

HERRAMIENTAS DE TRABAJO REMOTO

ÍNDICE

Página 2 - Secure shell

Página 2 - Login shell

Página 2 - Public keys

Página 4 - Transferencias

Página 5 - Multiplexor de terminales

Página 7 - Login host

Página 8 - Túneles

Página 10 - Desde Windows

Página 13 - Soporte a distancia

HERRAMIENTAS DE TRABAJO REMOTO

SECURE SHELL

Si usted no entiende qué quiere decir SSH, probablemente no lo necesite. Una vez dentro de la VPN, es posible ingresar por SSH a distintos servidores y estaciones, ya sea vía el shell de POSIX (Bash y similares), mediante sistemas que usan SSH como transporte (sftp, scp, rsync), desde programas gráficos para Linux (GNOME Terminal, Konsole), aplicaciones de Windows (PuTTY, Windows Terminal) o utilidades de macOS (Mac Terminal).

LOGIN SHELL

Una vez conectado a la VPN, podrá hacer SSH a cualquier computadora usando solo el hostname (e.g. ssh nagonal). Deberá conocer el nombre de su equipo personal (e.g. Ometeotl en UBI, Cabernet en LSBM) para ingresar directamente desde otro lugar. **No es necesario hacer un ‘puente’ por Hancock.** Esto es sumamente útil al efecto de transferir archivos; la transferencia puede ser inmediata sin tener que pasar por un servidor intermediario.

Por otra parte, la VPN es ‘resistente’ a los cambios de dirección IP forzados por los proveedores de Internet (e.g. ANTEL) cada aproximadamente 12 horas (con la consecuente desconexión). De todos modos, se recomienda utilizar [GNU Screen](#) para evitar pérdidas de conexión en terminales.

Simplemente trabaje como si estuviera dentro del instituto.

PUBLIC KEYS

Esto le permitirá conectarse por ssh sin tener que ingresar la contraseña. Puede ser usado entre la computadora de su hogar y su equipo personal en Pasteur, entre cualquier estación y un servidor, entre dos servidores, etc. En la computadora remota (e.g. en su hogar) debe crear dos llaves criptográficas: una pública y otra privada. Desde un equipo en posesión de la llave privada ingrese a otro en posesión de la llave pública. **Conserve la llave privada como si fuera su tarjeta de crédito** (no la preste, no la divulgue, no la distribuya, no la pierda). Distribuya la llave pública entre todos los equipos a los que quiera ingresar.

El siguiente ejemplo que ‘local’ es el nombre del equipo de su hogar y ‘remoto’ es el nombre de su equipo de Pasteur. Genere el par de llaves desde el equipo local con el comando ssh-keygen.

```
[usuario1@local ~]$ ssh-keygen -t rsa
```

Presione ‘Enter’ tres veces para aceptar los valores por defecto y dejar las llaves sin contraseña. La siguiente imagen muestra el procedimiento para el usuario ‘admin’ de un equipo con nombre ‘Contursi’.

```

Actividades Terminal 21 de mar 19:47 es
admin@contursi:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:20uEx0ozkiTgdZUOX5hceH1erT1AN0LmfqXQ+gEy/e0 admin@contursi.ipa.pasteur.uy
The key's randomart image is:
+----[RSA 3072]-----+
|
| ..*.. o= o.|
| ..B o oo+o.o|
| . . .+ = o *.+o.|
|... . = . o.+.+o|
|.. . . S . .+.+o|
| o o + ..o |
| o + . o . E |
| . o . . |
| . |
+----[SHA256]-----+
[admin@contursi ~]$

```

Las llaves serán generadas en el directorio ~/.ssh con nombres id_rsa (privada) y id_rsa.pub (pública). Los permisos muestran que la llave privada solo es accesible por el propietario.

```

Actividades Terminal 21 de mar 19:49 es
admin@contursi:~$ ls -l .ssh/
total 12
-rw-----, 1 admin admins 2622 mar 21 19:46 id_rsa
-rw-r--r--, 1 admin admins 583 mar 21 19:46 id_rsa.pub
-rw-r--r--, 1 admin admins 796 mar 17 15:22 known_hosts
[admin@contursi ~]$

```

En el equipo 'local' cree un archivo ~/.ssh/identification conteniendo el texto «IdKey id_rsa».

```
[usuario1@local ~]$ echo 'IdKey id_rsa' > ~/.ssh/identification
```

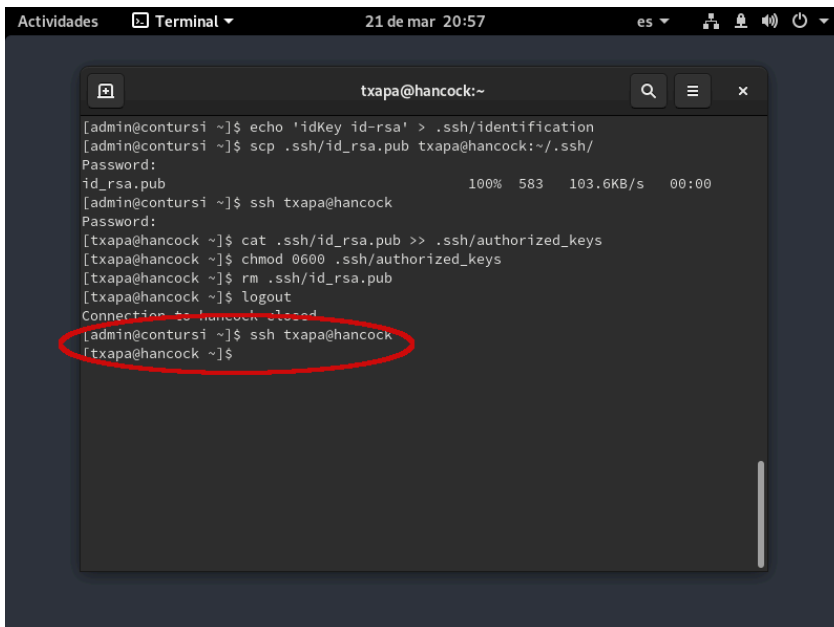
Copie la llave pública a la cuenta del equipo remoto (al que desea ingresar sin escribir la contraseña). Los nombres de usuario no tienen por qué ser los mismos. Por ahora, aún tiene que escribir la contraseña de scp.

```
[usuario1@local ~]$ scp ~/.ssh/id_rsa.pub usuario2@remoto:~/.ssh/
```

Ingresa por ssh al equipo remoto, agrégue el contenido de la llave pública al archivo ~/.ssh/authorized_keys, el cual **debe tener permisos 0600**. Por ahora, aún tiene que escribir la contraseña de ssh.

```
[usuario1@local ~]$ ssh usuario2@remoto
[usuario2@remoto ~]$ cat ~/.ssh/id_rsa.pub >>
~/.ssh/authorized_keys
[usuario2@remoto ~]$ chmod 0600~/.ssh/authorized_keys
[usuario2@remoto ~]$ rm ~/.ssh/id_rsa.pub
```

Si todo salió bien, ahora puede usar SSH (ssh, scp, sftp, etc.) desde 'local' sin precisar escribir la contraseña en 'remoto'.



```

Actividades Terminal 21 de mar 20:57 es
txapa@hancock:~
[admin@contursi ~]$ echo 'idKey id-rsa' > .ssh/identification
[admin@contursi ~]$ scp .ssh/id_rsa.pub txapa@hancock:~/.ssh/
Password:
id_rsa.pub 100% 583 103.6KB/s 00:00
[admin@contursi ~]$ ssh txapa@hancock
Password:
[txapa@hancock ~]$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
[txapa@hancock ~]$ chmod 0600 .ssh/authorized_keys
[txapa@hancock ~]$ rm .ssh/id_rsa.pub
[txapa@hancock ~]$ logout
Connection to Hancock closed.
[admin@contursi ~]$ ssh txapa@hancock
[txapa@hancock ~]$

```

TRANSFERENCIAS

Si bien el uso de la VPN en combinación con llaves públicas facilita la copia de archivos mediante sftp, scp y similares, la recomendación es utilizar rsync en todos los casos. Dado que rsync funciona sobre SSH, el acceso con llaves públicas (i.e. sin tener que escribir la contraseña) funcionará de forma transparente.

Rsync sincroniza colecciones enteras de archivos transfiriendo únicamente los cambios más recientes. Esto es útil ante la pérdida de conexión a Internet durante una copia grande, el reinicio de una transferencia fallida sin tener que empezar de nuevo o la subida y bajada incremental de directorios completos entre dos equipos de modo de mantener copias idénticas (local y remota) haciendo sucesivas sincronizaciones a medida que se trabaja.

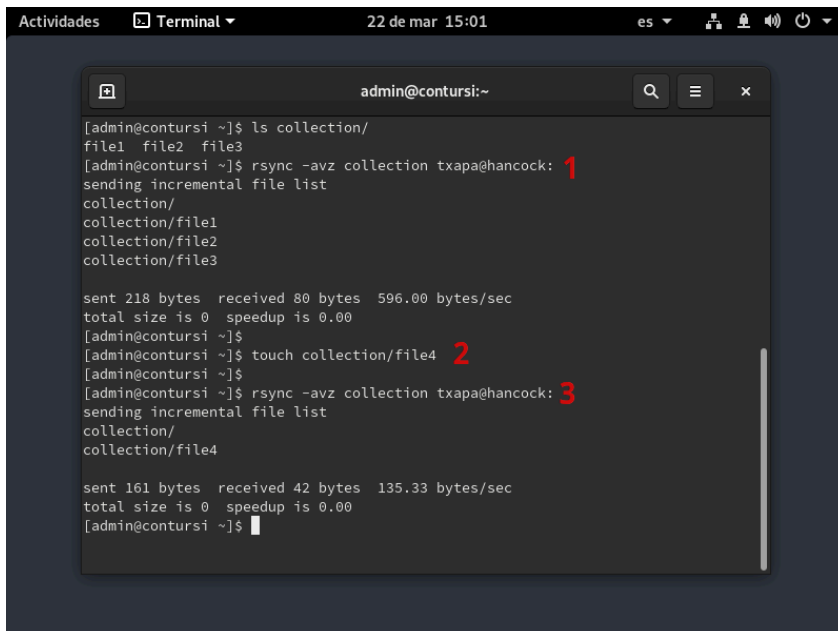
El programa [admite infinidad de opciones](#) aunque la sintaxis básica es simple y siempre la misma (use siempre las opciones -avz). Por ejemplo:

```
# transferir un archivo a la máquina remota rsync -avz
/dir1/archivo usuario@equipo:/dir2/

# transferir varios archivos a la máquina local rsync -avz
usuario@equipo:/dir1/archivo*_tar.gz /dir2/

# transferir un directorio y todos sus subdirectorios (/dir1 *no
debe* llevar / al final) rsync -avz /dir1 usuario@equipo:/dir2/
```

En la siguiente imagen se transfieren tres archivos entre dos equipos, se agrega un cuarto al equipo local y se vuelve a realizar la transferencia. Se puede observar como en el segundo rsync solo se transfiere la modificación más reciente.



```

[admin@contursi ~]$ ls collection/
file1 file2 file3
[admin@contursi ~]$ rsync -avz collection txapa@hancock: 1
sending incremental file list
collection/
collection/file1
collection/file2
collection/file3

sent 218 bytes received 80 bytes 596.00 bytes/sec
total size is 0 speedup is 0.00
[admin@contursi ~]$
[admin@contursi ~]$ touch collection/file4 2
[admin@contursi ~]$
[admin@contursi ~]$ rsync -avz collection txapa@hancock: 3
sending incremental file list
collection/
collection/file4

sent 161 bytes received 42 bytes 135.33 bytes/sec
total size is 0 speedup is 0.00
[admin@contursi ~]$

```

MULTIPLEXOR DE TERMINALES

Siempre que trabaje en emuladores de terminal (GNOME Terminal, PuTTY, etc.) intente hacerlo mediante un multiplexor de terminales. Estos son programas que permiten combinar varias terminales en un sola conexión, con dos ventajas principales:

Permiten ‘retomar’ una terminal desde otro equipo (e.g. en su hogar) en el mismo estado en el que la dejó (e.g. en Pasteur). Los programas en ejecución no se interrumpirán y el estado de la pantalla será exactamente el mismo.

Son ‘resistentes’ a los cortes en la conexión, cambios de dirección IP (que los proveedores, como ANTEL efectúan dos veces al día). Usted no deberá restablecer cada una de sus sesiones de trabajo constantemente para continuar con su trabajo.

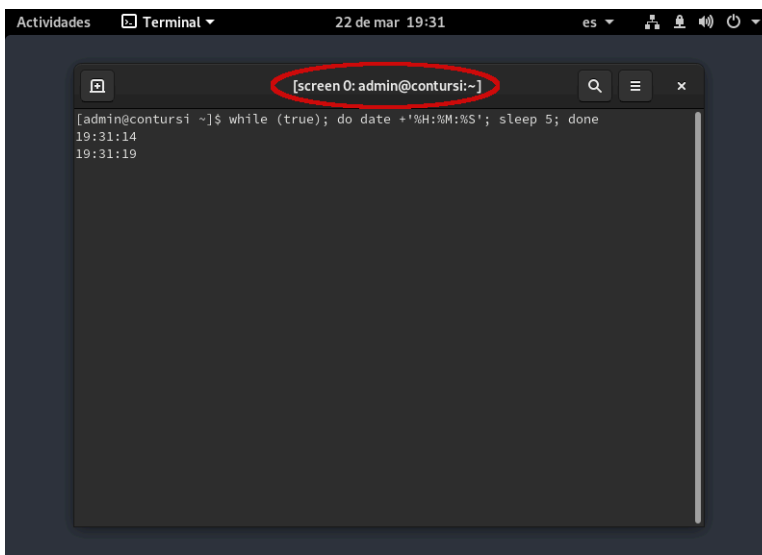
El programa más sencillo es [GNU Screen](#) aunque existen otros ([Tmux](#), [Byobu](#)). Es probable que no forme parte de una instalación estándar de Fedora. En ese caso, puede instalarlo con dnf.

```
dnf install -y screen
```

Si bien screen cuenta con [infinidad de opciones](#), el uso básico es simple. Dentro de una sesión de ssh puede iniciar tantos screens como desee. Se recomienda asignar un nombre a cada screen con la opción -S.

```
screen -S mi_sesion_uno
```

Dentro de GNOME, el título de la terminal cambiará para indicar que se encuentra dentro de una terminal virtual (e.g. screen N) que a su vez está dentro de la terminal física (e.g. una sesión de ssh). En la siguiente imagen, se dejó corriendo un while() que imprime la hora cada 5 segundos dentro de la terminal virtual.

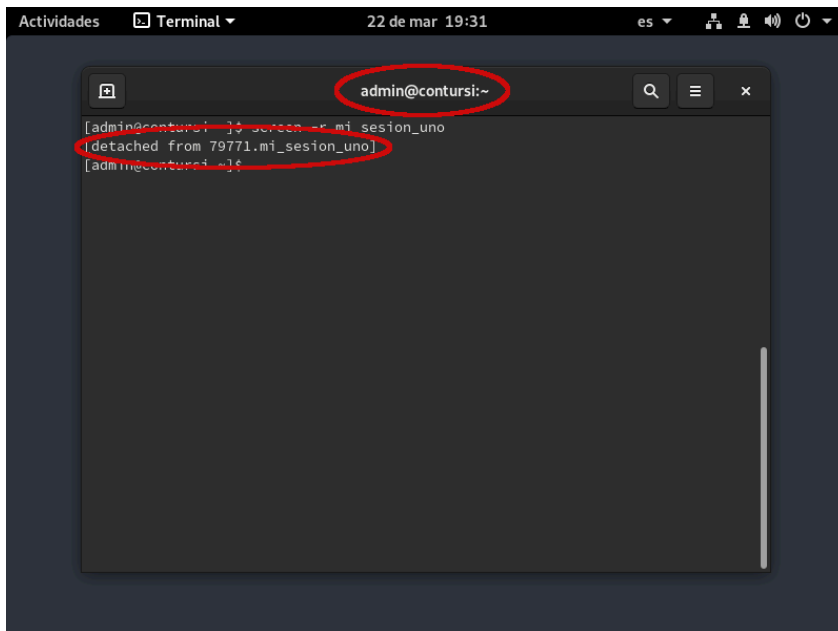


```

[screen 0: admin@contursi:~]
[admin@contursi ~]$ while (true); do date +%H:%M:%S'; sleep 5; done
19:31:14
19:31:19

```

A partir de ahora, estará trabajando dentro de la terminal virtual 'mi_sesion_1'. Puede salir de ella, manteniendo todos sus programas corriendo y el estado de la pantalla intacto, mediante la combinación **Ctrl-A+d** (primero 'Ctrl-A', luego soltar y a continuación 'd'). De este modo, la terminal virtual quedará desacoplada de la terminal física y podrá ser retomada en otro momento o desde otra sesión de ssh. El resultado de desacoplar el screen de la imagen anterior, luego de utilizar **Ctrl-A+d**, es el siguiente.



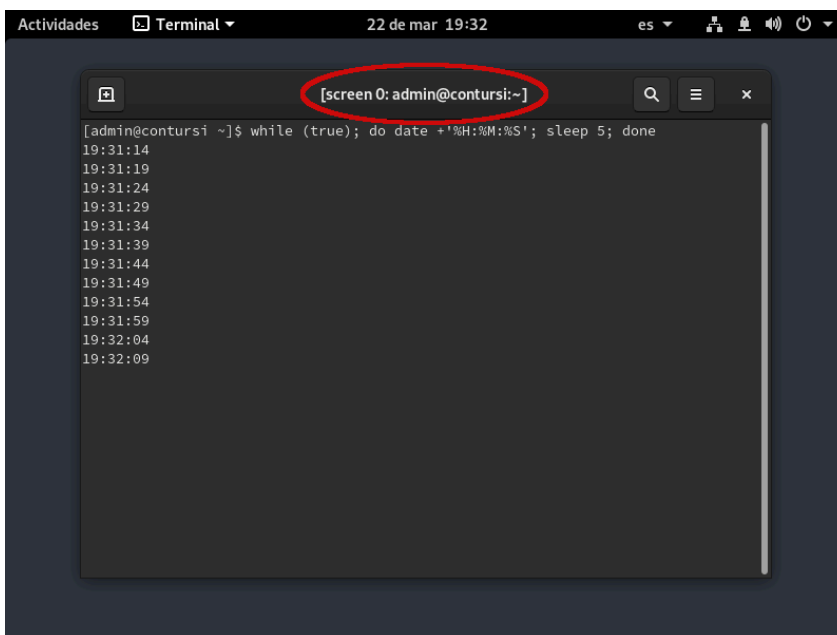
```

Actividades Terminal 22 de mar 19:31 es
admin@contursi:~
[admin@contursi ~]$ screen -r mi_sesion_uno
[detached from 79771.mi_sesion_uno]
[admin@contursi ~]$
  
```

En otro momento o lugar (e.g. desde su casa, más tarde, al perder la conexión, luego de un apagón, en otra sesión de ssh, etc.) puede 'recuperar' la terminal virtual desacoplada utilizando la opción **-r** seguida del nombre que le había asignado.

agregue `-d` si nunca fue desacoplada `screen -r mi_sesion_1`

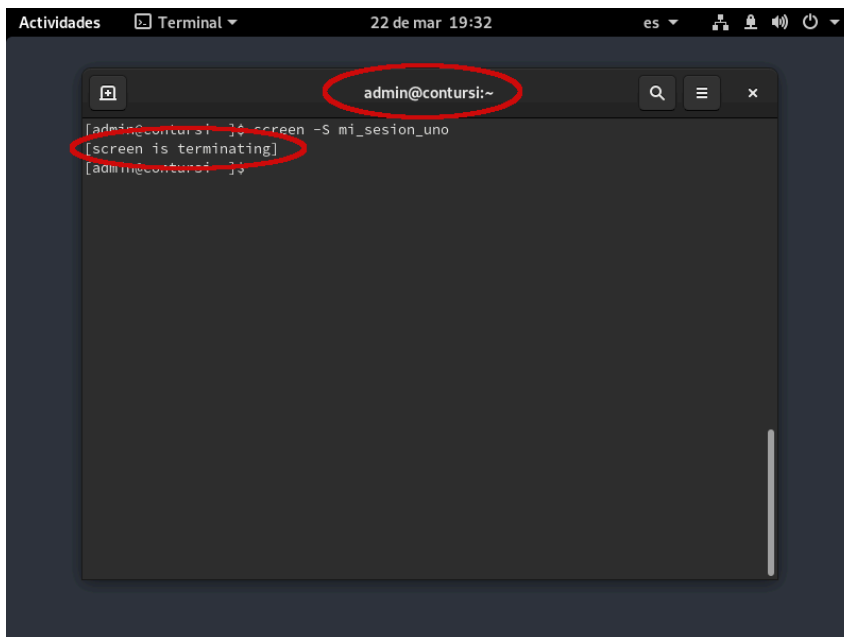
Como se ve en la siguiente imagen, el script ejecutado 'mi_sesion_uno' continuó corriendo mientras la terminal virtual estuvo desacoplada.



```

Actividades Terminal 22 de mar 19:32 es
[screen 0: admin@contursi:~]
[admin@contursi ~]$ while (true); do date +%H:%M:%S; sleep 5; done
19:31:14
19:31:19
19:31:24
19:31:29
19:31:34
19:31:39
19:31:44
19:31:49
19:31:54
19:31:59
19:32:04
19:32:09
  
```

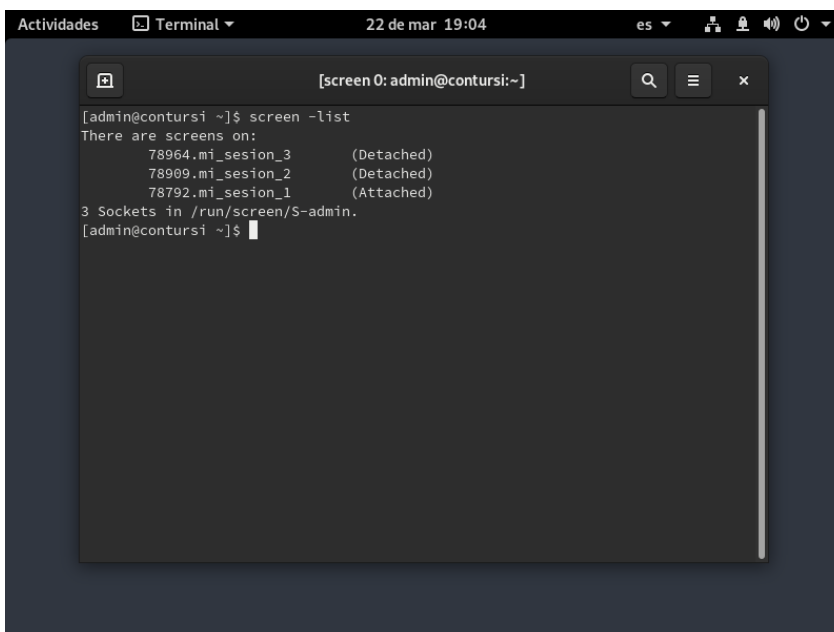
De esta forma, una terminal virtual puede continuar funcionando «eternamente» (siempre y cuando no se reinicie el sistema) y ser retomada en cualquier momento desde cualquier lugar. Para terminar una terminal virtual (note la diferencia entre «desacoplar» y «terminar») basta salir de la sesión como si se tratara de una terminal física (logout, exit, Ctrl-D, etc.).



```

Actividades Terminal 22 de mar 19:32 es
[admin@contursi:~]
[admin@contursi:~]$ screen -S mi_sesion_uno
[screen is terminating]
[admin@contursi:~]$
  
```

Si usted tiene varios screens corriendo y no recuerda cuántas o cómo se llaman, puede listarlos con la opción -list. Ese es el principal motivo para asignarle un nombre a cada una con la opción -S.



```

Actividades Terminal 22 de mar 19:04 es
[screen 0: admin@contursi:~]
[admin@contursi ~]$ screen -list
There are screens on:
  78964.mi_sesion_3      (Detached)
  78909.mi_sesion_2      (Detached)
  78792.mi_sesion_1      (Attached)
3 Sockets in /run/screen/S-admin.
[admin@contursi ~]$
  
```

LOGIN HOST

Por el motivo que sea, siempre habrá ocasiones en las que es imposible conectar con la VPN (e.g. en una computadora que no es la suya, ante una urgencia, etc.). La red del instituto cuenta con **un único punto de entrada por SSH** abierto a Internet desde el cual es posible ingresar a la red y con ello tener acceso a los sistemas internos. El nombre del servidor es Hancock y las 'direcciones' mediante las que se puede ingresar son dos.

Desde la red interna, la red inalámbrica, la VPN e Internet:

`central.pasteur.edu.uy` (también `164.73.118.2`)

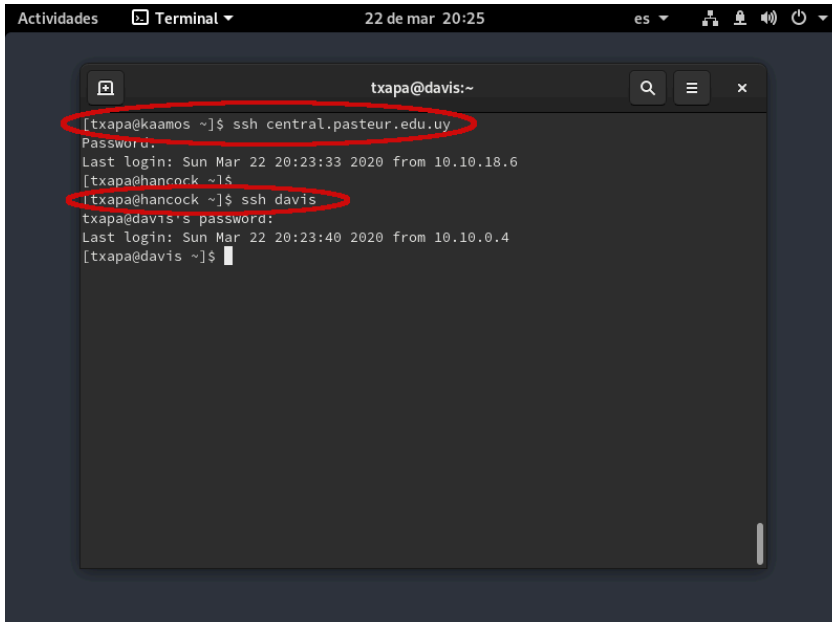
Solo desde la red interna y la VPN:

`hancock` (también `hancock.ipmont.lan`, `hancock.pasteur.uy`, `10.10.0.4`)

Por razones obvias, al tener conexión directa a Internet, permitir el ingreso por SSH y permitir logons con shell, **el acceso está restringido solo al personal autorizado**. Si usted no cuenta con permisos, por favor solicítelo escribiendo un e-mail a soporte@pasteur.edu.uy. El trámite es sencillo y no requiere su intervención.

Al utilizar un servidor intermediario, deberá hacer dos conexiones: una hasta Hancock y la otra hasta su computadora o servidor en la red interna. Si bien en este caso funcionan los pares de llaves y los multiplexores de terminales (ver las secciones correspondientes más arriba), el procedimiento de conexión es más engorroso. No se recomienda utilizar el login host a menos que no quede otra opción.

La imagen siguiente muestra los dos pasos del procedimiento; desde un sistema doméstico (Kaamos) en la VPN hasta Hancock y desde Hancock hasta un sistema en la red interna (Davis).



```

Actividades Terminal 22 de mar 20:25 es
txapa@davis:~
[txapa@kaamos ~]$ ssh central.pasteur.edu.uy
Password:
Last login: Sun Mar 22 20:23:33 2020 from 10.10.18.6
[txapa@ Hancock ~]$
[txapa@ Hancock ~]$ ssh davis
txapa@davis's password:
Last login: Sun Mar 22 20:23:40 2020 from 10.10.0.4
[txapa@davis ~]$
  
```

Una de las consecuencias de usar un servidor intermediario es que, para realizar una transferencia de archivos, es necesario copiarlos a Hancock y luego al sistema de destino, algo que no siempre es posible (i.e. por tamaño, por comodidad, etc.). Por favor, **no abuse del espacio de disco disponible en Hancock**. Si no es posible utilizar la VPN, la alternativa recomendada es usar un túnel de SSH (ver sección siguiente).

TÚNELES

Cualquier sistema (Linux, Windows, etc.) posee diferentes servicios de red que 'atienden' en 'ventanillas' numeradas llamadas puertos. Por ejemplo, un servidor web atiende a los navegadores en el puerto 80, un servidor de e-mail atiende a los programas de correo en el puerto 143 y un servidor de SSH atiende a las terminales en el puerto 22.

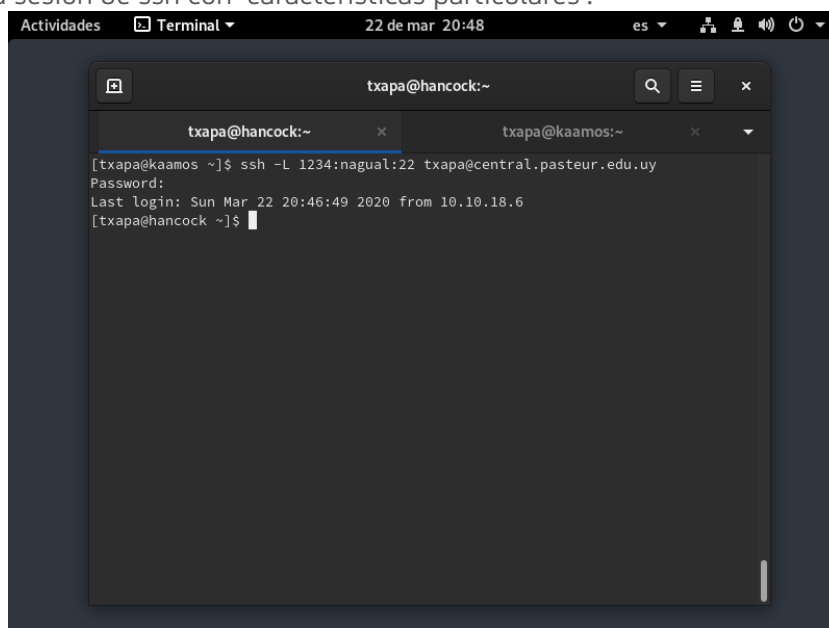
Si usted no puede conectarse a la VPN y decide utilizar a Hancock como login host (ver sección anterior), puede utilizarlo como intermediario para llegar «directamente» hasta su equipo en la

red interna. Esto conoce como [túnel de ssh](#). El servidor de SSH en Hancock permite ‘conectar’ o ‘asociar’ un puerto de su propia máquina al puerto 22 (ssh) de un equipo de Pasteur.

Suponga que, desde su hogar, quiere acceder a Nagual (nagual.ipmont.lan, un servidor de la UBI) para usar ssh, scp, sftp o rsync (todos usan SSH como transporte). Usted puede ‘asociar’ el puerto 1234 de su computadora (siempre debe ser un número mayor o igual a 1025) al puerto 22 de Nagual (el puerto del servicio ssh). Para ello, debe hacer un túnel usando a Hancock como intermediario. La sintaxis es:

```
ssh -L 1234:nagual:22 usuario@central.pasteur.edu.uy
```

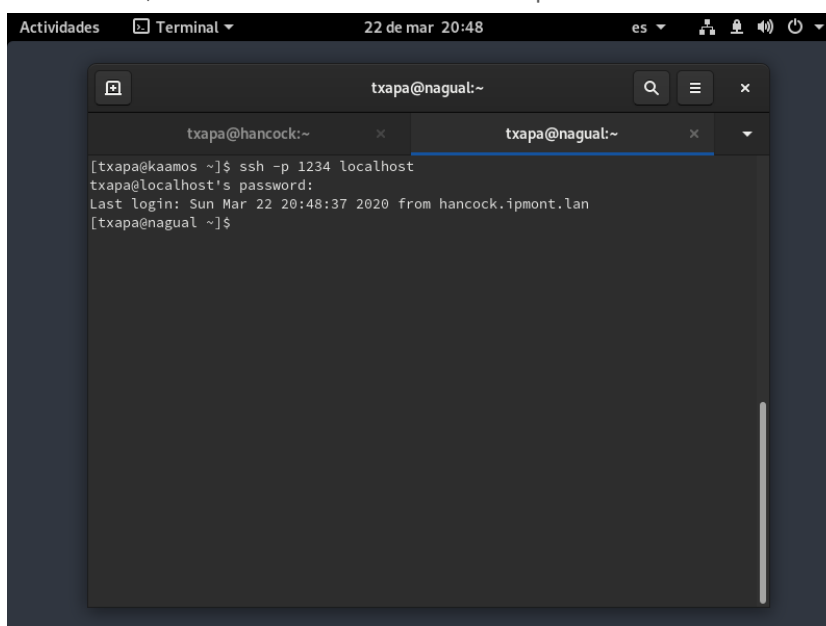
El resultado es una sesión de ssh con ‘características particulares’.



No cierre la terminal e inicie otra(s). Mientras esta sesión de ssh esté abierta, el puerto 1234 de su máquina estará ‘conectado’ al puerto de ssh de Nagual. Recuerde que su máquina (sea ésta la que fuere) **siempre tendrá como nombre ‘localhost’ y como dirección IP 127.0.0.1**. Entonces, podrá ingresar a Nagual con el siguiente comando:

```
ssh -p 1234 localhost
```

La siguiente imagen muestra cómo se ingresa a un shell interactivo en Nagual, **desde otra terminal**, utilizando el túnel, evitando hacer ssh a Hancock primero.



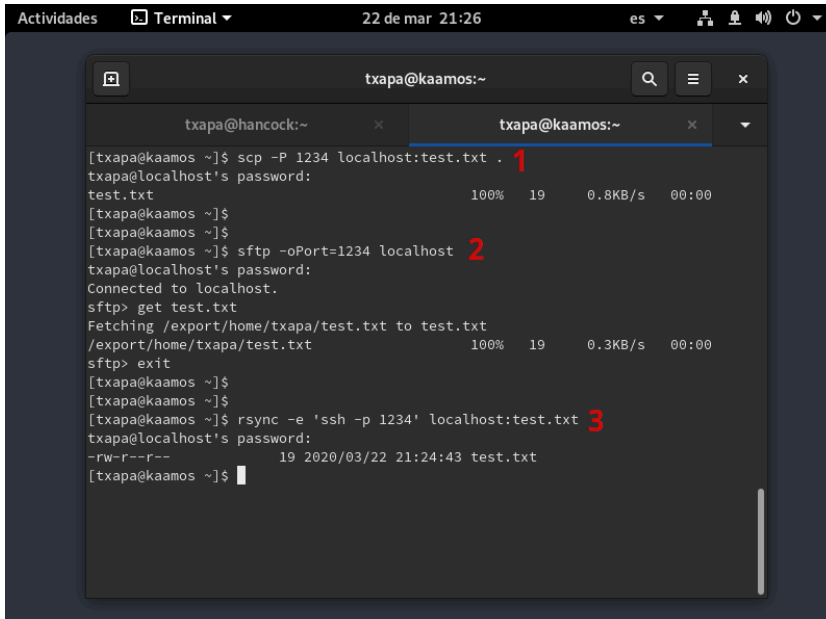
La principal utilidad de un túnel es la transferencia de archivos en un solo paso. Las sintaxis para scp, ftp y rsync son las siguientes:

```
sftp -oPort=1234 localhost
```

```
scp -P 1234 localhost:/dir1/archivo /dir2/
```

```
rsync -e 'ssh -p 1234' localhost:/dir1/archivo /dir2/
```

En la siguiente imagen se puede ver la misma transferencia mediante sftp, scp y rsync usando un túnel por Hancock sobre el puert 1234.



```

Actividades Terminal 22 de mar 21:26 es
txapa@kaamos:~
txapa@hancock:~ x txapa@kaamos:~ x
[txapa@kaamos ~]$ scp -P 1234 localhost:test.txt . 1
txapa@localhost's password:
test.txt 100% 19 0.8KB/s 00:00
[txapa@kaamos ~]$
[txapa@kaamos ~]$
[txapa@kaamos ~]$ sftp -oPort=1234 localhost 2
txapa@localhost's password:
Connected to localhost.
sftp> get test.txt
Fetching /export/home/txapa/test.txt to test.txt
/export/home/txapa/test.txt 100% 19 0.3KB/s 00:00
sftp> exit
[txapa@kaamos ~]$
[txapa@kaamos ~]$
[txapa@kaamos ~]$ rsync -e 'ssh -p 1234' localhost:test.txt 3
txapa@localhost's password:
-rw-r--r-- 19 2020/03/22 21:24:43 test.txt
[txapa@kaamos ~]$

```

DESDE WINDOWS

Si no tiene más remedio que usar Windows para ingresar en forma remota (e.g. desde su hogar) a un equipo Linux, deberá seguir tres pasos:

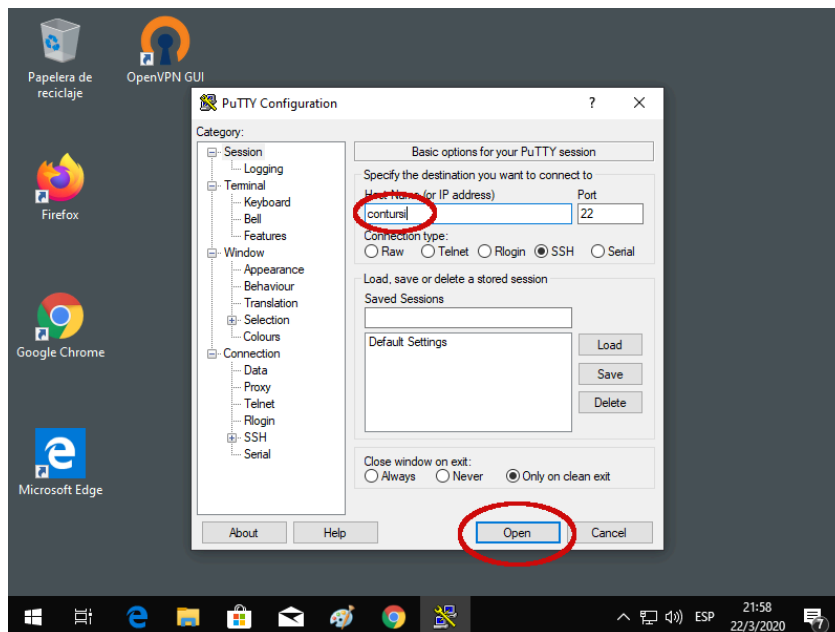
- Conectar su equipo Windows a la VPN (debe seguir las instrucciones para Windows)
- Configurar NoMachine para acceder remotamente al escritorio (gráfico) de su equipo de Pasteur (esto es opcional)
- Utilizar un emulador de terminal para Windows, de modo de acceder por SSH a su equipo de Pasteur
- Utilizar un programa de transferencia de archivos con soporte para SSH (sftp)

Esta sección se refiere únicamente a los dos últimos ítems. Existen varios emuladores de terminal para Windows ([PuTTY](#), [SecureCRT](#), [MobaXterm](#)) aunque se recomienda utilizar PuTTY (es liviano, gratuito, funciona bien y ante una urgencia ni siquiera precisa instalación).

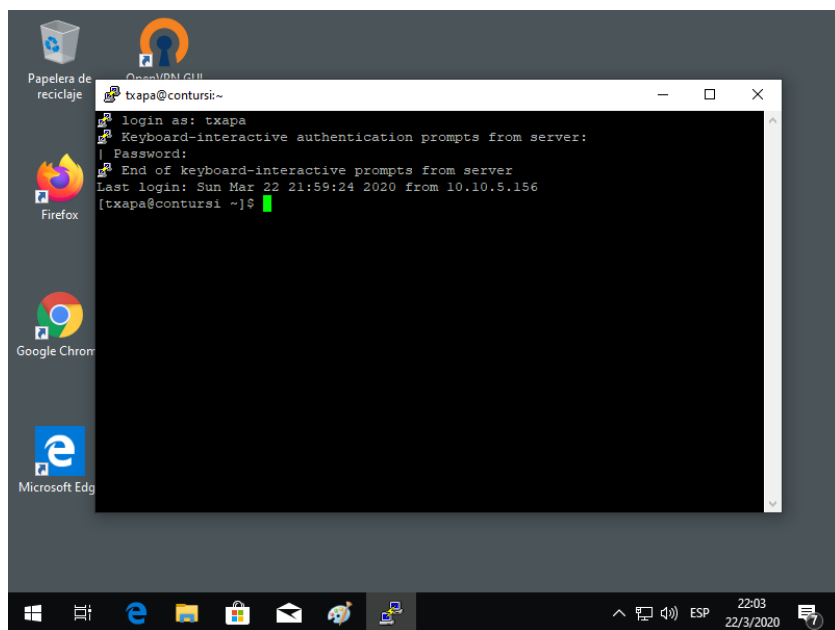
[Descargar el instalador de PuTTY para Windows de 64 bits](#)

[Descargar el ejecutable para iniciar directamente](#)

Ejecute el programa e ingrese los datos de la conexión. Deberá conocer el nombre de su computadora en la red de Pasteur. De no ser así, por favor solicite asistencia enviando un e-mail a soporte@pasteur.edu.uy.



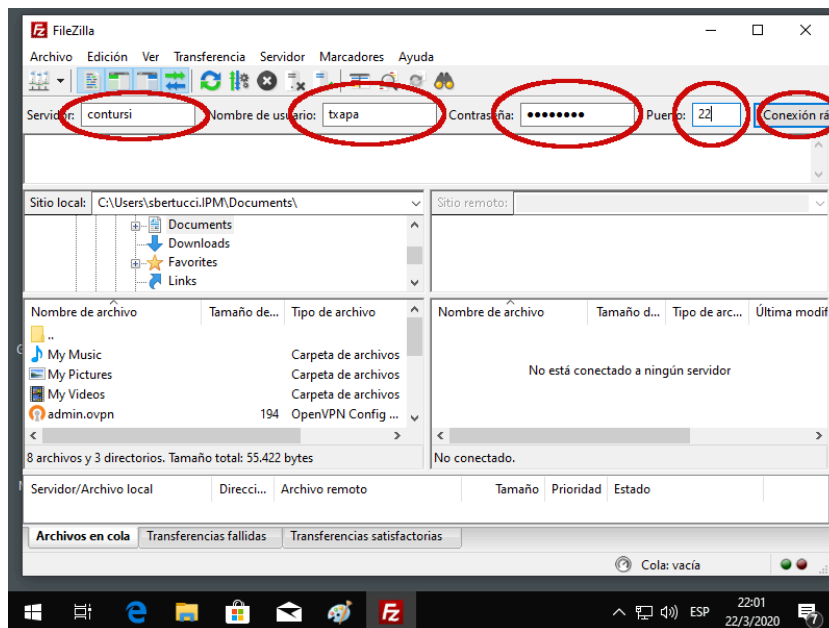
Una vez establecida la conexión, podrá ingresar sus credenciales y trabajar de forma similar a como lo hace desde una terminal en Linux.



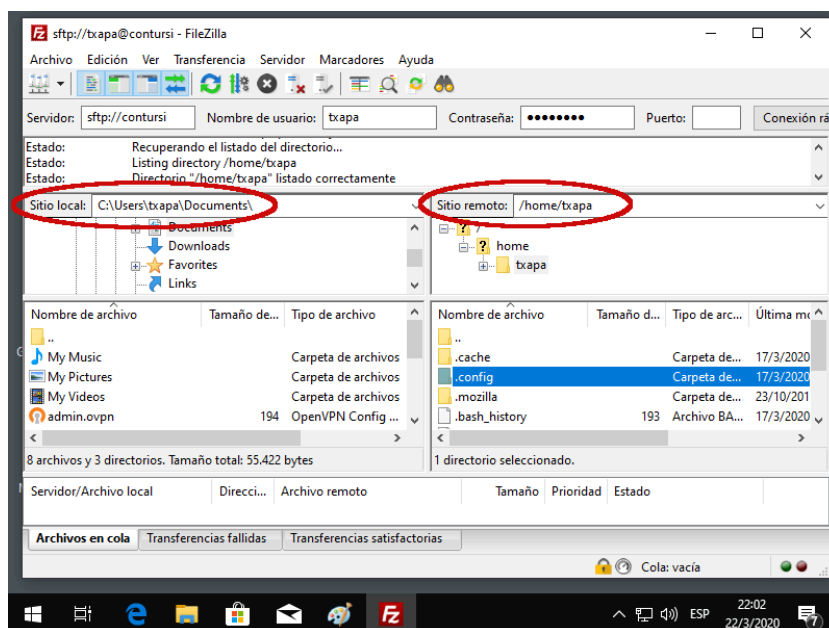
A los efectos de transferir archivos, sugerimos el uso de FileZilla (es gratuito, open source y está disponible para todas las plataformas). Le permitirá subir y bajar archivos entre un equipo local (e.g. en su hogar) y otro del instituto.

[Descargar el instalador de FileZilla para Windows de 64 bits](#)

Instale el programa y ejecútelo. En la pantalla de bienvenida se le solicitarán sus credenciales para ingresar al sistema en cuestión.



Una vez establecida la conexión, se le presentarán dos ‘ventanas’. A la izquierda tendrá el directorio de su equipo local en Windows (e.g. en su hogar) y a la derecha el directorio del equipo remoto en Linux (e.g. en Pasteur). Podrá arrastrar archivos y carpetas de un lado al otro.



Tanto PuTTY como FileZilla permiten el ingreso sin tener que escribir la contraseña, mediante el uso de llaves públicas (ver sección correspondiente más arriba). La implementación queda como ejercicio para el lector. Google is your friend.

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 TeamViewer 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)