

Manual para conectar a la VPN del ITC en Windows Vista y acceso a los servidores de pre-explotación y explotación desde la red de la Universidad de La Laguna.

En este documento se explica el procedimiento para instalar y configurar el cliente OpenVPN en una máquina con Windows Vista, para poder conectarla con el servidor OpenVPN que se encuentra en las instalaciones del ITC en Sixto Machado y así poder acceder a los servidores de pre-explotación y explotación.

1. Hay que descargar la versión de OpenVPN 2.1 rc19 que funciona correctamente bajo Windows Vista. Se puede descargar del siguiente enlace:

http://www.openvpn.net/release/openvpn-2.1_rc19-install.exe

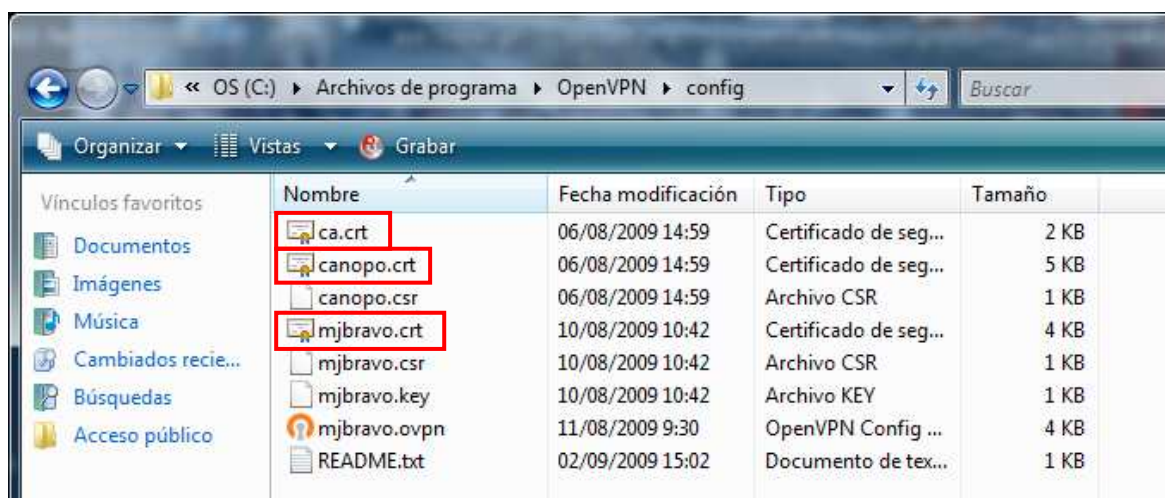
Se debe instalar la aplicación con sus opciones por defecto.

2. Una vez instalada la aplicación se debe extraer los ficheros del zip adjunto a este correo en la siguiente ruta "C:\Archivos de programas\OpenVPN\config".

Los ficheros que contiene el zip son los siguientes:

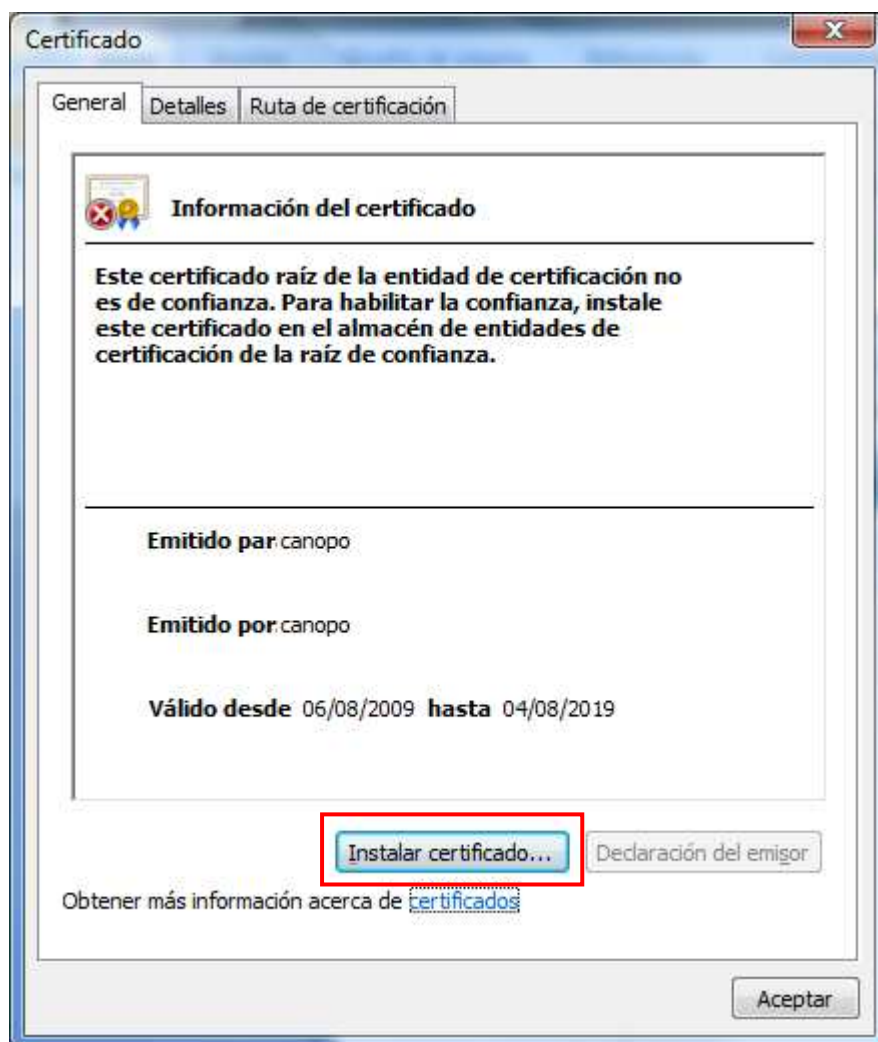
- Usuario.ovpn: Fichero de configuración del cliente OpenVPN.
- ca.crt: Certificado de la entidad certificador.
- canopo.crt: Certificado del servidor.
- usuario.crt: Certificado del cliente.
- usuario.key: Clave del cliente.
- usuario.csr: Petición de Firma de Certificado.

3. Instalar certificados en la máquina del cliente. Se tiene que instalar todos los certificados que se encuentran en la carpeta "config" (son aquellos ficheros con extensión ". crt").

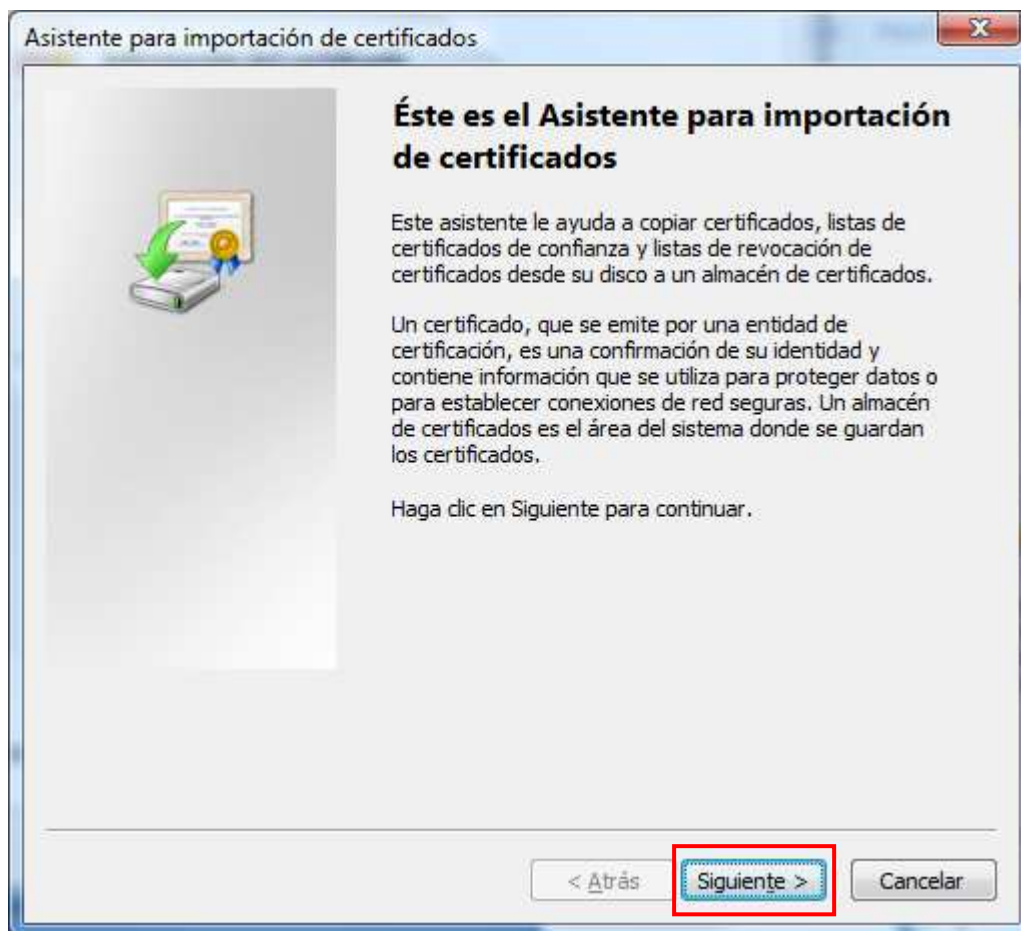


Para instalar un certificado se debe hacer doble click sobre el mismo y seguir los siguientes pasos:

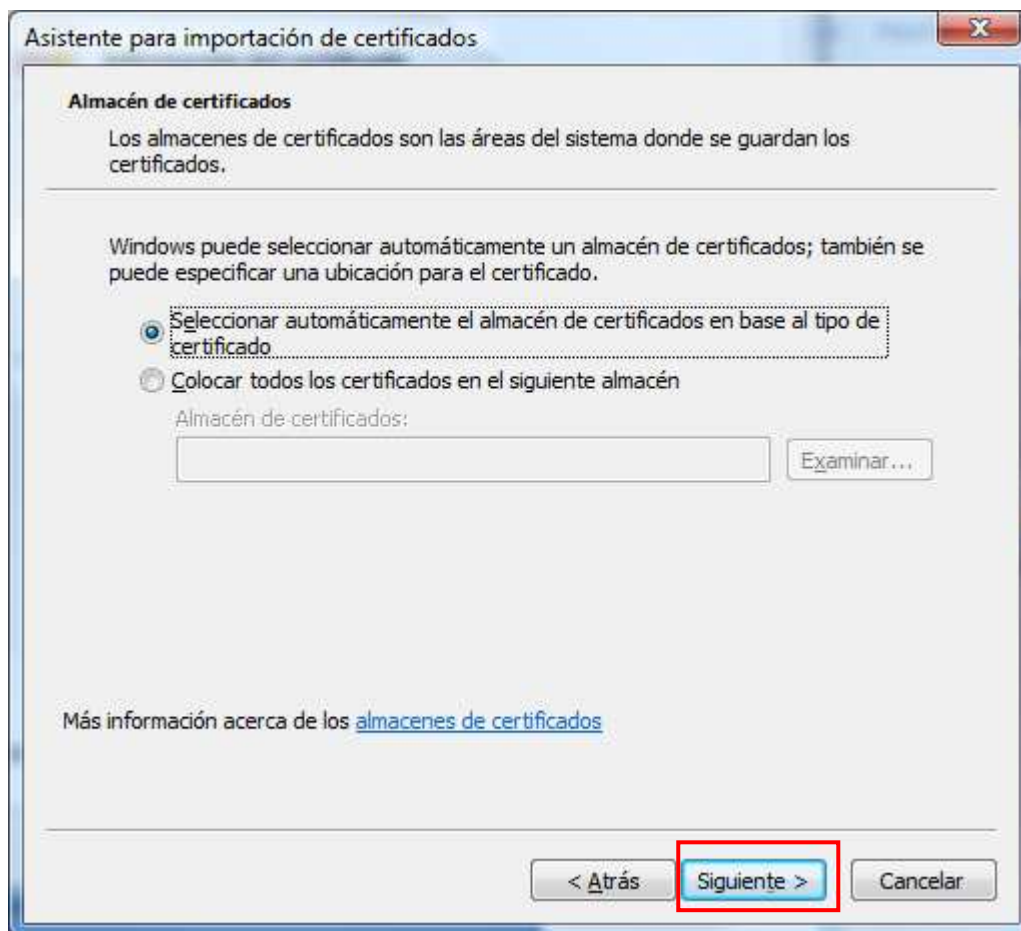
Click en “Instalar certificado...”



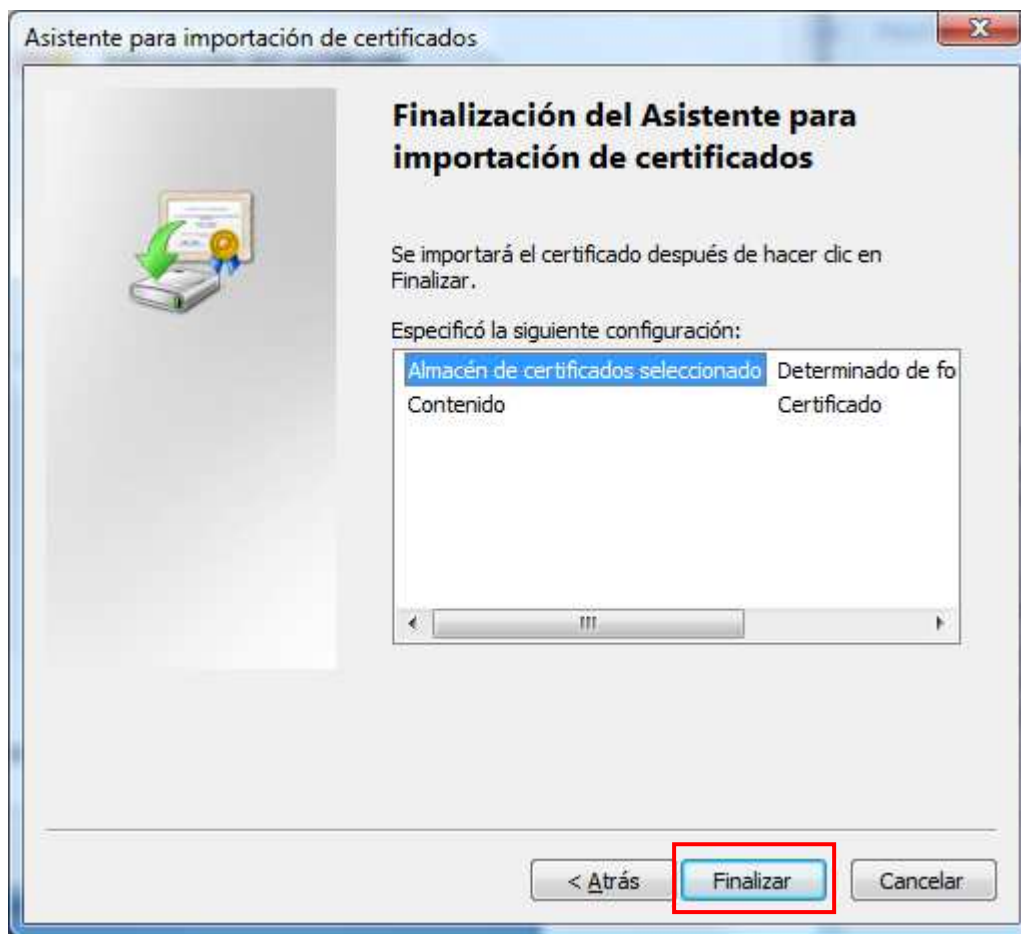
Click en “Siguiente”



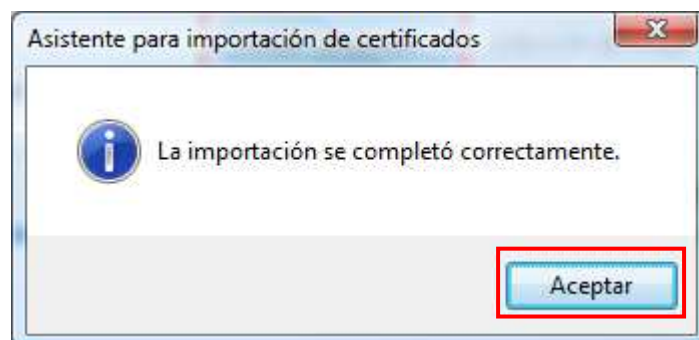
Dejar las opciones por defecto y hacer click en “Siguiente”.



Dejar las opciones por defecto y hacer click en “Finalizar”.

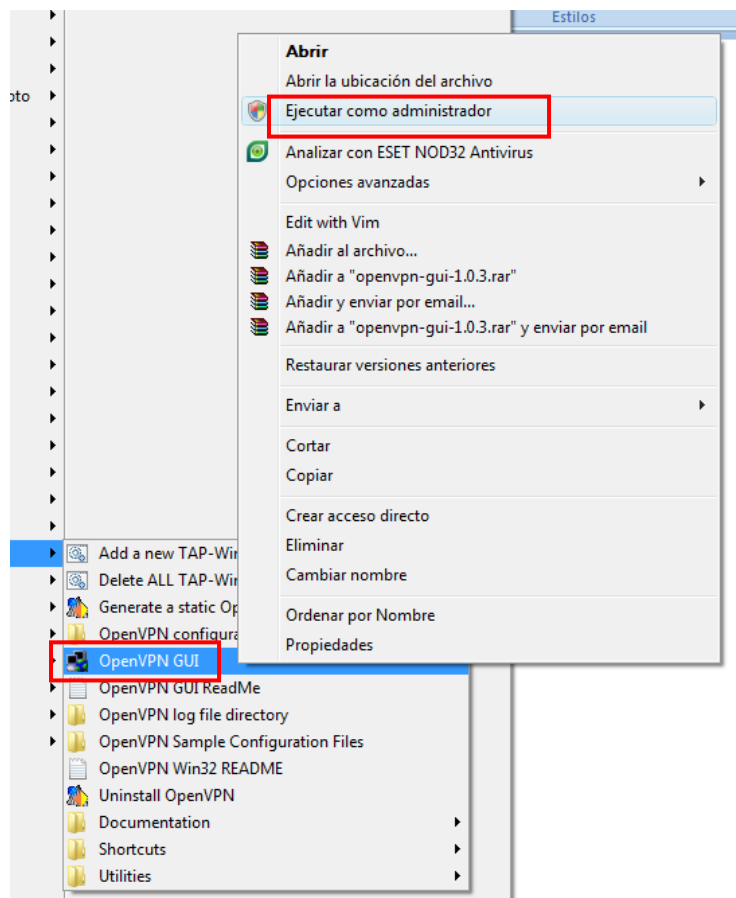
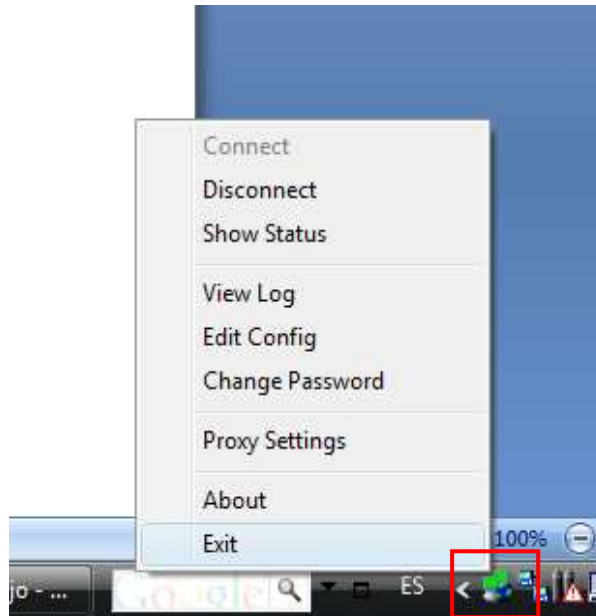


Si todo ha ido correctamente debe aparecer este mensaje. Salimos haciendo click en “Aceptar” en dicho mensaje y en la pantalla anterior.

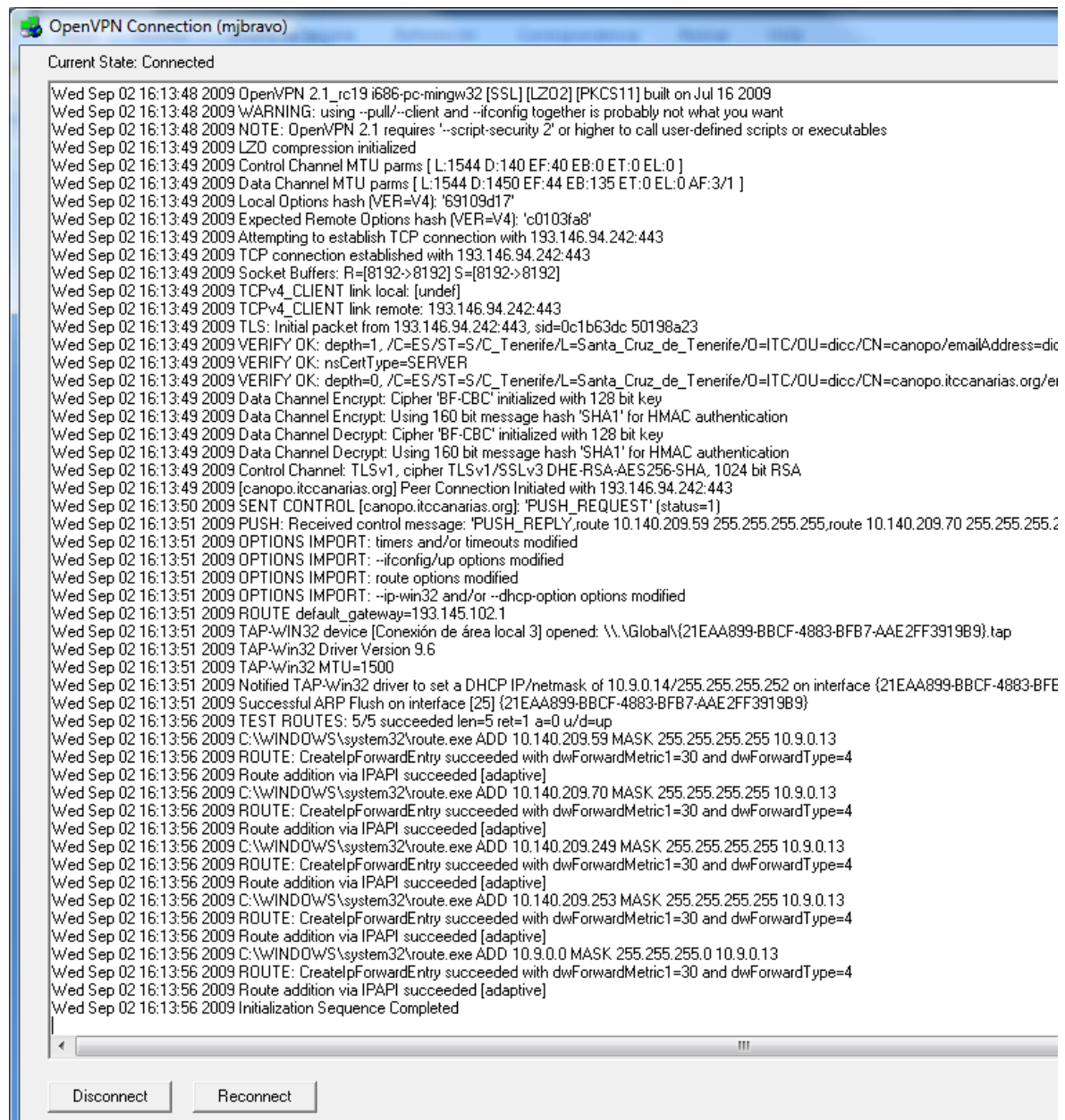


Una vez instalados los tres certificados y la aplicación se recomienda reiniciar el equipo.

4. Después de reiniciar el equipo, puede que la aplicación aparezca como programa residente en la barra de tareas junto al reloj. Para que la aplicación funcione correctamente debemos cerrarla y volver a abrirla pero esta vez se debe “Ejecutar como administrador”.



Una vez se ha ejecutado la aplicación como administrador, se debe hacer doble click sobre el icono de la barra del reloj para que se conecte y muestre el log de conexión. Si todo ha ido bien, el log que muestra es el siguiente:



Finalmente realizamos ping a las direcciones 10.9.0.1 y 10.140.209.253 para comprobar que todo está correcto.

```
C:\Users\Miguel>ping 10.9.0.1

Haciendo ping a 10.9.0.1 con 32 bytes de datos:
Respuesta desde 10.9.0.1: bytes=32 tiempo=108ms TTL=64
Respuesta desde 10.9.0.1: bytes=32 tiempo=109ms TTL=64
Respuesta desde 10.9.0.1: bytes=32 tiempo=108ms TTL=64
Respuesta desde 10.9.0.1: bytes=32 tiempo=107ms TTL=64

Estadísticas de ping para 10.9.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 107ms, Máximo = 109ms, Media = 108ms

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=110ms TTL=127
Respuesta desde 10.140.209.253: bytes=32 tiempo=109ms TTL=127
Respuesta desde 10.140.209.253: bytes=32 tiempo=108ms TTL=127
Respuesta desde 10.140.209.253: bytes=32 tiempo=108ms 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 = 108ms, Máximo = 110ms, Media = 108ms
```

Para acceder a las máquinas debe consultarse el segundo paso del manual “Manual VPN ITC y servidores” en el que se comenta como acceder, mediante Terminal Server, a las distintas máquinas.