Servicio de Informática

Vicerrectorado de Estrategia y Universidad Digital

Conexión mediante Escritorio Remoto (RDP)

Edición: 05
Última Actualización 18 de enero de 2024

Histórico de cambios

Fecha	Descripción	Autor
16/09/13	Primera edición	Servicio de Informática
22/01/15	Segunda edición. Actualización y corrección de errores	Servicio de Informática
13/05/20	Cuarta edición. Actualizaciones y correcciones	Servicio de Informática
16/12/20	Documentación del cliente RDP para MacOS	Servicio de Informática

Tabla de contenido

1.- Introducción 4
2.- Requisitos para conectarse mediante Escritorio Remoto a un equipo de la UJA 4
3.- Configuración del equipo al que nos vamos a conectar (equipo en la UJA) 4
4.- Equipo de casa. Configuración para conexión VPN 8
5.- Recomendaciones generales de seguridad 8
6.- Iniciar una conexión a un equipo mediante Escritorio Remoto 9

1.- Introducción

La **Conexión a Escritorio Remoto de Windows (RDP)** permite acceder a un equipo de la UJA de forma remota desde cualquier lugar con conexión a Internet. Esto permite, entre otras cosas, que el usuario pueda utilizar los datos, aplicaciones y recursos de red de su equipo de la UJA desde fuera de ella.

Esta guía explica cómo acceder al Escritorio Remoto de un equipo de la UJA a través de una conexión segura VPN.

2.- Requisitos para conectarse mediante Escritorio Remoto a un equipo de la UJA

Para acceder a nuestro equipo en la UJA mediante Escritorio Remoto de Windows, se necesita:

1. Una conexión a Internet.

2. Un equipo externo a la UJA (el de casa, por ejemplo) con Windows, desde el que se hará la conexión. Este equipo deberá tener:

    - Configurado el protector de pantalla, y protegido por contraseña con un tiempo de activación inferior a 30 minutos.
    - Antivirus actualizado.
    - Un navegador estándar: Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, Safari, etc...

3. Un equipo Windows en la UJA (debe estar encendido). Se debe:
    - Conocer la dirección IP o el nombre del equipo de la UJA al que nos vamos a conectar. Este equipo debe tener instalado Windows.
    - Disponer de cuentas de usuario y permisos adecuados en el equipo de la UJA.

4. Establecer una conexión VPN-SSL a la Universidad de Jaén.

3.- Configuración del equipo al que nos vamos a conectar (equipo en la UJA)

a) PASO 1: conocer el nombre o la dirección IP de nuestro equipo de la UJA

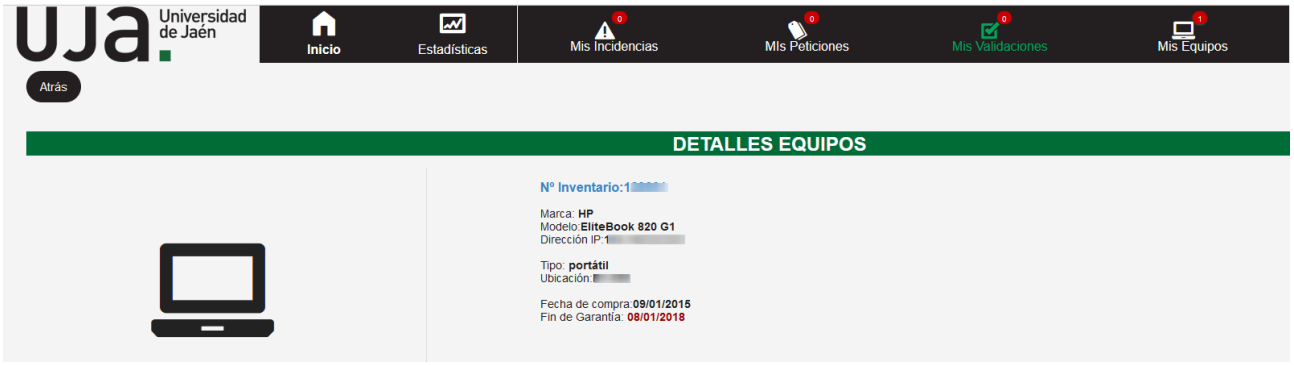
Para conocer la dirección IP de un equipo en Windows:

La forma más rápida es consultarla en Murphy 2.0, dentro de la Intranet de la web de la Universidad de Jaén:

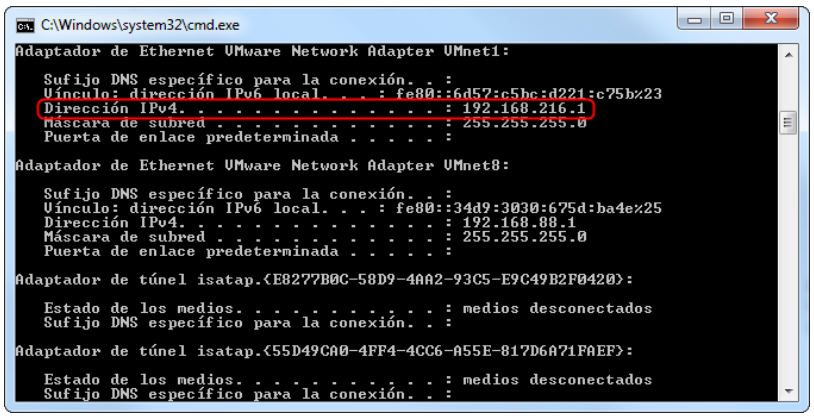
Murphy

Portal de Autoservicio TIC (Murphy)

En el menú superior tenemos que seleccionar **Mis Equipos**, que muestra los equipos a nuestro cargo, y en el campo correspondiente podemos encontrar la dirección IP asociada:



Una forma alternativa, consiste en entrar en el Botón de Inicio de Windows y en el cuadro **"Buscar programas y archivos"** escribimos **`cmd`**. Esto nos abrirá una ventana de línea de comandos. En esa ventana, teclearemos **`ipconfig`**, lo que nos mostrará información sobre la configuración de nuestra red:



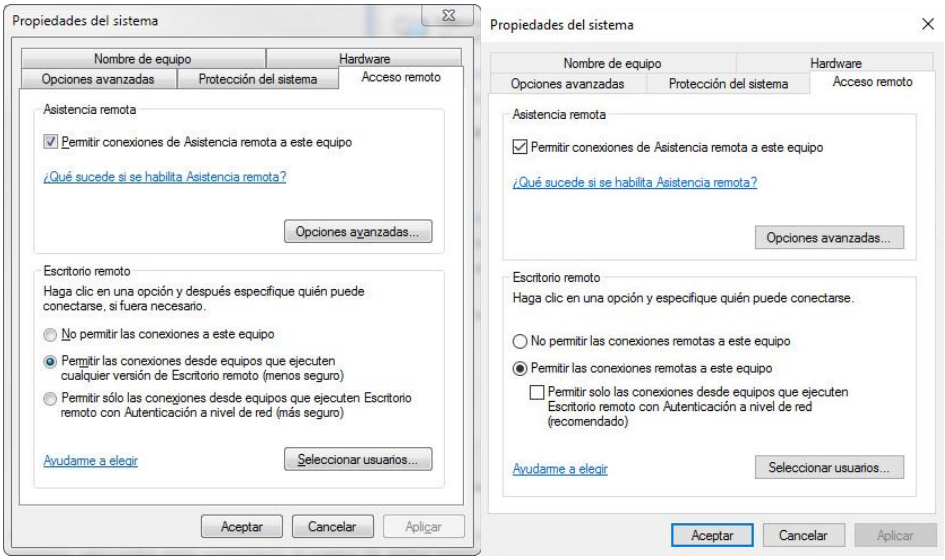
De la información mostrada, observaremos el apartado **Adaptador Ethernet Red de Área Local**, concretamente el campo **Dirección IP**. Será un conjunto de cuatro números de hasta tres dígitos en la forma **aaa.bbb.ccc.ddd**. Esa será la dirección IP de la máquina.

Para obtener el nombre del equipo de la UJA, podemos hacerlo tecleando **`hostname`** desde la línea de comandos. A este nombre tendremos que añadir el sufijo **ujaen.es**, para obtener finalmente un nombre del tipo: **equipo.ujaen.es.**

b) PASO 2: Habilitar acceso remoto al equipo de la UJA

Para permitir el acceso de manera remota a un equipo de la UJA, debemos habilitar la característica **Escritorio Remoto** en dicho equipo. La forma de hacerlo es la siguiente:

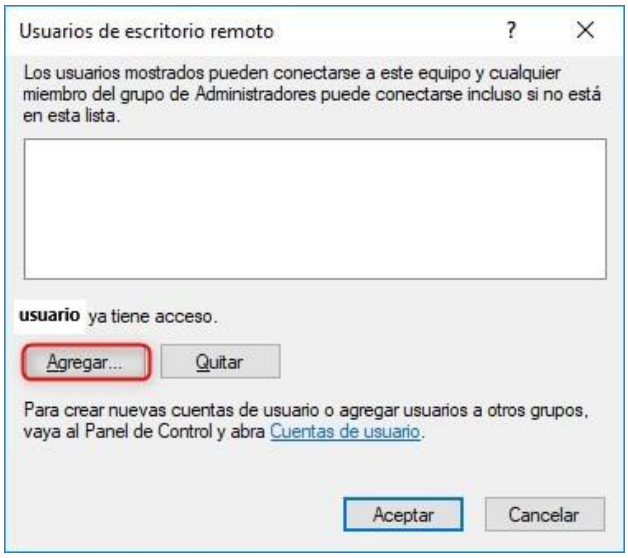
a) Haremos clic con el botón derecho sobre el icono de **Equipo** > **Propiedades**, seleccionamos el enlace **Configuración de acceso remoto** y activamos la opción correspondiente. Por defecto está en **No permitir las conexiones a este equipo**. En su lugar, debemos seleccionar la opción **Permitir la conexión desde equipos que ejecuten cualquier versión de Escritorio remoto (menos seguro, pero más compatible)** o la opción de Autenticación a nivel de red (más segura). En Windows 10/11, la opción a seleccionar es **Permitir las conexiones remotas a este equipo**.



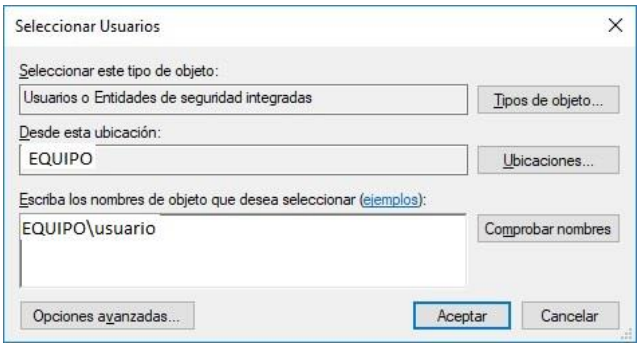
c) PASO 3: Selección de usuarios con permisos de acceso remoto

A continuación, debemos seleccionar los usuarios que queremos que se puedan conectar mediante acceso remoto al equipo de la UJA. Estos usuarios serán el usuario **Administrador** y/o cualquiera que sea miembro de los grupos **Administradores** o **Usuarios de escritorio remoto** en el equipo de la UJA.

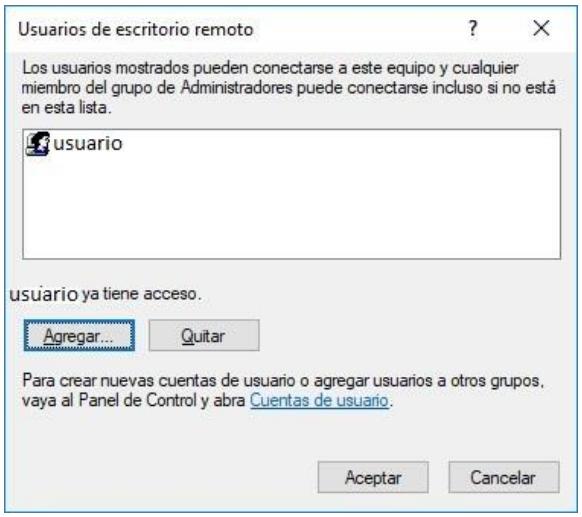
Para seleccionar los usuarios haremos clic en el botón **Seleccionar usuarios…** y pasamos a la ventana **Usuarios de escritorio remoto**. Aquí aparecen los usuarios que ya han sido seleccionados para utilizar Escritorio Remoto.



Si nuestro usuario (con el que entramos habitualmente en nuestro equipo de la UJA) no está en la lista, haremos clic en **Agregar…** y en la ventana **Seleccionar usuarios** escribiremos el nombre del usuario. A continuación, pulsaremos en **Comprobar nombres** para ver si ese usuario existe en el equipo.



Si todo es correcto y el usuario existe, aparecerá el nombre en la forma **EQUIPO\usuario**, tal y como se muestra en la imagen de arriba. Haciendo clic en **Aceptar** añadimos el usuario a la lista de usuarios de Escritorio Remoto.



Para finalizar pulsamos **Aceptar** dos veces.

d) PASO 4: Configurar las opciones de ahorro de energía

Si el equipo de la UJA está configurado en algún modo de ahorro de energía, pasado un tiempo entrará en estado de suspensión y no será posible la conexión mediante Escritorio Remoto, aun cuando el equipo está encendido.

Para asegurarnos de que no entra en estado de suspensión, tendremos que entrar en **botón de Inicio > Panel de Control > Sistema y Seguridad > Opciones de energía**. Una vez que entremos en el Plan de Energía que esté activo, tenemos que poner la opción **"poner al equipo en estado de suspensión"** con el valor **"Nunca"**.

e) PASO 5: Bloquear la pantalla de Windows

No olvide bloquear el equipo para evitar posibles accesos mientras esté encendido. Puede hacerlo pulsando la combinación de teclas **Windows + L**. Otra opción es activar un protector de pantalla.

⚠	**ATENCIÓN** Durante estos días el ordenador quedará desatendido. Asegúrese que la salida de aire del equipo no queda obstruida por papeles u otros objetos.

4.- Equipo de casa. Configuración para conexión VPN

El equipo de casa deberá cumplir los siguientes requisitos:

a) **Antivirus actualizado.** Por motivos de seguridad, el servidor VPN-SSL comprobará que si su equipo tiene instalado un antivirus y está actualizado. La plataforma de conexión VPN-SSL soporta un gran número de antivirus gratuitos y de pago que existen en el mercado.

b) **Protector de pantalla con un tiempo menor de 30 minutos y protegido por contraseña.** Por motivos de seguridad, el servidor VPN-SSL verificará si su equipo tiene configurado el protector de pantalla con contraseña para activarse cuando transcurra un máximo de 30 minutos sin actividad en el PC. Mientras el protector de pantalla no esté correctamente configurado, el cliente VPN-SSL no permitirá establecer la conexión.

c) **Un navegador web estándar en equipos de sobremesa/portátiles.** Se han realizado pruebas satisfactorias con los siguientes navegadores: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari y Opera. Para la conexión con un navegador web, necesitará instalar un complemento o plugin. El proceso de instalación del complemento suele ser bastante sencillo, pero si tiene algún problema puede consultar las soluciones a los problemas más frecuentes.

5.- Recomendaciones generales de seguridad

- **Utilice contraseñas robustas y renuévelas de forma periódica**. No reutilice la contraseña de su cuenta TIC de la UJA en otros servicios o aplicaciones. Asimismo, en general, **guardar las contraseñas en el navegador no es una buena práctica.**

- **Tenga siempre instalado en su equipo Windows la última versión de antivirus corporativo** (actualmente, Panda Dome). Recuerde que ningún antivirus le proporciona una seguridad contra virus/malware al 100%. Por ello, debe seguir siempre todas las recomendaciones de seguridad que aquí le indicamos.

- **Mantenga actualizado su sistema operativo y navegador** instalando los parches de seguridad que proporciona de forma automática y periódica el fabricante.

- Si utiliza un equipo portátil propiedad de la UJA, recuerde que debe utilizarlo exclusivamente para fines laborales. Asimismo, si utiliza su equipo particular para acceder a aplicaciones corporativas de la UJA, extreme las precauciones siguiendo todas las recomendaciones aquí indicadas y **procure realizar siempre una navegación segura por**

Internet.

- Para velar por la seguridad de la información corporativa, desde el Servicio de Informática se están monitorizando los accesos remotos (VPN, escritorio remoto, etc.) a los servicios y sistemas y, si fuera necesario, se activarán controles adicionales a los actuales.

- **Realice una copia de seguridad de forma periódica**. Recuerde que si sus ficheros son eliminados o cifrados por algún virus o software malicioso (malware), la única solución para recuperar su información es a partir de una copia de seguridad.

6.- Iniciar una conexión a un equipo mediante Escritorio Remoto

Para probar que todo es correcto, una vez configurado el equipo, déjelo en funcionamiento y asegúrese de que tiene conexión a la red de la UJA y puede navegar por Internet.

PASO 1: Establezca una conexión segura VPN (https://vpnssl.ujaen.es)

IMPORTANTE: El primer paso antes de hacer la conexión mediante Escritorio Remoto es establecer una conexión VPN-SSL con la UJA. Toda la información disponible sobre el servicio VPN-SSL está disponible en los siguientes enlaces:

- Descripción del servicio de conexión VPN-SSL
- VPN-SSL - Preguntas frecuentes

PASO 2: Conecte al Escritorio Remoto del equipo Windows en la UJA

Para conectarnos al equipo de la UJA desde un equipo en Internet (el de casa, por ejemplo), necesitamos disponer del software cliente para la conexión. Windows lleva integrado en el sistema el cliente de escritorio remoto. En otras plataformas, como MacOS, existe un cliente oficial de Microsoft que se puede descargar desde la Apple Store.

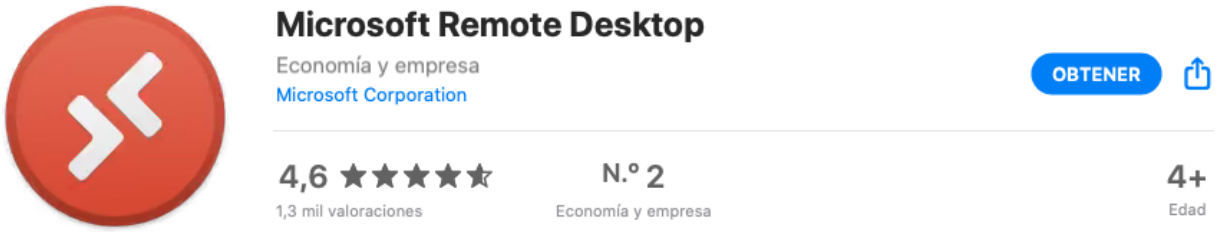
Conexión desde Windows

Ejecutar el cliente que se encuentra en el **Botón Inicio > Accesorios** y se denomina cliente de **Conexión a Escritorio Remoto**.

Para conectarnos al equipo de la UJA basta con poner el nombre del equipo o su dirección IP en el cuadro **Equipo**, y pulsar en **Conectar**.

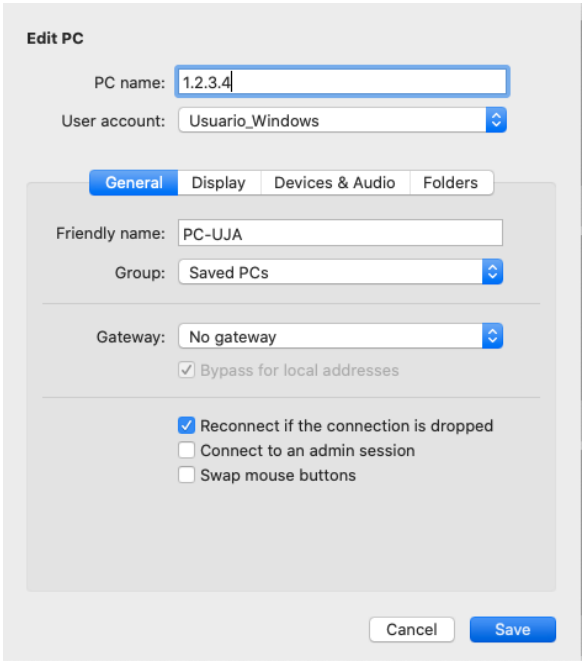
Conexión desde MacOS

El cliente RDP para MacOS no se incluye en el sistema, por lo que inicialmente hay que descargarlo desde la App Store e instalarlo (pulsando los botones OBTENER e INSTALAR):



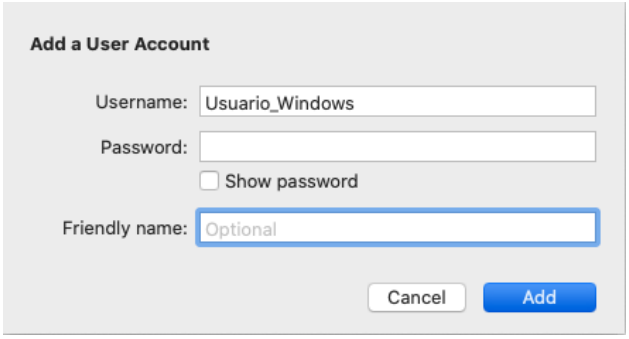
Una vez instalado, pulsamos el icono:

Y nos aparecerá la ventana de conexión donde tenemos que configurar una nueva sesión pulsando **Add PC**. Los parámetros que tenemos que configurar son los siguientes:



- **PC Name:** indicamos dirección IP del equipo de la UJA.

- **User Account:** indicamos el usuario de Windows de nuestro equipo de la UJA (**OJO:** NO nuestra cuenta TIC). En ese apartado, podemos seleccionar que nos lo pida en el momento de la conexión (**Ask when required**) o definirlo previamente, desplegando y seleccionando **Add user account**, con lo que nos aparece la siguiente ventana:



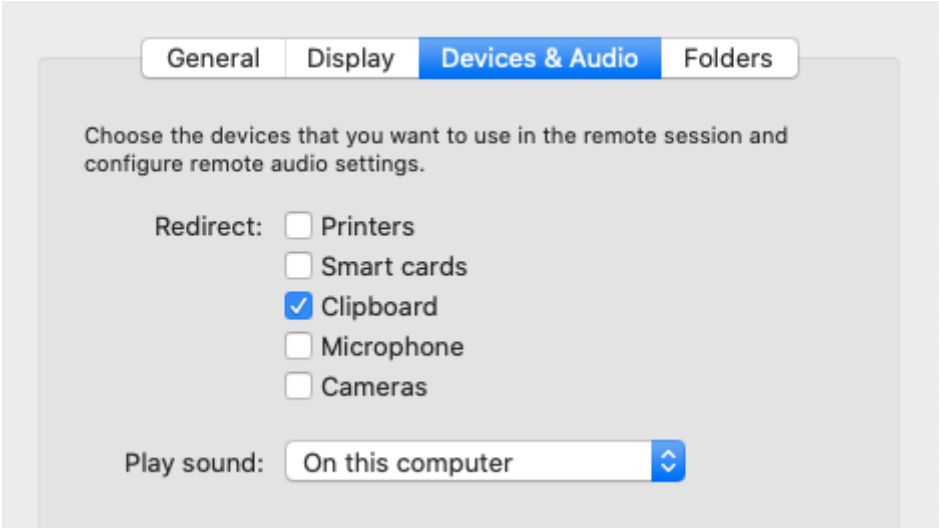
- **Friendly Name:** un nombre descriptivo para la conexión (ej: PC-UJA)
- **Group:** el grupo al que queremos añadir esta conexión. Podemos dejar el que viene por defecto (**Saved PCs**)
- **Gateway**: lo dejamos como está (**No gateway**)
- **Dejaremos marcada la casilla "Reconnect if the connecton is dropped"**
- El resto de parámetros los podemos dejar con sus valores por defecto.

A partir de aquí, la conexión y el funcionamiento son similares a la conexión desde el cliente de Windows.

Opcionalmente, podemos configurar algunos parámetros:

Display

Nos permite configurar con detalle algunas opciones de visualización:



Algunas opciones interesantes son:

- **Resolution:** nos permite cambiar la resolución por defecto.
- **Use all monitors:** nos permite usar varios monitores en caso de tener más de uno.
- **Color Quality:** permite cambiar la calidad de color (número de bits)
- **Optimize for Retina Display.** Mejora la calidad en monitores Retina. OJO: esto solo se recomienda cuando el equipo de destino es Windows 10/11, Windows Server 2016 y versiones superiores.

Devices & Audio

Nos permite configurar con detalle algunas opciones de audio y dispositivos:

Básicamente, nos permite redireccionar determinados dispositivos del equipo Windows remoto a nuestro equipo Mac local: impresoras, tarjetas inteligentes, el portapapeles (fundamental), micrófono, cámaras y audio (podemos hacer que suene en el equipo local o en remoto)

Folders

Esta opción nos permite seleccionar carpetas de nuestro equipo Mac local para que estén disponibles en el equipo remoto para compartir información. Para ello basta con marcar la casilla **Redirect Folders** y con **+** ir añadiendo las carpetas que queramos.