AE-3 CONEXIÓN CON LA RED

GRUPO 6

Carlos Rábago Torcates
Lidia Díaz Mendoza
Sergio Martínez Rivera

Requerimiento 1

1. Máscaras de subred y direcciones IP

✓ Para calcular la dirección de red primeramente hacemos la conversión de la dirección IP y la máscara de subred de decimal a binario y seguidamente hacemos un "AND" lógico entre ambas direcciones. Para calcular la difusión hacemos un "OR" lógico entre la dirección IP y el inverso de la máscara.

- **192.168.2.119 / 255.255.255.192**

	Decimal	**Binario**
Dirección IP	192.168.2.119	11000000.10101000.00000010.01110111
Máscara de subred	255.255.255.192	11111111.11111111.11111111.11000000
	AND lógico	11000000.10101000.00000010.01000000
	Dirección de red	192.168.2.64

	Decimal	**Binario**
Dirección IP	192.168.2.119	11000000.10101000.00000010.01110111
Máscara de subred inverso	255.255.255.192	00000000.00000000.00000000.00111111
	OR lógico	11000000.10101000.00000010.01111111
	Dirección de difusión	192.168.2.127

- **192.168.2.126 / 26**

	Decimal	**Binario**
Dirección IP	192.168.2.126	11000000.10101000.00000010.01111110
Máscara de subred	/26 (255.255.255.192)	11111111.11111111.11111111.11000000
	AND lógico	11000000.10101000.00000010.01000000
	Dirección de red	192.168.2.64

	Decimal	**Binario**
Dirección IP	192.168.2.126	11000000.10101000.00000010.01111110
Máscara de subred inverso	/26 (255.255.255.192)	00000000.00000000.00000000.00111111
	OR lógico	11000000.10101000.00000010.01111111
	Dirección de difusión	192.168.2.127

- **192.168.0.190 / 255.255.255.240**

	Decimal	**Binario**
Dirección IP	192.168.0.190	11000000.10101000.00000000.10111110
Máscara de subred	255.255.255.240	11111111.11111111.11111111.11110000
	AND lógico	11000000.10101000.00000000.10110000
	Dirección de red	192.168.0.176

	Decimal	**Binario**
Dirección IP	192.168.0.190	11000000.10101000.00000000.10111110
Máscara de subred inverso	255.255.255.240	00000000.00000000.00000000.00001111
	OR lógico	11000000.10101000.00000000.10111111
	Dirección de difusión	192.168.0.191

- **192.168.0.190 / 255.255.240.0**

	Decimal	**Binario**
Dirección IP	192.168.0.190	11000000.10101000.00000000.10111110
Máscara de subred	255.255.240.0	11111111.11111111.11110000.00000000
	AND lógico	11000000.10101000.00000000.00000000
	Dirección de red	192.168.0.0

	Decimal	**Binario**
Dirección IP	192.168.0.190	11000000.10101000.00000000.10111110
Máscara de subred inverso	255.255.240.0	00000000.00000000.00001111.11111111
	OR lógico	11000000.10101000.00001111.11111111
	Dirección de difusión	192.168.15.255

- **192.168.2.119 / 255.255.0.0**

	Decimal	**Binario**
Dirección IP	192.168.2.119	11000000.10101000.00000010.01110111
Máscara de subred	255.255.0.0	11111111.11111111.00000000.00000000
	AND lógico	11000000.10101000.00000000.00000000
	Dirección de red	192.168.0.0

	Decimal	**Binario**
Dirección IP	192.168.2.119	11000000.10101000.00000010.01110111
Máscara de subred inverso	255.255.0.0	00000000.00000000.11111111.11111111
	OR lógico	11000000.10101000.11111111.11111111
	Dirección de difusión	192.168.255.255

Todas redes de clase 'C' con un número máximo de 256 hosts que realmente serian 254 ya que uno es usado como dirección de difusión y otro como identificador de red.

✓ **Dadas las siguientes máscaras de subred, dinos cuántos hosts puede tener como máximo cada subred:**

- 255.255.255.128

Esta máscara de subred en Binario sería 11111111.11111111.11111111.10000000 puede tener 128 hosts como máximo (que en realidad serían 126) en 2 subredes.

- 255.255.255.255

Esta máscara de subred en Binario sería 11111111.11111111.11111111.11111111 no tiene hosts y puede tener 256 subredes.

- 255.255.255.224

Esta máscara de subred en Binario sería 11111111.11111111.11111111.11100000 puede tener 32 hosts como máximo (que en realidad serían 30) en 8 subredes.

✓ **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?

Ninguna ya que sólo admite 256 hosts.

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

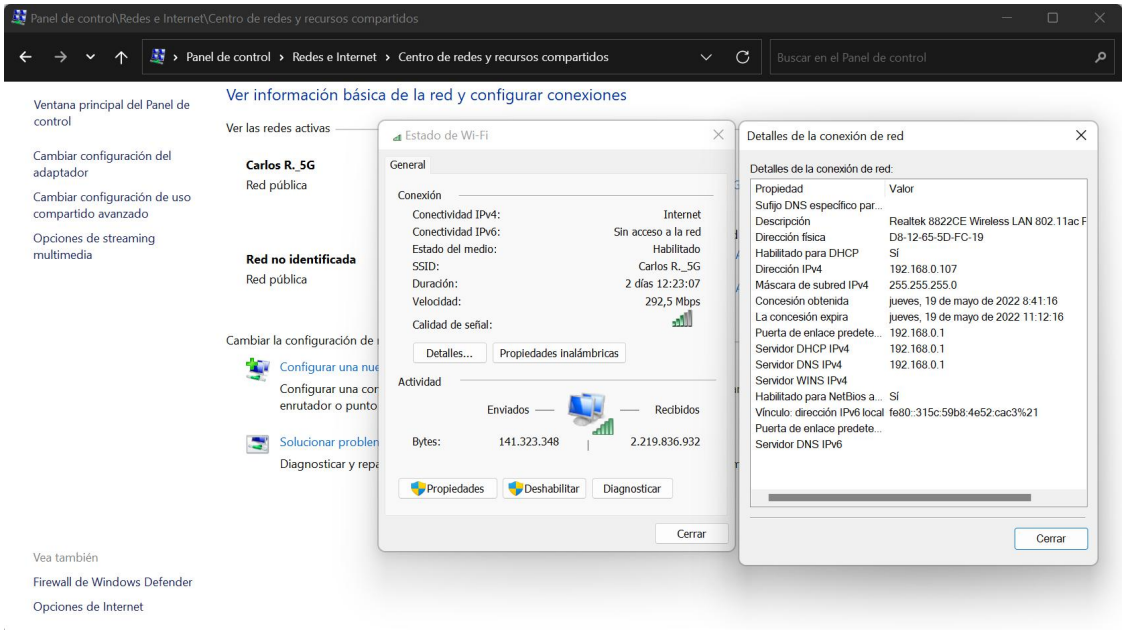
Ninguna ya que sólo admite 256 hosts.

2. 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.

Dirección IP ordenador personal

Para ubicarla nos vamos a panel de control > redes e Internet > centro de redes y recursos compartidos. Una vez allí entramos a la red que estamos conectados pulsamos en detalles y nos aparecerá una ventana con la información. En este caso la dirección IP es 192.168.0.107.

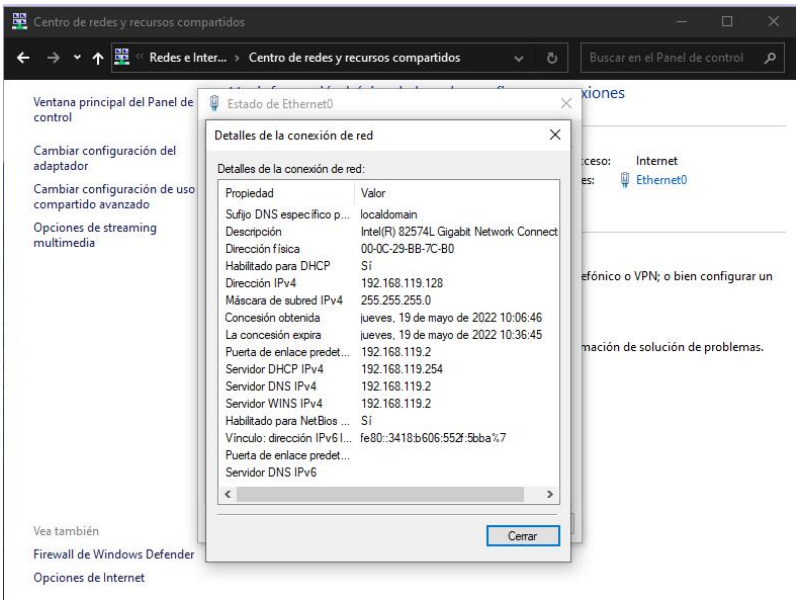


Para ver la dirección IP con la consola simplemente debemos teclear ipconfig y nos mostrará la información.

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::315c:59b8:4e52:cac3%21
   Dirección IPv4. . . . . . . . . . . . : 192.168.0.107
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1

Adaptador de Ethernet Conexión de red Bluetooth:

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

C:\Users\carlo>
```

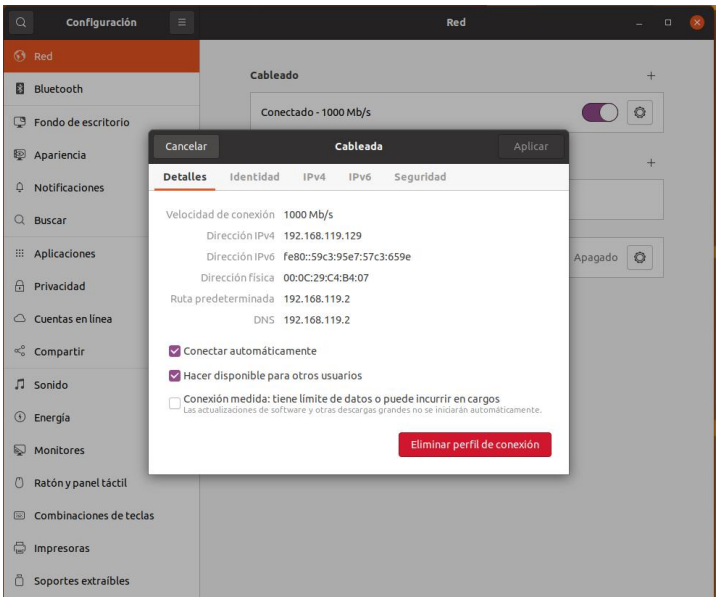
Dirección IP máquina virtual Windows 10

Se buscaría de la misma manera que en el caso anterior.

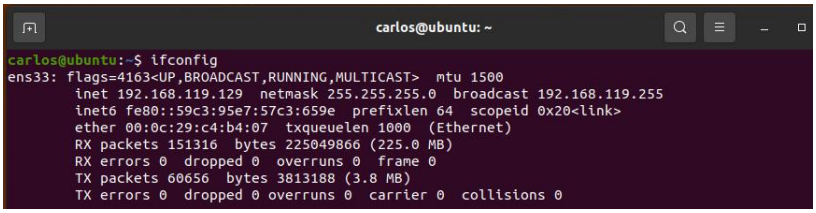


Dirección IP máquina virtual Ubuntu

Entramos a configuración > red > configuración de red conectada. Nos mostrará que la dirección IP es 192.168.119.129



Para verla en consola se debe teclear ‘ifconfig’



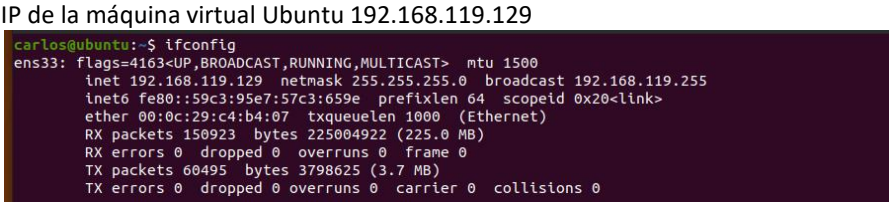
3. Conexión con internet

Para averiguar la dirección IP pública de la conexión a internet usaremos la página web http://www.cualesmiip.com/, lo cual nos muestra la siguiente información.

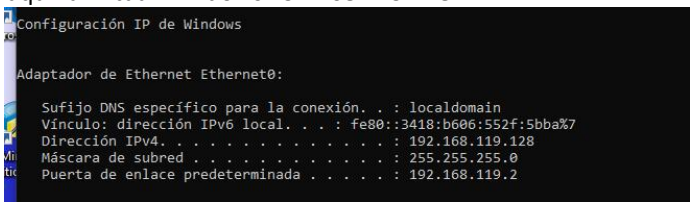
4. Practicar con “ping”

Visualizamos las direcciones IP de los tres sistemas, la máquina física y las dos máquinas virtuales. En los sistemas Windows usamos el comando "ipconfig" y en Ubuntu el comando "ifconfig".

Dirección IP de la máquina virtual Ubuntu 192.168.119.129

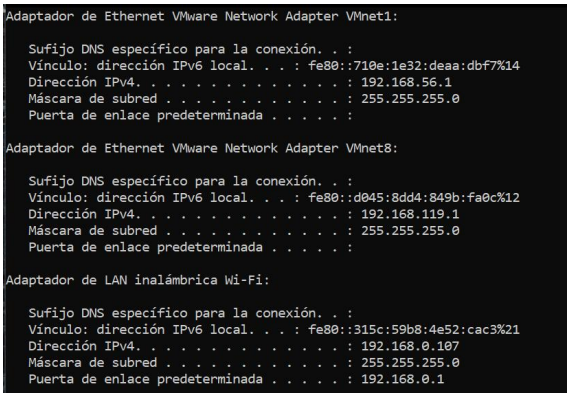


Dirección IP de la máquina virtual Windows 192.168.119.128



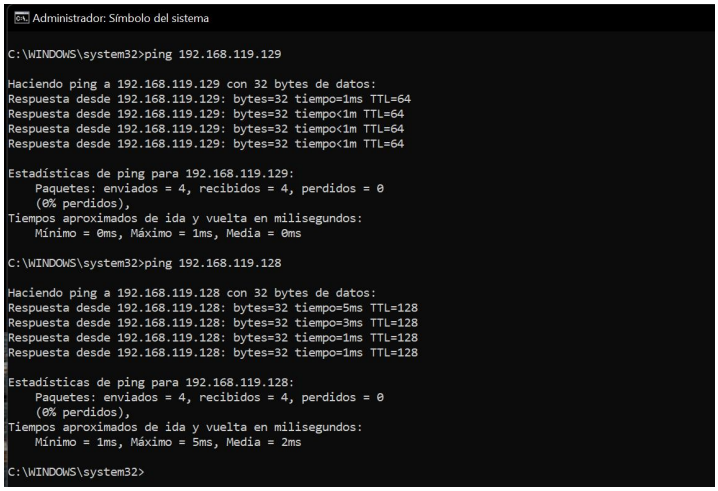
Dirección IP de la máquina física 192.168.0.107

Nota: al usar el comando ‘ipconfig’ en la máquina física, en el resultado también aparecen los adaptadores de red virtuales de las máquinas virtuales.

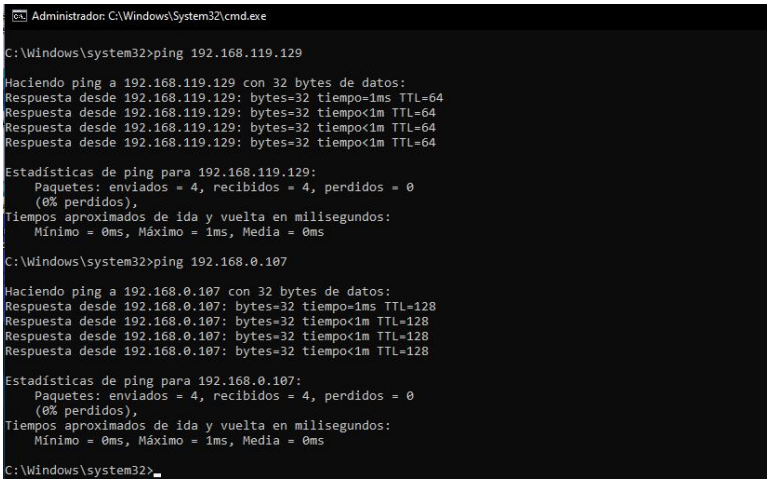


Usamos el comando "ping" para comprobar que desde cada sistema podemos ver/alcanzar los otros dos.

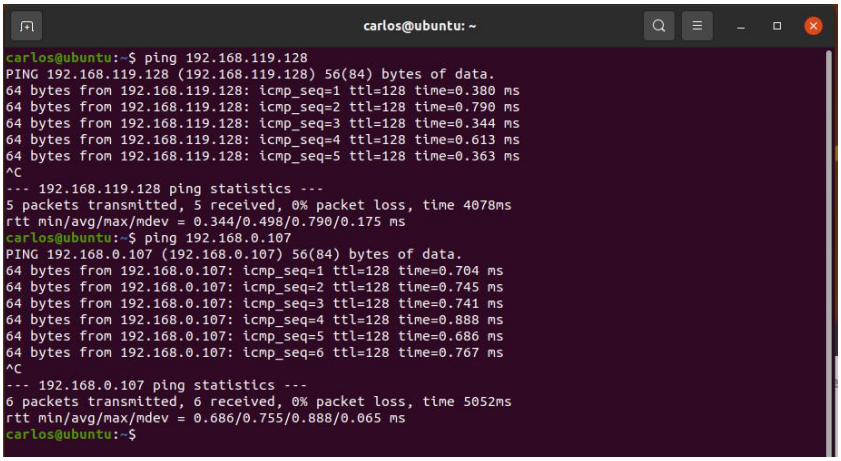
Desde la máquina física alcanzamos las dos máquinas virtuales.



Desde la máquina virtual de Windows alcanzamos la máquina virtual de Ubuntu y la máquina física



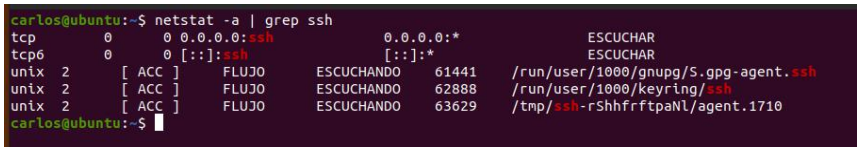
Desde la máquina virtual de Ubuntu alcanzamos la máquina virtual de Windows y la máquina física



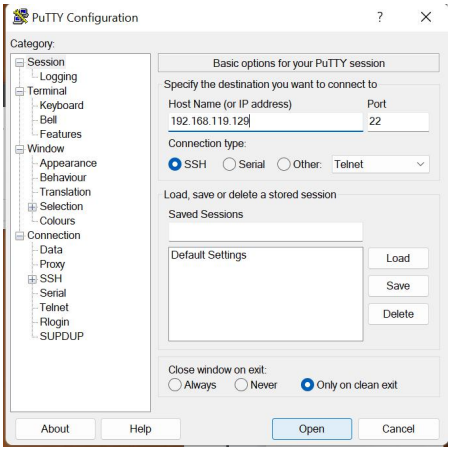
5. Conexión SSH Windows-Ubuntu

Vamos a hacer una conexión segura utilizando el protocolo SSH entre un sistema Windows y otro Linux. Primeramente instalamos el servidor SSH en la máquina virtual Ubuntu, para ello ejecutaremos el siguiente comando en la consola 'sudo apt-get install ssh'.

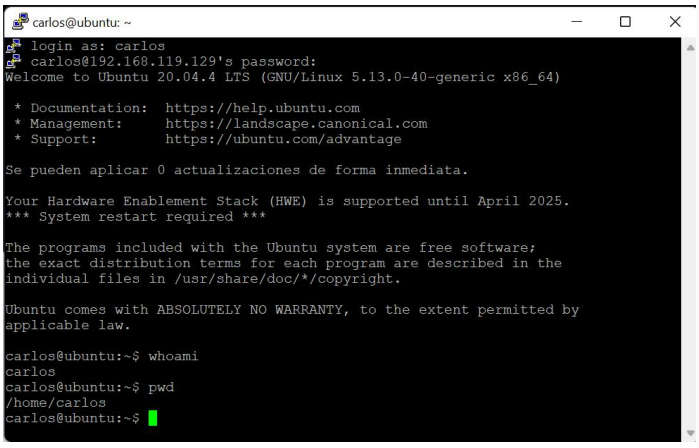
Luego con el comando 'ifconfig' comprobamos la dirección IP del sistema (192.168.119.129) y a continuación con el comando 'netstat -a | grep ssh' comprobamos que el SSH está activo y escuchando.



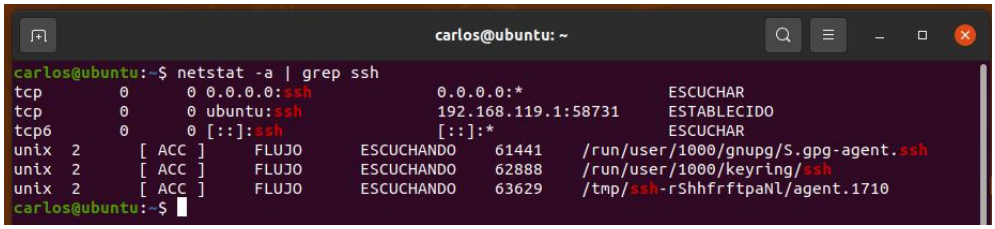
Vamos a la máquina física de Windows y descargamos la aplicación 'Putty' y la ejecutamos. Colocamos la dirección IP de la máquina virtual de Ubuntu y hacemos click en 'Open' para establecer la conexión.



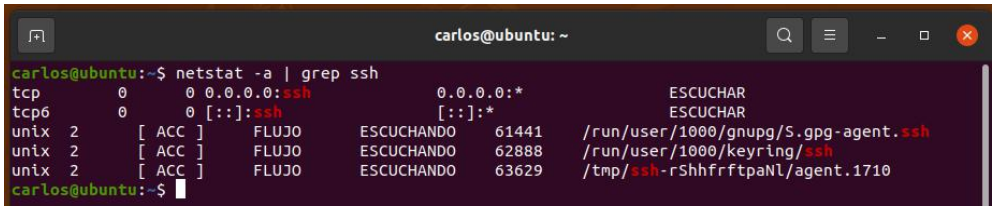
Una vez establecida la conexión nos logueamos con el usuario y la contraseña de Ubuntu y de esta manera ya tendríamos conexión a la máquina Ubuntu desde la máquina Windows.
Probamos algunos comandos para comprobar que funciona correctamente.



Luego visualizamos la sesión SSH en Ubuntu, para ello insertamos el comando "netstat –a | grep ssh" y vemos que en Ubuntu aparece como conectado el PC de Windows.



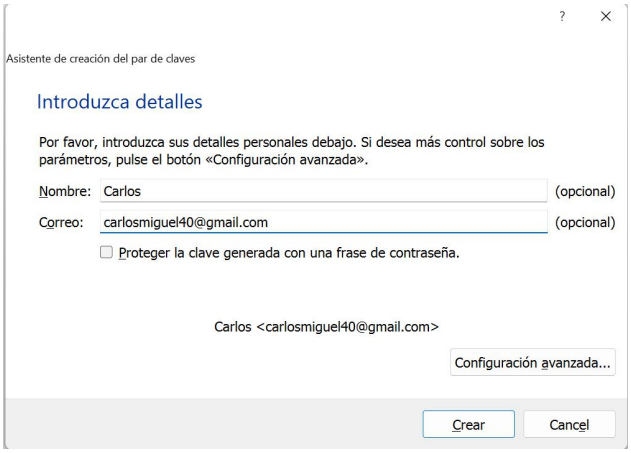
Luego sobre la ventana de 'Putty' (en Windows) tecleamos el comando 'logout' para finalizar la conexión y volvemos a comprobar con el comando 'netstat' (en Ubuntu) que el SSH sigue activo, pero ya no tiene la conexión establecida.



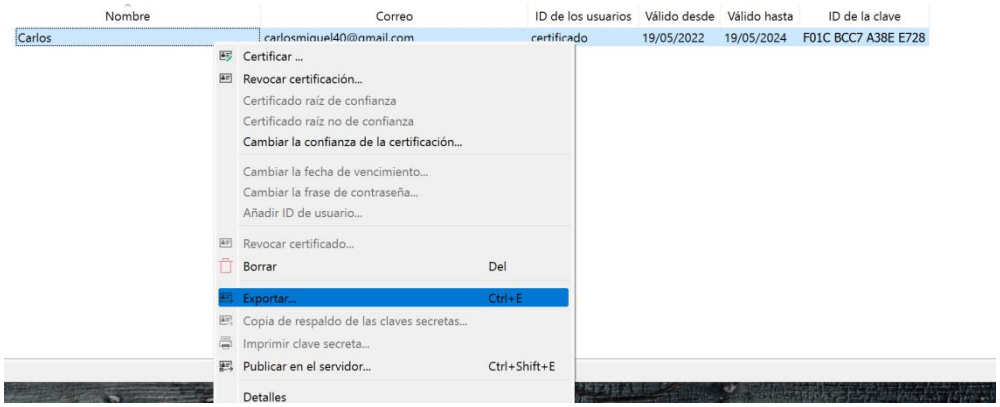
Requerimiento 2

- Para este requerimiento primero vamos a instalar la herramienta Gpg4Win en una primera máquina, en este caso la máquina de 'Carlos'.
- Luego una vez abierta la herramienta hacemos click en 'Nuevo par de claves' (privada y pública).

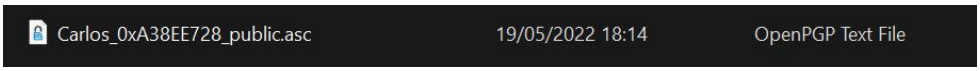
Pedirá un nombre y un correo, después de colocarlo hacemos click en crear.



- Exportamos la clave pública haciendo click derecho sobre el certificado que hemos creado y luego en 'exportar'



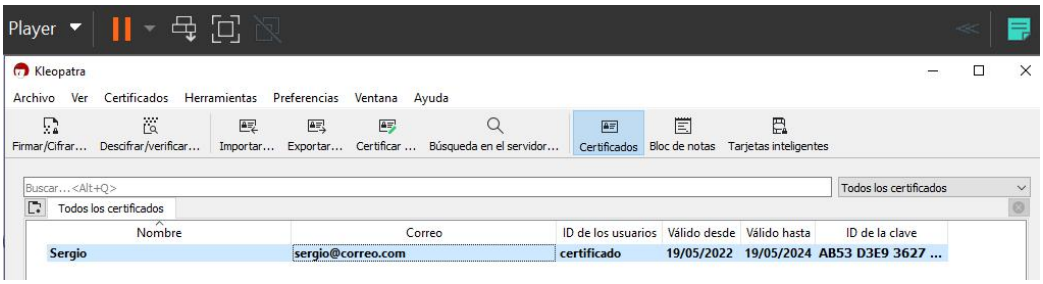
Obtendremos un archivo que es nuestra llave pública.



Esta clave pública es la que debemos enviar a la persona que queremos enviar la información cifrada, que en este caso práctico será 'Sergio'.

Para probar que funciona vamos a abrir una segunda máquina virtual, que será la máquina de 'Sergio', e instalamos la herramienta Gpg4Win y generamos también el par de claves.

Quedaría de la siguiente manera

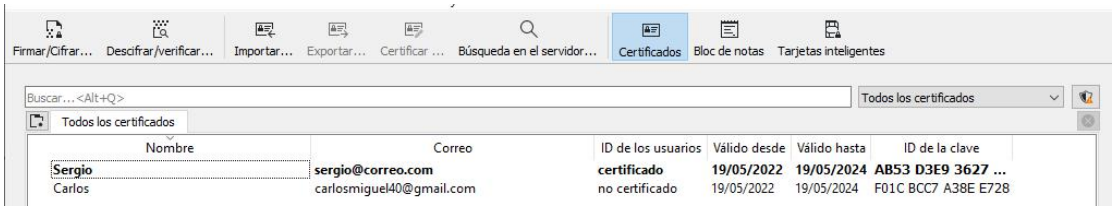


Exportaremos la llave pública (de Sergio) y nos la enviaremos al correo.

Nos vamos a la máquina de 'Carlos', descargamos el archivo (clave pública de Sergio) y hacemos doble click sobre el mismo.
Nos saldrá la siguiente ventana que nos indica que hemos importado la clave pública de 'Sergio'.

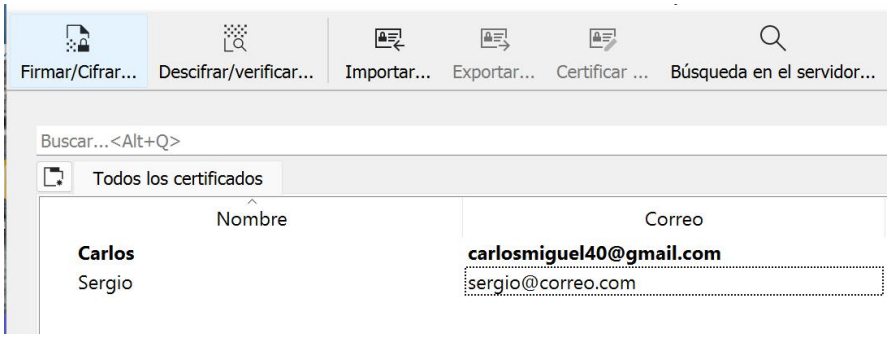
Carlos	**carlosmiguel40@gmail.com**	**certificado**	**19/05/2022**	**19/05/2024**	**F01C BCC7 A38E ...**
Sergio	sergio@correo.com	no certificado	19/05/2022	19/05/2024	AB53 D3E9 3627 5C...

De la misma manera lo haremos en la máquina de ‘Sergio’, quedando como se ve a continuación.

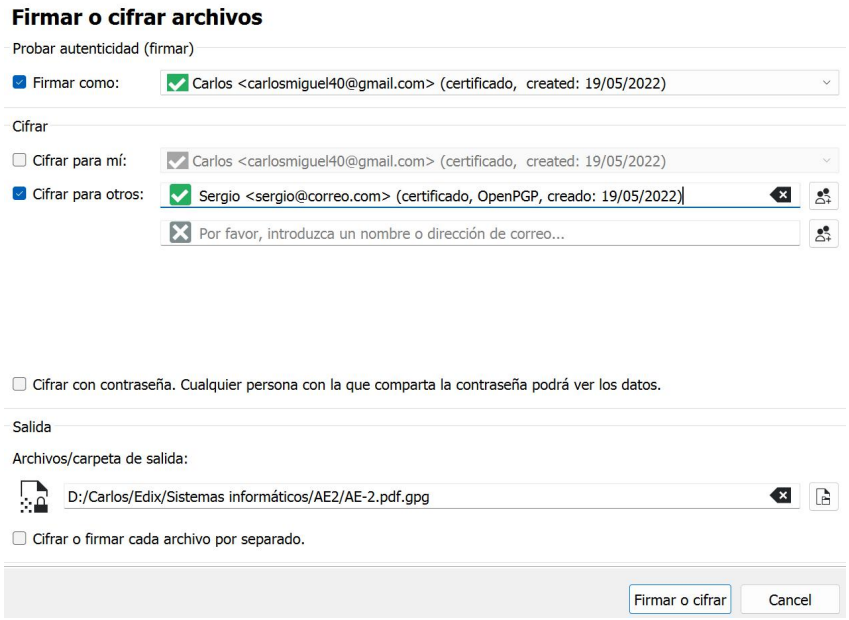


El siguiente paso es cifrar un documento, para esta prática usaremos el documento PDF de la AE-2.

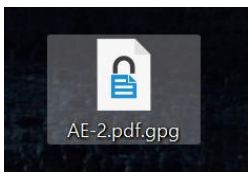
Entramos a la máquina de ‘Carlos’ y hacemos click en el botón Firmar/cifrar



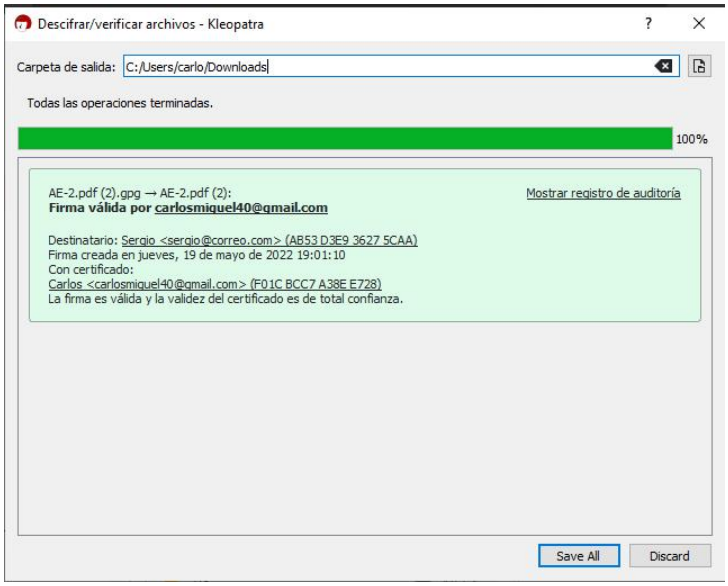
Elegimos el archivo que queremos cifrar y en el apartado de ‘Firmar como’ colocamos el certificado de ‘Carlos’ y en el apartado de ‘Cifrar para otros’ colocamos el certificado que hemos importado de ‘Sergio’ y hacemos click en ‘Firmar/cifrar’



Nos aparecerá un archivo como este.



Ahora le enviamos este archivo encriptado a la máquina de ‘Sergio’
De vuelta a la máquina de ‘Sergio’, descargamos el archivo encriptado y hacemos click derecho y seleccionamos la opción ‘descifrar y verificar’ y se nos abrirá una ventana con la siguiente información.



Hacemos click en ‘Save all’ y ya tendremos nuestro archivo desencriptado.