



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid

Bastionado de Windows server 2019

Héctor Ramírez López

Una vez iniciado el sistema lo primero que haremos 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.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> hostname
WIN-CAF6TKHLD1H
PS C:\Users\Administrador> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::62af:520:11d8:f1f1%5
    Dirección IPv4. . . . . : 172.16.11.92
    Máscara de subred . . . . . : 255.255.0.0
    Puerta de enlace predeterminada . . . . : 172.16.140.1
PS C:\Users\Administrador> systeminfo

Nombre de host: WIN-CAF6TKHLD1H
Nombre del sistema operativo: Microsoft Windows Server 2019 Datacenter Evaluation
Versión del sistema operativo: 10.0.17763 N/D Compilación 17763
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Servidor independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
```

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

Windows Update

* La organización administra algunos valores de configuración

[Directivas de actualización de vista configurada](#)



Actualizaciones disponibles

Última comprobación: hoy, 19:41

Faltan correcciones importantes de seguridad y calidad en tu dispositivo.

Actualización de inteligencia de seguridad para Microsoft Defender Antivirus - KB2267602 (versión 1.441.315.0) - Canal actual (ampliado)

Estado: Instalación pendiente

Actualización para la plataforma antimalware Microsoft Defender Antivirus: KB4052623 (versión 4.18.25100.9008) - Canal actual (ampliado)

Estado: Descargando - 0%

Herramienta de eliminación de software malintencionado de Windows x64, v5.137 (KB890830)

Estado: Descarga pendiente

2025-11 Actualización acumulativa para Windows Server 2019 (1809) para sistemas basados en x64 (KB5068791)

Estado: Descarga pendiente

2025-10 Actualización acumulativa de .NET Framework 3.5, 4.7.2 y

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

Seguridad de Windows

El servicio Seguridad de Windows es el lugar de inicio para administrar la seguridad y el estado de tu dispositivo.

[Abrir Seguridad de Windows](#)

Áreas de protección

 Protección contra virus y amenazas
No se requieren acciones.

Seguridad de Windows



Protección antivirus y contra amenazas



Protección contra amenazas para tu dispositivo.



Amenazas actuales



No hay amenazas actuales.

Último examen: No disponible



[Examen rápido](#)

[Opciones de examen](#)

[Historial de amenazas](#)

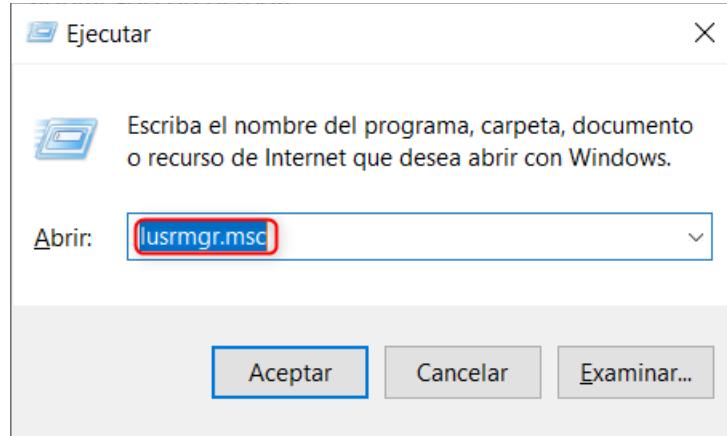
 Configuración de antivirus y protección contra amenazas

No se requiere ninguna acción.

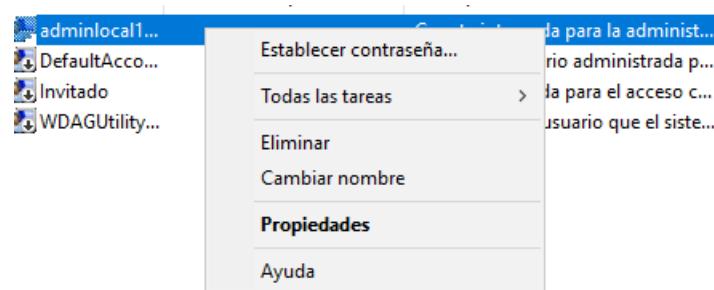
[Administrar la configuración](#)



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 .

Usuario nuevo

?

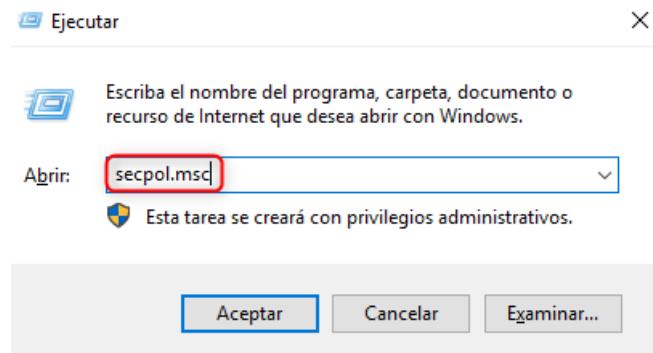
X

Nombre de usuario:	admin_rami
Nombre completo:	admin_rami
Descripción:	
Contraseña:	*****
Confirmar contraseña:	*****

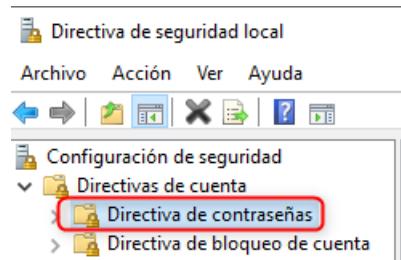
El usuario debe cambiar la contraseña en el siguiente inicio de sesión
 El usuario no puede cambiar la contraseña
 La contraseña nunca expira
 La cuenta está deshabilitada

[Ayuda](#) Crear [Cerrar](#)

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**.



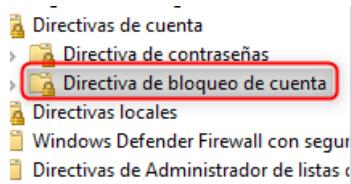
Una vez dentro nos iremos a directiva de contraseñas



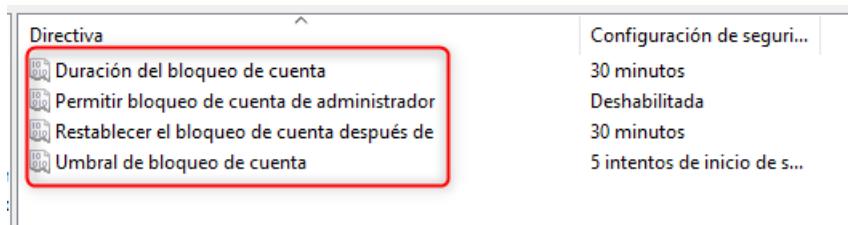
Los valores que nos aparecen aquí dentro los tendremos que dejar como en la imagen

Configuración de seguridad	Valor
Almacenar contraseñas con cifrado reversible	Deshabilitada 12 caracteres
Auditoría de longitud mínima de contraseña	Habilitada 12 caracteres
Exigir historial de contraseña	Habilitada 90 días
La contraseña debe cumplir los requisitos de complejidad	Habilitada 12 caracteres
Longitud mínima de la contraseña	Habilitada 12 caracteres
Vigencia máxima de la contraseña	Habilitada 90 días
Vigencia mínima de la contraseña	Habilitada 1 día

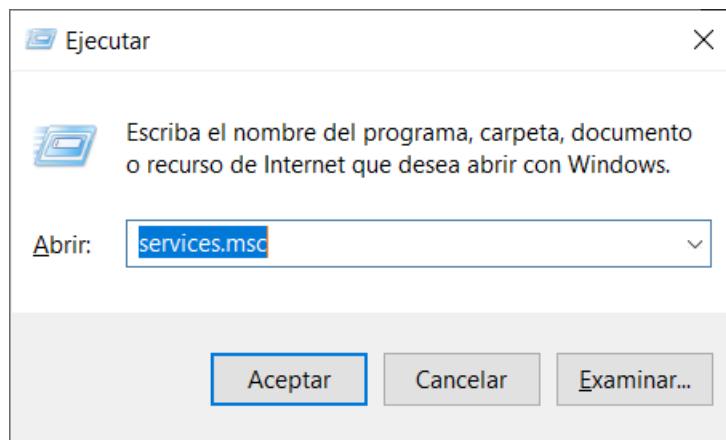
Después iremos a la parte de directiva de bloques de cuenta.



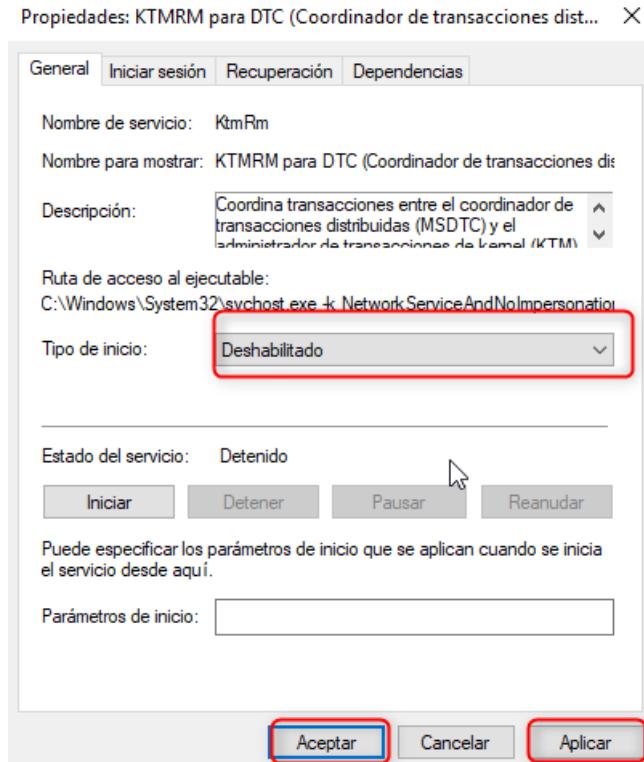
Y los campos marcados en rojo habría que ponerlos como se ve en la imagen.



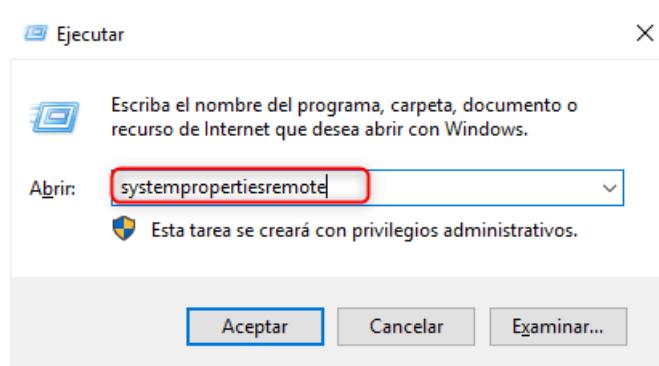
Una vez hecho esto no s iremos a deshabilitar servicios que no necesitemos, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **services.msc**.



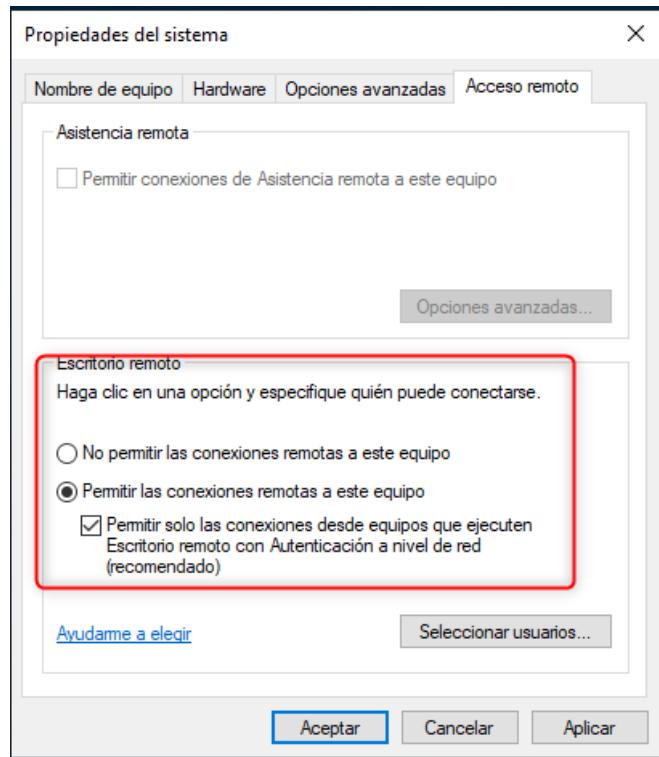
Nos saldrá una ventana con todos los servicios con doble click abrimos el que queramos deshabilitar y en inicio le ponemos la opción deshabilitada Y le daremos a aplicar y aceptar.



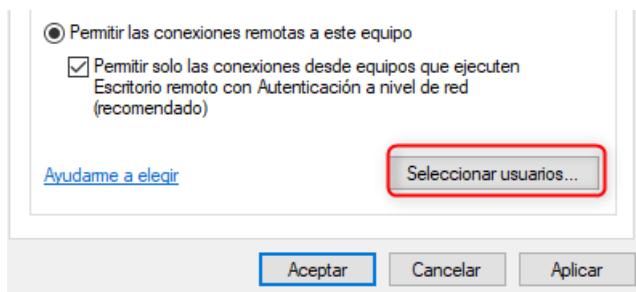
Ahora nos iremos a configurar el escritorio remoto, esto lo hacemos con las teclas Windows+r se nos abrirá el ejecutar y pondremos el comando **systempropertiesremote**.



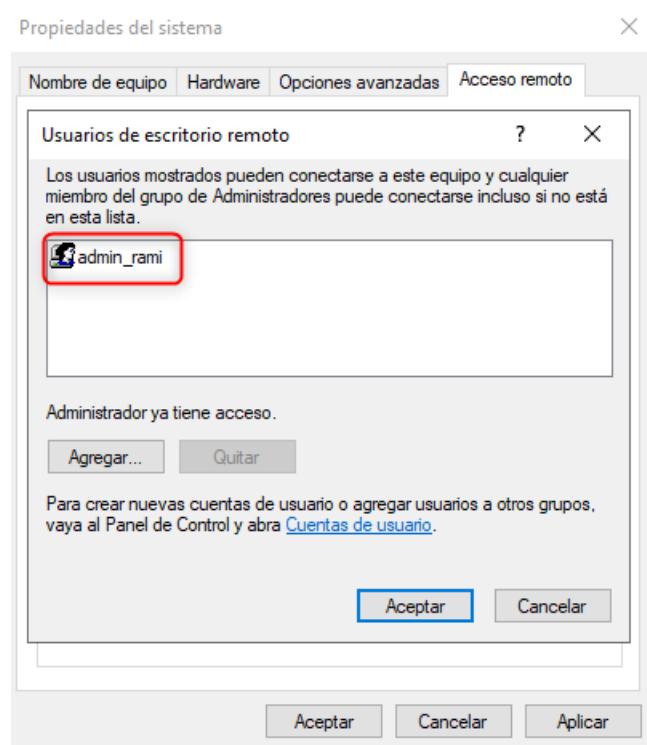
Se nos abrirá la ventana de la imagen aquí tendremos que seleccionar la casilla permitir las conexiones a este equipo y marcar la casilla escritorio remoto con autenticación de red.



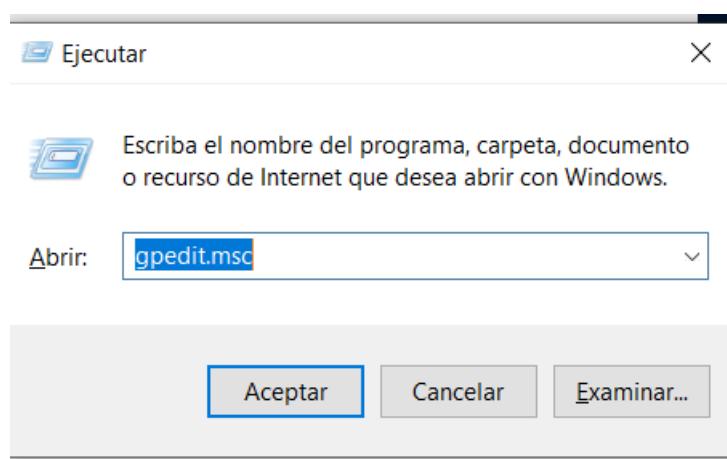
Después nos iremos a la pestaña seleccionar usuarios.



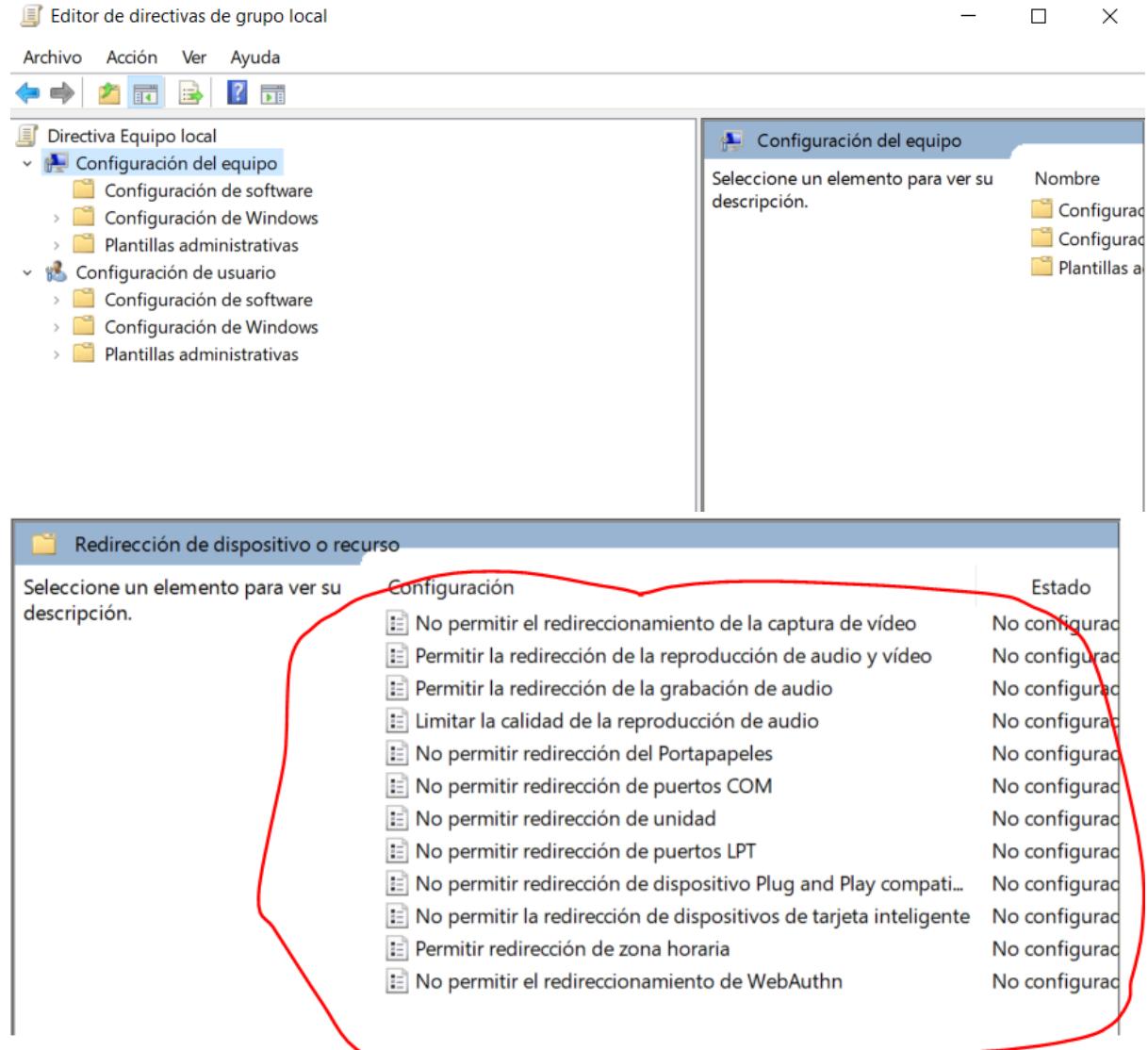
Pondremos el usuario con el que vamos a poder conectarnos



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**



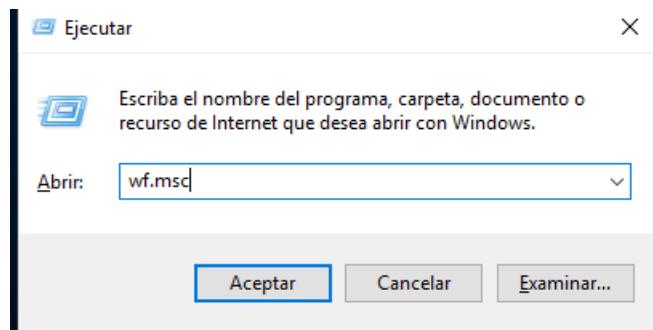
Se nos abrirá esta pantalla y nos iremos a la ruta configuración del equipo-->plantillas administrativas-->componentes de Windows-->servicios de escritorio remoto-->host de sesión de escritorio remoto-->redirección de dispositivo y recurso ahí podremos configurar las redirecciones.



The screenshot shows the Local Group Policy Editor window with the title 'Editor de directivas de grupo local'. The left pane displays a tree structure under 'Directiva Equipo local': 'Configuración del equipo' (selected), 'Configuración de software', 'Configuración de Windows', 'Plantillas administrativas'; and 'Configuración de usuario', 'Configuración de software', 'Configuración de Windows', 'Plantillas administrativas'. The right pane is titled 'Configuración del equipo' and contains the message 'Seleccione un elemento para ver su descripción.' Below this is a table titled 'Redirección de dispositivo o recurso' with the following data:

Configuración	Estado
No permitir el redireccionamiento de la captura de vídeo	No configurado
Permitir la redirección de la reproducción de audio y vídeo	No configurado
Permitir la redirección de la grabación de audio	No configurado
LIMITAR la calidad de la reproducción de audio	No configurado
No permitir redirección del Portapapeles	No configurado
No permitir redirección de puertos COM	No configurado
No permitir redirección de unidad	No configurado
No permitir redirección de puertos LPT	No configurado
No permitir redirección de dispositivo Plug and Play compatible	No configurado
No permitir la redirección de dispositivos de tarjeta inteligente	No configurado
Permitir redirección de zona horaria	No configurado
No permitir el redireccionamiento de WebAuthn	No configurado

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**.



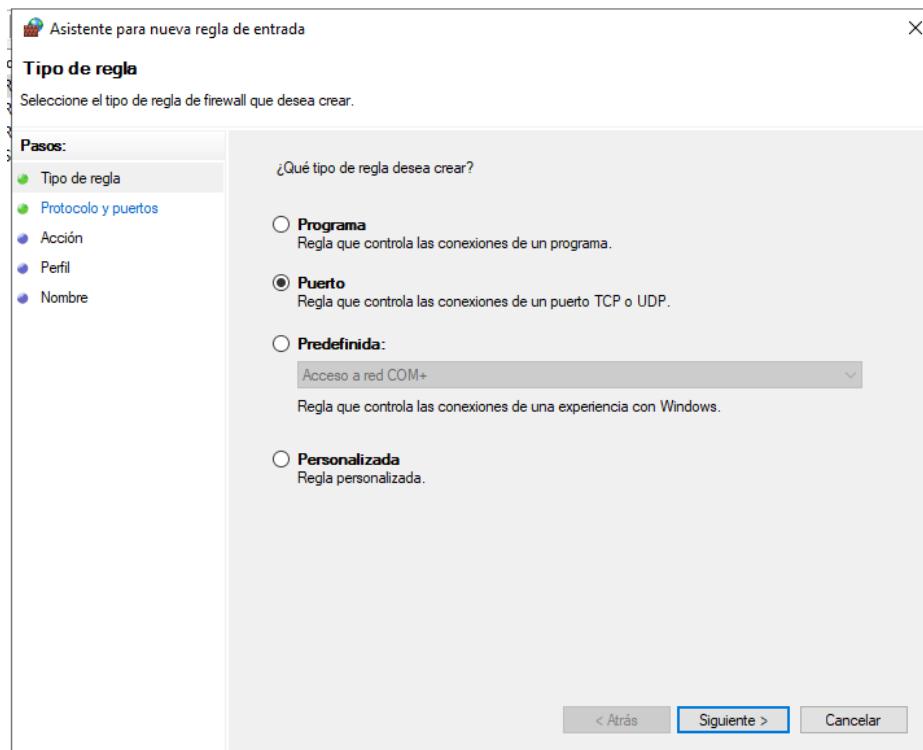
Lo primero que haremos será verificar que las reglas creadas de entrada estén habilitadas.

Nombre	Grupo	Perfil
Detección de redes (SSDP de entrada)	Detección de redes	Privado
Detección de redes (SSDP de entrada)	Detección de redes	Domi...
Detección de redes (UPnP de entrada)	Detección de redes	Domi...
Detección de redes (UPnP de entrada)	Detección de redes	Privado
Detección de redes (WSD de entrada)	Detección de redes	Privado
Detección de redes (WSD de entrada)	Detección de redes	Domi...
Enrutador AllJoyn (TCP de entrada)	Enrutador AllJoyn	Domi...
Enrutador AllJoyn (UDP de entrada)	Enrutador AllJoyn	Domi...
Enrutamiento y acceso remoto (GRE de entrada)	Enrutamiento y acceso rem...	Todo
Enrutamiento y acceso remoto (L2TP de entrada)	Enrutamiento y acceso rem...	Todo
Enrutamiento y acceso remoto (PPTP de entrada)	Enrutamiento y acceso rem...	Todo
Multiplexor de equilibrio de carga de software (TCP-In)	Equilibrador de carga de sof...	Todo
Escritorio remoto - instantánea (TCP de entrada)	Escritorio remoto	Todo
Escritorio remoto - Modo usuario (TCP de entrada)	Escritorio remoto	Todo
Escritorio remoto - Modo usuario (UDP de entrada)	Escritorio remoto	Todo
Escritorio remoto (TCP-WS-in)	Escritorio remoto (WebSoc...	Todo
Escritorio remoto (TCP-WSS de entrada)	Escritorio remoto (WebSoc...	Todo
Detección de SSDP de Transmitir en dispositivo (UDP entrante)	Funcionalidad de transmitir ...	Público
Eventos UPnP de Transmitir en dispositivo (TCP entrante)	Funcionalidad de transmitir ...	Público
Funcionalidad de transmitir en dispositivo (qWave-TCP de entrada)	Funcionalidad de transmitir ...	Priva...
Funcionalidad de transmitir en dispositivo (qWave-UDP de entrada)	Funcionalidad de transmitir ...	Priva...
Servidor de streaming de Transmitir en dispositivo (streaming HTT...)	Funcionalidad de transmitir ...	Público
Servidor de streaming de Transmitir en dispositivo (streaming HTT...)	Funcionalidad de transmitir ...	Privado
Servidor de streaming de Transmitir en dispositivo (streaming HTT...)	Funcionalidad de transmitir ...	Domi...
Servidor de streaming de Transmitir en dispositivo (streaming RTC...)	Funcionalidad de transmitir ...	Domi...
Servidor de streaming de Transmitir en dispositivo (streaming RTC...)	Funcionalidad de transmitir ...	Público
Servidor de streaming de Transmitir en dispositivo (streaming RTC...)	Funcionalidad de transmitir ...	Privado
Servidor de streaming de Transmitir en dispositivo (streaming RTS...)	Funcionalidad de transmitir ...	Privado
Servidor de streaming de Transmitir en dispositivo (streaming RTS...)	Funcionalidad de transmitir ...	Domi...

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:
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.

Asistente para nueva regla de entrada X

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

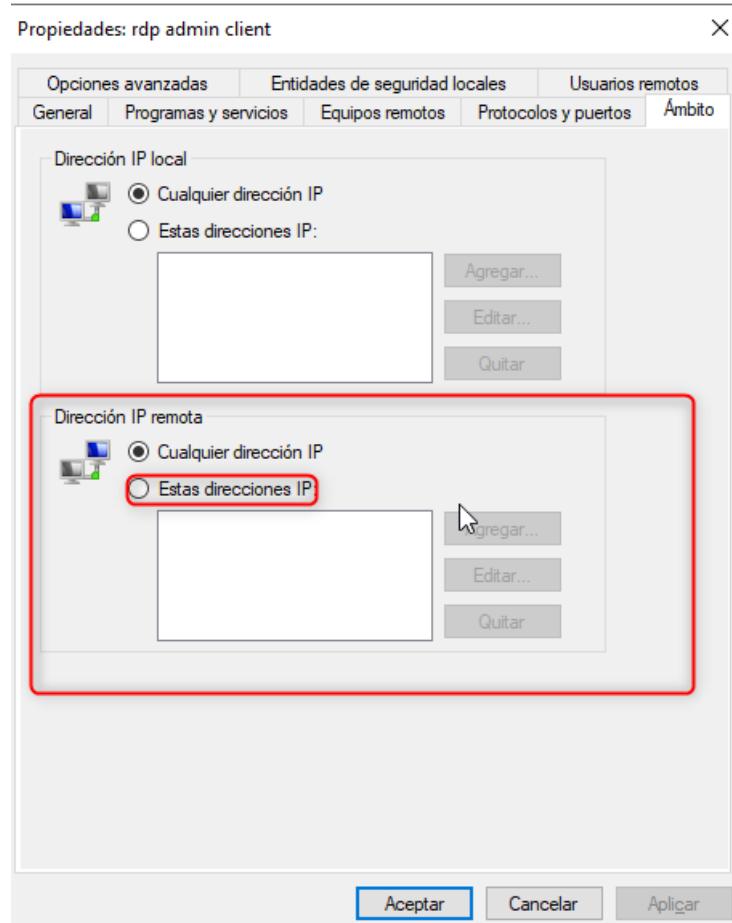
- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre**

Nombre:

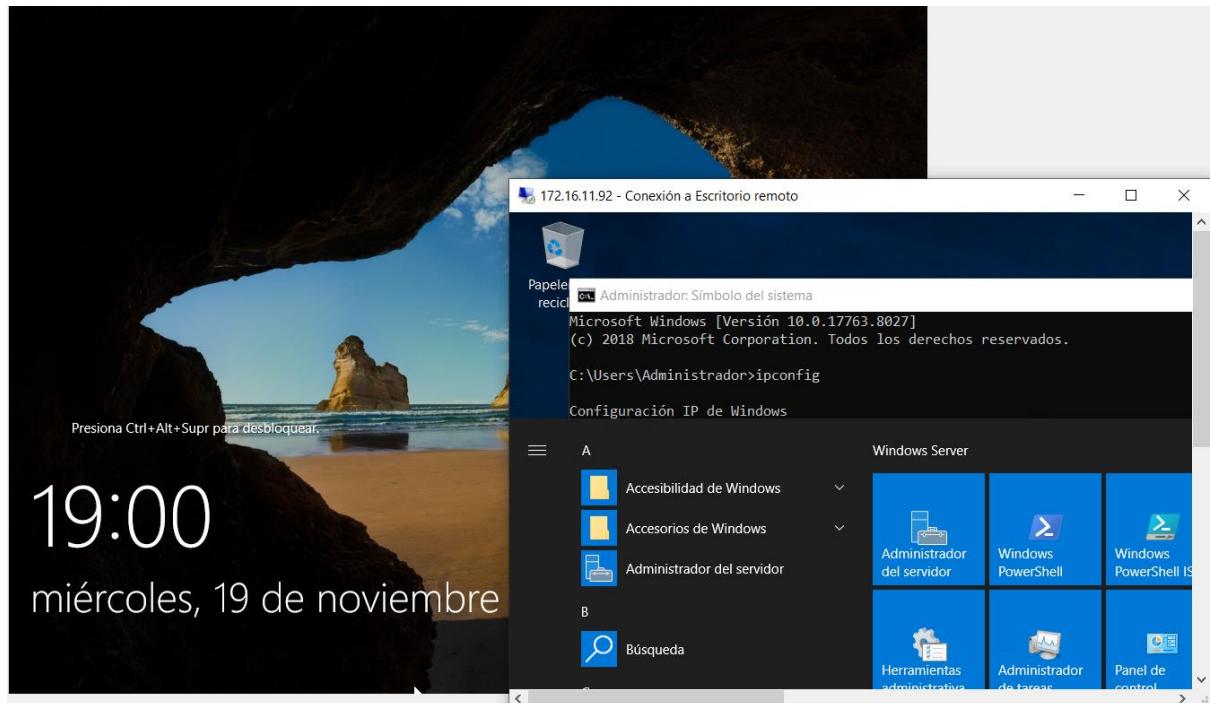
Descripción (opcional):

< Atrás Finalizar Cancelar

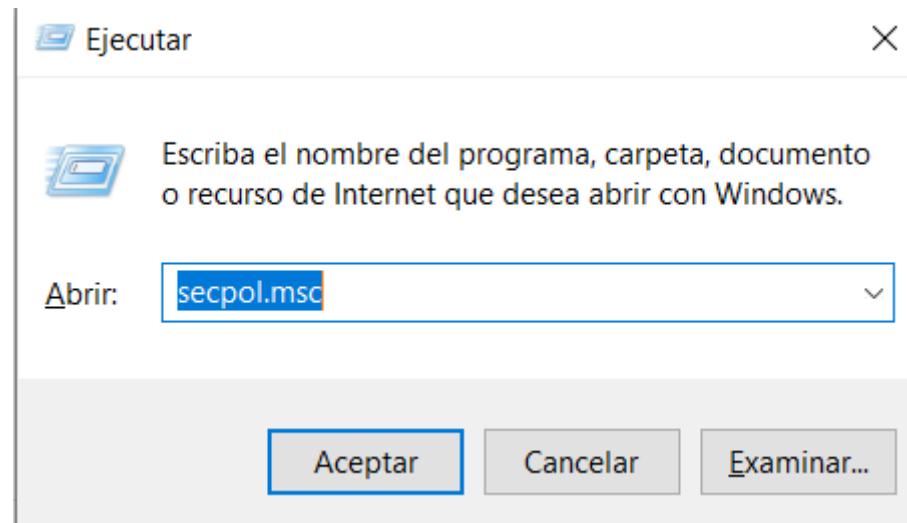
Una vez creada nos saldrá nuestra regla creada le damo doble clic y se nos abrirá la siguiente ventana, en el apartado ámbito en dirección ip remota pondremos la ip desde donde nos vallamos a conectar en este caso la ip seria 172.16.11.92.



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



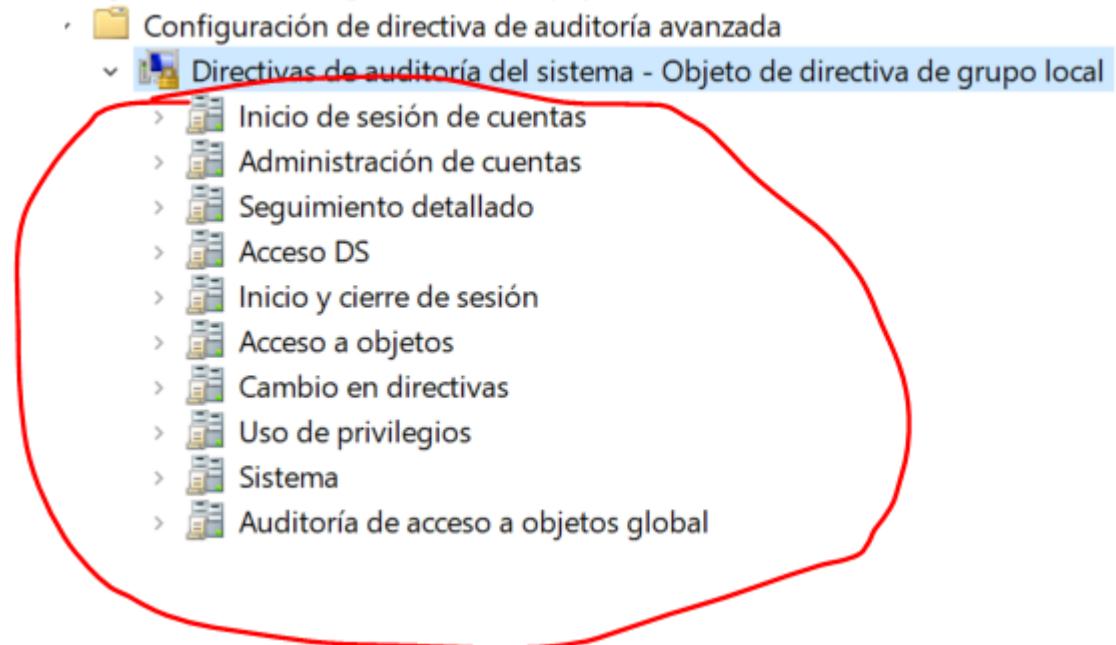
Para acabar nos iremos a la configuración de auditorías, con windows + r se nos abrirá ejecutar y escribimos el comando **secpol.msc**.



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

Nombre	Descripción
Directivas de cuenta	Directivas de bloqueo de contraseña y cuenta
Directivas locales	Directivas de opciones de seguridad, derechos d...
Windows Defender Firewall con seguridad...	Windows Defender Firewall con seguridad avan...
Directivas de Administrador de listas de...	Directivas de grupo de ubicación, ícono y nom...
Directivas de clave pública	
Directivas de restricción de software	
Directivas de control de aplicaciones	Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo loc...	Administración del protocolo de seguridad de l...
Configuración de directiva de auditoría av...	Configuración de directiva de auditoría avanzada

Aquí veremos las políticas de auditorías que podemos configurar.





Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid