

Pasarela SSH

Descripción del servicio

Proporciona acceso a un equipo de la red interna del centro a través de SSH desde el exterior. Este servicio está pensado para poder acceder a la red del centro en casos donde no es posible hacer uso de la [VPN](#).

Alta en el servicio

Comprueba primero en el [apartado Cuenta y Permisos de Xici](#) si aparece ya listado el servicio *Acceso ext. pasarela SSH*. En ese caso, el servicio ya está activo en tu cuenta.

El alta debe solicitarse mediante el [formulario de peticiones e incidentes](#). Para acceder al formulario necesitas usuario y contraseña del CiTIUS. Se tienes problemas recordando el usuario o contraseña, puedes solicitar una reactivación en citius.tic@usc.es.

También debes añadir una clave pública SSH en tu cuenta, en el [apartado «Cuenta y permisos» de Xici](#), ya que **sólo se acepta autenticación mediante claves SSH**.

Para generar las claves, desde una terminal ejecuta:

```
ssh-keygen -t rsa
```

Introduce una contraseña para proteger tus claves. Esto generará los archivos `~/.ssh/id_rsa` (la clave privada) y `~/.ssh/id_rsa.pub` (la clave pública). Esta última es la que debes añadir en XiCI.

Manual de usuario

Datos de conexión

- Servidor: `vpn2.citius.usc.es` (193.144.78.45)
- Puerto: 22
- Usuario: *Tu usuario del CiTIUS*
- Contraseña: *La contraseña de tu clave privada. Si no recuerdas la contraseña debes generar un nuevo par de claves y volver a enviarnos la clave pública.*

Conexión simple desde GNU/Linux

Para conectar, puedes hacer uso del comando SSH. Opcionalmente, puedes especificar la localización de la clave privada, si no se encuentra en su localización por defecto.

```
ssh -i ~/.ssh/id_rsa nombre.usuario@vpn.citius.usc.es
```

Una vez conectado, puedes conectarte a otros equipos del centro, por ejemplo a tu equipo de trabajo. Recuerda que puedes encenderlo (y apagarlo) haciendo uso del servicio de [encendido y apagado remoto](#).

Conexión simple desde Windows

Puedes utilizar el programa [PuTTY](#), haciendo uso de los mismos datos facilitados arriba. Para conectar, es necesario convertir previamente la clave personal del formato SSH al formato de PuTTY. Puedes hacerlo con PuTTYgen que puedes encontrar en la misma página de PuTTY. Para hacerlo:

- Accede al menú *Conversions* » *Import key*.
- Localiza la clave personal en formato SSH (el nombre por defecto es `id_rsa`).
- Introduce la clave de paso, si la tuviese.
- Presiona en el botón *Save private key* y selecciona un lugar donde guardar el archivo `.ppk` generado.

Una vez tengas el archivo con extensión `ppk`, puedes usarlo en el campo *Private key file* tanto de PuTTY como de WinSCP.

Conexión a un servicio haciendo un túnel SSH

Puedes usar la pasarela SSH para acceder a un servicio del CITIUS, mapeando los puertos necesarios de la máquina que ofrece el servicio tu máquina local.

Por ejemplo, puedes acceder al [almacenamiento a través de SSH](#) si mapeas así el servicio:

```
ssh -i ~/.ssh/id_rsa nome.usuario@vpn.citius.usc.es -L 8000:172.16.242.41:22
```

Una vez conectado, puedes acceder a los archivos a través de SSH en la dirección `127.0.0.1:8000`. De esta misma forma puedes acceder a otros servicios.

También se puede hacer desde Windows, a través del programa [WinSCP](#). Para hacerlo, debes pulsar en *Advanced options* y cubrir los datos de conexión en el panel *Tunnel*.

From:

<https://wiki.citius.usc.es/> - Wiki do CITIUS

Permanent link:

https://wiki.citius.usc.es/es:centro:servizos:pasarela_ssh

Last update: **2020/03/11 16:35**

