7

GESTIÓN DE ACCESO REMOTO

Mediante el **ACCESO REMOTO** se puede utilizar: un EQUIPO desde → OTRO gracias a:

- **una Red Local**
- o **Internet**

(respetando, siempre, los protocolos correspondientes).

Cuando se utiliza el **ACCESO REMOTO** entre (**2**) **EQUIPOS** (cliente-servidor),

➔ el Usuario del **EQUIPO cliente**

toma el control del **EQUIPO servidor**, de tal forma que puede hacer uso de cualquiera de sus recursos

- *archivos*, - *herramientas* de *configuración*, - *etcétera*).

Para poder trabajar mediante **ACCESO REMOTO** es conveniente que los ordenadores que intervengan… *tengan instaladas* aquellas aplicaciones necesarias para tal fin.

7.1. TERMINALES en MODO texto y MODO GRÁFICO

TERMINALES MODO TEXTO

Los Terminales en **modo texto** son aquellos que se componen de:

a) un **PUERTO SERIE**, → para poder llevar a cabo la comunicación con un equipo informático,

b) un **TECLADO**, → para introducir los datos y

c) un **MONITOR**, → que permita ver los datos alfanuméricos

MODO TEXTO

Los diferentes emuladores de terminales en **modo texto** están basados principalmente en **dos (2) PROTOCOLOS**: **Tel- net** y **SSH**.

• Telnet (*telecommunication network*)

Este **Protocolo de Red** permite utilizar el **ACCESO REMOTO** entre distintos equipos. Cuenta con una estructura (cliente-servidor), especificado en la **RFC 854**.

➔ Utiliza el puerto **23** para realizar la comunicación.

Comenzó a utilizarse en la década de los 60 y en esta época tenía mucho sentido, ya que los equipos eran bastante lentos y los servidores mucho más potentes.

Con el paso de los años, esta herramienta se fue mejorando para poder:

- Administrar un ordenador remoto,
- configurarlo
- y solucionar los diferentes errores.

Al realizar un **Telnet** a un EQUIPO, es necesario:

- un ***Usuario***
- y ***Contraseña*** para **conectarse**.

Si se trabaja con servidores públicos, los nombres que se suelen utilizar son, entre otros, **guest**, **visitor**, **newuser**. Para la ***contraseña***, basta con pulsar la tecla **Intro**.

✗ Uno de sus principales **inconvenientes** es la **seguridad** que ofrece, **ya que no cifra ningún tipo de datos** (***usuarios***, ***contraseñas***).

Para solucionar este **problema** se creó el protocolo **SSH** en 1995.

- Actualmente, se utiliza mayormente para poder acceder a los **Dispositivos de red**, como los *routers*.

- Se trata de un protocolo que, hace uso de unas reglas básicas que permiten:

  - relacionar a un cliente (*pantalla*, *teclado*) con un intérprete de comandos (*disco duro*, *procesador*).

Telnet se utiliza solo en redes locales, porque en este tipo de redes las comunicaciones no se cifran,por tanto, **NO** son seguras y, mediante algún programa *sniffer*, se pueden **DESCIFRAR**.

- También permite realizar conexión como: *root*.

• SSH (secure shell)

Este protocolo se crea con la idea de poder ofrecer una solución al protocolo **TELNET**. De este modo, se puede acceder remotamente a otra MÁQUINA de forma segura, ya que incorpora diferentes mecanismos para cifrar la información.

Los distintos ***usuarios*** y ***contraseñas*** que se utilicen para poder:

enviar y transmitir → señales, lo hacen mediante:

- → **CLAVES** RSA, DSA, o
- → **ALGORITMOS de firma digital**.

También presenta una estructura cliente-servidor,

aunque en este caso, el cliente puede **autenticar** al servidor.

→ Realiza la comunicación mediante el **puerto 22.**

EN ESTE PROTOCOLO PODEMOS DIFERENCIAR ENTRE DOS VERSIONES: SSH-1 SSH-2

- **SSH-1**: Apenas se utiliza en la actualidad porque solo ofrece el cifrado RSA y esto plantea problemas de seguridad.

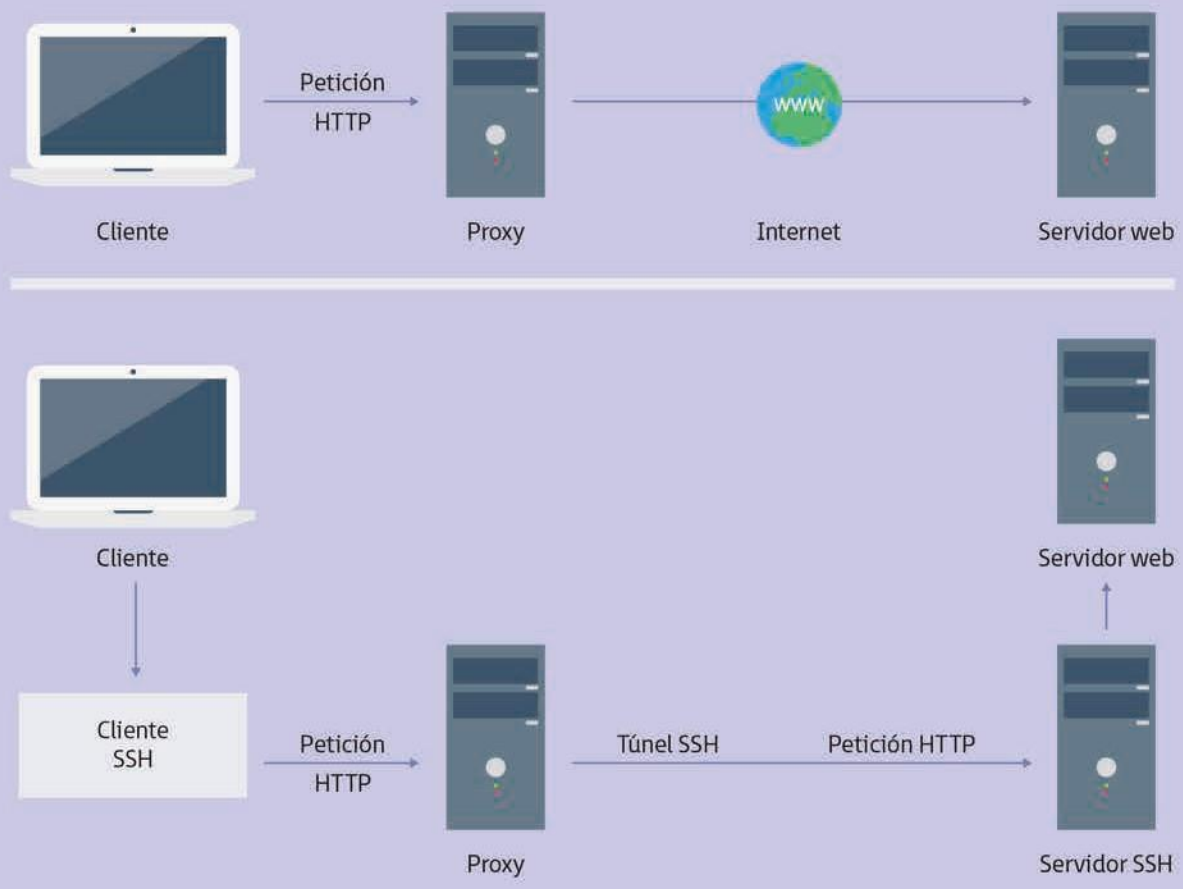
→ Especificada en RFC **4251**.

- **SSH-2**: Aumenta el nivel de seguridad de la versión anterior.

Especificada en RFC **4625**.

Entre sus principales ***características*** se encuentran las siguientes:

- **Autenticación**: se autentifican los usuarios y contraseñas.
- **Confidencialidad**: debido al cifrado de las conexiones.
- **Integridad**: si en el proceso de comunicación el paquete se altera, se puede detectar.
- **Acceso desde dispositivos móviles**: existen clientes y servidores SSH para sistemas operativos móviles.
- ***Tunneling*** **(creación de túneles)**: puede realizar la función de encapsular un protocolo de red dentro de otro.



1. El funcionamiento del SSH se inicia cuando un cliente ABRE: **una conexión TCP (puerto 22).**

Tanto el servidor como el cliente deben negociar la versión de:

- SSH que van a utilizar,
- tipo de cifrado
- y algún dato más.

2. A continuación, el servidor ya puede enviar su **clave pública** al **cliente**.

3. Este debe compararla con una lista de **claves** que tiene.

4. Si es la primera vez que van a comunicarse, hay que indicar:

V si la clave es válida

X o no.

Si es correcta, el cliente genera una **clave aleatoria** que es la que enviará --> al servidor en un paquete cifrado (con un algoritmo elegido junto con su **clave pública**).

5. Llegados a este punto, la comunicación se puede llevar a cabo basándose en el algoritmo simétrico para encriptar que se haya seleccionado.

TERMINALES MODO GRÁFICO

Hay varios programas que ofrecen la posibilidad de manejar un ORDENADOR desde OTRO de forma remota.

Son dispositivos de ***entrada/salida*** que pueden hacer representaciones de gráficos y mostrarlos.

(Se utilizan con bastante frecuencia).

En función de la finalidad de la que se disponga a la hora de conectar un ordenador con un equipo remoto, es posible determinar la siguiente clasificación:

---

a) **ACCESO REMOTO**

b) **CONTROL REMOTO**

a) ACCESO REMOTO

Utiliza varios protocolos de comunicación para poner en marcha el acceso desde

- un **EQUIPO LOCAL** (cliente),

hasta

- el escritorio del servidor de terminales del otro equipo (remoto).

Gracias al **acceso remoto** es posible iniciar

(a distancia) distintas sesiones en diferentes equipos.

Sin embargo, si alguien más utiliza la consola del dispositivo al que se accede, **no se notifica** en la pantalla que otros usuarios la están utilizando.

Entre sus principales **VENTAJAS** se destacan las siguientes:

V Utiliza distintas aplicaciones del servidor.

Cuando ejecuta programas, usa los recursos *hardware* ofrecidos por el servidor, como

- la velocidad y
- memoria RAM.

V Tiene acceso a ficheros o carpetas del servidor.

V Los clientes y servidor que trabajen bajo Windows pueden hacer uso del navegador web para la conexión al servidor.

Aunque también deben cumplir una serie de **requisitos**:

a) El **EQUIPO** REMOTO debe activar un *software* para recibir la conexión de los clientes al iniciar sesión.

b) El **EQUIPO** LOCAL necesita

(vía intranet o internet) al servidor REMOTO (que debe estar encendido).

El cliente necesita *permiso* para

- poder *establecer conexión* con → la máquina remota.

- **Windows** cuenta con una aplicación **Terminal Server** como *software* servidor de diferentes terminales.

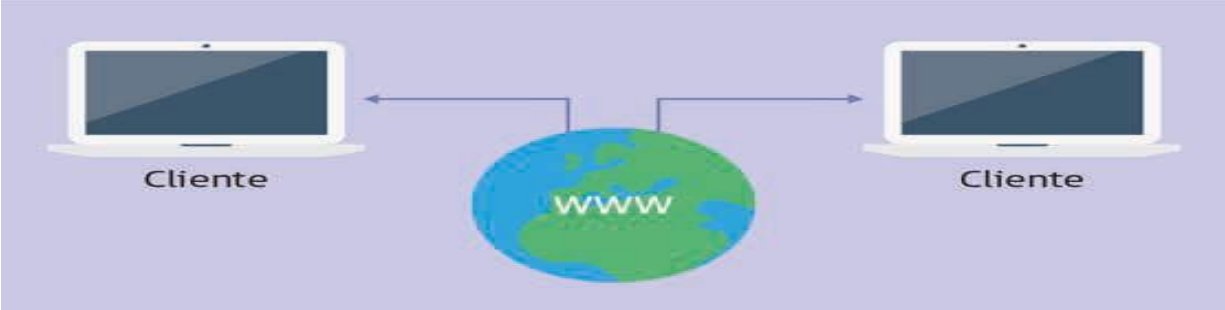
Como conexión a escritorio remoto vía RDP mediante HTTPS para poder conectar desde el cliente.

- **GNU/Linux** cuenta con una aplicación con licencia GPL (X2Go). Se puede descargar desde https://wiki.x2go.org/doku.php/download:start

b) CONTROL REMOTO

El **control remoto** permite el acceso a un **EQUIPO remoto** para tomar el control del mismo.

➔ Por ello, es fundamental que solo se permita el acceso a aquellos usuarios autorizados y de confianza, ya que van a tener acceso a toda la información.



- **Windows denomina al CONTROL REMOTO como ASISTENCIA REMOTA**

a) Se genera una invitación para colaborar en forma de archivo y se envía a la persona con la que se desea conectar.

b) El *software* permanece a la espera de una contestación.

c) Cuando conecta se solicita una *contraseña* y una vez aceptada, se produce la conexión vía intranet o internet.

- **VNC *(VIRTUAL NETWORK COMPUTING)***: permite ver:

el escritorio de un **EQUIPO remoto** (servidor) a través de:

- una pantalla (visor) a través de **intranet** o **internet**. Utilizando los dispositivos de *teclado* y *ratón* se puede controlar al servidor de forma remota.

c) Administración REMOTA

Cada día aumenta la necesidad de tener acceso remoto a los servidores (por ejemplo, de una determinada empresa).

Con esto se pueden realizar las diferentes operaciones para mantenimiento y administración sin necesidad de estar presente en la propia empresa.

Existe un gran número de aplicaciones encargadas de realizar estas tareas y suelen tener en común la utilización de ***front-end***, que se divide en dos tipos:

1. **Aplicaciones que hacen uso de un pequeño programa que se conecta al servidor de la empresa**, la cual lo lleva a cabo para ofrecer el servicio que le permita establecer la conexión del cliente con el EQUIPO que desea controlar.

2. **Aplicaciones basadas en la utilización de una interfaz basada en web**, o lo que es lo mismo, que utilizan protocolo **HTTP** para la conexión y administración del **EQUIPO** REMOTO.

LogMeIn - TeamViewer - Webmin

- **LogMeIn:** utilizado por los sistemas Windows y Apple.

Es necesario instalar la aplicación en el equipo que se desee controlar y, desde el equipo cliente, acceder a la web de la empresa para realizar la administración de manera remota.

- **TeamViewer:**

En este caso, el programa debe estar instalado en los **EQUIPOS** cliente y servidor para su correcto funcionamiento. Es un ***software*** multiplataforma.

- **Webmin:**

También es un ***software*** multiplataforma basado en web que permite la administración remota en sistemas Unix.

7.2. Instalación De un servicio De acceso remoto en línea De comanDos. En un sistema oPerativo Linux

1. **INSTALAR** el programa Remmina desde un **repositorio**, el cual permite conectarse remotamente a otro usuario con VNC.

2. **ACCEDER** al terminal para introducir el comando e instalar el programa VNC: *apt-get install remmina*. Al finalizar la instalación,

3. **ABRIR** el programa para la compartición de escritorio. Una vez abierto, modificar según se quiera para acceder remotamente.

4. **PASAR** a *Configuración las opciones básicas y acceso remoto* en las pestañas correspondientes. Una vez configuradas estas opciones

5. **IR A** otro cliente Linux que será *desde el que se quiere conectar* y

6. abrir el programa Remmina.

7. En el programa de **ACCESO** REMOTO del cliente, seleccionar la opción *Crear nuevo escritorio remoto*, el nombre de la conexión y el **protocolo** VNC. A continuación, solo

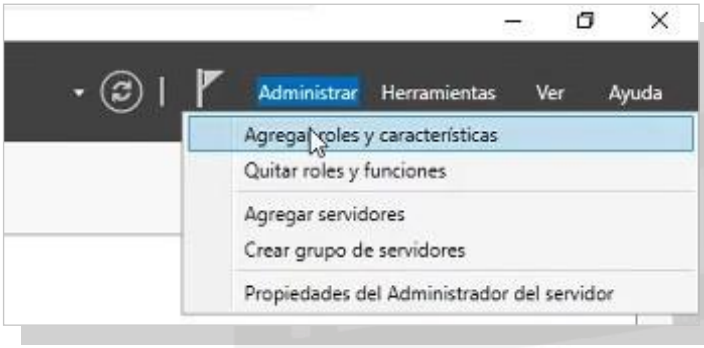
d) INSTALACIÓN DE UN SERVICIO DE ACCESO REMOTO

TERMINALES MODO GRÁFICO

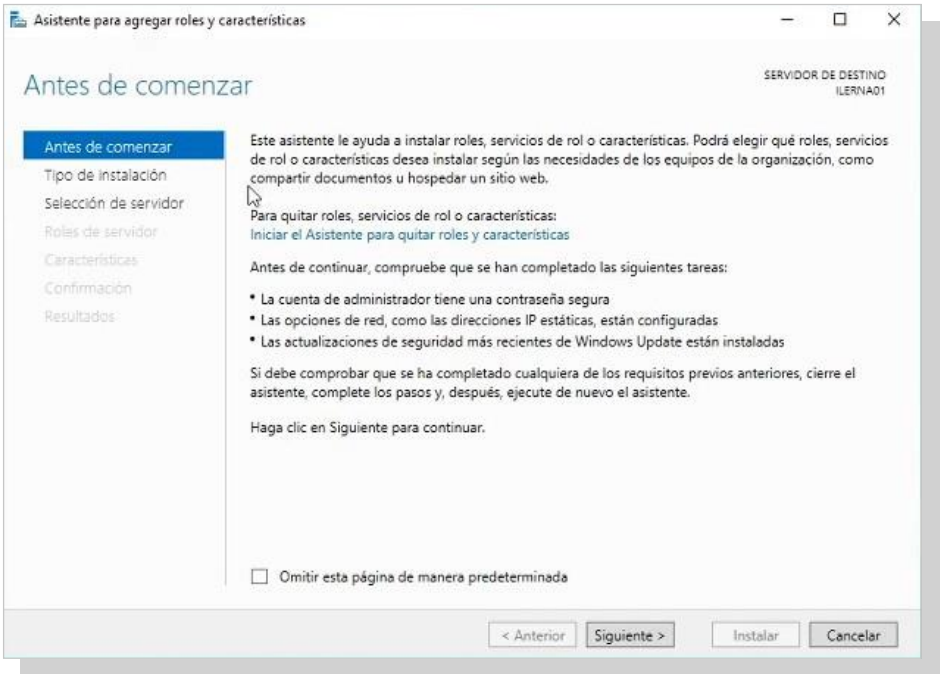
Para llevar a cabo el proceso de **instalación del servidor,** hay que seguir los siguientes **pasos:**

1. **SELECCIONAR** la opción *Inicio/ Administrador del servidor*.

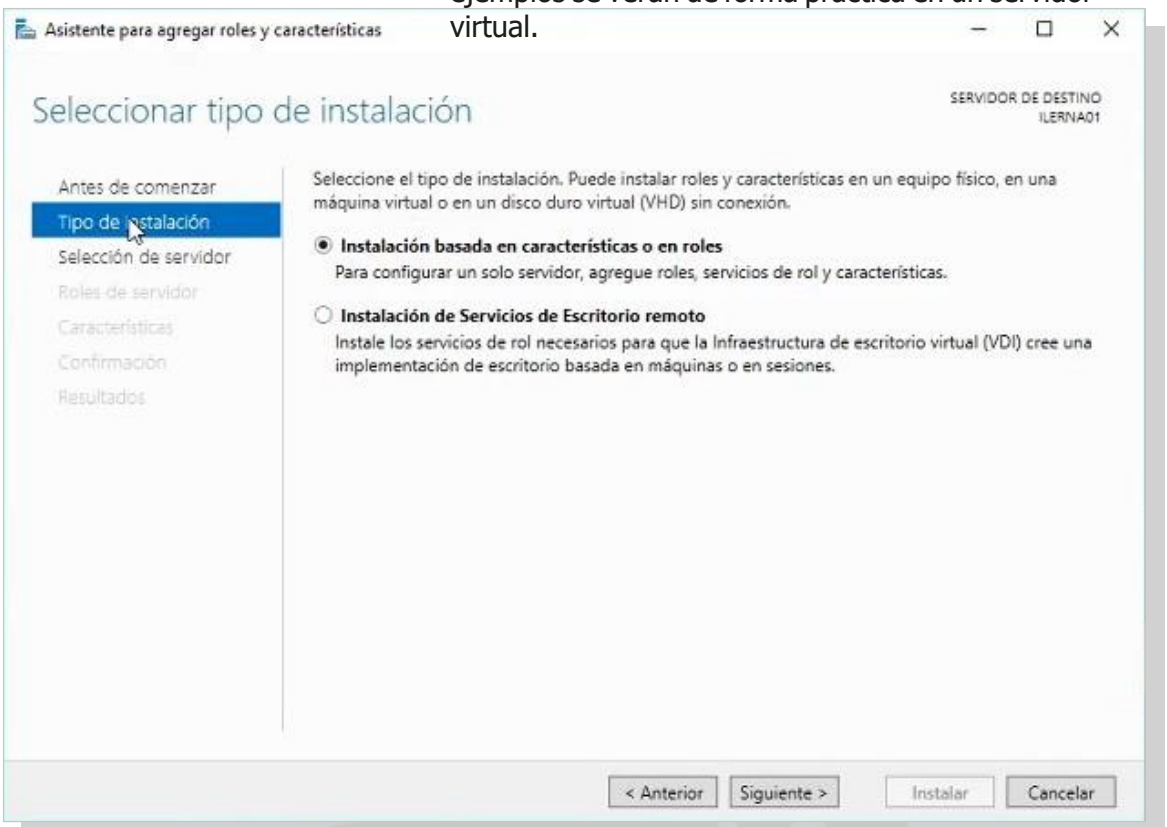
2. En la ventana que aparece, hacer **clic** en *Resumen de agregar roles y características*.



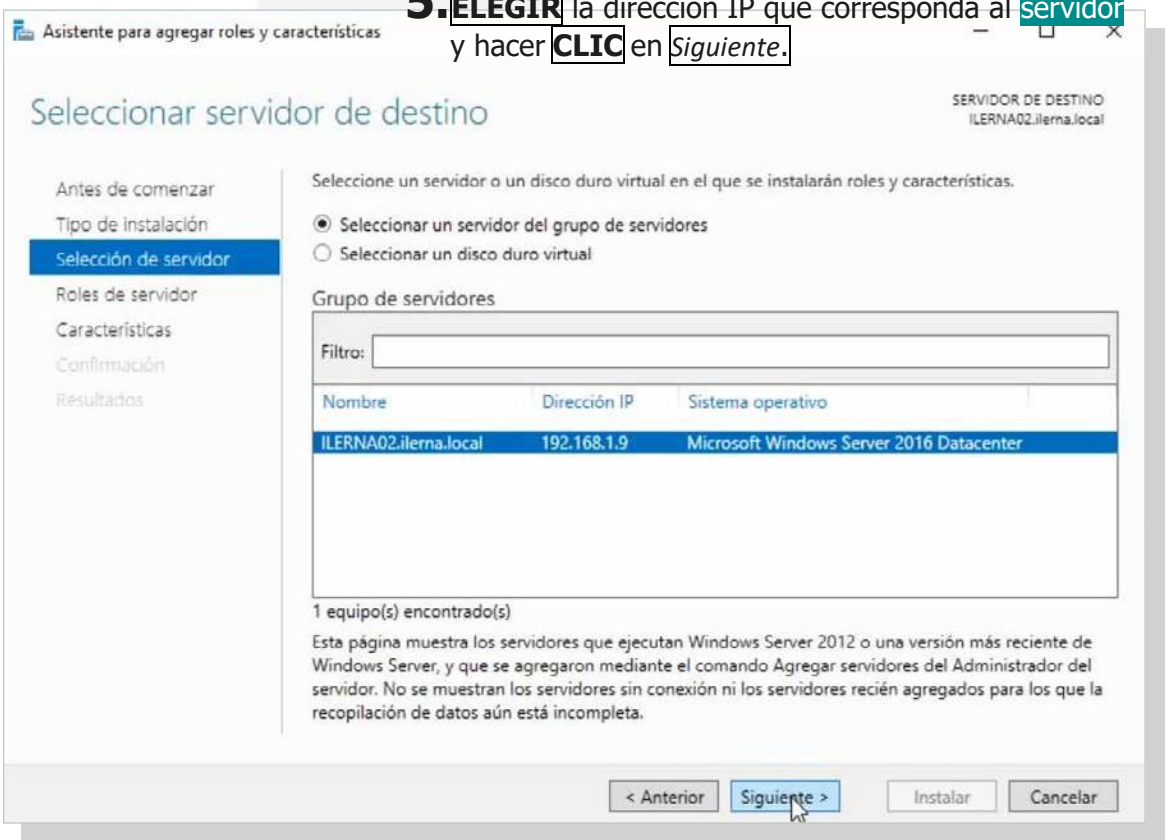
3. Comienza a ejecutarse el asistente para agregar roles. Leer la información que se proporciona y clicar en *Siguiente*.



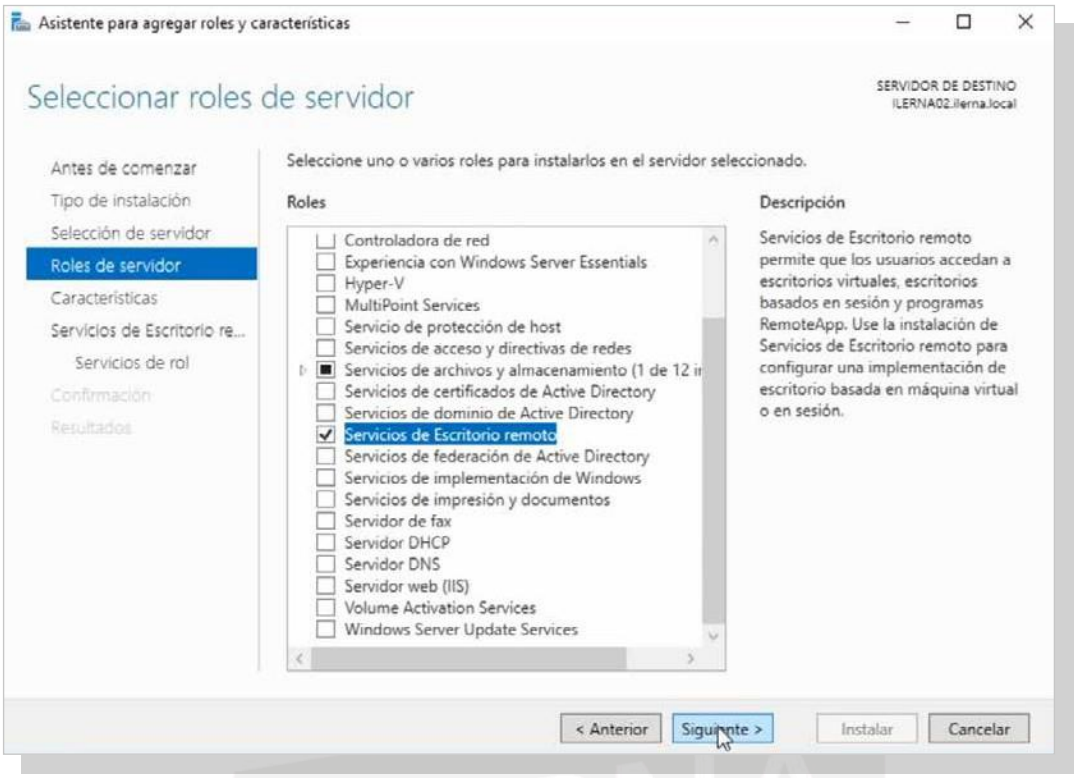
4. ELEGIR la **instalación basada en roles**, ya que estos ejemplos se verán de forma práctica en un servidor virtual.



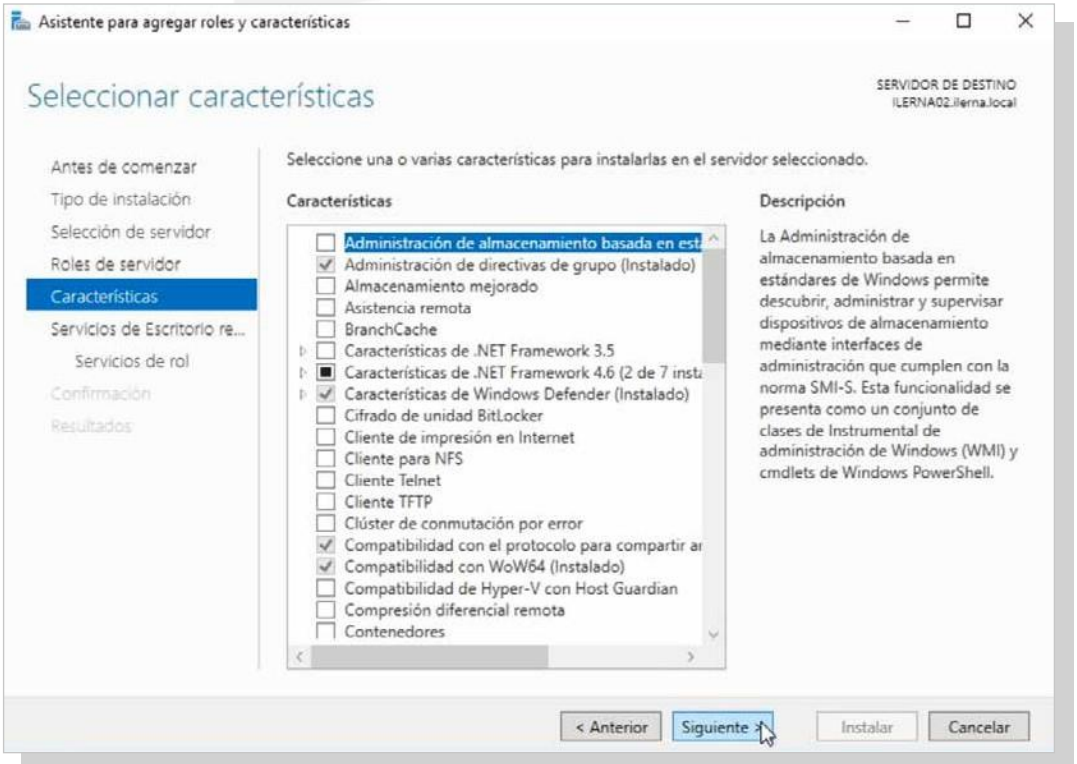
5. **ELEGIR** la dirección IP que corresponda al servidor y hacer **CLIC** en *Siguiente*.



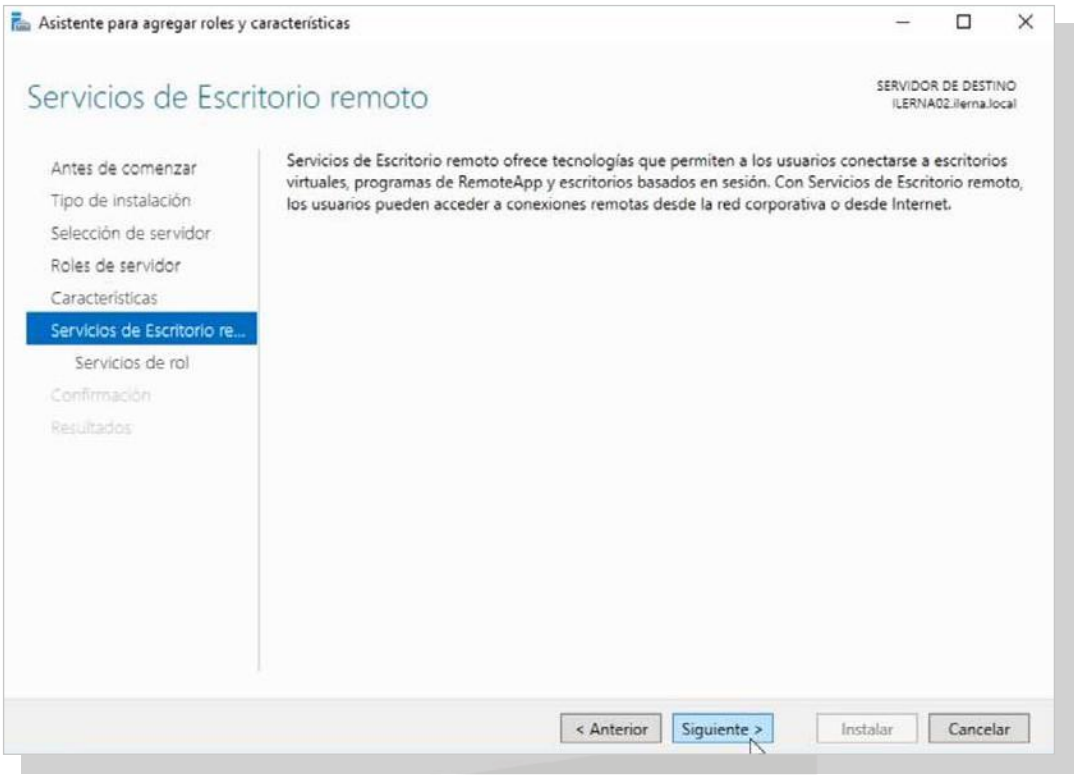
6. En la ventana Seleccionar roles del servidor, marcar la opción *Terminal services* (servicios de escritorio remoto). Hacer clic en ***SIGUIENTE***.



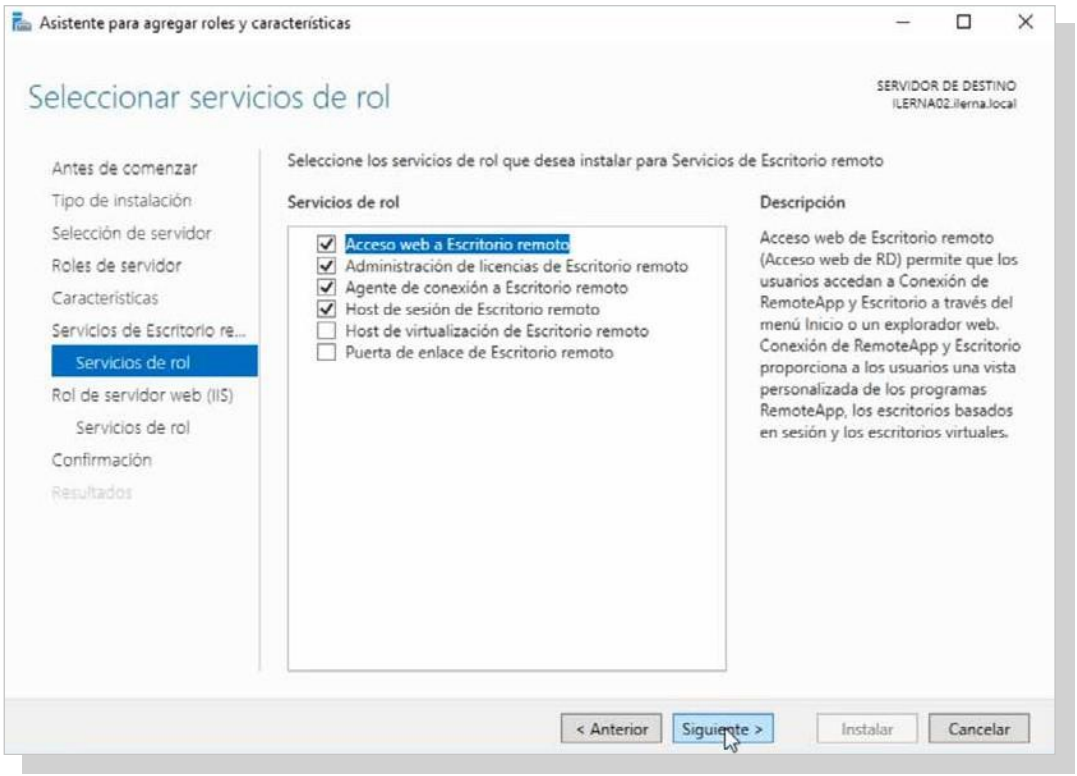
7. La ventana *Terminal services* ofrece las diferentes características del servicio. Hacer clic en *Siguiente.*



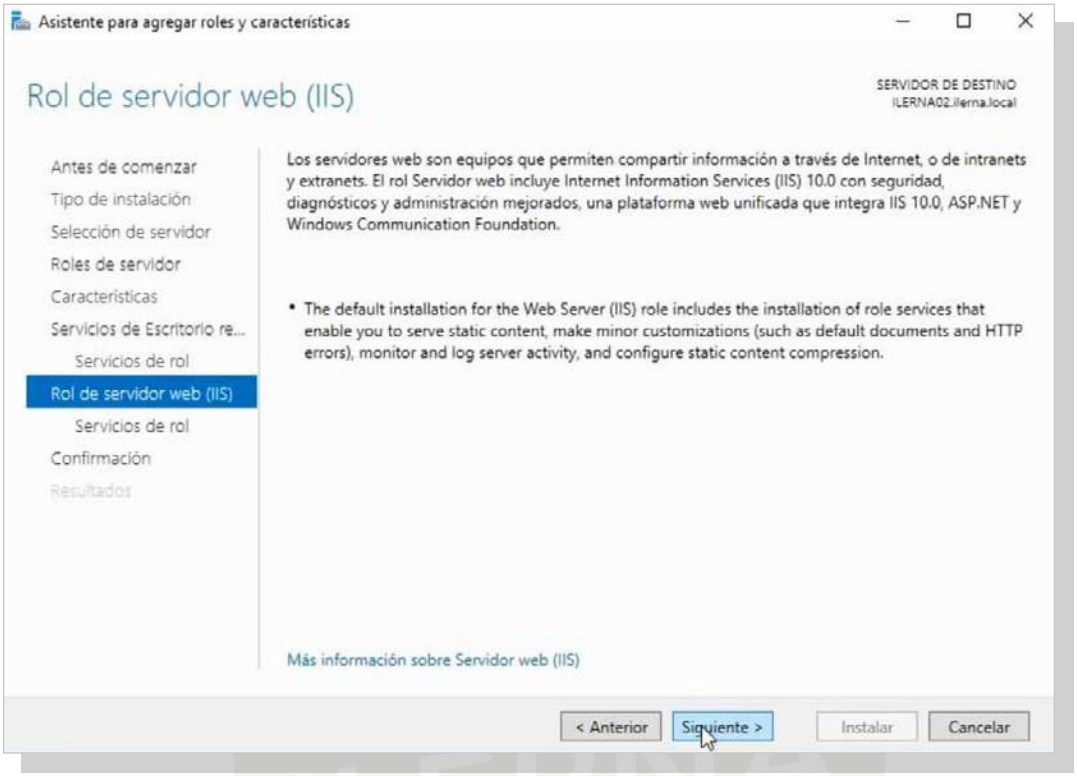
8. Se muestra una pantalla con una descripción del servicio. Leer atentamente y hacer clic en *Siguiente.*



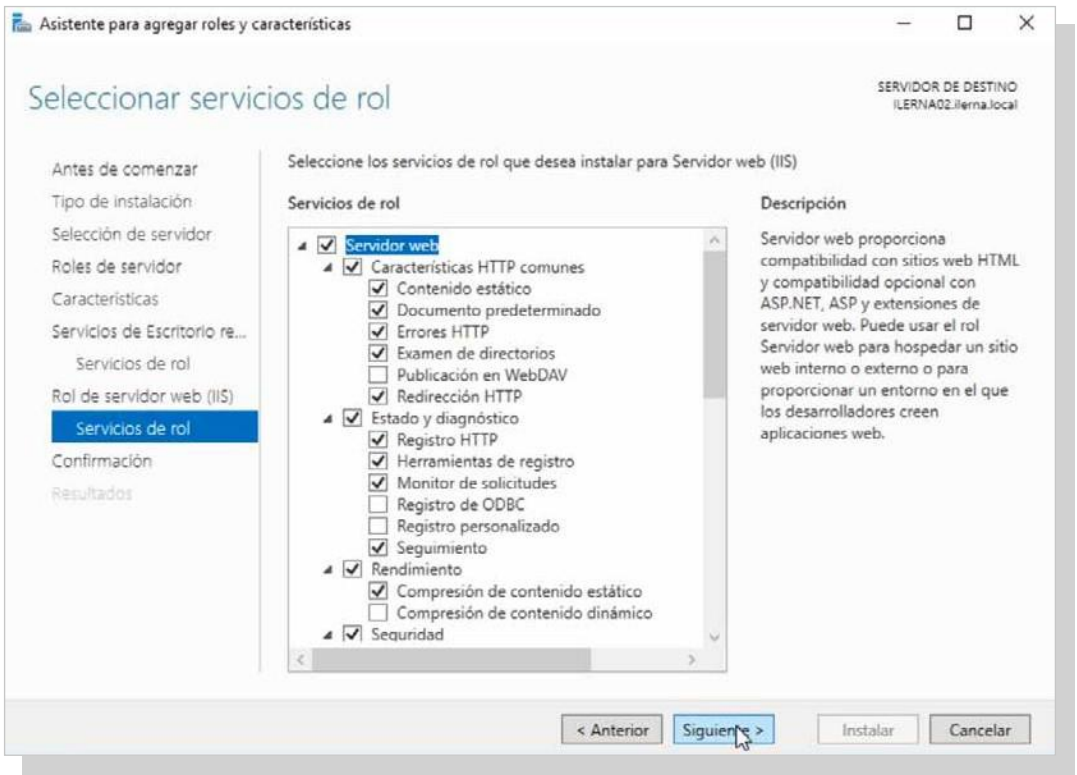
9. Aparece la ventana *Seleccionar servicios del rol.* En esta pantalla elegiremos los servicios que queremos utilizar de este rol, con sus respectivas descripciones de funcionamiento. En el caso de ejemplo, se han elegido los servicios que vemos en la imagen.



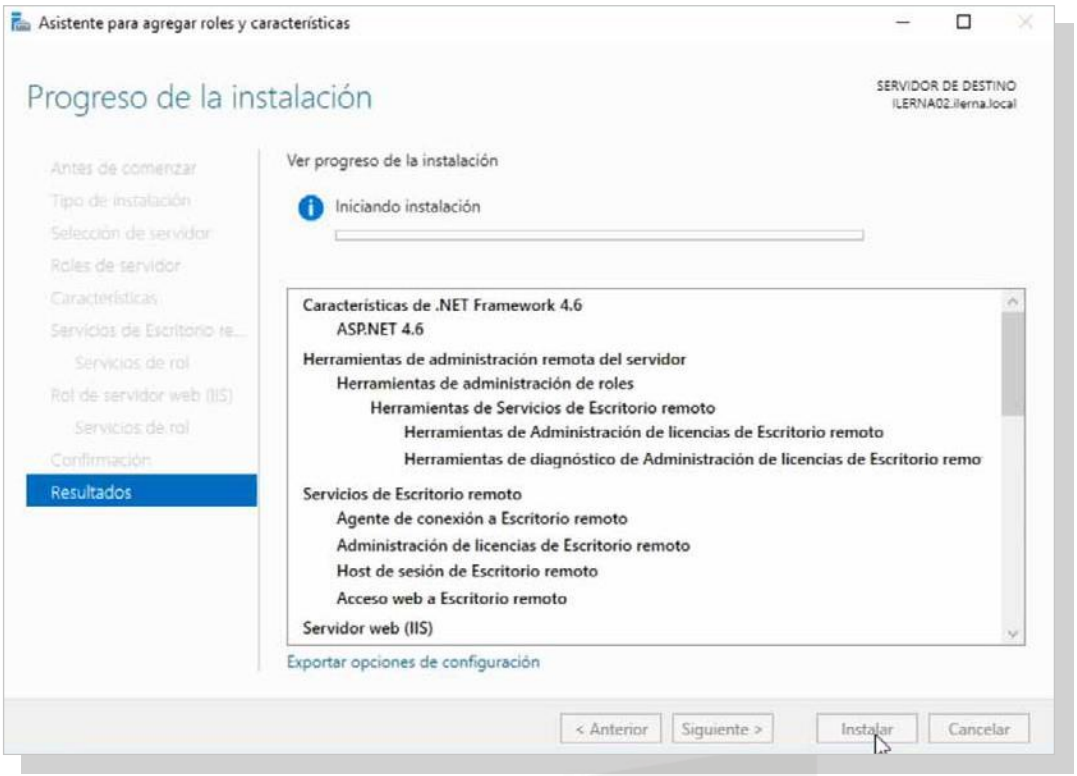
10. Se muestra una ventana con la descripción del rol de servidor IIS (en el caso de que no este instalado), debido a que son necesarios algunos de sus servicios. Hacer clic en *Siguiente.*

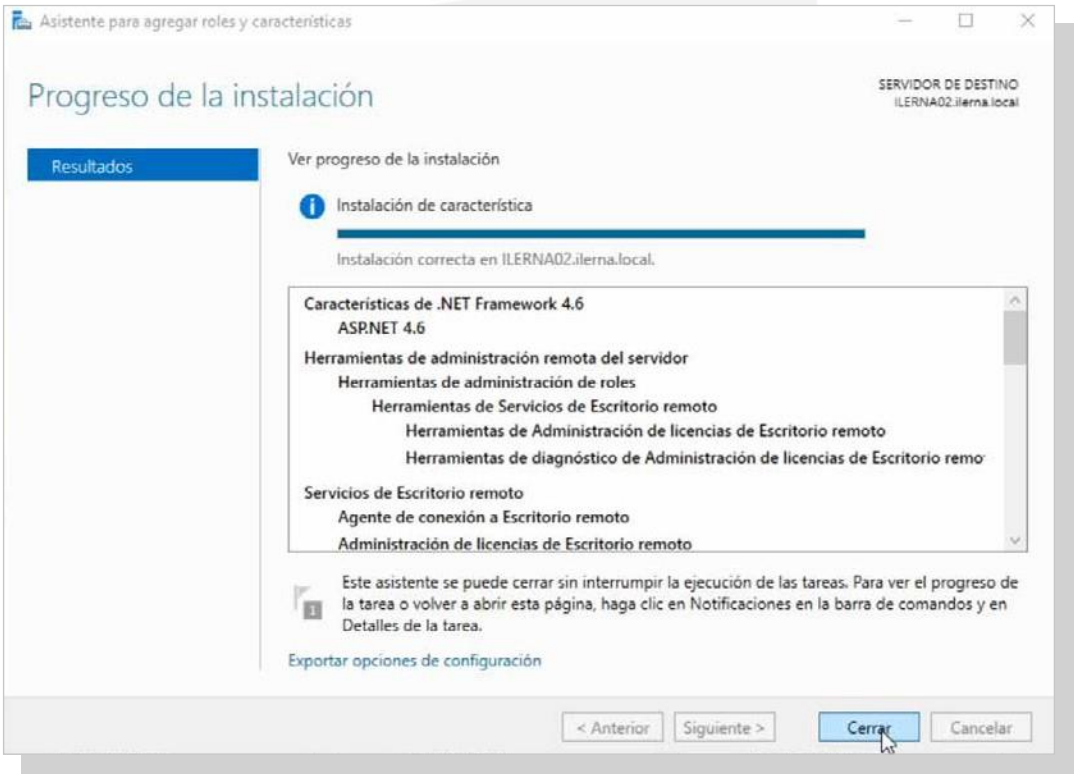


11. Se muestran los diferentes servicios del rol IIS que se van a instalar. Hacer clic en *Siguiente.*



12. Realizar la instalación.





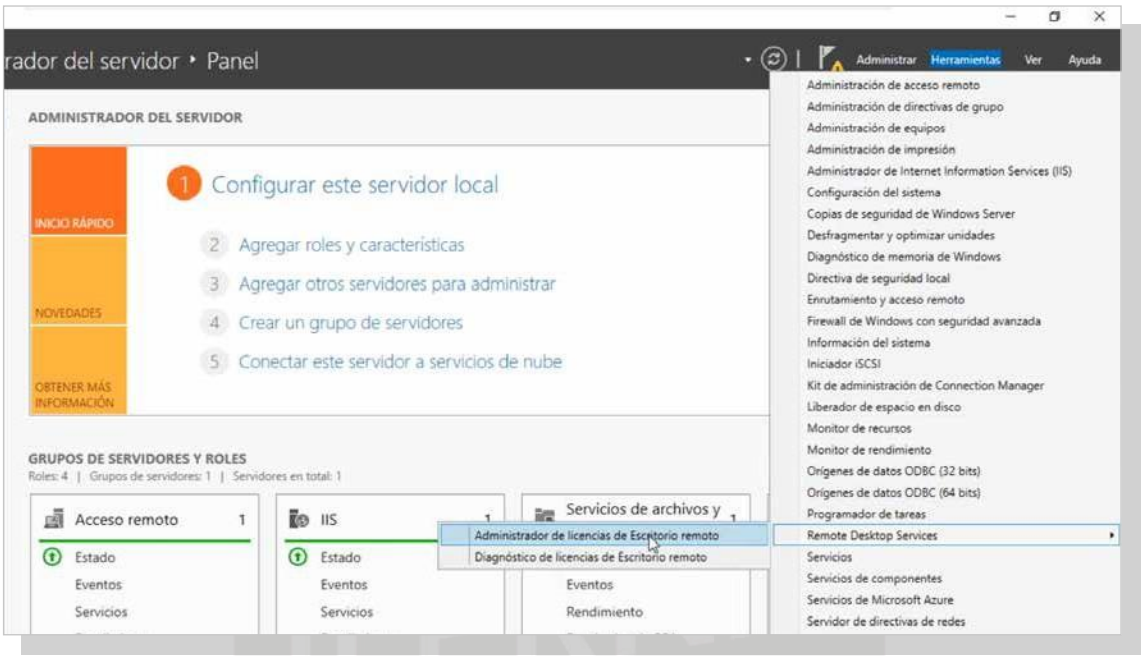
Aquellos usuarios que sean administradores ya deben estar añadidos al grupo *Usuarios de escritorio remoto* y no pueden salir de él.

Activación del servidor

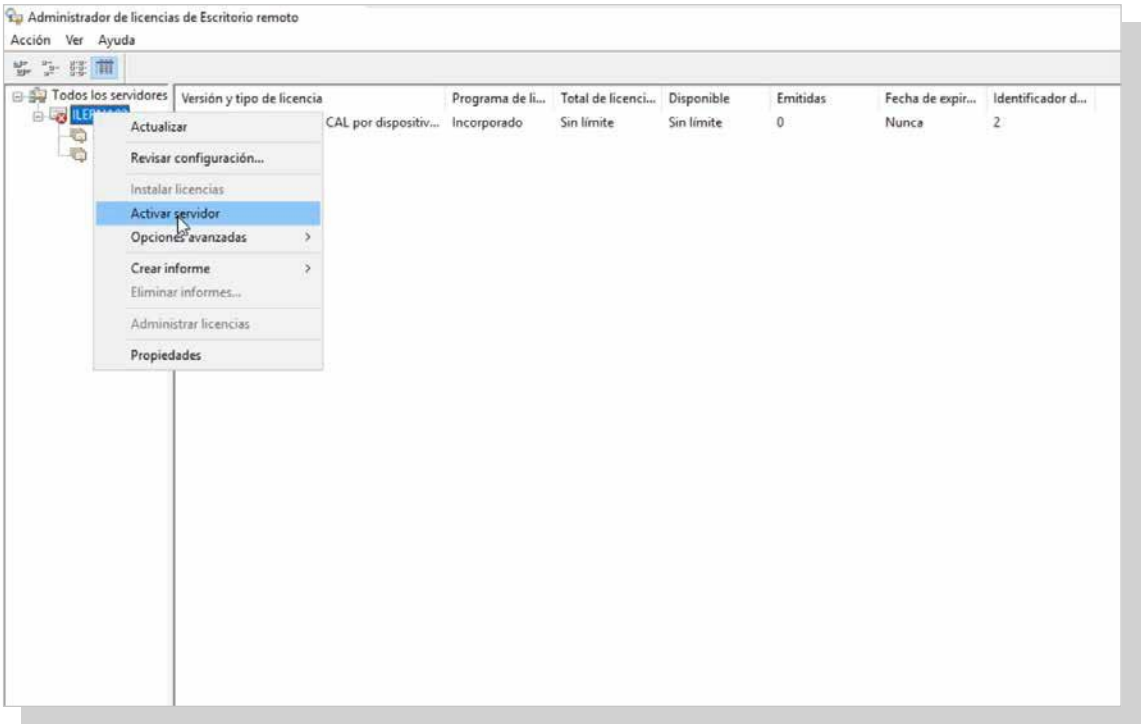
Una vez concluido el proceso de instalación, se procede a activar el servidor.

Para ello se llevarán a cabo los siguientes pasos:

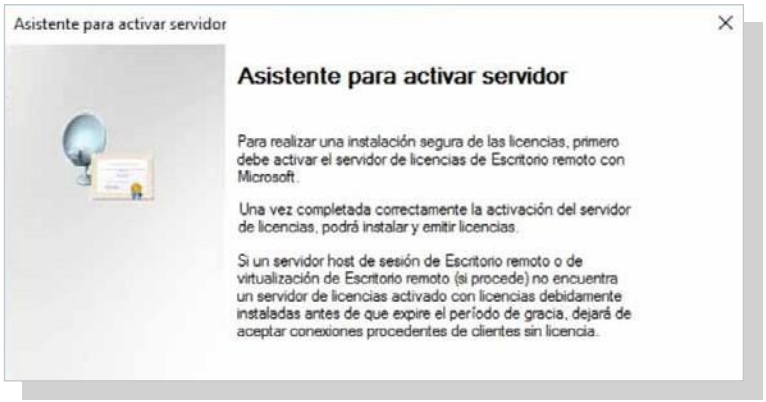
1. Seleccionar la opción *Herramientas* y, dentro de esta, escoger la herramienta instalada: *Remote Desktop Services* y *Administrador de licencias de escritorio remoto*.



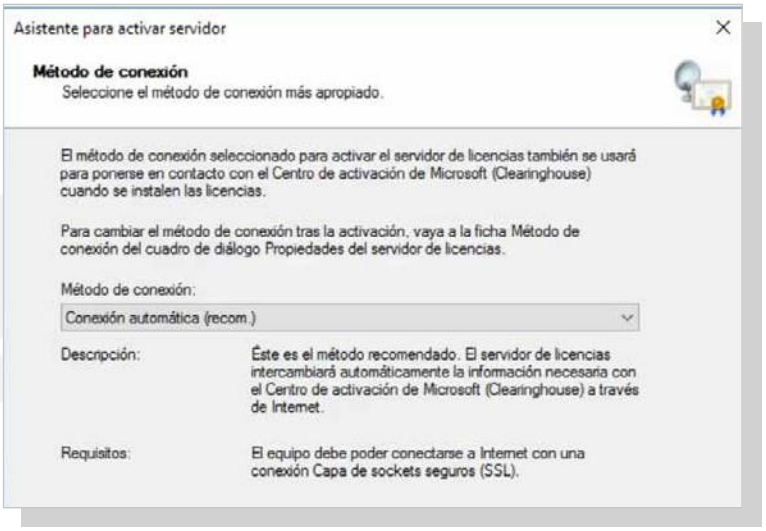
2. Una vez dentro, seleccionar nuestro servidor y, con clic secundario, elegir la opción *Activar el servidor*.



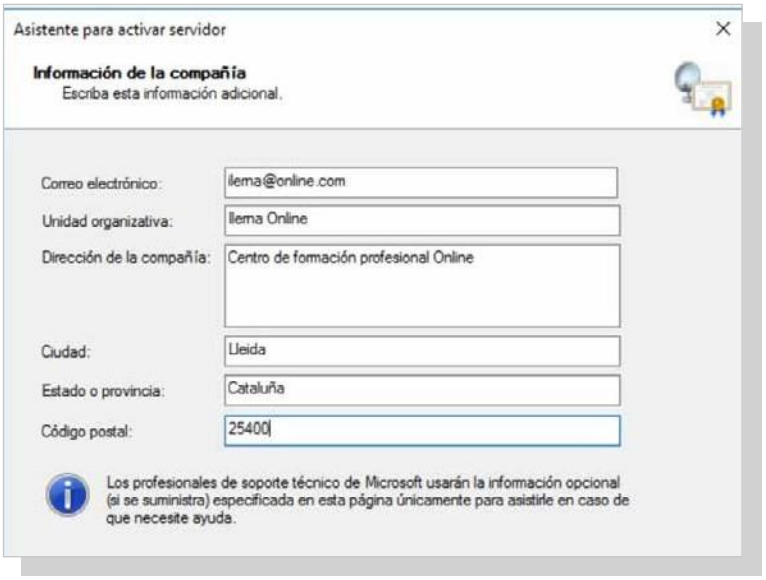
3. Se abre el asistente de activación. Leer la descripción y hacer clic en *Siguiente*.



4. Elegir el modo de conexión automático y hacer clic en *Siguiente*.



5. Rellenar el formulario con los datos requeridos.



6. El servidor está activado.

Configuración del servidor

Una vez concluido el proceso de instalación, se procede a configurar el servidor de forma adecuada para que cumpla con los requisitos que se soliciten.

e) Configuración del certificado de seguridad

En primer lugar, un aspecto primordial al que se debe prestar atención para conseguir mejorar la seguridad en el servicio de acceso remoto es configurar el servidor para que pueda utilizar un certificado digital. De esta forma, un usuario que acceda de forma remota recibirá la firma del servidor para que pueda confiar en él.

Para configurar el certificado de seguridad para el servicio de acceso remoto en el servidor, hay que seguir los pasos a continuación:

1. Abrir la ventana *Administrador de RemoteApp de TS.*
2. En la opción *Configuración de firma digital,* hacer clic en *Cambiar.*
3. En la ventana *Configuración de implementación de RemoteApp*, se debe:
   - Seleccionar la casilla *Firmar con un certificado digital* y hacer clic en *Cambiar.*
   - Cuando aparece la ventana *Seleccionar certificado*, seleccionar el que corresponda. Hacer clic en *Aceptar.*
   - Por último, cerrar la ventana haciendo clic en *Aceptar.*
4. En *Configuración de firma digital* debe aparecer el mensaje *Firmando como: "dirección correspondiente".*
5. Cerrar la ventana *Administrador de remoteApp de TS.*

- **Configuración de la directiva *inicio de sesión* a través de TS**

  En segundo lugar, hay que configurar algunos de los permisos del grupo al que pertenecen los usuarios del servicio de acceso remoto, en el grupo ***Usuarios de escritorio remoto*.**

  Para configurar la directiva ***Permitir el inicio de sesión a través de Terminal Services*** al grupo *Usuarios de escritorio remoto,* se siguen los pasos a continuación:

  1. Abrir la ventana *Administración de directivas de grupo.*
  2. En la ruta *Administración de directivas de grupo/ Bosque*, seleccionar la opción *Editar.*
  3. En la ventana *Editor de las directivas de grupo,* seleccionar la opción *Asignación de derechos de usuario.*
  4. En la ventana que se muestra en la parte de la derecha, seleccionar con doble clic la opción *Permitir inicio de sesión a través de Terminal Services.*
  5. Aparece el cuadro de diálogo *Propiedades de Permitir el inicio de sesión local.* Marcar la casilla *Definir esta configuración de directiva.*
  6. Hacer clic en *Agregar usuario o grupo.*
  7. En la ventana *Agregar usuario o grupo,* seleccionar la opción *Examinar.*
  8. En cuadro de diálogo *Seleccionar Usuarios, Equipos o Grupos,* seleccionar *Escriba los nombres de objeto que desea seleccionar.*
  9. En la siguiente ventana, hacer clic en *Comprobar nombres.* A continuación, hacer clic en *Aceptar.*
  10. En *Agregar usuario o grupo*, se puede observar que ya aparece escrito el grupo *Usuarios de escritorio remoto.* Hacer clic en *Aceptar.*
  11. Si el nuevo grupo se ha añadido bien, ahora hay que ir a *Propiedades y Permitir inicio de sesión a través de Terminal Services* y hacer clic en *Aceptar.*
  12. Se pueden ir cerrando las ventanas de *Editor de administración de directivas de grupo y Administración de directivas de grupo.*

Con esta serie de pasos, los usuarios que estén en el grupo *Usuarios de escritorio remoto* pueden iniciar sesión mediante Terminal Services para conectarse al servidor de forma remota.

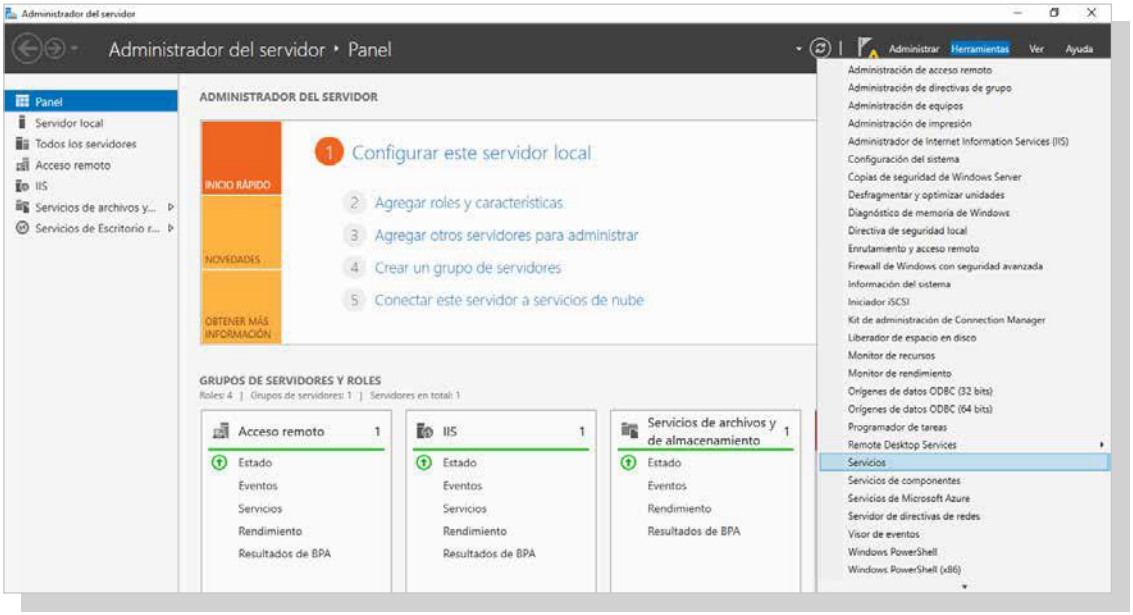
ComProbación

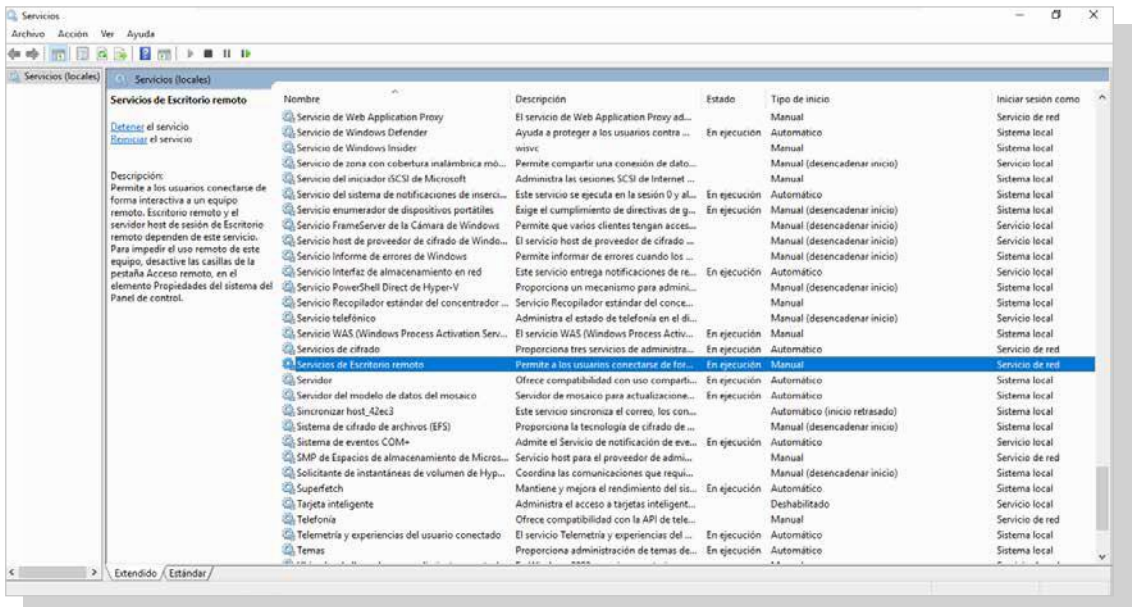
Una vez realizada la instalación y configuración del servidor, es conveniente comprobar que todos los pasos se han realizado de forma correcta y que, por tanto, todo funciona bien.

- **Verificación del estado del servicio**

Para comprobar el estado del servicio de acceso remoto, se recurre a la ruta *Inicio/ Herramientas administrativas*, clicando en ***Servicios***.

En la ventana que se muestra, hay que buscar el servicio **Terminal Services** y, una vez localizado, si el campo ***Estado*** tiene asignado el valor de ***Iniciado*** y en ***Tipo de inicio*** aparece el valor de ***Automático***, significa que el servicio de acceso remoto está funcionando y se iniciará cada vez que arranque el equipo servidor.

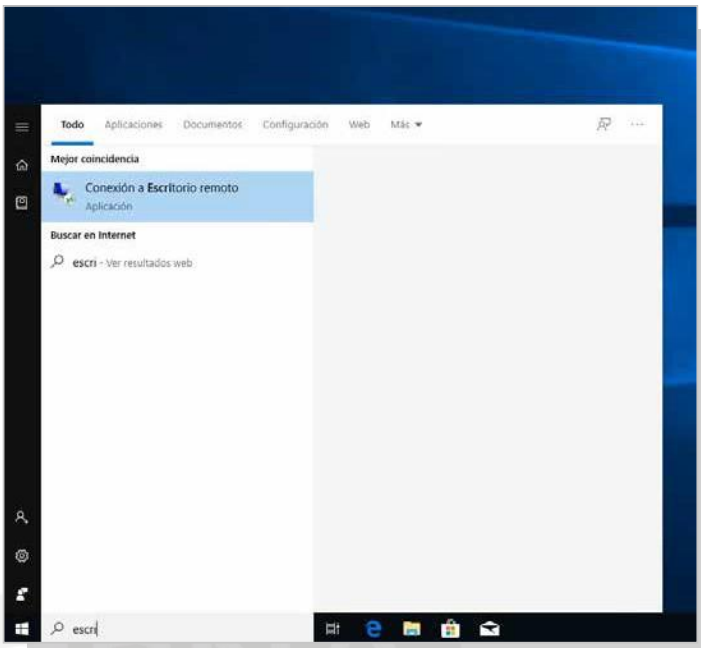




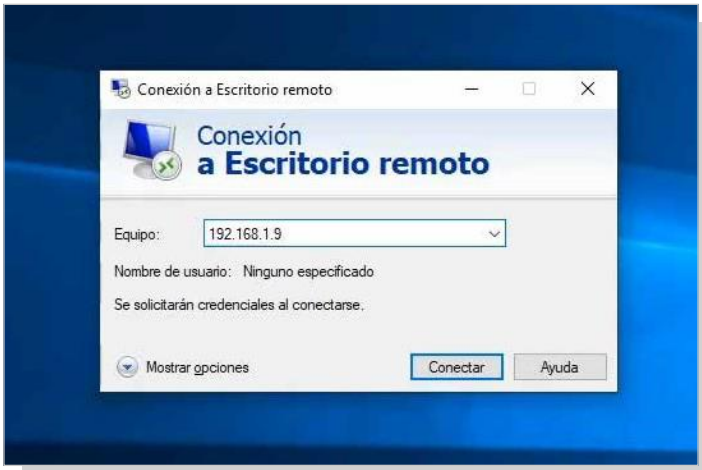
- **Verificación del servicio con conexión a escritorio remoto**

Para comprobar el servicio mediante conexión al escritorio remoto, es necesario seguir los siguientes pasos:

1. En el equipo del cliente, abrir el programa *Conexión a escritorio remoto,* que sigue la ruta *Inicio/Todos los programas/Accesorios.*



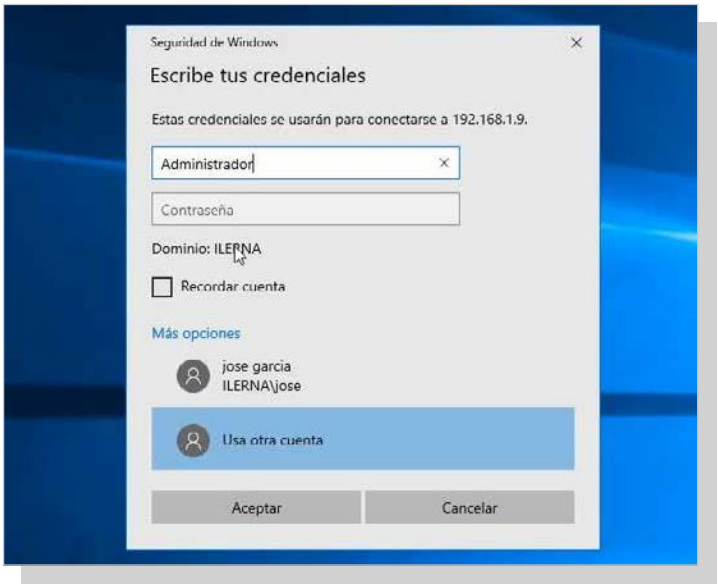
2. Aparece una lista desplegable en la que hay que insertar la dirección del servidor. A continuación, hacer clic en *Conectar.*



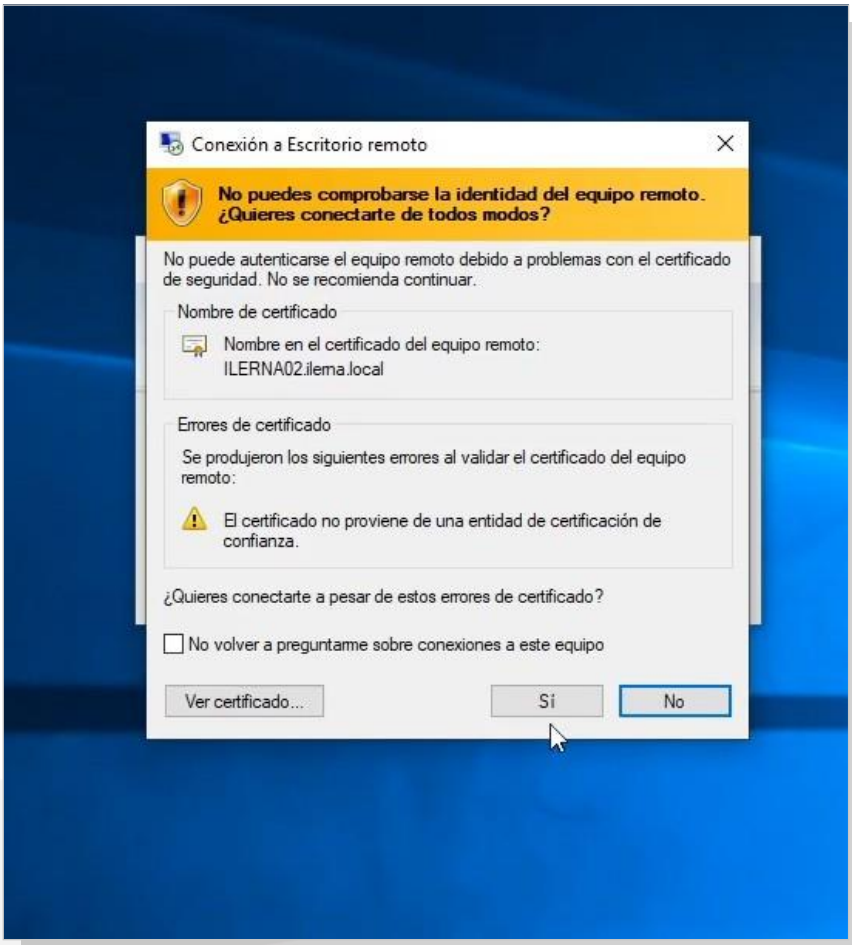
3. Se muestra la ventana *Seguridad de Windows* en la que se debe escribir el nombre del usuario que se tenga habilitado, en este caso utilizamos el administrador. En primer lugar, probar con un usuario de domino que no tiene permisos.

4. Como se puede comprobar, este usuario no puede realizar esta conexión debido a la falta de permisos.

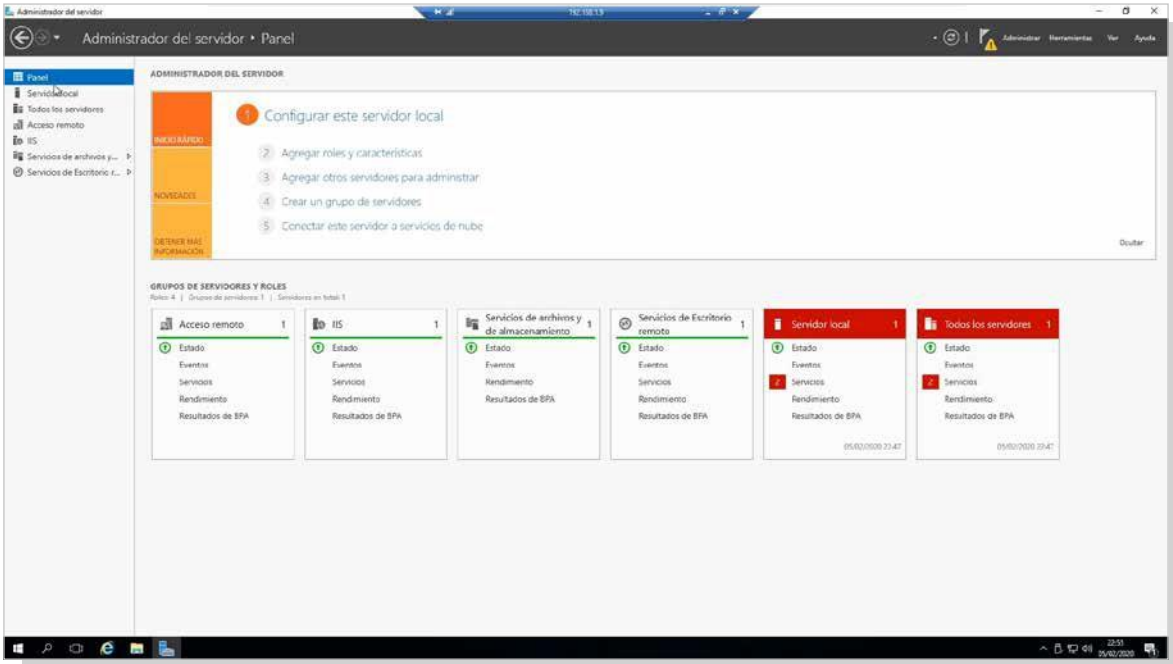
5. A continuación, elegir la opción *Usar otra cuenta* para elegir el usuario con permisos.



6. Antes de conectarse de forma remota, se muestra un aviso para indicar que el certificado no está firmado por ninguna CA. Seleccionar *Sí*.



7. Por último, establecer la conexión remota al servidor.



- **Verificación del servicio con el navegador Internet Explorer**

Para verificar que se puede acceder al servicio mediante el navegador Internet Explorer, basta con abrir dicho navegador desde un equipo cliente, escribir una URL y seguir realizando los pasos de la misma forma que se ha hecho en el apartado anterior.

Ventajas y Deficiencias De ambos métoDos

Interfaz gráfica

- Ventajas
  - Es más fácil el manejo de los diferentes procedimientos.
  - Cada comando se puede ver en pantalla a través de una imagen que lo representa.
  - Ofrece diversos mecanismos estándar de control como pueden ser las ventanas y los cuadros de diálogo.
  - Permite que el usuario interactúe con el sistema de una forma sencilla
- Inconvenientes
  - Necesita utilizar más recursos del sistema.
  - Es bastante más compleja de utilizar.
  - Es bastante más cara.

Interfaz de consola

- Ventajas
  - Ocupan menos espacio, por lo que son bastante más ligeras.
  - Son más rápidas realizando las distintas operaciones.
- Inconvenientes
  - Son más complejas a la hora de operar.
  - Necesita conocer la funcionalidad de los comandos
  - No son atractivas hacia la vista del usuario.

BIBLIOGRAFÍA / WEBGRAFÍA

- Andreu, J. (2010). *Servicios en red.* Madrid: Editex.
- Carceller, R., Campos, C., García, C., & González, J. (2010). *Servicios en red.* Madrid: MACMILLAN Professional.
- Carceller, R., Campos, C., García, C., & González, J. (2013). *Servicios en red.* Madrid: MACMILLAN Iberia, S.A.