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 separador con un punto, cada bit tiene un valor decimal exacto. El valor más alto seria 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.*

**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 |

|  |
| --- |
| 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 |

|  |
| --- |
| 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 |

|  |
| --- |
| 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 |

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

**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.

**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 2¹⁷= 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 2²⁰ = 1048576 - 2 = **1048574** Subredes que se pueden crear.

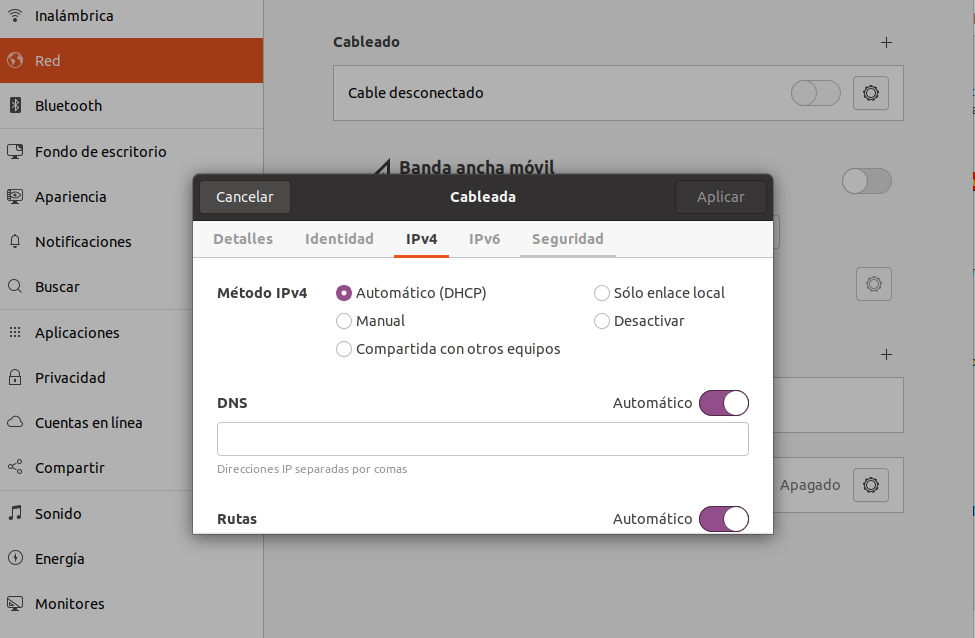
La subred 255.255.255.240 puede direccionar hasta **16** hosts.

**Configuración IP**

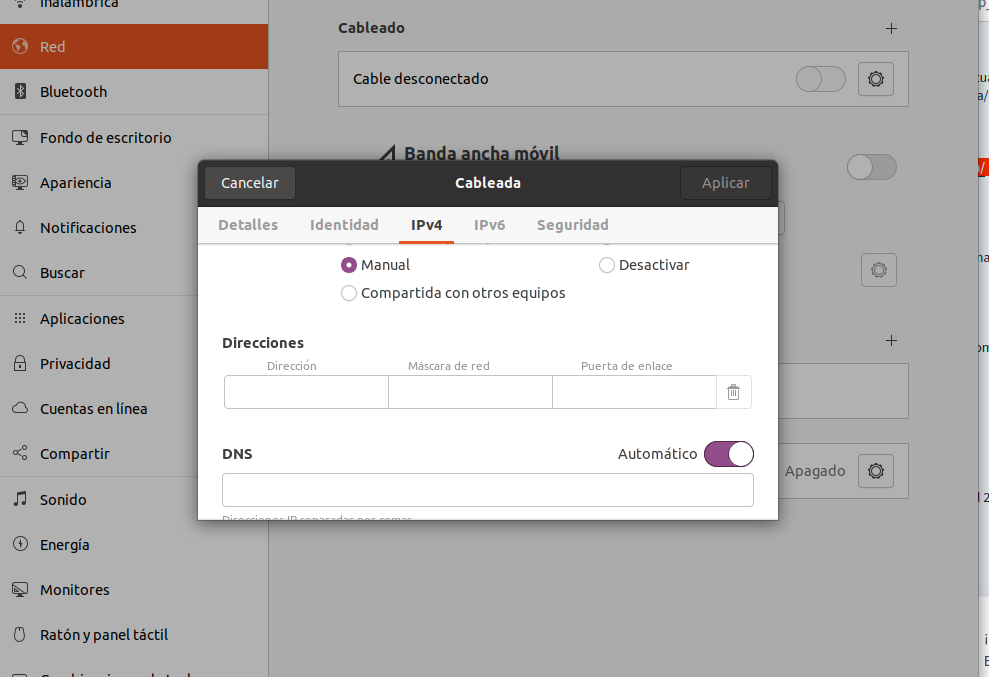
**Averigua la dirección IP (estática o dinámica) de tu ordenador personal, de tu máquina virtual de Windows10 y de tu máquina virtual Ubuntu. En la respuesta puedes copiar las pantallas/ventanas de cada sistema, pero incluye también la visualización utilizando comandos de consola/terminal.**

***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.

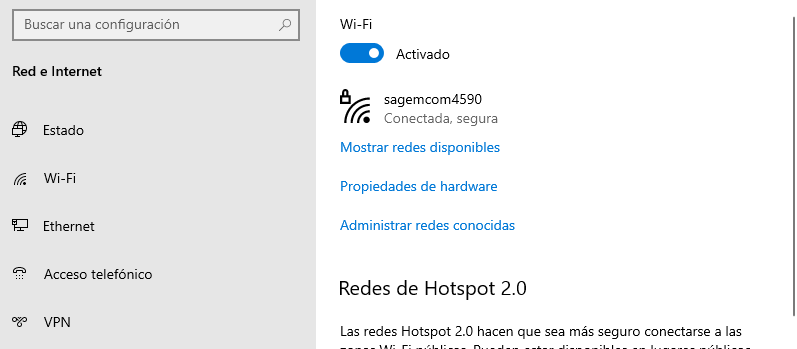


Si quisiéramos establecer una ip estática, tendríamos que escoger la opción Manual y rellenar los campos de la ip:

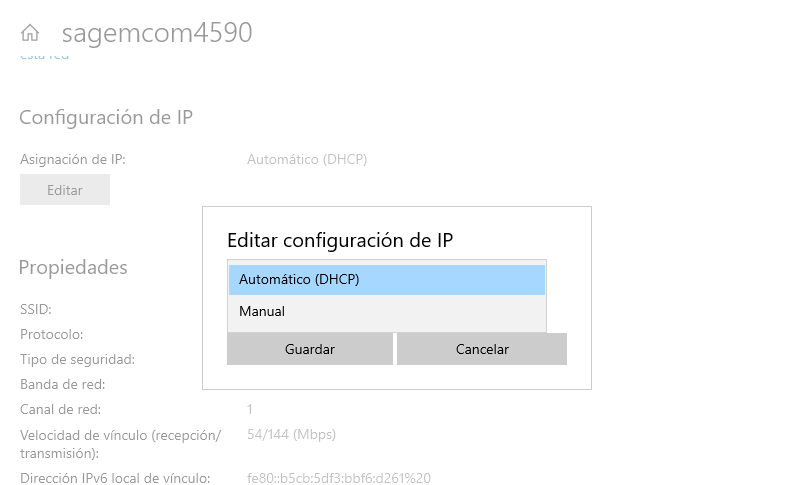


**En el caso de Windows**, la forma de averiguar si tenemos una ip estática o dinámica es muy similar a Linux, tendríamos que ir a:

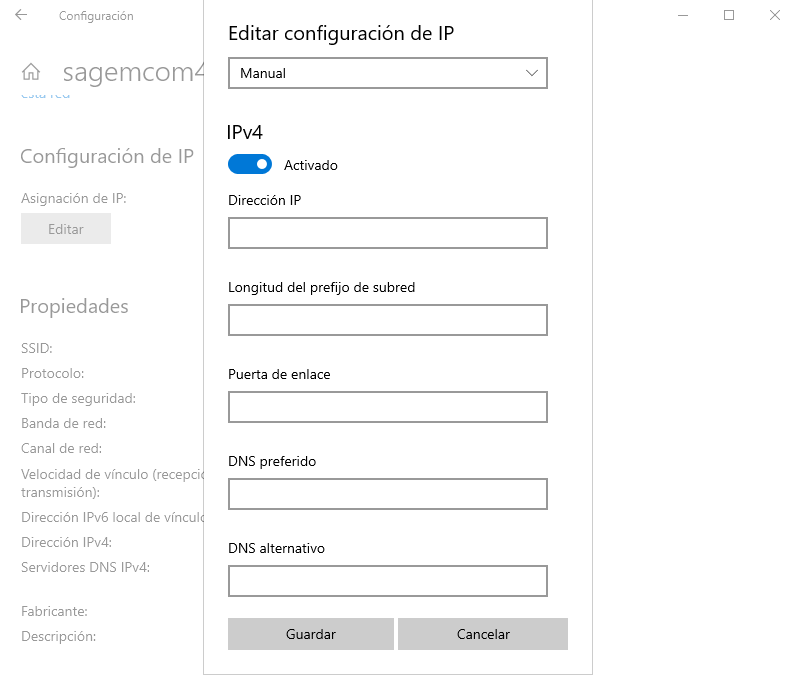
Configuración y en la parte de Red haríamos click en el apartado de nuestro Router o Modem:



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

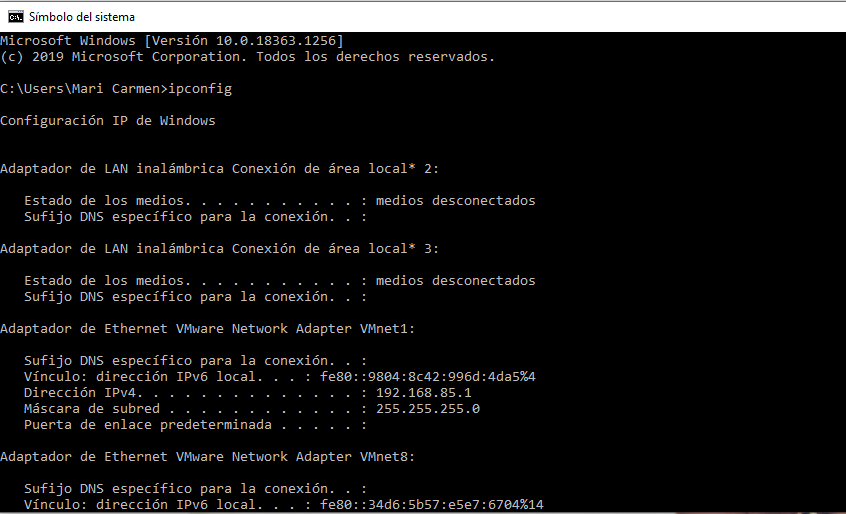


Si queremos cambiarla a fija o estática, en el desplegable, hacemos click en Manual y ahí introducimos los parámetros de nuestra IP fija:

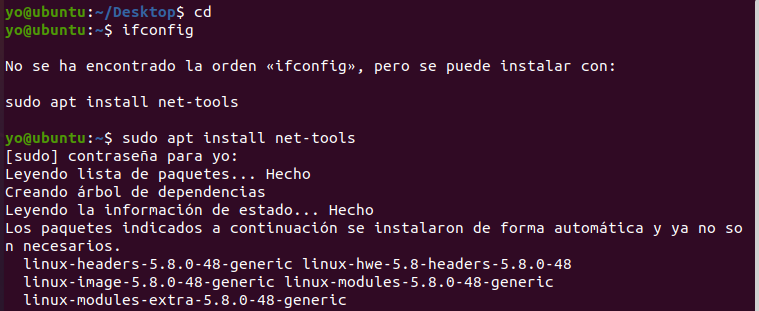


***VISUALIZACIÓN MEDIANTE COMANDOS***

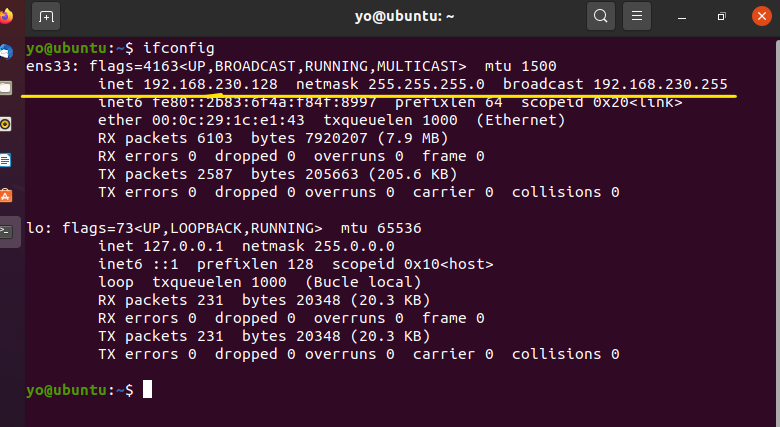
En Windows podemos activar la consola con cmd y con el comando ipconfig podemos ver la información de nuestra configuración del protocolo TCP/IP de nuestro ordenador personal.



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



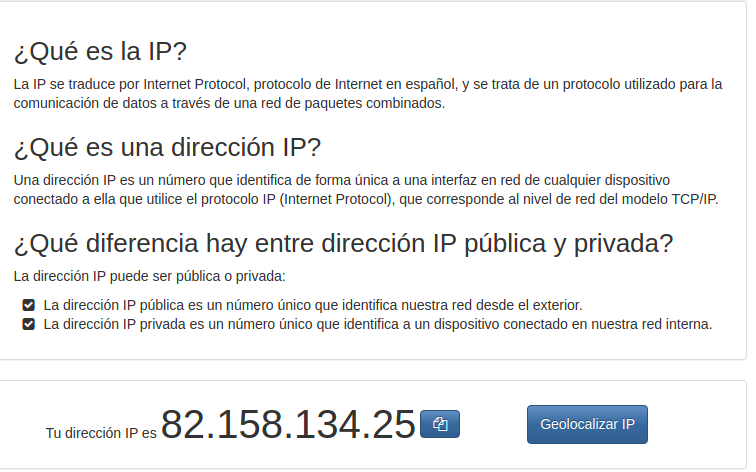
Después de instalarla, ya podemos acceder a la información de la ip a través del comando ifconfig:

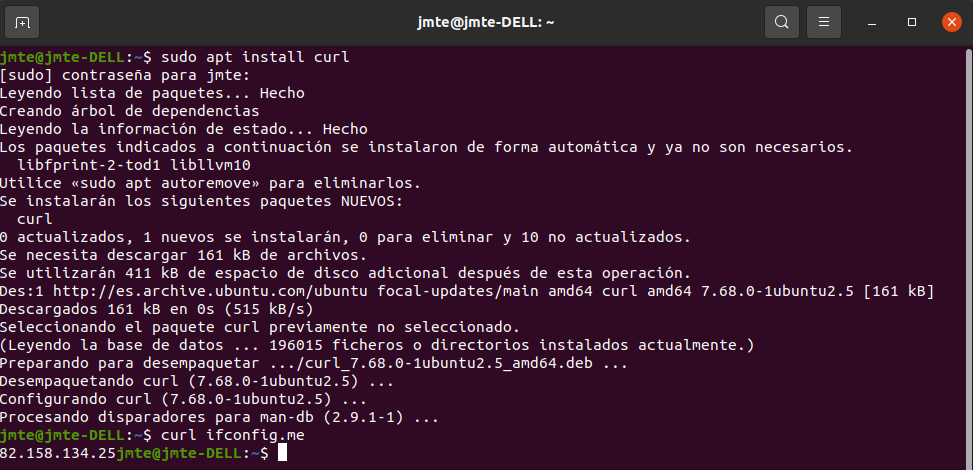


**Conexión con Internet**

**Averigua también la dirección IP pública de tu conexión a Internet. Puedes usar por ejemplo la página**[**http://www.cualesmiip.com/**](http://www.cualesmiip.com/)**o cualquier otra similar.**

Mediante la página web cualesmiip es muy fácil y rápido saber cuál es nuestra ip:

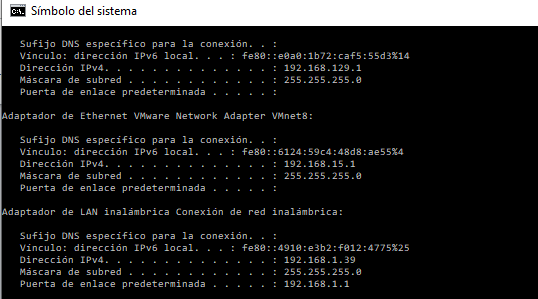


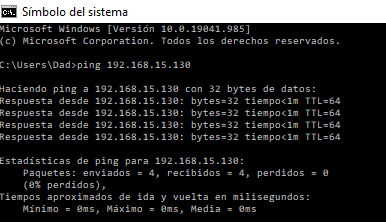
Existe una forma de averiguar tu ip pública mediante comandos en linux que es instalando un paquete llamado curl, se haría de la siguiente forma:

**Practicar con “ping”**

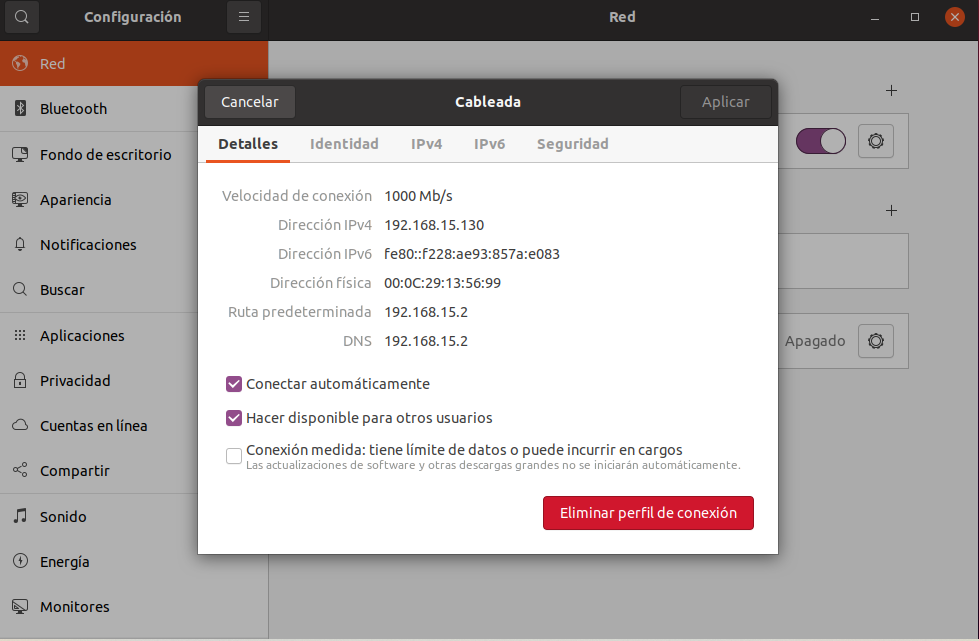
**Realiza el ejercicio propuesto en el módulo 5.2 con el comando “ping” y comprueba la conexión entre tu máquina física y tus máquinas virtuales. Si tu ordenador lo soporta comprueba también la conexión entre ellas, y si no solamente de cada una con la máquina física.**

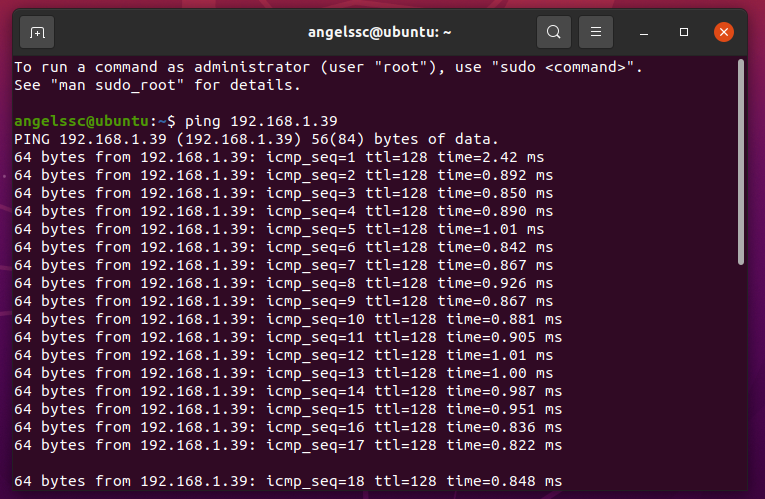
Lanzamos Ping desde nuestro ordenador personal (IP 192.168.1.39) a nuestra máquina virtual Ubuntu con IP 192.168.15.130





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





**Conexión SSH Windows-Ubuntu**

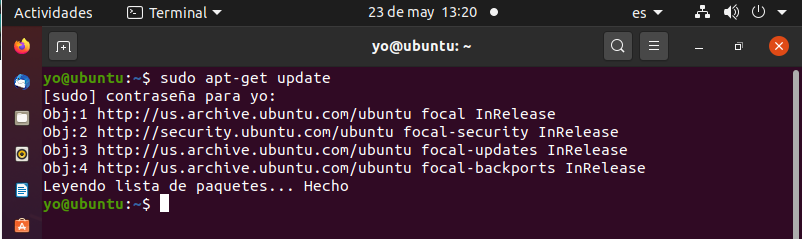
**Realiza el ejercicio práctico propuesto en la lección 5.3 Seguridad en la red siguiendo los pasos que en él se indican. Aporta como resultado los pantallazos de tus máquinas virtuales.**

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

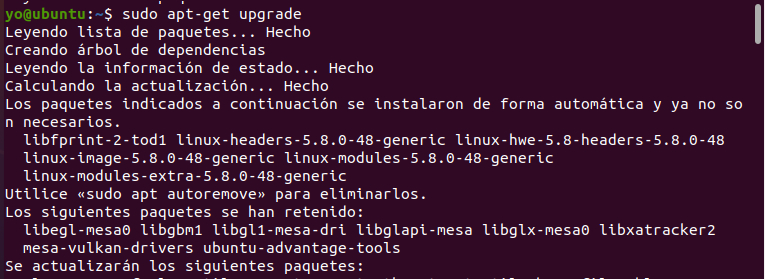
Para hacerlo utilizaremos nuestro sistema anfitrión y nuestra máquina virtual Linux Ubuntu. Como en toda conexión de este tipo necesitaremos un "cliente SSH" (lo usaremos sobre Windows) y un "servidor SSH" (en este caso sobre Ubuntu). Ambos, cliente y servidor, no suelen estar preinstalados en los sistemas,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

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

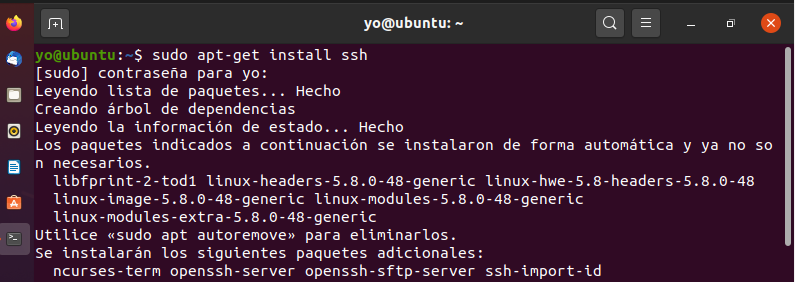
***sudo apt-get update***



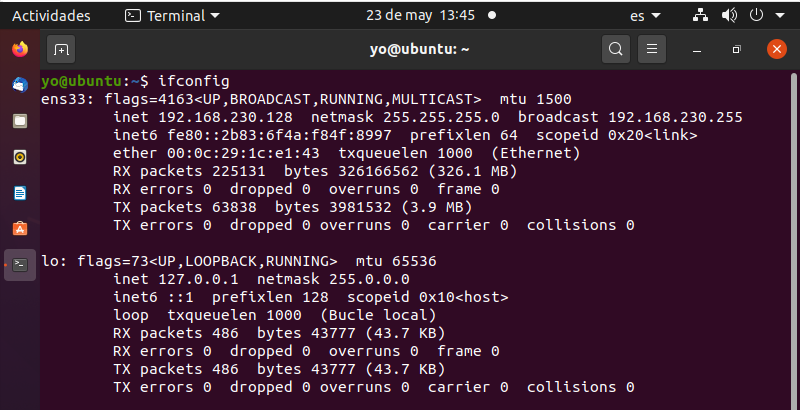
***sudo apt-get upgrade***



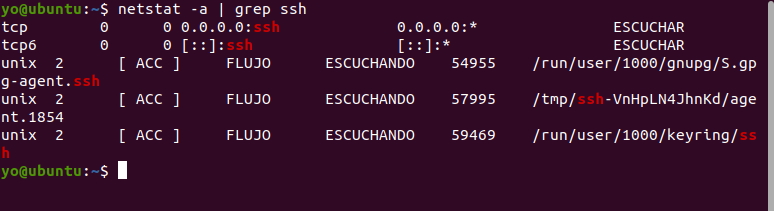
***sudo apt-get install ssh*** (con esto instalamos el servidor SSH).



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

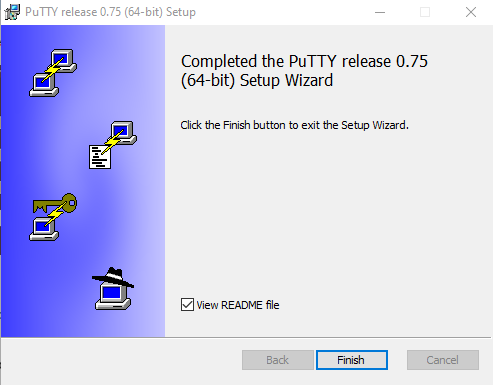


***netstat –a | grep ssh*** (comprobamos que SSH está activo y escuchando).

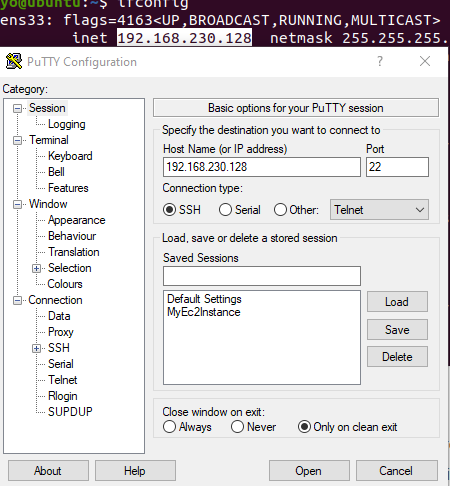


### Ahora en nuestro sistema anfitrión Windows:

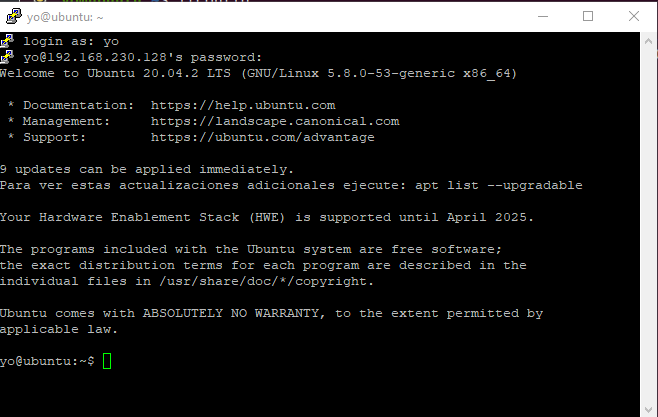
Descargamos la aplicación “**putty.exe**” desde <https://www.putty.org/>



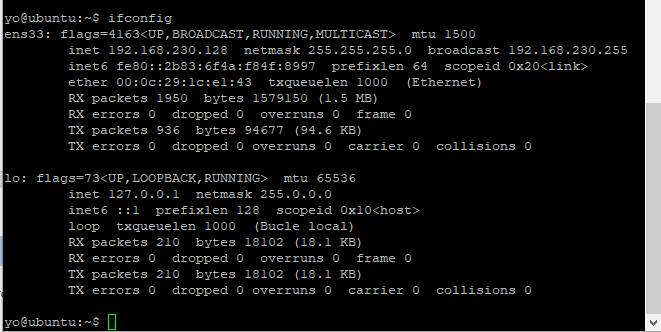
Ejecutamos **putty.exe** y ponemos la dirección IP de la máquina virtual Ubuntu. Hacer clic sobre "Open" para establecer la conexión.



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



Probamos algún comando de Linux:



### Podemos visualizar la sesión SSH en Ubuntu:

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



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 desencriptar lo recibido y entender el mensaje, asegurándonos que la información no se ha alterado durante el proceso.

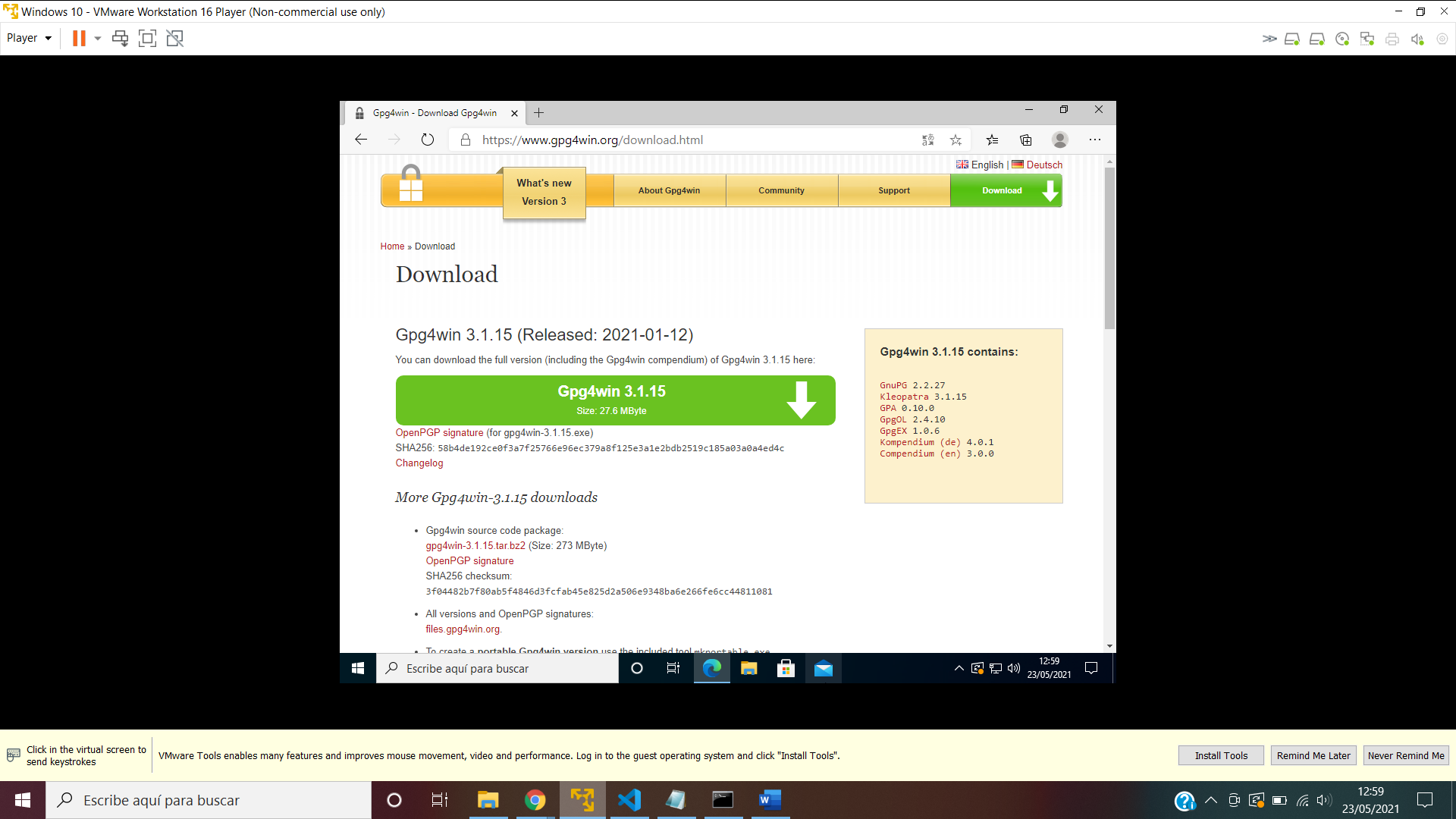
Existen diferentes sistemas de criptografía:

* Simétrica: utilizan la misma clave para encriptar y desencriptar 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 desencriptado de la información.

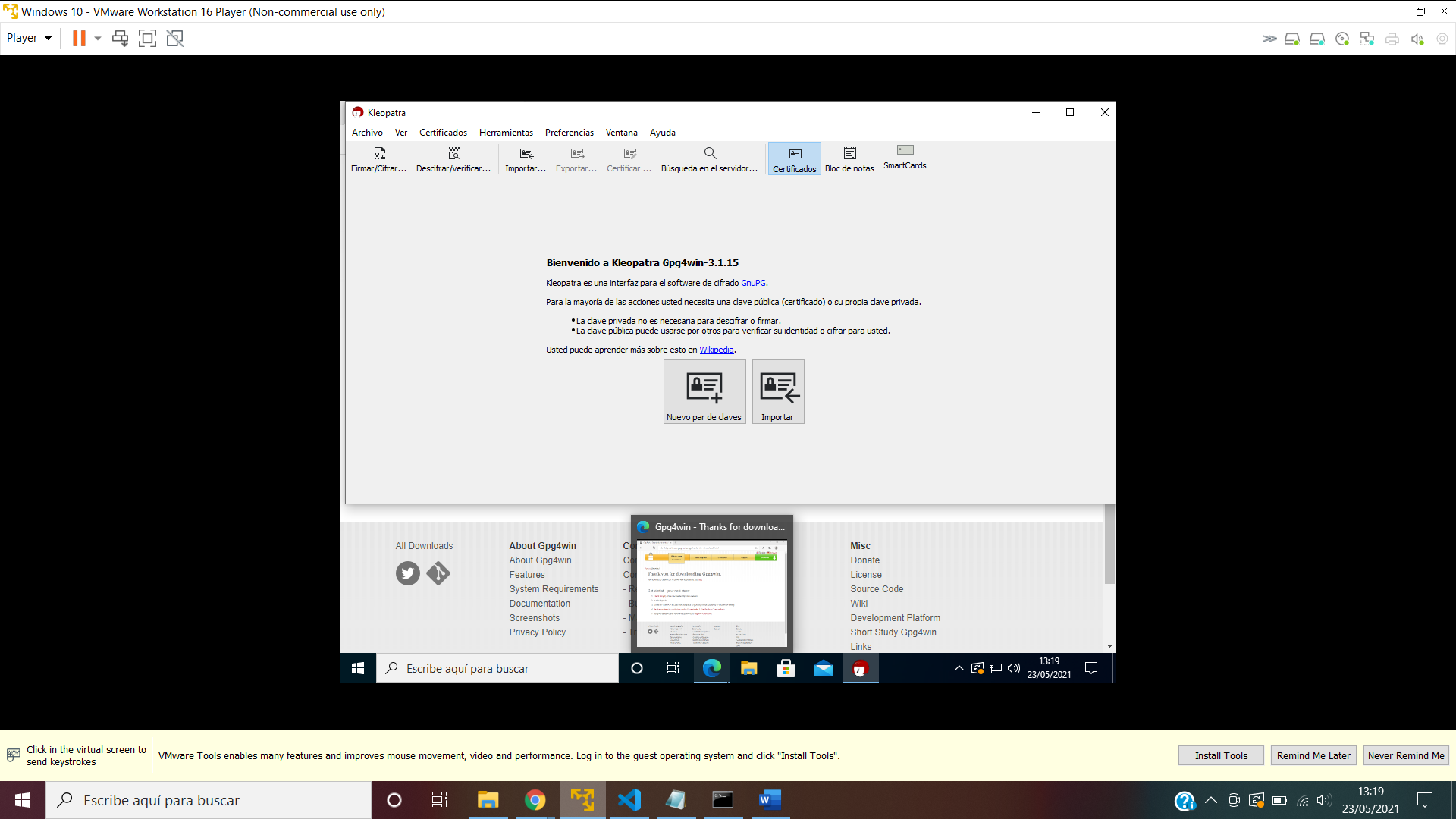
1. **Instalación de Gpg4Win en tu MV Windows 10**

**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.



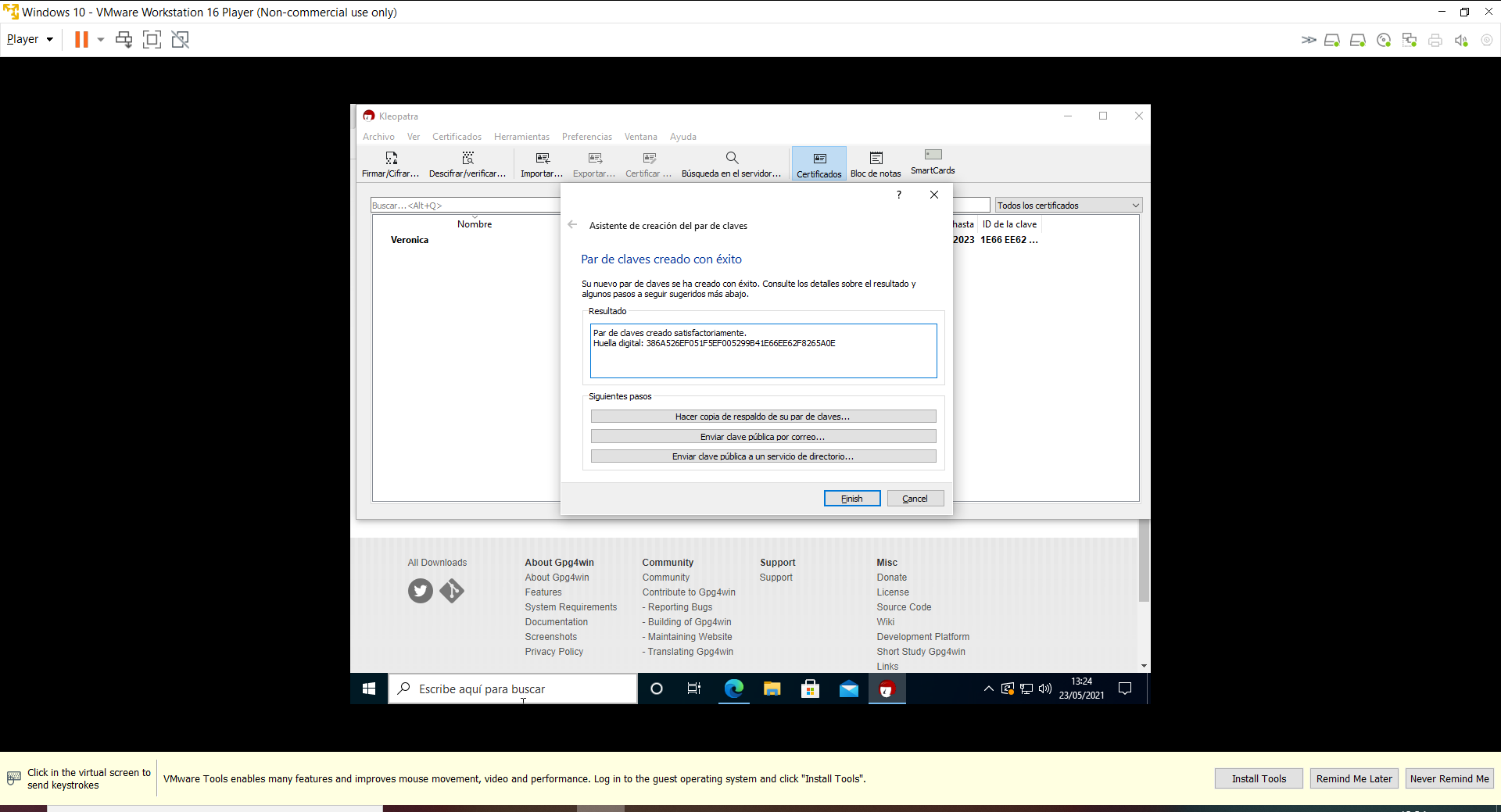
1. **Generación de una pareja de claves (privada y pública) personales tuyas.**

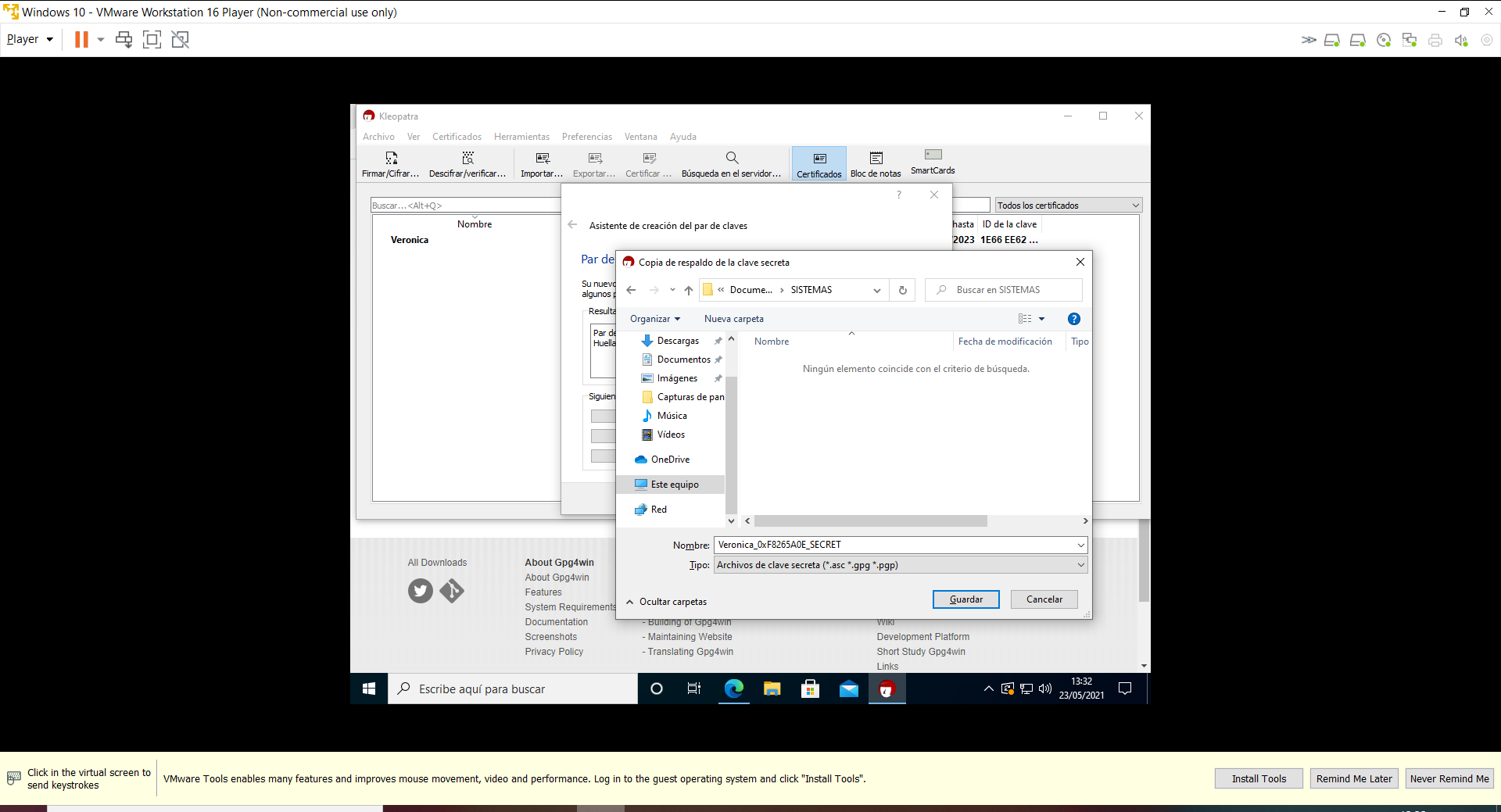
Después de instalar Gpg4Win ejecutamos Kleopatra ( gestor de claves por defecto para GnuPG) . Dado que es la primera vez que lo ejecutamos nos pide generar un nuevo par de claves:



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).

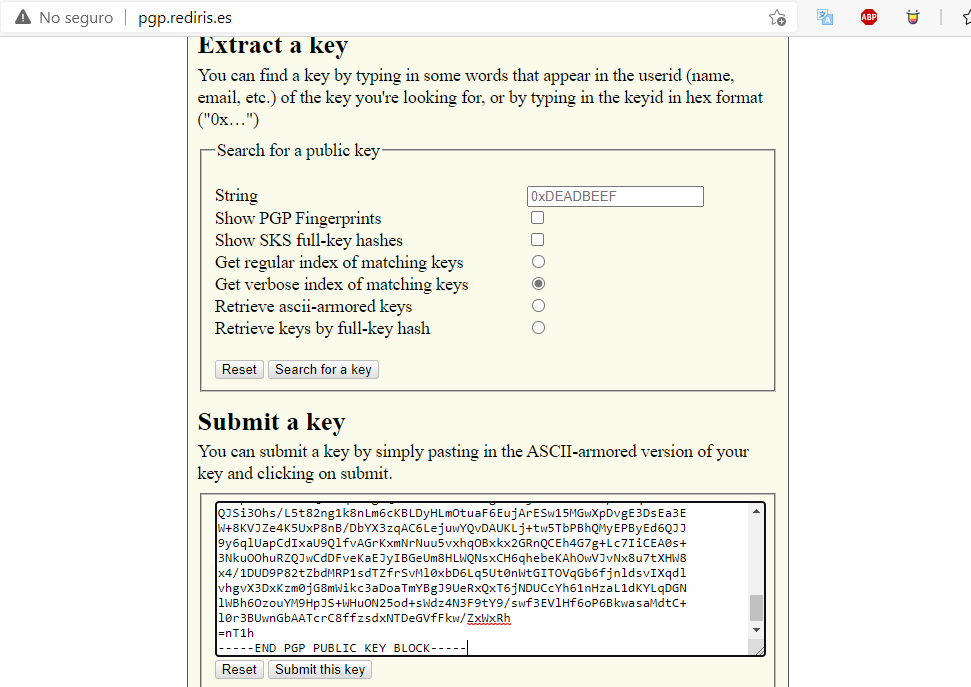
Finalmente generará nuestro par de claves, la huella digital es el identificador de la clave, hacemos una copia de respaldo de nuestro par de claves.



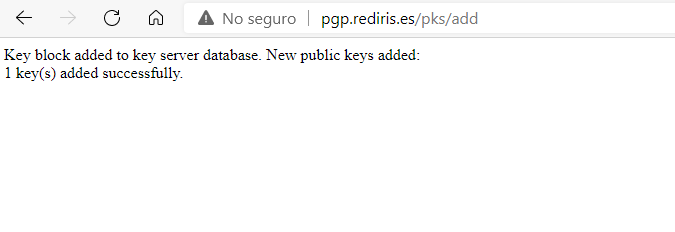


Nos da la opción de hacer una copia de la clave privada. Y posteriormente en la pestaña de exportar podemos guardar la clave pública.

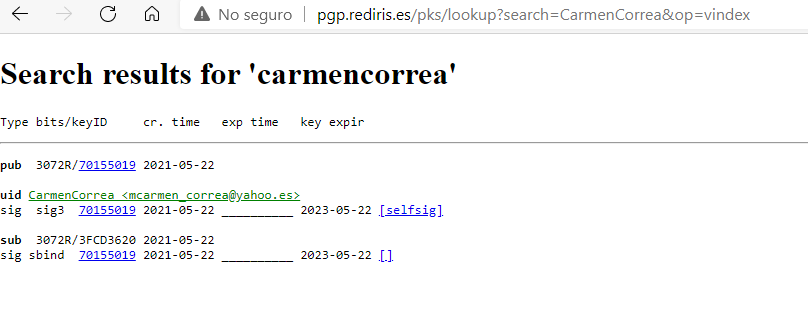
1. **Exportación de tu clave pública y almacenamiento en un servidor externo en Internet (así cualquiera podrá verificar los documentos que firmes)**
2. La subimos al servidor RedIRIS, para lo cual pegamos el código ASCII que encontramos al abrir el fichero en algún editor que reconozca la extensión .asc



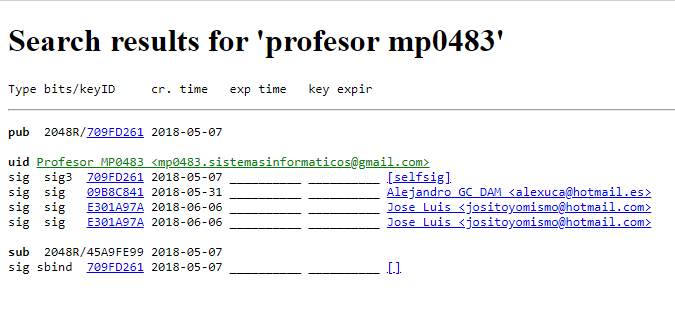
Nos dice que la clave ha sido añadida al servidor.



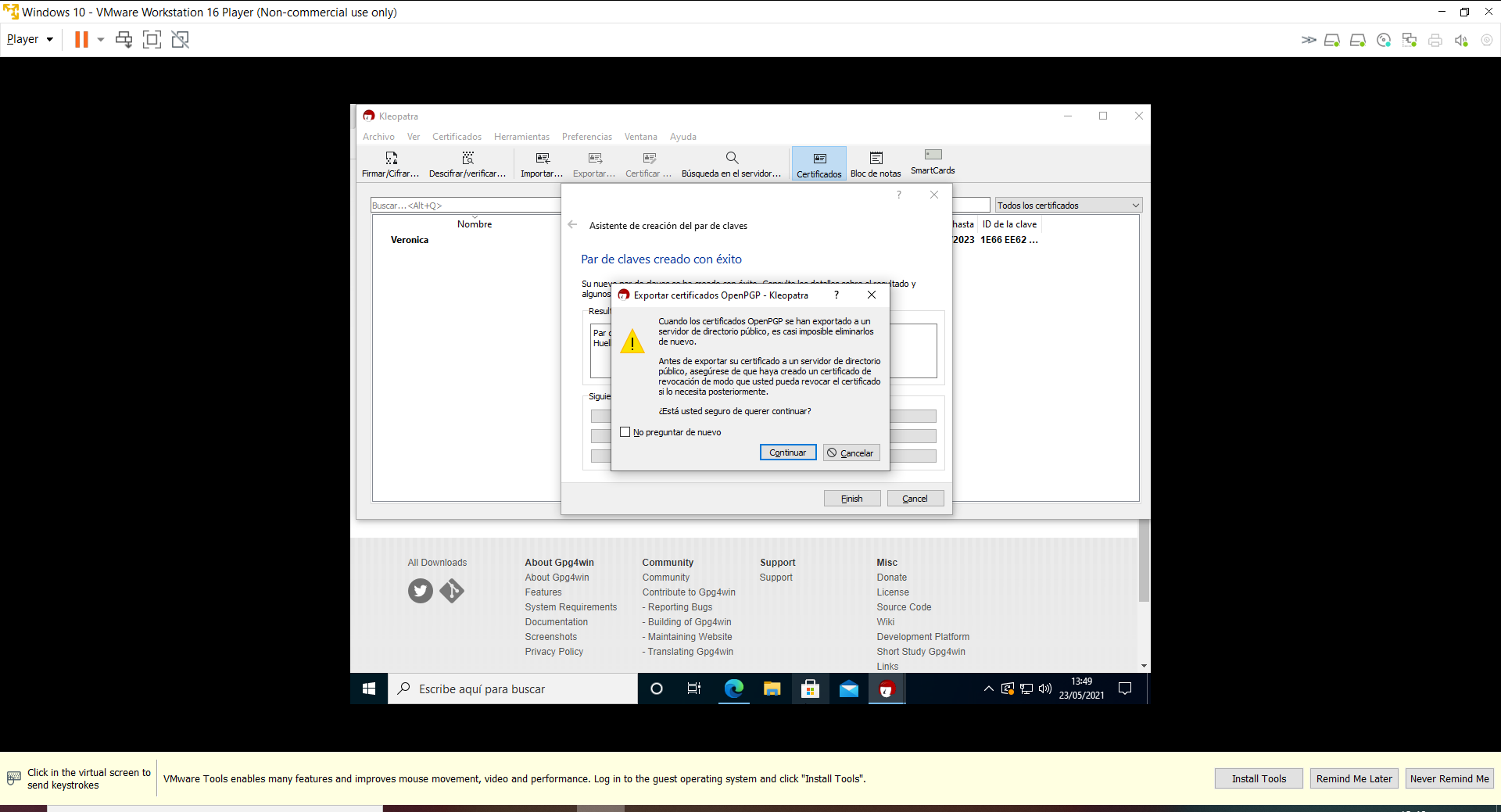
Si la buscamos por el nombre, nos encuentra.

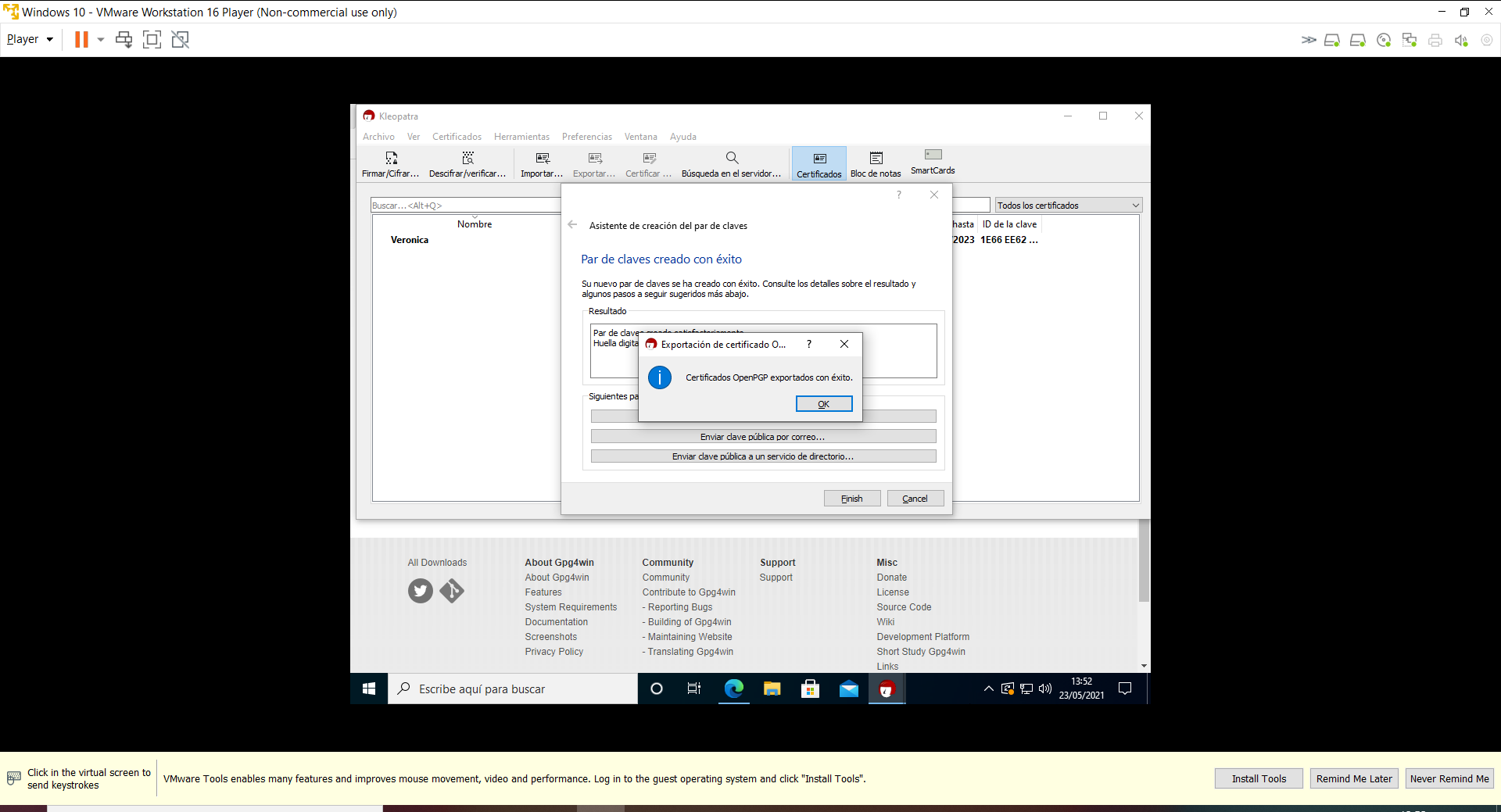


Si buscamos la clave del profesor como en el ejemplo:



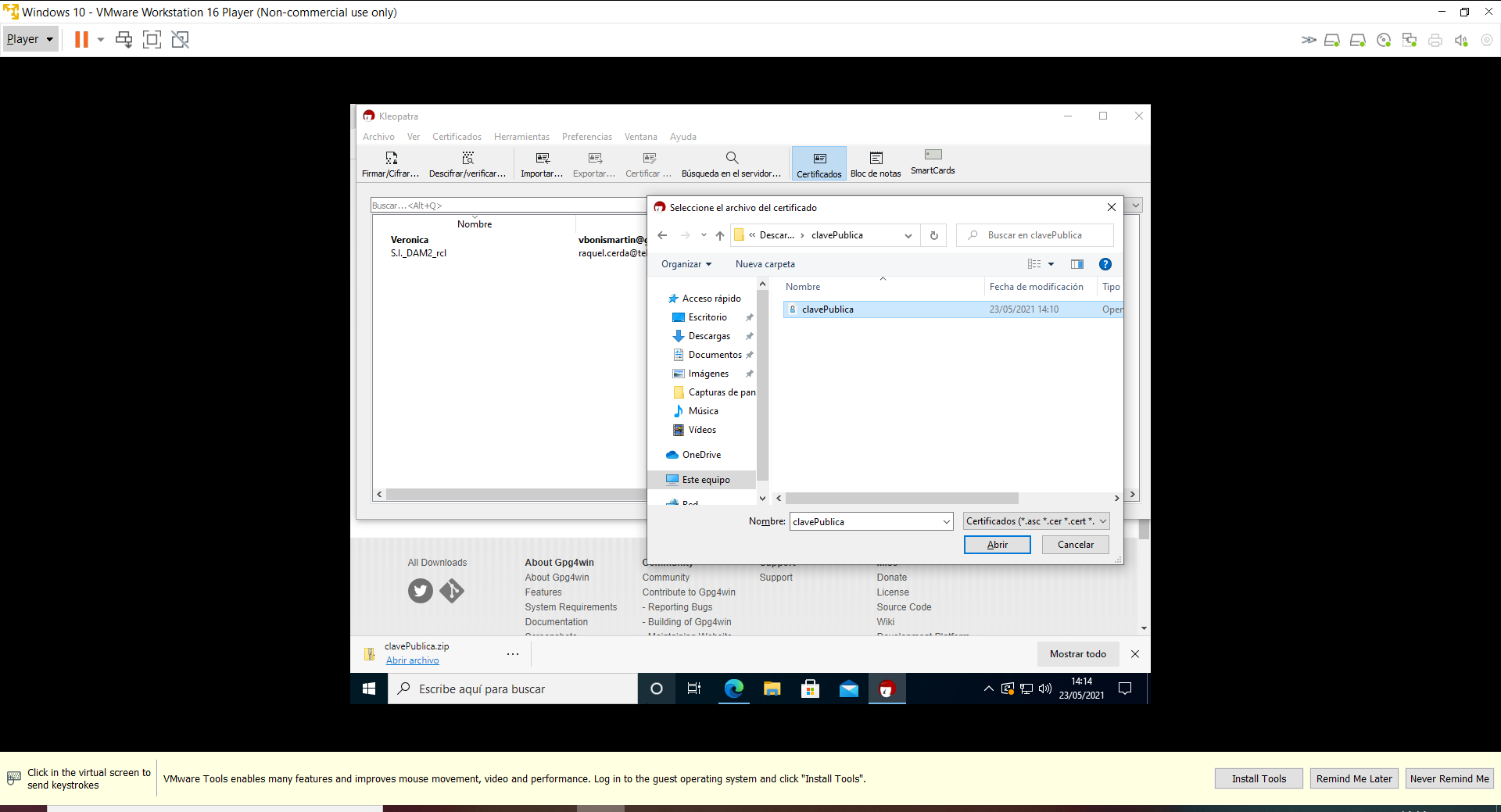
Con Kleopatra también podemos subir la clave pública a un servidor externo en Internet, con Kleopatra es sencillo y podemos usar la opción “Enviar clave pública a un servicio de directorio”. (ignoramos el mensaje sobre el certificado de revocación porque este se crea automáticamente en el proceso anterior).





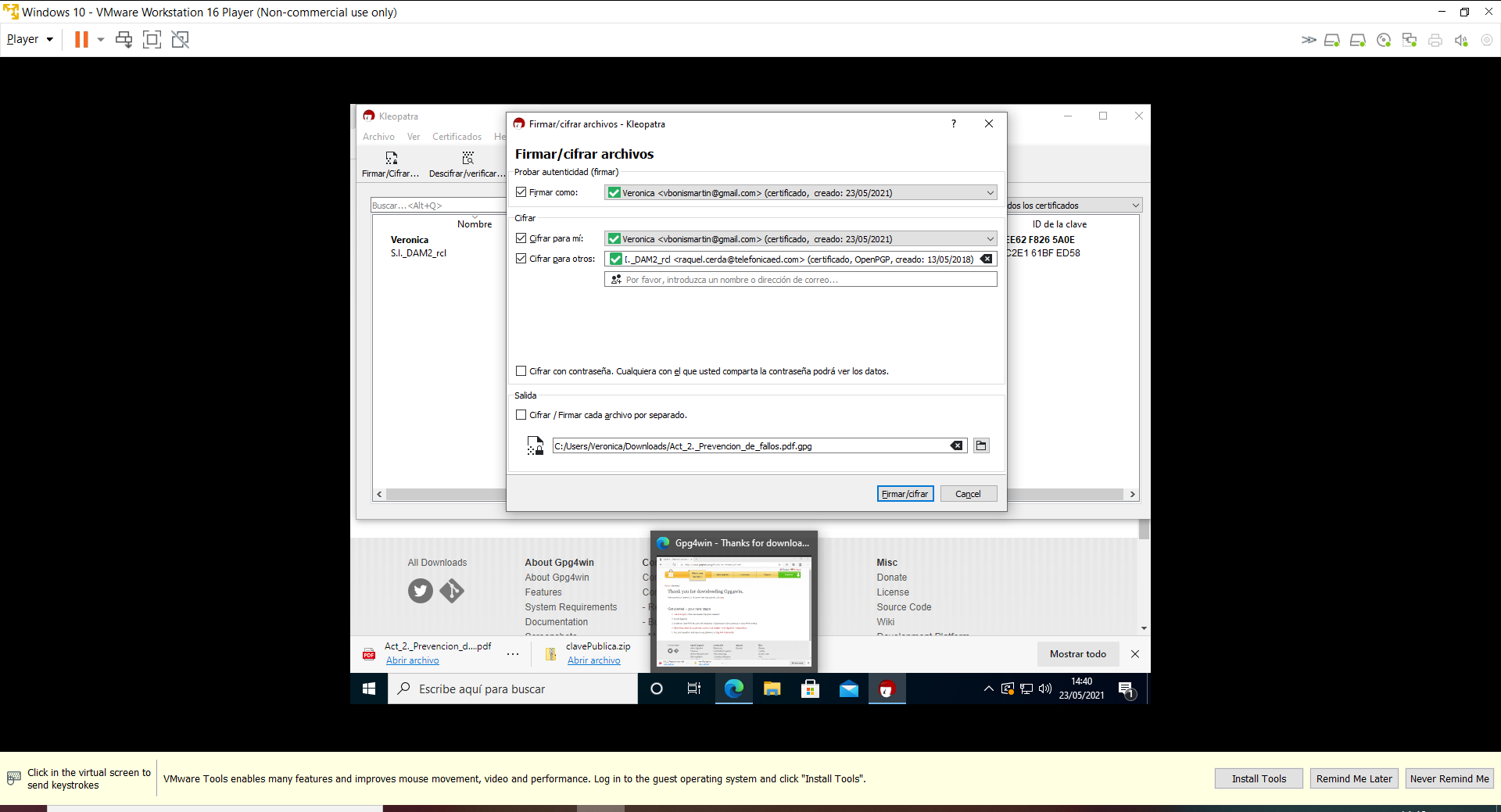
1. **Cifrado del documento entregable de tu práctica AI4 con la clave pública de tu profesor. Para esto primero tendrás que bajártela desde un servidor externo y luego importarla en tu sistema de claves.**

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

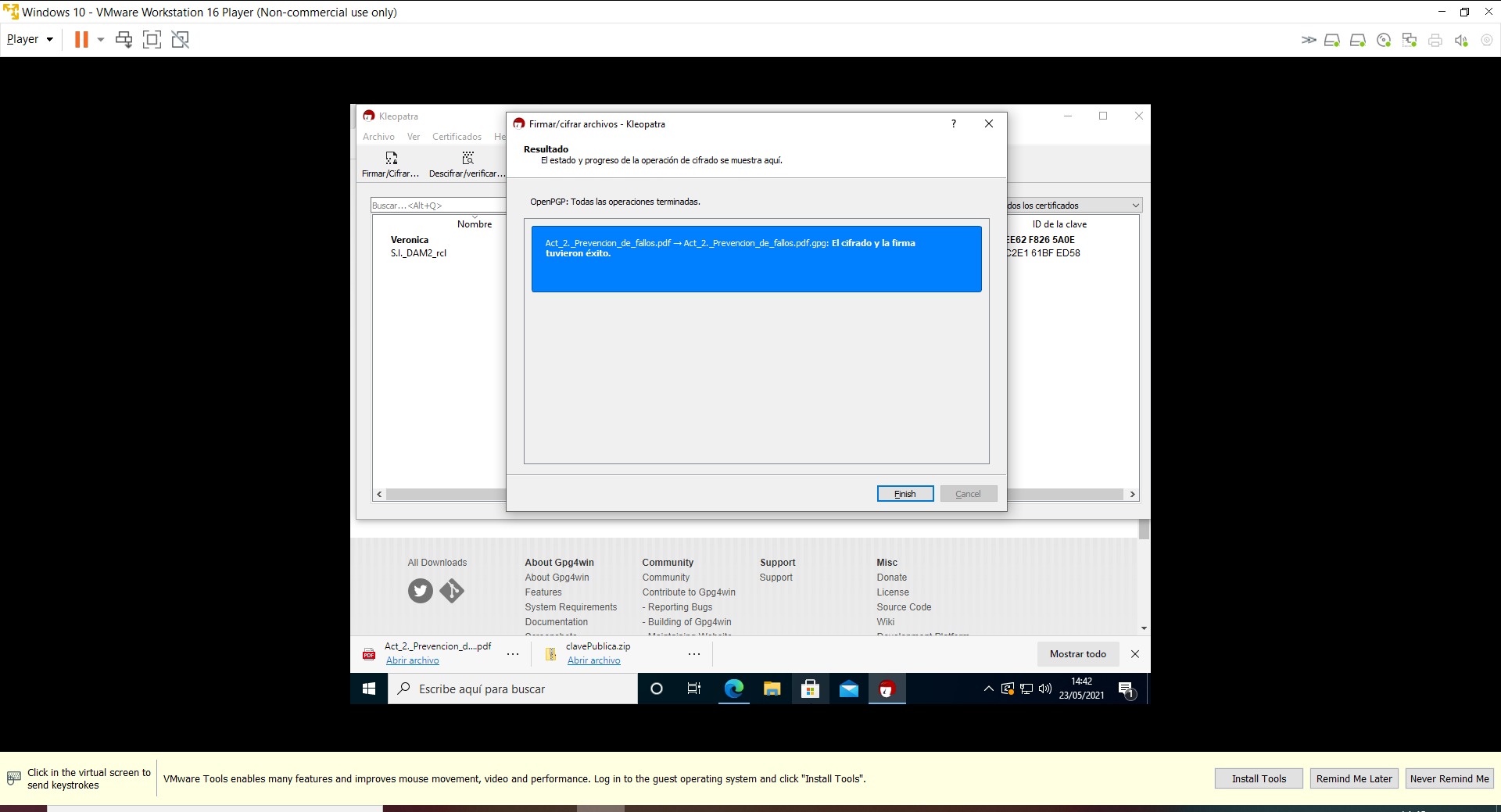


Una vez añadido podemos indicar que es de confianza (certificar la validez de las claves al importarlas), y a continuación podemos cifrar cualquier archivo usando la opción Firmar/ Cifrar.

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

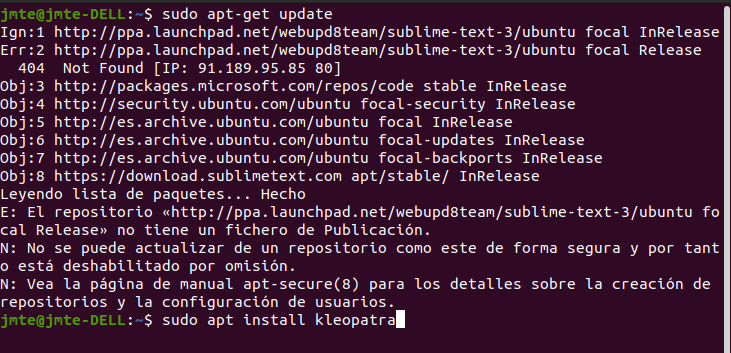


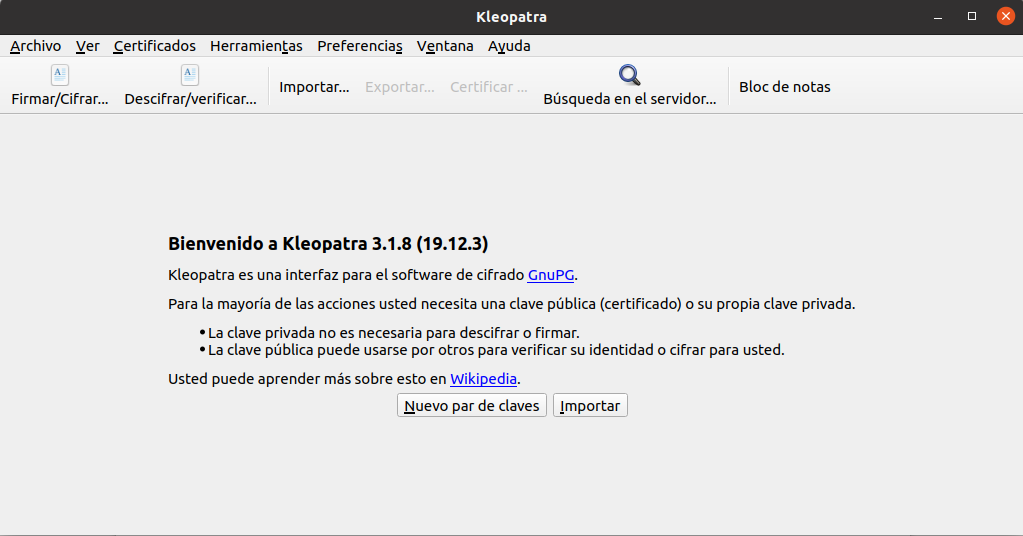
Se nos genera un archivo \*. .gpg que el destinatario podrá desencriptar y visualizar con su clave.



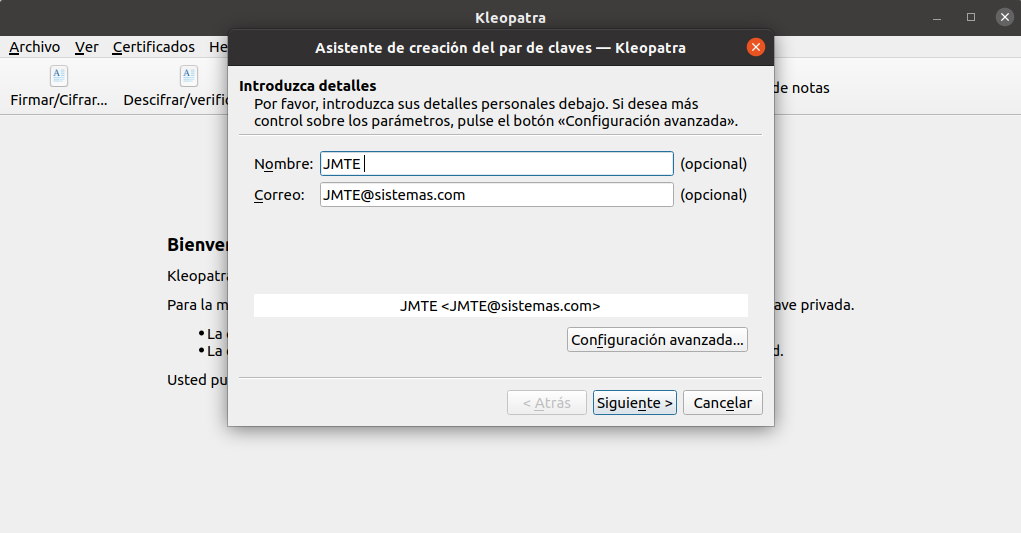
**Instalación de Kleopatra y creación de par de claves desde el entorno Ubuntu**

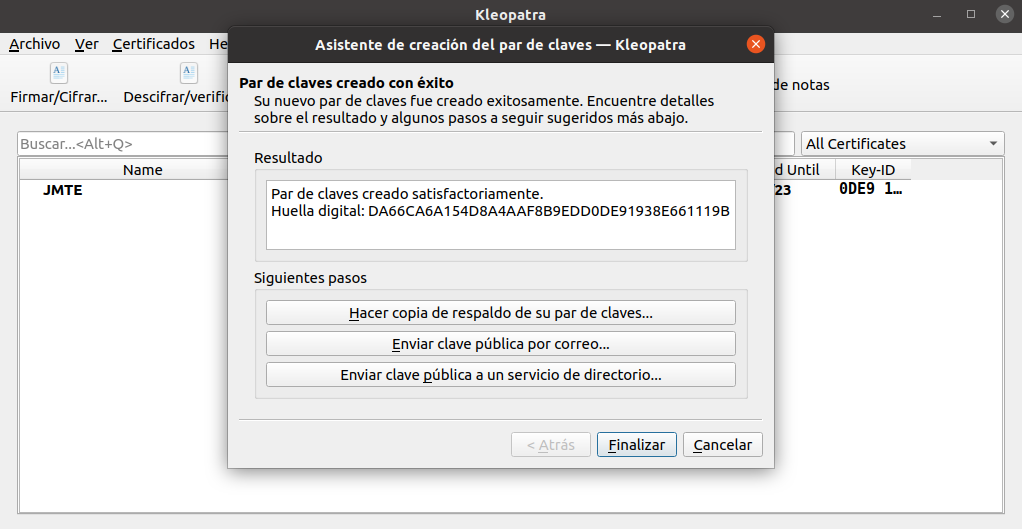
La forma tanto de la instalación como de la creación de las claves desde el entorno Linux es muy parecido a Windows, para ello nos situamos en la terminal e instalamos el paquete de Kleopatra:



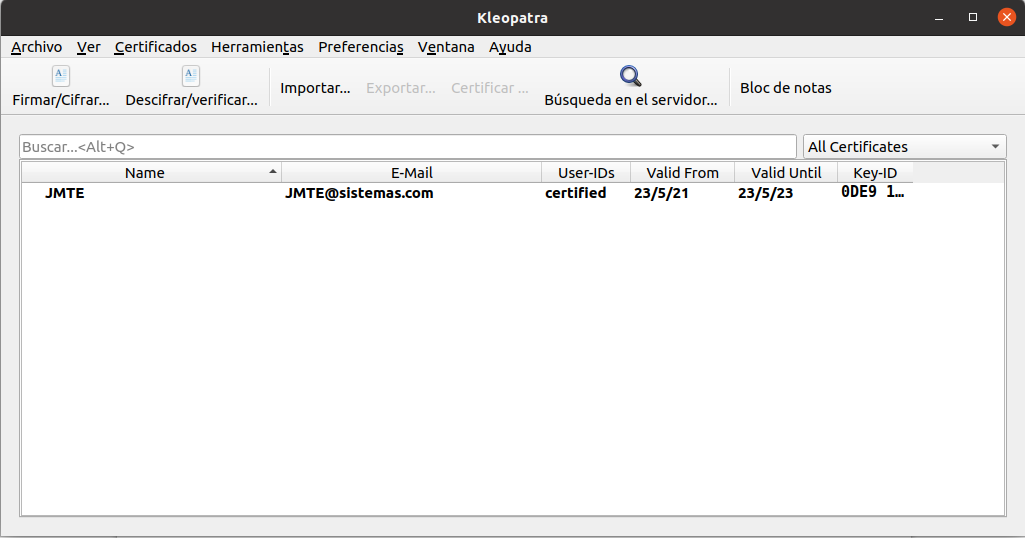
Cuando termina, ya podremos buscar el programa en la lista y lo ejecutaremos:

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).



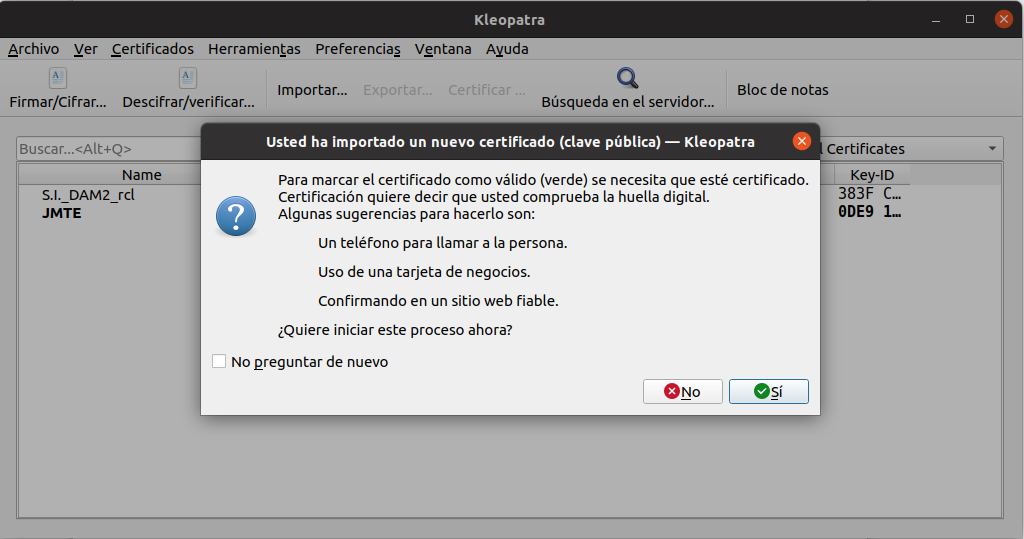
En esta pantalla es donde podemos elegir qué tipo de copia realizar, al elegir una, debemos de introducir la contraseña que configuramos anteriormente.

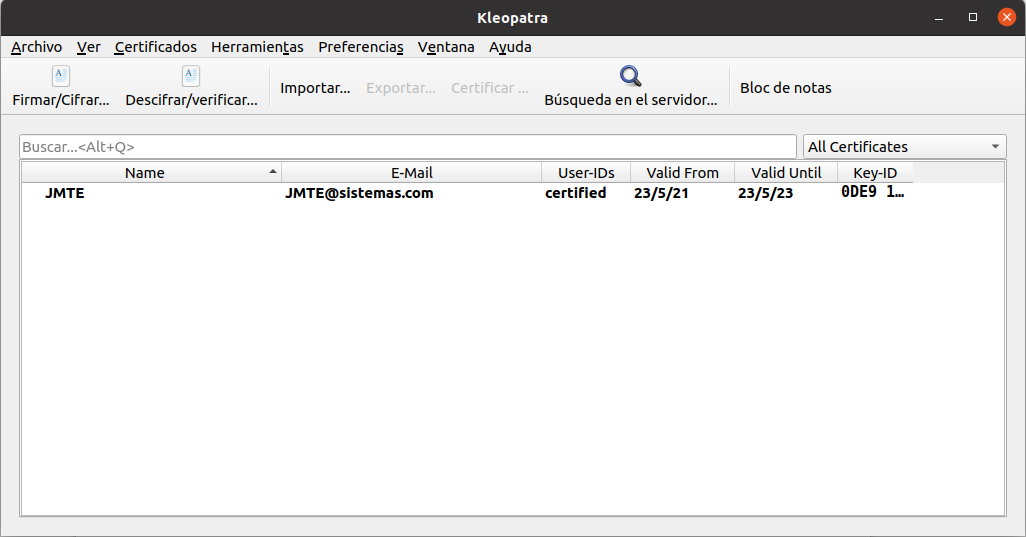
Ya tendríamos nuestro par de claves creada.

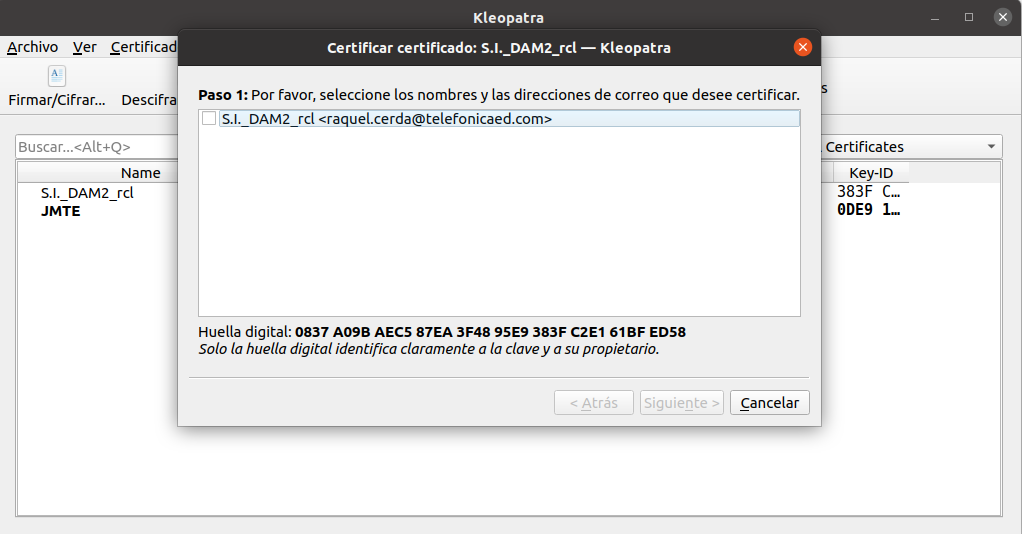
Para finalizar, debemos de encriptar el documento .pdf que entregamos en la Actividad 2 con la clave que nos facilitan y que se encuentra en el foro de la asignatura. La descargamos en archivo .zip y la se descomprime para después seleccionarla.

El proceso a llevar a cabo es el siguiente:

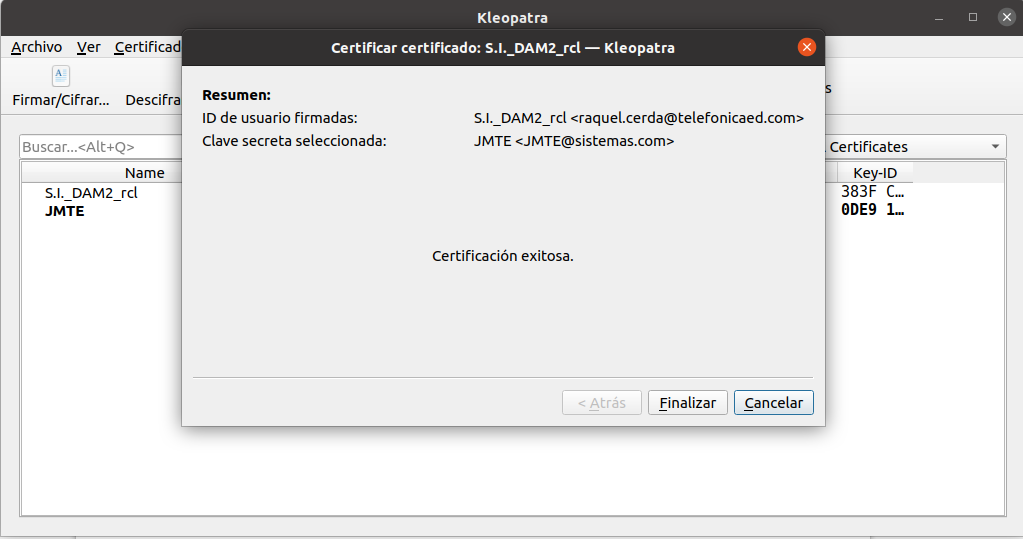
Seleccionamos la opción importar para tener nuestro certificado facilitado en Kleopatra:

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

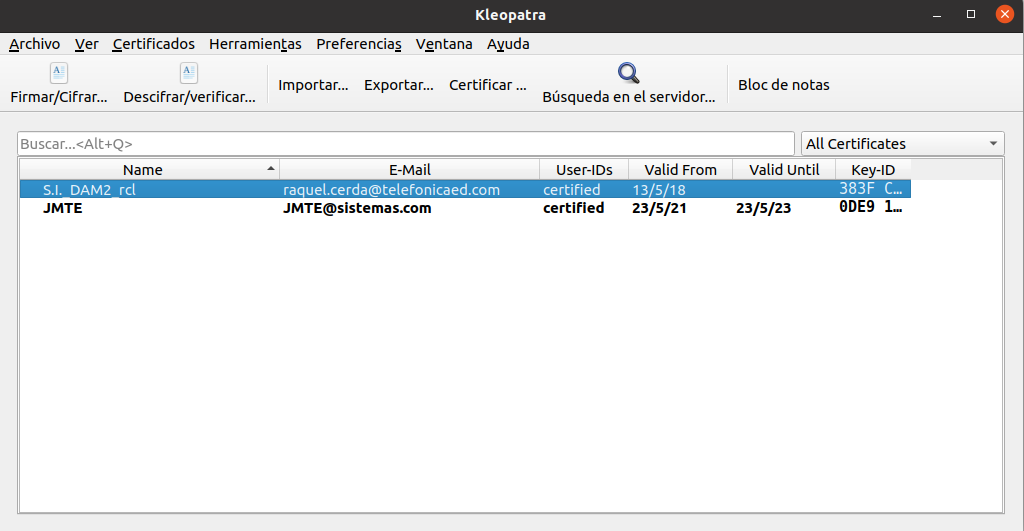
SELECCIONAR: IMPORTAR

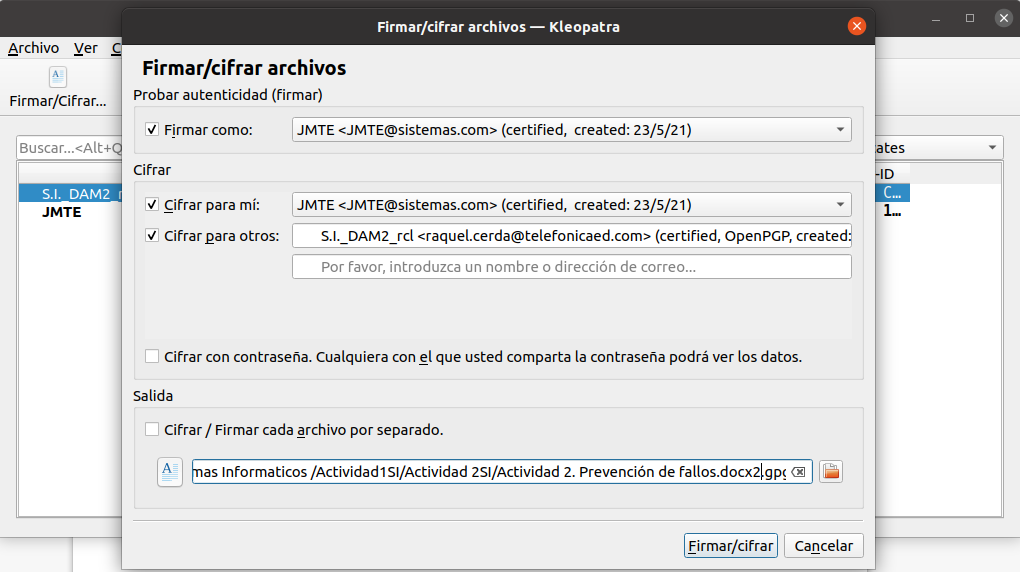
Marcamos la opción que tenemos indicando que la clave proporcionada es válida:

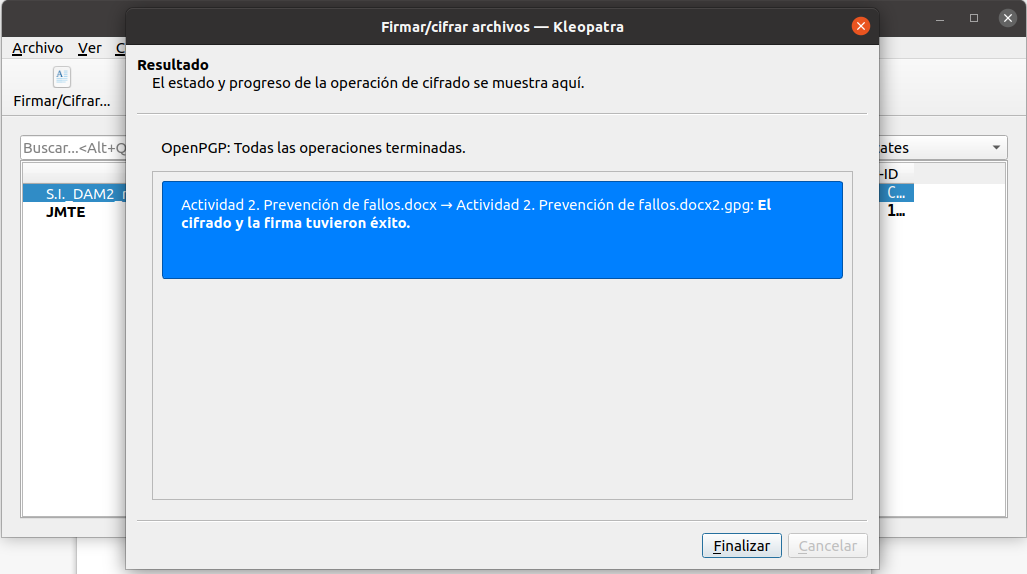
Y ya se nos indica que ha concluido con éxito:



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.

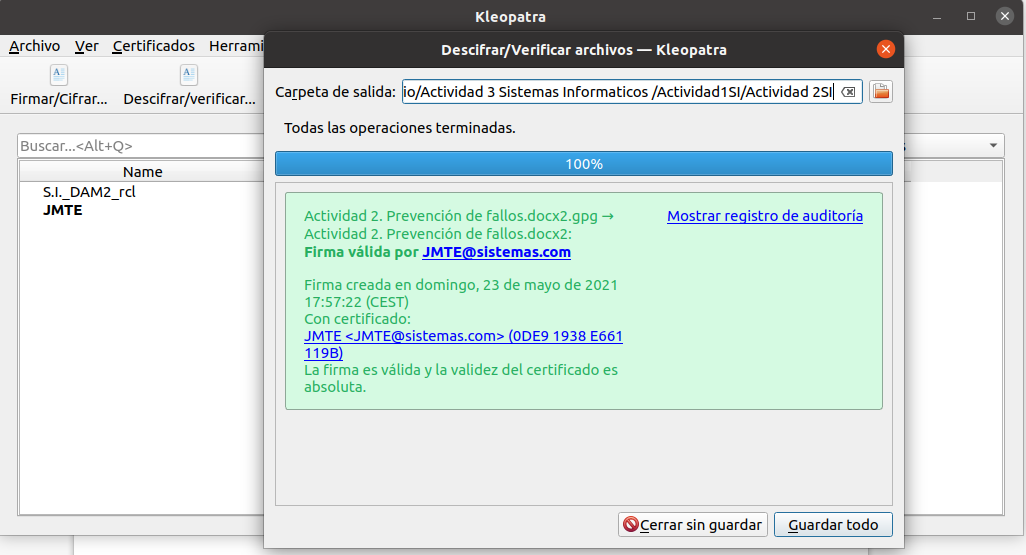


De esta manera habremos cifrado el documento de manera exitosa para que la persona que nos ha facilitado las claves pueda descifrarlo mediante ellas.

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



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.