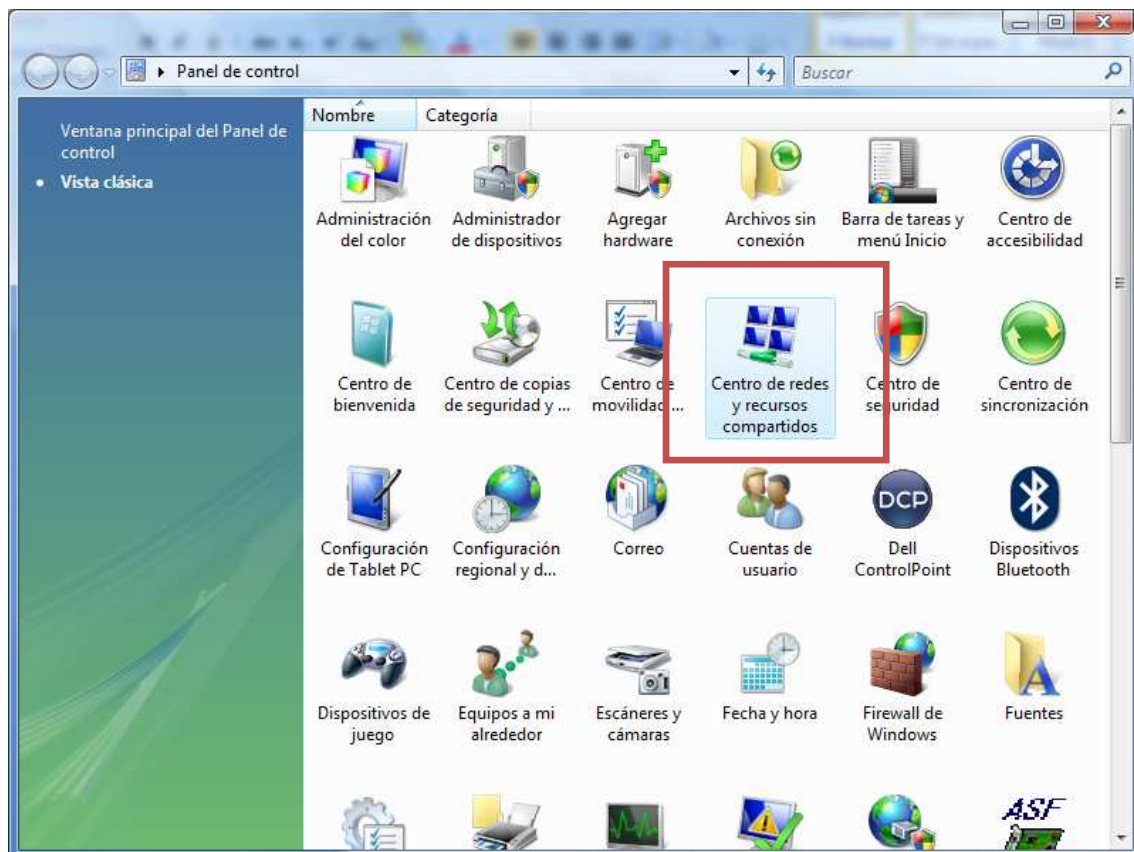


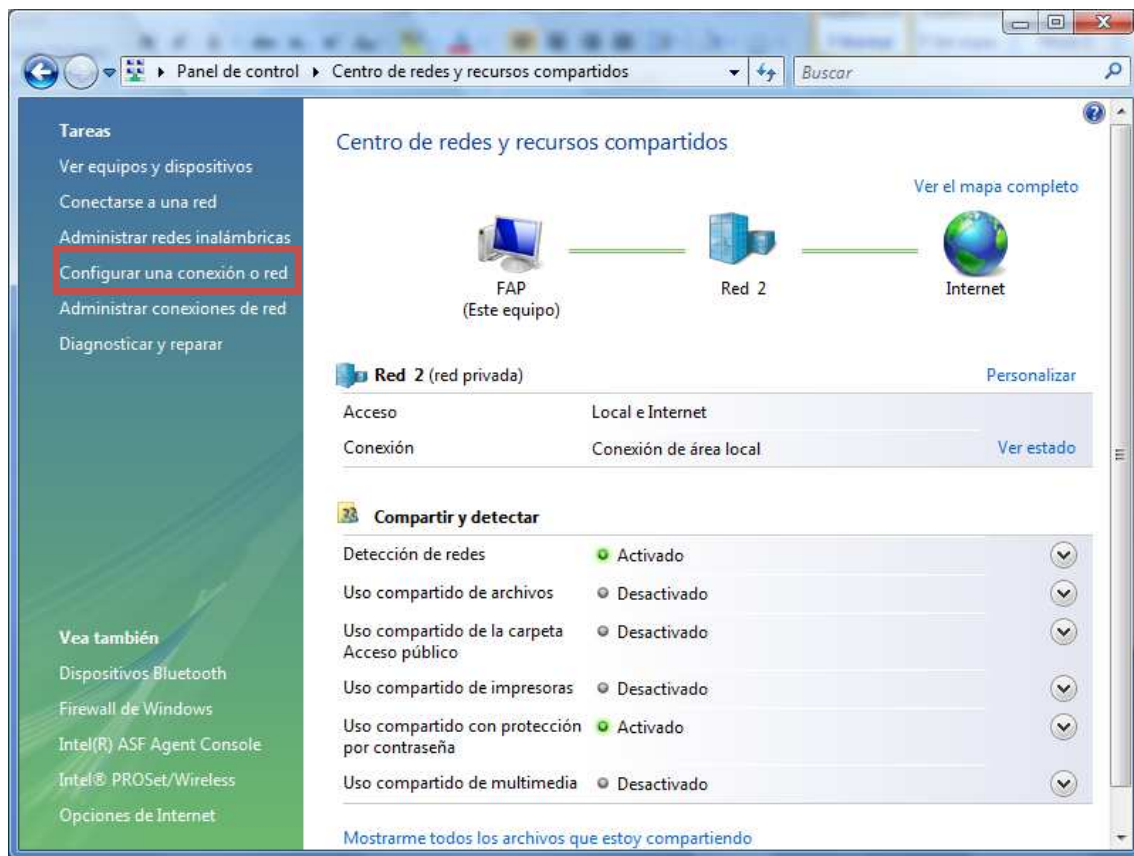
## Manual para conectar a la VPN del ITC en Windows Vista y acceso a los servidores de pre-explotación y explotación.

### Primer paso: Conexión a la VPN del ITC

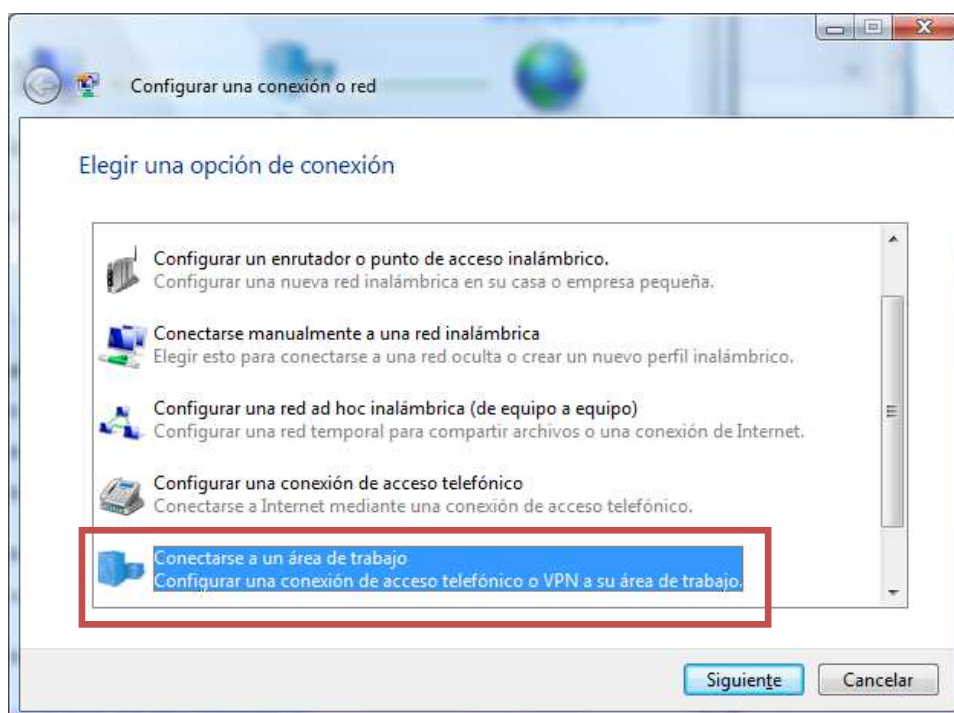
Para poder acceder a los servidores de explotación del ITC, lo primero que se debe hacer es crear una conexión VPN que de acceso a la red del ITC. Para ello se debe abrir el “Panel de control” y luego abrir el “Centro de redes y recursos compartidos”



Una vez abierto el Centro de redes, seleccionar la opción “Configurar una conexión o red” del menú de la izquierda.



En el menú que aparece se debe seleccionar la opción “Conectarse a un área de trabajo” y pinchar en el botón “Siguiente”.



En la siguiente pantalla se debe seleccionar la opción “Usar mi conexión a Internet (VPN)”.



En la siguiente pantalla se debe introducir la dirección a la que se debe conectar y el nombre de destino.

**Dirección de destino: svpntf.itccanarias.org**

**Nombre del destino: ITV\_VPN**

Alternativamente, se puede utilizar el servidor vpn de Las Palmas, utilizando la dirección **svpngc.itccanarias.org**, aunque no debería ser necesario.

Además, se debe marcar la opción “No conectarse ahora; configurar para conectarse más tarde”

Finalmente se debe pinchar en el botón “Siguiente”.

Conectarse a un área de trabajo

Escriba la dirección de Internet a la que se conectará

El administrador de red puede darle esta dirección.

Dirección de Internet: svpnf.itccanarias.org

Nombre del destino: ITC\_VPN

☐ Usar una tarjeta inteligente

☐ Permitir que otras personas usen esta conexión

Esta opción permite el uso de esta conexión para cualquier persona con acceso a este equipo.

☒ No conectarse ahora; configurar para conectarse más tarde

Siguiente Cancelar

En la siguiente pantalla se pedirán el usuario y contraseña de acceso a la VPN. Los miembros de FAP autorizados para el acceso son: Carlos Coloma, Enrique García, Juan Antonio Hernández y Miguel Bravo. En dicha pantalla se puede marcar la opción de “Recordar esta contraseña” para que no esté pidiendo estos parámetros cada vez se quiera conectar a la VPN. Este último paso queda a decisión personal de cada uno. Finalmente se debe pinchar en el botón “Crear”.

Conectarse a un área de trabajo

Escriba el nombre de usuario y la contraseña

Nombre de usuario: mjbravo

Contraseña: .....

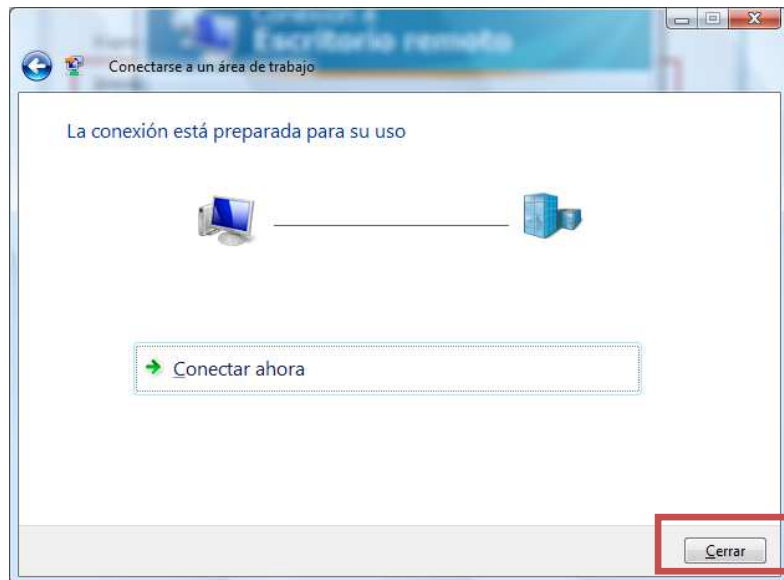
☐ Mostrar caracteres

☒ Recordar esta contraseña

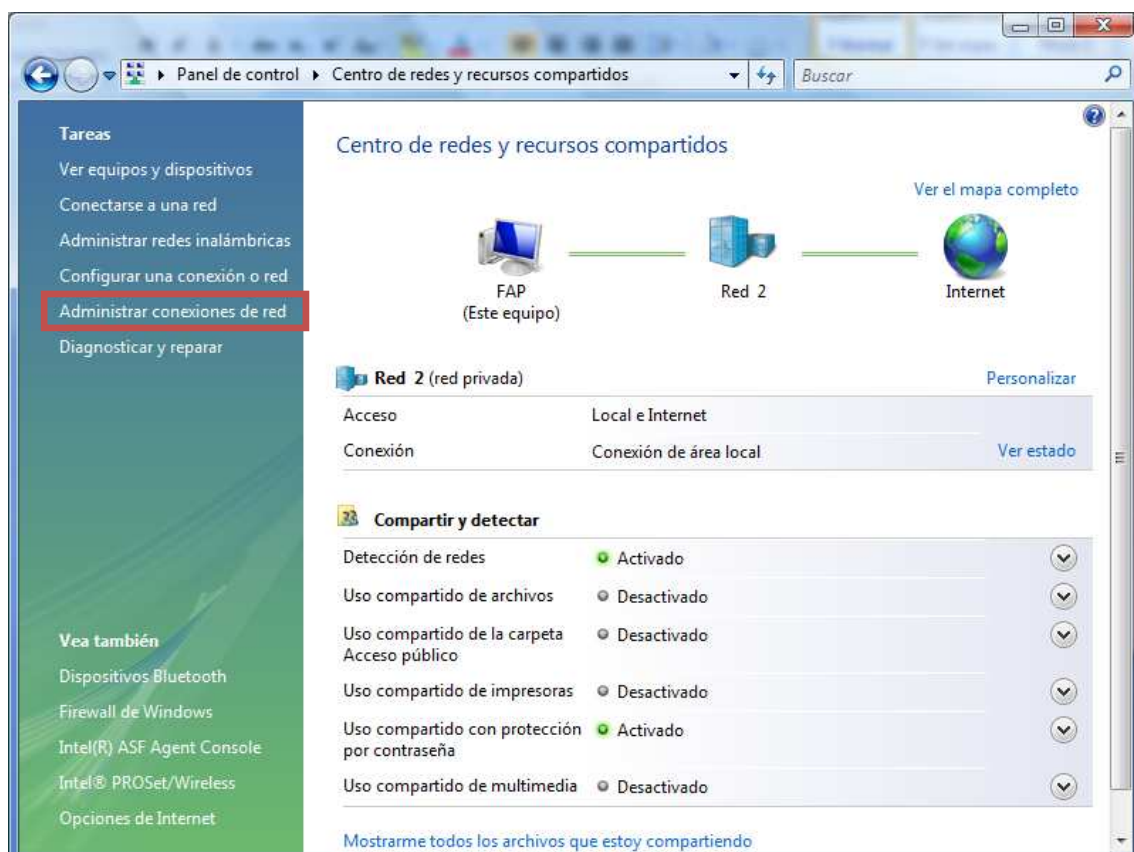
Dominio (opcional):

Crear Cancelar

Se debe finalizar el proceso pulsando el botón de cerrar. Se debe tener cuidado en este último paso ya que si se pincha en conectar ahora no se guardará la conexión que se acaba de crear y debemos repetir el proceso.

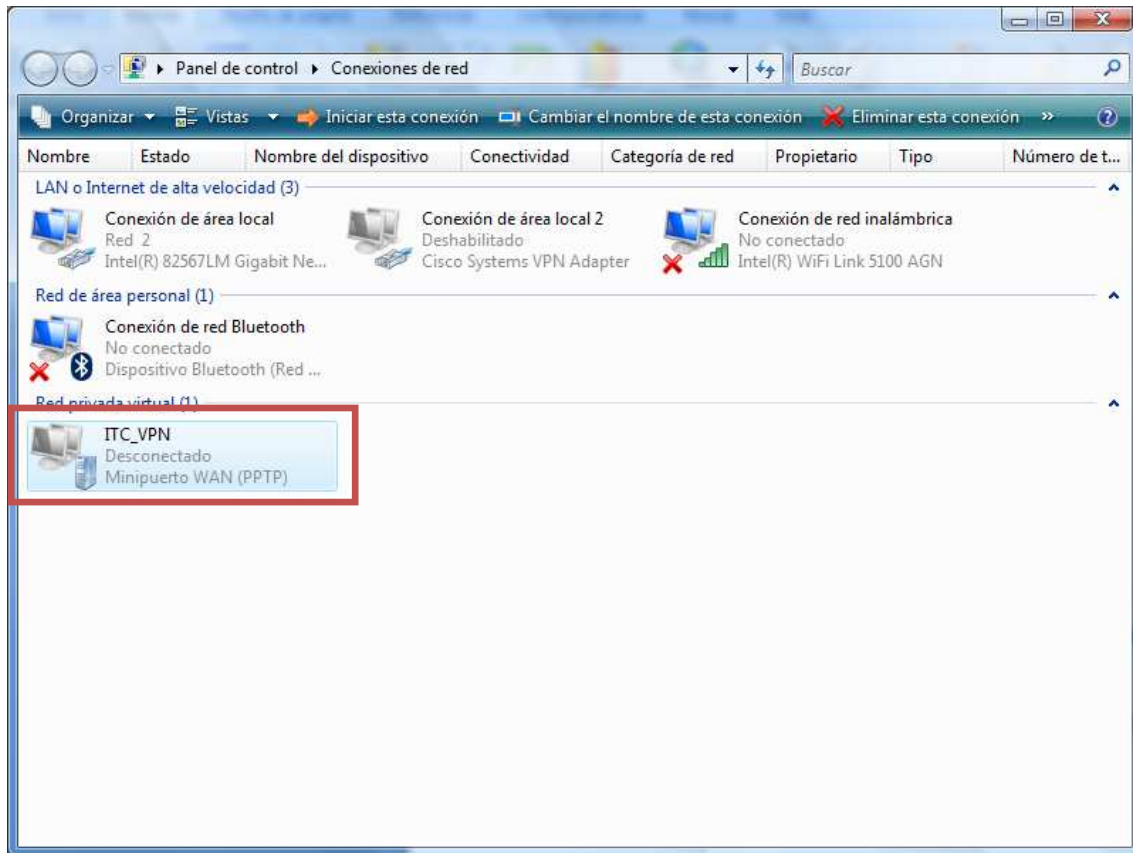


Por último, para conectarse a la VPN de ITC debemos volver al menú "Centro de redes y recursos compartidos" y seleccionar la opción "Administrar conexiones de red"

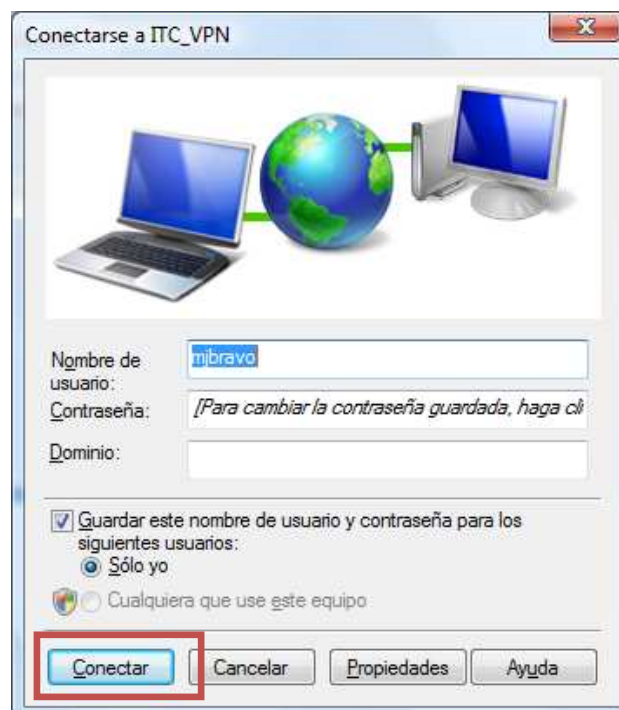




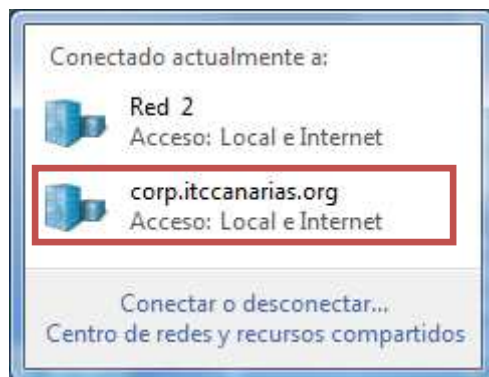
En el menú que se abre, hacer doble click sobre la conexión VPN\_ITC



Pinchar en el botón “Conectar”



Si todo ha ido bien, debería aparecer la conexión de red del itc en el icono de las redes a las que se está conectado que está situado junto al reloj del sistema.



### Segundo paso: Acceso a las máquinas

Actualmente existen tres máquinas a las que tenemos acceso:

**TUCANA:** Máquina de **PRODUCCIÓN** donde se encuentra el AED de la ACIISI y que parece que tiene instalados los certificados necesarios para consumir los servicios de **platino**. Se debe tener **especial cuidado** con lo que se instala en esta máquina para que no entre en conflicto con las aplicaciones que se encuentran en producción. **Es de vital importancia conocer que cosas tiene instaladas para no romper el trabajo de los demás**. En el momento de la redacción de este manual, el equipo de desarrollo de FAP-Devel se encuentra a la espera de recibir un correo de la gente de Arte Consultores en el que se comente que tienen instalado en esa máquina. En caso de que sea necesario utilizar dicha máquina y no se disponga de dicha información se debe avisar a Daniel González para que mueva los hilos necesarios para obtenerla. En este servidor se debe poner en funcionamiento la aplicación de **PORTAFIRMA** y los programas asociados para su correcto funcionamiento.

**VESPA:** Máquina de **PRODUCCIÓN** sin acceso a los servicios de Platino donde se encuentra instalada la aplicación de congresos. Actualmente tiene instalado Jboss 5.1 con CXF, MySQL 5.x versión 64bits, OpenOffice como servicio y un servidor FTP para transferir archivos. Tanto el Jboss como el servidor FTP deben arrancarse a mano una vez que sea necesario. El Jboss se encuentra instalado también como servicio y se puede configurar para que arranque cada vez que se reinicia la máquina, pero se ha dejado con arranque manual para poder ver la consola. En este servidor se deben poner las nuevas versiones que saquemos de **CONGRESOS**. Sería recomendable instalar apache en este servidor para filtrar el acceso a la consola de administración de Jboss etc. Tanto la **máquina** como el **servidor de aplicaciones no deben ser reiniciados en horas laborables** en las que los usuarios puedan estar accediendo a las mismas. Por ello se debe **escoger una hora prudencial**, especialmente en horario de **tarde**, para **desplegar nuevas versiones y realizar las distintas operaciones que sean necesarias**. Por último, comentar que en el directorio c:\ft puploads\ se está llevando el **control de las distintas versiones de la aplicación de congresos que se han puesto en producción**. Cada nueva **versión** que se ponga en la misma debe estar incluida en un **directorío con la fecha** en la que se pone en producción en el **formato aaaammdd**.

**ORIÓN:** Máquina de **PREPRODUCCIÓN** sin acceso a los servicios de Platino totalmente **virgen**. En el momento de la redacción de este manual no se ha procedido a la instalación de ninguno de los programas necesarios para la puesta en pre-explotación de cualquiera de las aplicaciones desarrolladas en fap-devel. **Se debe afrontar esta puesta a punto del servidor cuando se vaya a sacar algún nuevo entregable.** Aunque no está confirmado, las versiones de **TESIS y ESTANCIAS** deberán ser instaladas en este servidor antes de su puesta en explotación. Al igual que en VESPA, sería recomendable instalar apache en este servidor para filtrar el acceso a la consola de administración de Jboss etc.

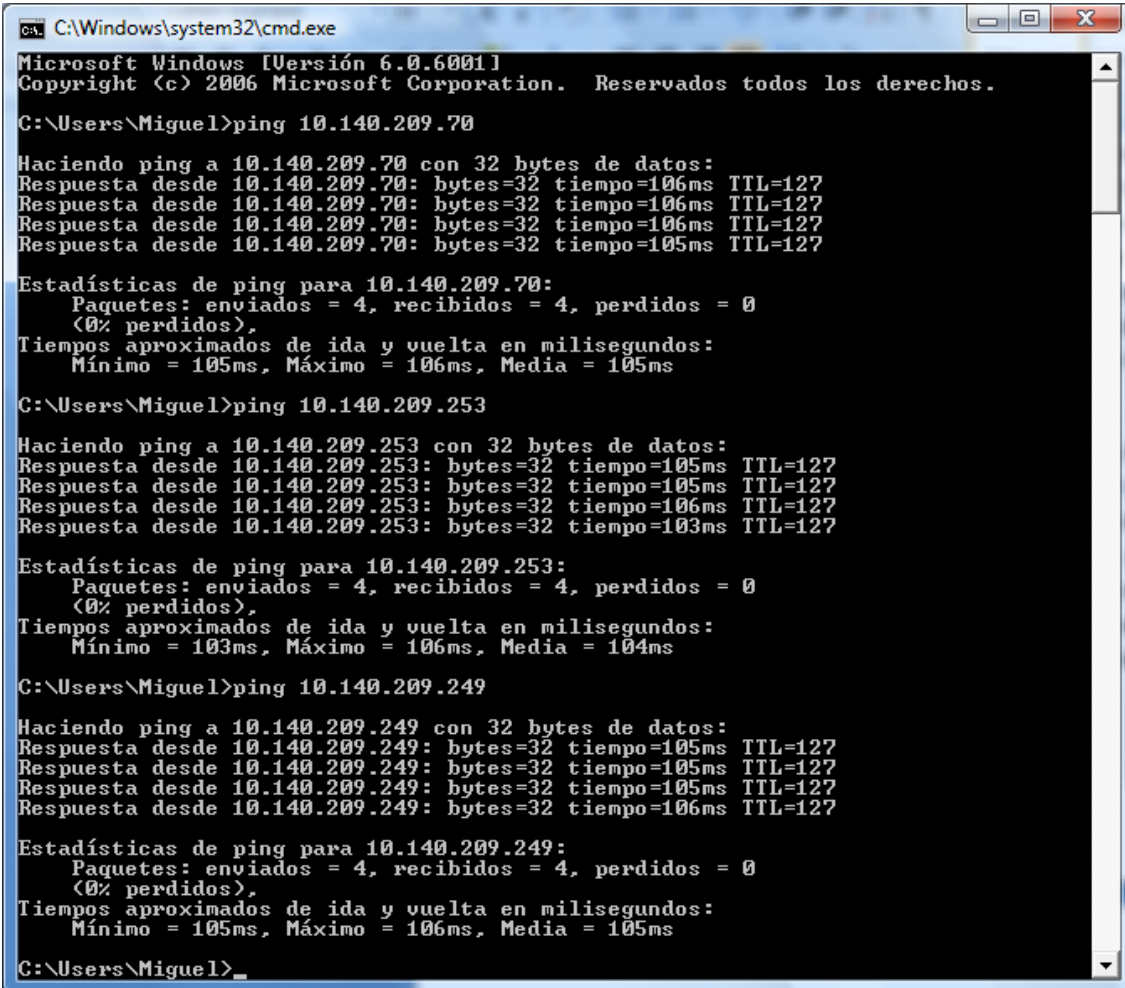
La dirección IP de dichas máquinas es:

**TUCANA 10.140.209.70**

**VESPA 10.140.209.253**

**ORIÓN 10.140.209.249**

Para comprobar que el acceso a la VPN del ITC ha sido correcto se puede hacer un ping a dichas máquinas.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Miguel>ping 10.140.209.70

Haciendo ping a 10.140.209.70 con 32 bytes de datos:
Respuesta desde 10.140.209.70: bytes=32 tiempo=106ms TTL=127
Respuesta desde 10.140.209.70: bytes=32 tiempo=106ms TTL=127
Respuesta desde 10.140.209.70: bytes=32 tiempo=106ms TTL=127
Respuesta desde 10.140.209.70: bytes=32 tiempo=105ms TTL=127

Estadísticas de ping para 10.140.209.70:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 105ms, Máximo = 106ms, Media = 105ms

C:\Users\Miguel>ping 10.140.209.253

Haciendo ping a 10.140.209.253 con 32 bytes de datos:
Respuesta desde 10.140.209.253: bytes=32 tiempo=105ms TTL=127
Respuesta desde 10.140.209.253: bytes=32 tiempo=105ms TTL=127
Respuesta desde 10.140.209.253: bytes=32 tiempo=106ms TTL=127
Respuesta desde 10.140.209.253: bytes=32 tiempo=103ms TTL=127

Estadísticas de ping para 10.140.209.253:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 103ms, Máximo = 106ms, Media = 104ms

C:\Users\Miguel>ping 10.140.209.249

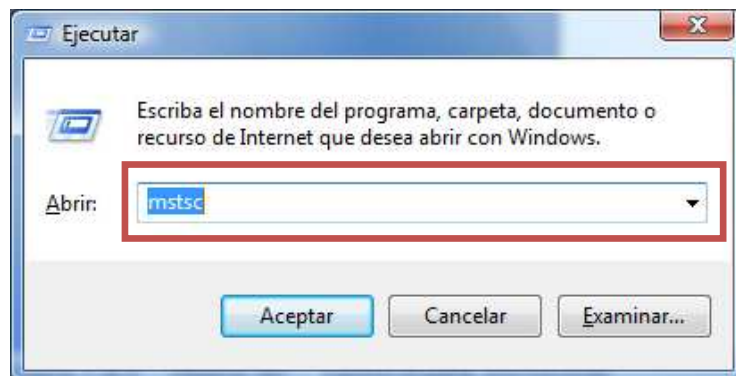
Haciendo ping a 10.140.209.249 con 32 bytes de datos:
Respuesta desde 10.140.209.249: bytes=32 tiempo=105ms TTL=127
Respuesta desde 10.140.209.249: bytes=32 tiempo=105ms TTL=127
Respuesta desde 10.140.209.249: bytes=32 tiempo=105ms TTL=127
Respuesta desde 10.140.209.249: bytes=32 tiempo=106ms TTL=127

Estadísticas de ping para 10.140.209.249:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 105ms, Máximo = 106ms, Media = 105ms

C:\Users\Miguel>
```



Comentar que todas estas máquinas disponen de un SO **Windows Server 2003** y debemos conectarnos a ellas mediante un **cliente de Terminal Server**. Para ello vamos a la opción del menú de inicio de Windows “Ejecutar” y escribimos el comando “mstsc” y pulsamos el botón aceptar.



A continuación, se abrirá el programa mediante el que nos conectaremos a la máquina. En el campo “Equipo” debemos poner la dirección IP de la máquina a la que nos queremos conectar, en este caso a VESPA. Introducimos la dirección y pinchamos en el botón “Conectar”.



Pedirá confirmación de conexión, se debe pinchar en el botón “Sí”.



Finalmente, debe abrirse una ventana en la que se solicita introducir el login y password facilitados para el acceso a la VPN del ITC. Además, debe seleccionarse el dominio CORP en la pestaña "Conectarse a". Por último se debe pinchar en "Aceptar".



Pasados unos segundos, entraremos al escritorio de la máquina como si estuviéramos accediendo a ella de forma local. En mi caso, aparecen una serie de consolas que se quedaron abiertas en la sesión anterior.

