

Sistemas Informáticos DAW



# Conexión con la RED

VERÓNICA BONIS MARTÍN  
MARIA CARMEN CORREA HERAS  
ÁNGEL SÁNCHEZ-SIERRA CRUZ  
JOSÉ MARÍA TENREIRO EIRANOVA  
JUAN RAMON VARÓ NÚÑEZ

## Requerimiento 1

### FUNDAMENTACIÓN

- En la DIRECCIÓN IP hay una parte de bits que identifican la red y otra parte que identifican el host. En binario son 4 octetos que por convención se suelen separar con un punto, cada bit tiene un valor decimal exacto. El valor más alto sería 128 y a partir de ahí el siguiente bit tiene la mitad de valor.
- Para convertir de decimal a binario, el bit que está a 1 suma el de su posición. Debemos activar los bits que den la suma del decimal.

Ej. 192.x.x.x para calcular el primer octeto de una dir.IP que sea 192. (clase C) así haremos con cada octeto.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

- La MÁSCARA DE SUBRED aparece después de la dirección IP separada por una barra y puede aparecer en dos formatos distintos, representando los octetos en decimal o el número de bits que tienen a 1 en binario.
- La máscara de subred me va a indicar la cantidad de bits que identifican a la red, con ella otros dispositivos pueden saber si se están conectando a la misma red. En función de su tamaño tenemos varios tipos de direcciones, las más habituales son la CLASE A (0-127), CLASE B (128-191) y CLASE C (192-223).
- Las de clase C tienen menor número de bits para Host que las de B y a su vez éstas menor que las de A.
- Hay tres tipos de direcciones, una para host y otras dos reservadas para la dirección de Red y la dirección de broadcast (difusión).
- La DIRECCIÓN DE RED la parte que identifica al host está todo a 0 en binario. Se calcula haciendo un AND lógico.
- La DIRECCIÓN DE BROADCAST la parte que identifica al host está todo a 1 en binario. Se calcula haciendo un OR lógico.

### Actividad 3. Conexión con la RED

#### TAREAS:

Calcula las direcciones de red y difusión en las siguientes redes, suponiendo que tu dirección IP y máscara de subred es la que está indicada en cada caso. Especifica también la clase de red de que se trata y el número máximo de "hosts" (equipos con dirección IP asignada) podemos tener en cada una de ellas.

192.168.2.119 / 255.255.255.192	
Dir. IP:	11000000 10101000 00000010 01110111
Máscara:	11111111 11111111 11111111 11000000
AND Lógico:	11000000 10101000 00000010 01000000
Dir. De red	192. 168.2.64
Dir IP:	11000000 10101000 00000010 01110111
Mascara!:	00000000 00000000 00000000 00111111
OR Lógico:	11000000 10101000 00000010 01111111
Dir. Difusión	192.168.2.127
Hosts:	Máximo 64 dispositivos (-2 de la red de difusión y número de red)
Clase:	C

### Actividad 3. Conexión con la RED

**192.168.2.126/26**

Con esa mascara de 26 bits en la máscara de subred nos están comunicando que de los 32 bits que constituyen la dirección, 26 le pertenecen a la red. Por lo tanto, tenemos la misma máscara de subred que en el anterior ejemplo:

**Dir. IP: 11000000 10101000 00000010 01111110**

**Mascara: 11111111 11111111 11111111 11000000**

**AND Lógico: 11000000 10101000 00000010 11111110**

**Dir. De red 192. 168.2.255**

**Dir. IP: 11000000 10101000 00000010 01111110**

**Mascara!: 00000000 00000000 00000000 00111111**

**OR Lógico: 11000000 10101000 00000010 01111111**

**Dir. Difusión 192.168.2.127**

**Hosts: Máximo 64 dispositivos (-2 de la red de difusión y numero de red)**

**Clase: C**

### Actividad 3. Conexión con la RED

**192.168.0.190 / 255.255.255.240**

**Dir. IP: 11000000 10101000 00000000 10111110**

**Mascara: 11111111 11111111 11111111 11110000**

**AND Lógico: 11000000 10101000 00000000 10110000**

**Dir. De red 192.168.0.176**

**Dir IP: 11000000 10101000 00000000 10111110**

**Mascara!: 00000000 00000000 00000000 00001111**

**OR Lógico: 11000000 10101000 00000000 10111111**

**Dir. Difusión 192.168.0.191**

**Hosts: Máximo 16 dispositivos (-2 de la red de difusión y numero de red)**

**Clase: C**

### Actividad 3. Conexión con la RED

**192.168.0.190 / 255.255.240.0**

**Dir. IP: 11000000 10101000 00000000 10111110**

**Mascara: 11111111 11111111 11110000 00000000**

**AND Lógico: 11000000 10101000 00000000 00000000**

**Dir. De red 192.168.0.0**

**Dir IP: 11000000 10101000 00000000 10111110**

**Mascara!: 00000000 00000000 00001111 11111111**

**OR Lógico: 11000000 10101000 00001111 11111111**

**Dir. Difusión 192.168.15.255**

**Hosts: Máximo 256 dispositivos (-2 de la red de difusión y numero de red)**

**Clase: C**

### Actividad 3. Conexión con la RED

<b>40.168.2.119 / 255.255.0.0</b>	
<b>Dir. IP:</b>	<b>00101000 10101000 00000010 01110111</b>
<b>Mascara:</b>	<b>11111111 11111111 00000000 00000000</b>
<b>AND Lógico:</b>	<b>00101000 10101000 00000000 00000000</b>
<b>Dir. De red</b>	<b>40.168.0.0</b>
<b>Dir IP:</b>	<b>00101000 10101000 00000010 01110111</b>
<b>Mascara!:</b>	<b>00000000 00000000 11111111 11111111</b>
<b>OR Lógico:</b>	<b>00101000 10101000 11111111 11111111</b>
<b>Dir. Difusión</b>	<b>40.168.255.255</b>
<b>Hosts:</b>	<b>Máximo 65.536 dispositivos (-2 de la red de difusión y numero de red)</b>
<b>Clase:</b>	<b>A</b>

Si te damos las siguientes máscaras de subred, dinos cuántos hosts puede tener como máximo cada subred:

**255.255.255.128**

(256-128-2 direcciones especiales) =126 host pueden conectarse.

**255.255.255.255**

No se puede conectar ningún host.

### Actividad 3. Conexión con la RED

**255.255.255.224**

(256-224-2 direcciones especiales) =30 host pueden conectarse

Por último, si tienes una red de Clase A con máscara de subred 255.255.255.0...

**¿Cuántas subredes con máscara 255.255.255.128 podemos tener dentro de ella?**

Mascara red clase A    255.255.255.0            Parte de red / Reservado subred / hosts

11111111 11111111 11111111 00000000

Mascara subred        255.255.255.128

11111111 11111111 11111111 10000000

Reservadas para subredes 17 bits, por lo tanto  $2^{17} = 131072 - 2 = 131070$  Subredes que se pueden crear.

La subred 255.255.255.128 puede direccionar hasta **128** hosts.

**¿Cuántas subredes con máscara 255.255.255.240 podemos tener dentro de ella?**

Mascara red clase A    255.255.255.0            Parte de red / Reservado subred / hosts

11111111 11111111 11111111 00000000

Mascara subred        255.255.255.240

11111111 11111111 11111111 11110000

Reservadas para subredes 20 bits, por lo tanto  $2^{20} = 1048576 - 2 = 1048574$  Subredes que se pueden crear.

La subred 255.255.255.240 puede direccionar hasta **16** hosts.



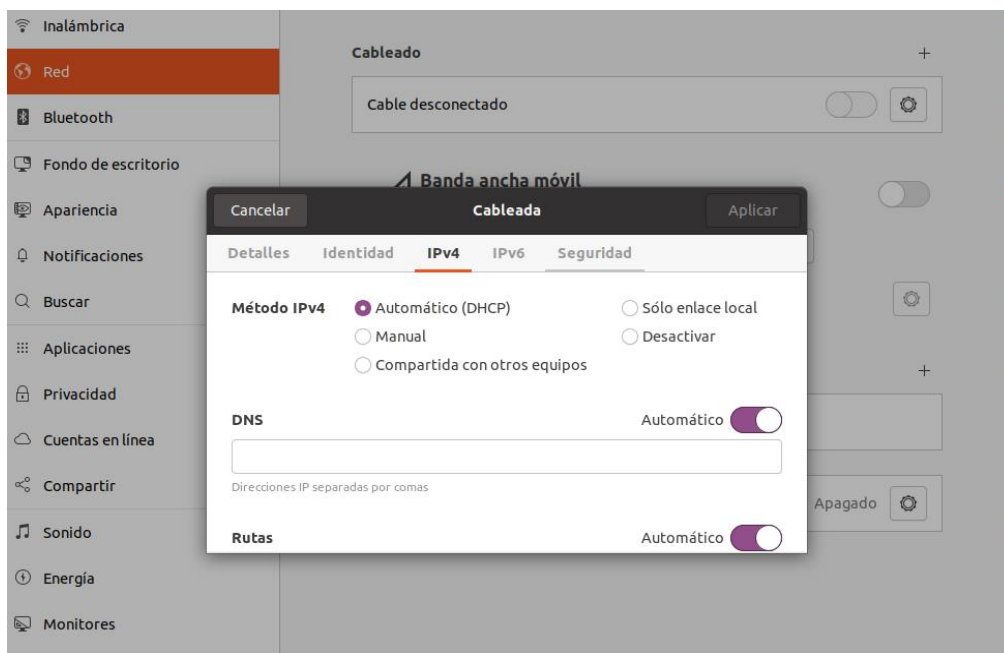
## Actividad 3. Conexión con la RED

### Configuración IP

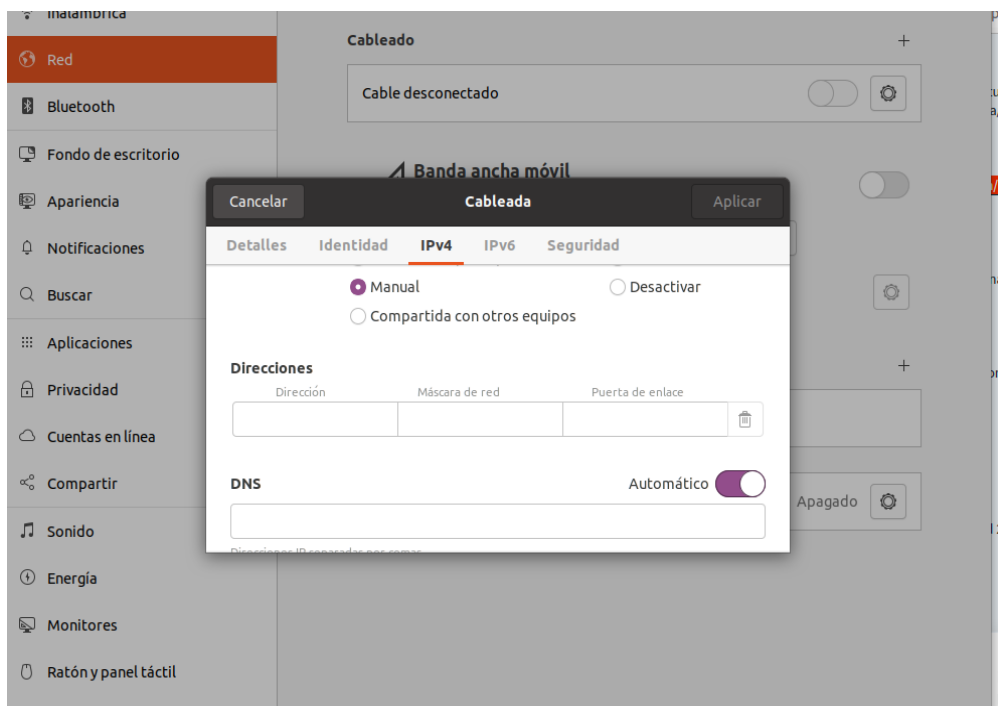
Averigua la dirección IP (estática o dinámica) de tu ordenador personal, de tu máquina virtual de Windows10 y de tu máquina virtual Ubuntu. En la respuesta puedes copiar las pantallas/ventanas de cada sistema, pero incluye también la visualización utilizando comandos de consola/terminal.

### VISUALIZACIÓN CON INTERFAZ GRÁFICA

En Ubuntu nos desplazaremos en mostrar aplicaciones/ Configuración/Red y opciones en Cableado, allí observaremos que nos va a establecer la IPv4 de forma automática.



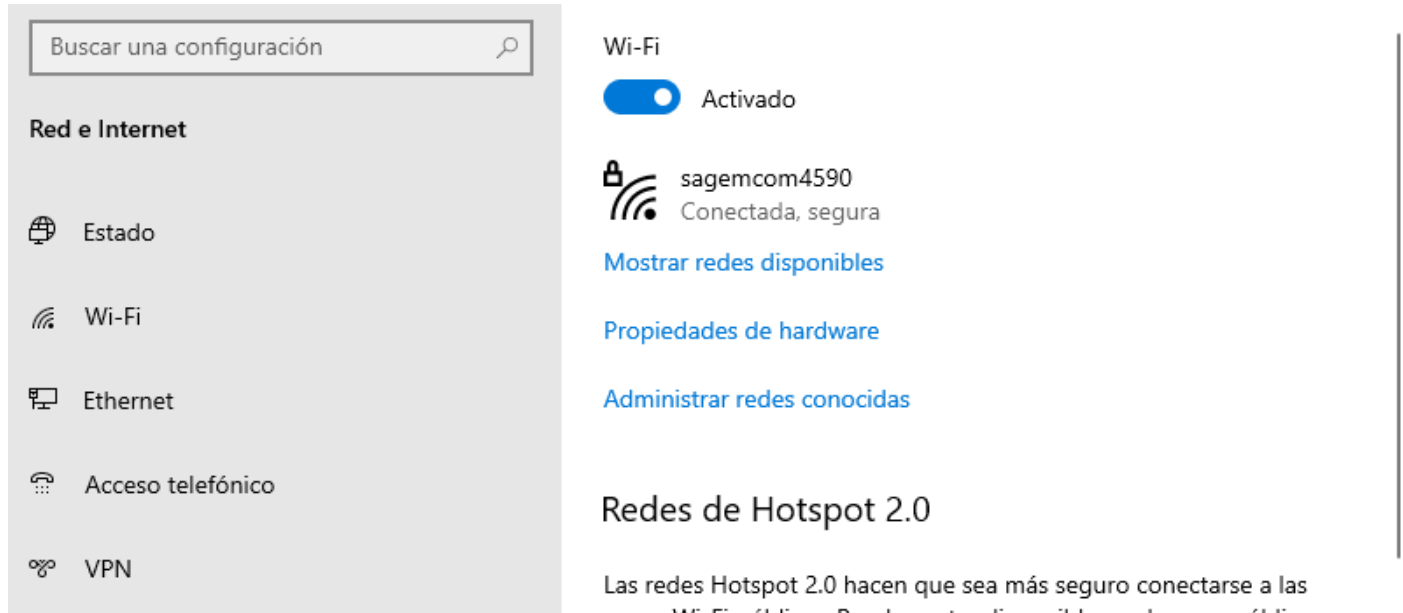
Si quisiéramos establecer una ip estática, tendríamos que escoger la opción Manual y rellenar los campos de la ip:



### Actividad 3. Conexión con la RED

En el caso de Windows, la forma de averiguar si tenemos una ip estática o dinámica es muy similar a Linux, tendríamos que ir a:

Configuración y en la parte de Red haríamos click en el apartado de nuestro Router o Modem:



Después, buscamos la parte de configuración de IP, y ahí ya nos aparece si tenemos por defecto la IP dinámica (automático DHCP).

 sagemcom4590

#### Configuración de IP

Asignación de IP:

Automático (DHCP)

[Editar](#)

#### Propiedades

SSID:

Protocolo:

Tipo de seguridad:

Banda de red:

Canal de red:

1

Velocidad de vínculo (recepción/  
transmisión):

54/144 (Mbps)

Dirección IPv6 local de vínculo:

fe80::b5cb:5df3:bbf6:d261%20

#### Editar configuración de IP

Automático (DHCP)

Manual

[Guardar](#)

[Cancelar](#)

### Actividad 3. Conexión con la RED

Si queremos cambiarla a fija o estática, en el desplegable, hacemos click en Manual y ahí introducimos los parámetros de nuestra IP fija:

Configuración

sagemcom4

Configuración de IP

Asignación de IP:

Editar

Propiedades

SSID:

Protocolo:

Tipo de seguridad:

Banda de red:

Canal de red:

Velocidad de vínculo (recepción y transmisión):

Dirección IPv6 local de vínculo:

Dirección IPv4:

Servidores DNS IPv4:

Fabricante:

Descripción:

Editar configuración de IP

Manual

IPv4

Activado

Dirección IP

Longitud del prefijo de subred

Puerta de enlace

DNS preferido

DNS alternativo

Guardar Cancelar

### VISUALIZACIÓN MEDIANTE COMANDOS

En Windows podemos activar la consola con cmd y con el comando ipconfig podemos ver la información de nuestra configuración del protocolo TCP/IP de nuestro ordenador personal.

```

C:\> Símbolo del sistema

Microsoft Windows [Versión 10.0.18363.1256]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Mari Carmen>ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 3:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet VMware Network Adapter VMnet1:

    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::9804:8c42:996d:4da5%4
    Dirección IPv4. . . . . : 192.168.85.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

Adaptador de Ethernet VMware Network Adapter VMnet8:

    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::34d6:5b57:e5e7:6704%14
```

### Actividad 3. Conexión con la RED

En el caso de Ubuntu, primero nos pedirá instalar un paquete de datos para poder acceder a la información de la ip privada:

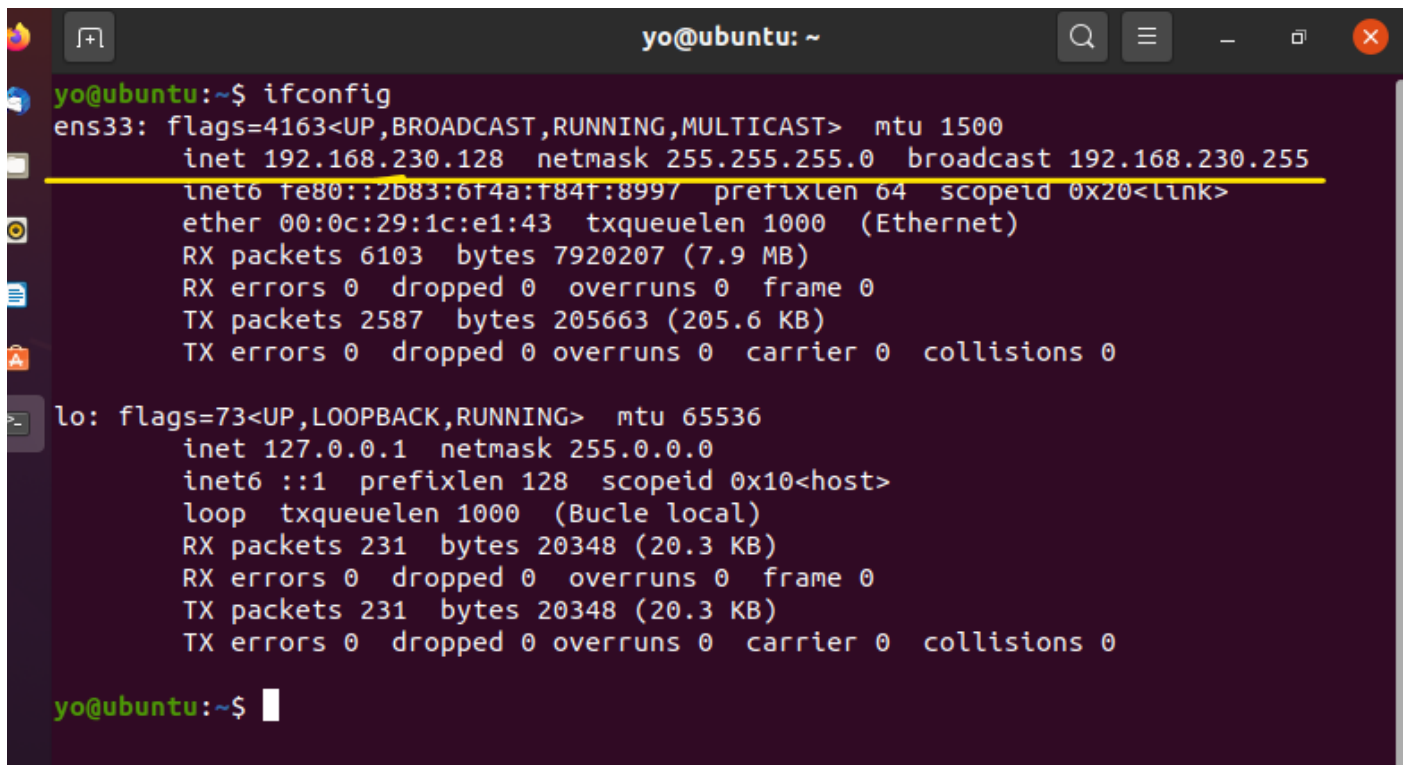
```
yo@ubuntu:~/Desktop$ cd
yo@ubuntu:~$ ifconfig

No se ha encontrado la orden «ifconfig», pero se puede instalar con:

sudo apt install net-tools

yo@ubuntu:~$ sudo apt install net-tools
[sudo] contraseña para yo:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
linux-headers-5.8.0-48-generic linux-hwe-5.8-headers-5.8.0-48
linux-image-5.8.0-48-generic linux-modules-5.8.0-48-generic
linux-modules-extra-5.8.0-48-generic
```

Después de instalarla, ya podemos acceder a la información de la ip a través del comando ifconfig:



```
yo@ubuntu: ~
yo@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.230.128  netmask 255.255.255.0  broadcast 192.168.230.255
    inet6 fe80::2b83:6f4a:f84f:8997  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:1c:e1:43  txqueuelen 1000  (Ethernet)
    RX packets 6103  bytes 7920207 (7.9 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 2587  bytes 205663 (205.6 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Bucle local)
    RX packets 231  bytes 20348 (20.3 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 231  bytes 20348 (20.3 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

yo@ubuntu:~$
```

## Actividad 3. Conexión con la RED

### Conexión con Internet

Averigua también la dirección IP pública de tu conexión a Internet. Puedes usar por ejemplo la página <http://www.cualesmiip.com/> o cualquier otra similar.

Mediante la página web [cualesmiip](http://www.cualesmiip.com/) es muy fácil y rápido saber cuál es nuestra ip:

### ¿Qué es la IP?

La IP se traduce por Internet Protocol, protocolo de Internet en español, y se trata de un protocolo utilizado para la comunicación de datos a través de una red de paquetes combinados.

### ¿Qué es una dirección IP?

Una dirección IP es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

### ¿Qué diferencia hay entre dirección IP pública y privada?

La dirección IP puede ser pública o privada:

- ✓ La dirección IP pública es un número único que identifica nuestra red desde el exterior.
- ✓ La dirección IP privada es un número único que identifica a un dispositivo conectado en nuestra red interna.

Tu dirección IP es **82.158.134.25** 

[Geolocalizar IP](#)

Existe una forma de averiguar tu ip pública mediante comandos en linux que es instalando un paquete llamado curl, se haría de la siguiente forma:

```
jnte@jnte-DELL: ~  
jnte@jnte-DELL:~$ sudo apt install curl  
[sudo] contraseña para jnte:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
  libfprint-2-tod1 libllvm10  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes NUEVOS:  
  curl  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 10 no actualizados.  
Se necesita descargar 161 kB de archivos.  
Se utilizarán 411 kB de espacio de disco adicional después de esta operación.  
Des:1 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 curl amd64 7.68.0-1ubuntu2.5 [161 kB]  
Descargados 161 kB en 0s (515 kB/s)  
Seleccionando el paquete curl previamente no seleccionado.  
(Leyendo la base de datos ... 196015 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar ../curl_7.68.0-1ubuntu2.5_amd64.deb ...  
Desempaquetando curl (7.68.0-1ubuntu2.5) ...  
Configurando curl (7.68.0-1ubuntu2.5) ...  
Procesando disparadores para man-db (2.9.1-1) ...  
jnte@jnte-DELL:~$ curl ifconfig.me  
82.158.134.25jnte@jnte-DELL:~$
```

### Actividad 3. Conexión con la RED

#### Practicar con “ping”

Realiza el ejercicio propuesto en el módulo 5.2 con el comando “ping” y comprueba la conexión entre tu máquina física y tus máquinas virtuales. Si tu ordenador lo soporta comprueba también la conexión entre ellas, y si no solamente de cada una con la máquina física.

Lanzamos Ping desde nuestro ordenador personal (IP 192.168.1.39) a nuestra máquina virtual Ubuntu con IP 192.168.15.130

```
C:\> Símbolo del sistema

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::e0a0:1b72:caf5:55d3%14
Dirección IPv4. . . . . : 192.168.129.1
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . . :

Adaptador de Ethernet VMware Network Adapter VMnet8:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::6124:59c4:48d8:ae55%4
Dirección IPv4. . . . . : 192.168.15.1
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . . :

Adaptador de LAN inalámbrica Conexión de red inalámbrica:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::4910:e3b2:f012:4775%25
Dirección IPv4. . . . . : 192.168.1.39
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . . : 192.168.1.1
```

```
C:\> Símbolo del sistema

Microsoft Windows [Versión 10.0.19041.985]
(c) Microsoft Corporation. Todos los derechos reservados.

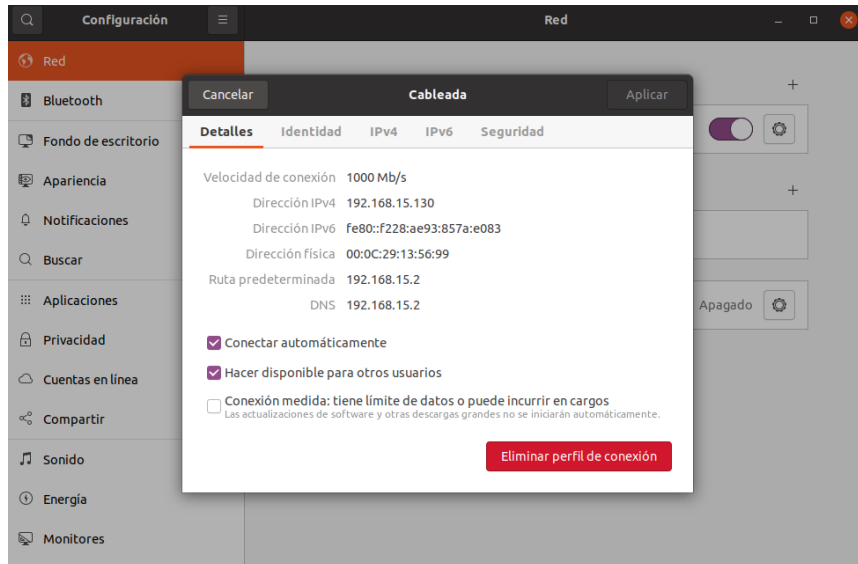
C:\Users\Dad>ping 192.168.15.130

Haciendo ping a 192.168.15.130 con 32 bytes de datos:
Respuesta desde 192.168.15.130: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.15.130: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.15.130: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.15.130: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.15.130:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

### Actividad 3. Conexión con la RED

Lanzamos Ping desde nuestra máquina virtual Ubuntu IP 192.168.15.130 a nuestro ordenador personal con Windows10 con IP 192.168.1.39:



```
angelssc@ubuntu: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
angelssc@ubuntu:~$ ping 192.168.1.39  
PING 192.168.1.39 (192.168.1.39) 56(84) bytes of data.  
64 bytes from 192.168.1.39: icmp_seq=1 ttl=128 time=2.42 ms  
64 bytes from 192.168.1.39: icmp_seq=2 ttl=128 time=0.892 ms  
64 bytes from 192.168.1.39: icmp_seq=3 ttl=128 time=0.850 ms  
64 bytes from 192.168.1.39: icmp_seq=4 ttl=128 time=0.890 ms  
64 bytes from 192.168.1.39: icmp_seq=5 ttl=128 time=1.01 ms  
64 bytes from 192.168.1.39: icmp_seq=6 ttl=128 time=0.842 ms  
64 bytes from 192.168.1.39: icmp_seq=7 ttl=128 time=0.867 ms  
64 bytes from 192.168.1.39: icmp_seq=8 ttl=128 time=0.926 ms  
64 bytes from 192.168.1.39: icmp_seq=9 ttl=128 time=0.867 ms  
64 bytes from 192.168.1.39: icmp_seq=10 ttl=128 time=0.881 ms  
64 bytes from 192.168.1.39: icmp_seq=11 ttl=128 time=0.905 ms  
64 bytes from 192.168.1.39: icmp_seq=12 ttl=128 time=1.01 ms  
64 bytes from 192.168.1.39: icmp_seq=13 ttl=128 time=1.00 ms  
64 bytes from 192.168.1.39: icmp_seq=14 ttl=128 time=0.987 ms  
64 bytes from 192.168.1.39: icmp_seq=15 ttl=128 time=0.951 ms  
64 bytes from 192.168.1.39: icmp_seq=16 ttl=128 time=0.836 ms  
64 bytes from 192.168.1.39: icmp_seq=17 ttl=128 time=0.822 ms  
  
64 bytes from 192.168.1.39: icmp_seq=18 ttl=128 time=0.848 ms
```



## Actividad 3. Conexión con la RED

### Conexión SSH Windows-Ubuntu

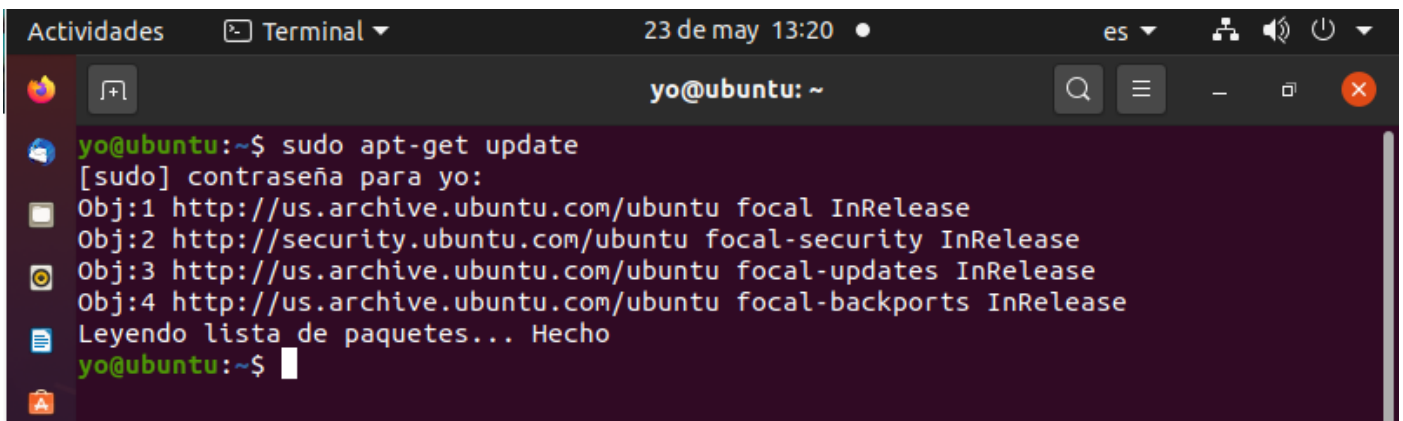
**Realiza el ejercicio práctico propuesto en la lección 5.3 Seguridad en la red siguiendo los pasos que en él se indican. Aporta como resultado los pantallazos de tus máquinas virtuales.**

Vamos a ver cómo podríamos hacer una conexión segura utilizando el protocolo SSH entre un sistema Windows y otro Linux:

Para hacerlo utilizaremos nuestro sistema anfitrión y nuestra máquina virtual Linux Ubuntu. Como en toda conexión de este tipo necesitaremos un "cliente SSH" (lo usaremos sobre Windows) y un "servidor SSH" (en este caso sobre Ubuntu). Ambos, cliente y servidor, no suelen estar preinstalados en los sistemas, así que los cargaremos.

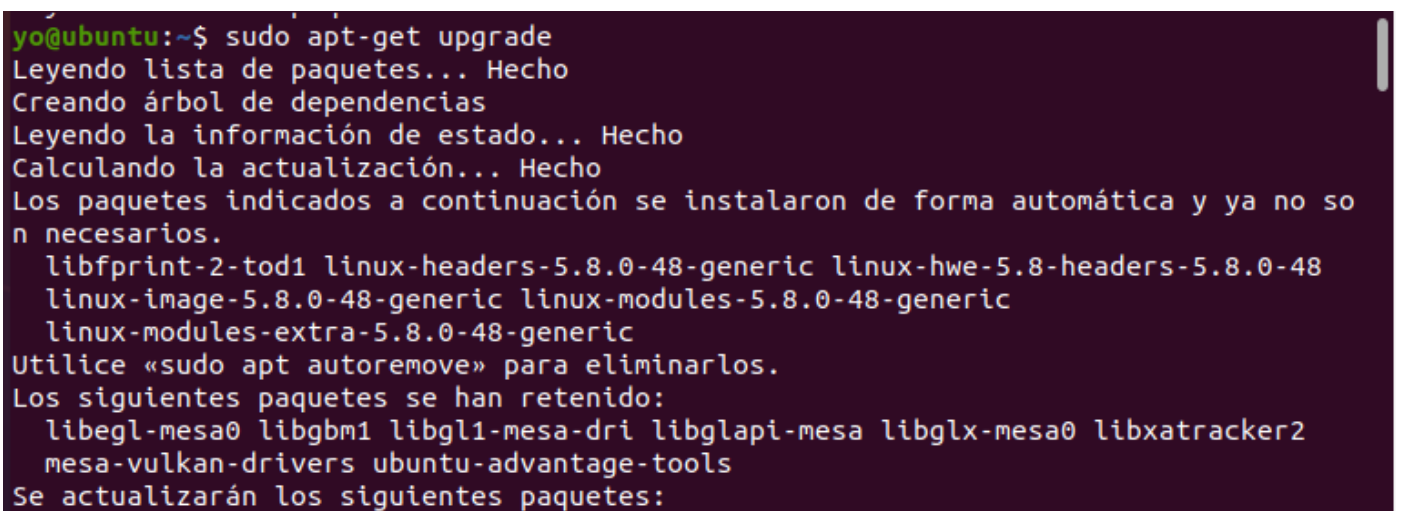
Ejecutamos sobre el terminal de la máquina virtual de Ubuntu los siguientes pasos:

***sudo apt-get update***



```
yo@ubuntu: ~$ sudo apt-get update
[sudo] contraseña para yo:
Obj:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Obj:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Obj:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Obj:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Leyendo lista de paquetes... Hecho
yo@ubuntu:~$
```

***sudo apt-get upgrade***

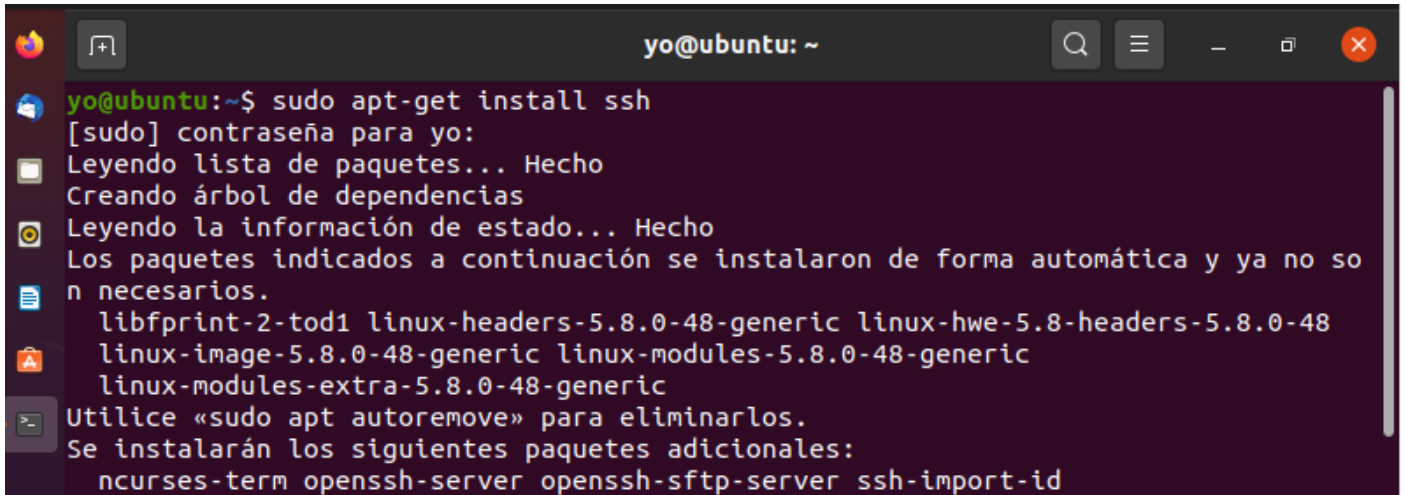


```
yo@ubuntu:~$ sudo apt-get upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 libfprint-2-tod1 linux-headers-5.8.0-48-generic linux-hwe-5.8-headers-5.8.0-48
 linux-image-5.8.0-48-generic linux-modules-5.8.0-48-generic
 linux-modules-extra-5.8.0-48-generic
Utilice «sudo apt autoremove» para eliminarlos.
Los siguientes paquetes se han retenido:
 libegl-mesa0 libgbm1 libgl1-mesa-dri libglapi-mesa libglx-mesa0 libxatracker2
 mesa-vulkan-drivers ubuntu-advantage-tools
Se actualizarán los siguientes paquetes:
```



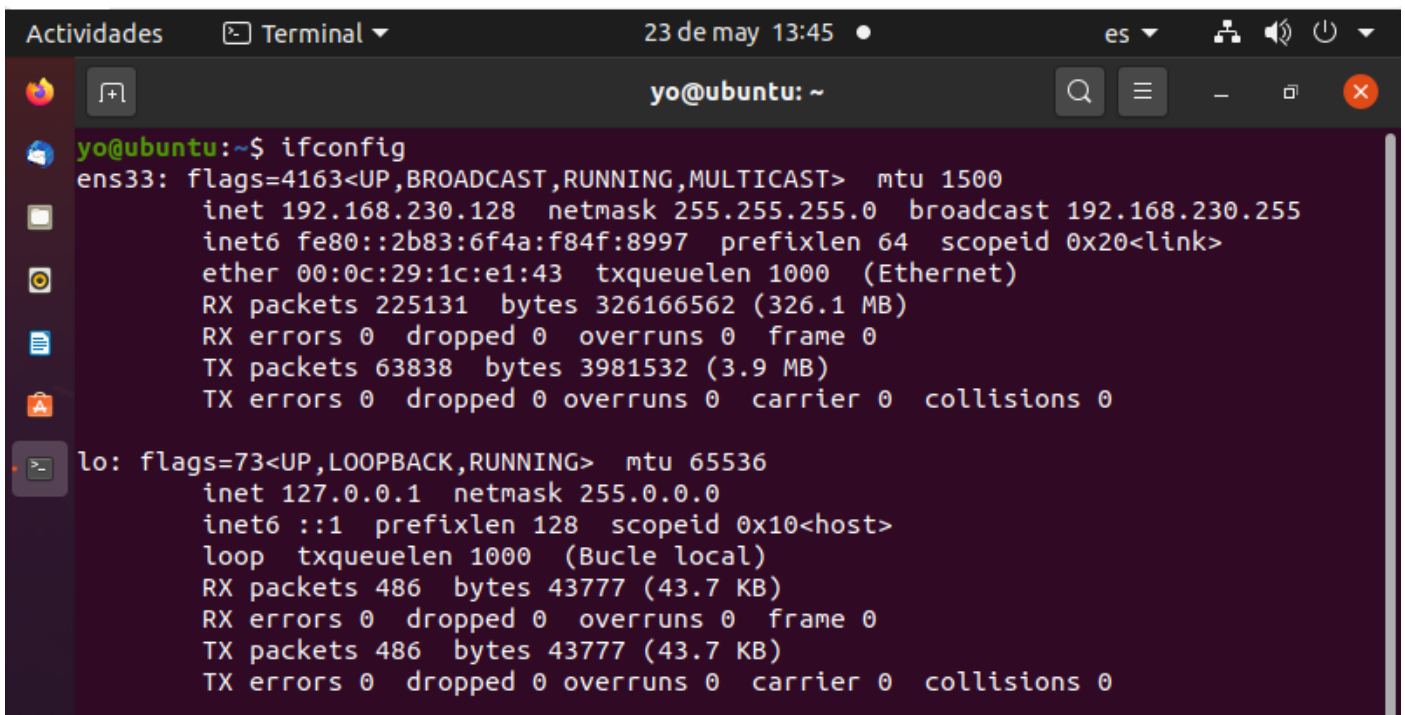
### Actividad 3. Conexión con la RED

**sudo apt-get install ssh** (con esto instalamos el servidor SSH).



```
yo@ubuntu: ~  
yo@ubuntu:~$ sudo apt-get install ssh  
[sudo] contraseña para yo:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
libfprint-2-tod1 linux-headers-5.8.0-48-generic linux-hwe-5.8-headers-5.8.0-48  
linux-image-5.8.0-48-generic linux-modules-5.8.0-48-generic  
linux-modules-extra-5.8.0-48-generic  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
ncurses-term openssh-server openssh-sftp-server ssh-import-id
```

**ifconfig** (para comprobar la dirección IP de nuestro sistema Ubuntu).



```
Actividades Terminal 23 de may 13:45 es  
yo@ubuntu: ~  
yo@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.230.128 netmask 255.255.255.0 broadcast 192.168.230.255  
inet6 fe80::2b83:6f4a:f84f:8997 prefixlen 64 scopeid 0x20<link>  
ether 00:0c:29:1c:e1:43 txqueuelen 1000 (Ethernet)  
RX packets 225131 bytes 326166562 (326.1 MB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 63838 bytes 3981532 (3.9 MB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Bucle local)  
RX packets 486 bytes 43777 (43.7 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 486 bytes 43777 (43.7 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

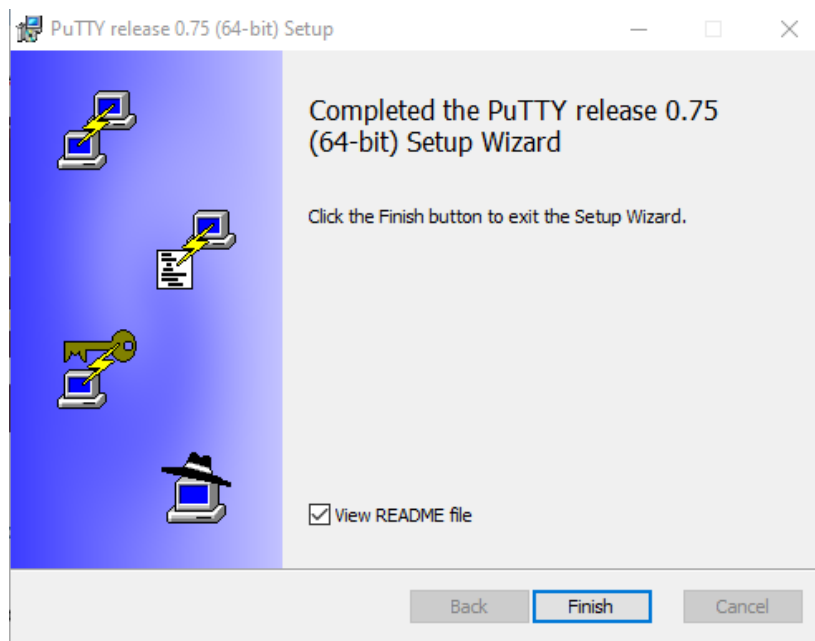
### Actividad 3. Conexión con la RED

`netstat -a | grep ssh` (comprobamos que SSH está activo y escuchando).

```
yo@ubuntu:~$ netstat -a | grep ssh
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*        ESCUCHAR
tcp6       0      0 :::ssh             :::*             ESCUCHAR
unix  2      [ ACC ]     FLUJO          ESCUCHANDO        54955      /run/user/1000/gnupg/S.gp
g-agent.ssh
unix  2      [ ACC ]     FLUJO          ESCUCHANDO        57995      /tmp/ssh-VnHpLN4JhnKd/age
nt.1854
unix  2      [ ACC ]     FLUJO          ESCUCHANDO        59469      /run/user/1000/keyring/ss
h
yo@ubuntu:~$
```

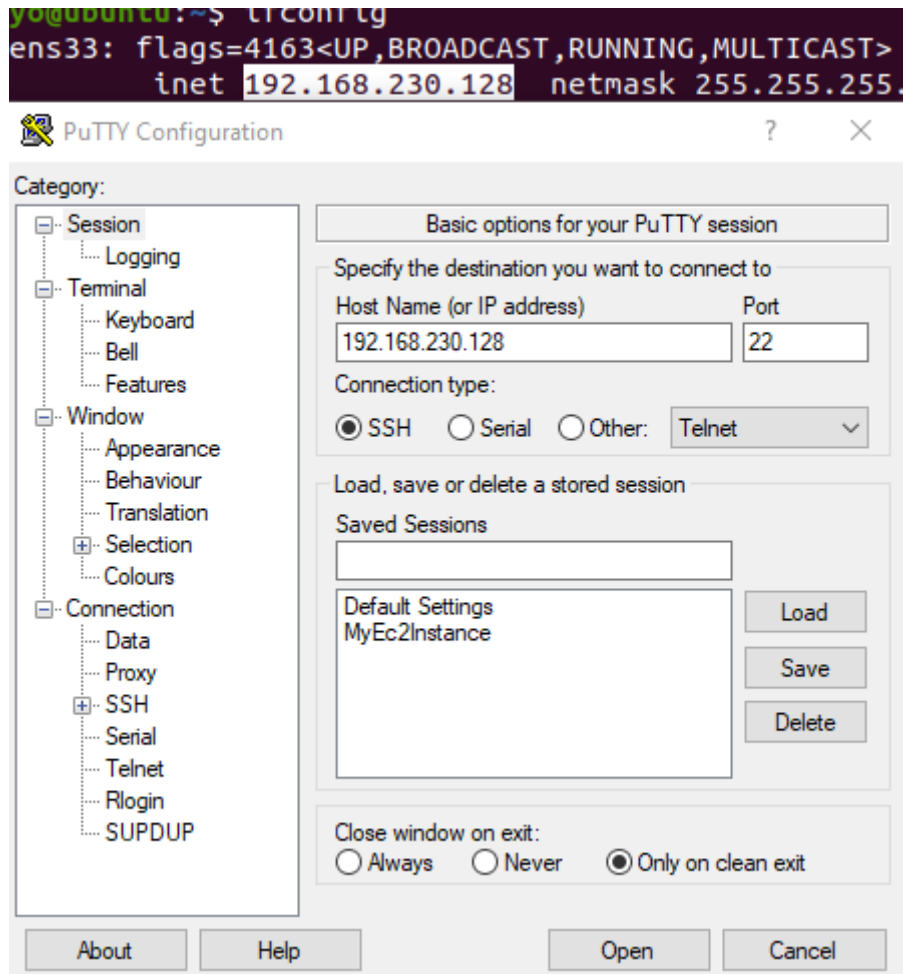
Ahora en nuestro sistema anfitrión Windows:

Descargamos la aplicación “**putty.exe**” desde <https://www.putty.org/>

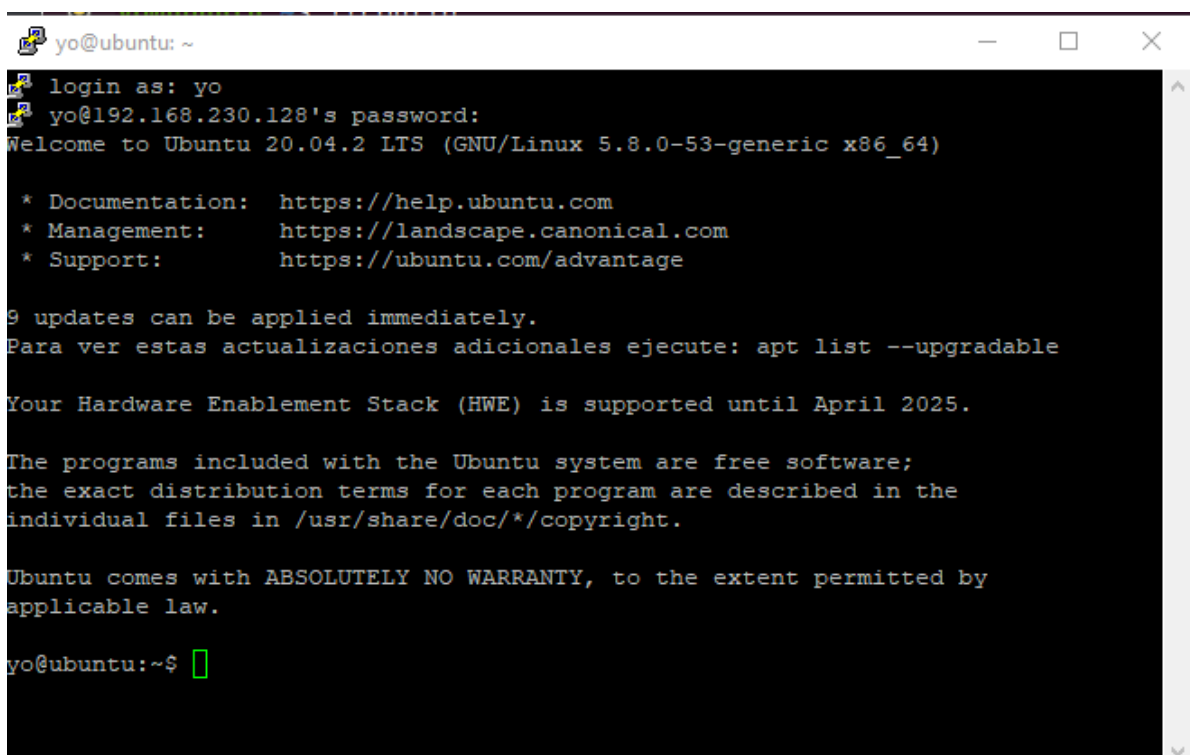


### Actividad 3. Conexión con la RED

Ejecutamos **putty.exe** y ponemos la dirección IP de la máquina virtual Ubuntu. Hacer clic sobre "Open" para establecer la conexión.



En la ventana que aparecerá, introducir usuario y clave de Ubuntu, y luego podemos probar comandos de Linux:



### Actividad 3. Conexión con la RED

Probamos algún comando de Linux:

```
yo@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.230.128 netmask 255.255.255.0 broadcast 192.168.230.255
    inet6 fe80::2b83:6f4a:f84f:8997 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:1c:e1:43 txqueuelen 1000 (Ethernet)
    RX packets 1950 bytes 1579150 (1.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 936 bytes 94677 (94.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Bucle local)
    RX packets 210 bytes 18102 (18.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 210 bytes 18102 (18.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

yo@ubuntu:~$
```

Podemos visualizar la sesión SSH en Ubuntu:

Insertamos el comando **netstat -a | grep ssh** :

```
yo@ubuntu:~$ netstat -a | grep ssh
tcp        0      0 ubuntu:ssh                192.168.230.1:58822      ESTABLECIDO
yo@ubuntu:~$
```

Hacemos logout en la conexión de SSH de putty y de esta forma ya solo se quedaría en escucha, pero se cerraría la conexión.

### Requerimiento 2

Te proponemos practicar con el cifrado asimétrico de la información. Para ello, primero debes contar con el entregable de la actividad 2 (será un fichero “pdf”) y el objetivo es volver a enviarlo a tu profesor, pero cifrado.

#### TAREAS:

1. Instalación de Gpg4Win en tu MV Windows 10
2. Generación de una pareja de claves (privada y pública) personales tuyas.
3. Exportación de tu clave pública y almacenamiento en un servidor externo en Internet (así cualquiera podrá verificar los documentos que firmes)
4. Cifrado del documento entregable de tu práctica AI4 con la clave pública de tu profesor. Para esto primero tendrás que bajártela desde un servidor externo y luego importarla en tu sistema de claves.
5. Envío a tu profesor (por el medio acostumbrado) del documento cifrado que él podrá ver con su clave privada.

En la práctica, aplicaremos un algoritmo sobre la información a transmitir (en este caso el PDF entregable) utilizando unas claves, de esta forma solamente el conocedor del proceso inverso puede descryptar lo recibido y entender el mensaje, asegurándonos que la información no se ha alterado durante el proceso.

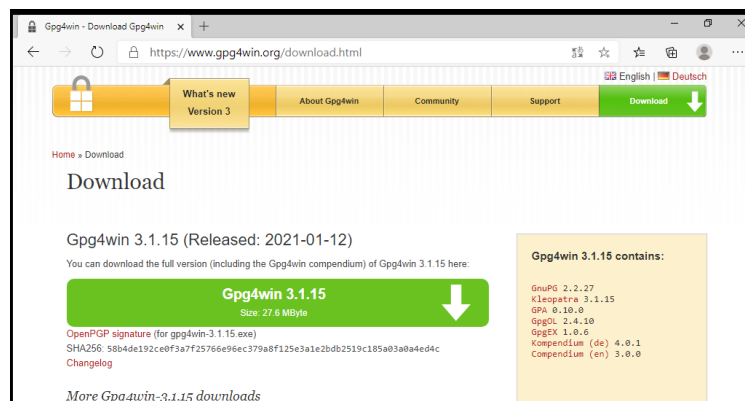
Existen diferentes sistemas de criptografía:

- Simétrica: utilizan la misma clave para encriptar y descryptar la información
- Asimétrica: utilizan dos claves (*pública* - que se puede enviar y ser conocida por cualquiera – y *privada* - que se guarda con seguridad y no se transmite ni publica-).
- Híbrida: utiliza ambos sistemas beneficiándose de los dos anteriores, utilizando un sistema de cifrado asimétrico para intercambiar de forma segura una clave (simétrica) que luego será usada para encriptar la información útil a transmitir.

En el ejemplo utilizaremos claves asimétricas, para ello debemos distinguir dos procesos: generación de claves (privada y pública) y el encriptado y descryptado de la información.

#### 1. Instalación de Gpg4Win en tu MV Windows 10

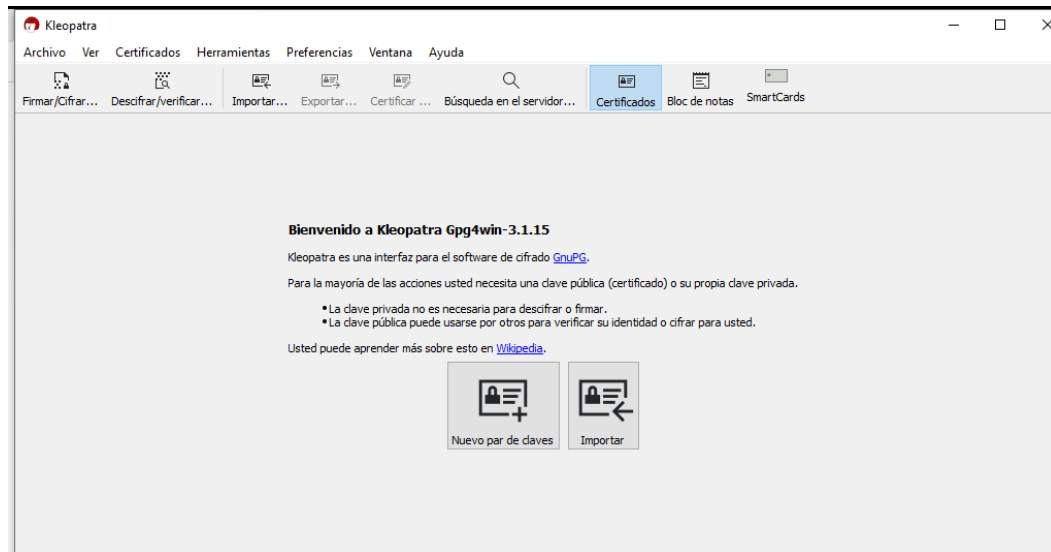
**Gpg4Win** es un paquete de cifrado de correo electrónico y archivos para Microsoft Windows, que utiliza criptografía de clave pública GnuPG (GNU Privacy Guard) para el cifrado de datos y firmas digitales. Descargamos e instalamos el software en nuestra MV Windows 10.



## Actividad 3. Conexión con la RED

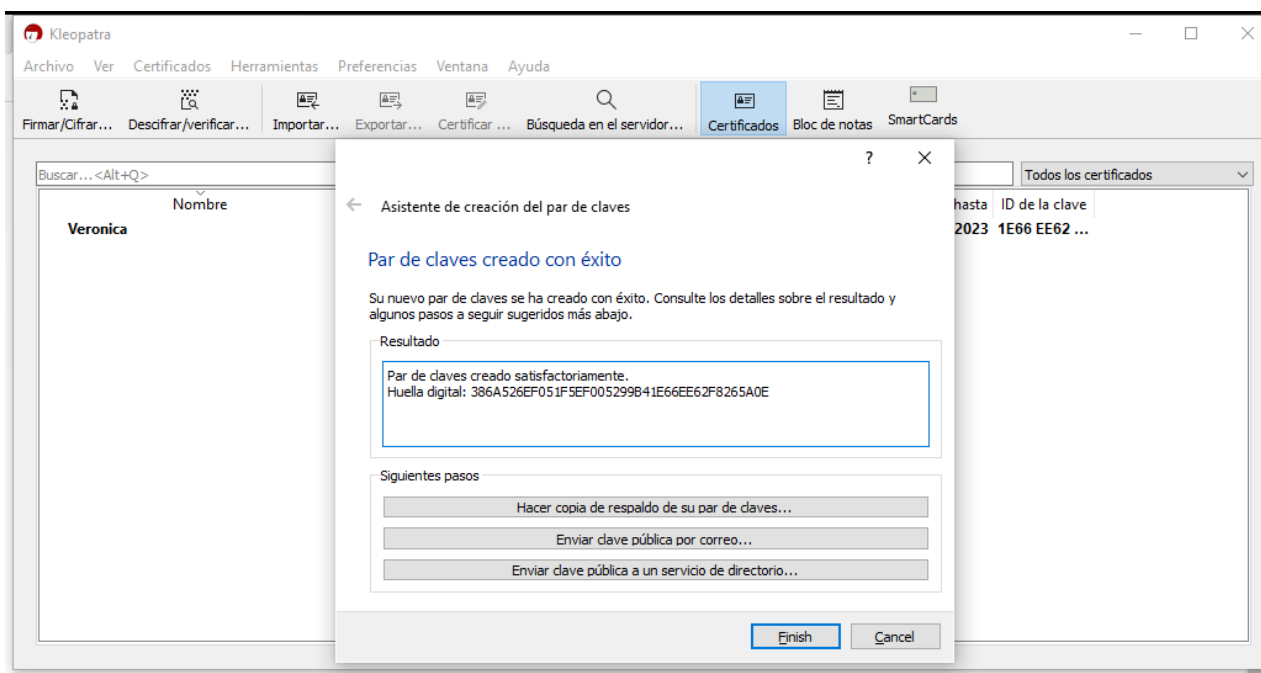
### 2. Generación de una pareja de claves (privada y pública) personales tuyas.

Después de instalar Gpg4Win ejecutamos Kleopatra ( gestor de claves por defecto para GnuPG) . Dado que es la primera vez que lo ejecutamos nos pide generar un nuevo par de claves:

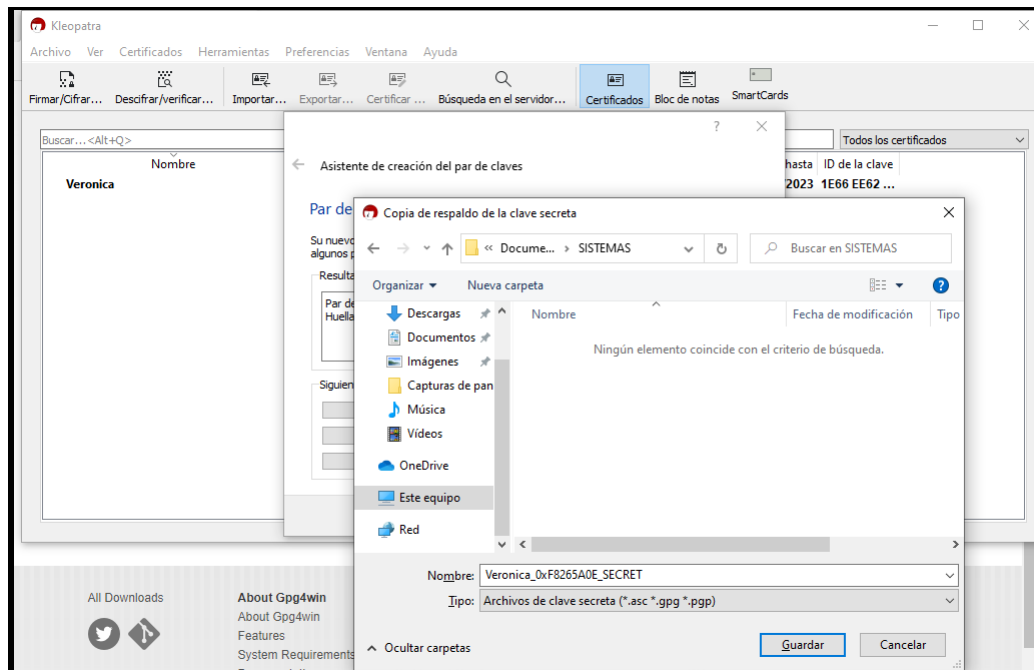


Nos pedirá un nombre de usuario y un correo, y la clave se configurará por defecto (si quisiéramos cambiar estas configuraciones podemos hacerlo desde Configuración avanzada).

Finalmente generará nuestro par de claves, la huella digital es el identificador de la clave, hacemos una copia de respaldo de nuestro par de claves.



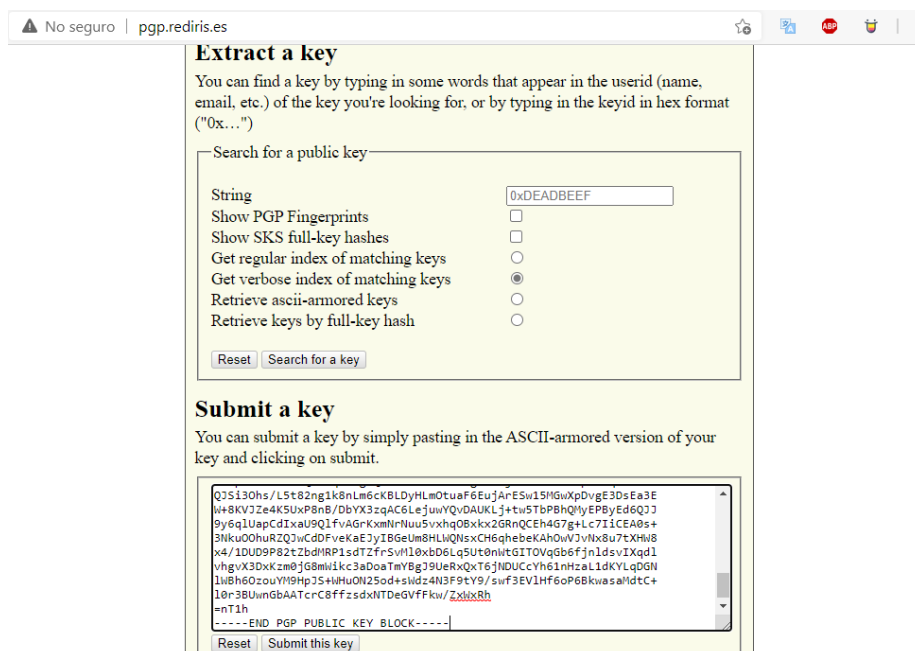
## Actividad 3. Conexión con la RED



Nos da la opción de hacer una copia de la clave privada. Y posteriormente en la pestaña de exportar podemos guardar la clave pública.

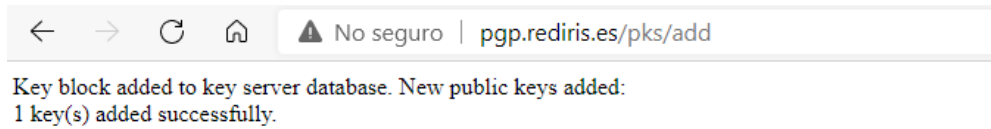
### 3. Exportación de tu clave pública y almacenamiento en un servidor externo en Internet (así cualquiera podrá verificar los documentos que firmes)

- La subimos al servidor RedIRIS, para lo cual pegamos el código ASCII que encontramos al abrir el fichero en algún editor que reconozca la extensión .asc



Nos dice que la clave ha sido añadida al servidor.

### Actividad 3. Conexión con la RED



Si la buscamos por el nombre, nos encuentra.



Si buscamos la clave del profesor como en el ejemplo:

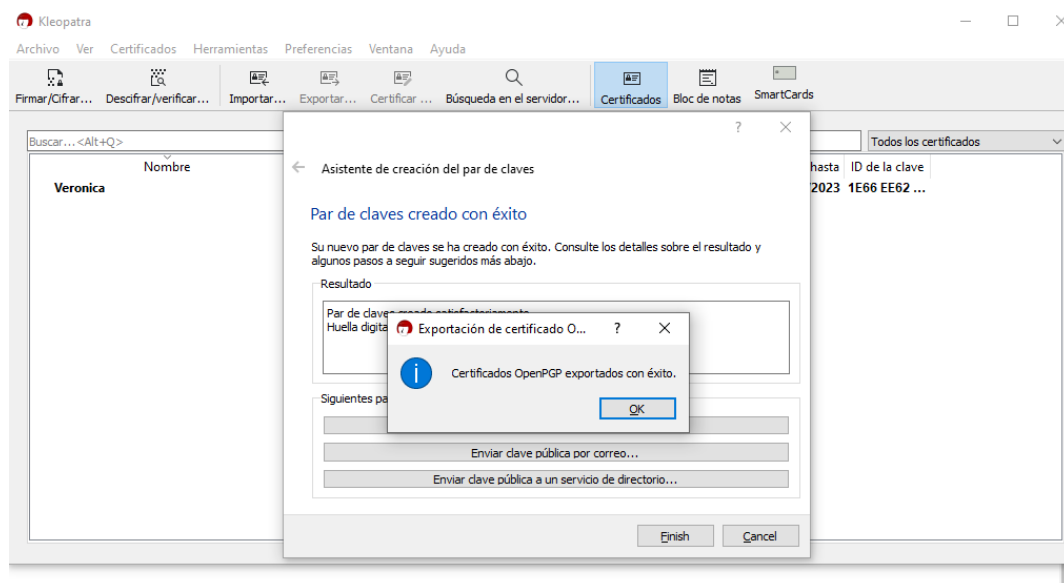
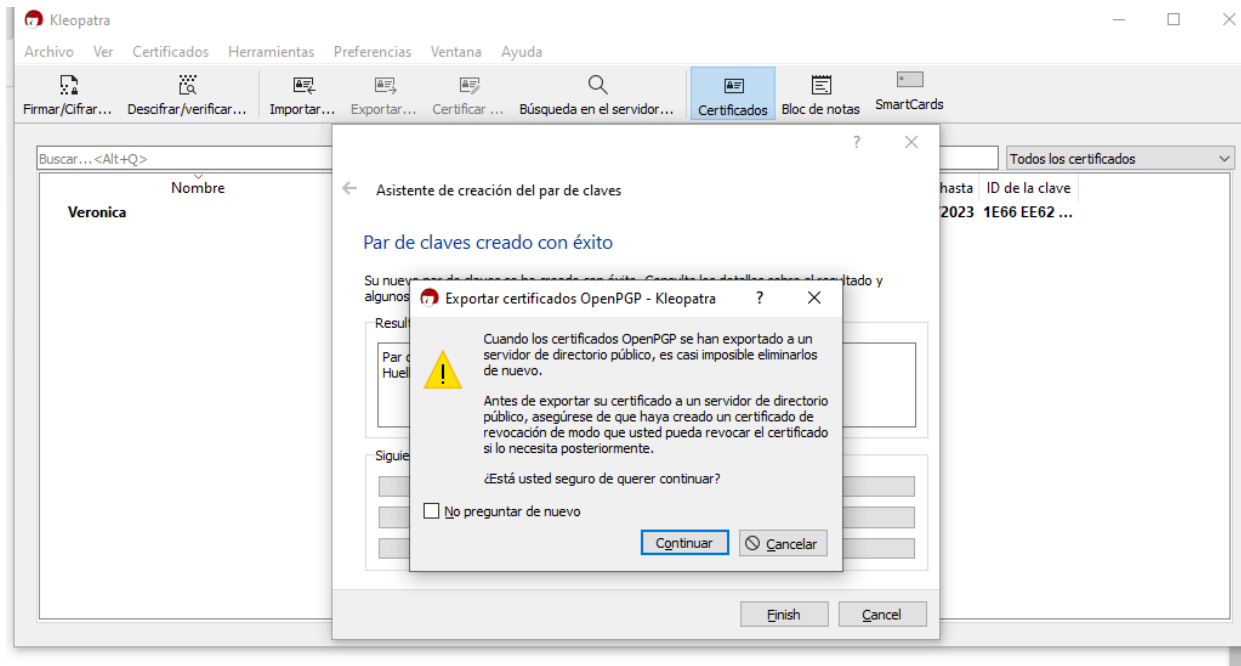
### Search results for 'profesor mp0483'

Type	bits/keyID	cr. time	exp time	key expir
pub	2048R/709FD261	2018-05-07		
uid	Profesor MP0483 <mp0483.sistemasinformaticos@gmail.com>			
sig	sig3 709FD261	2018-05-07		[selfsig]
sig	sig 0988C841	2018-05-31		Alejandro GC DAM <alexuca@hotmail.es>
sig	sig E301A97A	2018-06-06		Jose Luis <jositoyomismo@hotmail.com>
sig	sig E301A97A	2018-06-06		Jose Luis <jositoyomismo@hotmail.com>
sub	2048R/45A9FE99	2018-05-07		
sig	sbind 709FD261	2018-05-07		[.]



### Actividad 3. Conexión con la RED

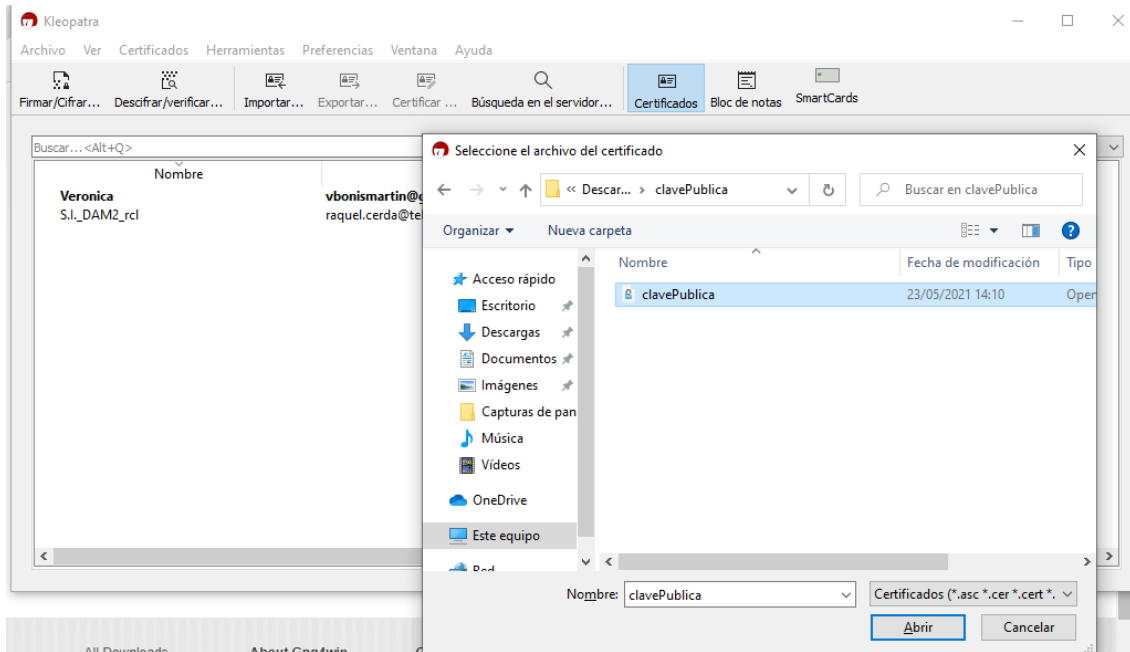
Con Kleopatra también podemos subir la clave pública a un servidor externo en Internet, con Kleopatra es sencillo y podemos usar la opción “Enviar clave pública a un servicio de directorio”. (ignoramos el mensaje sobre el certificado de revocación porque este se crea automáticamente en el proceso anterior).



### Actividad 3. Conexión con la RED

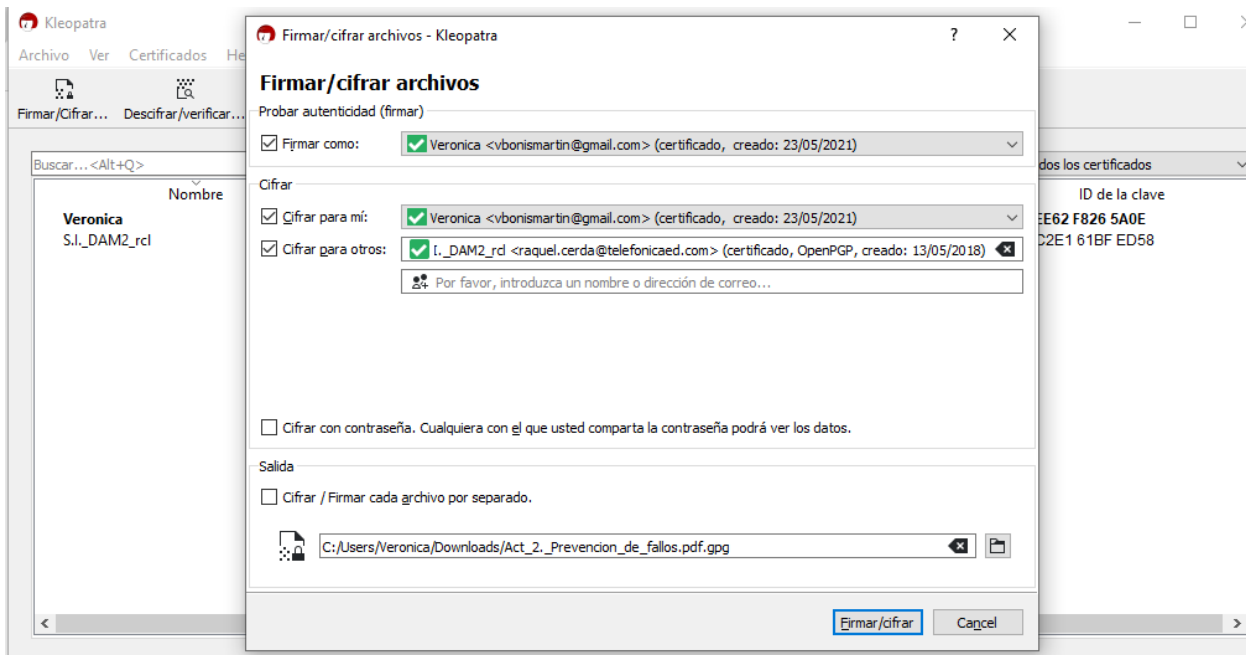
4. Cifrado del documento entregable de tu práctica AI4 con la clave pública de tu profesor. Para esto primero tendrás que bajártela desde un servidor externo y luego importarla en tu sistema de claves.

Se nos proporciona una clave pública desde un archivo externo (.zip). Importamos este archivo en Kleopatra



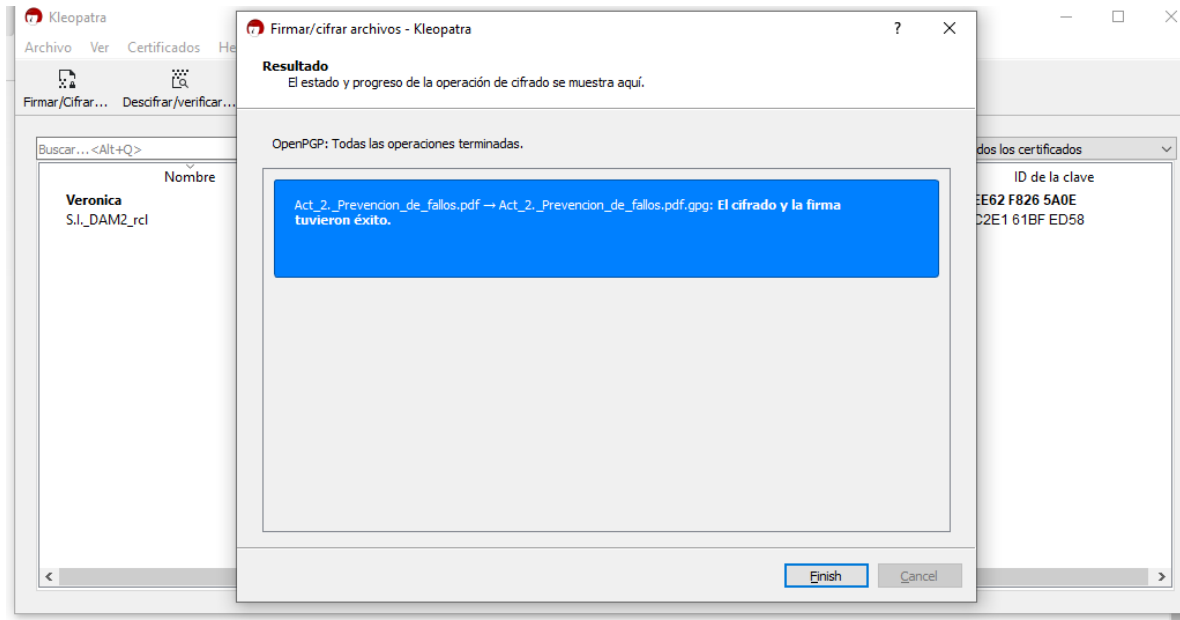
Una vez añadido podemos indicar que es de confianza (certificar la validez de las claves al importarla), y a continuación podemos cifrar cualquier archivo usando la opción Firmar/ Cifrar.

Elegimos el archivo que queremos cifrar (en este caso Act\_2.\_Prevencion\_de\_fallos.pdf) y elegimos la clave pública que acabamos de importar.



### Actividad 3. Conexión con la RED

Se nos genera un archivo \*.gpg que el destinatario podrá descryptar y visualizar con su clave.



#### Instalación de Kleopatra y creación de par de claves desde el entorno Ubuntu

La forma tanto de la instalación como de la creación de las claves desde el entorno Linux es muy parecido a Windows, para ello nos situamos en la terminal e instalamos el paquete de Kleopatra:

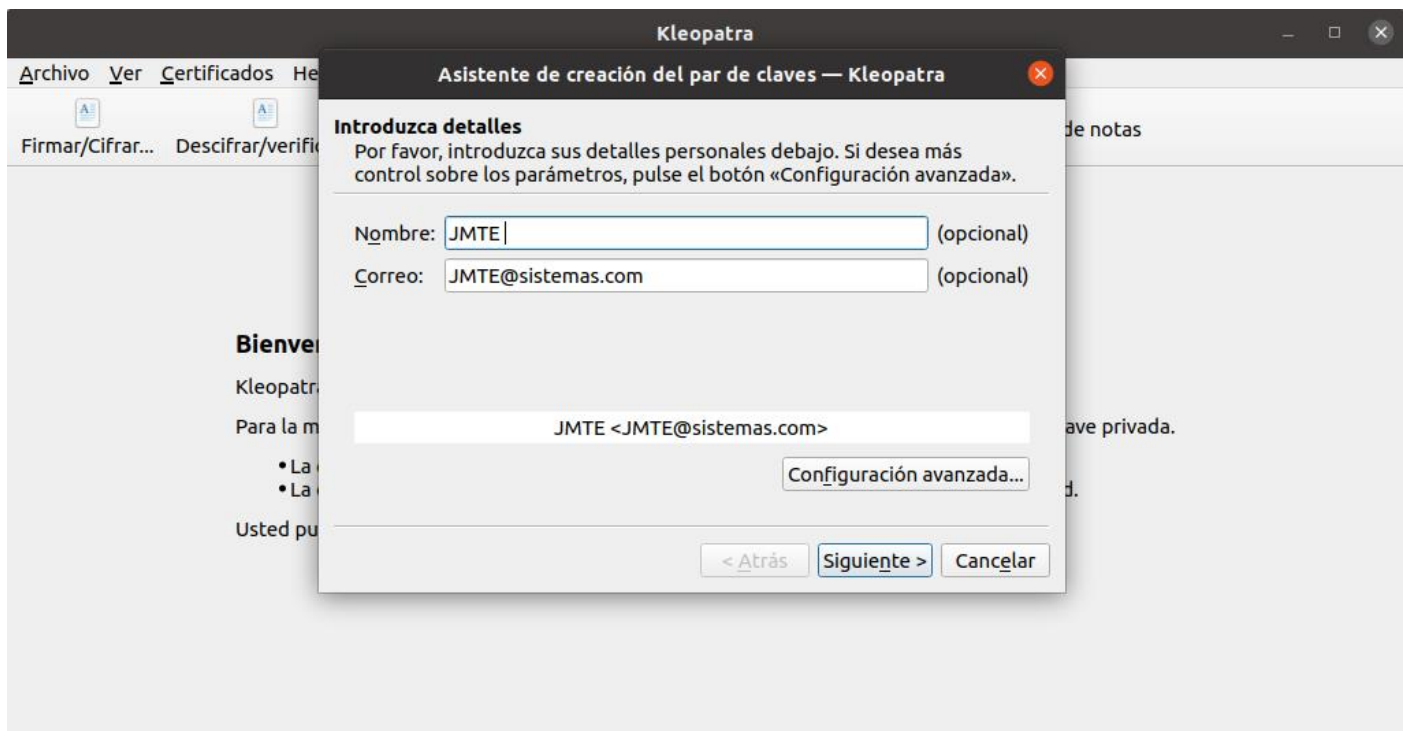
```
jnte@jnte-DELL:~$ sudo apt-get update
Ign:1 http://ppa.launchpad.net/webupd8team/sublime-text-3/ubuntu focal InRelease
Err:2 http://ppa.launchpad.net/webupd8team/sublime-text-3/ubuntu focal Release
  404 Not Found [IP: 91.189.95.85 80]
Obj:3 http://packages.microsoft.com/repos/code stable InRelease
Obj:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Obj:5 http://es.archive.ubuntu.com/ubuntu focal InRelease
Obj:6 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease
Obj:7 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease
Obj:8 https://download.sublimetext.com apt/stable/ InRelease
Leyendo lista de paquetes... Hecho
E: El repositorio «http://ppa.launchpad.net/webupd8team/sublime-text-3/ubuntu fo
cal Release» no tiene un fichero de Publicación.
N: No se puede actualizar de un repositorio como este de forma segura y por tant
o está deshabilitado por omisión.
N: Vea la página de manual apt-secure(8) para los detalles sobre la creación de
repositorios y la configuración de usuarios.
jnte@jnte-DELL:~$ sudo apt install kleopatra
```

### Actividad 3. Conexión con la RED

Cuando termina, ya podremos buscar el programa en la lista y lo ejecutaremos:

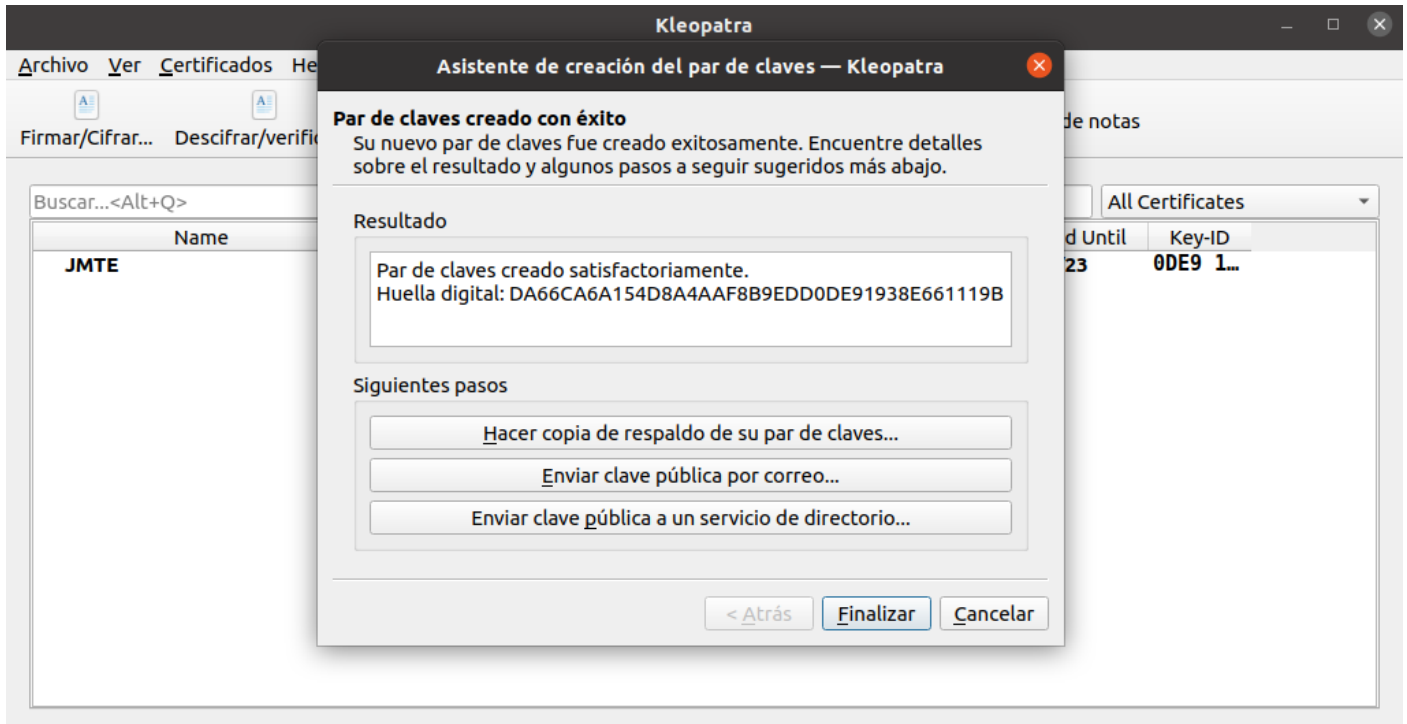


En este momento ya podemos crear nuestro primer par de claves:

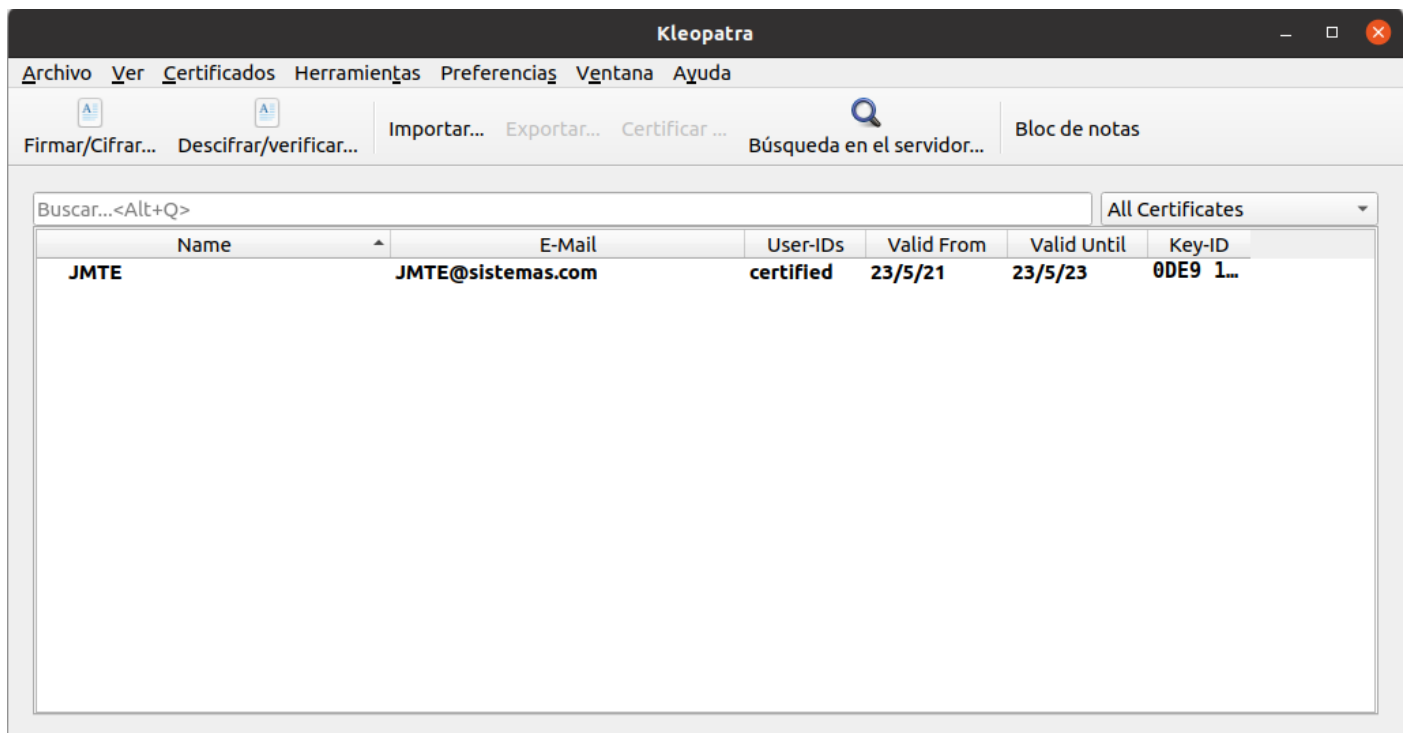


A la hora de escribir el nombre, a veces, da error y hay que introducir un espacio. Cuando se le da a siguiente nos va a pedir una frase de seguridad la cual será necesaria para hacer copia de seguridad de las llaves (En el entorno Windows con Kleopatra esto no es necesario).

### Actividad 3. Conexión con la RED



En esta pantalla es donde podemos elegir qué tipo de copia realizar, al elegir una, debemos de introducir la contraseña que configuramos anteriormente.



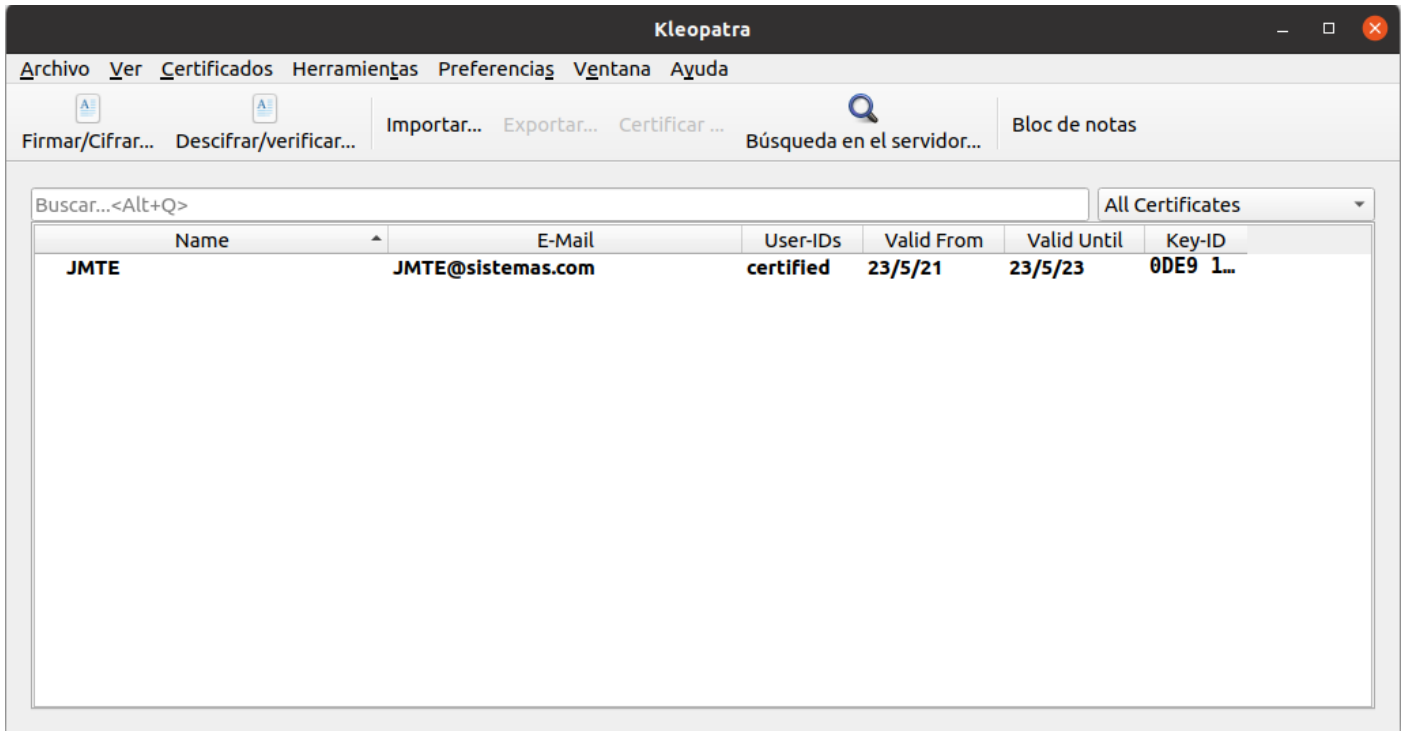
Ya tendríamos nuestro par de claves creada.

### Actividad 3. Conexión con la RED

Para finalizar, debemos de encriptar el documento .pdf que entregamos en la Actividad 2 con la clave que nos facilitan y que se encuentra en el foro de la asignatura. La descargamos en archivo .zip y la se descomprime para después seleccionarla.

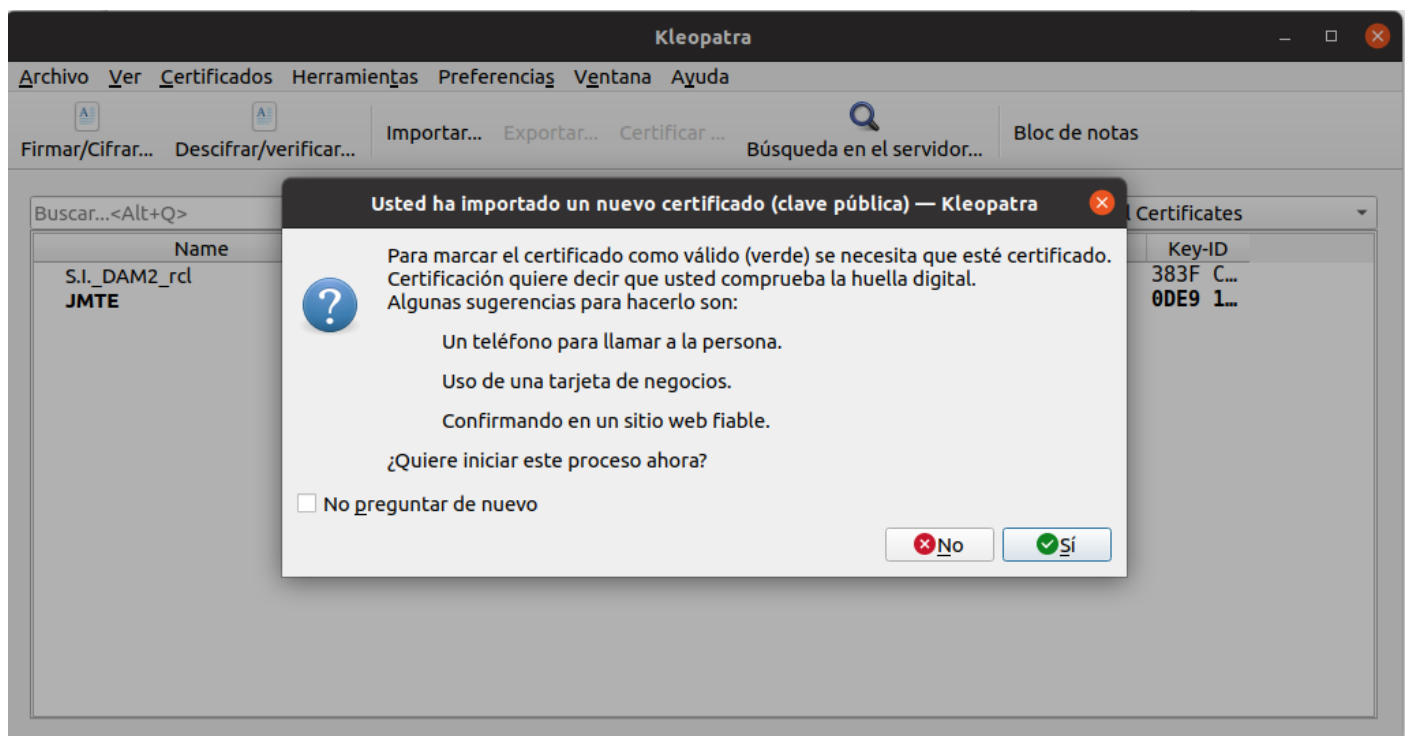
El proceso a llevar a cabo es el siguiente:

Seleccionamos la opción importar para tener nuestro certificado facilitado en Kleopatra:



**SELECCIONAR: IMPORTAR**

A continuación, seleccionamos la clave pública proporcionada y le damos que si a la certificación:

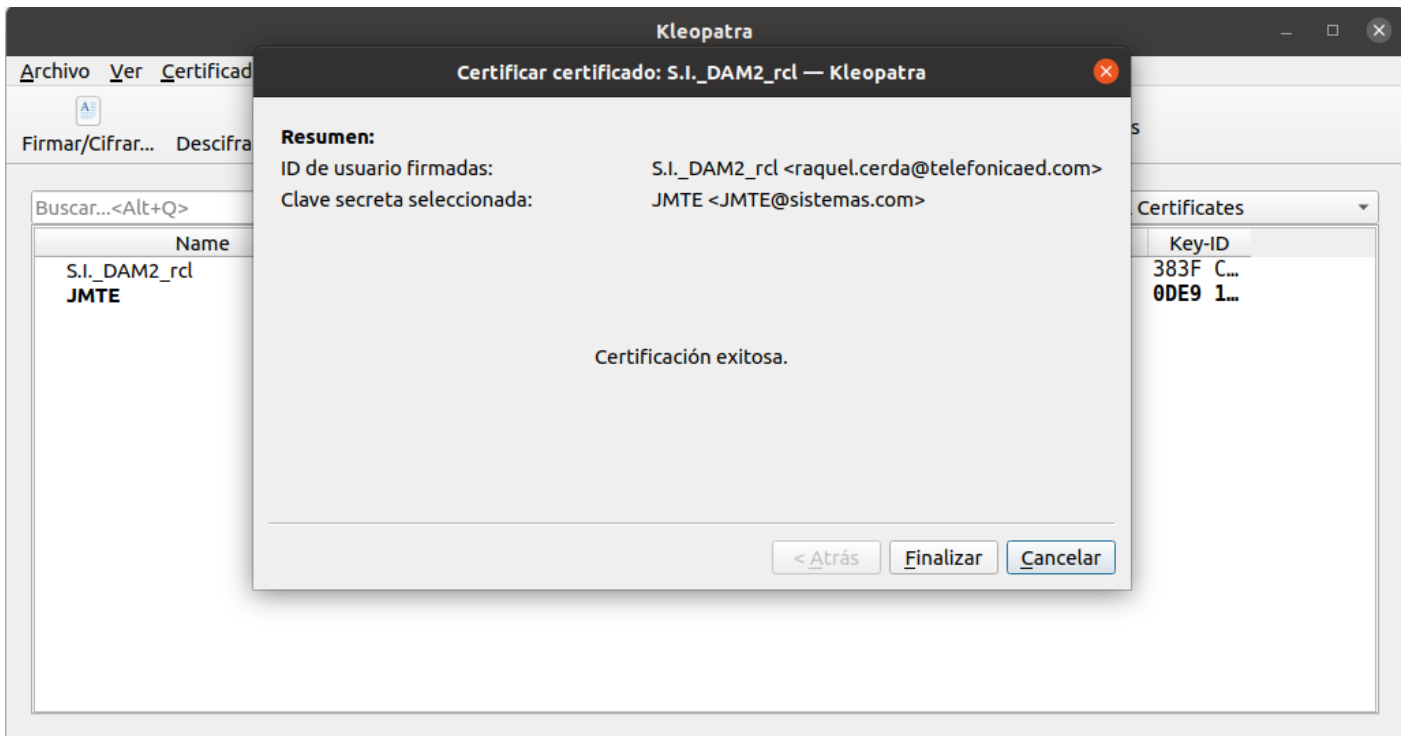


### Actividad 3. Conexión con la RED

Marcamos la opción que tenemos indicando que la clave proporcionada es válida:

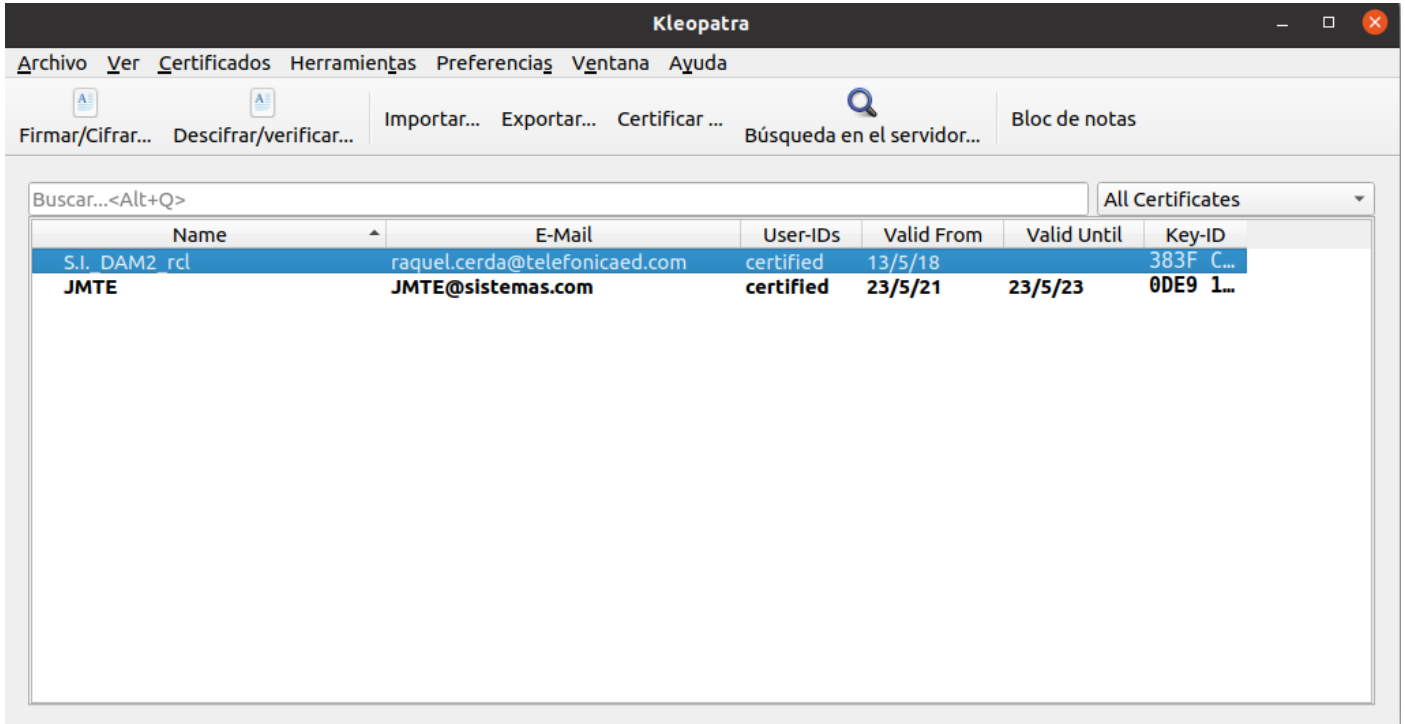


Y ya se nos indica que ha concluido con éxito:

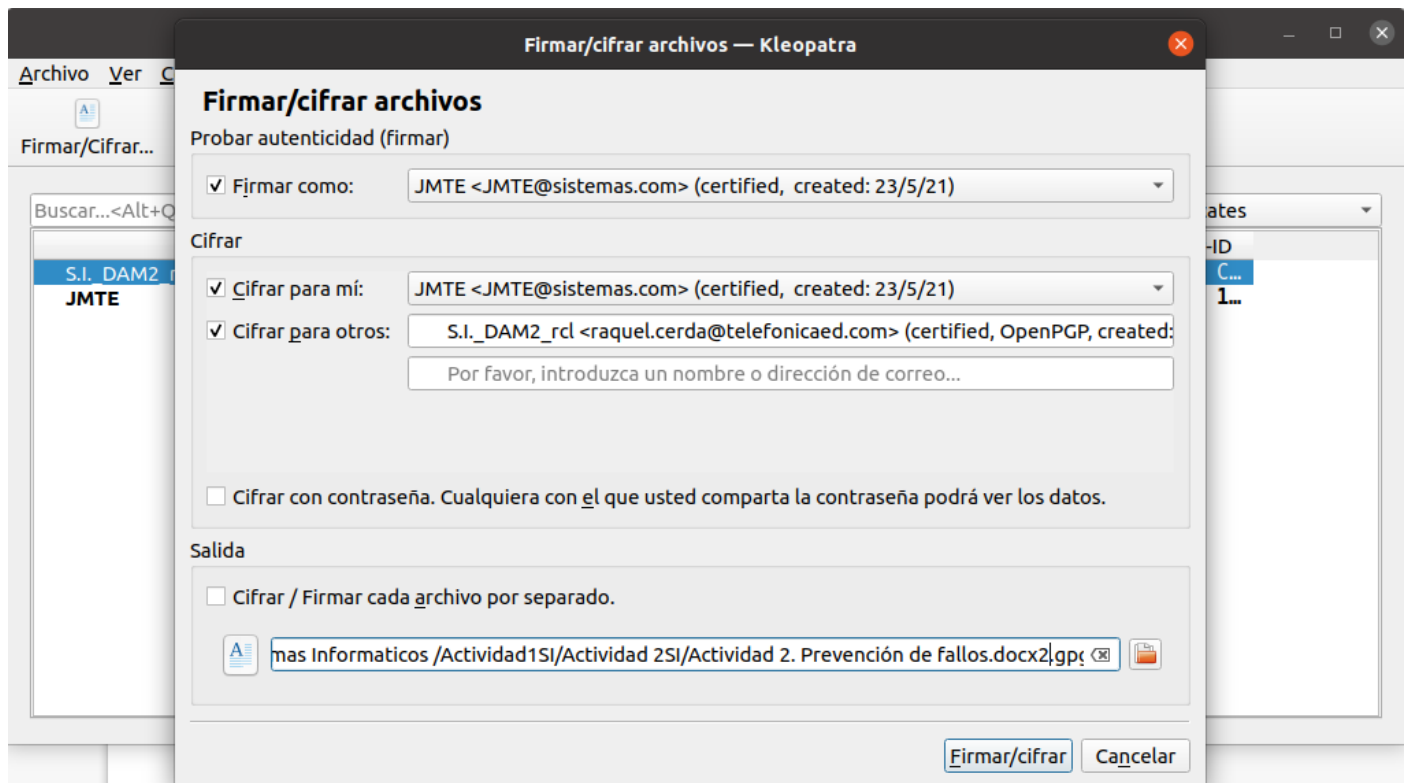


### Actividad 3. Conexión con la RED

Ahora que ya disponemos de las claves para cifrar nuestro documento, procedemos a realizar este apartado, para ello, hacemos click en firmar/cifrar:



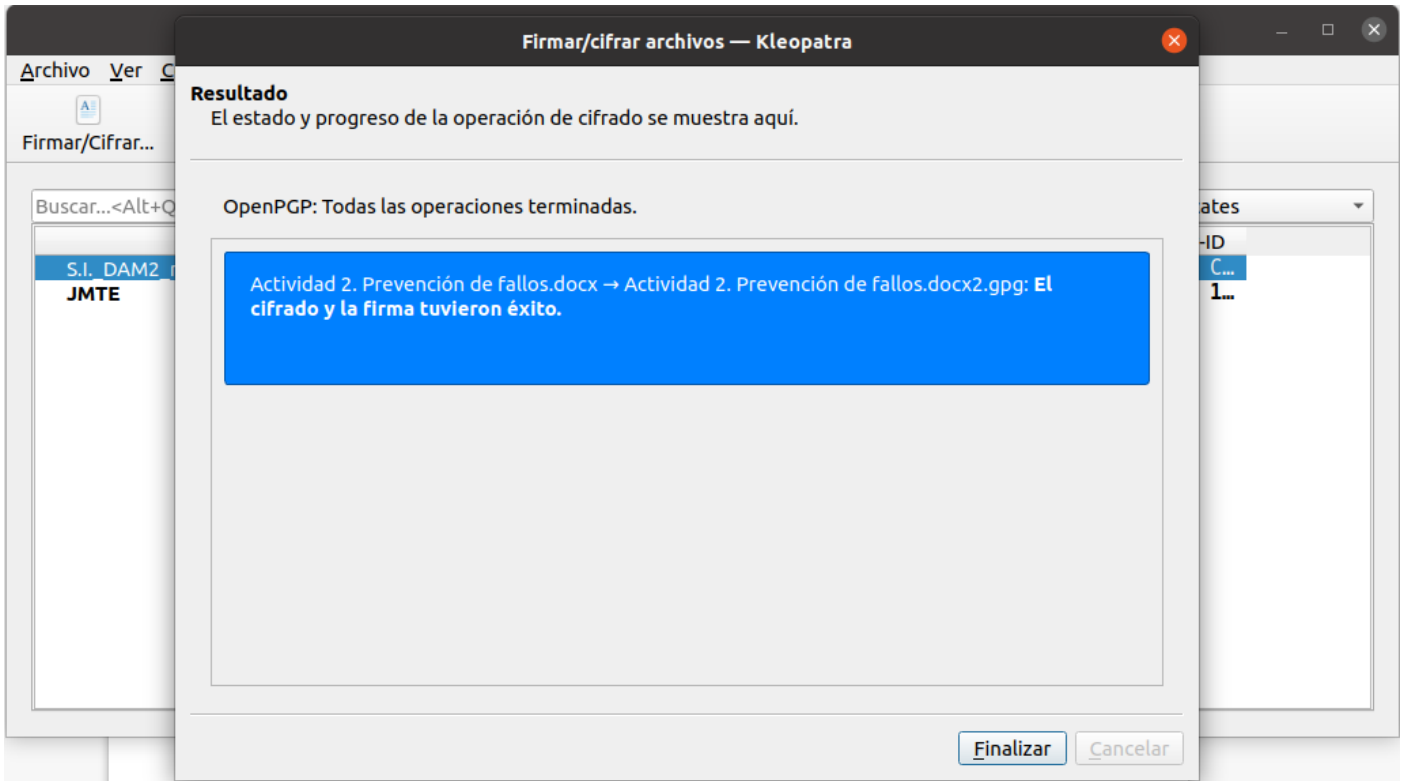
Y elegimos IMPORTANTE en cifrar para otros la clave que se nos ha facilitado, si no lo hacemos, este archivo será indescifrable para la persona que se lo enviemos y tenga su clave proporcionada.





### Actividad 3. Conexión con la RED

De esta manera habremos cifrado el documento de manera exitosa para que la persona que nos ha facilitado las claves pueda descifrarlo mediante ellas.



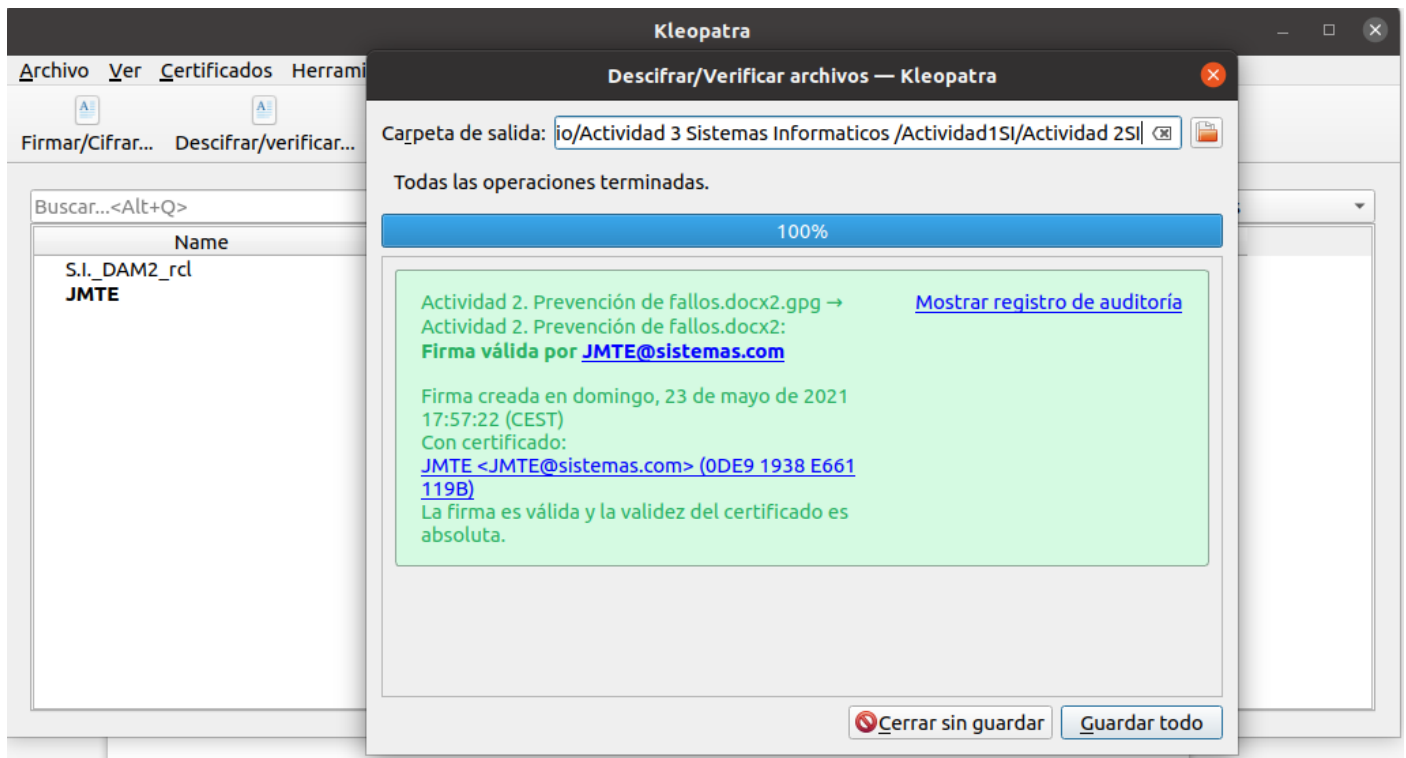
Si otra persona intenta abrir el archivo sin las claves, este será el resultado obtenido:



### Actividad 3. Conexión con la RED

Cuando la persona con las claves recibe el archivo, la forma de descifrarlo será la siguiente:

Se pulsaría en Descifrar/verificar y como tenemos nuestras claves creadas, nos desbloquearía el archivo pudiendo guardar el mismo haciendo click en Guardar todo.



Al final se puede observar que la forma de realizarlo tanto en entorno Windows como en entorno Linux es muy parecido ya que Kleopatra utiliza el mismo entorno gráfico.