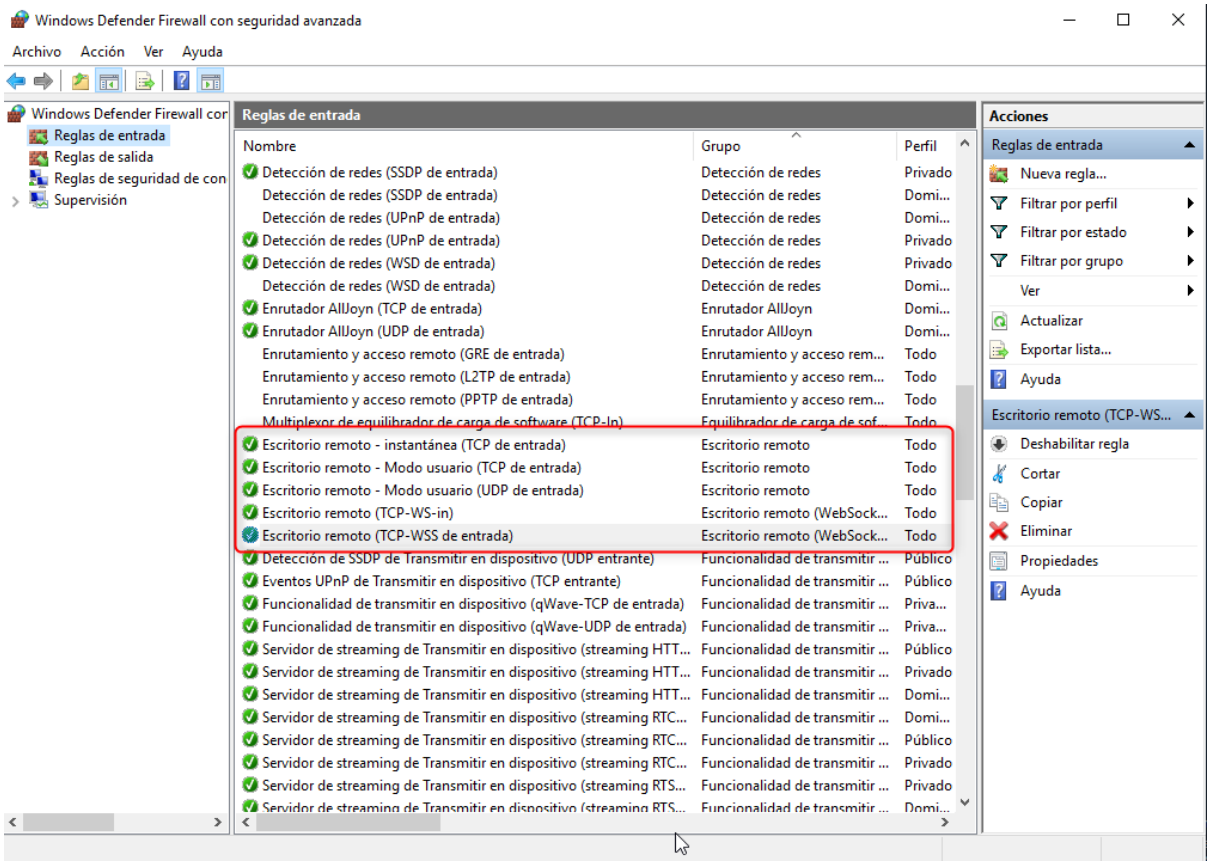
Se nos abrirá esta pantalla y nos iremos a la ruta configuración del equipo-->plantillas administrativas-->componentes de Windows-->servicios de escritorio remoto-->host de sesion de escritorio remoto-->redireccion de dispositivo y recurso ahí podremos configurar las redirecciones.



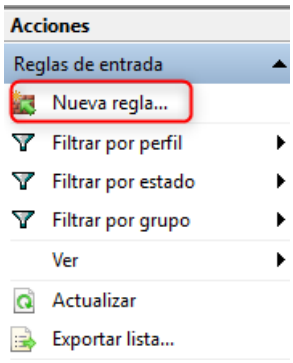
El siguiente paso sería configurar el firewall para ello con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **wf.msc.**



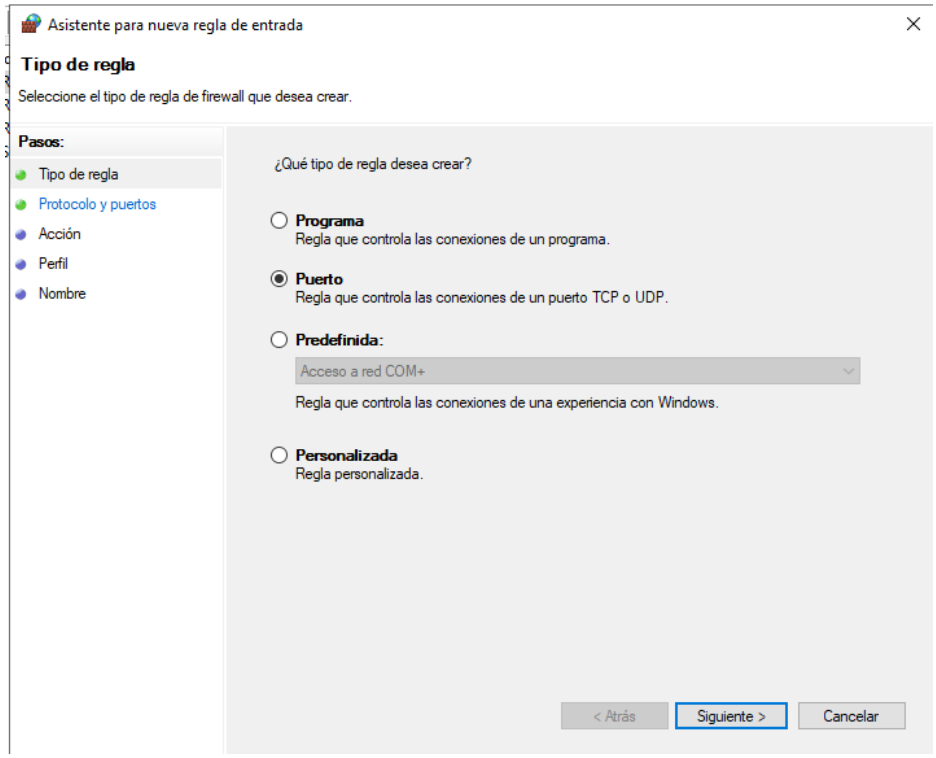
Lo primero que haremos será verificar que las reglas creadas de entrada estén habilitadas.

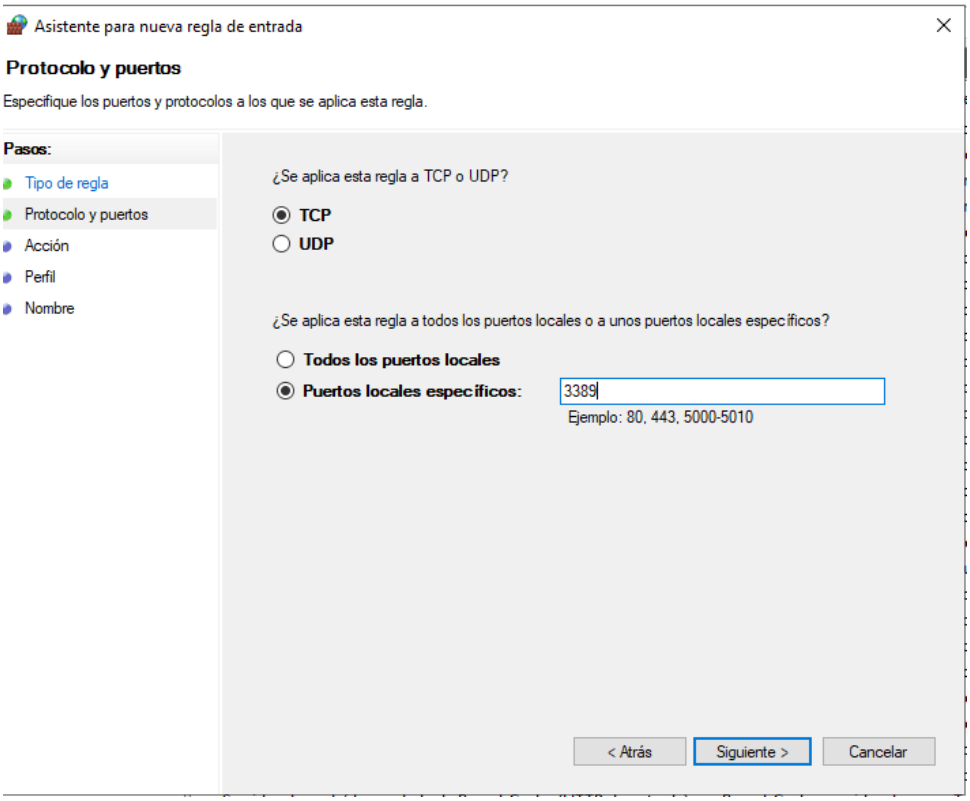


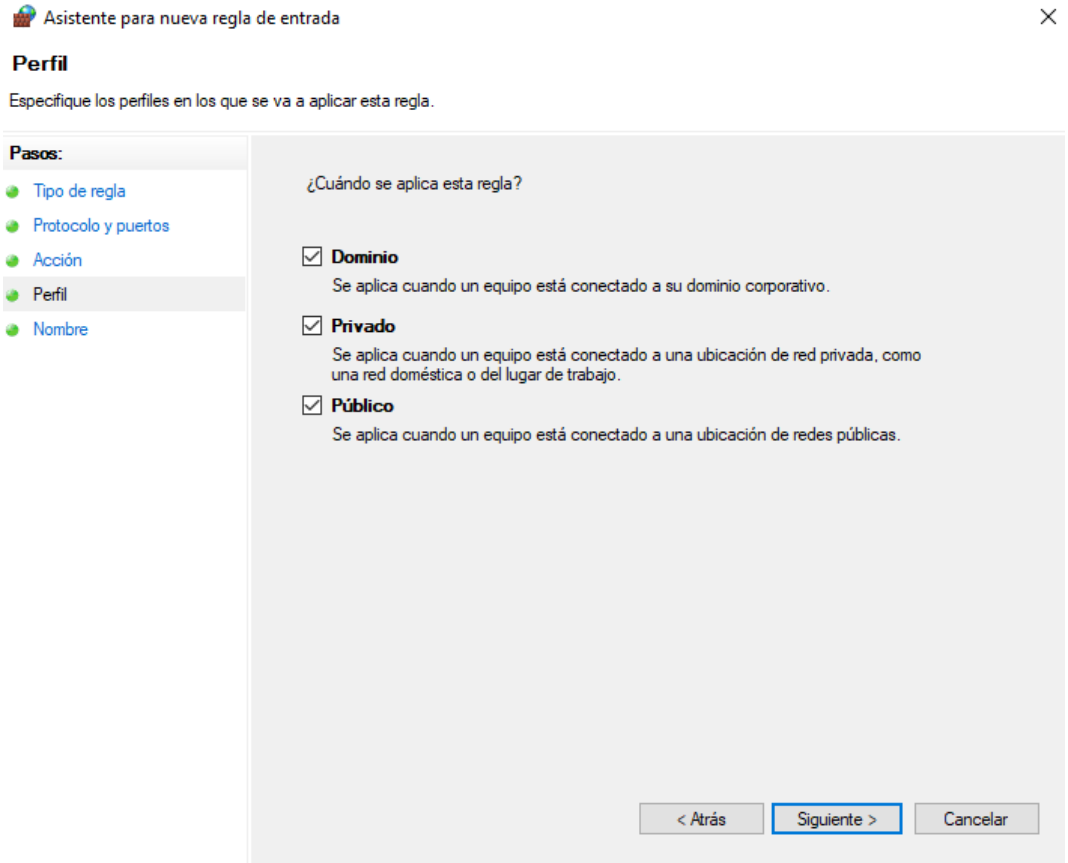
Ahora nos iremos a crear una nueva regla.



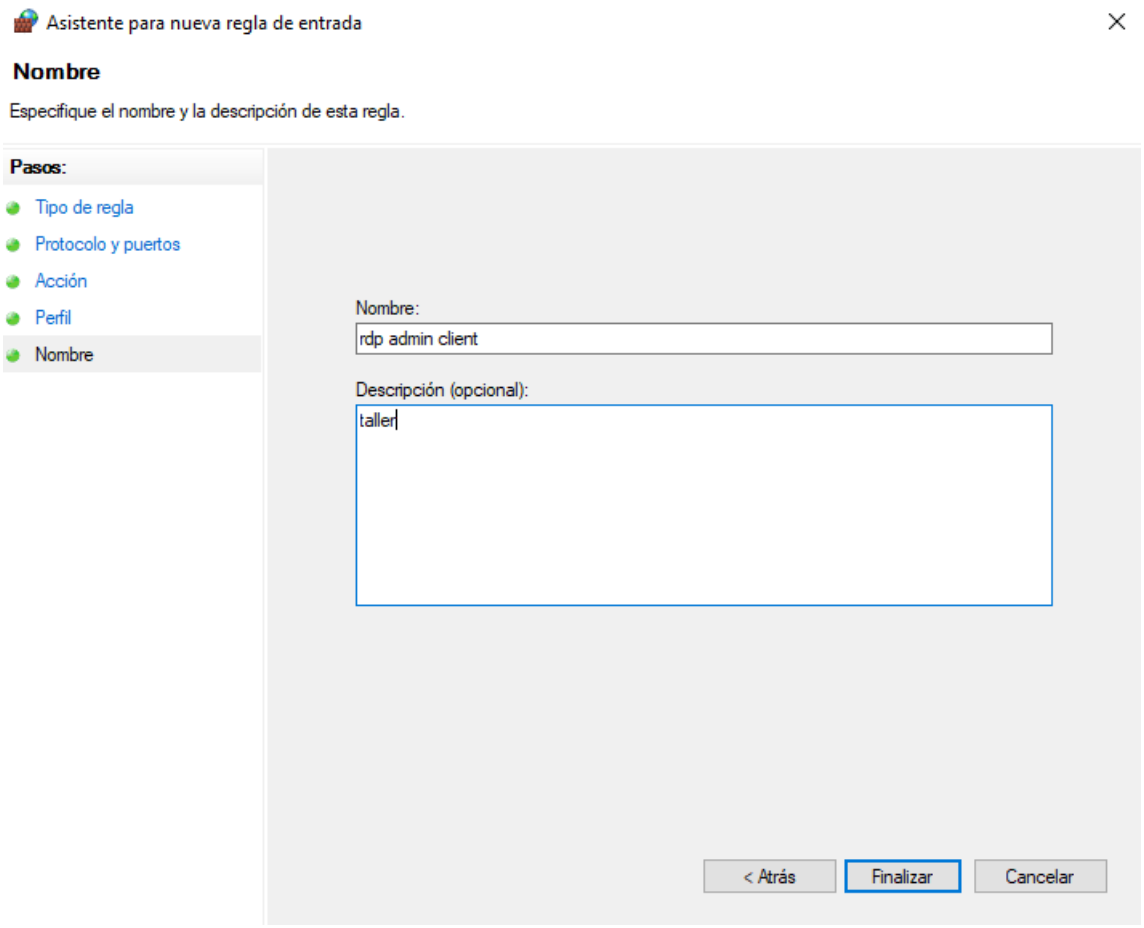
En tipo de regla marcamos puerto después personalizado y ponemos el puerto 3389 que es el del rdp.



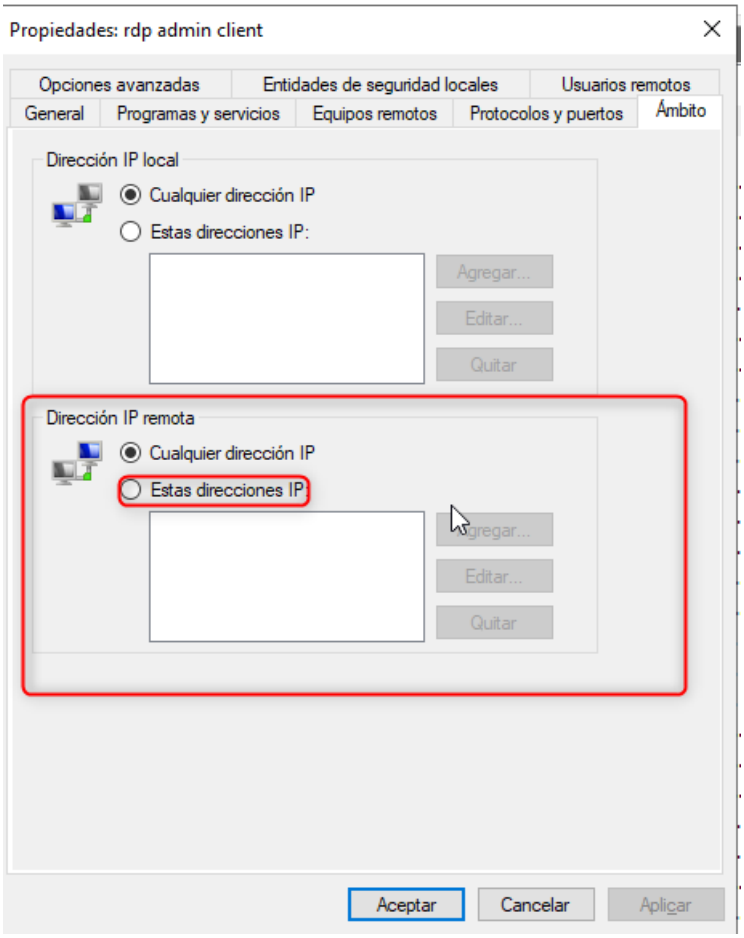

Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Se aplica esta regla a TCP o UDP?
TCP
UDP
¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?
Todos los puertos locales
Puertos locales específicos:
3389
Ejemplo: 80, 443, 5000-5010
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de entrada
Perfil
Especifique los perfiles en los que se va a aplicar esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Cuándo se aplica esta regla?
Dominio
Se aplica cuando un equipo está conectado a su dominio corporativo.
Privado
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.
Público
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.
< Atrás
Siguiente >
Cancelar

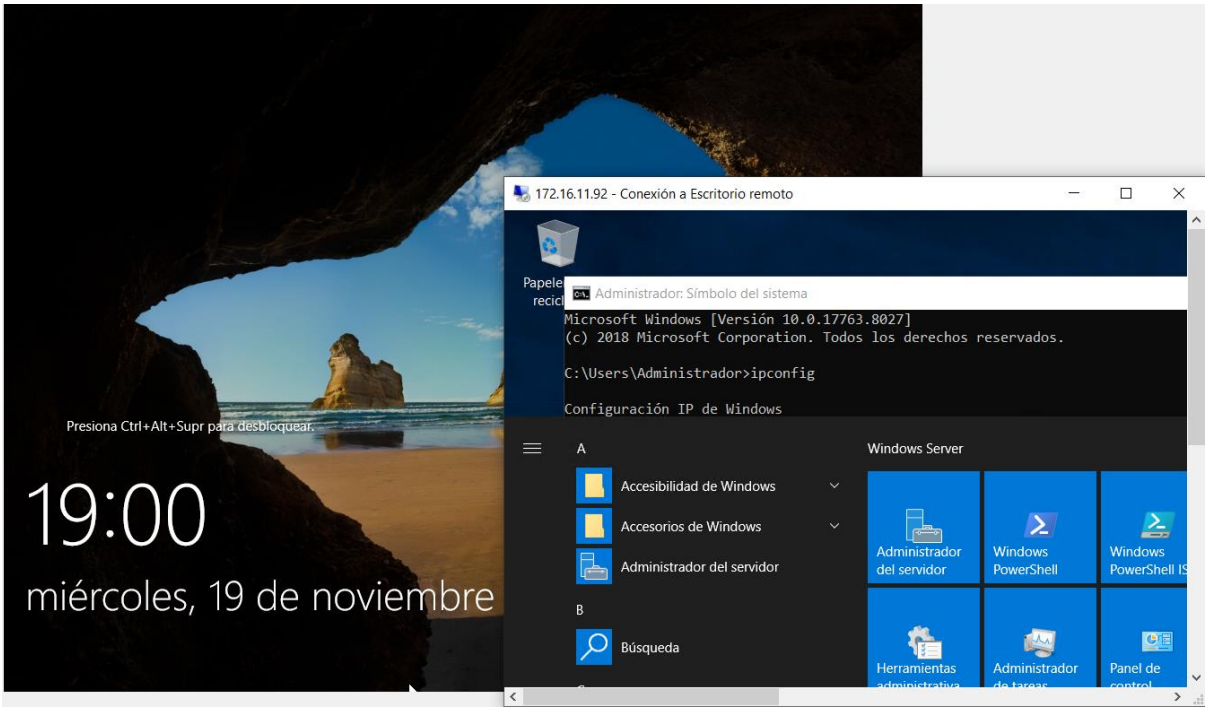
En el último paso le pondremos un nombre a la regla.



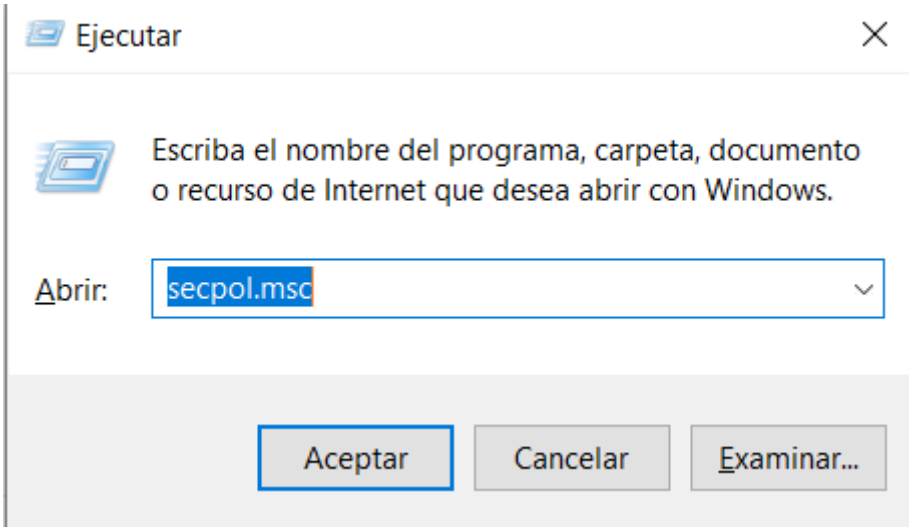
Una vez creada nos saldrá nuestra regla creada le damo doble clic y se nos abrirá la siguiente ventana, en el apartado ámbito en dirección ip remota pondremos la ip desde donde nos vallamos a conectar en este caso la ip seria 172.16.11.92.



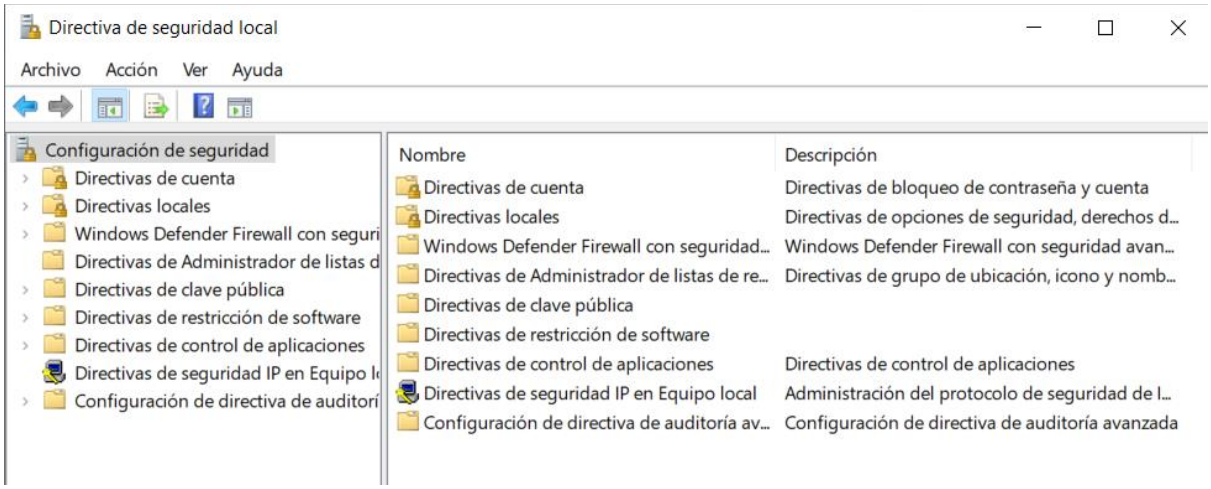
Una vez realizado esto intentamos conectarnos por escritorio remoto al Windows server y tendriamos que poder conectarnos.



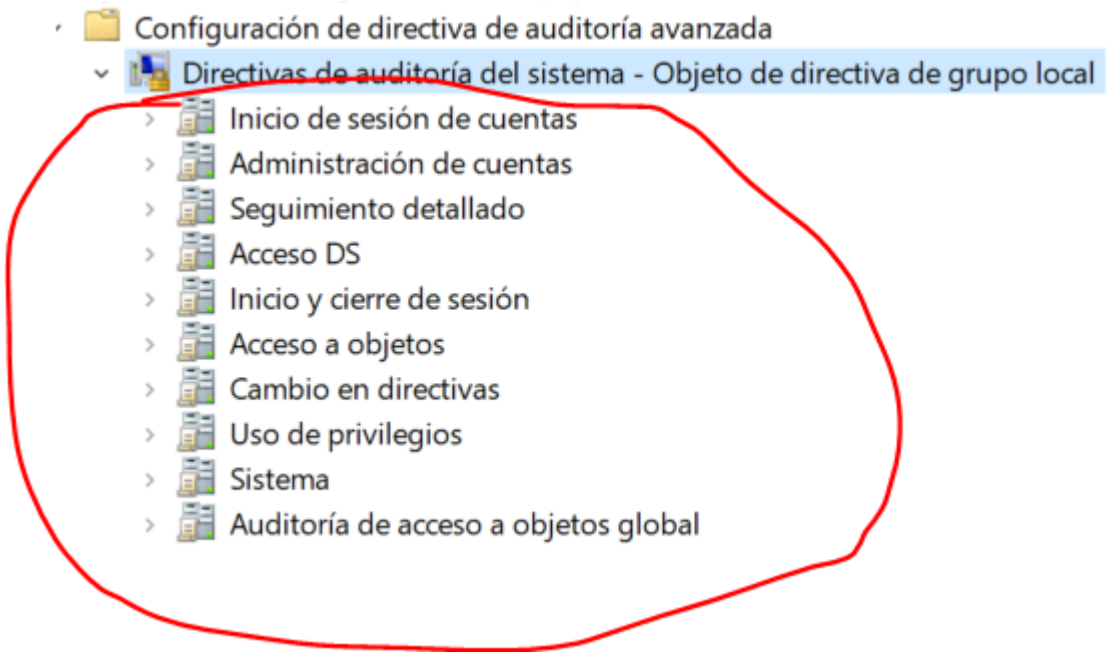
Para acabar nos iremos a la configuración de auditorías, con windows + r se nos abrirá ejecutar y escribimos el comando **secpol.msc.**



Se nos abrirá esta pestaña y nos iremos a la ruta configuracion de auditoria avanzada-->directivas de auditoría del sistema



Aquí veremos las políticas de auditorías que podemos configurar.



Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid