HERRAMIENTAS DE TRABAJO REMOTO

ÍNDICE

HERRAMIENTAS DE TRABAJO REMOTO

ACCESO A LA RED DEL INSTITUTO

Para formar parte de la red interna del instituto desde una ubicación remota (e.g. en el hogar) alcanza con disponer de una conexión a Internet y configurar una VPN (red privada virtual) que permita establecer conexiones seguras y confiables. Para ello, utilizamos el software OpenVPN que está disponible para Windows, Linux y macOS. Además de la cuenta y su contraseña, cada usuario de la red precisa un certificado digital, personal e intransferible, que debe ser expedido por la Unidad de Recursos Informáticos.

Paso 1: obtención de certificados digitales

Debe solicitar sus certificados escribiendo un e-mail a soporte@pasteur.edu.uy. Se le enviará una respuesta con un ZIP conteniendo cuatro archivos:

- ca.crt
- client.crt
- client.key
- pasteur.ovpn (el nombre puede variar)

Este ZIP debe ser extraído en cualquier carpeta para ser utilizado luego durante la configuración de la VPN.

Paso 2: instalación de OpenVPN

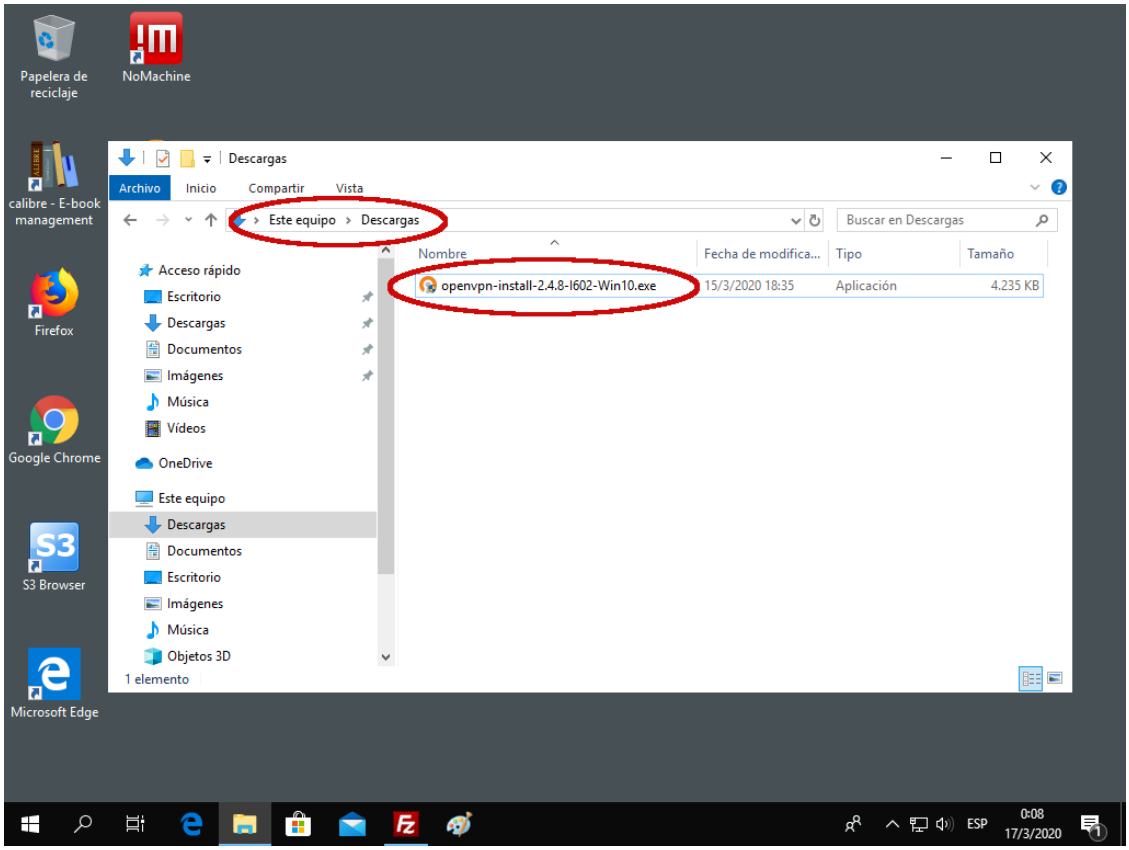
En las siguientes instrucciones podrá obtener información sobre cómo instalar la VPN en los distintos sistemas operativos soportados por la Unidad de Recursos Informáticos. Si encuentra problemas durante la configuración o si el procedimiento le resulta complejo para llevarlo a cabo por cuenta propia, tenga a bien escribir a soporte@pasteur.edu.uy para solicitar asistencia remota (mediante TeamViewer). Por favor, evite en lo posible llevar su laptop a la oficina de la unidad para su configuración dado que, por motivos obvios, en estos momentos no contamos con capacidad para atender in situ todas las solicitudes.

Instalación de la VPN en Windows

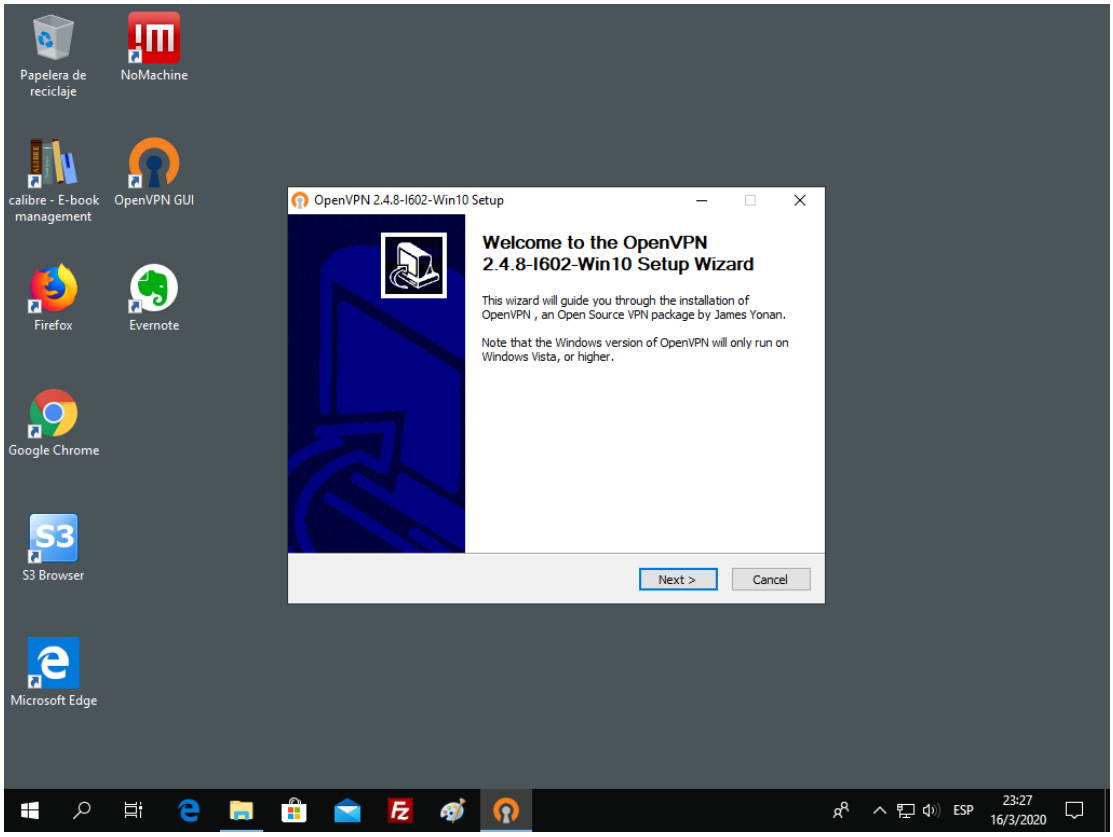
Con soporte únicamente para Windows 10. Podría funcionar en versiones anteriores. No es compatible con Windows XP o anteriores. Es recomendable tener las actualizaciones más recientes (1909).

Siga estos pasos en la computadora **desde la que quiere conectarse** a la red interna de Pasteur (e.g. desde su hogar). No es necesario realizar ninguna acción en los equipos (estaciones, servidores, etc.) del instituto sobre los cuales desea trabajar una vez conectado a la VPN. Usted precisa disponer de un certificado digital.

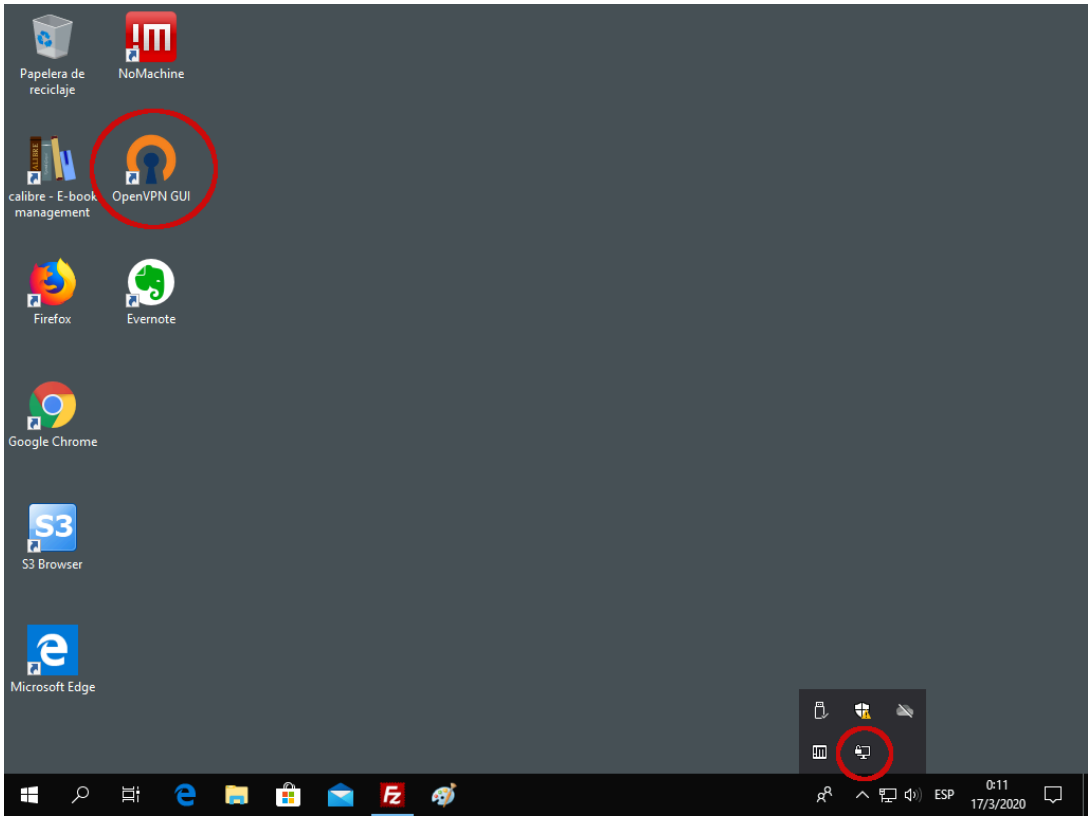
Descargue el programa para Windows 10 desde aquí. Si utiliza una versión anterior de Windows, utilice este enlace. Esta configuración no está soportada para Windows XP o anteriores; en ese caso, tenga a bien consultar por e-mail a la dirección **soporte@pasteur.edu.uy**. Guarde el archivo descargado en una carpeta que pueda recordar (e.g. Descargas).



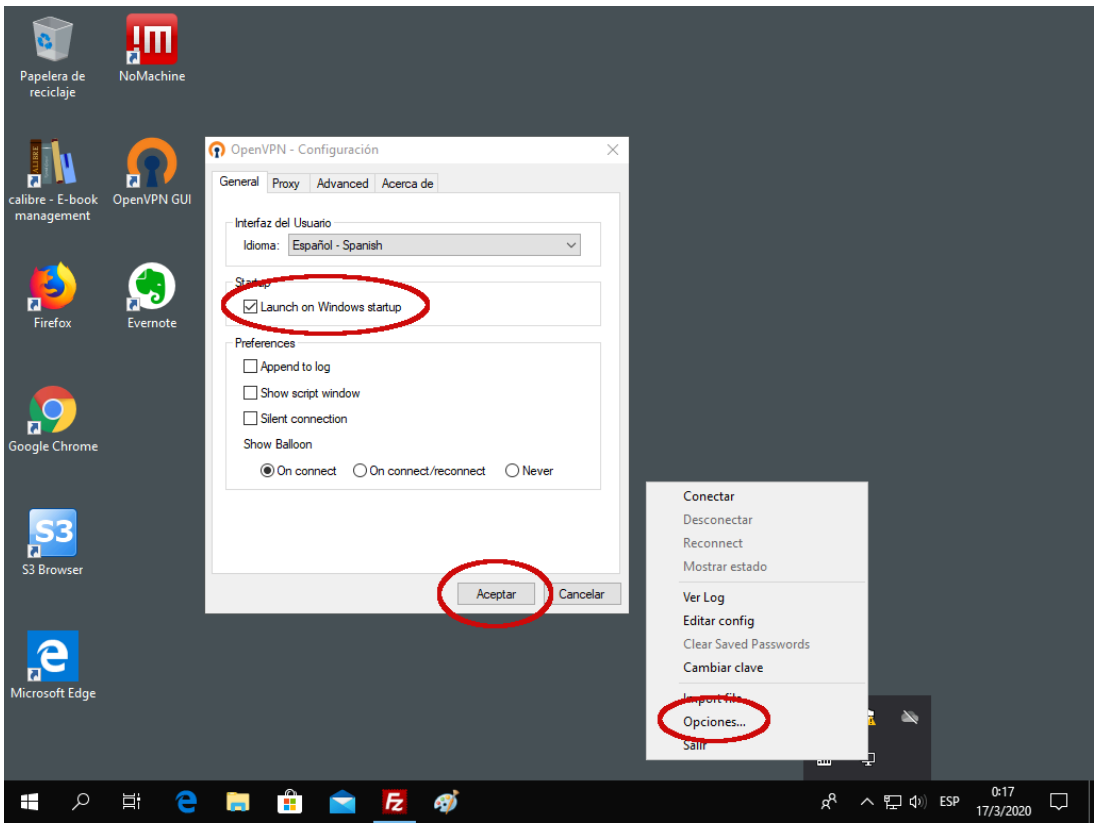
Ejecute la instalación (doble click sobre el archivo descargado) dejando todas las opciones por defecto (siguiente, siguiente... finalizar).



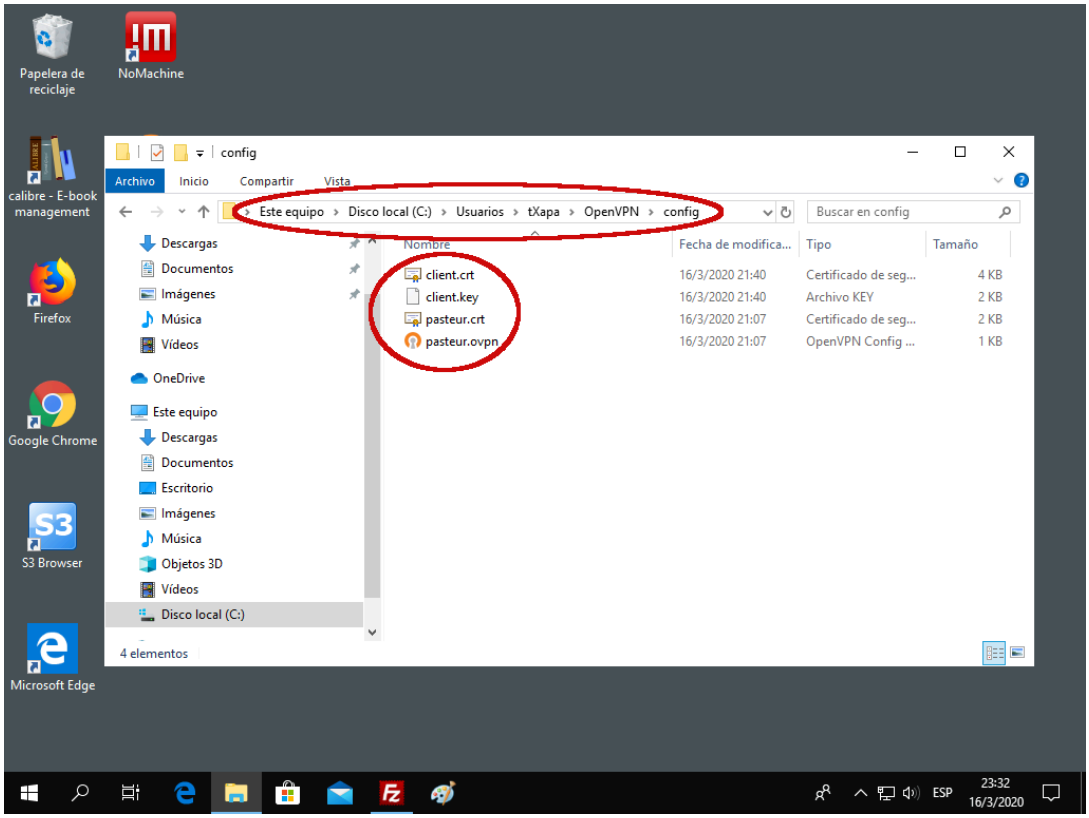
Ejecute OpenVPN haciendo doble click sobre el ícono que apareció en el escritorio. El programa ahora se podrá controlar desde la bandeja del sistema, en la esquina inferior derecha (parecido a un monitor con candado).



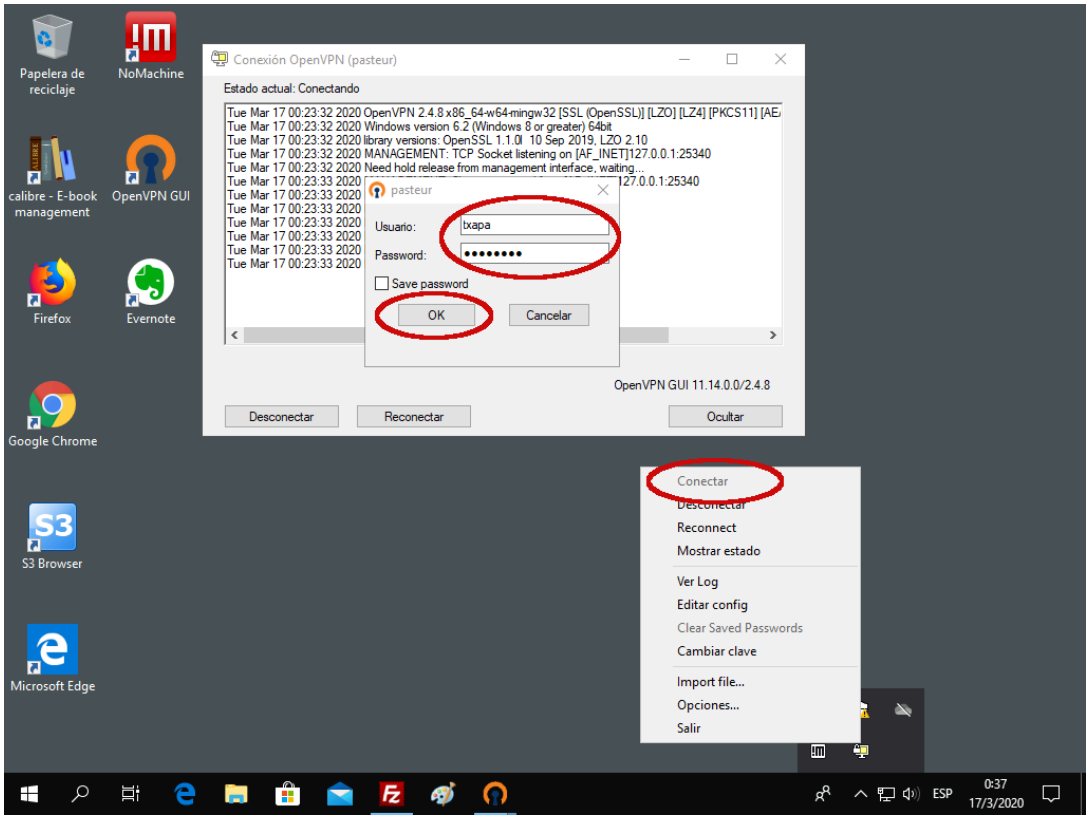
Haga click con el botón derecho sobre el ícono de OpenVPN en la bandeja del sistema (el del monitor con candado) y seleccione 'Opciones...'. En el diálogo a continuación, dentro de la pestaña 'General', marque la casilla 'Launch on Windows startup' para ejecutar OpenVPN en cada inicio del sistema y presione 'Aceptar'.



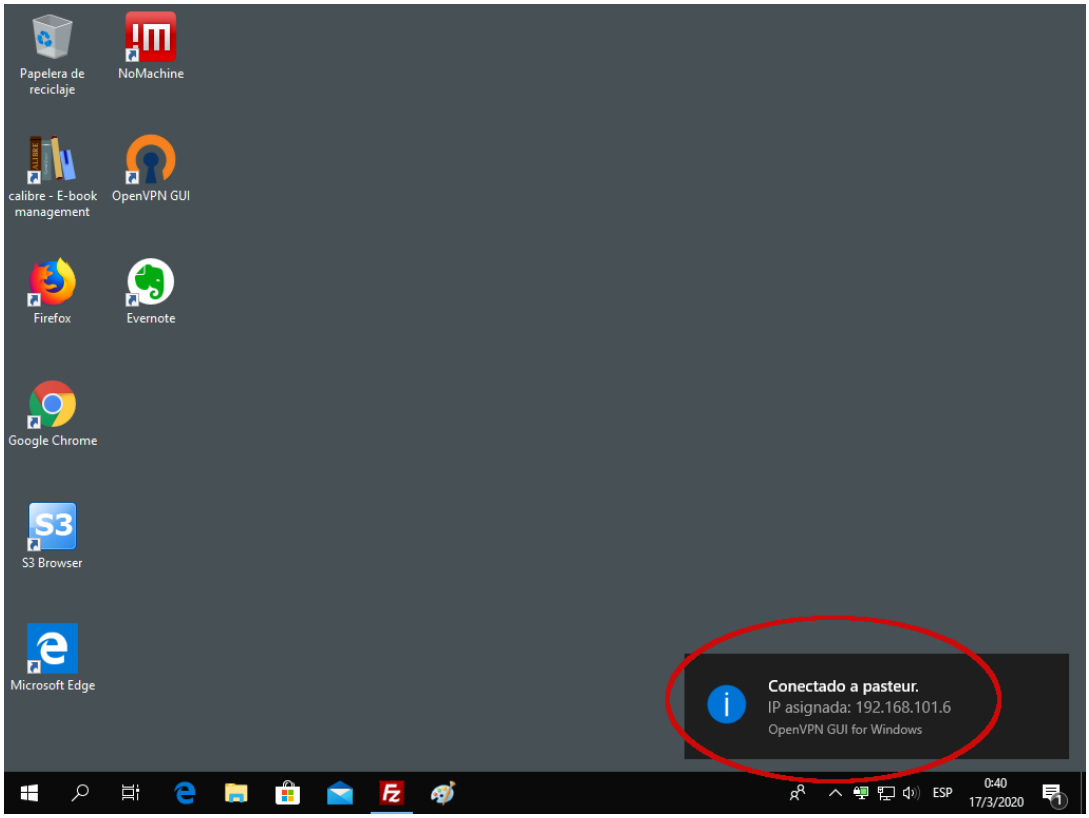
Copie los cuatro archivos extraidos del ZIP en **C:\Usuarios\<su nombre>\OpenVPN\config** (cambie <su nombre> por el nombre de usuario que utiliza en Windows). En la imagen siguiente, los archivos fueron copiados en la carpeta del usuario tXapa.



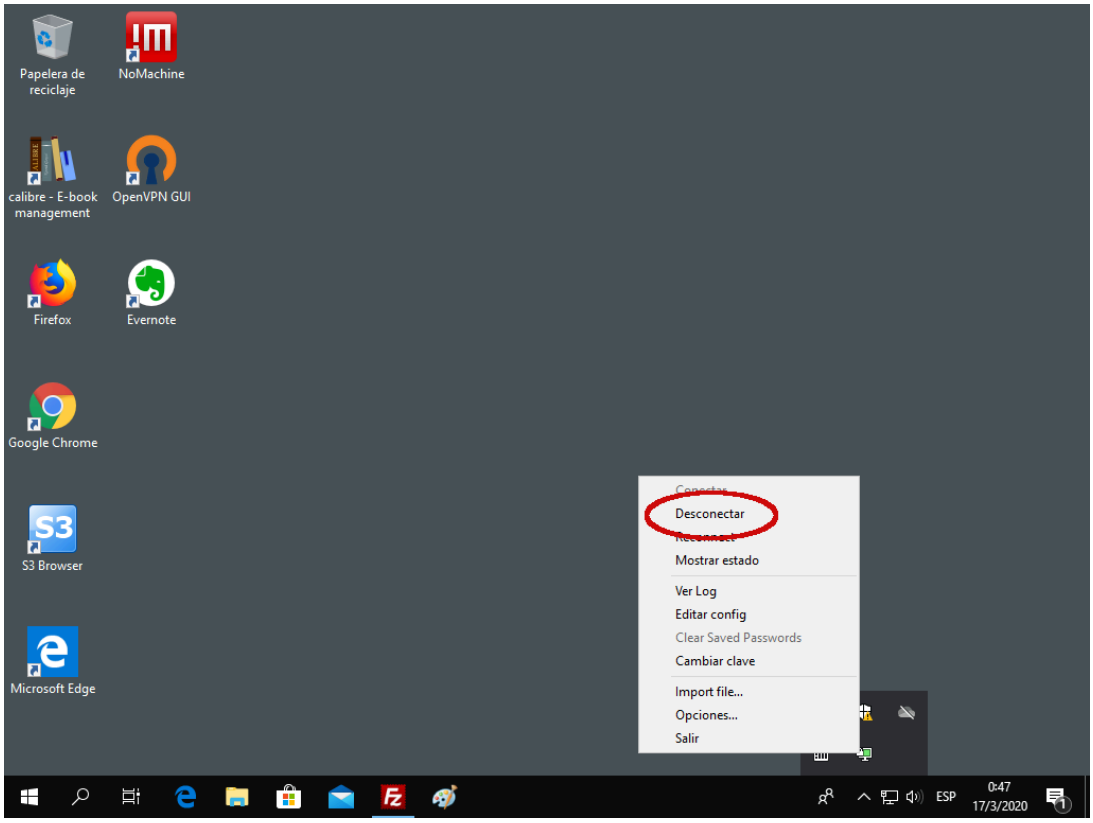
La VPN está ahora instalada y configurada. Solo resta establecer una conexión a la red del instituto cada vez que se precise. Para ello, deberá hacer click con el botón derecho en el ícono de OpenVPN (en la esquina inferior derecha, el del monitor con candado) y pulsar la opción 'Conectar'. Aparecerá una ventana de diálogo solicitando sus credenciales (nombre de usuario y contraseña de Pasteur).



Aguarde unos instantes mientras se establece la conexión. Una vez establecida, aparecerá una notificación en la esquina inferior derecha indicando su dirección IP en la red del instituto. ¡Felicitaciones! Ya puede comenzar a utilizar recursos internos desde una ubicación remota.



Por favor, una vez que termine de utilizar recursos de la red interna, no olvide desconectar la VPN. Esto redundará en un mejor aprovechamiento del ancho de banda y una mayor calidad del resto de sus conexiones a Internet (que ya no estarán pasando por Pasteur). Para ello, deberá hacer click con el botón derecho en el ícono de OpenVPN en la bandeja del sistema (abajo a la derecha) y seleccionar la opción 'Desconectar'.



Instalación de la VPN en Linux

Con soporte únicamente para Fedora 28 y posteriores. Podría funcionar en otras distribuciones (Ubuntu, Mint, Arch, etc.) siempre y cuando utilicen una versión moderna de GNOME. Debería funcionar en otros escritorios (KDE, XFCE, etc.) e incluso sin entorno gráfico (NetworkManager) aunque no sabemos cómo.

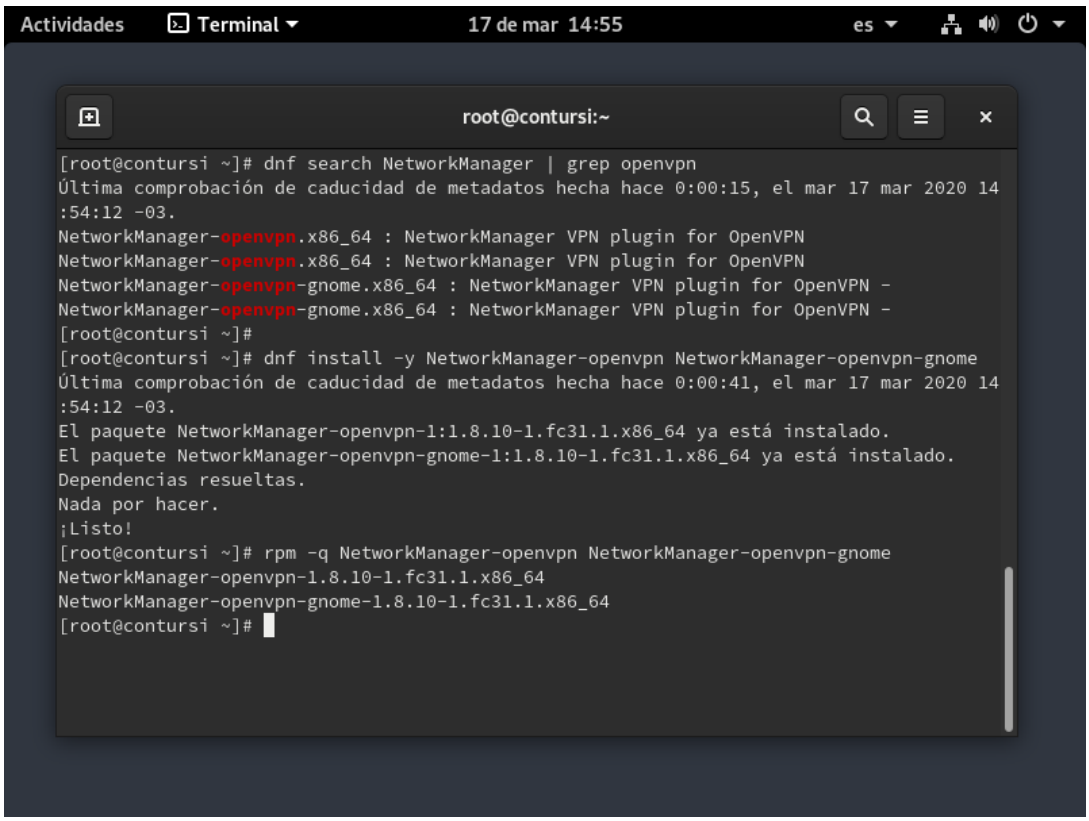
Siga estos pasos en la computadora desde la que quiere conectarse a la red interna de Pasteur (e.g. desde su hogar). No es necesario realizar ninguna acción en los equipos (estaciones, servidores, etc.) del instituto sobre los cuales desea trabajar una vez conectado a la VPN. Usted precisa disponer de un certificado digital.

Estas instrucciones funcionan sobre Fedora 28 y posteriores usando GNOME como entorno de escritorio. Es probable que la mayor parte funcione también en otras distribuciones (Ubuntu, Mint, Arch, etc.) para los que la Unidad de Recursos Informáticos no ofrece soporte. En tales casos, la resolución de problemas queda a cargo del usuario.

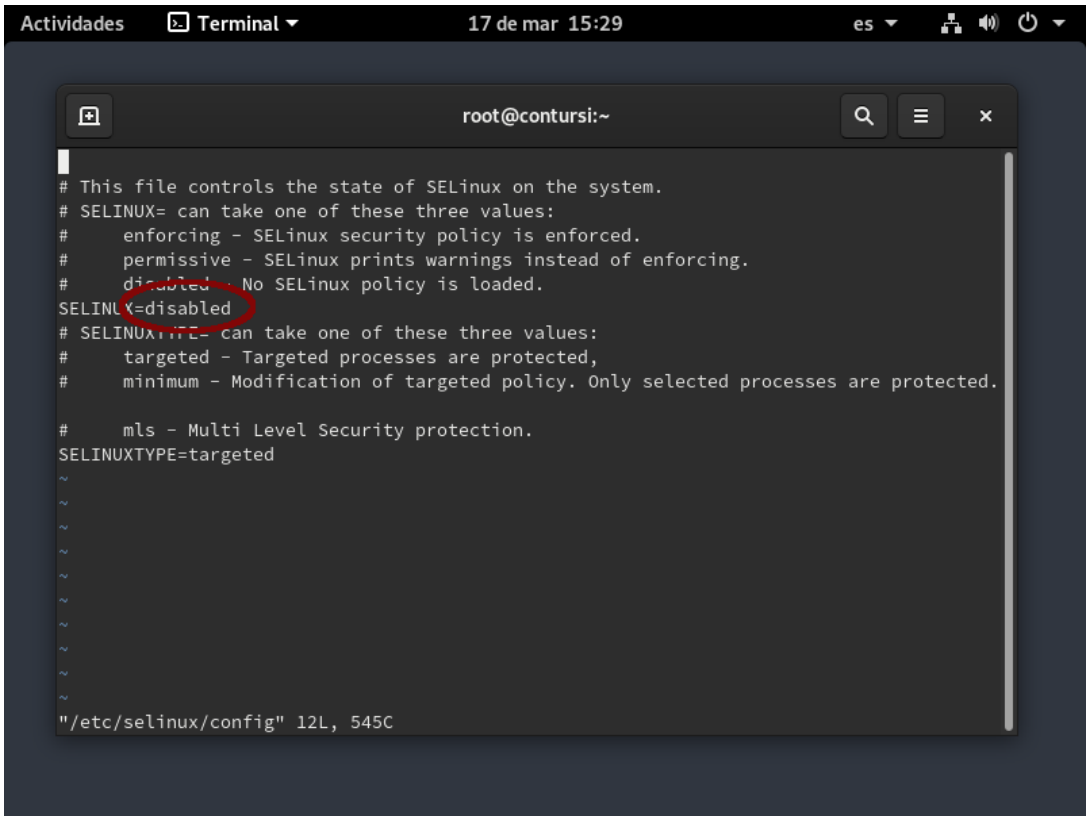
Si usted está conectado a Internet desde un entorno gráfico, es casi seguro que ya tenga instalado NetworkManager (el gestor de redes de GNOME). Debe instalar además el plugin de NetworkManager para OpenVPN y el applet de GNOME para el plugin anterior. Puede ejecutar el siguiente comando como root.

```
dnf install -y NetworkManager-openvpn NetworkManager-openvpn-gnome
```

La siguiente imagen muestra la situación más común en Fedora 28 y posteriores. En este caso, ya se encontraban instalados todos los paquetes necesarios (como parte de la instalación estándar de Fedora 31).



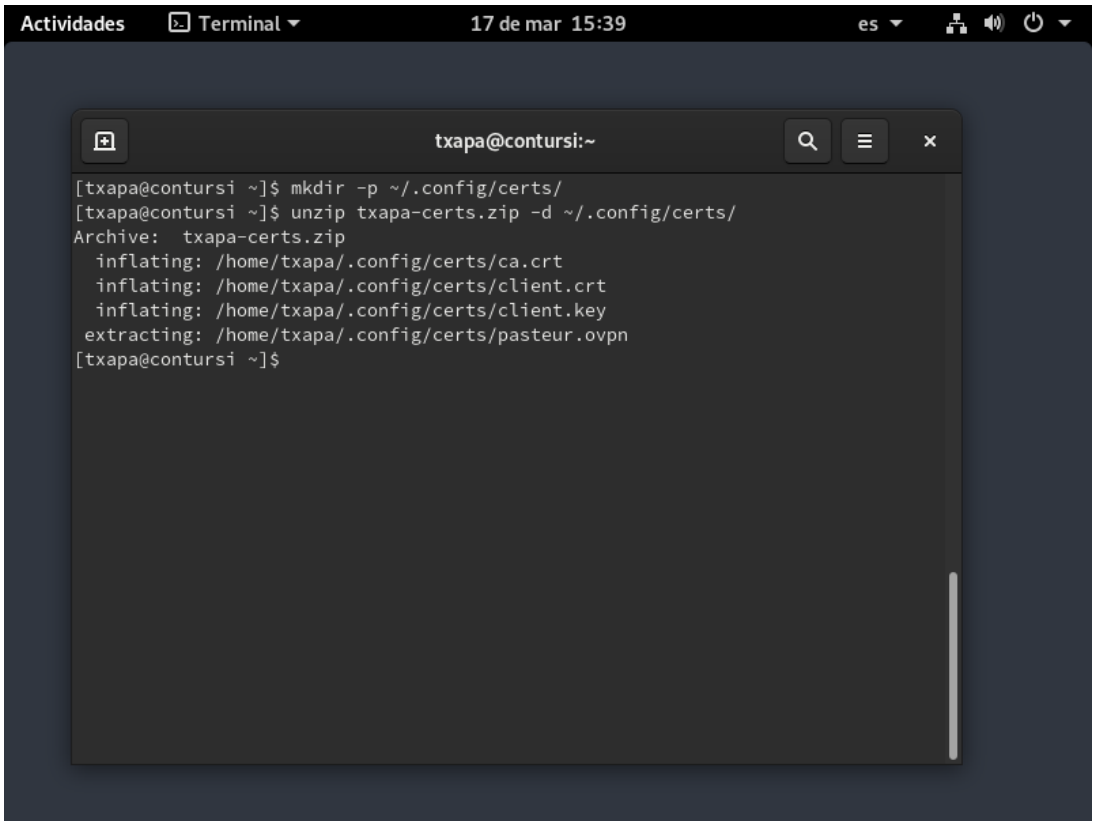
Este paso es opcional pero le evitará problemas; le sugerimos completarlo a menos que sepa lo que está haciendo. Como root, deshabilite SELinux editando el archivo de configuración /etc/selinux/config. Luego de salvarlo, **reinicie la computadora**.



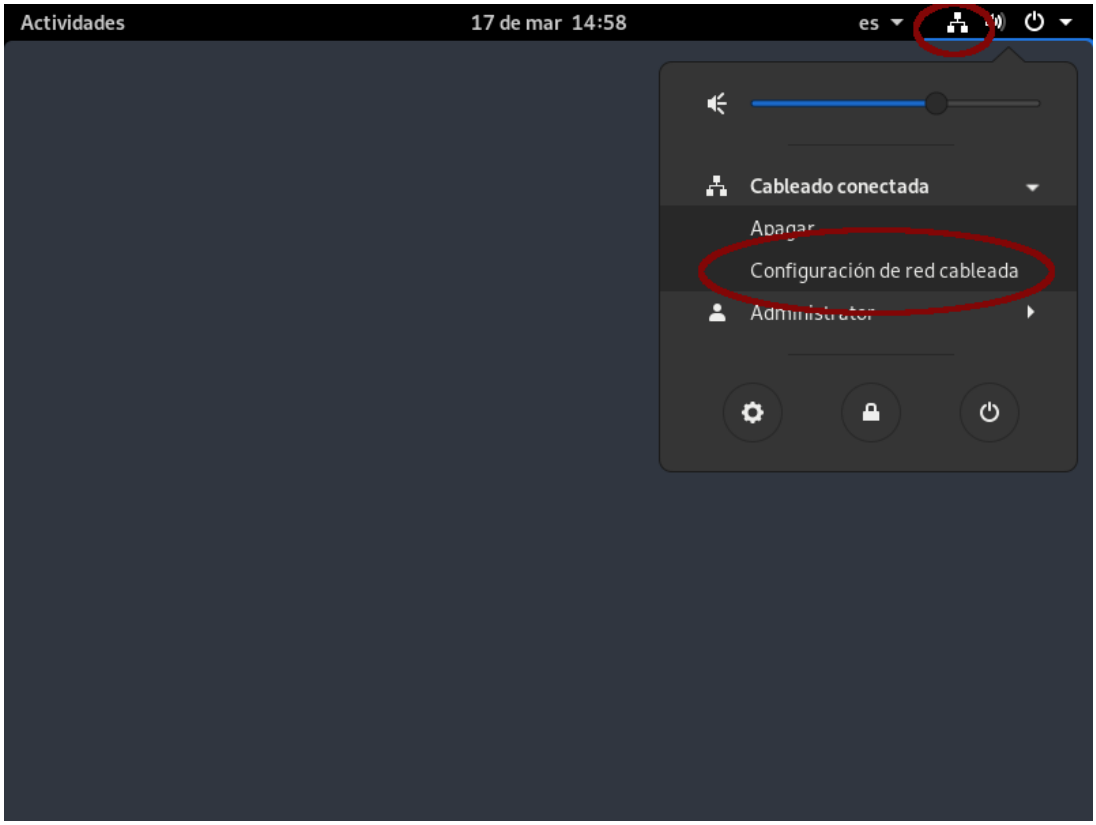
Luego de reiniciar, esta vez desde su cuenta (i.e. no como root) extraiga los archivos contenidos en el ZIP de certificados digitales que le fue enviado. Pueden ser extraídos en cualquier directorio aunque recomendamos ~/.config/certs.

```
mkdir -p ~/.config/certs/ unzip txapa-certs.zip -d ~/.config/certs/
```

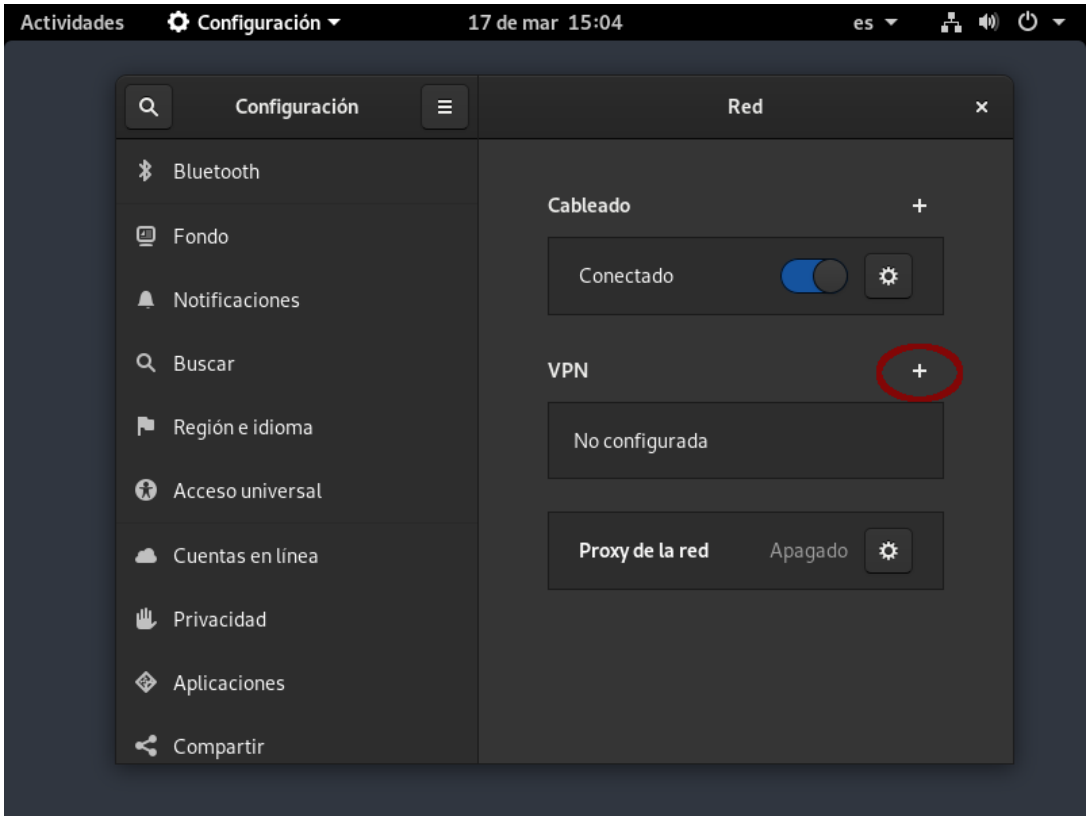
La siguiente imagen muestra la ejecución desde la cuenta del usuario 'txapa' en Fedora 31.



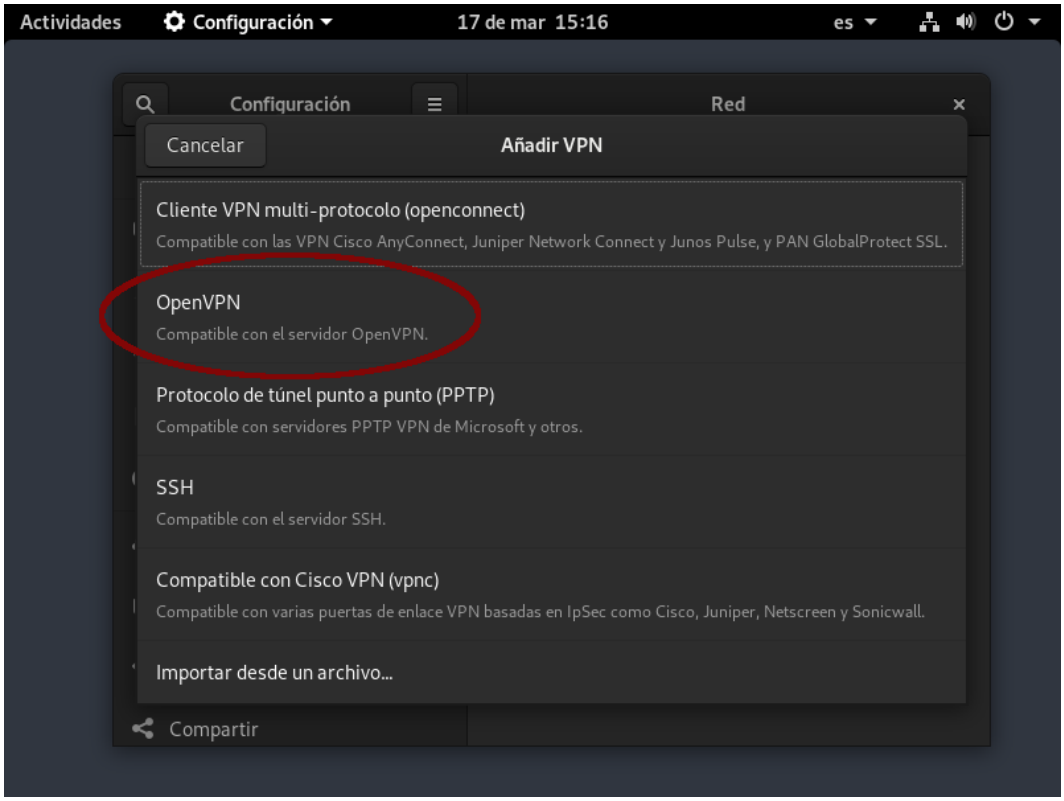
Agregue una nueva VPN, utilizando el ícono de red en la esquina superior derecha y seleccione la opción 'Red cableada / Configuración de la red cableada'.



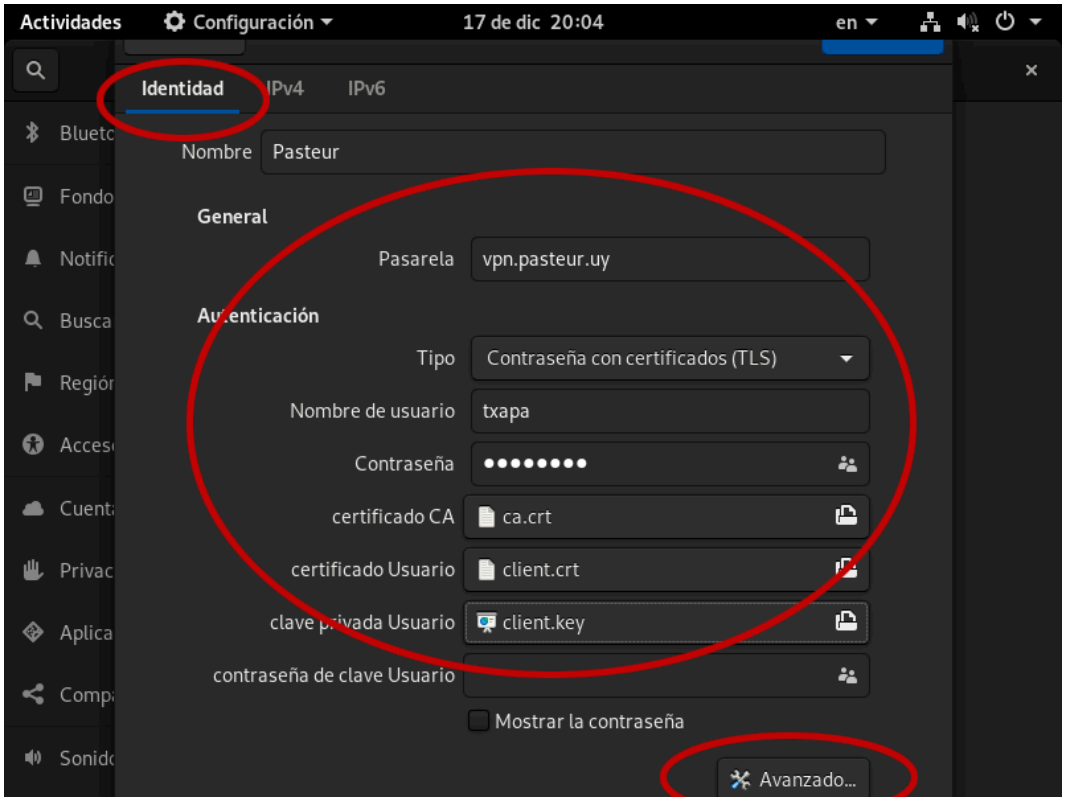
Cree una VPN nueva haciendo click en el botón '+' a la derecha del subtítulo VPN. Puede ocurrir que ya tenga otras VPN configuradas. No las edite, en su lugar cree siempre una nueva.



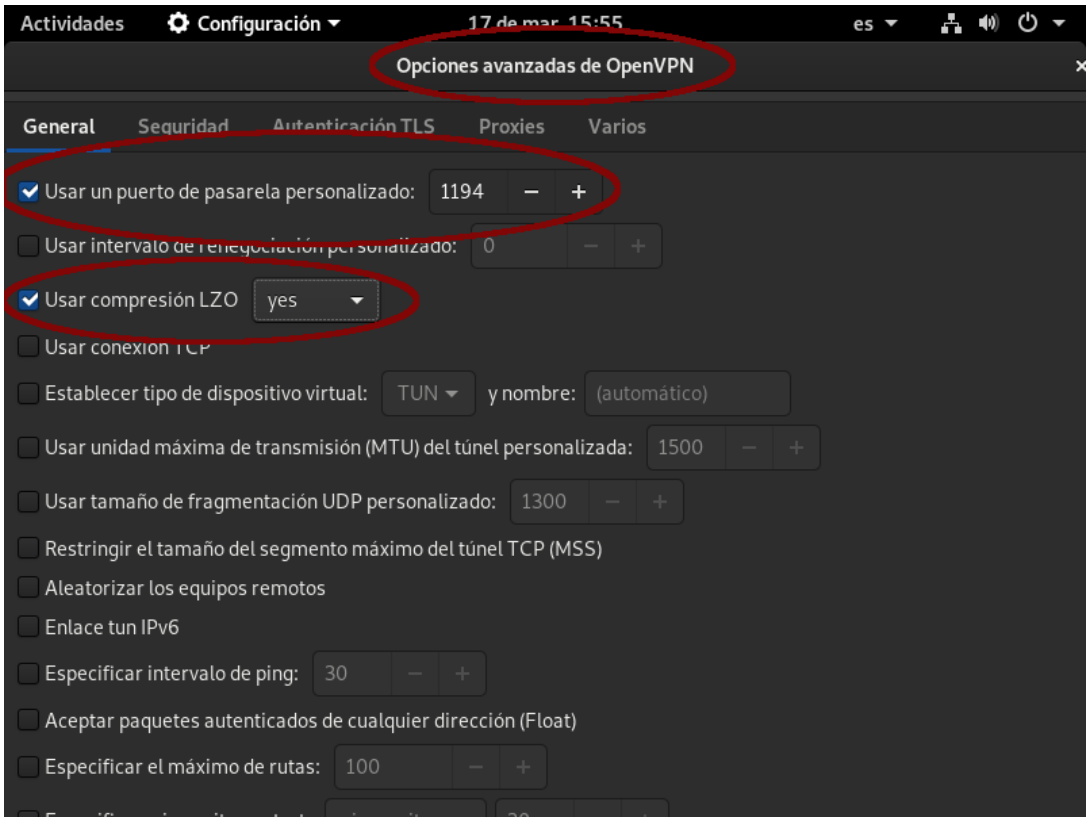
Seleccione la opción OpenVPN. Esta opción debería estar presente si tiene todo el software necesario instalado en el primer paso.



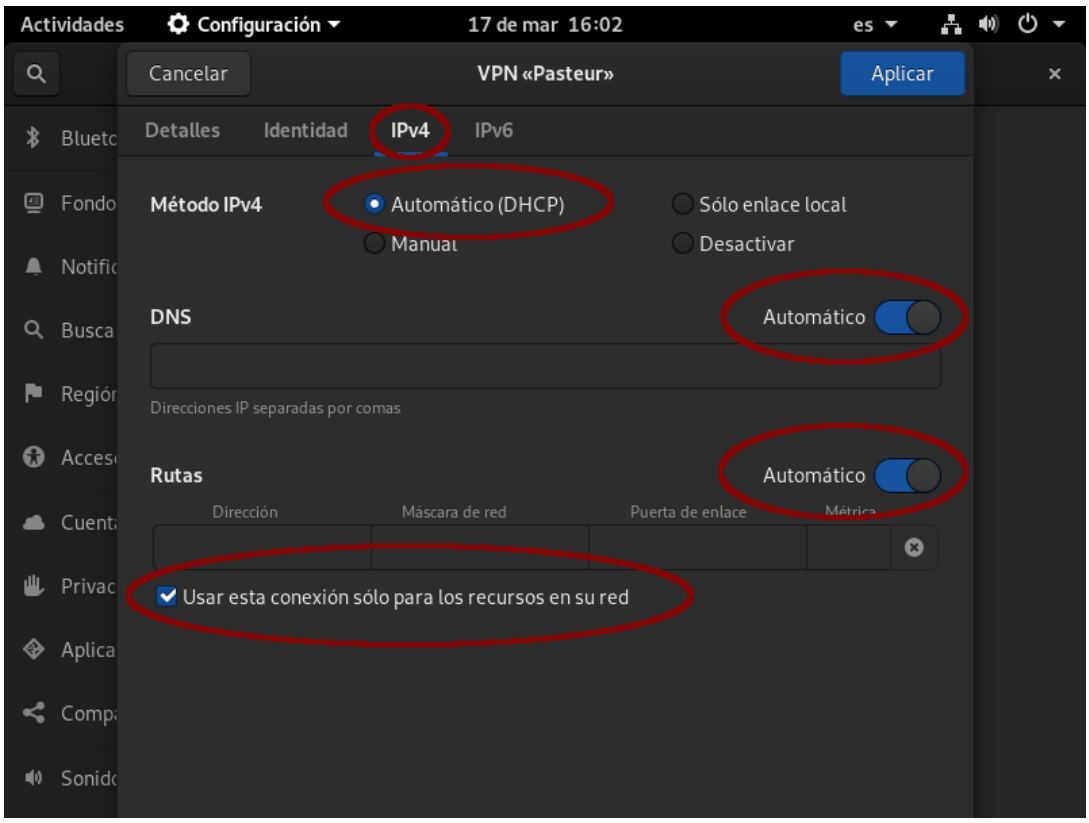
Llene la pestaña 'Identidad' con los datos tal y como se muestra en la siguiente imagen (utilice sus propios nombre de usuario y contraseña en la red de Pasteur). Los dos certificados (ca.crt y client.crt) y la llave privada (client.key) son los que extrajo anteriormente en ~/.config/certs/ (TIP: para ver directorios que empiezan con un punto, presione Ctrl-H en el diálogo de selección de archivos).



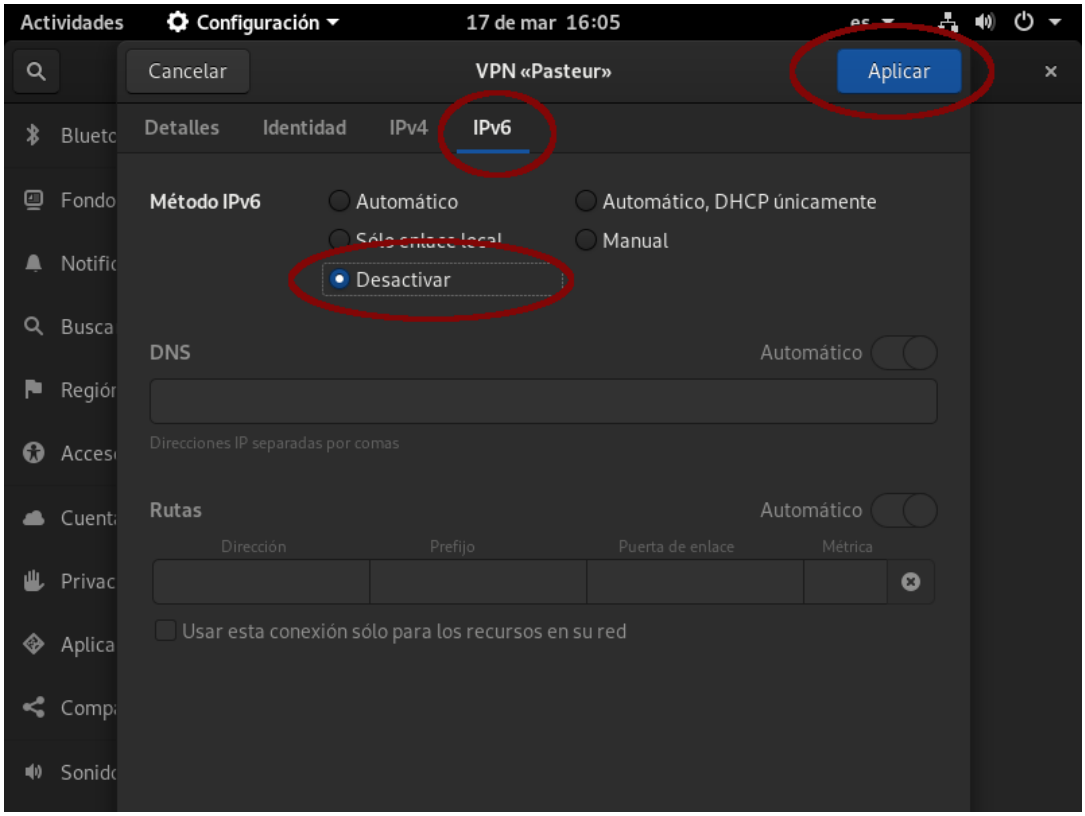
Presione el botón ‘Avanzado...’ y en la pestaña ‘General’ marque las casillas ‘Usar un puerto de pasarela personalizado’ (deje el valor 1194 por defecto) y ‘Usar compresión LZO’ (cambiando el valor a ‘yes’). No modifique ninguna otra opción avanzada y presione ‘Aceptar’.



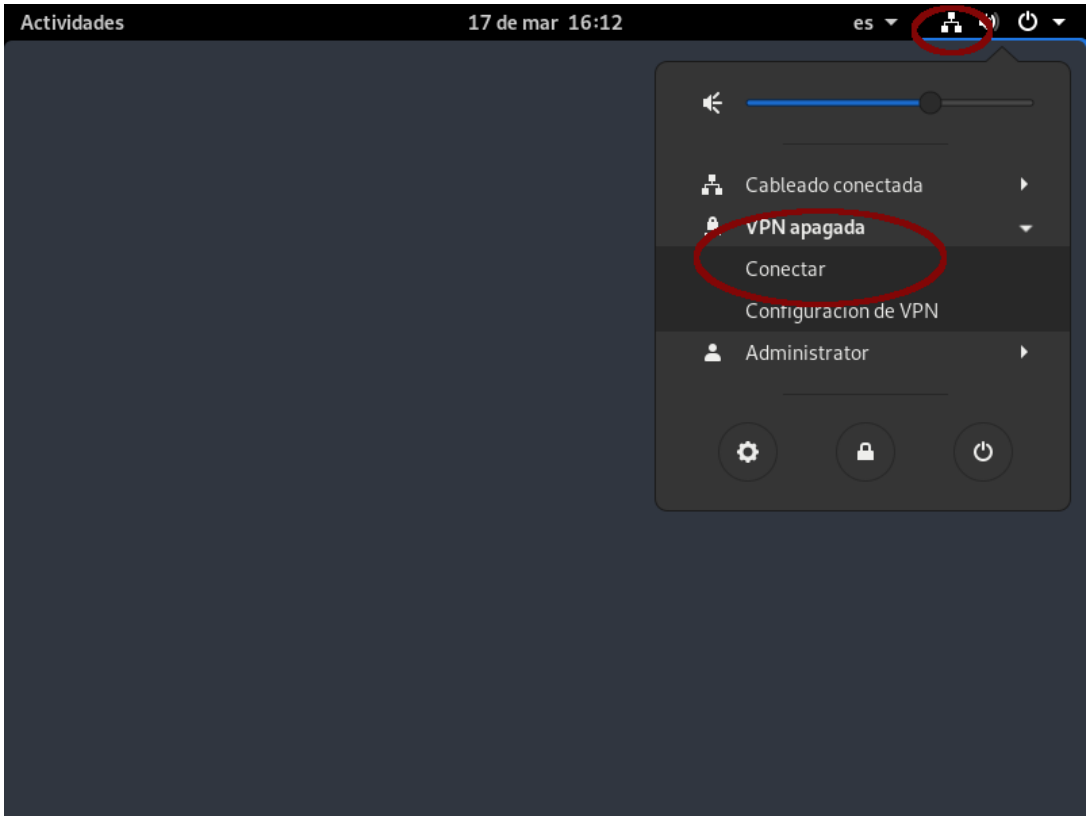
En la pestaña IPv4, marque las casillas ‘Automático (DHCP)’ como método IPv4 y ‘Usar esta conexión solo para los recursos en su red’ (esto último es *muy* importante).



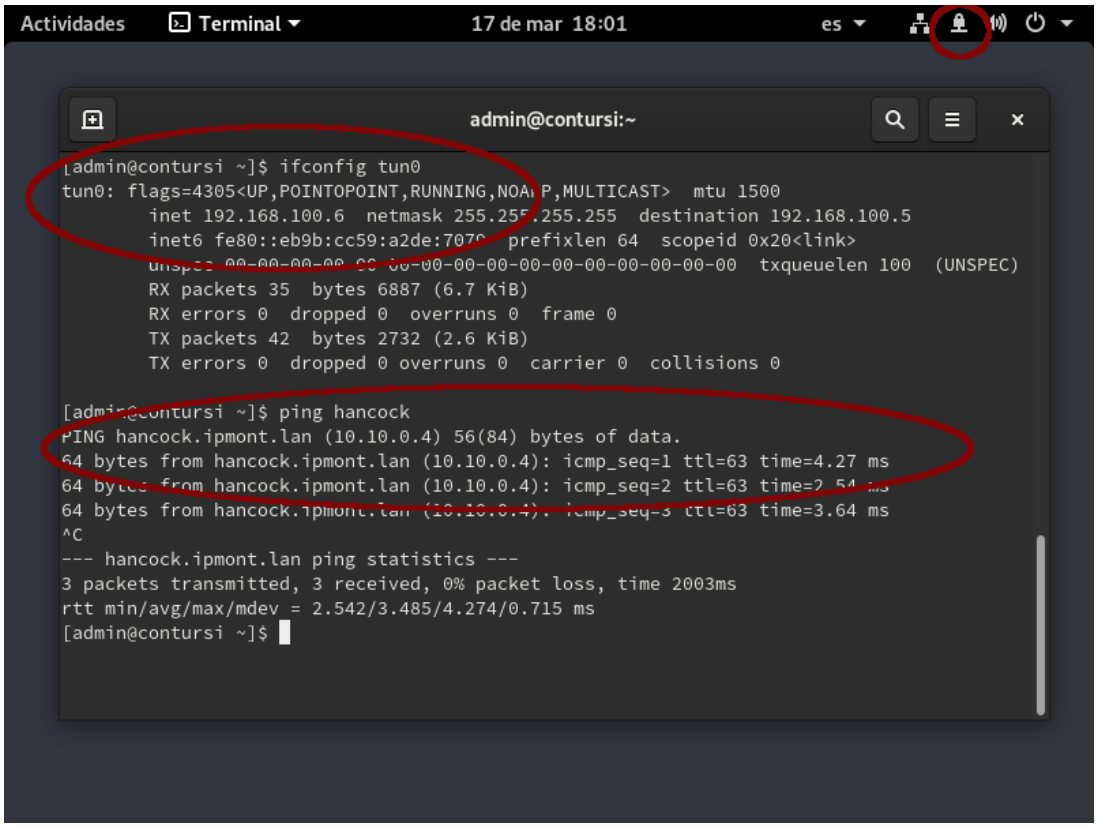
Por último, en la pestaña IPv6 deshabilite por completo todas las opciones. Presione ‘Aplicar’ para guardar toda la configuración generada y cierre el diálogo de configuraciones de red.



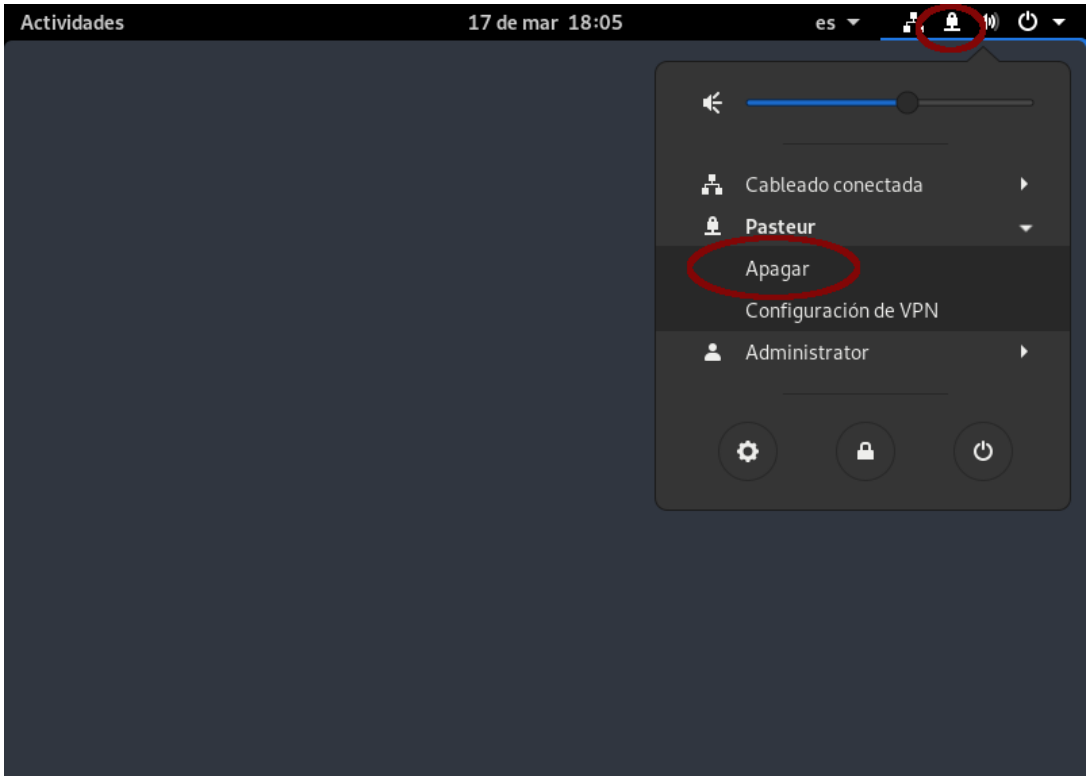
Ahora puede establecer una conexión a la red interna del instituto mediante la VPN creada. Para ello deberá utilizar el ícono de red (en la zona superior derecha) y seleccionar ‘VPN / Conectar’.



Si todo sale bien, notará un ícono nuevo con forma de candado en la barra superior. También puede verificar la existencia de una interfaz de red (casi seguramente 'tun0') con una dirección IP nueva (de la forma 192.168.x.x o 10.10.x.x). Por último, la prueba definitiva de que la conexión resultó exitosa se obtiene haciendo 'ping' a un servidor de la red interna, por ejemplo, Hancock.



Por favor, una vez que termine de utilizar recursos de la red interna, no olvide desconectar la VPN. Esto redundará en un mejor aprovechamiento del ancho de banda y una mayor calidad del resto de sus conexiones a Internet (que ya no estarán pasando por Pasteur). Para ello, deberá utilizar el ícono de red en la barra superior y seleccionar la opción 'Apagar' en la VPN en cuestión.

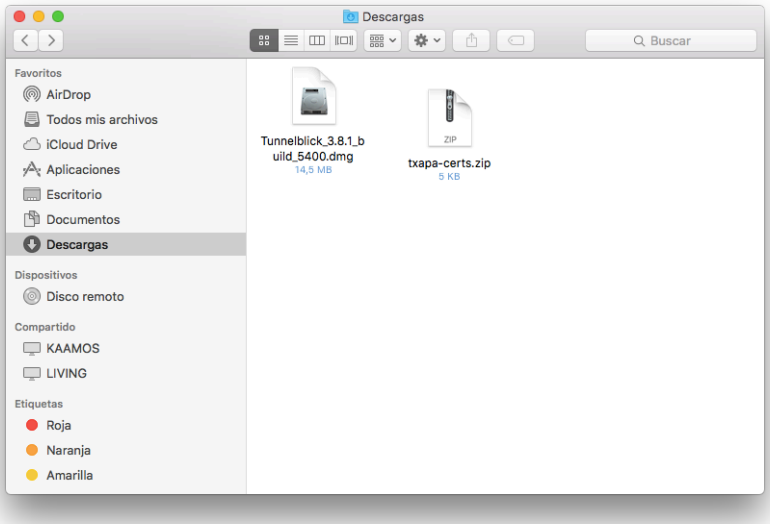


Instalación de la VPN en macOS

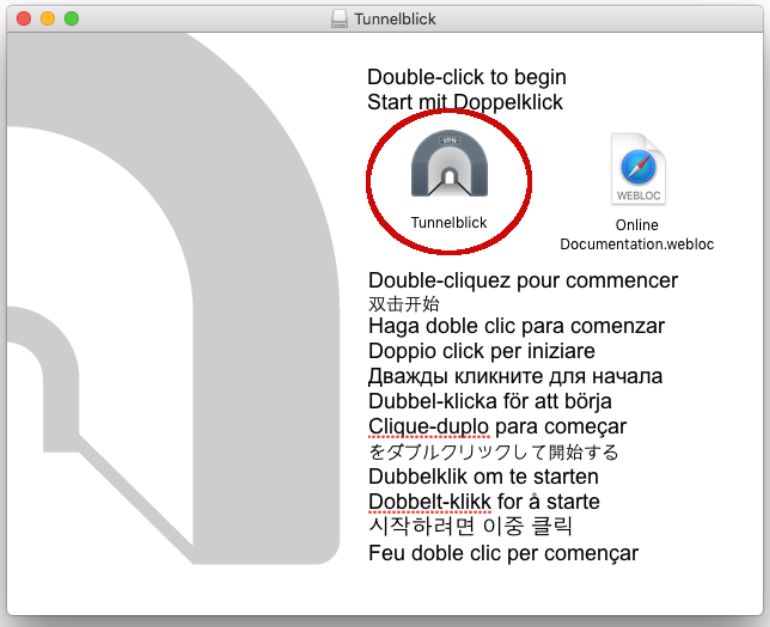
Con soporte únicamente para El Capitan (OS X 10.11) y posteriores. Es recomendable utilizar la última versión ofrecida por Apple, en la actualidad Catalina (macOS 10.15).

Siga estos pasos en la computadora desde la que quiere conectarse a la red interna de Pasteur (e.g. desde su hogar). No es necesario realizar ninguna acción en los equipos (estaciones, servidores, etc.) del instituto sobre los cuales desea trabajar una vez conectado a la VPN. Usted precisa disponer de un certificado digital.

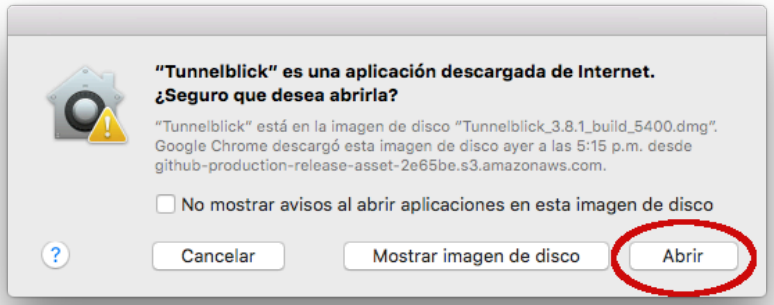
Descargue el programa Tunnelblick desde aquí. Deberá tener una versión de macOS posterior a Lion (OS X 10.7.5), de lo contrario, consulte el listado de versiones obsoletas en la página de Tunnelblick por una versión acorde a su sistema operativo. Esto último no es soportado por la Unidad de Recursos Informáticos; en ese caso, tenga a bien consultar por e-mail a la dirección soporte [arroba] pasteur.edu.uy. Guarde el archivo descargado en una carpeta que pueda recordar (e.g. Descargas).



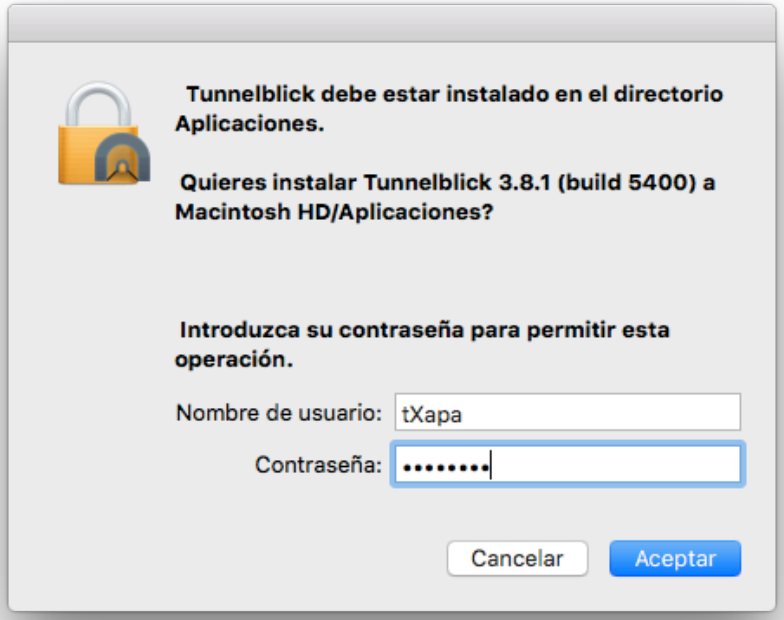
Se desplegará el diálogo incial del instalador de Tunnelblick. Haga doble click sobre el ícono del programa (un túnel) para iniciar la instalación.



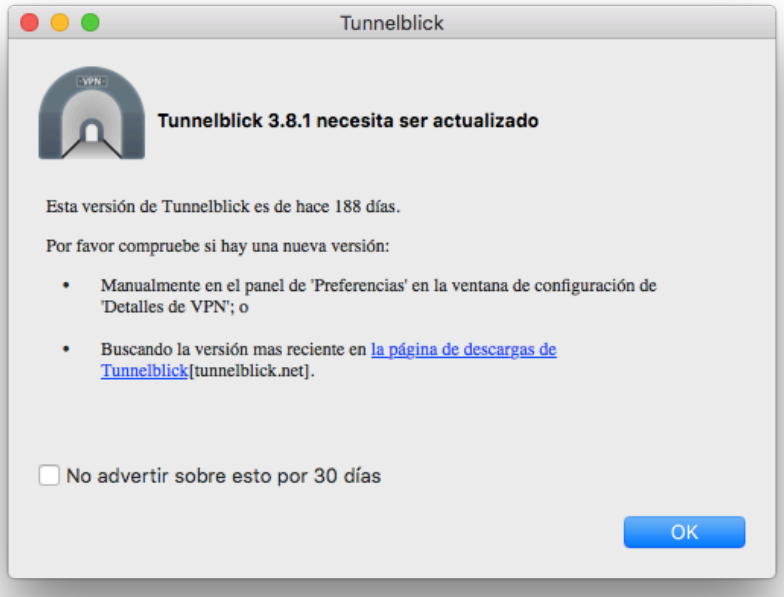
En caso de recibir la siguiente pregunta sobre 'aplicación descargada de Internet', acepte el diálogo presionando el botón 'Abrir'.



En caso de que su sistema solicite credenciales administrativas, ingrese el nombre de usuario y la contraseña de **su máquina** (i.e. no la de la red de Pasteur).

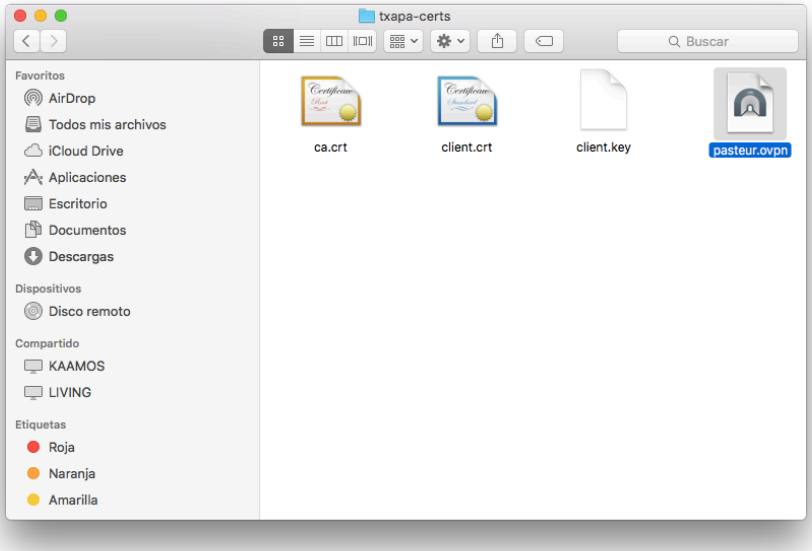


Aguarde unos instantes para completar la instalación. Es probable que, al finalizar, se le solicite la actualización del programa. Simplemente ignore el mensaje y presione 'OK'.

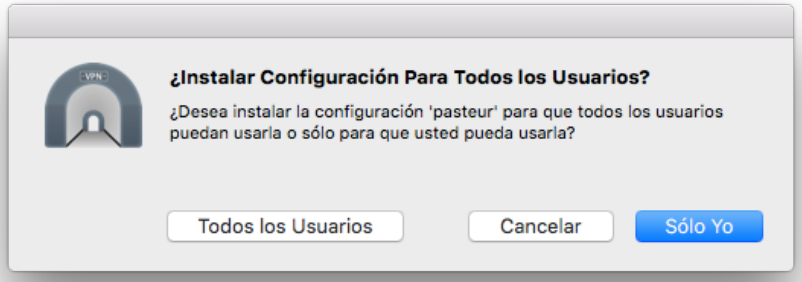


El programa está ahora instalado. Se debería ver el ícono (un túnel gris) en la barra superior.

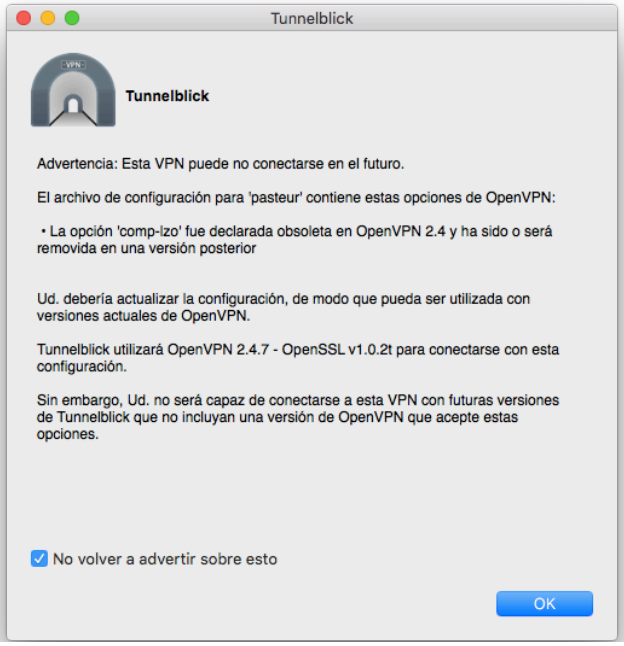
Extraiga el contenido del ZIP con los certificados digitales en una carpeta provisoria (e.g. haciendo doble click sobre el archivo ZIP). Deberá contar con cuatro archivos.



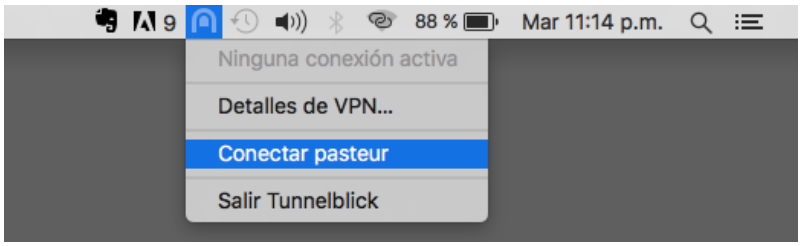
Arrastre el archivo ‘pasteur.ovpn’ (el nombre puede cambiar pero la extensión será siempre .ovpn) hasta el ícono de Tunnelblick en la barra superior (el túnel gris). Esto instalará la configuración. En el diálogo siguiente, elija la opción ‘Solo yo’ (instalar la VPN solo para la sesión actual).



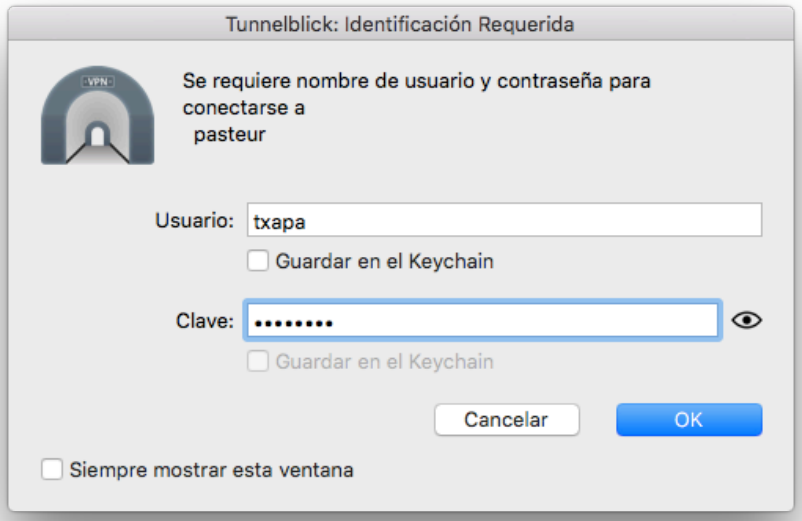
Acepte la advertencia acerca de la obsolescencia de la opción ‘comp-lzo’. Por el momento, no afecta al funcionamiento de la VPN.



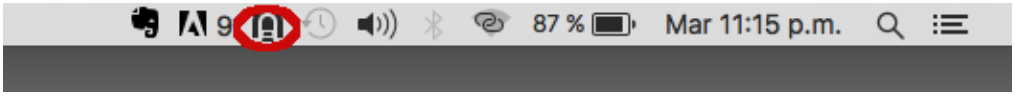
La VPN está ahora instalada y configurada. Para establecer una conexión a la red interna de Pasteur, utilice el ícono de la barra superior (el túnel gris) y seleccione la opción 'Conectar'.



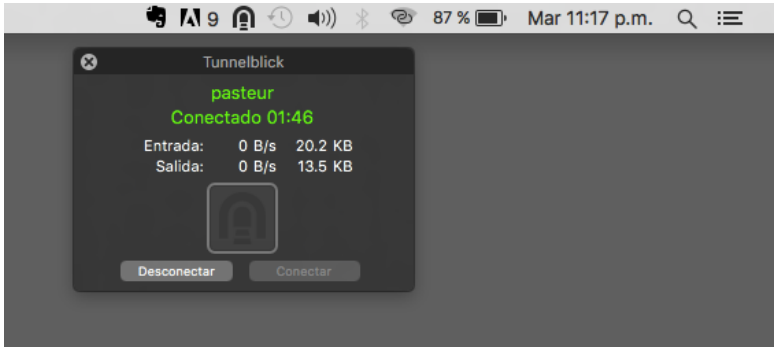
El programa solicitará las credenciales de acceso (nombre de usuario y contraseña en la red de Pasteur). Pueden ser guardadas para futuras conexiones.



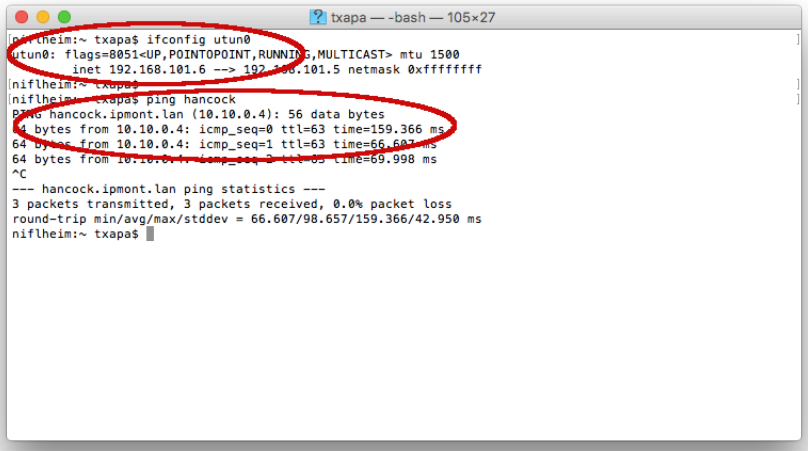
Aguarde unos instantes a que se establezca la conexión. El ícono en la barra superior (el túnel gris) pasará a ser negro, lo que indica que su computadora ya forma parte de la red interna del instituto.



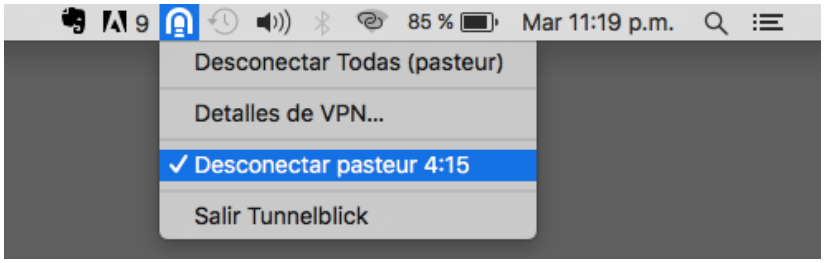
Como comprobación, puede posicionar el puntero sobre el ícono de la barra superior para observar el estado de la conexión, además de conectar y desconectar la VPN en cualquier momento.



También puede verificar la existencia de una interfaz de red (casi seguramente 'utun0') con una dirección IP nueva (de la forma 192.168.x.x o 10.10.x.x). Por último, la prueba definitiva de que la conexión resultó exitosa se obtiene haciendo 'ping' a un servidor de la red interna, por ejemplo, Hancock.



Por favor, una vez que termine de utilizar recursos de la red interna, no olvide desconectar la VPN. Esto redundará en un mejor aprovechamiento del ancho de banda y una mayor calidad del resto de sus conexiones a Internet (que ya no estarán pasando por Pasteur). Para ello, deberá utilizar el ícono de Tunnelblick en la barra superior y seleccionar la opción 'Desconectar' en la VPN en cuestión.



SOPORTE A DISTANCIA

La Unidad de Recursos Informáticos cuenta con un servicio de soporte a distancia durante el horario de oficina, de lunes a viernes entre 09:00 y 17:00, aunque podría haber razones para atender solicitudes urgentes fuera de horario (se ruega no abusar).

Por favor, envíe un correo electrónico a **soporte@pasteur.edu.uy** y en breve un integrante de la unidad se contactará con usted. Tenga a bien incluir los datos de contacto que entienda relevantes (unidad, laboratorio u oficina, nombre, e-mail, teléfono, etc.).

Al efecto de solucionar problemas en computadoras personales, es probable que se requiera el uso de TeamViewer, un programa que permite el acceso a la computadora de su hogar por parte de un informático del instituto. Por favor, descargue TeamViewer desde alguno de los siguientes enlaces:

Descargar TeamViewer (Quick Support) para Windows

Descargar TeamViewer (Quick Support) para macOS

Descargar TeamViwer para Fedora/CentOS

En los casos de Windows y macOS, alcanza con ejecutar el programa. En los casos de Fedora y CentOS, es necesario instalar el RPM como root y utilizar la opción de asistencia remota.

Una vez que ejecute el programa, obtendrá un código y una clave que le serán solicitados (por teléfono, chat, etc.). Con estos datos, un integrante de la unidad podrá ingresar a su equipo

mientras usted ve en todo momento qué se está haciendo (verá en su pantalla los movimientos y acciones del mouse y el teclado). Cuando finalice la asistencia, el código utilizado perderá validez y ya no será posible acceder remotamente a su computadora.

De esta forma, intentaremos resolver a distancia las situaciones que nos llegan habitualmente dentro del instituto.

Información de contacto

Formas de contactar al personal de la unidad:

- Teléfono: +598 2522 0910* #123
- E-mail: soporte@pasteur.edu.uy
- No usamos mensajería instantánea (i.e. WhatsApp)