Administración de Sistemas Operativos - 1a Evaluación (RA 4 – CE a, b)

Unidad Didáctica 4. Configuración multiusuario centralizada

1. **Busca información sobre métodos de acceso y administración remota de sistema. Además, detalla las diferencias entre los servicios orientados a sesión y los no orientados a sesión.**

**Métodos de acceso**

Los métodos de acceso se refieren a las diferentes formas en que los usuarios o administradores pueden interactuar con un sistema, red, aplicación o dispositivo. Mediante el uso de plantillas de directiva de control de acceso, un administrador puede aplicar la configuración de directiva mediante la asignación de la plantilla directiva a un grupo de usuarios de confianza.

1. **Métodos más comunes de acceso:**
   1. **Autenticación basada en contraseña:** Utilización de una contraseña secreta para verificar la identidad.
   2. **Autenticación de dos factores (2FA):** Combinación de algo que el usuario sabe (contraseña) y algo que el usuario tiene (como un teléfono móvil para recibir un código).
   3. **Autenticación biométrica:** Reconocimiento facial, huellas dactilares, etc.
   4. **Acceso basado en certificados:** Uso de certificados digitales para autenticación sin necesidad de contraseñas.
2. **Acceso remoto:**
   1. **VPN (Red Privada Virtual):** Conexión segura a una red privada desde una ubicación remota.
   2. **SSH (Secure Shell):** Usado principalmente para acceso remoto a servidores Linux/Unix de forma segura.
   3. **RDP (Remote Desktop Protocol):** Protocolo de Microsoft para acceso remoto a escritorios de Windows.

* *¿Qué son las plantillas de directivas de control de acceso?*

Las plantillas de directivas de control de acceso son configuraciones predefinidas que determinan las reglas y permisos que controlan el acceso a recursos y servicios. Se utilizan en entornos como Active Directory (AD) para gestionar quién tiene acceso a qué recursos y con qué permisos.

Las tres fases en las plantillas de directivas son:

1. **Autenticación:** Verificación de la identidad del usuario.
2. **Autorización:** Determinación de los permisos y acceso que se otorgan al usuario una vez autenticado.
3. **Emisión de notificaciones:** Proceso para informar a los administradores o usuarios sobre las decisiones de acceso.

**Administración remota**

En Windows Server, el Administrador del servidor permite realizar tareas de administración en servidores remotos. Esta funcionalidad está habilitada por defecto en Windows Server 2016. Para usarla, es necesario agregar los servidores remotos al grupo de servidores del Administrador del servidor.

1. **Habilitación de la administración remota:**

* En Administrador del servidor, la administración remota está habilitada por defecto, pero debe activarse si se desactiva.
* Se pueden utilizar herramientas como PowerShell y la línea de comandos para habilitarla y configurarla

1. **Comunicaciones remotas:**

* **WinRM (Windows Remote Management):** Utilizado para la administración remota mediante PowerShell.
* **DCOM (Distributed Component Object Model):** Utilizado para servidores con versiones anteriores a Windows Server 2016.
* *¿Cómo habilitar o deshabilitar la administración remota?*

En Windows Server 2016, la administración remota está habilitada por defecto, pero debe configurarse si ha sido deshabilitada. El Administrador del servidor usa WinRM y DCOM para comunicaciones remotas, dependiendo de la versión del servidor remoto.

* **Administración remota con la Interfaz de Windows:**

Para administrar un equipo de forma remota, abra el Administrador del servidor y en la página de Servidores locales, haga clic en el valor de Administración remota. Para habilitar la administración remota, seleccione la opción correspondiente; para deshabilitar, desmarque la casilla de habilitación.

* **Para habilitar la administración remota del Administrador con PowerShell**

Para administrar un equipo de forma remota, abra Windows PowerShell con permisos elevados (haciendo clic derecho y seleccionando "Ejecutar como administrador"). Luego, ejecute el siguiente comando para habilitar las excepciones de firewall necesarias:

**Configure-SMremoting.exe -enable.**

* **Para habilitar la administración remota del Administrador con linea de comandos:**

Para administrar un equipo de forma remota, abra el Símbolo del sistema como administrador y ejecute el comando **%windir%\system32\Configure-SMremoting.exe**. Luego, use uno de los siguientes comandos:

* **- disable:** para deshabilitar la administración remota.
* **- enable:** para habilitar.
* **- get:** para ver la configuración actual

### **Servicios orientados a sesión y no orientados a sesión:**

1. **Servicio orientado a sesión:**

Un servicio orientado a sesión mantiene una conexión activa durante la duración de la sesión de un usuario. La sesión se mantiene hasta que el usuario se desconecta. Como por ejemplo **RDP** o **SSH**

Estas permiten un control interactivo completo del sistema, con la posibilidad de ejecutar aplicaciones y manipular el entorno como si estuvieras físicamente presente

1. **Servicios no orientados a sesión**

Los servicios no orientados a la sesión no mantienen una sesión persistente. Las conexiones son de corta duración y se utilizan principalmente para ejecutar comandos sin necesidad de mantener una conexión constante. Como por ejemplo **WinRM**

**Comparación:**

| **Aspecto** | **Orientado a Sesión** | **No Orientado a Sesión** |
| --- | --- | --- |
| **Persistencia** | Mantiene conexión continua | Cada petición es independiente |
| **Uso de recursos** | Alto (por almacenamiento de sesión) | Bajo |
| **Autenticación** | En el inicio de la sesión | Requiere autenticación por petición |
| **Ejemplos** | SSH, RDP | HTTP, DNS |
| **Escalabilidad** | Menor | Mayor |

1. **Investiga y comenta sobre los distintos tipos de licencias de acceso de clientes.**

Las **Licencias de Acceso de Cliente (CAL)** son licencias que permiten a los usuarios o dispositivos acceder a los servicios proporcionados por un servidor, como los de **Windows Server**. Estas licencias no están incluidas en el sistema operativo del servidor, sino que deben adquirirse por separado. Existen diferentes tipos de CAL según cómo se utiliza el acceso:

### ***Tipos de CAL***

#### ***1. CAL por Usuario (User CAL)***

* **Descripción:** Esta licencia se asigna a un usuario individual, permitiéndole acceder al servidor desde múltiples dispositivos.
* **Casos de uso:**
  + Entornos donde los empleados necesitan acceder al servidor desde distintos dispositivos, como computadoras de oficina, portátiles, tablets y teléfonos.
  + Ideal para empresas con personal móvil o que usan dispositivos personales para trabajar.
* **Ventajas:**
  + Mayor flexibilidad si un usuario utiliza múltiples dispositivos.
* **Limitación:** Cada usuario adicional requiere una CAL.

#### ***2. CAL por Dispositivo (Device CAL)***

* **Descripción:** Se asigna a un dispositivo específico, y cualquier usuario que use este dispositivo puede acceder al servidor.
* **Casos de uso:**
  + Organizaciones donde varios usuarios comparten un mismo dispositivo, como terminales en hospitales, bibliotecas, o áreas de producción.
  + Entornos con dispositivos fijos compartidos por turnos.
* **Ventajas:**
  + Es más rentable en escenarios donde se comparten dispositivos.
* **Limitación:** Si los usuarios necesitan usar múltiples dispositivos, esta opción puede ser menos eficiente.

#### ***3. CAL de Servicios de Escritorio Remoto (RDS CAL)***

* **Descripción:** Específicamente diseñada para acceder a los Servicios de Escritorio Remoto (RDS), permitiendo a los usuarios o dispositivos conectarse a escritorios virtuales o aplicaciones remotas.
* **Tipos disponibles:**
  + **Por usuario:** Ideal si los usuarios acceden al servidor desde múltiples dispositivos.
  + **Por dispositivo:** Mejor para terminales compartidos.
* **Casos de uso:**
  + Empresas que implementan escritorios virtuales.
  + Organizaciones con empleados remotos que acceden al servidor a través de RDP.
* **Requisito adicional:** Necesita un servidor configurado para gestionar las CAL RDS.

#### ***4. CAL de Active Directory Rights Management Services (AD RMS CAL)***

* **Descripción:** Requerida para usar los servicios de protección de información de Active Directory (AD RMS), que permiten aplicar políticas de control de acceso a documentos, correos electrónicos y otros archivos.
* **Casos de uso:**
  + Empresas que manejan información sensible y necesitan asegurar que solo usuarios autorizados puedan acceder a ciertos recursos.
* **Tipos disponibles:**
  + Por usuario.
  + Por dispositivo.

#### ***5. CAL de Multipoint Services***

* **Descripción:** Habilita a múltiples usuarios para compartir un único servidor de manera simultánea. Comúnmente utilizado en aulas, laboratorios y bibliotecas.
* **Casos de uso:**
  + Instituciones educativas que buscan optimizar recursos mediante dispositivos compartidos.

#### ***6. CAL de Exchange Server***

* **Descripción:** Permite a usuarios o dispositivos acceder a los servicios de Exchange Server para correo electrónico, calendarios y tareas compartidas.
* **Casos de uso:**
  + Organizaciones que implementan Exchange Server como solución de correo electrónico.
* **Tipos disponibles:**
  + Por usuario.
  + Por dispositivo.

#### ***7. CAL de SharePoint Server***

* **Descripción:** Habilita el acceso a las funcionalidades de SharePoint, como colaboración en documentos, intranets, y portales.
* **Casos de uso:**
  + Empresas que necesitan colaboración intensiva entre equipos.
* **Opciones adicionales:**
  + SharePoint ofrece modelos alternativos que incluyen CAL estándar y empresarial, dependiendo de las funcionalidades utilizadas

### ***Características Generales de las CAL***

1. ***Modelos de Licenciamiento:***
   * Algunas CAL están disponibles tanto en modalidad **por usuario** como **por dispositivo**, mientras que otras (como las CAL de Multipoint Services) tienen licencias específicas.
2. ***Compatibilidad:***
   * Las CAL deben corresponder a la versión del servidor.
   * Ejemplo: Una CAL para Windows Server 2019 puede ser usada en Windows Server 2016, pero no al revés.
3. ***Duración:***
   * Las CAL estándar no caducan y se pueden usar mientras el servidor esté activo.
   * Las CAL de Servicios de Escritorio Remoto tienen un período de validez y se renuevan automáticamente.
4. ***Consideraciones de Uso:***
   * No cubren software adicional o licencias para aplicaciones como SQL Server o Exchange Server; estas requieren sus propias CAL específicas.
5. **Acceso mediante Terminal Server (Escritorio remoto) / Web a Terminal Server.**

***3.1. Conceptos generales.***

El acceso mediante **Terminal Server** (Escritorio Remoto) es una tecnología clave en los entornos de redes modernas. Permite que los usuarios se conecten a un servidor o equipo remoto para utilizar sus recursos como si estuvieran físicamente presentes. A continuación, exploramos los conceptos fundamentales para entender esta tecnología y su implementación en Windows Server.

### **¿Qué es el Escritorio Remoto?**

El Escritorio Remoto (Remote Desktop Protocol, RDP) es una funcionalidad de Microsoft que permite establecer una conexión gráfica a un equipo remoto a través de la red. Este servicio utiliza el protocolo RDP, que proporciona una experiencia interactiva completa con transmisión de pantalla, entrada de teclado y ratón, y transferencia de archivos.

#### ***Características principales de RDP:***

1. Transmisión gráfica: Permite al cliente ver y controlar el escritorio del servidor.
2. Soporte para periféricos: Incluye funciones como redirección de impresoras, unidades locales y portapapeles.
3. Seguridad: Utiliza cifrado de 128 bits y autenticación para proteger las conexiones.
4. Escalabilidad: Soporta múltiples sesiones de usuario en entornos avanzados.

### **¿Qué es Terminal Server?**

Terminal Server, también conocido como Host de Sesión de Escritorio Remoto, es un rol dentro de Windows Server diseñado para manejar múltiples sesiones remotas simultáneamente. A través de este rol, un servidor actúa como un "hub" al que los usuarios se conectan para ejecutar aplicaciones o acceder a escritorios remotos.

#### ***Ventajas del uso de Terminal Server:***

* Centralización: Las aplicaciones y datos se gestionan desde un único servidor, facilitando la administración.
* Reducción de costos: Disminuye los requisitos de hardware en los equipos cliente.
* Acceso desde cualquier lugar: Permite que los usuarios trabajen de forma remota sin necesidad de estar físicamente presentes en la oficina.

### **¿Cómo funciona la tecnología?**

El proceso se divide en varios componentes y pasos:

1. **Cliente RDP:** Es el software que utiliza el usuario en su dispositivo para conectarse al servidor. En Windows, es la herramienta "Conexión a Escritorio Remoto" (mstsc).
2. **Servidor de Escritorio Remoto**: Es el servidor que proporciona el acceso remoto. Está configurado para aceptar conexiones entrantes, gestionar sesiones y garantizar la seguridad.
3. **Protocolo RDP**: Es el puente que transmite la información entre el cliente y el servidor, optimizando el tráfico de red y la experiencia del usuario.

#### ***Flujo de trabajo típico:***

1. El cliente inicia una solicitud de conexión.
2. El servidor autentica al usuario.
3. Una vez autenticado, se establece una sesión en el servidor.
4. El usuario interactúa con el escritorio remoto como si estuviera en un equipo local.

### **Usos Comunes de Terminal Server**

1. **Ambientes empresariales**:
   * Proveer acceso a software y recursos centralizados.
   * Facilitar el trabajo remoto para empleados distribuidos geográficamente.
2. **Educación**:
   * Ofrecer entornos virtuales para estudiantes.
   * Acceso remoto a laboratorios de software.
3. **Proveedores de servicios**:
   * Proporcionar servicios de alojamiento de aplicaciones (SaaS).
   * Gestión de infraestructura centralizada para clientes.

### **Componentes Clave en Windows Server**

1. **Host de Sesión de Escritorio Remoto (RDSH):**
   * Administra y aloja las sesiones remotas.
   * Es el núcleo de la funcionalidad de Terminal Server.
2. **Gestión de Conexiones RDP:**
   * Supervisa y organiza las conexiones activas.
   * Asegura que las sesiones sean estables y seguras.
3. **Directivas de Grupo (GPO):**
   * Permiten configurar permisos y restricciones, como limitar usuarios o establecer tiempos de inactividad.
4. **Licenciamiento de Escritorio Remoto:**
   * Garantiza que los accesos estén legalmente autorizados mediante licencias CAL (por usuario o dispositivo).

### **Seguridad en el Acceso Remoto**

El acceso remoto introduce riesgos de seguridad, por lo que es esencial implementar medidas robustas:

1. **Autenticación a Nivel de Red (NLA):**

* Obliga a los usuarios a autenticarse antes de iniciar una conexión RDP.

1. **Cifrado de sesiones:**

* Todas las comunicaciones se cifran para proteger los datos transmitidos.

1. **Restricciones de acceso:**

* Se pueden definir listas blancas de IP y usuarios para limitar quién puede conectarse.

1. **Firewall y puertos:**

* El puerto 3389 (usado por RDP) debe estar protegido con reglas específicas.

***3.2. Instalación y configuración (Herramientas, directivas y servicios implicados).***

La instalación y configuración de un entorno de Escritorio Remoto en Windows Server 2016 implica una serie de pasos estructurados que aseguran que los usuarios puedan acceder de manera remota al servidor para utilizar aplicaciones o escritorios completos. En este apartado, se detallan los procesos necesarios, así como las herramientas, directivas, y servicios involucrados.

### **1. Preparativos Previos**

Antes de comenzar con la instalación y configuración, asegúrate de lo siguiente:

#### **Sistema Actualizado**

* Asegúrate de que el servidor cuente con las últimas actualizaciones de seguridad y funcionalidad aplicadas a través de Windows Update. Esto minimiza riesgos de vulnerabilidades y mejora la estabilidad.

#### **Roles Administrativos**

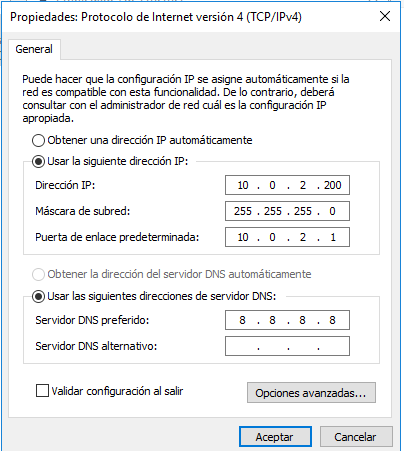
* Utiliza una cuenta con privilegios administrativos para acceder al servidor, ya que la configuración de Escritorio Remoto requiere permisos elevados.

**Conexión de máquinas**

* Asegurate de tener en las dos máquinas “red interna”
* Debemos asegurarnos de que nuestras máquinas hagan la conexión de ping correctamente

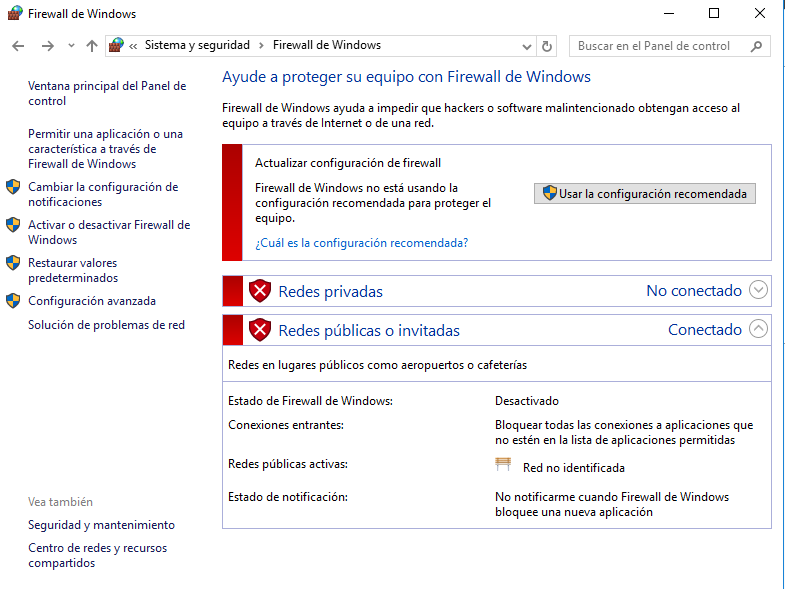
#### **Conexión de Red Estable**

* Configura una IP estática para el servidor:
  + Esto asegura que las configuraciones de red no cambien, manteniendo la consistencia en las conexiones de los clientes remotos.
  + Configura también el DNS preferido (por ejemplo, 8.8.8.8 de Google) y la puerta de enlace predeterminada correcta.



#### **Firewall y Seguridad**

1. **Permitir Conexiones RDP en el Firewall:**
   * Abre el Administrador de Firewall de Windows con Seguridad Avanzada.
   * Crea una regla entrante para habilitar el puerto 3389, que es el predeterminado para Escritorio Remoto:
     + Tipo de regla: Puerto.
     + Protocolo: TCP.
     + Puerto: 3389 (puedes cambiarlo si personalizaste el puerto RDP).
     + Permitir conexiones desde cualquier red de confianza.
   * Guarda y habilita la regla.
2. **Alternativa**: Desactivar el Firewall Si estás en un entorno controlado o realizando pruebas iniciales, puedes desactivar el firewall temporalmente para facilitar la conectividad:
   * Abre el Panel de Control > Sistema y seguridad > Firewall de Windows Defender.
   * Selecciona Activar o desactivar el Firewall de Windows Defender.
   * Desactiva el firewall tanto para redes privadas como públicas.



### **2. Instalación del Rol de Servicios de Escritorio Remoto**

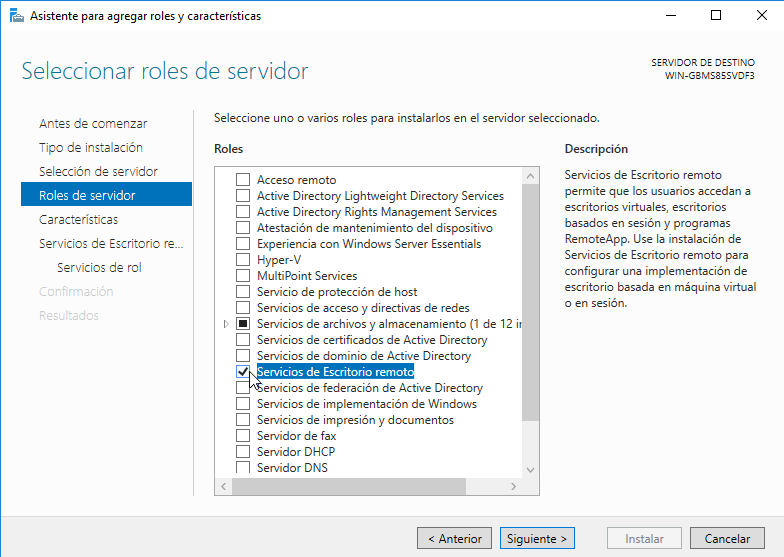
El Host de Sesión de Escritorio Remoto (RDSH) es el componente clave para permitir el acceso remoto. Sigue estos pasos para instalarlo:

#### **Acceder al Administrador del Servidor**

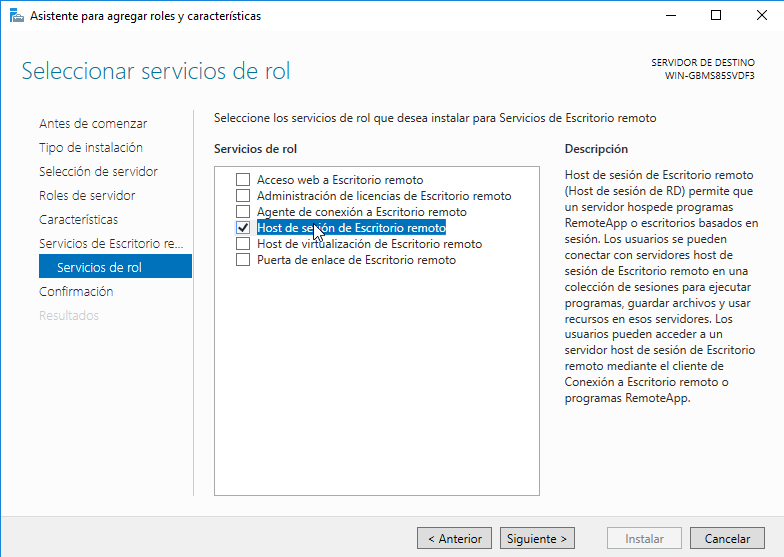
1. Inicia sesión en el servidor y abre el Administrador del Servidor desde la barra de tareas o el menú de inicio.
2. Haz clic en Agregar roles y características para iniciar el asistente.

#### **Agregar el Rol de Servicios de Escritorio Remoto**

1. En el asistente, selecciona Instalación basada en roles o características y elige el servidor objetivo.
2. Marca el rol Servicios de Escritorio Remoto.



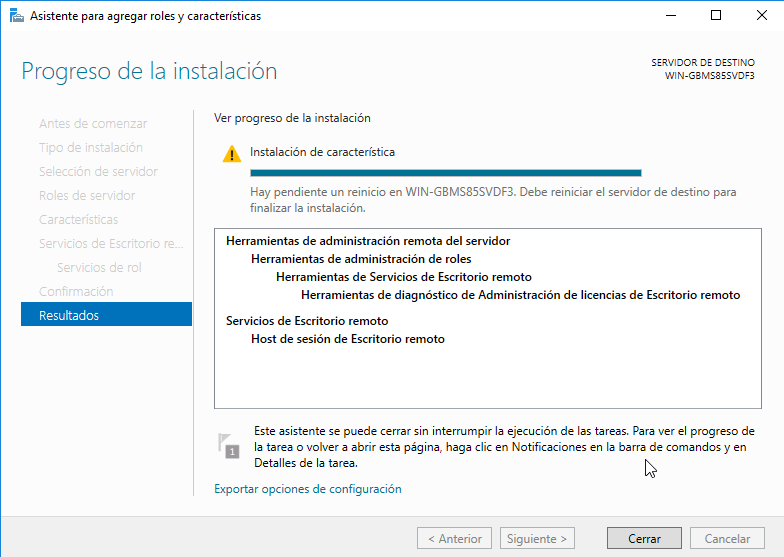
1. Selecciona la característica Host de Sesión de Escritorio Remoto.



1. Sigue las indicaciones y acepta cualquier solicitud de instalación adicional.

#### 

#### **Configuración durante la instalación**

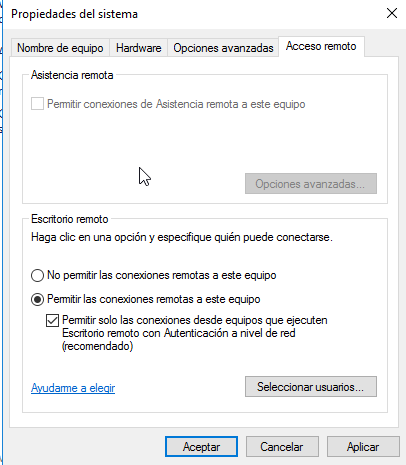
* Reinicio automático: Permite que el servidor se reinicie automáticamente si es necesario.
* Confirmación de roles: Verifica que los roles y características seleccionados sean los correctos antes de proceder.

### **3. Configuración del Entorno de Escritorio Remoto**

Una vez instalado el rol, debes configurar las opciones específicas para que el entorno sea funcional y seguro.

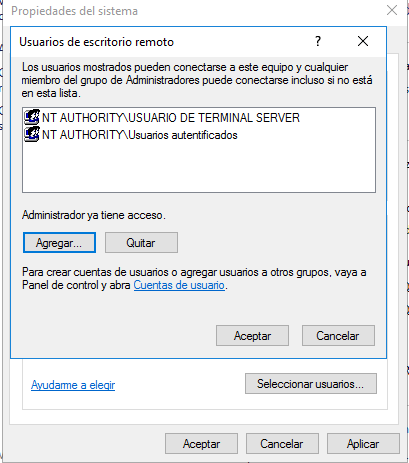
#### **Activar Conexiones Remotas**

1. Ve a Panel de Control > Sistema > Configuración avanzada del sistema.
2. En la pestaña Remoto, selecciona Permitir conexiones remotas a este equipo.
3. Marca la casilla para permitir conexiones solo desde dispositivos que utilicen Autenticación a Nivel de Red (NLA), lo cual mejora la seguridad.

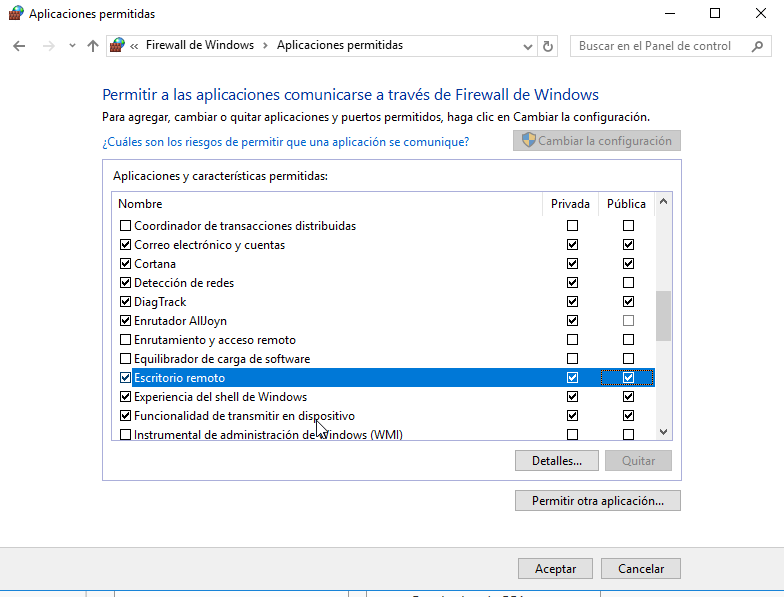


#### **Configurar Usuarios Autorizados**

1. En el mismo menú de configuración remota, haz clic en Seleccionar usuarios.
2. Agrega las cuentas o grupos de usuarios que tendrán acceso al servidor mediante RDP.



3. Asegúrate de habilitar el acceso remoto y permitir conexiones desde dispositivos que usen **RDP**.



### 

### **4. Herramientas y Directivas Implicadas**

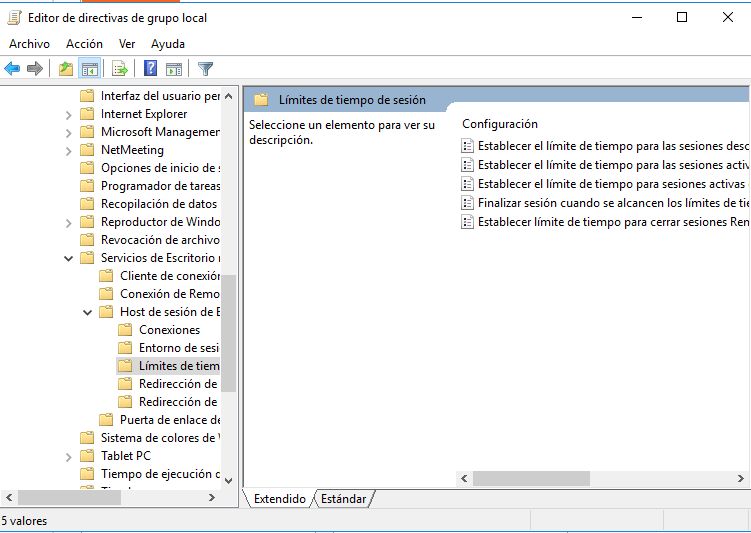
#### **Herramientas de Administración**

1. Administrador del Servidor: Para la instalación de roles y características.
2. Consola de Usuarios y Grupos Locales: Para gestionar usuarios autorizados a acceder al servidor.
3. Editor de Directivas de Grupo (GPO): Herramienta clave para definir políticas de seguridad y acceso.

#### **Directivas de Seguridad**

Configura las siguientes directivas para asegurar el entorno:

1. **Tiempo de inactividad**: Define un tiempo máximo de inactividad antes de desconectar las sesiones.
   * GPO: Configuración de usuario > Plantillas administrativas > Componentes de Windows > Servicios de escritorio remoto > Tiempo de inactividad.
2. **Límite de sesiones**: Establece un número máximo de sesiones simultáneas.
3. **Autenticación**: Obliga a los usuarios a autenticar con NLA antes de establecer conexión.



### **5. Servicios Involucrados**

El correcto funcionamiento de Escritorio Remoto depende de varios servicios:

1. **Servicio de Host de Sesión de Escritorio Remoto (Remote Desktop Session Host - RDSH):**
   1. Este es el servicio principal que permite a los usuarios conectarse al servidor mediante RDP (Remote Desktop Protocol).
   2. Administra las sesiones de usuario, permitiendo acceder a escritorios completos o aplicaciones publicadas.
   3. Asegura que las sesiones sean administradas eficientemente, liberando recursos cuando se desconectan o terminan.
2. **Servicio de Gestión de Conexiones de Escritorio Remoto (Remote Desktop Connection Broker - RDCB):**
   1. Supervisa y controla las conexiones activas y en espera de los usuarios.
   2. Distribuye las conexiones entrantes de forma equilibrada si hay múltiples servidores configurados.
   3. Es clave para entornos con alta disponibilidad, donde se necesitan varios servidores.
3. **Servicio de Redirección de Dispositivos:**
   1. Permite la redirección de recursos del cliente al servidor, como impresoras, unidades USB, y portapapeles.
   2. Es necesario para escenarios donde los usuarios remotos necesitan imprimir o acceder a sus archivos locales desde una sesión remota.
4. **Servicio de Licencias de Escritorio Remoto (Remote Desktop Licensing):**
   1. Gestiona las CAL (Client Access Licenses) necesarias para que usuarios o dispositivos accedan al servidor.
   2. Se asegura de que solo los usuarios con licencias válidas puedan establecer conexiones.
5. **Servicio de Seguridad de Escritorio Remoto:**
   1. Garantiza la autenticación de usuarios y la encriptación de las conexiones RDP para proteger la información.
   2. Asegura el cumplimiento de políticas de seguridad, como el uso de contraseñas fuertes y la autenticación de red (NLA).
6. **Servicio de Web de Acceso Remoto (RD Web Access):**
   1. Permite a los usuarios conectarse a recursos publicados a través de un navegador web.
   2. Ofrece flexibilidad al proporcionar acceso desde dispositivos que no tienen instalada la aplicación de Conexión a Escritorio Remoto.

### **Servicios Complementarios**

1. **Servicio de Red de Escritorio Remoto:**
   * Gestiona las comunicaciones entre el cliente y el servidor.
   * Optimiza el rendimiento en redes de baja velocidad mediante la compresión de datos.
2. **Servicio de Monitorización y Diagnóstico:**
   * Recoge y analiza estadísticas sobre el rendimiento y uso de las sesiones remotas.
   * Es útil para identificar problemas y optimizar el entorno.
3. **Servicio de Publicación de Aplicaciones Remotas (RemoteApp):**
   * Facilita la publicación de aplicaciones específicas en lugar de un escritorio completo.
   * Ayuda a ahorrar recursos y mejorar la experiencia del usuario.

***3.3. Licencias asociadas.***

Las **Licencias de Acceso de Cliente (CAL)** son fundamentales para el funcionamiento de los servicios de **Escritorio Remoto en Windows Server 2016.** Estas licencias permiten que los usuarios o dispositivos se conecten legalmente al servidor para acceder a sus recursos, ya sea para usar aplicaciones o escritorios completos de forma remota. A continuación, te proporciono una explicación más profunda sobre qué son las CAL, los tipos disponibles, cómo se gestionan y adquieren, y otros detalles relevantes para su implementación.

### **Concepto de Licencias en Escritorio Remoto**

El sistema de Licencias de Acceso de Cliente (CAL) es el mecanismo de Microsoft que regula el acceso de los usuarios o dispositivos a los servicios de Escritorio Remoto. Las CAL son necesarias para cumplir con la legislación de uso de software de Microsoft, y cada usuario o dispositivo que se conecta debe contar con una licencia válida.

#### **¿Por qué son necesarias las CAL?**

El propósito de las CAL es asegurar que cada conexión a un servidor esté correctamente registrada y licenciada. A través de este sistema, Microsoft garantiza que los usuarios o dispositivos que se conectan a sus productos no infringen sus términos de uso. Si bien el servidor y los servicios de Escritorio Remoto pueden ser instalados sin las CAL, los usuarios no podrán realizar conexiones sin que las licencias estén correctamente asignadas.

### **Tipos de Licencias CAL**

Existen dos tipos principales de Licencias de Acceso de Cliente (CAL) que se utilizan para la conexión a Escritorio Remoto: Licencia por Usuario y Licencia por Dispositivo. Ambas opciones tienen ventajas dependiendo del escenario de uso de tu organización.

#### **1. CAL por Usuario:**

* **Definición**: En este modelo, se asigna una licencia a cada usuario que se conectará al servidor, sin importar cuántos dispositivos utilice ese usuario para acceder.
* **Escenario ideal**: Este tipo de licencia es ideal para empresas o entornos donde los empleados acceden a los recursos desde múltiples dispositivos. Por ejemplo, un empleado que se conecta a su escritorio remoto tanto desde su laptop, su teléfono móvil y su PC de escritorio.
* **Ventaja**: Proporciona flexibilidad para los usuarios que necesitan acceder desde varios dispositivos en diferentes ubicaciones.
* **Costo**: Aunque puede ser más costosa a nivel individual, es más adecuada en situaciones donde se requieren múltiples dispositivos por usuario.

#### **2. CAL por Dispositivo:**

* **Definición**: Aquí, se asigna una licencia a cada dispositivo que se conectará al servidor, independientemente de cuántos usuarios utilicen dicho dispositivo.
* **Escenario ideal**: Este modelo es más adecuado para entornos con estaciones de trabajo compartidas, como por ejemplo en bibliotecas, colegios, o áreas donde varios empleados utilizan los mismos equipos de trabajo. En este caso, el número de dispositivos es menor que el número de usuarios.
* **Ventaja**: El costo por dispositivo es generalmente más bajo, y se aprovecha cuando múltiples personas comparten un dispositivo. Ideal para escenarios de uso compartido.
* **Costo**: Más económico para entornos donde el dispositivo se utiliza por varios usuarios, como estaciones de trabajo compartidas o dispositivos de uso público.

### **Gestión y Configuración del Licenciamiento de Escritorio Remoto**

#### **Instalación y Activación del Servidor de Licencias**

Para que las CALs sean efectivas, es necesario configurar un servidor de licencias que administre las conexiones de Escritorio Remoto. El servidor de licencias es el componente que valida si los usuarios o dispositivos están habilitados para conectarse de forma legal.

Una vez que has instalado y configurado el rol de Licencias de Escritorio Remoto en tu servidor, deberás activar el servidor de licencias. Esta activación se realiza mediante la herramienta Administrador de Licencias de Escritorio Remoto que puedes encontrar dentro de las opciones del Administrador del Servidor. Asegúrate de registrar las CAL adquiridas para permitir las conexiones.

### **¿Cómo Adquirir y Gestionar las Licencias CAL?**

Las CALs no están incluidas con la compra de Windows Server; deben adquirirse por separado a través de Microsoft o sus distribuidores autorizados. Dependiendo del número de usuarios o dispositivos que accederán al servidor, se deberá determinar el número total de licencias necesarias.

#### **Costo y Adquisición:**

* **Costo** **de Licencias CAL**: El precio de las CALs puede variar dependiendo de varios factores, incluyendo el tipo de licencia (usuario o dispositivo) y el número de licencias que se adquieran. El precio suele ser más alto por usuario que por dispositivo, pero si tu organización tiene usuarios que necesitan acceso desde varios dispositivos, la CAL por usuario es la opción más conveniente.
* **Acuerdos de Licenciamiento por Volumen**: Para empresas con un número elevado de usuarios o dispositivos, Microsoft ofrece programas de licenciamiento por volumen. Este tipo de acuerdos permite adquirir licencias a precios más reducidos en función del volumen total de la compra.
* **Distribuidores Autorizados**: Las CALs deben ser adquiridas a través de distribuidores autorizados o directamente desde Microsoft, a fin de asegurar que las licencias sean legítimas.

#### **Comprobación de Licencias y Cumplimiento:**

Una vez adquiridas las licencias, es importante realizar una verificación periódica para asegurarse de que todas las CALs estén correctamente registradas y asignadas. Esto se realiza en el Administrador de Licencias de Escritorio Remoto, donde puedes consultar el número de licencias activas y asegurarte de que no hay problemas de sobrecarga o violaciones de licencia.

El servidor de licencias también te alertará si hay alguna licencia expirada o si el número de usuarios o dispositivos supera el número de licencias disponibles.

### **Consecuencias de No Tener Licencias Adecuadas**

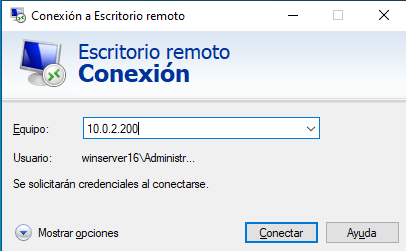
Es fundamental que todas las conexiones a Escritorio Remoto sean cubiertas por las licencias correspondientes. Microsoft realiza auditorías de licencias, y si se descubre que no se dispone de las CAL adecuadas, pueden surgir penalizaciones o incluso el corte del servicio de Escritorio Remoto. Además, no cumplir con las normativas de licenciamiento puede resultar en problemas legales para la organización.

***3.4. Prueba de uso.***

Una vez que se haya completado la instalación y configuración de los servicios de Escritorio Remoto en el servidor, es crucial realizar una prueba de uso para verificar que todo esté funcionando correctamente y que el entorno esté listo para ser utilizado por los usuarios finales. Aquí se detalla cómo realizar una prueba de conexión desde un cliente Windows 10, y qué aspectos validar para asegurar que el servicio esté configurado correctamente.

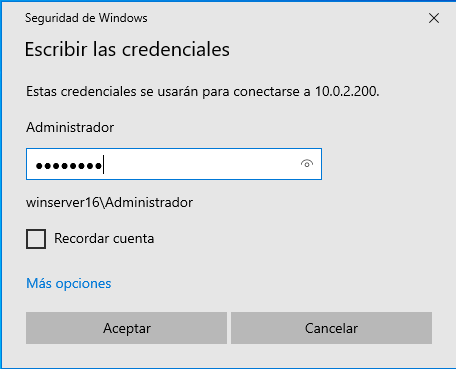
#### **Conexión desde el Cliente Windows 10**

1. **Abrir Conexión a Escritorio Remoto (mstsc) en el Cliente:**
   * En el equipo cliente, abre la aplicación Conexión a Escritorio Remoto (mstsc).
   * Puedes hacerlo buscando "mstsc" en el menú de inicio o ejecutando el comando mstsc desde la ventana de ejecución (presionando Win + R).
2. **Introducir la IP o el nombre del servidor:**
   * En la ventana de Conexión a Escritorio Remoto, en el campo de Nombre del equipo, introduce la IP estática del servidor al que deseas conectar o el nombre del servidor (en mi caso seria la 10.0.2.200, que es la del servidor).

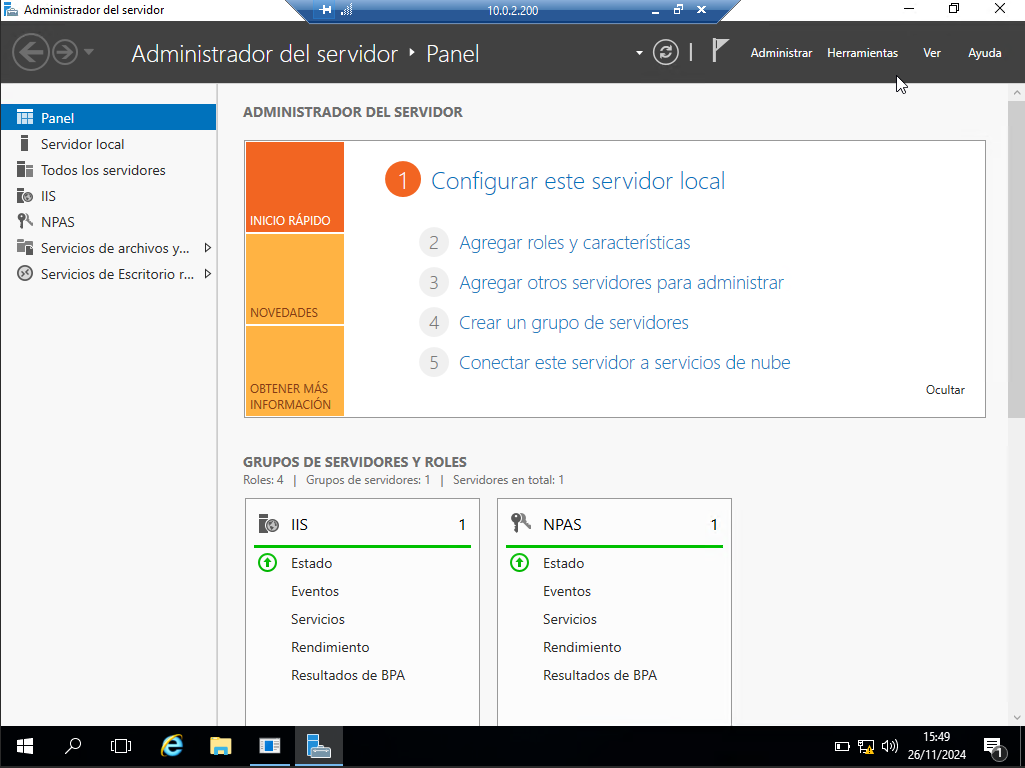


* + Si estás utilizando un nombre, asegúrate de que el cliente Windows 10 pueda resolver correctamente ese nombre, lo cual es especialmente importante si el servidor está en un dominio o en una red de trabajo compartida.

1. **Proporcionar las Credenciales del Usuario:**
   * Una vez que ingreses la IP o el nombre del servidor, haz clic en Conectar. Se abrirá una ventana solicitando las credenciales de inicio de sesión.
   * Debes ingresar el nombre de usuario y la contraseña de un usuario configurado en el servidor, que debe tener privilegios para acceder de forma remota al sistema.



* + Si la autenticación es exitosa, la sesión de Escritorio Remoto se iniciará y podrás ver el escritorio del servidor como si estuvieras trabajando directamente en él.
  + Finalmente como podemos observar en la siguiente imagen, la conexión a partir del escritorio remoto ha sido exitosa, y hemos conseguido acceder.



1. **Acceso mediante RemoteApp.**

**4.1. Conceptos generales.**

* *¿Qué es RemoteApp?*

RemoteApp es una solución flexible y eficiente que permite ejecutar aplicaciones de servidor como si fueran locales en el dispositivo cliente, mejorando la seguridad, la administración y la experiencia del usuario. Su integración con los Servicios de Escritorio Remoto (RDS) de Windows, junto con RDP, hace que sea una opción ideal para entornos de trabajo remotos, virtualización de aplicaciones y administración centralizada de recursos

* *Componentes Implicados en RemoteApp*

1. **Servicios de Escritorio remoto:**

RemoteApp es una característica de los Servicios de Escritorio Remoto (RDS). RDS es un conjunto de tecnologías que permiten el acceso remoto a aplicaciones, escritorios completos y sesiones de servidor. Entre ellas se encuentran: Remote Desktop Session Host, Remote Desktop Web Access, Remote Desktop Gateway, Remote Desktop Licensing

1. **Remote Desktop Protocol (RDP):**

El RDP es un protocolo de comunicación de red desarrollado por Microsoft para permitir la visualización y control de escritorios remotos. En el caso de RemoteApp, el RDP se utiliza para enviar únicamente la interfaz gráfica de la aplicación al cliente, sin que se visualice todo el escritorio del servidor.

1. **Cliente RemoteApp:**

El cliente RemoteApp es un software o una aplicación en el dispositivo cliente que permite que las aplicaciones de RemoteApp se ejecuten de manera local en el cliente, pero ejecutadas en el servidor. Este cliente puede ser un equipo con Windows, macOS, Linux, o incluso un dispositivo móvil

* *¿Cómo funciona RemoteApp?*

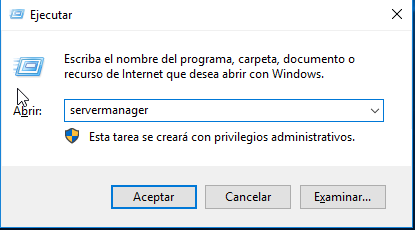
1. **Instalación y publicación de las aplicaciones:** El administrador instala las aplicaciones en un servidor con el rol de Remote Desktop Session Host (RDSH). Luego, las aplicaciones se publican en el servidor utilizando el Administrador de servicios de escritorio remoto.
2. **Acceso del cliente a RemoteApp:** El cliente se conecta al servidor a través del protocolo RDP, pero en lugar de acceder a un escritorio completo, el cliente solo recibe la interfaz gráfica de la aplicación publicada. Esto es transparente para el usuario.
3. **Interacción del usuario:** Una vez que el cliente accede a la aplicación RemoteApp, puede interactuar con ella como si estuviera ejecutándose localmente, pero en realidad, todos los procesos de la aplicación se están ejecutando en el servidor.
4. **Seguridad y acceso remoto:** Si los usuarios están fuera de la red local, el acceso a RemoteApp puede ser habilitado de manera segura a través de un Remote Desktop Gateway.

**4.2. Instalación y configuración (Herramientas, directivas y servicios implicados).**

**Pasos para la Instalación y Configuración de RemoteApp**

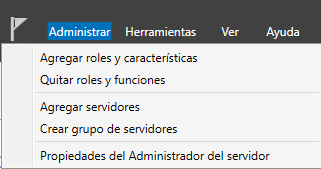
1. **Abrir el administrador del Servidor:**

Haz clic en el icono del Administrador del Servidor en la barra de tareas o presiona Windows + R, escribe servermanager y presiona Enter



1. **Agregar Roles y Características:**

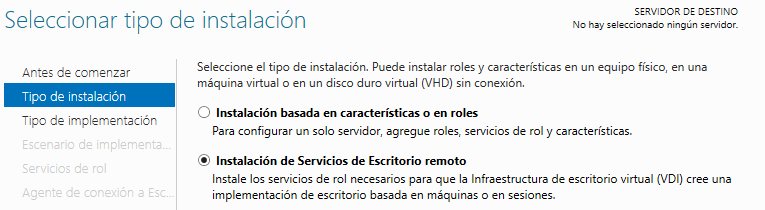
En el panel Administrador del Servidor, selecciona Agregar roles y características.



Se abrirá el asistente de instalación. Haz clic en Siguiente

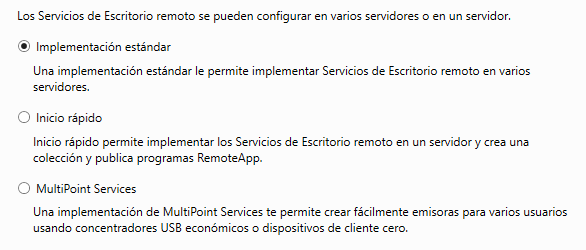
1. **Tipo de instalación:**

Elegiremos la instalación de Servicios de Escritorio Remoto



1. **Tipo de implementación y escenario:**

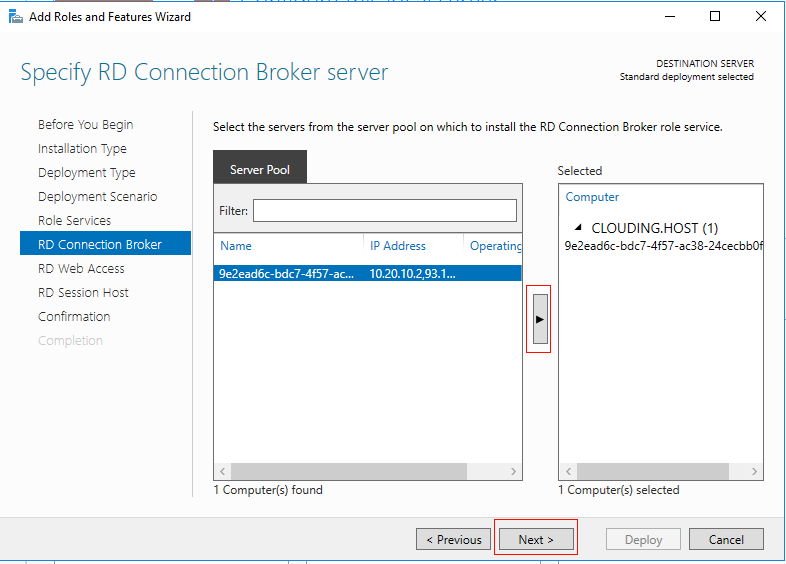
A continuación elegiremos la implementación de tipo estándar:



Seguidamente usaremos la implementación basada en sesión.

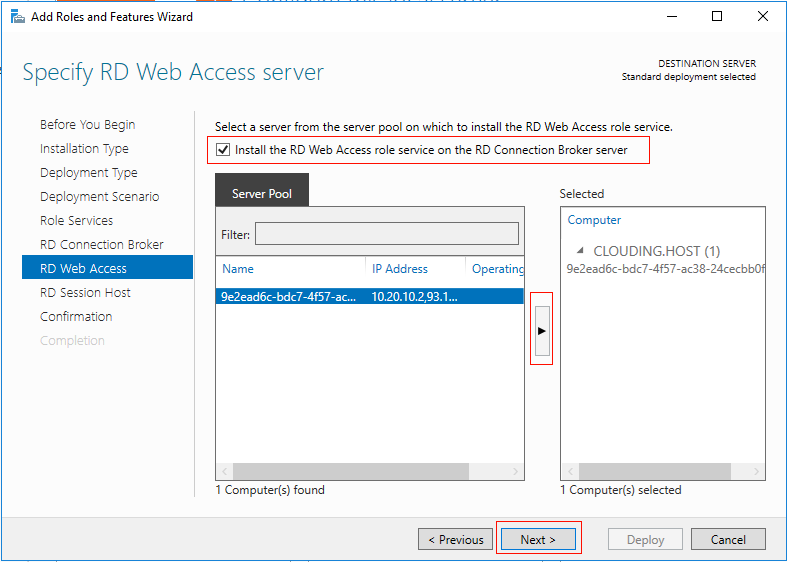
1. **Especificar Servidor**

Para añadir el servidor pulsaremos sobre la flecha para añadir automáticamente la máquina al Equipo



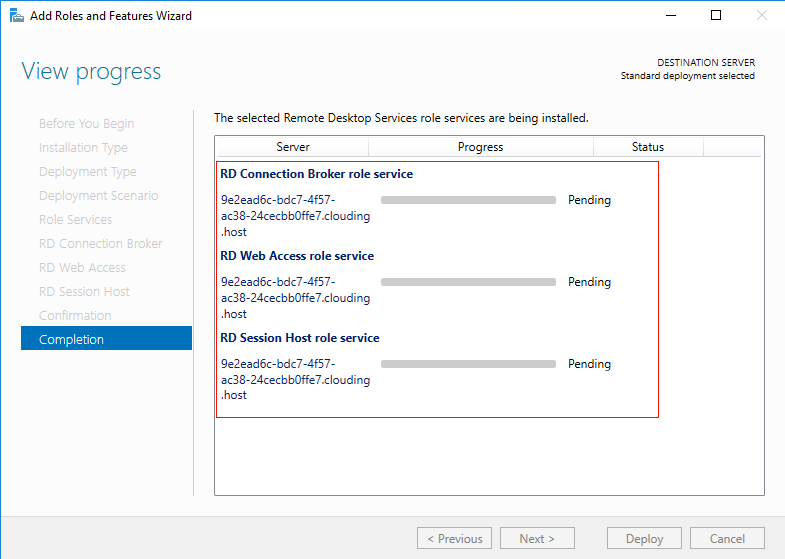
1. **Acceso Web:**

Haz clic en la flecha para añadir nuestro servidor para que instale el rol "RD Web Access Role Service". Adicionalmente, activa el check "Install the RD Web Access role service on the RD Connection Broker Server".



1. **Confirma la instalación:**

El asistente te mostrará un resumen de los servicios seleccionados. Haz clic en Instalar para proceder con la instalación y esperar su finalización

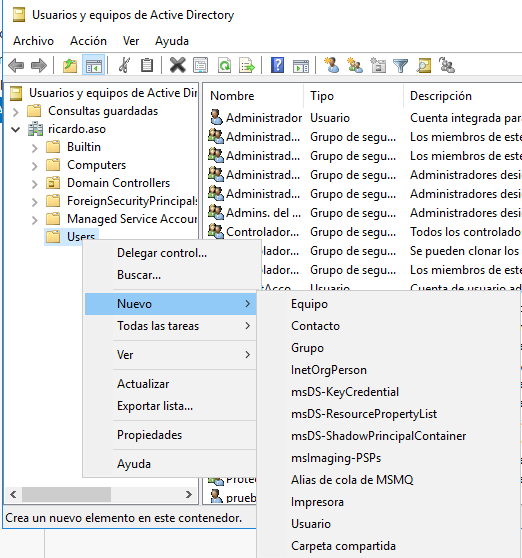


**Crear usuario y grupo en Active Directory**

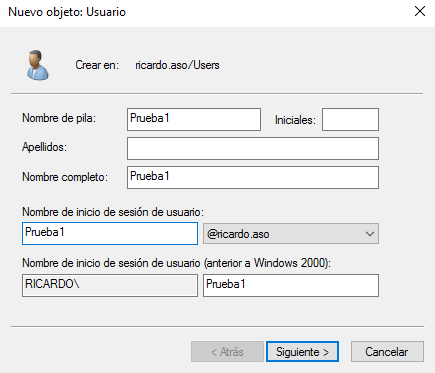
1. **Crear usuario:**

Para llevar un control de los usuarios que pueden acceder a RemoteAPP es importante crear un grupo para su fin en Active Directory, ya que posteriormente se utilizará para la colección en RemoteAPP.

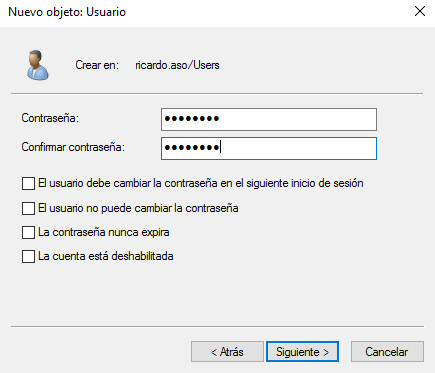
Abre "Usuarios y equipos de Active Directory" y en "Usuarios" haz clic en "Nuevo" - "Usuario".



A este usuario lo llamaremos Prueba1

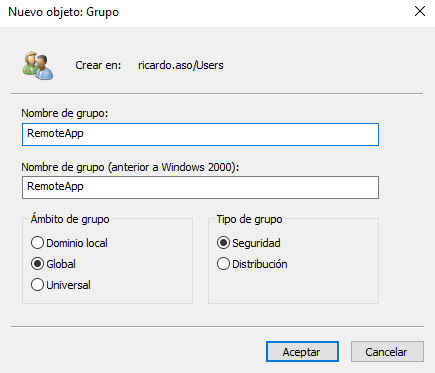


A este usuario deberemos de aplicarle una contraseña para que pueda iniciar sesión más tarde.



1. **Crear grupo:**

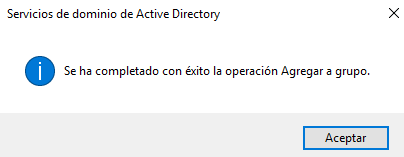
En el mismo apartado donde hemos creado el usuario podemos crear un grupo, a este le llamaremos RemoteApp y añadiremos al usuario Prueba1 creado anteriormente a este grupo.



1. **Añadir usuario a grupo:**

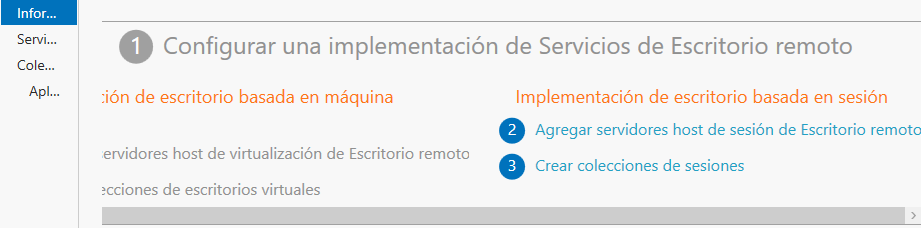
Para que nuestro usuario creado sea añadido seguiremos los siguientes pasos:

* Pulsaremos con el clic derecho sobre el usuario Prueba1
* Pulsaremos sobre la opción de Agregar a un grupo
* Escribiremos el nombre de nuestro grupo creado (RemoteApp) y comprobaremos su nombre
* Una vez lo completamos, podremos ver el siguiente apartado

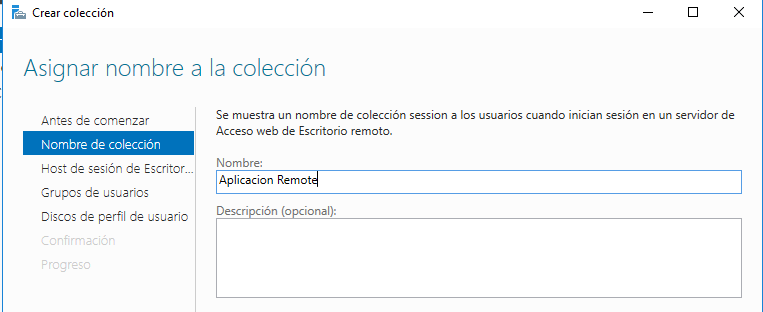


**Configuración para publicar una aplicación**

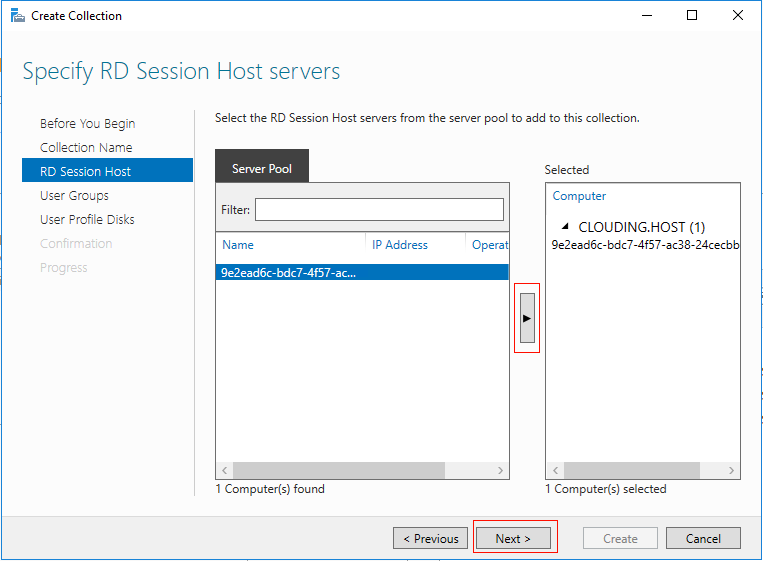
Desde la administración del servidor haz clic en "Servicios de Escritorio Remoto" → Crear colecciones de sesiones:



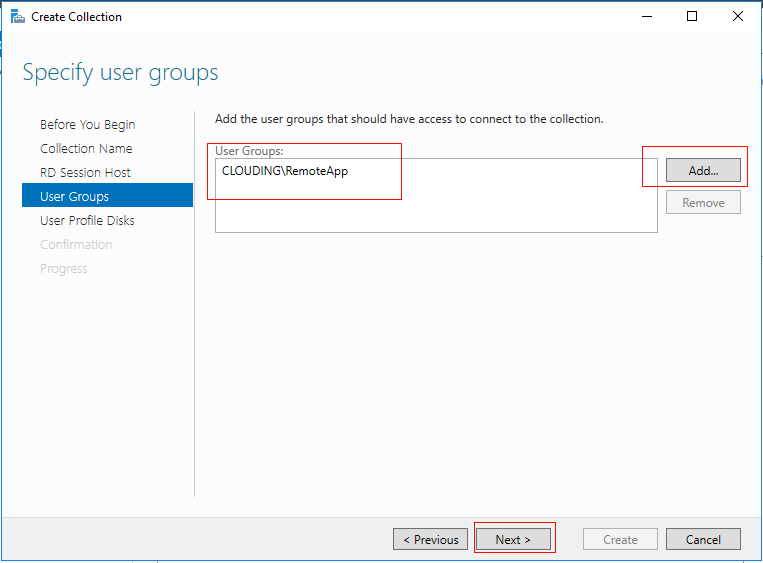
Para el nombre de la conexión podemos usar el que queramos, en nuestro caso usaremos: Aplicación Remote



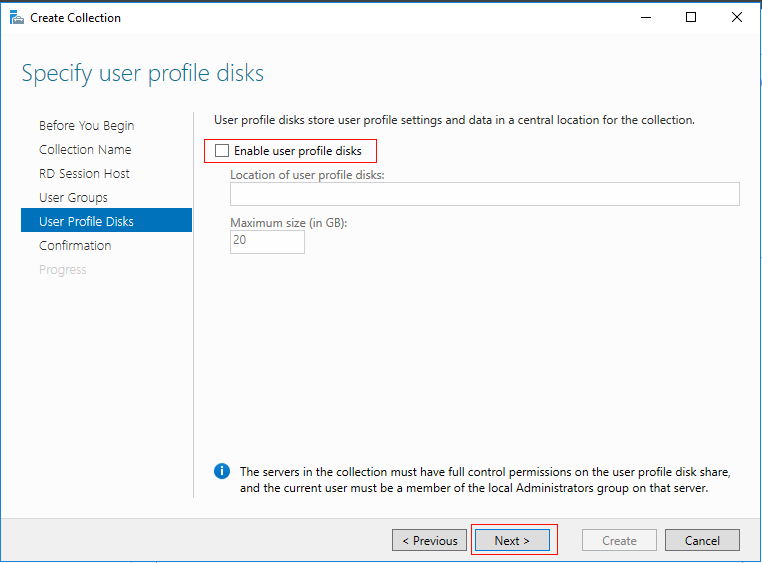
A continuación nos pedirá que seleccionemos el host que vayamos a utilizar, como hemos hecho anteriormente, pulsaremos en la flecha para añadir la dirección.



Añade el grupo de usuarios que hemos creado anteriormente en Active Directory los cuales tendrán acceso a la colección.



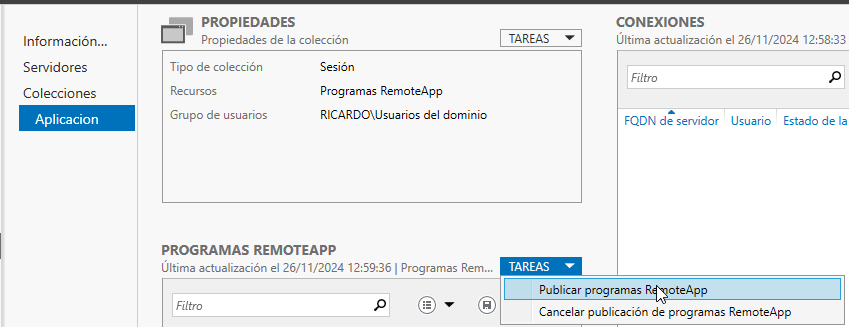
Deshabilita la opción "Enable user profile disks"



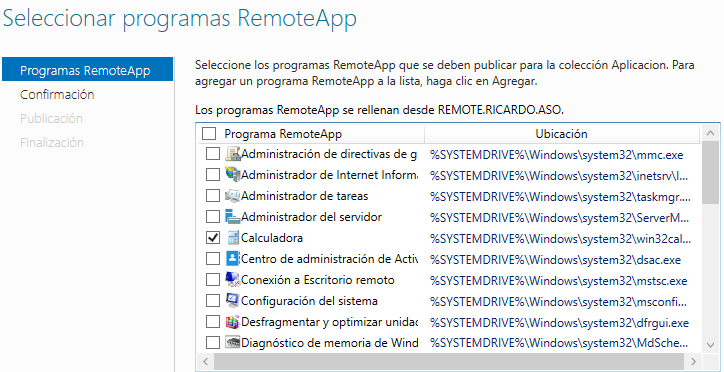
Para terminar, pulsaremos en Create y solo deberemos esperar a que el programa realize la instalacion

**Publicar la Aplicación**

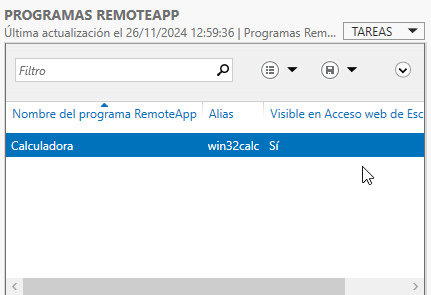
Para finalizar las configuraciones tienes que publicar una aplicación para que los usuarios puedan acceder por RemoteApp. Para ello, desde la administración del servidor haz clic en "Servicios de Escritorio Remoto" y en el menú de la izquierda seleccionamos la colección creada anteriormente. En "PROGRAMAS REMOTEAPP" → "Tareas" → "Publicar programas RemoteApp".



Selecciona el programa que queremos publicar. Para el ejemplo seleccionamos "Calculadora".



Haremos clic en Publicar para finalizar con la publicación y a través del propio menú de Aplicación podremos ver como la aplicación Calculadora se encuentra entre las tareas.



**4.3. Licencias asociadas.**

Cada usuario o dispositivo que se conecta a un servidor de Escritorio Remoto (RDS) necesita una **Licencia de Acceso de Cliente (CAL)**. Estas licencias son gestionadas por un servidor de licencias RDS y se emiten cuando un cliente se conecta al servidor.

* **Período de gracia de 120 días**: Durante este tiempo, no se necesita un servidor de licencias, pero después de este período, los clientes deben tener una CAL válida para conectarse.
* **Tipos de CAL de RDS**:
  1. **CAL por dispositivo**: Asignada a un dispositivo específico. Ideal para entornos donde varios usuarios utilizan el mismo dispositivo en diferentes turnos. Las licencias pueden ser revocadas y se asigna una licencia temporal al primer inicio de sesión.
  2. **CAL por usuario**: Asignada a un usuario específico. Ideal para entornos donde los usuarios utilizan varios dispositivos. Las licencias no pueden ser revocadas y las temporales no existen.
* **Renovación de CAL**: Las CAL permanentes tienen un período de validez que se renueva automáticamente si el cliente sigue utilizando el servicio. Las CAL temporales son válidas por 90 días.
* **Compatibilidad de versiones**: Las CAL deben ser compatibles con la versión de Windows Server que se utiliza. Se pueden usar versiones más nuevas de CAL para versiones anteriores de Windows Server, pero no al revés.
* **Licencias del servidor de licencias**: La versión del servidor de licencias debe ser compatible con la versión de las CAL de RDS. Un servidor de licencias más reciente puede gestionar licencias de versiones anteriores, pero no al revés.

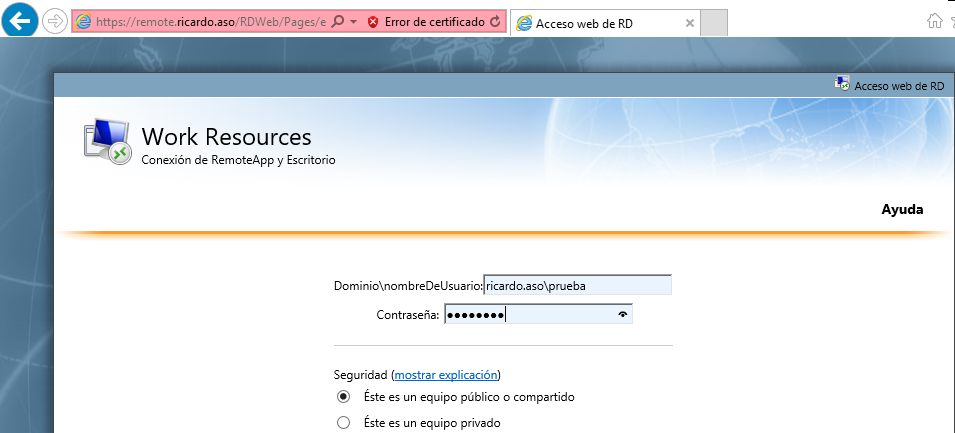
Este sistema asegura que los usuarios o dispositivos tengan acceso adecuado a los recursos de RDS, manteniendo el control sobre las licencias.

**4.4. Prueba de uso.**

**Conectar a RemoteAPP para utilizar la aplicación publicada**

Para conectarnos a RemoteAPP podemos acceder por "https://ip\_pública/rdweb".

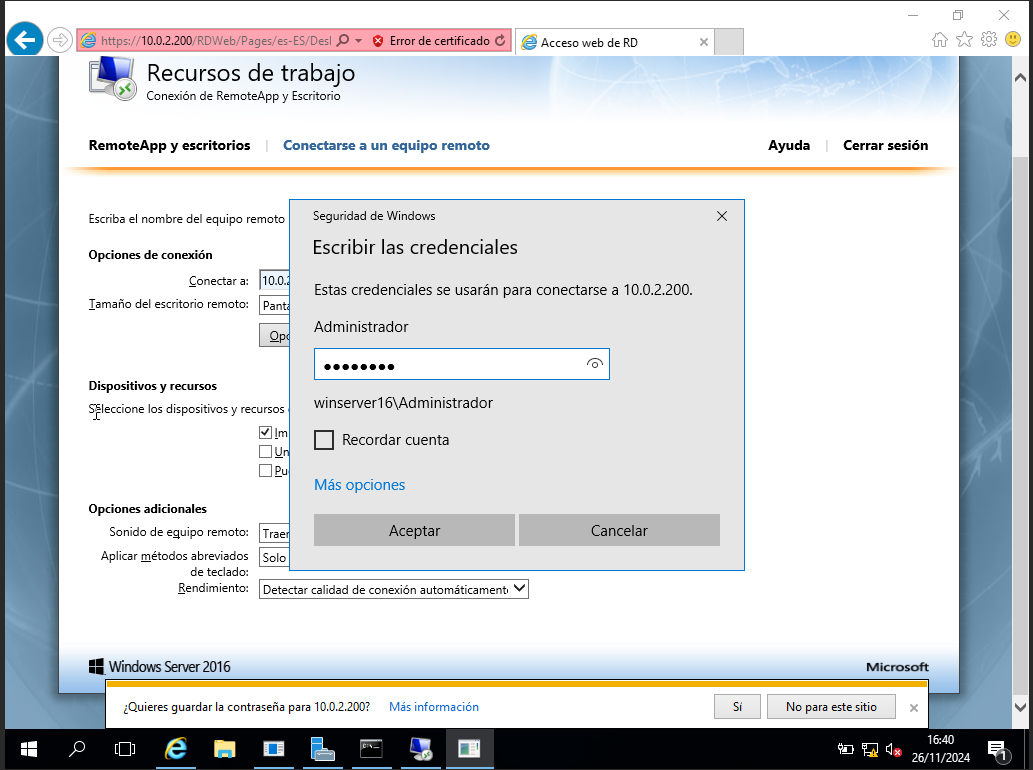
Una vez cargada la URL puedes conectar con el usuario creado anteriormente que has añadido al grupo "RemoteAPP" y hacer clic en "Iniciar Sesión".



A continuación, una vez iniciada la sesión te aparecerán las aplicaciones publicadas y podrás hacer clic en el icono de la aplicación y empezará a cargar la aplicación.



Una vez aquí probaremos la conexión a un equipo remoto, para ello deberemos aplicar la dirección IP del equipo deseado. Primero realizará una conexión a través de red, si no tenemos ningún fallo la propia aplicación nos pedirá que ingresemos las credenciales del usuario a donde nos queremos conectar.



Finalmente, podremos entrar a la máquina cliente por Escritorio Remoto.

