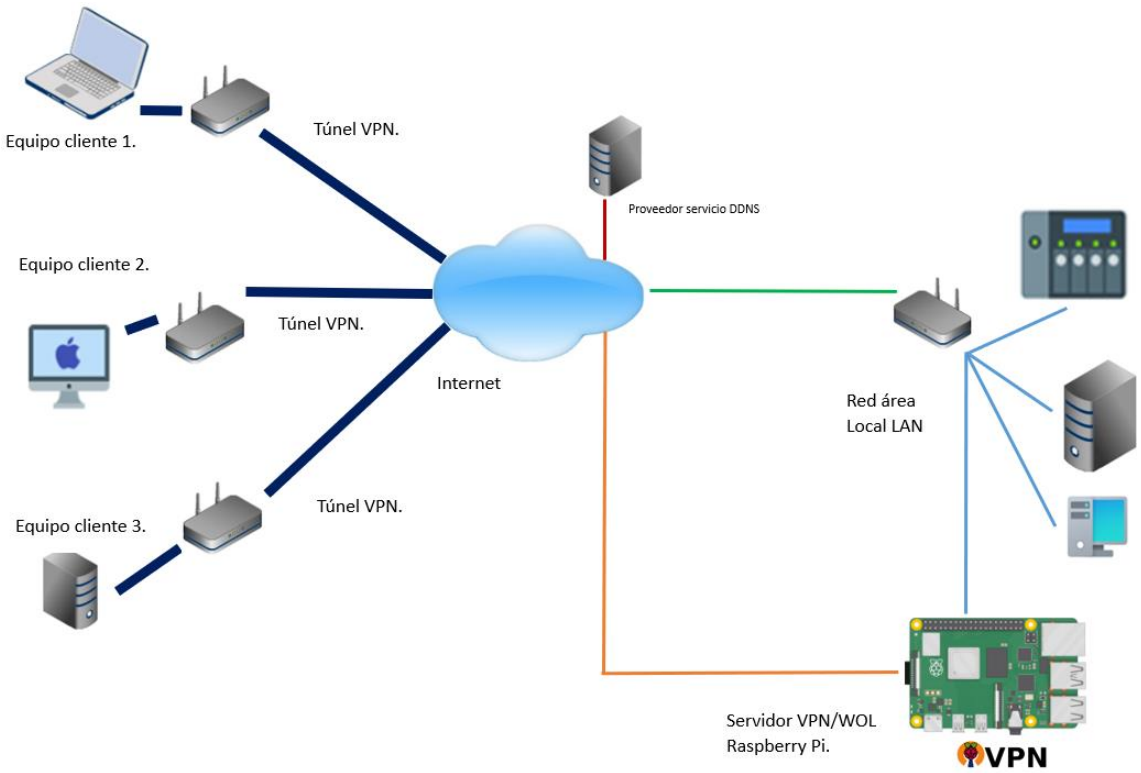


VPN WOL

Proyecto CFGS ASIR Miguel Ángel Sierra Bustos M@SB PiVPN & WOL

Miguel Ángel Sierra Bustos

Índice de contenido

Introducción. 9

Agradecimientos. 11

Consideraciones previas. 13

Tecnologías utilizadas. 18

VPN. 18

Protocolos de seguridad para garantizar la autenticación. 19

Tipos de VPN. 19

OpenVPN. 21

PiVPN. 23

DDNS. 25

Wake On LAN. 27

WEBMIN. 29

RDP. 30

SSH. 32

UFW. 33

Xming. 34

XQartz. 35

Caso práctico proyecto PiVPN y Wake On LAN WOL. 36

iPad caso práctico proyecto PiVPN y Wake On LAN WOL. 37

Windows caso práctico proyecto PiVPN y Wake On LAN WOL. 46

MacOS caso práctico proyecto PiVPN y Wake On LAN WOL. 65

Linux caso práctico proyecto PiVPN y Wake On LAN WOL. 74

Creación de cuenta gratuita en proveedor de servicio DDNS. 87

Creación nombre de dominio en proveedor de servicios de DNS. 92

Configuración proveedor de servicio DDNS NO-IP en Router. 98

Apertura de puertos en Router. 105

Preparación Tarjeta microSD. 114

Preparación en Sistema Operativo Apple macOS. 114

Descarga e instalación de la aplicación Raspberry Pi Imager. 114

Descarga del fichero imagen del S.O. Raspberry Pi OS. 119

Preparación e instalación del S.O. en la tarjeta microSD. 123

Preparación en Sistema Operativo Linux. 133

Descarga e instalación de la aplicación Raspberry Pi Imager. 133

Descarga del fichero imagen del S.O. Raspberry Pi OS. 139

Preparación e Instalación del S.O. en la tarjeta microSD. 142

Preparación en Sistema Operativo Windows. 151
Descarga e instalación de la aplicación Raspberry Pi Imager. 151
Descarga del fichero imagen del S.O. Raspberry Pi OS. 155
Preparación e Instalación del S.O. en la tarjeta microSD. 159

Primer arranque Raspberry Pi. 169

Primer inicio configuración Raspberry PI. 175

Primer inicio y asistente de configuración. 175

Asistente de configuración gráfico Raspberry Pi. 181

Asistente de configuración en terminal. 188

Instalación parte servidor. 199

Instalación local. 199
Instalación NO-IP. 199
Instalación PiVPN. 207
Instalación aplicaciones necesarias a través de terminal en local. 234
Instalación WEBMIN. 238
Instalación aplicación TeamViewer en Raspberry Pi. 242
Activación instalación VNC. 249
Activación instalación SSH. 251
Habilitar X11Forwarding. 253
Fichero configuración servicio SSH. 255
Habilitar tráfico en cortafuegos Linux ufw. 257

Instalación remota vía SSH. 261
Conexión vía SSH. 261
Instalación PiVPN a través de SSH. 265
Instalación WEBMIN vía SSH. 276
Instalación aplicaciones necesarias vía SSH. 281
Configuración Raspberry Pi vía remota a través de SSH. 285

Creación usuarios conexión remota PiVPN. 292

Envió de los ficheros de configuración OVPN creados por correo. 296

Instalación parte cliente. 298

Descarga e instalación aplicación OpenVPN. 298
Descarga en S.O. Apple macOS. 298
Instalación en S.O. Apple macOS. 300
Descarga e instalación en S.O. Linux. 305
Descarga e instalación en S.O. Windows. 306
Descarga en S.O. Windows. 306
Instalación en S.O. Windows. 308

Importación ficheros OVPN configuración conexión aplicación OpenVPN. 312
Importación en S.O. macOS. 312
Importación en S.O. Windows. 317
Importación en S.O. Linux. 322

Descarga instalación configuración y conexión Microsoft Remote Desktop y remmina. 328

Instalación y configuración aplicación XQuartz en S.O. macOS. 347

Descarga e instalación aplicación Xming en S.O. Windows. 355
Descarga e Instalación PuTTY en S.O. Windows. 362
Descarga instalación y configuración aplicación RealVNC. 384
Configuración creación fichero arranque equipos wakeonlan local. 414
Configuración creación fichero arranque Gwakeonlan Linux local. 417
Creación fichero arranque equipos en terminal remoto. 419
Creación fichero arranque equipos entorno gráfico Linux remoto. 425
Wake On LAN (WOL) 432
Habilitar Wake On LAN en equipo MSI Gaming Trident 3. 433
BIOS. 433
S.O. Windows opciones de energía. 436
Configuración tarjeta de red S.O. Windows. 438
Habilitar Wake On LAN en equipo Intel NUC. 441
BIOS. 441
S.O. Windows opciones de energía. 443
Configuración tarjeta de red S.O. Windows. 445
Habilitar Wake On LAN en placa base ASUS. 448
Habilitar Wake On LAN en placa Gigabyte. 450
Habilitar Wake On LAN en NAS QNAP. 451
Problemas, errores. 454
Ejecución PuTTY. 454
Error al acceder a través de SSH. 455
Problema con RealVNC. 460
ANEXO 462
Conexión remota vía SSH. 462
Conexión a través de terminal. 462
Conexión a través de la aplicación PuTTY S.O. Windows. 466
Configurar o habilitar tráfico en cortafuegos Linux ufw. 470
Actualización renovación nombre de domino o host proveedor servicios DDNS. 474
Comprobación usuarios conectados y su estado en servidor PiVPN. 478
Posibilitar configuración fichero OpenVPN cliente Linux Debian. 479
Habilitar conexión remota en cliente S.O. Windows. 481
Averiguar dirección IP y dirección física MAC. 486
S.O. Windows. 486
S.O. Linux. 487
S.O. Apple macOS. 489
Facturas de dispositivos. 490
Dispositivos básicos ..... ¡Error! Marcador no definido.

Fichero noip.sh **496**
Fichero script instalación pivpn. **497**
Fichero sshd_config en /etc/ssh. **498**
Ficheros configuración servidor OpenVPN. **501**
Desinstalación PiVPV. **502**
Desinstalación No-IP, noip-duc. **503**
Desinstalación aplicaciones en servidor Raspberry Pi. **504**
Wake On LAN en equipos con S.O. Linux. ***505***
Bibliografía. ***508***
Raspberry Pi. **508**
VPN. **508**
OpenVPN. **508**
PiVPN. **508**
DDNS. **508**
Wake On LAN. **508**
WEBMIN. **509**
RDP. **509**
SSH. **509**
UFW. **509**
Xming **509**
Xquartz. **509**

Introducción.

Todas las imágenes que aparecen a fecha de creación de este documento y todas las que engloban este proyecto, pueden cambiar o ser diferentes/modificadas en las aplicaciones sin previo aviso, pudiendo estas sufrir alguna actualización añadiendo o quitando alguna funcionalidad por parte de los desarrolladores.

Todos los datos proporcionados se encuentran sujetos a posibles variaciones sin previo aviso como ciertos datos incluidos, que al ser trascripciones pueden incluir sin querer algún tipo de error tipográfico.

Ciertos datos como cuentas de correo electrónico han sido creadas y utilizadas para la creación de este proyecto y su documentación, no se utilizarán para prestar soporte de ningún tipo.

El planteamiento de esta solución, que se desarrollara más adelante y aunque es o empezó siendo para un uso privado, es ideal para una pequeña empresa en la que se quiera poder realizar conexiones externas a través de protocolos como VPN, SSH, RDP y simplificar el poder conectar desde cualquier parte fuera de la red interna, conectándonos a esta red desde el exterior y poder iniciar o “encender/arrancar” un ordenador, conectarnos a él y poder utilizar los recursos de la red desde el exterior de esa red, como si estuviésemos en esa misma red.

Este proyecto, que como se indicó nace para poder vigilar en el ámbito privado, permitiendo el encendido de un ordenador y la activación de una Web Cam, se realiza para solventar la problemática y la poca colaboración por no decir ninguna, por parte de los Proveedores de Servicios de Internet (ISP), los cuales no facilita ninguna ayuda ni dispositivo (router) que permita realizar Wake On LAN (WOL), aunque pueda parecer para alguien un poco matar moscas a cañonazos, como se me indico en un post, al consultar con el proveedor de mi servicio de Internet, si, esa fue la contestación “matar moscas a cañonazos”, para mí ha sido gratificante con las pocas indicaciones que se me indicaron lo que he logrado, conectar a la red desde cualquier dispositivo ya sea un ordenador, un móvil, una tablet y una combinación de estos como una Tablet conectada a través de un móvil o un ordenador conectado a un móvil, otras soluciones pasan por conectar dos routers con el consiguiente gasto de electricidad o incluso un router que permita Wake On LAN y en este caso disponga de fibra óptica, este último con un precio algo elevado, este proyecto permite la conexión desde cualquier lugar, siendo una manera no muy costosa para solventar la problemática de poder arrancar remotamente un ordenador.

Desafortunadamente, no hace mucho, cobra más relevancia si cabe el uso de conexiones VPN, y aunque no parecía que estuviésemos preparados para el trabajo de forma remota, hasta que no hemos sufrido una desgracia como la que recientemente hemos sufrido a nivel global, y más concretamente donde el 14 de marzo de 2020, cuando en España el gobierno decreto el estado de alarma en todo el territorio nacional, amparado en esta medida, cuyo resultado fue un confinamiento de la población en sus lugares de residencia, limitándose la libre circulación de los ciudadanos a actos esenciales entre ellos adquisición de alimentos, medicamentos, acudir a centros médicos o al lugar de trabajo y más tarde, el 28 de marzo de ese mismo año, se suspendió toda actividad laboral presencial no esencial durante quince días. El Congreso de los Diputados fue autorizando sucesivas prórrogas del estado de alarma hasta un total de seis veces.

Pues sí, parece que si se estaba preparado, aunque las empresas tuvieron que reaccionar rápido, si se estaba preparado para el teletrabajo en este país y en el resto del mundo, siempre hablando de trabajos que lo permitan.

Intentare en todo el documento, poder aclarar ciertos datos o conceptos técnicos en la medida de lo posible, explicar todo con palabras más llanas y simples, como para que una persona sin muchos conocimientos técnicos informáticos sea capaz de realizar todos los pasos y llevar a buen término sino todo, lo que cada cual necesite, de todo lo que aquí se va a documentar y explicar.

Aunque como se puede observar hay gran cantidad de páginas, no es necesario la lectura de todo el documento, puesto que se explica de una manera estructurada la instalación parte servidor y su configuración en un S.O. (Sistema Operativo) Linux, siendo este el que utiliza una Raspberry Pi, como la parte cliente instalación y configuración de las aplicaciones necesarias para todo lo que se muestra en este documento, por lo que dependiendo del S.O. cliente que se use, se seguirán los pasos para este y se podrán desechar si se quiere las explicaciones del resto.

Como no, pedir disculpas si por el poco tiempo en la preparación de toda la documentación, se han cometido algunas faltas de ortografía, se ha olvidado la integración de algún paso decisivo, o se repite alguna explicación.



Agradecimientos.

Principalmente, a mis familiares más cercanos como mis padres José, Dolores y mis hermanos José y Jorge, también y no quiero olvidarme de ellos a mis compañeros de estudios de grado medio en el IES Palomeras Vallecas Javier, Krastin, Sergio, Eduardo, Tiberiu, David, Carlos, profesores de este instituto como Raquel, Mario, Eduardo, Iván, compañeros de estudios de grado superior en el IES Vista Alegre como Javier, Álvaro, Alejandro, Juan, Andrés e Iván, no quiero olvidarme de mis compañeros de trabajo Manuel Navarro, Rafael, Jorge, Javier, Álvaro, Candela (Cande), Fernando, Lolo, Ángel, Lidia, Iván, Daniel, Raúl, un nuevo Daniel, Pablo, José Miguel (Josemi), Jonathan, Gines, Adrián, Ney, Carlos, Gonzalo, Noe, Raquel, Raquel si, es otra Raquel, Miguel, Rubén, otro Rubén, Asier, en estos últimos años a José Ramon, Miguel Ángel, Juan Carlos, otro nuevo Rubén, Pedro y otros tantos principalmente, aunque seguro que se me olvidan algunos, les pido disculpas, por desgracia, todos o alguno puede que hayan tenido muy a pesar mío que aguantar o sufrir algunos momentos de estrés en ciertos momentos por la ansiedad a la hora de realizar mis estudios y encontrarme trabajando, mis más sinceras disculpas si en algún momento lo han pasado mal por culpa mía.

Puedo decir que, aun así, ha sido una etapa de mi vida muy enriquecedora, estar estudiando y poder ayudar a gente tan joven con la que he tenido el gusto de poder coincidir en mis primeros años de estudios, como estos últimos, sinceramente es una experiencia muy gratificante y aunque en ciertos momentos agotadora y estresante la recomiendo.

Mi agradecimiento especial a mi compañero de trabajo Jonathan García Rodríguez (Jonh DelBoy), por prestarme desde que realice mis estudios de grado medio dos canciones para poder realizar y presentar los videos, creados y presentados a mi profesor Eduardo en el módulo de Servicios en el instituto IES Palomeras Vallecas.

“Jonh DelBoy - Travel To The Sun [Progressive House Mix]”

https://soundcloud.com/jonhdelboy

A todos ellos, y a los que posiblemente haya olvidado mencionar en los agradecimientos y ellos saben que las merecen, gracias y mil gracias, por aguantarme en esta etapa en la que he sufrido lo indecible para poder sacar mis estudios.

Se comienza el desarrollo de este proyecto exponiendo con un pequeño resumen explicativo de las tecnologías utilizadas para pasar a las explicaciones prácticas de las instalaciones y/o configuraciones de los programas en diferentes Sistemas Operativos (S.O.), por lo que no es necesaria la lectura integra del presente documento, es más bien una guía para realizar el proyecto, dependiendo del S.O. del que se disponga en los equipos cliente, se tendrá que seguir los pasos para realizar la instalación y configuración de las aplicaciones en ese S.O., mientras que en la parte servidor al tratarse de una Raspberry Pi, o se utiliza un mismo dispositivo Raspberry Pi modelo 3 o 4 o en su defecto se puede utilizar como servidor VPN/WOL un equipo de escritorio en el que su S.O. sea una distribución de Linux, se ha probado a realizar dichas instalaciones en distribuciones derivadas de Debian como Ubuntu y en el propio Debian, pudiendo realizar todas las instalaciones con más o menos trabajo de las aplicaciones en el equipo de escritorio que haría de servidor, mencionar que las instalaciones de la parte servidor también han sido probadas a ser instaladas en máquinas virtuales con el S.O. Ubuntu y Debian, siendo el resultado satisfactorio, pudiendo llevar a cabo las instalaciones también con más o menos trabajo.

Consideraciones previas.

Las explicaciones u expresiones que se utilizan en este proyecto, no serán todo lo rigurosas que para una persona con conocimientos o conocimientos avanzados de informática pudiera desear, se crea esta documentación para facilitar la comprensión a las personas que no dispongan de esos conocimientos, por lo que puede que las explicaciones expuestas en este documento no sean tan rigurosas y con tantos tecnicismos como debiera.

Todas las imágenes que aparecen a fecha de creación de este documento y todas las que engloban este proyecto, pueden cambiar o ser diferentes/modificadas en las aplicaciones sin previo aviso, si estas sufren alguna actualización añadiendo o quitando alguna funcionalidad por parte del o los desarrolladores.

Todos los datos proporcionados se encuentran sujetos a posibles variaciones sin previo aviso como ciertos datos incluidos, que al ser trascripciones pueden incluir sin querer algún tipo de error tipográfico.

Para este proyecto se ha seleccionado ciertas versiones de las aplicaciones a utilizar por su facilidad de instalación, lo que ha conllevado la necesidad de instalar un cierto Sistema Operativo (S.O.) en la Raspberry Pi, como posteriormente se podrá observar, todo ello para facilitar la labor a cualquier persona sin muchos conocimientos técnicos de informática.

Este procedimiento que se escribe a continuación, puede realizarse la parte servidor en una Raspberry Pi modelo 3 o 4 con S.O. Raspberry Pi OS (RasPi OS), equipos físicos, máquinas virtuales con S.O. Linux, distribuciones Linux como Debian, Ubuntu, las aplicaciones PiVPN, No-IP y demás aplicaciones, están disponibles para distribuciones Linux y derivados de RedHat como Centos, no habiendo probado las instalaciones en estas distribuciones, respecto a la parte cliente, las aplicaciones pueden ser instaladas en equipos con S.O. Windows como PuTTY, Xming, Escritorio remoto de Microsoft, Microsoft Remote Desktop, ciertas aplicaciones solo se encuentran disponibles para macOS como XQuartz, y otras solo se pueden instalar en equipos con S.O. Linux como vinagre, remmina, WEBMIN, PiVPN y otras tantas.

Ciertos datos como cuentas de correo electrónico que han sido creadas y utilizadas para la creación de este proyecto y su documentación, no se utilizarán para prestar soporte de ningún tipo.

El nombre de dominio o host que se crea en este caso en el proveedor de servicios DDNS No-IP, al ser en este proyecto una cuenta gratuita, cada 30 días habrá que actualizarlo/renovarlo, se recibirá un correo en la cuenta utilizada para realizar la actualización/renovación, se explica los pasos a seguir para llevar a buen término este proceso.

Quiero mencionar, que se ha intentado utilizar tanto en la instalación de la parte servidor como en la instalación de la parte cliente aplicaciones que no precisan compra siendo estas de uso gratuito, o si tienen coste como TeamViewer, para uso personal no conlleva coste.

Cabe destacar, que en el proyecto se intenta explicar de una forma clara el uso de aplicaciones de control remoto como algo de administración, usando para ello todas las aplicaciones que, en mi dilatada carrera tanto de estudios, como hobby**,** o incluso como en el desempeño de mi trabajo, he llegado a usar, por ello para la conexión vía remota, no explico solo un posible método de conexión, sino varias formas para poder establecer la conexión remota si por algún motivo una falla.

Por último y antes de comenzar, hay que explicar que en las distribuciones de S.O. Linux, al tratarse de un sistema multiusuario y multiplataforma, por seguridad para realizar ciertas tareas como actualización de la lista de repositorios comando apt-get update, instalación de aplicaciones comando apt-get install “nombre_aplicación”, es necesario realizar estas y otras labores de “administración” como consultar el estado iniciar, parar o reiniciar un servicio comando por ejemplo systemctl status ssh, con los privilegios del usuario administrador o superusuario (root), por eso se coloca delante de los comandos indicados la palabra sudo, este usuario administrador suele ser por defecto el usuario con el que se crea o se realiza la instalación del Sistema Operativo (S.O.), en este proyecto se utiliza el usuario pi, aun así, por seguridad, cuando se ejecutan comandos administrativos incluyendo sudo, se solicitará la contraseña de este usuario, tras facilitarse la contraseña el comando se ejecutará, con los comandos puestos como ejemplo anteriormente estos serian.

```
sudo apt-get update
sudo apt-get install “nombre_aplicación”
sudo systemctl status ssh
```

De ahí, que en ciertas líneas del documento no empiecen con la letra en mayúsculas, ni terminen en punto, no se trata de faltas de ortografía es más que nada para dejar claro el comando, puesto que en Linux hay que tener claro que diferencia entre mayúsculas y minúsculas, hay que escribir correctamente comandos y sus opciones.

Puede que una vez dentro de un terminal, al ejecutarse un comando administrativo con sudo, tras autenticarnos y volver a realizar otra labor administrativa ya no se nos solicite contraseña.

Se puede y no se explicará a utilizar su, (comando que permite hacer un salto de usuario, se mantendrá en el terminal como root hasta escribir exit, cuando se saldrá del usuario root), o añadir el usuario a sudoers.

En macOS, al ser un S.O. Unix, este funciona de una forma similar a Linux, pudiendo variar algo en algunos comandos.

En Windows, por ejemplo, se hace uso de Control de Cuentas de Usuario o UAC.

El porqué de este orden de instalación sugerido en este proyecto.

- La creación de la cuenta y el nombre de dominio o host en un proveedor de servicios DDNS, es imprescindible para poder llevar a cabo las instalaciones o administración vía conexión remota.

- La apertura de los puertos en el router y en caso de elegir configurar el servicio DDNS en el router, en este punto si no todos los puertos, por lo menos el de conexión vía SSH habrá que habilitarlo para poder conectar vía SSH remotamente a la Raspberry Pi, además de habilitar el tráfico de datos en el cortafuegos.

- Para poder disponer del servidor en este caso la Raspberry Pi, es necesario preparar, insertar, iniciar y configurarla la tarjeta microSD como posteriormente el S.O. del servidor VPN/WOL.

- Tras la preparación del servidor VPN/WOL y en caso de querer realizar la instalación de las aplicaciones necesarias remotamente, es imprescindible tener configurado el servicio DDNS en el router o en caso contrario, realizar la instalación del cliente DDNS del proveedor del que se disponga.

- Otra cosa muy importante, es que habrá que habilitar el tráfico de datos en el cortafuegos de los protocolos y números de puertos que se utilicen.

- Instalación de las aplicaciones necesarias en la parte servidor.

    - Localmente.
        - Se podrá realizar todas las acciones e instalaciones.
    - Remotamente, vía SSH, será necesario para poder establecer la conexión.
        - Creación cuenta y nombre de dominio o host proveedor DDNS.
        - Apertura del puerto necesario en el router.
        - Configuración servicio DDNS en router, servidor Raspberry Pi o en un equipo cliente si se puede esto último.

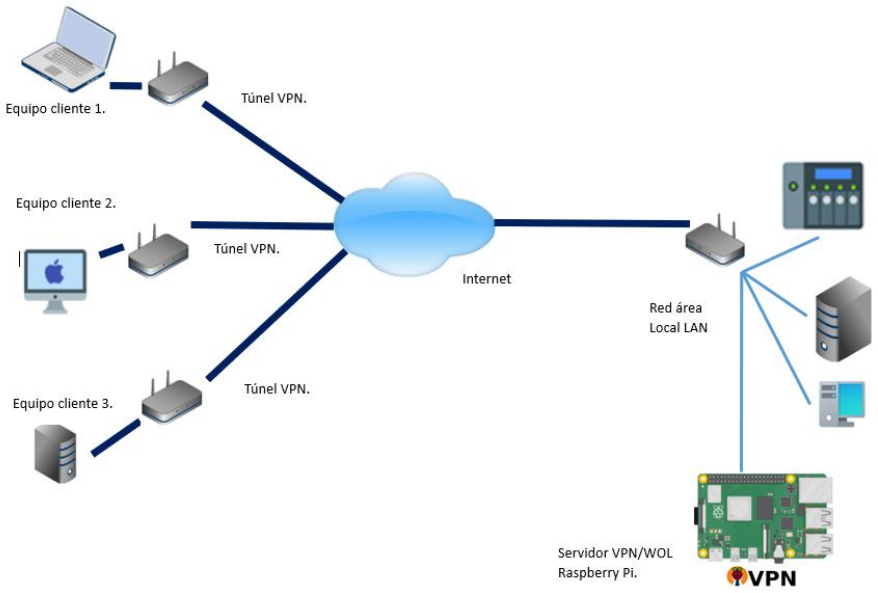
- Posteriormente, las instalaciones o configuraciones que se hagan en el servidor VPN/WOL, se podrán realizar local o remotamente, instalaciones como el software de aplicaciones necesarias, configuración de estas o del propio servidor VPN/WOL.

- Instalaciones en clientes, se podrá decidir cómo realizar la instalación y configuración en los equipos clientes, las indicaciones que se detallan son una mera sugerencia.

Llegado a este punto, y sin más dilación como diría un compañero de trabajo, comienzo a explicar y desarrollar todo el proceso de este proyecto, muchas gracias por la atención prestada.

Tecnologías utilizadas.

VPN.



Virtual Private Network, Red Privada Virtual.

Tecnología que permite extender de forma segura una red de área local (LAN, Local Area Network, Red de Área Local, red de una oficina o residencia), esta se extiende sobre una red pública y no segura como lo es Internet, permitiendo que un ordenador por ejemplo ubicado en la LAN (Red de Área Local, red oficina o residencia), se comunique enviando o recibiendo datos con otro ubicado fuera de esta red LAN, como si se tratase de la misma red privada (LAN), con las mismas funcionalidades, políticas de gestión y seguridad.

“Permite establecer una conexión segura y encriptada entre dispositivos a través de una red pública como Internet”.

Establecida la conexión, se crea un “Túnel VPN” virtual, de extremo a extremo, de equipo a equipo, este túnel cifrado proporciona privacidad y seguridad protegiendo los datos transmitidos.

Los datos a enviar a través de una red pública como Internet, hay que evitar que puedan ser leídos en caso de ser interceptados, por lo que además de la identificación del usuario para evitar el acceso a aquellos no autorizados, estos datos han de cifrarse, para esta tarea se usan algoritmos de cifrado simétrico como DES, 3DES o AES (Advanced Encryption Standard, en sus opciones AES128, AES192 o AES256) que únicamente pueden ser leídos por el emisor y receptor.

Protocolos de seguridad para garantizar la autenticación.

La elección del protocolo dependerá de los requisitos de seguridad, compatibilidad con dispositivos y sistemas operativos, y las políticas de seguridad de la organización. Habrá que evaluar las necesidades antes de seleccionar el protocolo para una implementación de VPN.

- Autentificación/autorización, verificación de quien está al otro extremo y cuál es el nivel de acceso que debe tener.
- Integridad, usando funciones de Hash, siendo estos algoritmos de hash los más comunes Message Digest (MD2 y MD5) y Secure Hash Algorithm (SHA), de esta forma se asegura que los datos enviados no han sido alterados.
- Confidencialidad/privacidad, con el uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES), la comunicación solo puede ser interpretada por el destinatario.
- No repudio, un mensaje tiene que ir firmado, quien envió firmado el mensaje no puede negar que lo envió.
- Control de acceso, habrá que asegurar que los usuarios autentificados solo tienen acceso a los datos a los que están autorizados.
- Auditoría y registro de actividades, asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio, asegurando un buen rendimiento, sin degradación en la velocidad de transmisión.

Tipos de VPN.

En la actualidad existen diferentes tipos de VPN, estos que se indican son algunos de los principales utilizados, los cuales se utilizan en diferentes escenarios y entornos. Cada tipo tiene sus propias características y casos de uso específicos.

- Acceso remoto (Remote Access VPN).
  Permite a los usuarios acceder de forma segura a una red privada desde ubicaciones remotas a través de Internet. por ejemplo, empleados conectando con la empresa remotamente usando una red pública como Internet para establecer la conexión, una vez conectado y al autentificarse es como si se encontrase en la red de área local de la empresa.

- Sitio a sitio, o VPN de red a red.
  Permite la conexión segura entre dos redes privadas separadas geográficamente. Estableciéndose un túnel VPN entre los enrutadores de las dos redes, permitiendo que los recursos y servicios de una red sean accesibles desde la otra red. Es utilizado por organizaciones para conectar sucursales o sitios dispersos geográficamente.

- VPN de acceso dedicado.
  En este caso el proveedor de servicios de red (ISP) ofrece una conexión VPN dedicada a un cliente. El ISP establece y mantiene la conexión VPN entre la ubicación del cliente y la red privada.

- VPN over LAN, (VPN sobre LAN), variante del "acceso remoto", en vez de utilizar Internet como medio de conexión, emplea la red de área local (LAN) de la empresa. Permite aislar zonas y servicios de la red interna, permite mejorar las prestaciones de seguridad de las redes inalámbricas (WIFI).

- VPN de capa 2, VPN de puente.
  Extiende una red local (LAN) a través de Internet, creando una conexión virtual entre dos sitios de manera que parezca que están en la misma red física.
  Se usa cuando se necesita unir dos redes locales geográficamente separadas como si estuvieran en la misma red física.

- VPN de capa 3, VPN de enrutamiento.
  Basada en protocolos de enrutamiento, permitiendo a las redes comunicarse entre sí utilizando Internet como medio de transporte.
  Los paquetes de datos se enrutan a través de túneles VPN desde la ubicación de origen hasta la ubicación de destino.

OpenVPN.

Solución de conectividad basada en software libre, SSL (Secure Sockets Layer), ofrece conectividad punto a punto, protocolo de tunelización.

Según la WEB oficial, es un proyecto de código abierto. Aunque no es sólo eso.

- Proyecto de código abierto al que llaman, Community Edition.
  - Proyecto de red privada virtual (VPN).
  - Conexiones seguras a través de Internet con protocolo de seguridad personalizado utilizando SSL (Secure Sockets Layer)/TLS.
  - Utiliza licencia GPL.
  - Respaldo de colaboradores de OpenVPN Inc., desarrolladores y de la comunidad extendida de OpenVPN.
  - Implementación CE gratuita, aunque requiere conocimientos de Linux y el uso de la interfaz de línea de comandos.

- Protocolo de tunelización.
  - Utiliza el protocolo de encriptación Secure Socket Layer (SSL).
  - Encriptación AES-256, para garantizar privatización datos compartidos a través de Internet.
  - Disponibilidad del código para auditorías.
    - (cualquiera puede encontrar y corregir vulnerabilidades).
  - Protocolo de tunelización de VPN más seguro.
  - Ofrece conexiones más rápidas.
  - Puede eludir la mayoría de los cortafuegos.

Beneficios.
Tunelización.

- Cualquier subred IP o adaptador Ethernet virtual a través de un único puerto UDP, (protocolo de datagramas de usuario) o TCP, (protocolo de control de transmisión).
- Redes públicas con extremos dinámicos, DHCP o clientes de acceso telefónico.
- Redes a través de cortafuegos, orientados a conexión, sin uso de reglas explicitas de cortafuegos.
- Redes sobre NAT (traducción de direcciones de red).

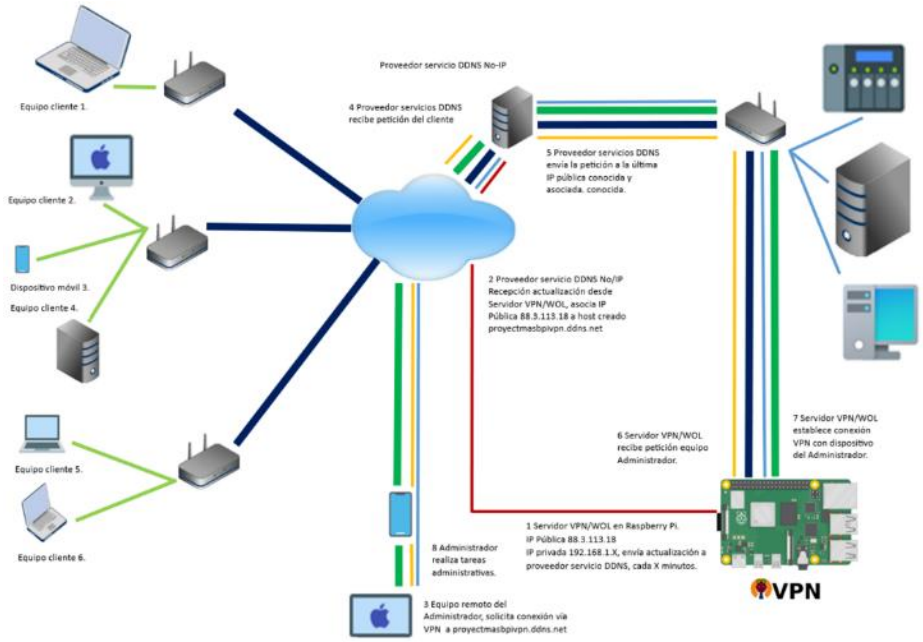
Soporte.

- Todas las características de encriptación, autenticación y certificación de la biblioteca OpenSSL.
- Cualquier cifrado, tamaño de clave o resumen HMAC, compatible con la biblioteca OpenSSL.
- Claves estáticas previamente compartidas o intercambio dinámico de claves basado en TLS.
- Compresión de enlace adaptable en tiempo real, modelado de tráfico.

Usabilidad.

- Posibilidad se configurar granja de servidores VPN con equilibrio de carga y escalable.
- Permite elegir entre el cifrado convencional, basado en clave estática o el cifrado de clave pública basado en certificado.
- Posibilita la creación de puentes ethernet seguros, utilizando dispositivos TAP virtuales.
- Control de OpenVPN a través de interfaz gráfica (GUI) en Windows o macOS.

PiVPN.



Se trata de un proyecto que utiliza un conjunto de scripts de Shell, (intérprete de comandos S.O. Unix/Linux), desarrollados para convertir una Raspberry Pi™ en un servidor VPN, utilizando dos protocolos gratuitos de código abierto.

- Wireguard
- OpenVPN

Este script, posibilita a un usuario sin muchos conocimientos técnicos informáticos, disponer de una VPN en una pequeña, mediana oficina o residencia, PiVPN utiliza un instalador de un solo comando y facilita la gestión de la VPN con el comando pivpn, todo esto utilizando una Raspberry Pi.

PiVPN es la forma más sencilla, rápida de instalar y configurar un servidor OpenVPN o Wireguard, siendo extremadamente seguro en la Raspberry Pi. Con configuraciones de seguridad reforzadas de forma predeterminada, no siendo en gran medida necesario una guía, puesto que gracias al script de instalación este lo hará prácticamente todo.

Desde este proyecto, se recomienda ejecutar PiVPN en la última imagen del S.O. Raspberry Pi OS Lite en una Raspberry Pi, en una pequeña o mediana oficina como en una vivienda u hogar, para poder acceder a través de VPN a su red desde cualquier ubicación remota no segura y usar Internet de manera segura. Aunque se tiene la posibilidad de usar PiVPN, en cualquier proveedor de VPS en la nube que ejecute Ubuntu o Debian para ayudar a aquellos con ISP no confiables.

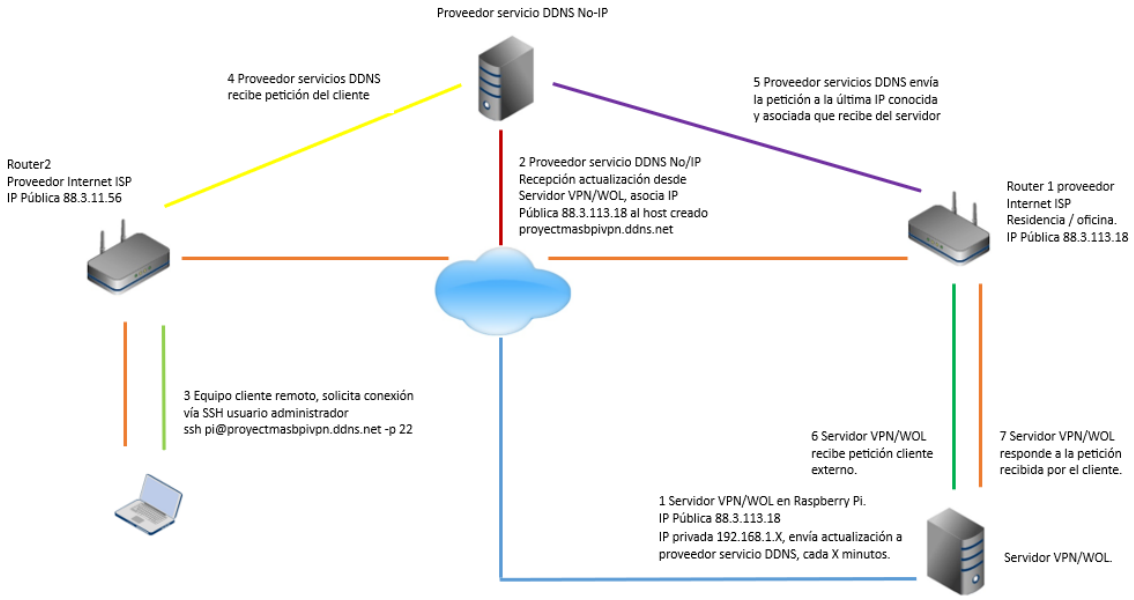
PiVPN, debería funcionar correctamente en la mayoría de distribuciones Linux basadas en Debian y Ubuntu, incluso en las que de forma predeterminada usan el cortafuegos UFW en lugar de iptables sin formato.

PiVPN y sus características.

- Soporta OpenVPN 2.4.
- Soporta WireGuard.
- Claves de cifrado de curva elíptica de hasta 512 bits.
- Se integra con Bitwarden.
- Compatibilidad con llavero iOS.
- Admite múltiples proveedores de DNS.
- Admite servidores DNS personalizados.
- Dominios de búsqueda personalizados (solo OpenVPN).
- Funciona con Pi-Hole®.
- No es necesario una Raspberry Pi™, se ejecuta en cualquier equipo con S.O. Linux basado en distribución Debian o Ubuntu x86_64.
- Admite instalación desatendida, para implementaciones automatizadas.

- Actualizaciones de seguridad automáticas.
- Servidor VPN tipo client to client, permite a los clientes conectados al servicio VPN verse y comunicarse.
- Autentificación TSL, evitando escaneo de puertos para evitar vulnerabilidades y ataque de Denial Of Service (DoS), Denegación de Servicio.
- Servidor OpenVPN client-to-client, por lo que el tráfico entre clientes es gestionado por el servidor openvpn.
- Conexión a servicios de la red desde cualquier lugar.

DDNS.



1. (———), Servidor VPN/WOL en Raspberry Pi. IP Pública 88.3.113.18, IP privada 192.168.1.X, envía actualizaciones de la IP pública al proveedor de servicios DDNS, cada X minutos configurables.
2. (———), Proveedor servicio DDNS No/IP, recibe la actualización desde servidor VPN/WOL, asociando IP Pública 88.3.113.18 al host creado proyectmasbpivpn.ddns.net
3. (———), Equipo cliente remoto, solicita conexión vía SSH usuario administrador ssh pi@proyectmasbpivpn.ddns.net -p 22.
4. (———), Proveedor servicios DDNS recibe petición del cliente.
5. (———), Proveedor servicios DDNS envía la petición a la última IP conocida y asociada que recibe del servidor.
6. (———), Servidor VPN/WOL recibe petición cliente externo.
7. (———), Servidor VPN/WOL responde a la petición recibida por el cliente.

Dynamic (Domain Name System), en español, Sistema de Nombres de Dominio Dinámico.

Servicio que permite asignar un nombre de dominio o host a una dirección IP dinámica asignada a un dispositivo o red.

Al conectarnos a nuestro Proveedor de Servicios de Internet (ISP), lo habitual es que este asigne una dirección IP pública dinámica (dinámica, que puede cambiar), a nuestro router, esta dirección IP es bastante más difícil de recordar y máxime cuando puede cambiar que intentar recordar un nombre de dominio o host para acceder a la red desde Internet.

El servicio DDNS proporciona un servicio de actualización automática de la dirección IP asociándola a un nombre de dominio o host, facilitándonos de esta forma poder conectarnos.

Funcionamiento.

- Es necesario el registro de un nombre de dominio con un proveedor de servicios DDNS.
- Habrá que configurar el router o el S.O. de un equipo cliente o servidor, para que actualice automáticamente la dirección IP asignada por el ISP al proveedor de servicios DDNS.
- El proveedor de servicios DDNS, actualiza la dirección IP asociándola al nombre de dominio cada vez que cambia la IP.
- Al intentar conectar utilizando el nombre de dominio registrado, el proveedor de servicio DDNS redirecciona la solicitud a la dirección IP actualizada.

El servicio DDNS, es especialmente útil para acceder a nuestra red o dispositivo desde ubicaciones remotas y no se dispone de una dirección IP estática.

Wake On LAN.

Wake On LAN (WOL)

Se trata de un estándar de redes de computadoras sobre tarjetas ethernet, permite encender remotamente equipos apagadas.

En la actualidad, se implementa en la placa base del ordenador. La mayoría de placas base modernas incorporan un controlador Ethernet con soporte WOL sin la necesidad de un cable externo. En placas base antiguas, estas disponen de un conector WAKEUP-LINK el cual, debe ser conectado a la tarjeta de red a través de un cable de 3 PIN, en los sistemas con soporte PCI 2.2 junto con una tarjeta de red PCI compatible normalmente no requieren de un cable WOL, siendo provista la energía necesaria por el bus PCI.

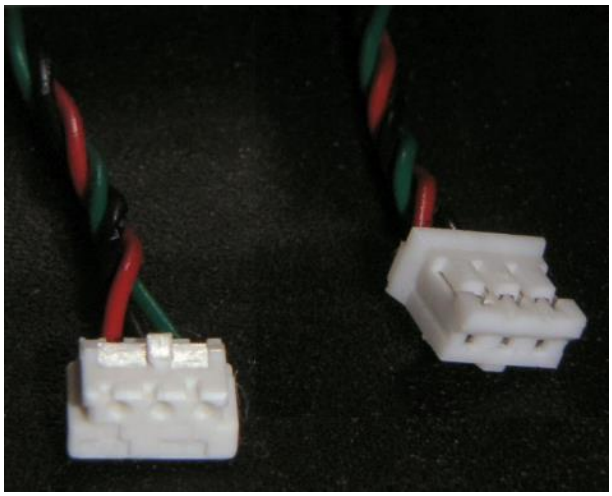


Imagen antiguo cable con conector 3 PIN, para WOL.

Para que esta funcionalidad funcione es necesario ciertas configuraciones.

- Wake On LAN deberá activarse en la configuración de la BIOS de la placa base.
- Puede ser necesario que el ordenador sea configurado para reservar energía para la tarjeta de red al encontrarse apagado.
- Habrá que activar esta característica en la configuración del adaptador de red.
- Así mismo, se tendrá que modificar la opción Activar inicio rápido (recomendado), dentro de las opciones de energía en el S.O.

Habitualmente el paquete mágico se envía como un datagrama UDP al puerto 7 o 9, en la capa de transporte.

Wake-On-LAN está implementado utilizando un paquete llamado "Paquete mágico", este paquete mágico es enviado a todos los equipos de la red, encontrándose entre ellos el equipo a ser encendido. El "paquete mágico" contiene la dirección MAC del equipo destino, que es un identificador numérico que dispone cada tarjeta de Red, que hace posible ser reconocido dentro de la red.

Los equipos que se encuentran apagados y son compatibles con Wake ON LAN, pueden contener dispositivos de red "escuchando" paquetes entrantes en modo de bajo consumo de energía mientras el sistema está apagado. Al recibir un "paquete mágico" y este, está enviado a la dirección MAC del dispositivo en cuestión, la tarjeta de red envía una señal a la fuente de energía o placa base para iniciar el encendido del sistema.

Paquete mágico
Se denomina paquete mágico (magic packet), a una trama de difusión conteniendo esta una cadena de 6 bytes de valor 255 ("FF FF FF FF FF FF" en hexadecimal), seguida de 16 repeticiones de la dirección MAC del ordenador destino. Este paquete transporta un mensaje de red especial, el cual posee la facultad bajo unas condiciones determinadas de activar el equipo al que va dirigido.

Para proceder con el encendido de un ordenador remotamente, la tarjeta de red como la placa base tienen que soportar el servicio Wake On LAN, el procedimiento comienza con él envió de un paquete mágico a la red con la dirección MAC del equipo que se quiere despertar, la tarjeta de red en cuestión reconoce el paquete con la dirección MAC especificada y la tarjeta responde "despertando" el equipo mediante una señal enviada a la placa base del equipo.

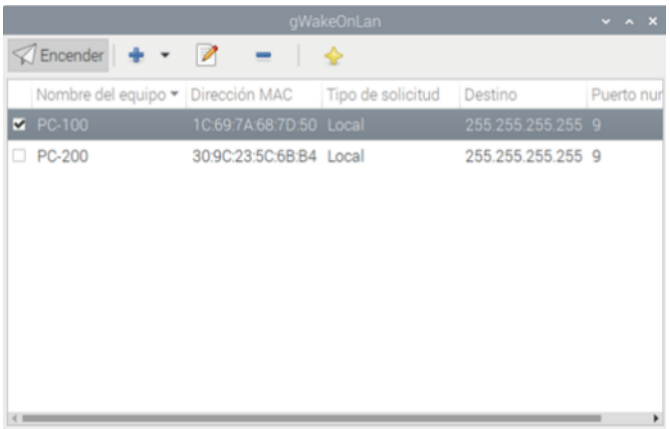
Los ordenadores portátiles con el chipset Intel 3945 o posterior (con soporte BIOS), permiten usar el estándar usando Wireless (IEEE 802.11). Esto es llamado Wake On Wireless LAN (WoWLAN).

Existen múltiples aplicaciones para el S.O. Windows, Linux e incluso WEB´s que nos facilitan realizar Wake On LAN, un ejemplo que se utiliza en este proyecto.

Bajo línea de comando en Linux, captura imagen inferior.

```
wakeonlan 1C:69:7A:68:7D:50
```

Mientras que, si se quiere utilizar la interfaz gráfica, se puede utilizar con la aplicación gWakeOnLan, captura de imagen derecha.



WEBMIN.

Herramienta de configuración de sistemas vía web para sistemas Unix, como GNU/Linux y OpenSolaris. Pudiendo configurar sistemas libres, como el servidor web Apache, PHP, MySQL, DNS, Samba, DHCP, entre otros.

Se trata de un panel de control basado en WEB para administrar servidores Unix/Linux.

Codificado por Jamie Cameron, Webmin está liberado bajo Licencia BSD. Existe también Usermin, siendo esta última la versión reducida del Webmin.

Escrito en Perl versión 5, se ejecuta como su propio proceso y servidor web. Comunicación por defecto a través del protocolo TCP a través del puerto 10000, puede ser configurado para usar SSL si OpenSSL está instalado con módulos de Perl.

Se encuentra construido a partir de módulos, estos módulos disponen de una interfaz a los archivos de configuración y el servidor Webmin. Permitiendo añadir nuevas funcionalidades. Cualquiera puede escribir extensiones al disponer un diseño modular.

Permite el control de varias máquinas a través de una interfaz simple, o incluso iniciar sesión en otros servidores Webmin, siendo estos de la misma subred o red de área local.

RDP.

RDP (Remote Desktop Protocol), Protocolo de Escritorio Remoto.

Protocolo patentado y propietario, desarrollado por Microsoft, proporciona una interfaz gráfica con la que se puede realizar conexiones con otro equipo remoto a través de una conexión de red, para lo que el equipo que realiza la llamada de conexión utiliza el cliente RDP mientras que el que recibe la llamada ejecuta el servidor RDP.

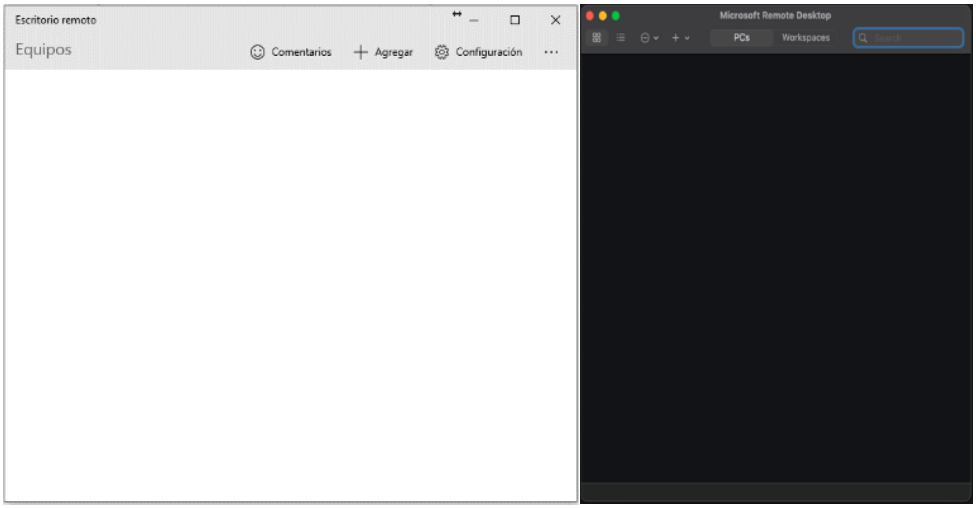
Los servidores RDP se encuentran integrados en los S.O. Windows, existiendo servidor RDP para UNIX y OSX como XRDP, el servidor RDP escucha en el puerto TCP 3389 y UDP 3389 de forma predeterminada.

En la actualidad, existen clientes para una infinidad de S.O. como por ejemplo Microsoft Windows, Windows Mobile para este el soporte por parte de Microsoft ha finalizado, Linux remmina, Unix, macOS, IOS, Android.

Este protocolo es una extensión del protocolo de uso compartido de aplicaciones ITU-T T.128, anteriormente Microsoft le hacía referencia como "Cliente de servicios de terminal" y en la actualidad como Conexión de escritorio remoto.

Entre otras características y sin entrar en las más técnicas son.

- Compatibilidad con colores de 32 bits.
- Cifrado de 128 bits, utilizando el algoritmo de cifrado RC4 , a partir de la versión 6. Compatibilidad con TLS desde la versión 5.2.
- Redirección de audio.
- Redirección del sistema de archivos.
- Compartición entre computadora remota y local del portapapeles.
- Windows sin problemas.
- Programas remotos.
- Terminal Services Gateway
- Autenticación a nivel de red.
- Compatibilidad con la comunicación remota de Aero Glass Theme (o Composed Desktop),
- RemoteFX : RemoteFX proporciona compatibilidad con GPU virtualizada etc.



Ejemplos de aplicación Escritorio remoto de Microsoft, imagen superior izquierda S.O. Windows, imagen superior derecha S.O. macOS.



Imagen superior aplicación remmina S.O. Linux.

SSH.

Secure Shell (SSH), Secure SHell, en español intérprete de órdenes seguro.

Nombre de un protocolo y del programa que lo implementa, permite a los usuarios acceder y administrar de forma segura usando una arquitectura cliente/servidor, servidores remotos a través de un canal seguro en la que la conexión está cifrada.

SSH permite copiar datos de forma segura, gestionar claves RSA, paso de los datos de otras aplicaciones por un canal seguro tunelizado, SSH también puede redirigir el tráfico del Sistema de Ventanas X, pudiendo ejecutar programas gráficos remotamente.

El protocolo por defecto asignado para SSH es el TCP con número de puerto 22, aunque como se explicará se puede modificar.

Su funcionamiento requiere de usuario, puerto y servidor.

- El cliente SSH contacta con el servidor.
- Ese servidor escucha a través del puerto 22 por defecto, o el asignado.
- El servidor envía la clave pública, comenzando la apertura de un canal seguro.
- El cliente inicia sesión, conectándose al servidor.

Versiones de SSH.
SSH 1, La más antigua del protocolo SSH, obsoleta debido a vulnerabilidades de seguridad.
SSH 2, Versión más actualizada y utilizada, proporciona mejoras en seguridad y funcionalidad. SSH 2 es más resistente a los ataques utilizando algoritmos de cifrado y autenticación más fuerte.

Autenticación: SSH admite diferentes métodos de autenticación, incluyendo:

- Contraseña.
- Claves públicas/privadas, se utiliza un par de claves (clave pública y clave privada) para autenticar al cliente y al servidor. El cliente posee la clave privada y el servidor almacena la clave pública correspondiente.
- Autenticación basada en certificados, en lugar de utilizar claves individuales, se utilizan certificados emitidos por una autoridad de certificación (CA) para autenticar al cliente y al servidor.

UFW.

Uncomplicated Firewall (ufw), (UFW - Cortafuegos sin complicaciones).

Se trata de un cortafuegos GNU/Linux, escrito en Python es el firewall predeterminado para Ubuntu, diseñado para facilitar la configuración del cortafuegos de iptables, usando un pequeño número de comandos simples, basado en host IPv4 o IPv6.

Ufw es un cortafuegos que se utiliza bajo línea de comandos dentro de un terminal, existiendo una versión con interfaz gráfica siendo esta Gufw.

Más información en la WEB oficial.

https://help.ubuntu.com/community/UFW

Xming.

Es una implementación portátil del sistema de ventanas X para los S.O. Microsoft Windows, este servidor está basado en el servidor X.org.

Se encuentra disponible con soporte Mesa 3D, soporta múltiples lenguajes, al contrario que Cygwin/X, Xming no requiere de bibliotecas Cygwin.

Se usa en implementaciones de Secure Shell (SSH), asegurando sesiones X11 en equipos remotos, soporta PuTTY, SSH y tiene una versión del plink.exe de PuTTY.

XQartz.

URL: https://support.apple.com/es-es/HT201341

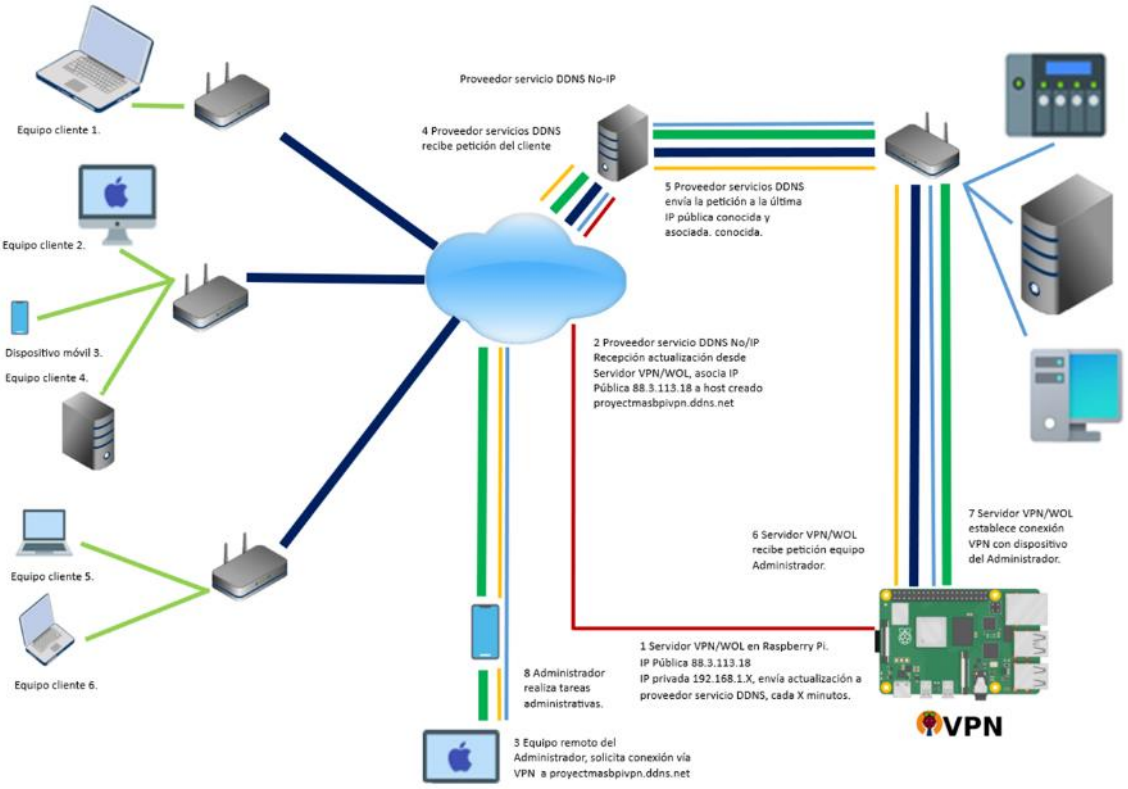
“Apple creó el proyecto XQuartz como un esfuerzo comunitario para desarrollar más y ofrecer más soporte técnico para X11 en los Mac. El proyecto XQuartz se basaba originalmente en la versión de X11 incluida en Mac OS X v10.5. Desde entonces ha habido varios lanzamientos de XQuartz con parches, soporte técnico para nuevas prestaciones y mejoras adicionales para la experiencia X11. Apple es un colaborador del proyecto XQuartz y ha trabajado para garantizar que X11 funcione según lo esperado con macOS con las versiones más recientes disponibles de XQuartz.

Las bibliotecas de servidor y cliente de X11 para macOS están disponibles en el proyecto XQuartz en www.xquartz.org. Descarga la versión más reciente.”

XQuartz, es un proyecto de código abierto, es el desarrollo para una versión del sistema X.Org, X Window, que se ejecuta en macOS. Junto con las bibliotecas y aplicaciones compatibles, forma la aplicación X11.app que Apple envió con las versiones 10.5 a 10.7 de OS X.

Caso práctico proyecto PiVPN y Wake On LAN WOL.

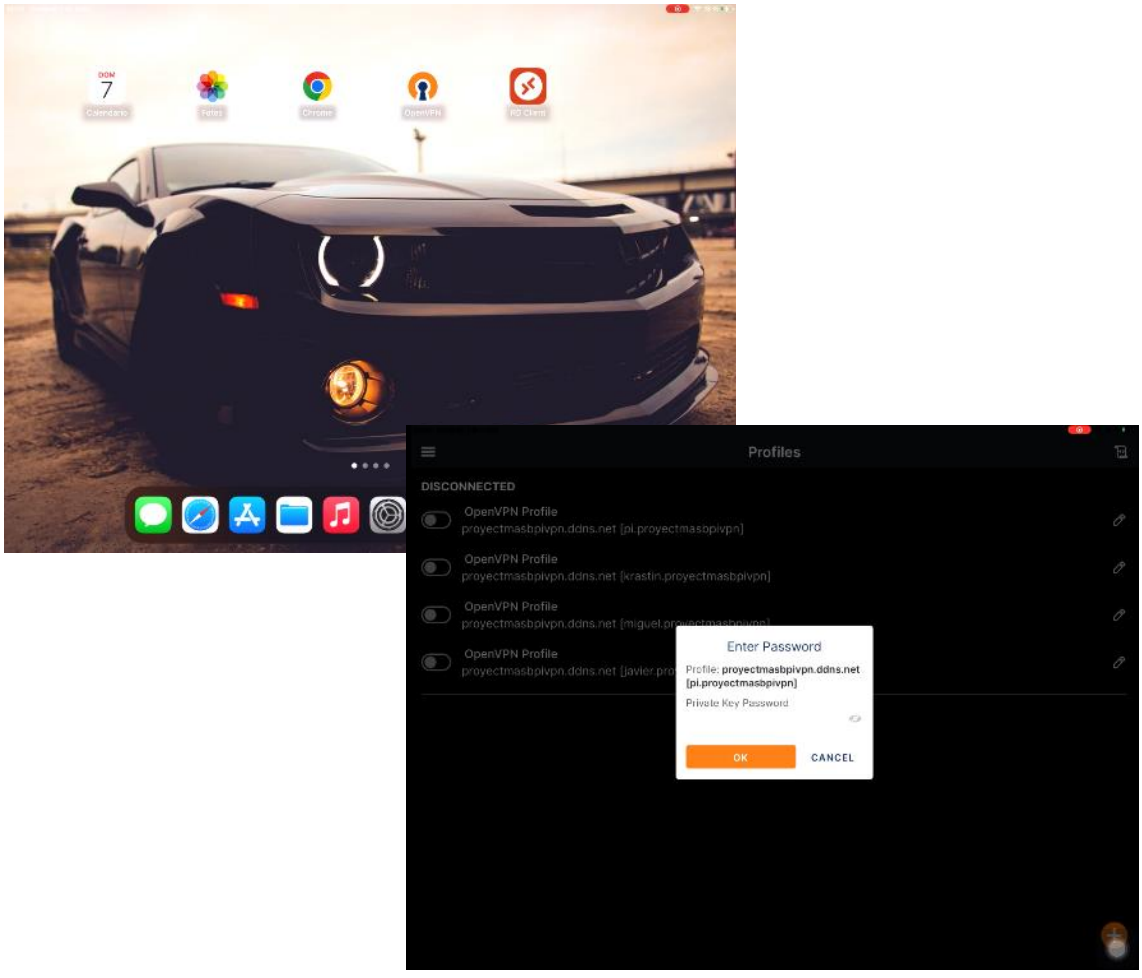
Antes de pasar a comentar y explicar todas las instalaciones y configuraciones llevadas a cabo para este proyecto, empezare explicando para que se puede utilizar.



Soy un Administrador de una pequeña o mediana empresa, en la que para poder ahorrar y además poder facilitar las labores de trabajo de los trabajadores, es imprescindible el ahorro energético y habilitar el teletrabajo, para lo que se tiene en producción en un pequeño dominio un equipo servidor VPN y Wake On LAN (WOL), es por lo que la importancia de poder realizar la conexión al servidor de múltiples formas y todas ellas de forma segura, a través de conexión VPN como por el protocolo SSH, realizada la conexión al servidor VPN/WOL, como Administrador, se podrá revisar la configuración del servidor o servidores, el estado de los servicios y algo muy importante encender/arrancar los equipos o máquinas virtuales en caso de ser necesario para que los usuarios se conecten a ellos, como por ejemplo un dispositivo de almacenamiento en la nube (NAS), terminada la jornada laboral, se comprobara que los equipos arrancados se encuentran apagados y en caso contrario si es posible su apagado, apagarlos.

iPad caso práctico proyecto PiVPN y Wake On LAN WOL.

Este proceso se ha probado como se indica en estas instrucciones en un iPad de Apple, aunque también se ha probado en dispositivos móviles como teléfonos con S.O. IOS, Android y tablet Android, esta prueba que se describe, se realiza con conexión de datos móviles a través de un teléfono, las pruebas realizadas con portátiles con S.O. Windows o macOS también fueron probadas con conexión de datos móviles como con conexiones WIFI.



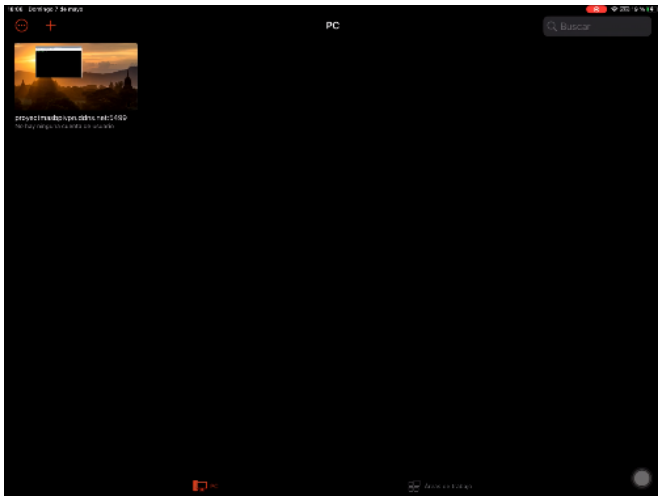
Dentro del dispositivo móvil y conectado a una conexión de datos móviles, se abrirá la aplicación OpenVPN (OpenVPN Connect), en la que, dentro de esta, se podrá pulsar sobre el deslizador  de uno de los usuarios que se disponga su configuración importada para realizar la conexión VPN.

Como se puede observar en la captura de la ventana superior, se facilitará la contraseña del usuario, en este ejemplo el usuario pi y se pulsará sobre OK.



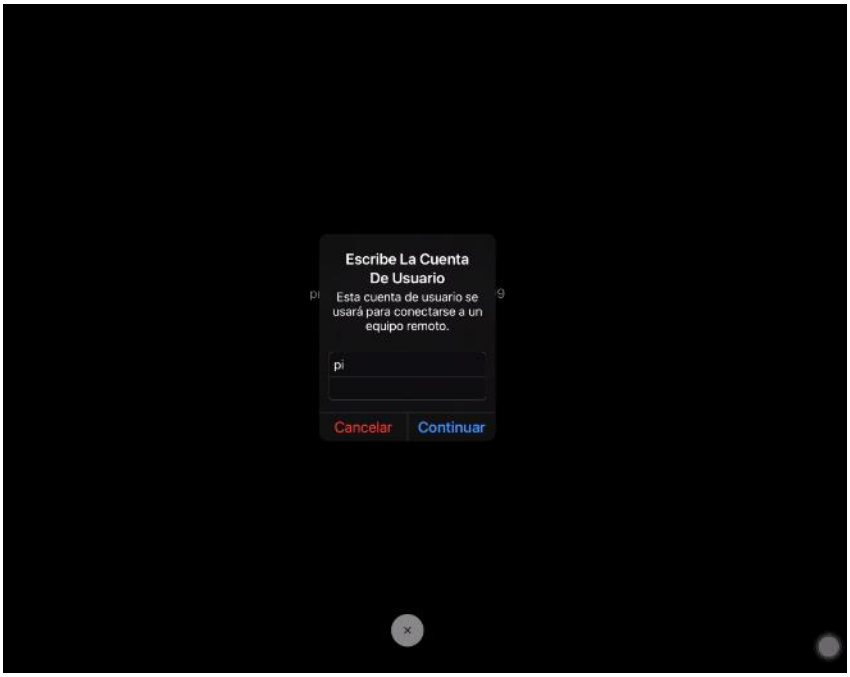
Establecida la conexión con el servidor VPN/WOL, el deslizador cambia de color pasando a tener el siguiente aspecto  .
Como se puede observar en la ventana de la captura superior, en esta, se facilitan datos como.

- CONNECTION STATS (Estado de la conexión).
- DURATION (Duración).
- PACKET RECEIVED (Paquetes recibidos).
- YOUR PRIVATE IP (Dirección IP privada, 10.171.209.5).
- SERVER (Servidor, proyectmasbpivpn.ddns.net).
- SERVER PUBLIC IP (IP pública del servidor, 83.3.113.18).

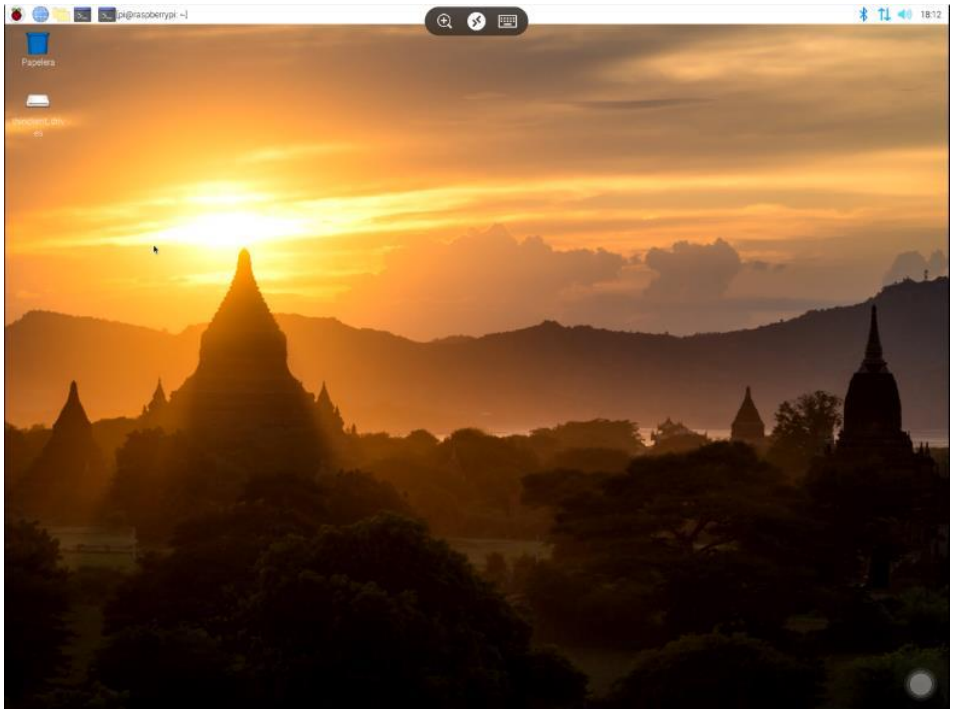


Estando ya conectados a través de VPN al servidor VPN/WOL, se podrá cambiar de aplicación manteniendo la conexión establecida, en este caso, se abre la aplicación Microsoft escritorio remoto.

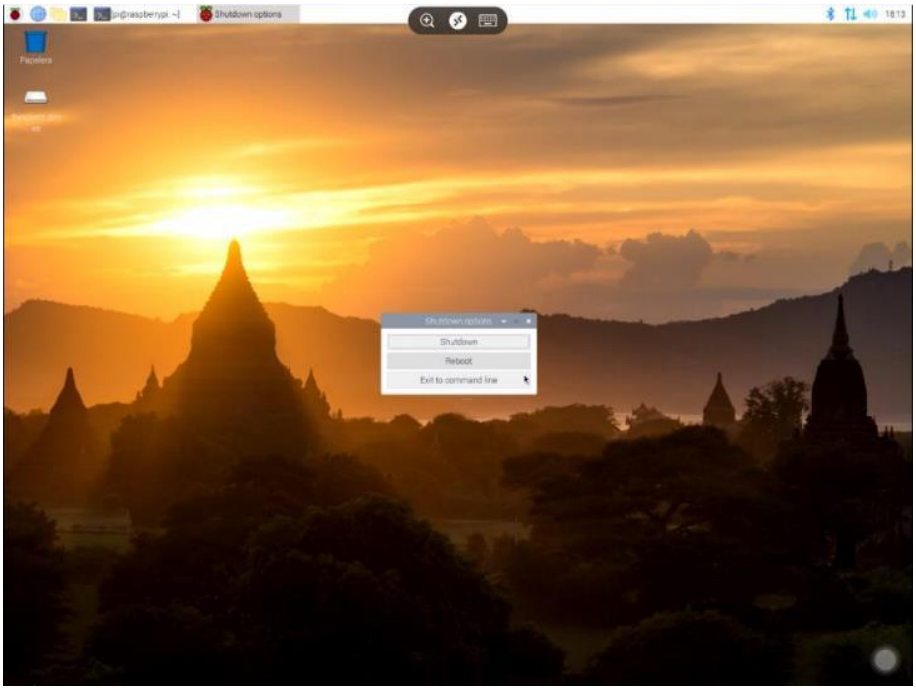
Al pulsar sobre la miniatura de la conexión creada al servidor VPN/WOL, se comenzará a establecer la conexión.



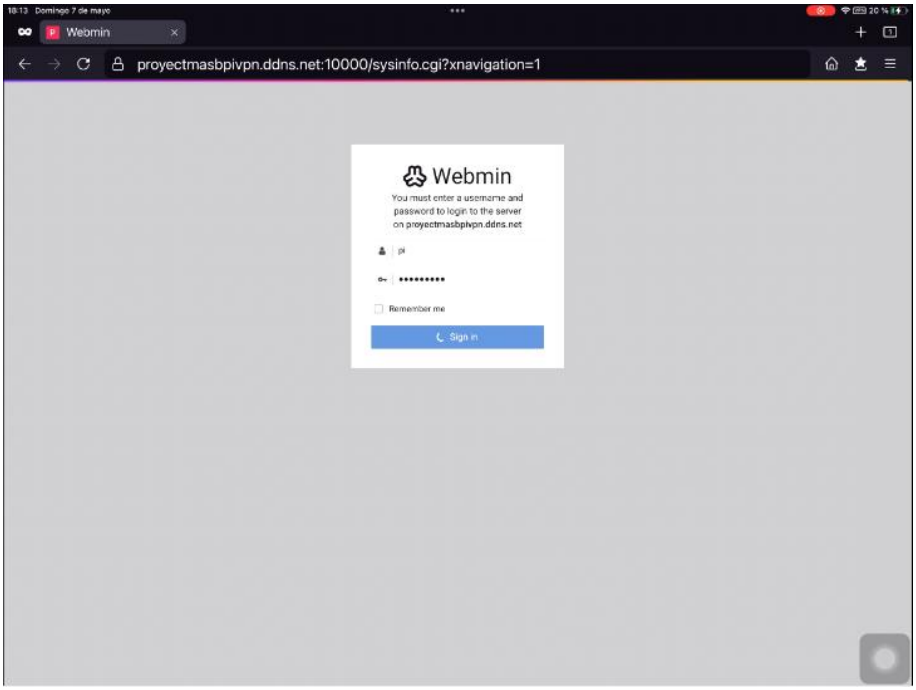
Posteriormente se tendrá que facilitar en este caso las credenciales de un usuario, en este ejemplo se facilitan las credenciales del usuario pi.



Estando conectado vía VPN y por escritorio remoto, se podrán realizar las tareas administrativas necesarias, acceder a un terminal y consultar, iniciar, parar, reiniciar servicios, ejecutar el o los scripts de encendido/arranque de los equipos, incluso iniciar la aplicación para realizar esta última acción desde el entorno grafico con la aplicación gWakeOnLan.

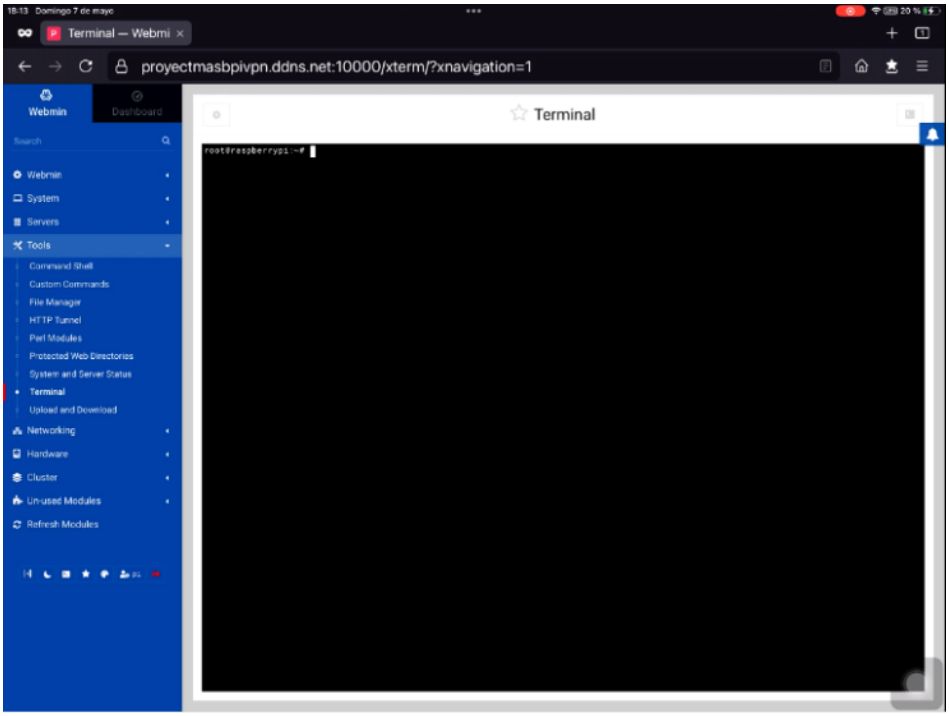


Finalizadas las operaciones administrativas, se podrá cerrar la conexión de escritorio remoto.

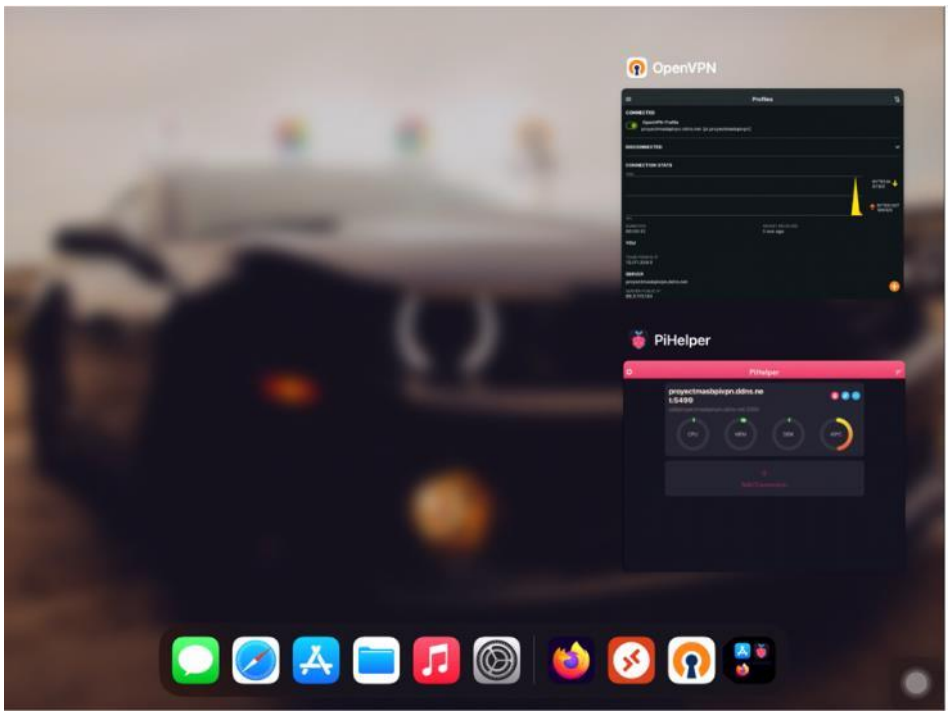


Otra forma que se desarrollará más adelante es acceder a través de WEBMIN, se colocara como URL en un navegador https://proyectmasbpivpn.ddns.net:10000

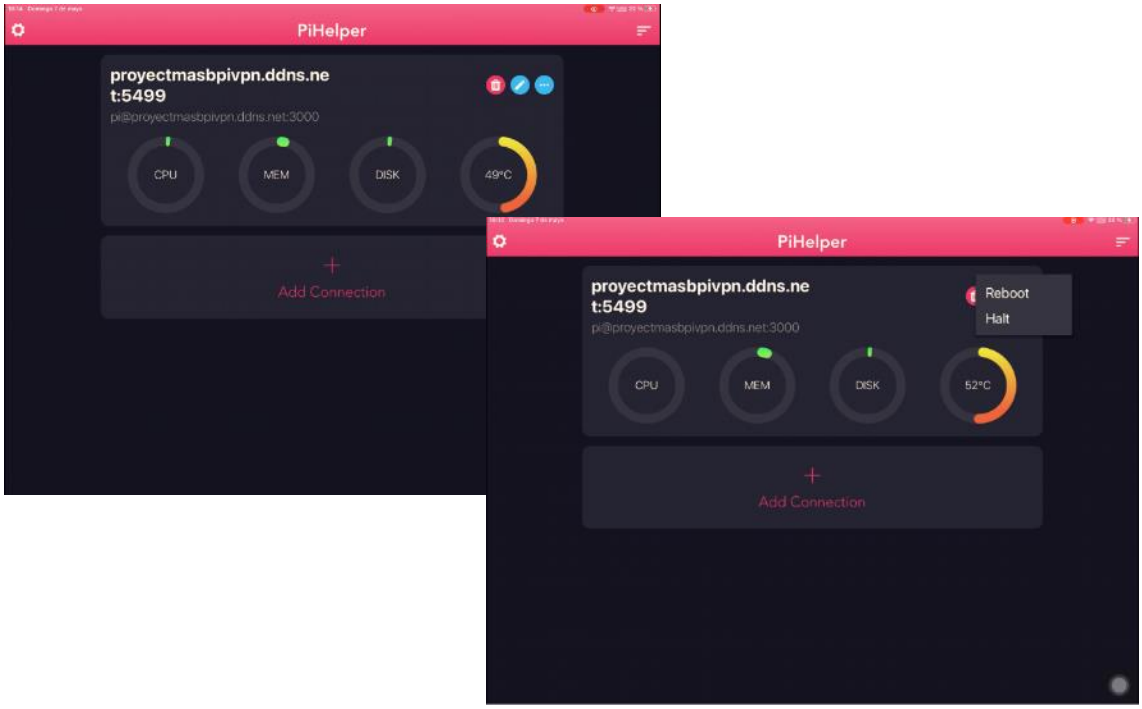
Correspondiendo al nombre de dominio/host creado en el proveedor de servicios DDNS, junto el puerto de acceso por defecto a WEBMIN que es el 10000.



Dentro de WEBMIN, se podrá acceder al terminal, teniendo que pulsar en el panel izquierdo sobre Tools \ Terminal, donde se podrá realizar las operaciones de administración desde este terminal.



Una utilidad que, aunque para quitar la publicidad es necesario realizar un pequeño pago, es en este caso PiHelper, en Android se dispone de su homologo siendo RaspManager.

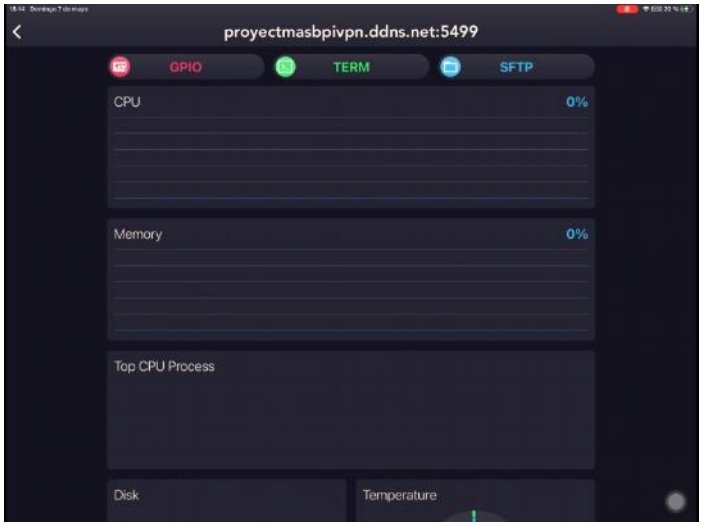


En la pantalla principal, se muestra un estado de cómo se encuentra el servidor CPU, Memoria (MEM), disco (Disk) y temperatura.

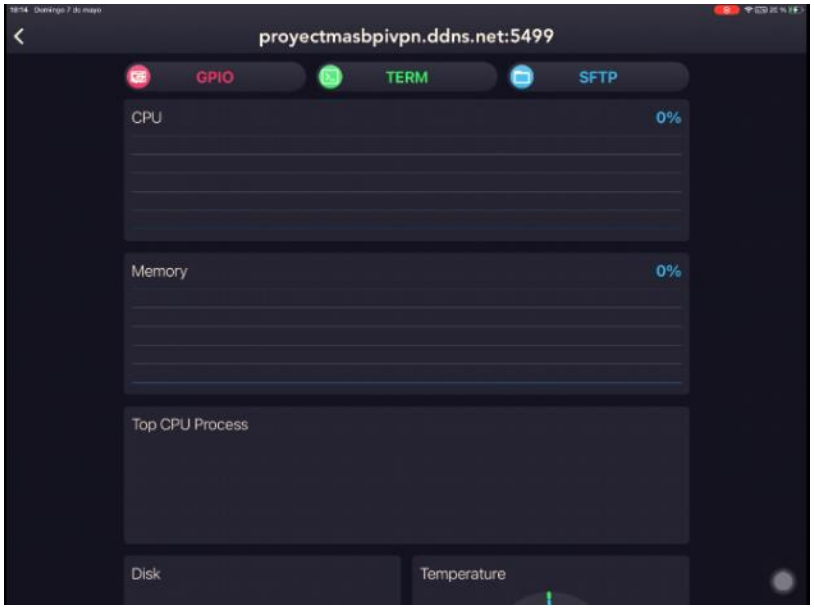
Si se pulsa sobre los puntos superiores derechos  , se podrá reiniciar o apagar el servidor VPN/WOL siendo este la Raspberry Pi.



Al pulsar sobre la zona que se muestra en la ventana de la captura superior.

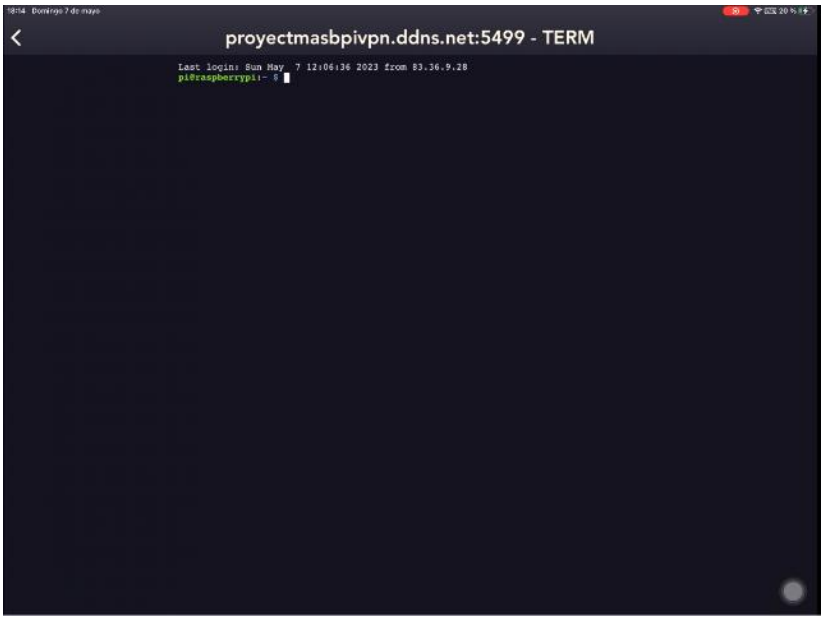


Aparecerá otra ventana en la que se mostrará más información, incluso al deslizar la barra de deslizamiento lateral derecha.

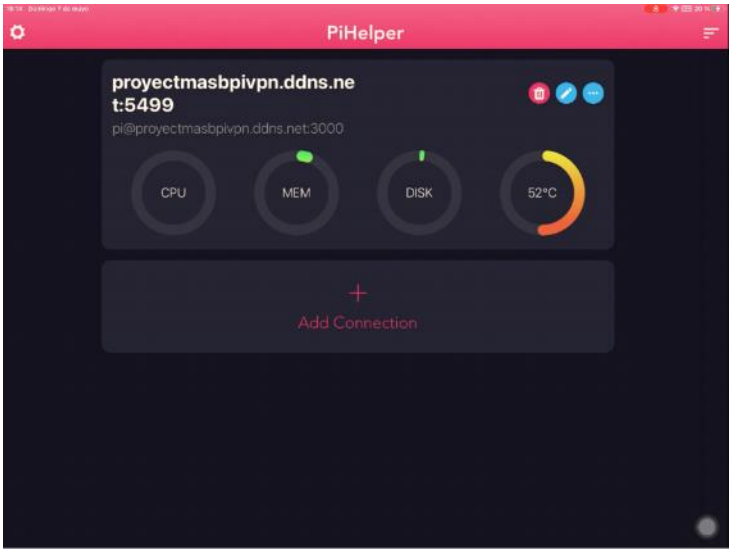


En la ventana de la captura superior, al pulsar sobre TERM

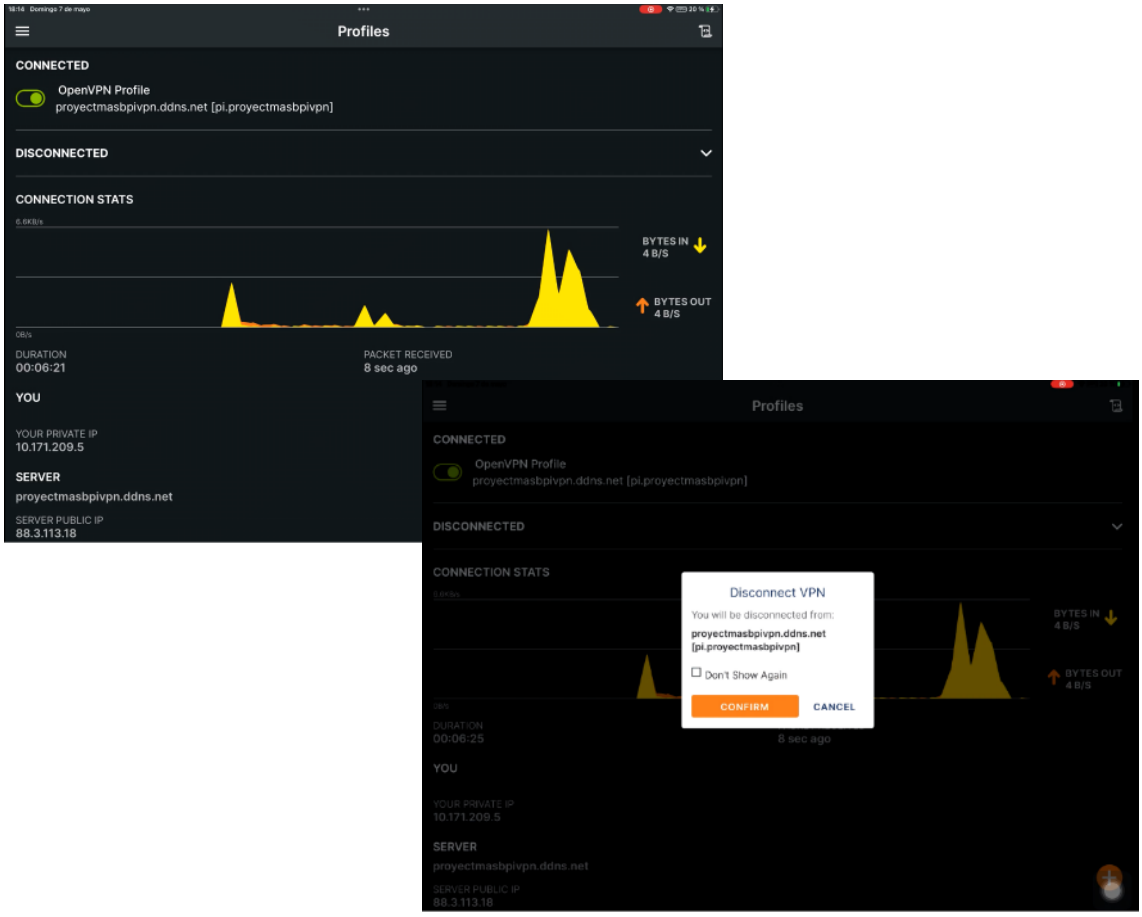
.



Dentro de este terminal, como en cualquier otro, se podrá ejecutar los comandos necesarios.



Una vez finalizadas las tareas administrativas necesarias, se procederá a cerrar la aplicación.



Para finalizar la conexión dentro de la aplicación OpenVPN, se pulsará sobre el deslizador  , en el cuadro de dialogo que se muestra habrá que pulsar sobre CONFIRM para finalizar la conexión.



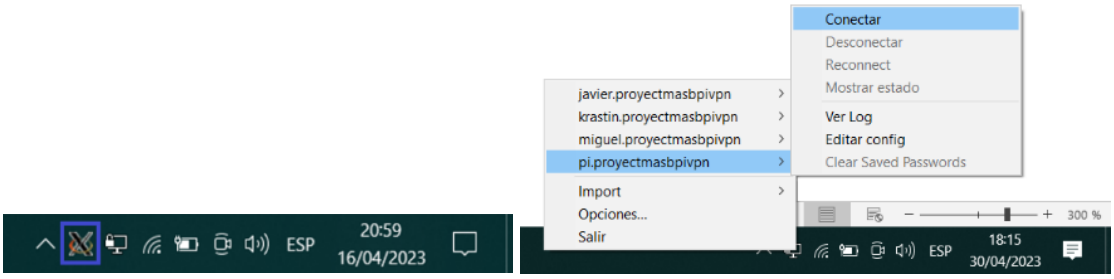
Por motivos obvios de extensión del documento, ya no se describe las instalaciones a realizar en un dispositivo como una tablet o un móvil, solo se informará de las aplicaciones utilizadas en ambos S.O., IOS y Android y lo que se tendrá que instalar para poder llevar a cabo este proyecto incluso en uno de estos dispositivos.

Aplicaciones a instalar dependiendo del S.O. que disponga este.

IOS (tienda AppStore).	Android (tienda Play Store).
OpenVPN Connect, se buscará opnvpn en Apple Store.	OpenVPN Connect, se buscará opnvpn en Play Store.
Escritorio remoto de Microsoft, se buscará RDP en Apple Store.	Remote Desktop, se buscará RDP en Play Store.
PiHelper, se buscará pihelper en Apple Store.	RaspManager, se buscará raspmanager en Play Store.

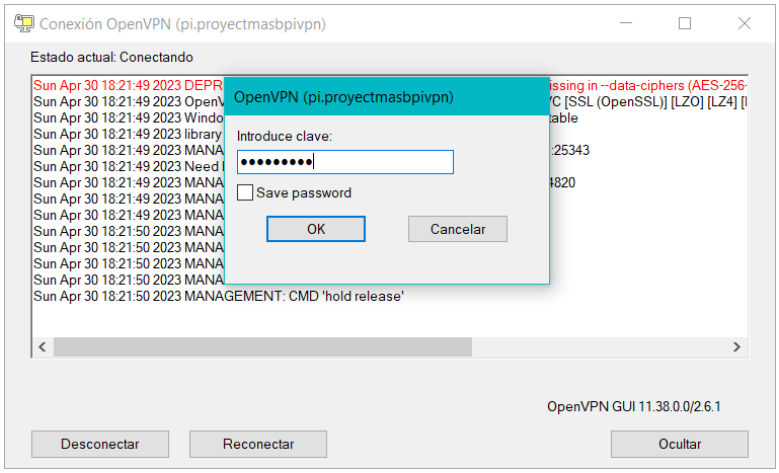
Windows caso práctico proyecto PiVPN y Wake On LAN WOL.

Este caso es el resultado de proceder a la instalación y configuración de lo necesario para llevar a cabo este procedimiento, no es necesario la lectura de todo el documento, como se puede comprobar se explica cómo realizar la instalación y configuración de las aplicaciones en los S.O. Windows, Linux y MAC, como proceder a la misma localmente o en remoto vía SSH.

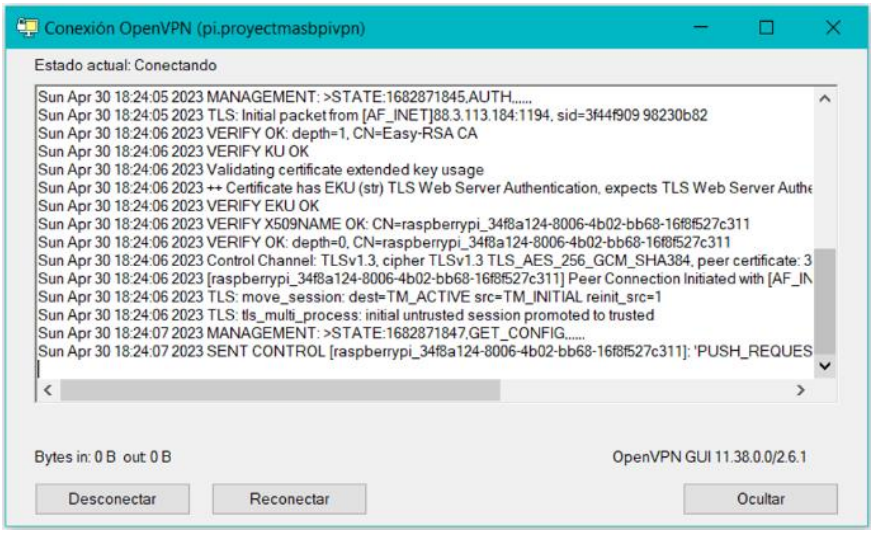


En este caso práctico, al disponer el equipo cliente un S.O. Windows, es necesario tener instalado y en ejecución la aplicación Xming, se explicará cómo instalar y configurar la aplicación ejecutando (XLaunch), imagen de la captura superior izquierda.

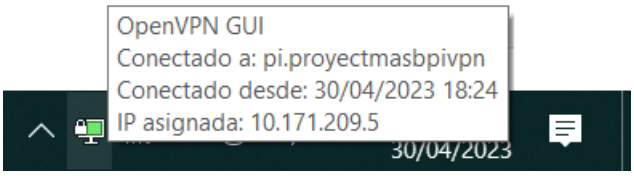
Una vez descargados e importados los ficheros de conexión en la aplicación OpenVPN, en el icono  de la barra de tareas en el área de notificaciones, se pulsará con el botón derecho del ratón y al seleccionar uno de los usuarios para conectarnos como administrador, en el menú que aparece se pulsará sobre Conectar.

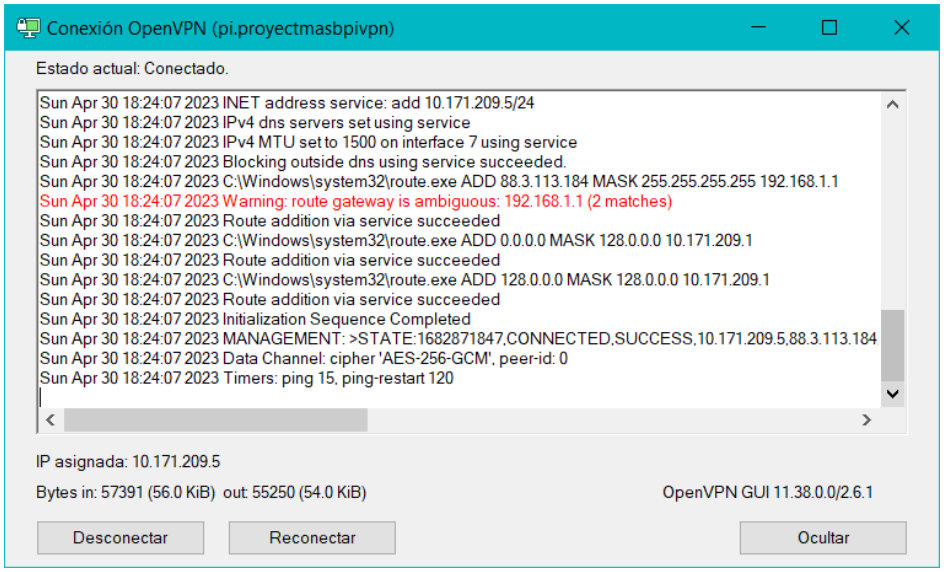


Tras facilitar la contraseña de conexión se pulsará OK.  , antes de pulsar OK el icono cambia de color a color amarillo.

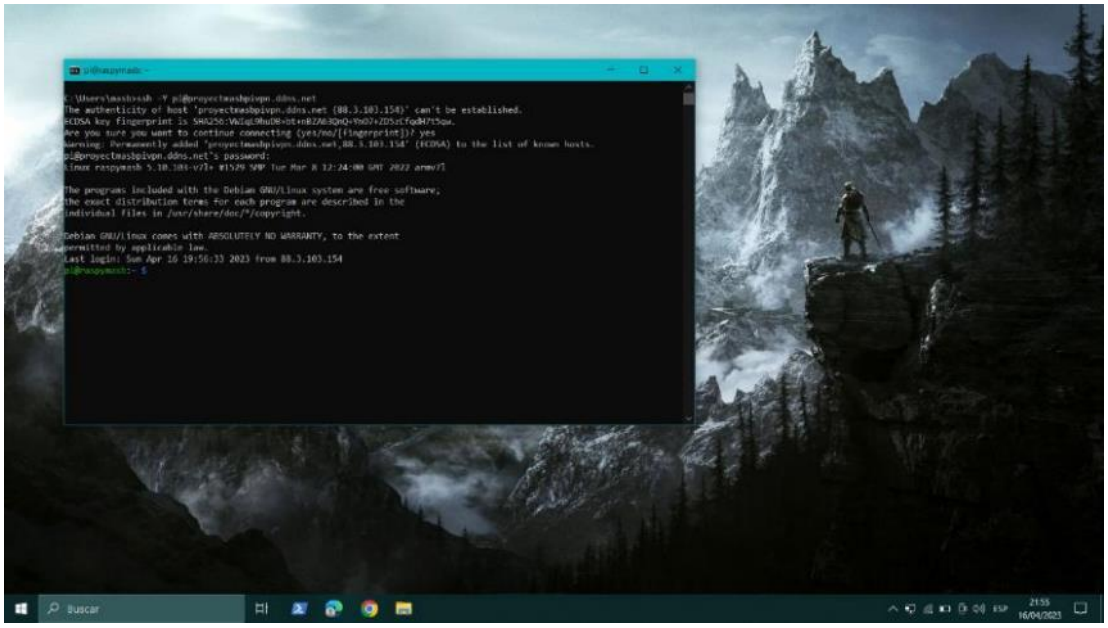


Una vez que se ha realizado la conexión el icono cambia a color verde  .



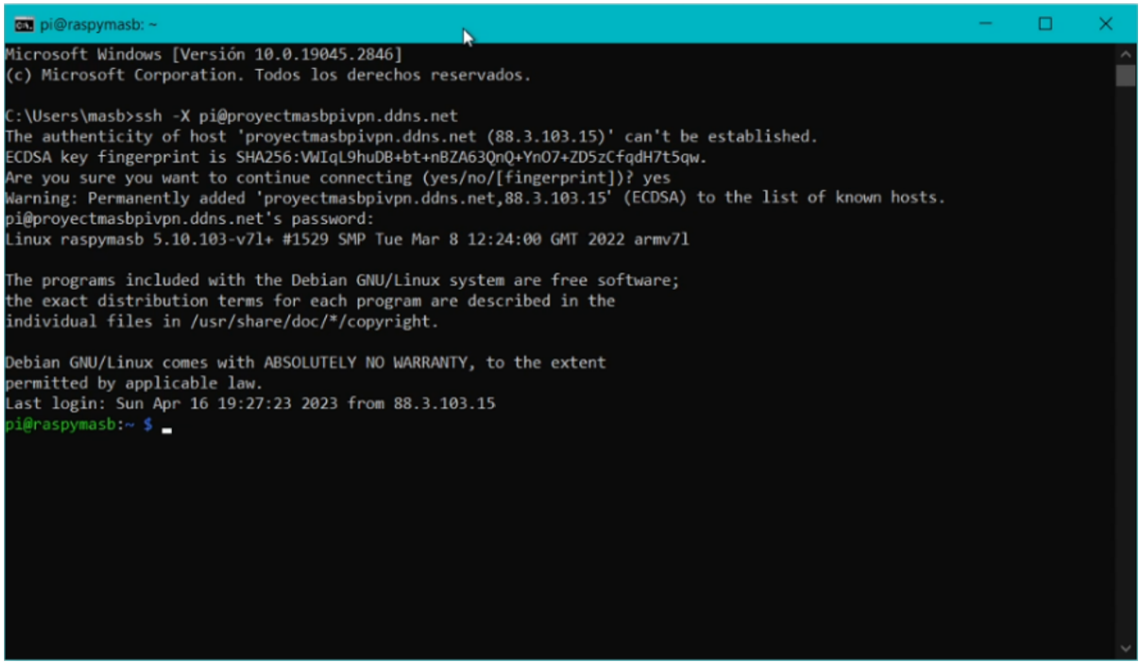


Si se pasa el ratón sobre el icono indicado, se mostrará información sobre la conexión y en caso de hacer doble clic con el botón izquierdo del ratón aparecerá la ventana de la captura de la imagen superior.

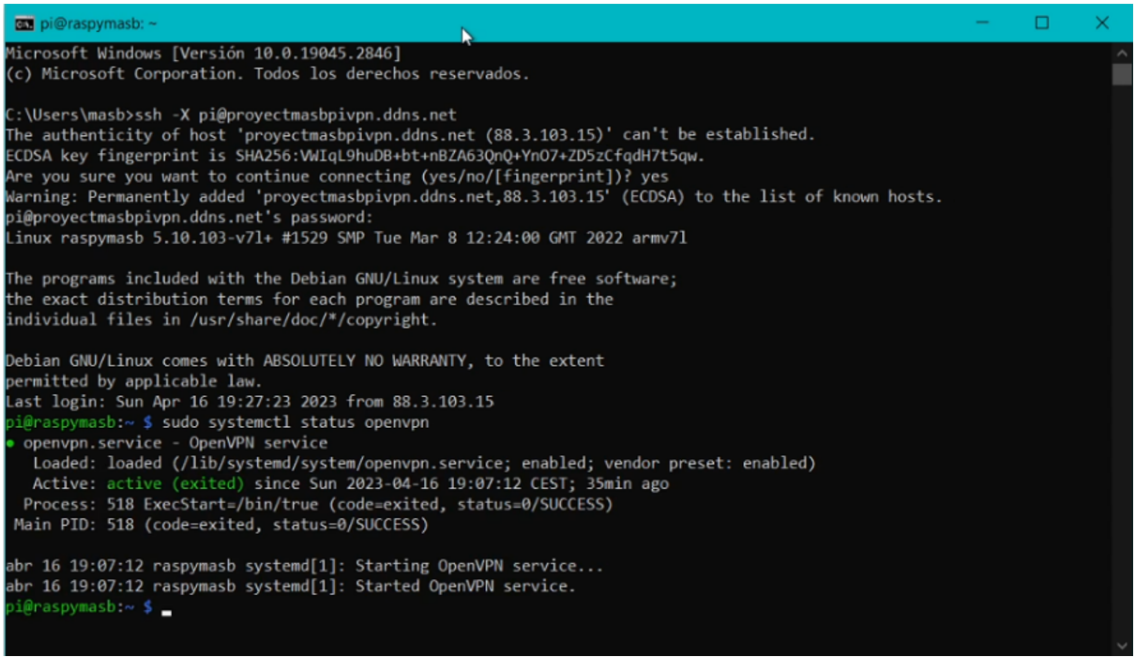


Con la conexión VPN realizada y la aplicación XLaunch iniciada, se accederá a un terminal y se procederá a llevar a cabo una conexión vía SSH al servidor VPN/WOL.

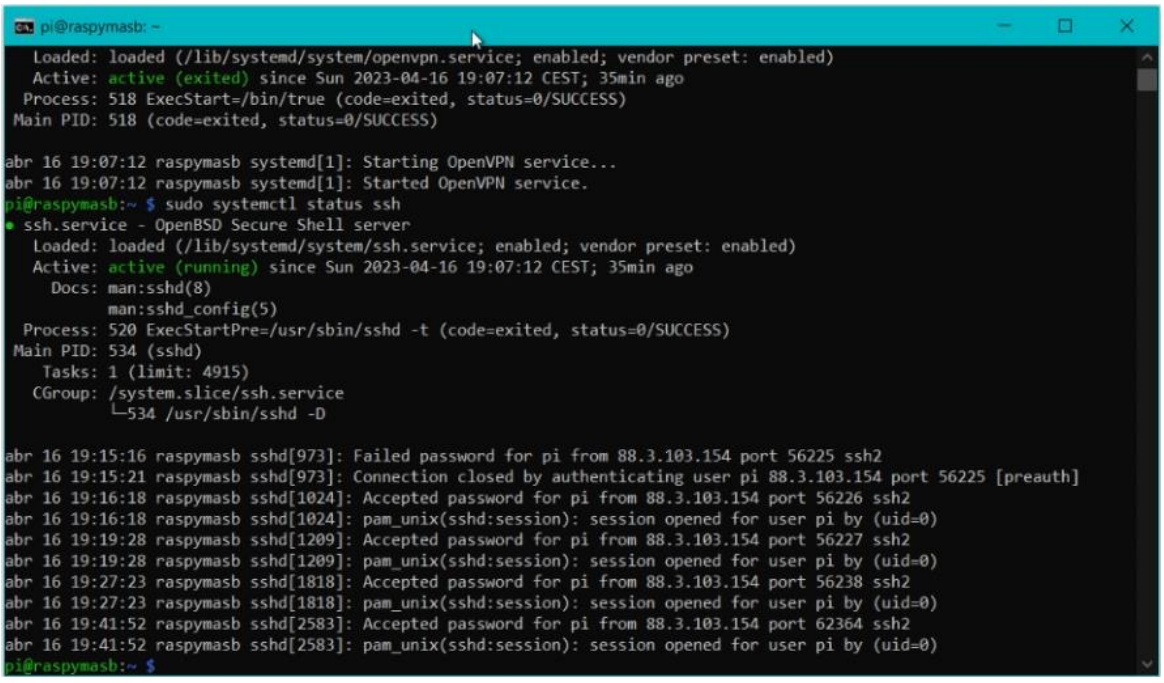
Comandos. (-X, habilita la redirección X).
ssh -X pi@proyectmasbpivpn.ddns.net -p 22
plink.exe -X pi@proyectmasbpivpn.ddns.net gwakeonlan



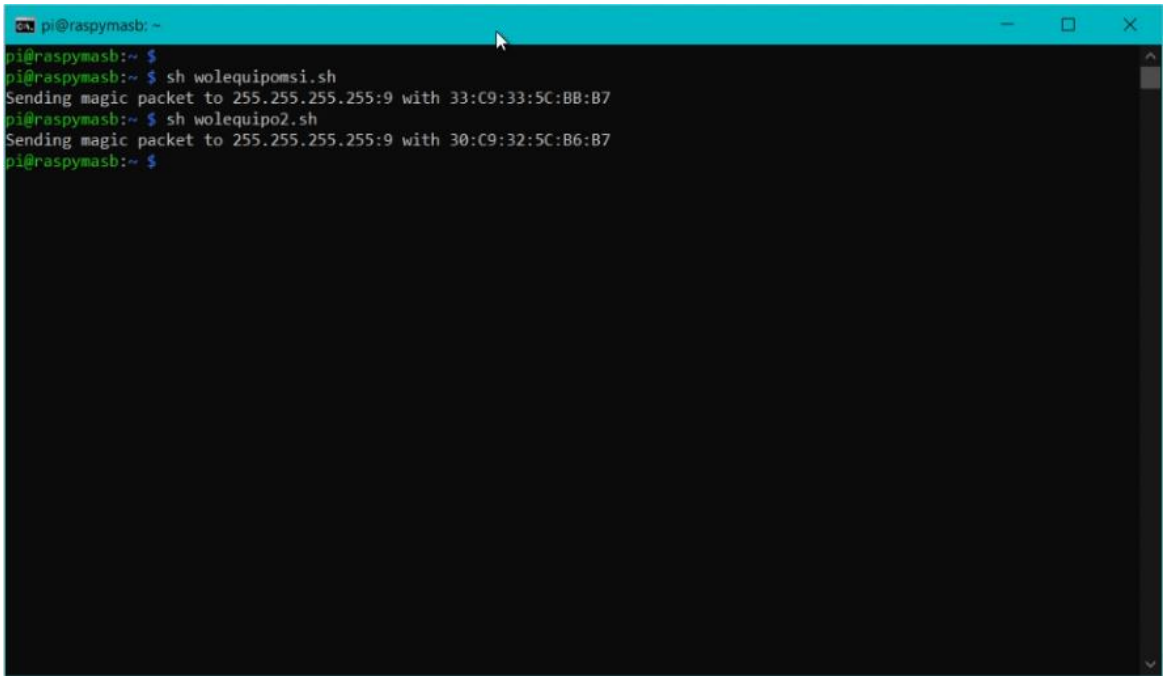
Al ejecutar el comando, habrá que autenticarse, facilitando la contraseña del usuario.



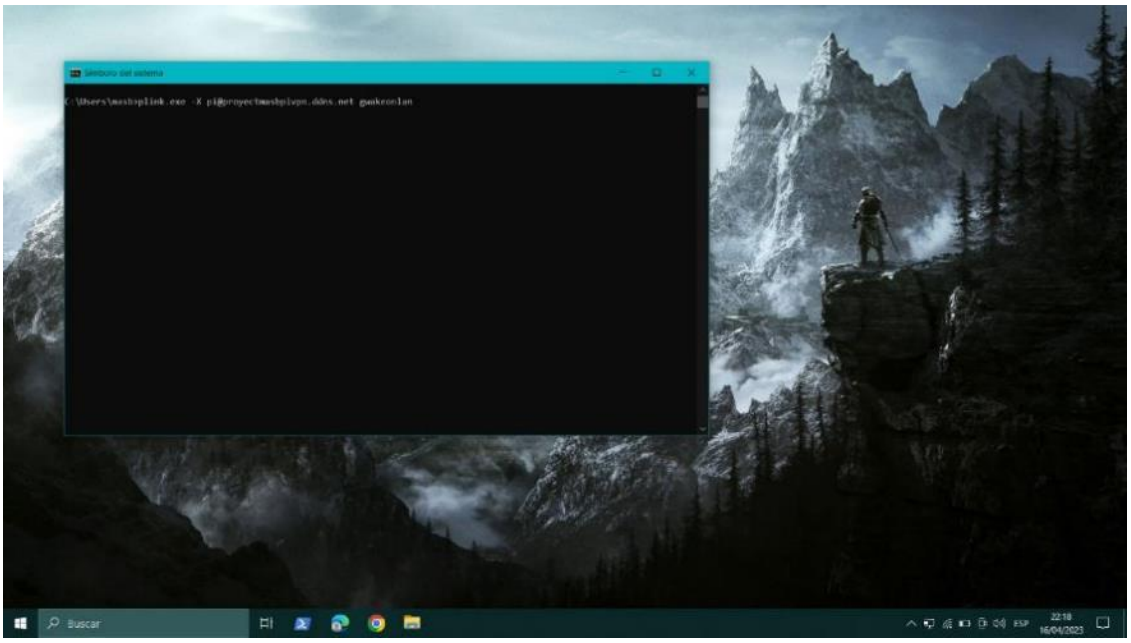
Conectado vía SSH, como administrador se podrá comprobar el estado de los servicios necesarios para el buen funcionamiento del servidor VPN/WOL, como por ejemplo ver el estado del servicio openvpn con el comando sudo systemctl status openvpn

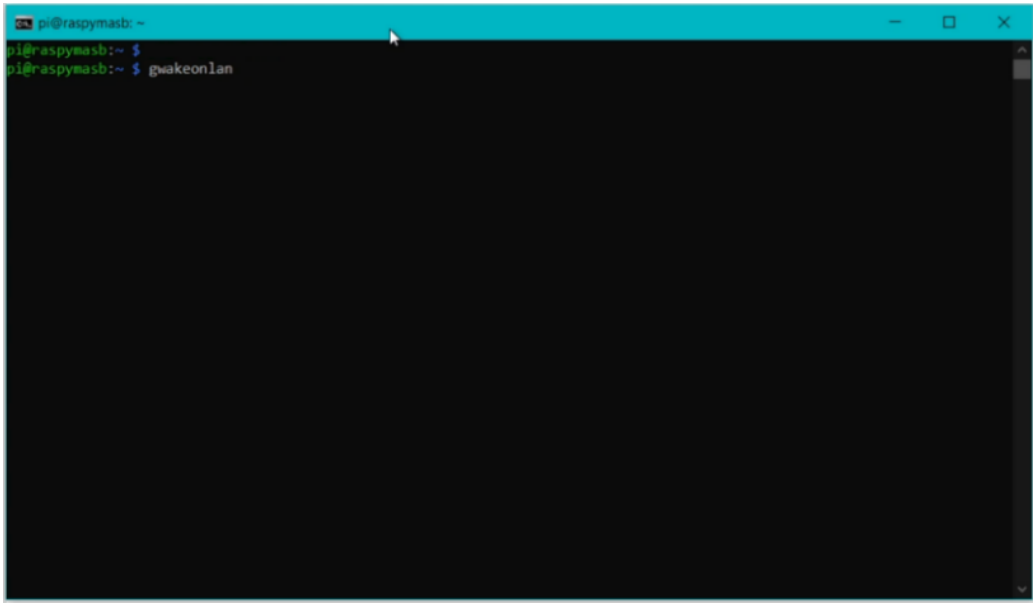


Comprobar el estado del servicio SSH con el comando sudo systemctl status ssh



Dentro del terminal remoto, se podrá con el comando adecuado mandar el “paquete mágico”, para encender/arrancar los equipos y posteriormente la conexión a ellos por parte de los usuarios, en este caso como se aprecia en la captura de la imagen superior, se ejecuta un script donde en su interior se encuentra el comando a ejecutar para iniciar el o los equipos a arrancar, este proceso de creación del o los ficheros se explicará más adelante.



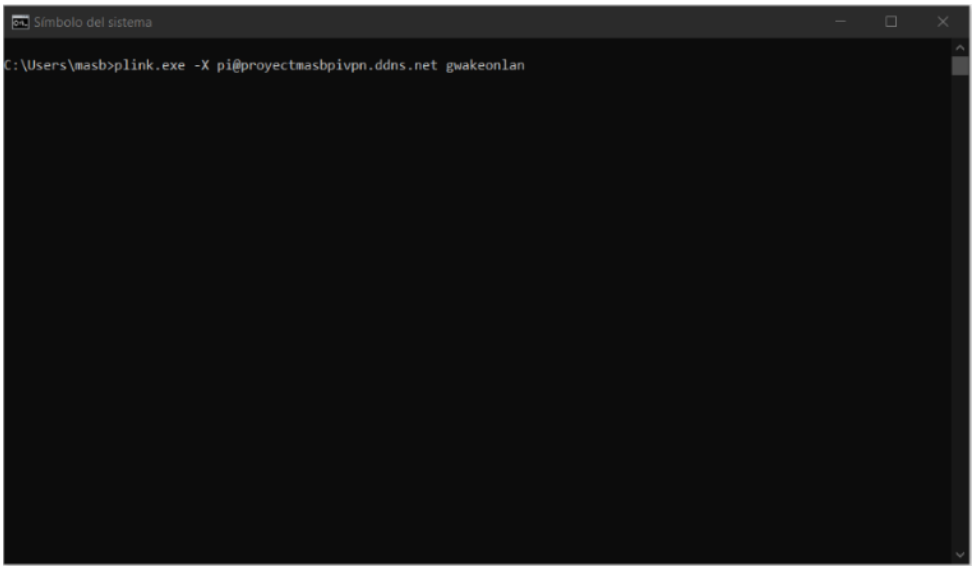


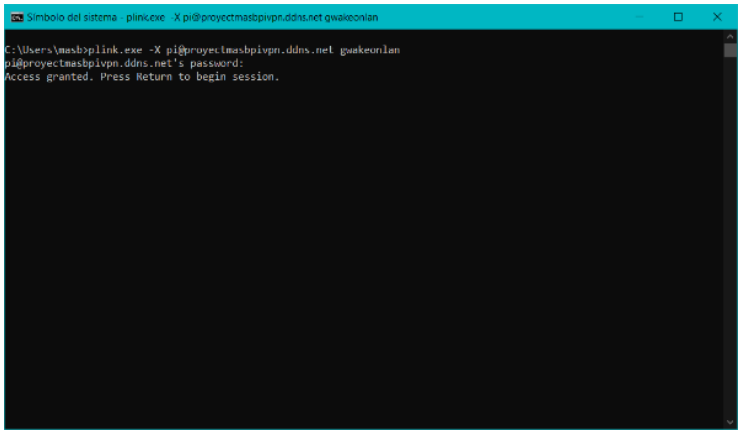
Incluso al tener configurada la redirección X, en caso de querer como administrador arrancar aplicaciones graficas remotamente por el terminal, al acceder vía SSH y con la opción necesaria, se podrá ejecutar la aplicación instalada en el servidor Linux en el equipo remoto como se explicará también más adelante.

Como adelanto, los comandos de conexión.

ssh -X pi@proyectmasbpivpn.ddns.net -p 22 (opción -X es para la redirección de las X).

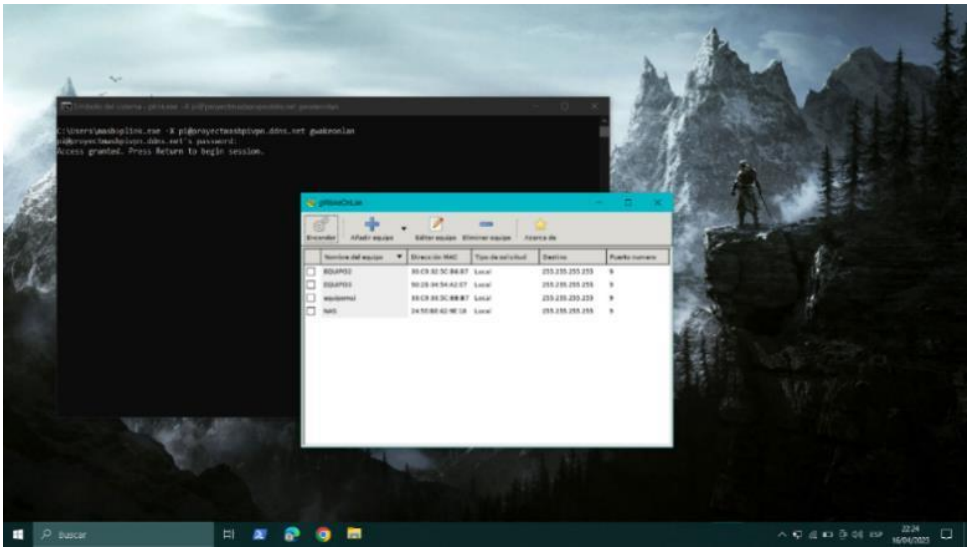
Comando. plink.exe
(es necesario tener instalado PuTTY, para poder ejecutar el comando plink.exe).
plink.exe -X pi@proyectmasbpivpn.ddns.net gwakeonlan

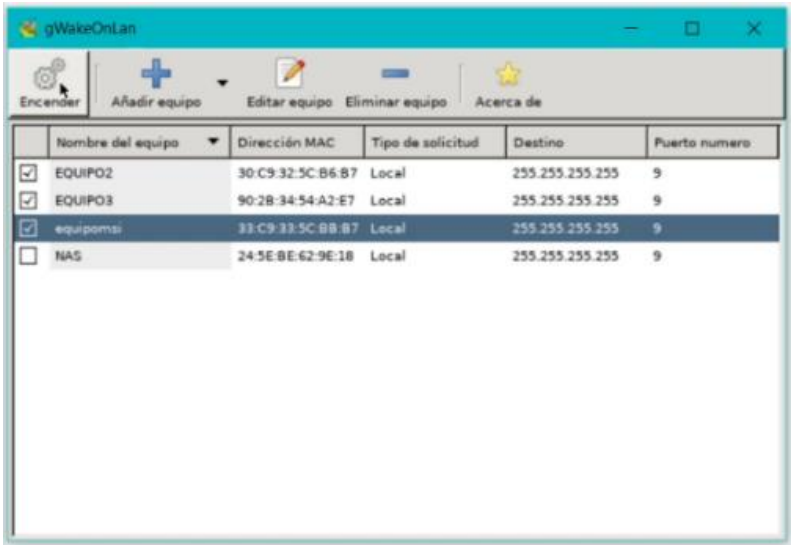




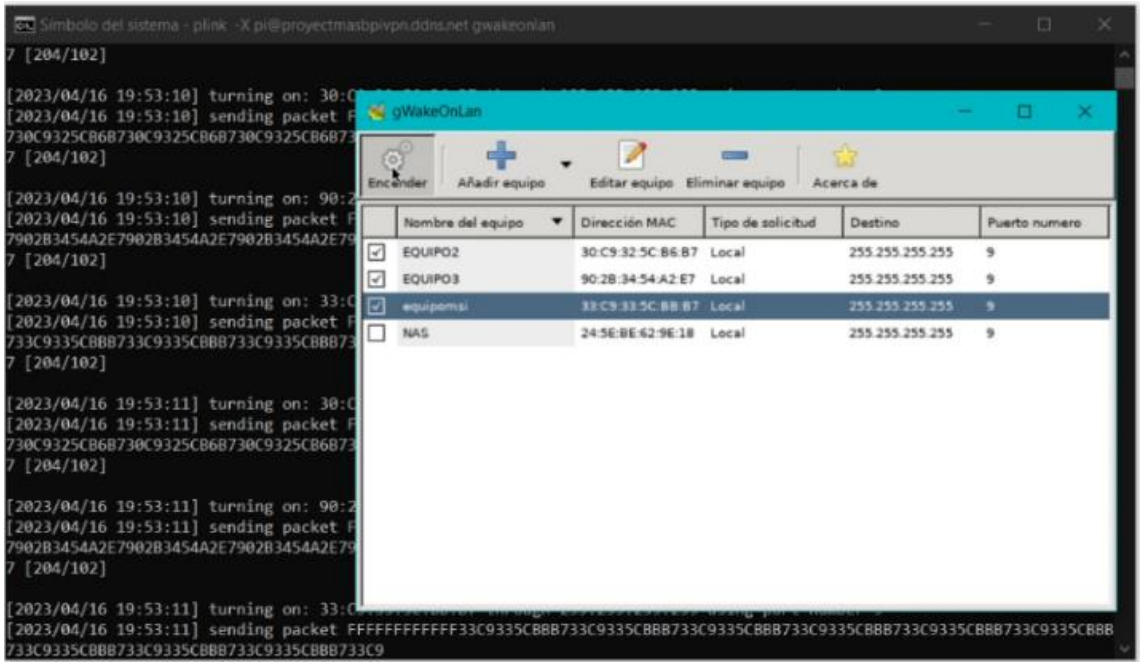
Comando. plink.exe -X pi@proyectmasbpivpn.ddns.net gwakeonlan

Tras introducir la contraseña y pulsar Return (INTRO) para continuar.

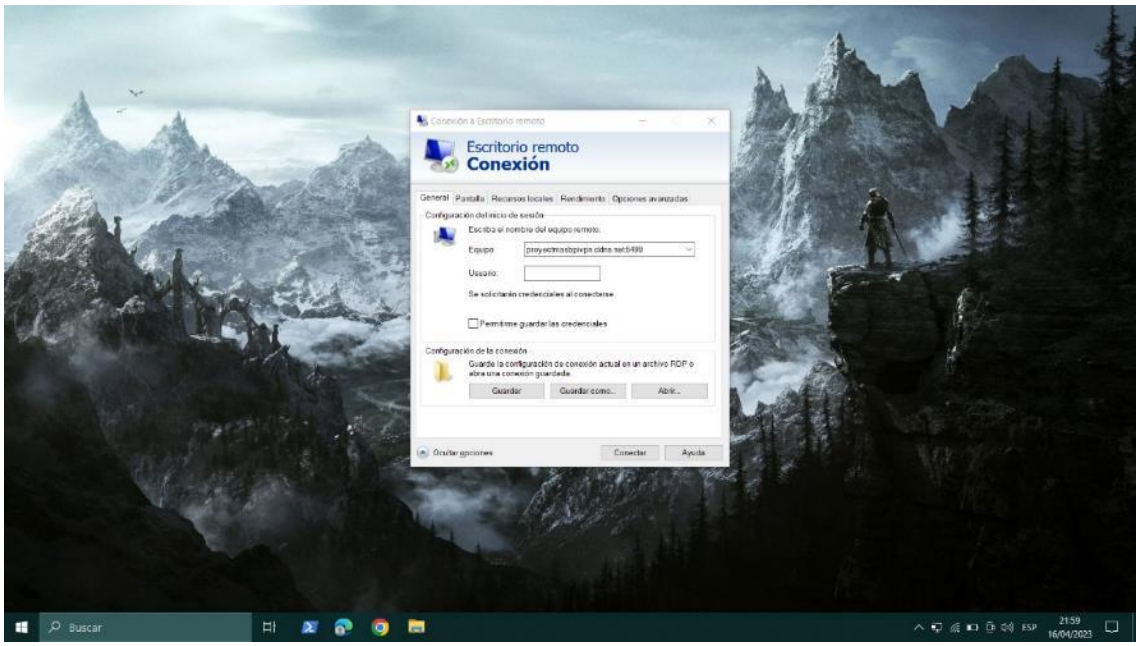




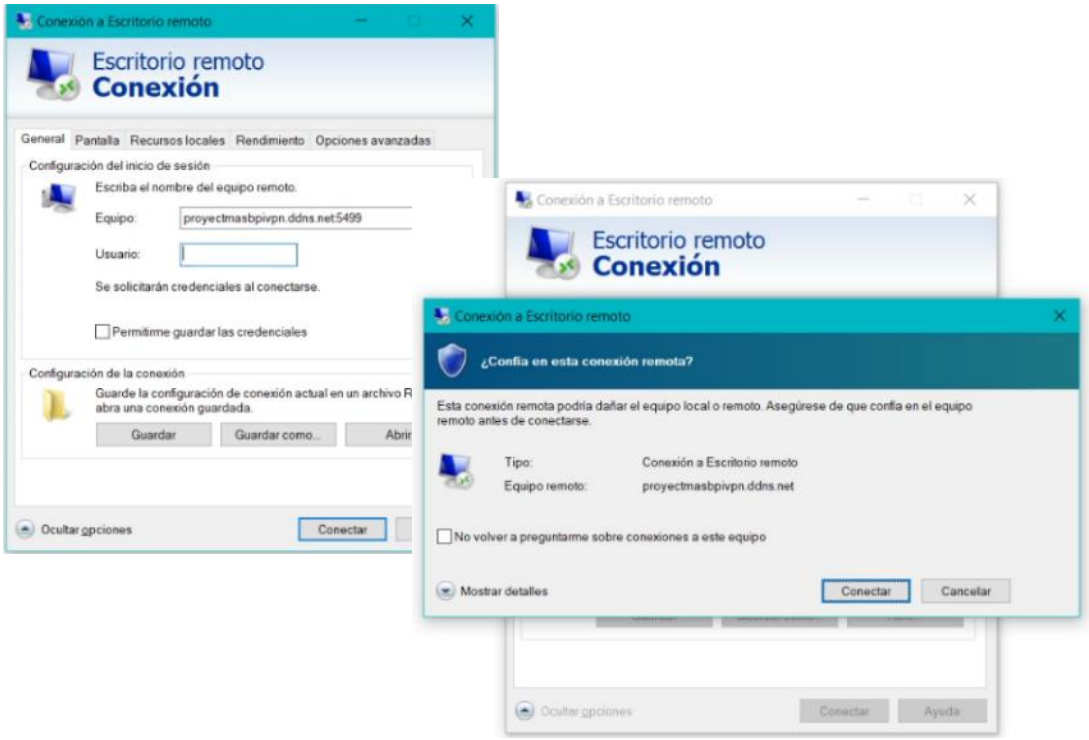
Se puede observar en la ventana de la captura superior, como se abre la aplicación instalada en el servidor VPN/WOL gwakeonlan en el equipo con S.O. Windows, en la que se podrá seleccionar el o los equipos a arrancar y se pulsará sobre Encender para encender los equipos.



La aplicación vía SSH, manda los comandos necesarios para la ejecución remota de la orden que se está ejecutando en el equipo con S.O. Windows.

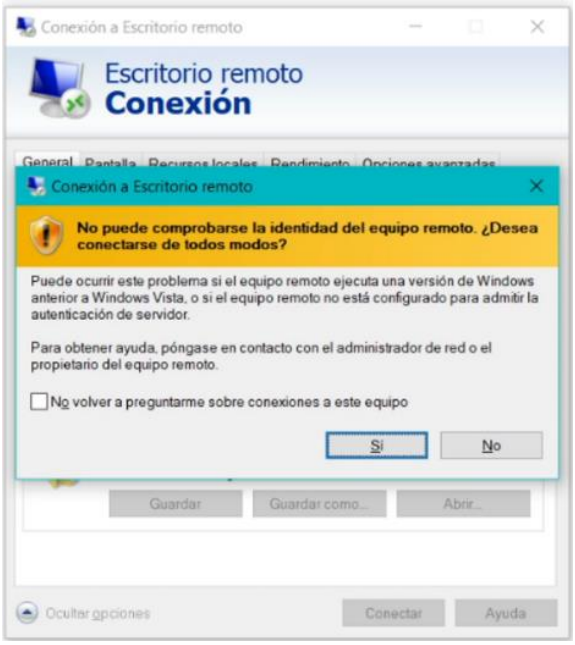


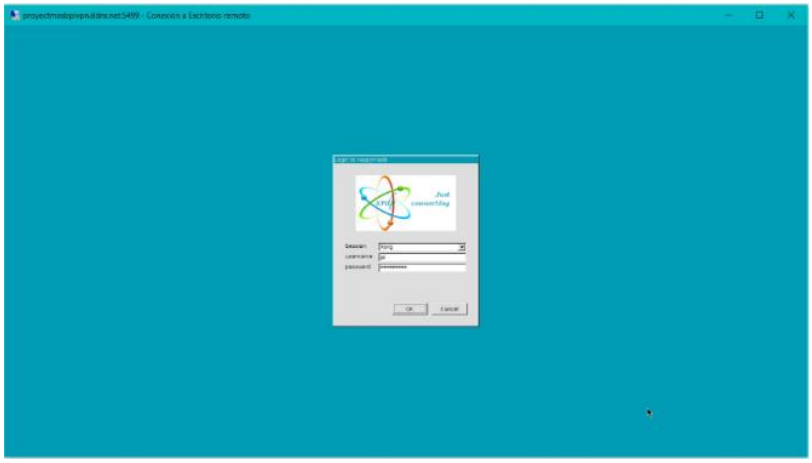
Otra opción para conectarse al servidor VPN/WOL mediante la conexión RDP, y traer al equipo con S.O. Windows el escritorio del servidor VPN/WOL, es el uso de la aplicación Conexión Escritorio remoto, aplicación gratuita de Microsoft.



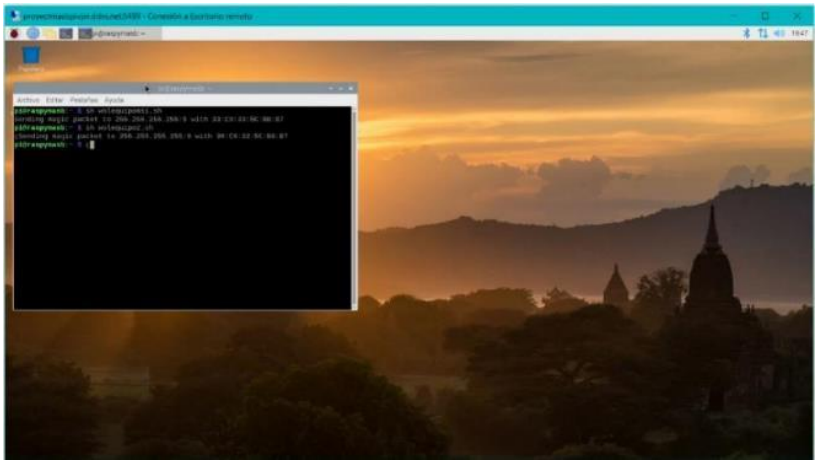
Una vez introducido el nombre del equipo, en este caso al disponer del servicio DDNS se puede acceder gracias al nombre de dominio/host creado, no teniendo que recordar la IP pública que nos da nuestro proveedor de servicios de Internet (ISP), en el apartado Equipo, se escribirá el nombre del host o el dominio creado y el puerto abierto para la conexión remota a través de RDP, separados por ":", siendo en este caso: proyectmasbpivpn.ddns.net:5499, en el apartado Usuario, se podrá facilitar el nombre de usuario, rellenados los campos, se pulsará en Conectar, en la siguiente ventana nuevamente se pulsará sobre conectar.

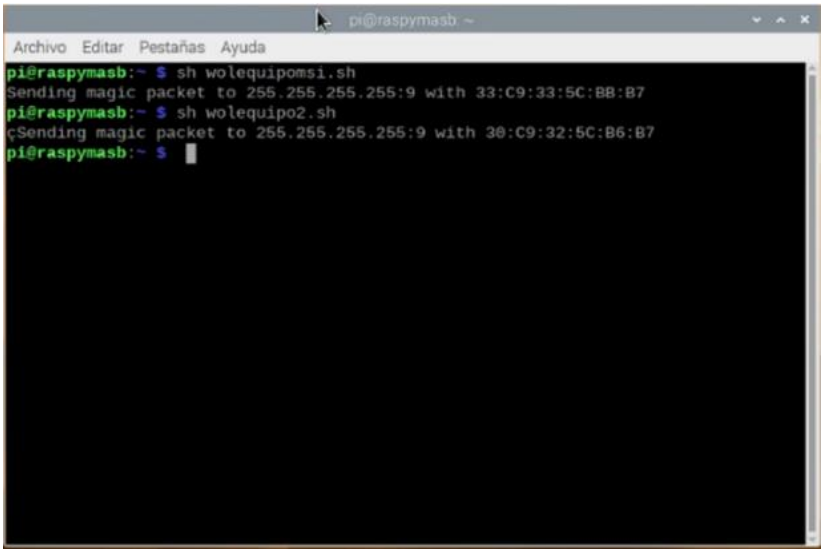
En la nueva ventana, en la que se indica que no se puede comprobar la integridad del equipo remoto, se pulsará sobre Sí.



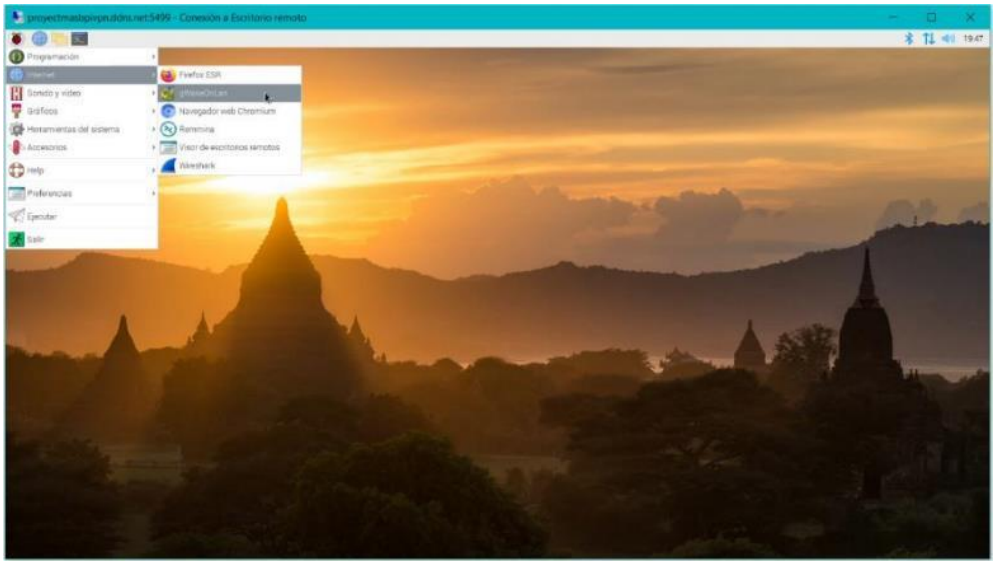


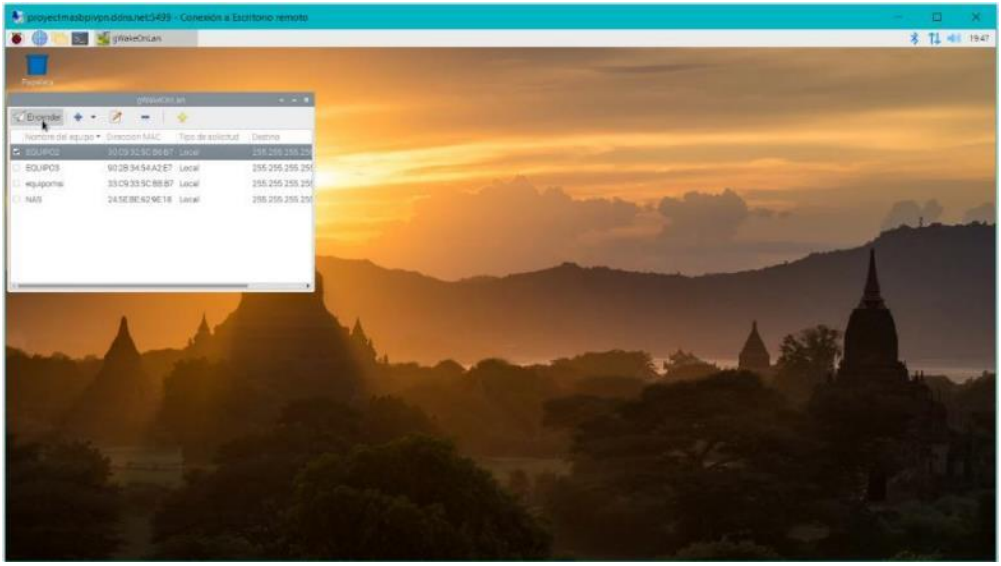
Posteriormente, al facilitar la contraseña de acceso se pulsará OK y se accederá remotamente al escritorio del servidor VPN/WOL.



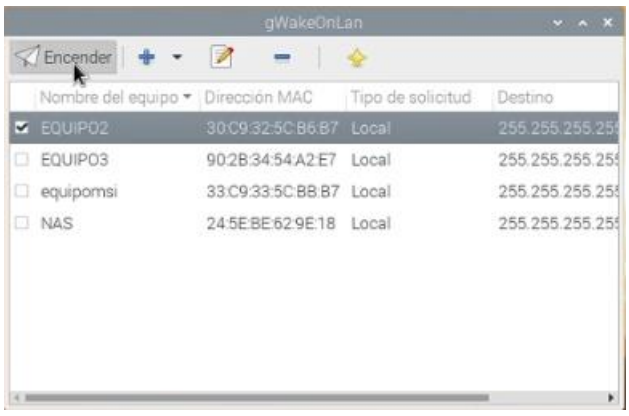


Dentro del escritorio, remotamente se podrán ejecutar los comandos en un terminal como si nos encontrásemos localmente en la ubicación del servidor VPN/WOL.

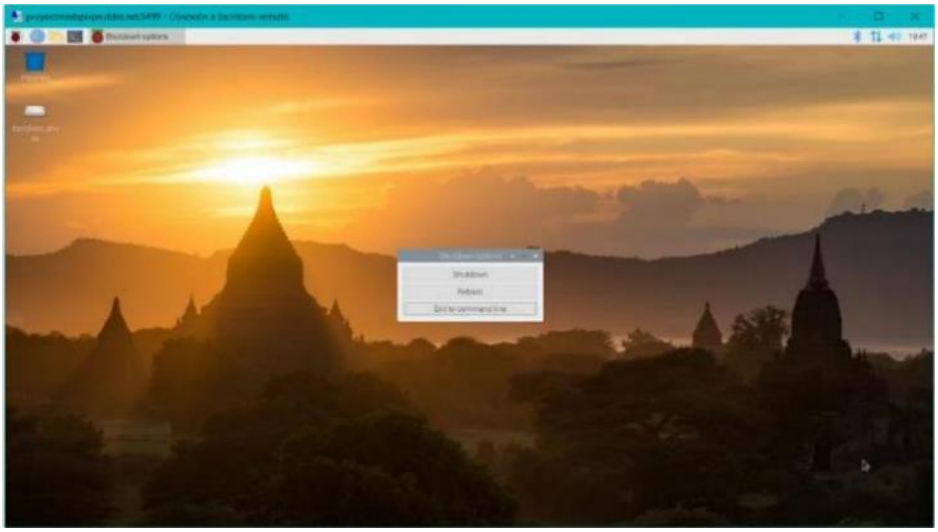




Incluso iniciar la aplicación gwakeonlan e iniciar/arrancar los equipos que se quieran arrancar, seleccionándolo/os y pulsando sobre el botón superior izquierdo Encender.

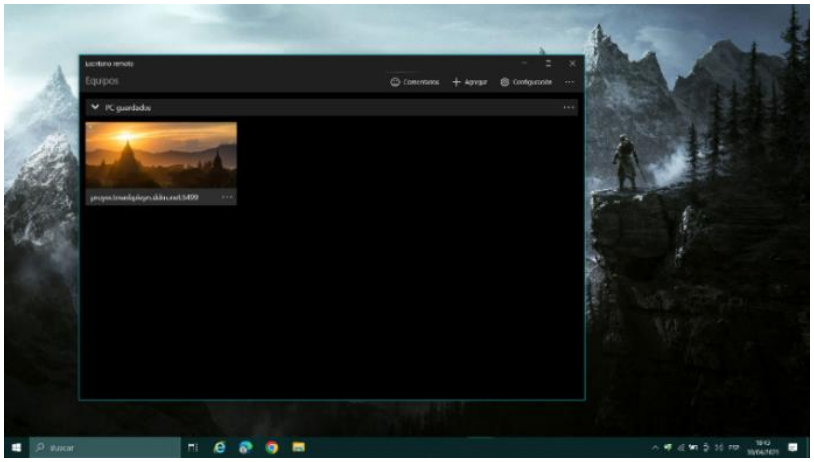


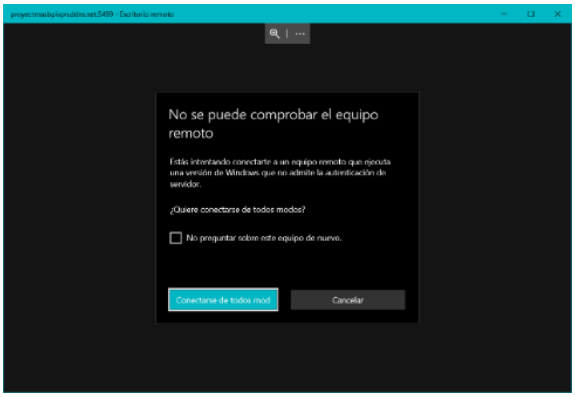




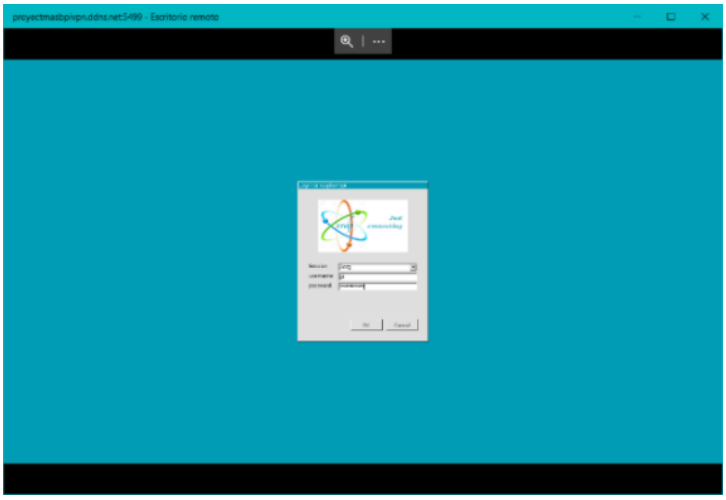
Terminadas las acciones de administración, como se puede apreciar en la captura de la imagen superior, se podrá salir del servidor VPN/WOL, saliendo del entorno gráfico y dejándolo en modo línea de comando.

Se dispone de la aplicación gratuita Escritorio remoto de Microsoft la cual, habrá que descargarla e instalarla desde la tienda de Microsoft.

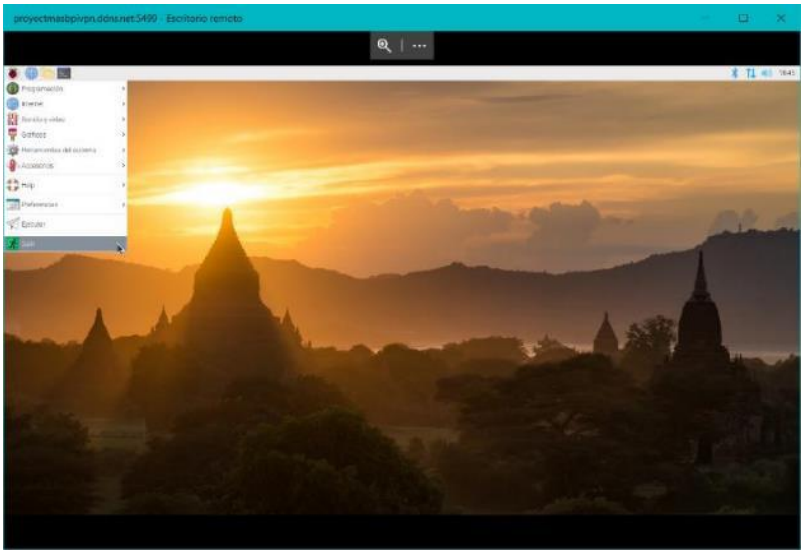


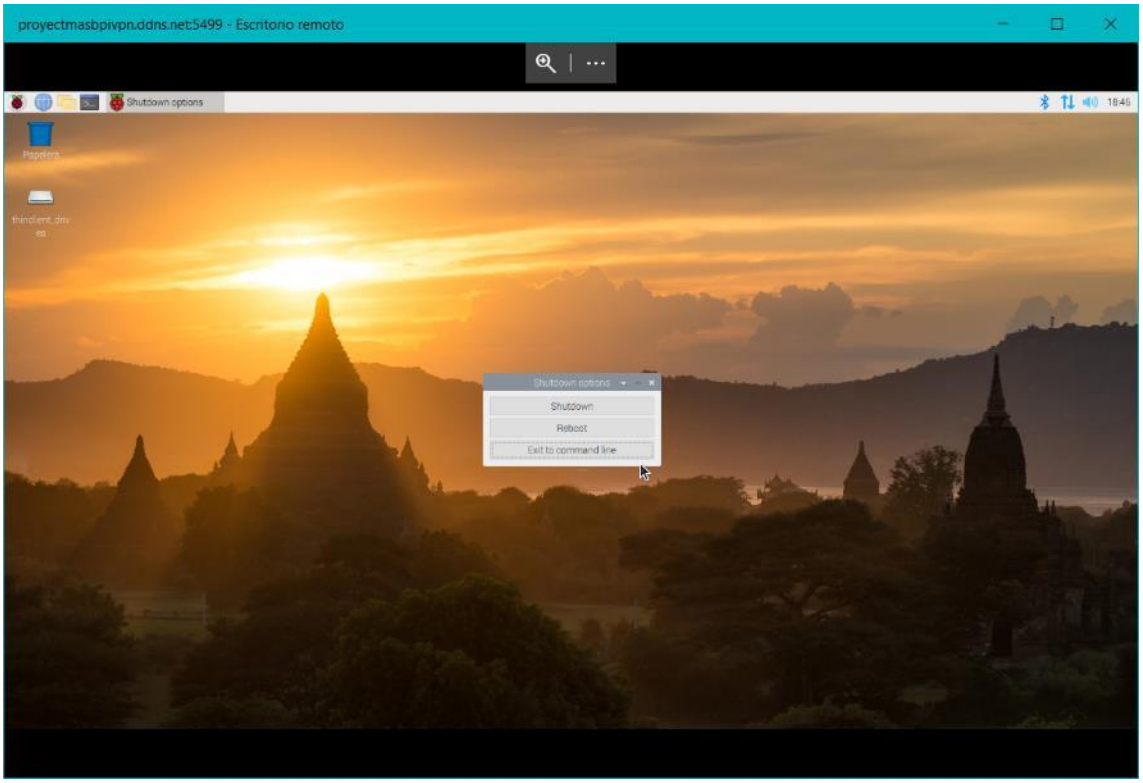


Con la conexión creada, se hará doble clic sobre ella y se pulsará sobre el botón Conectarse de todos modos.



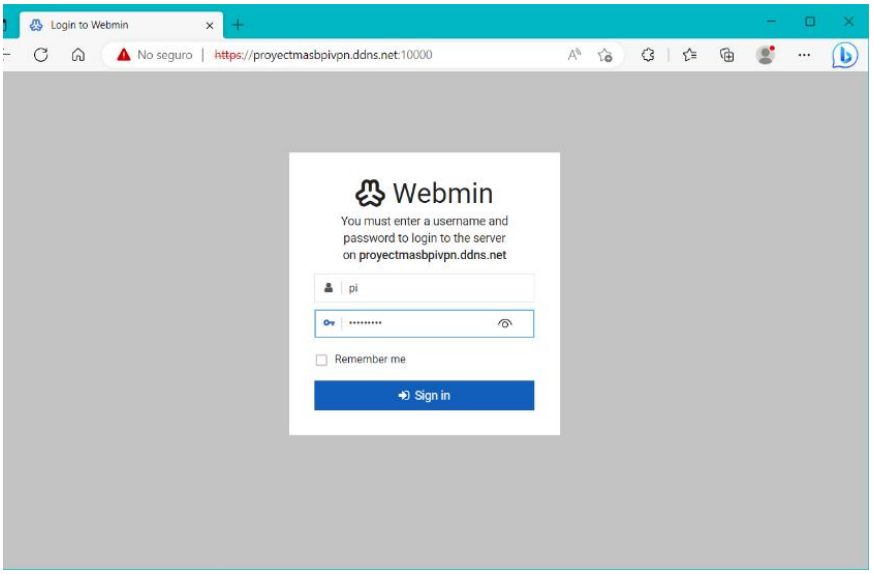
Si no se han proporcionado las credenciales en la configuración se pedirán y se pulsará OK.





Pudiendo realizar las operaciones de administrador dentro de un terminal ejecutar los scripts de arranque de los equipos, iniciar la aplicación grafica gwakeonlan o comprobar el estado de los servicios como otras tareas administrativas.

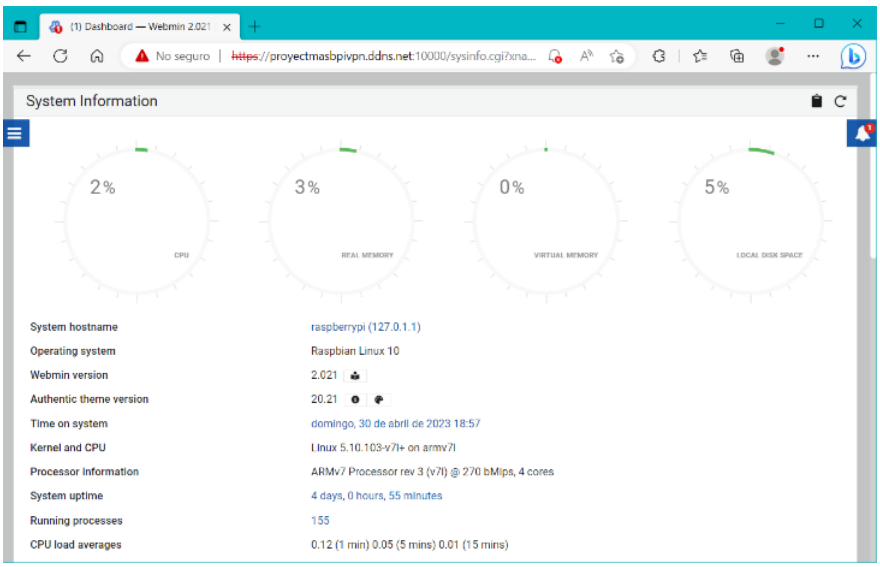
Por último, y aunque hay otros métodos de conexión como VNC, TeamViewer, otro método gratuito es conectarnos mediante WEBMIN.



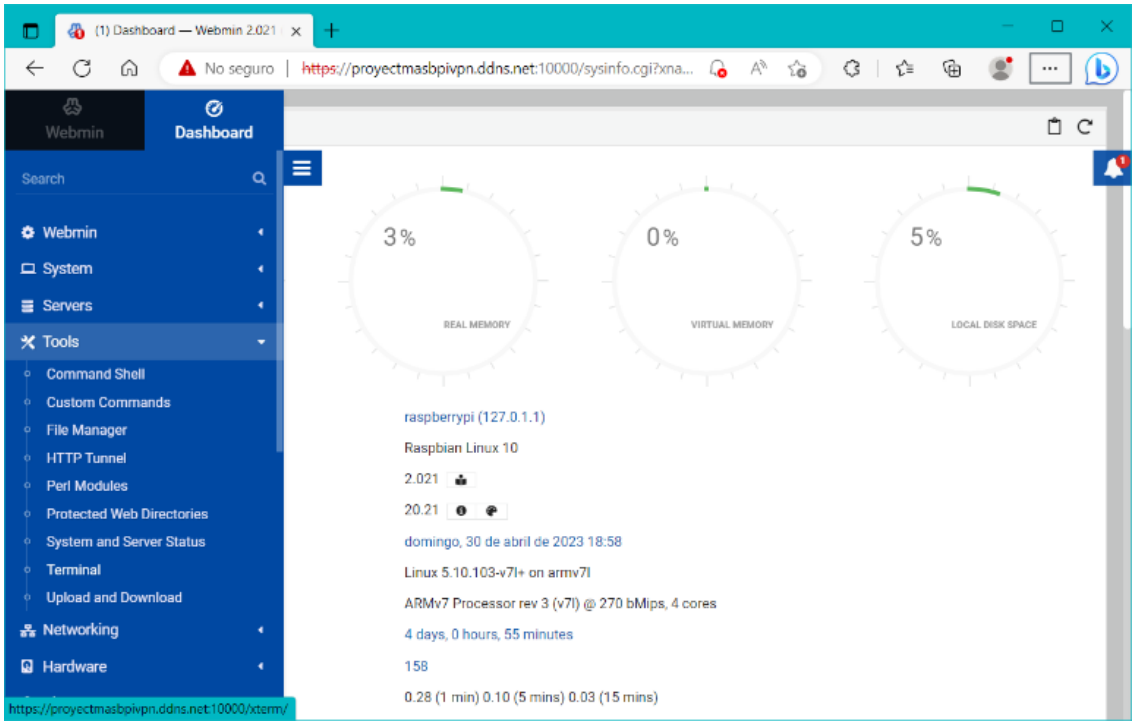
WEBMIN, acceso mediante el navegador, como URL, se colocará el nombre de dominio o host creado en el proveedor de servicio DDNS, con el número de puerto abierto para el acceso a través de WEBMIN, por defecto es el 10000, separado entre ":", el cual habrá que haberlo abierto en el router y habilitar el acceso a través del cortafuegos, cosas que se explicaran.

URL: https://proyectmasbpivpn.ddns.net:10000/

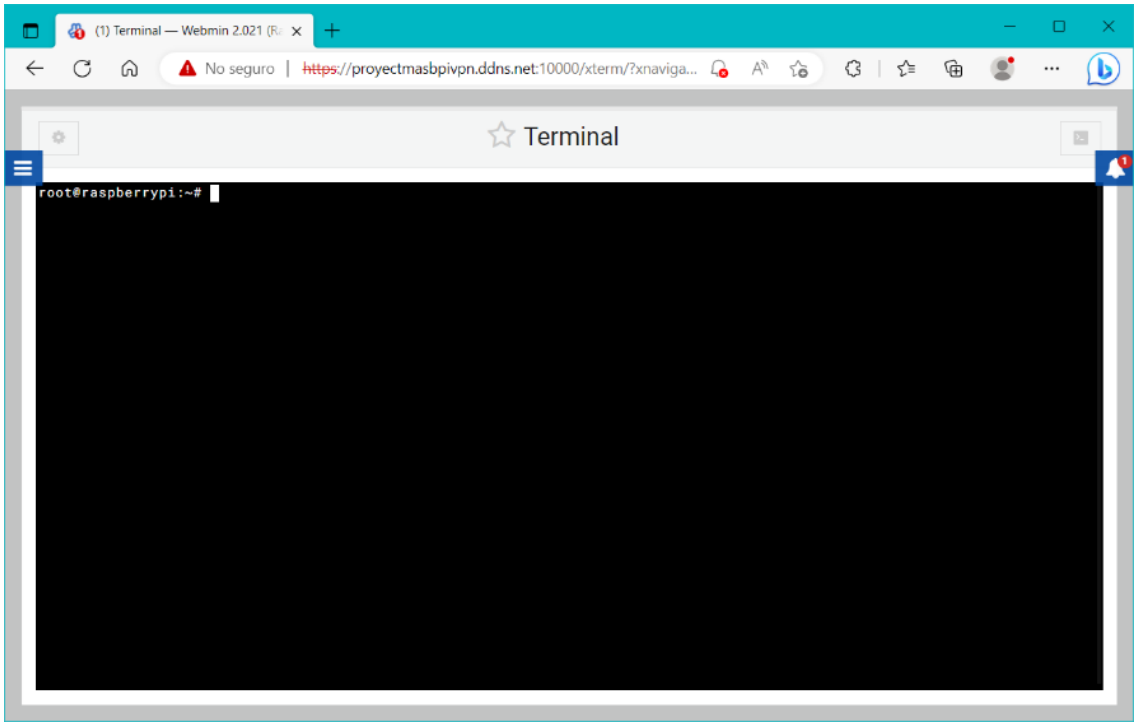
Introducidas las credenciales de acceso se pulsará sobre el botón Sign in.

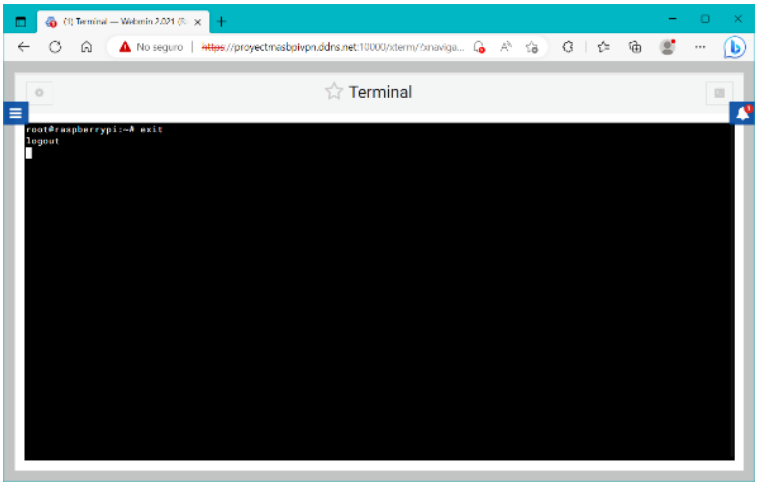


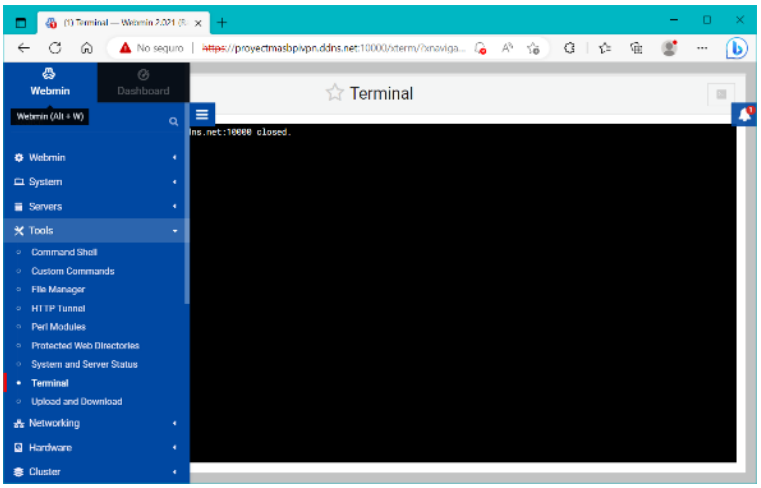
Ventana principal de WEBMIN.



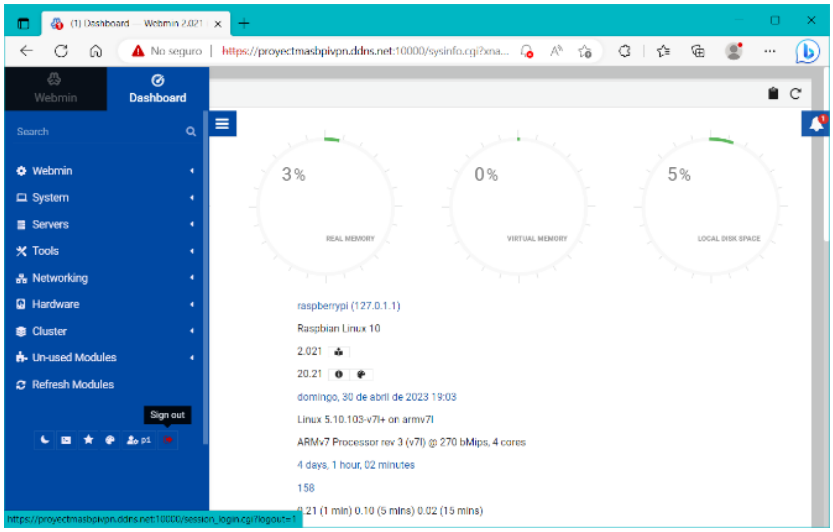
Por la investigación realizada, aun no se ha localizado ningún módulo para el manejo de PiVPN dentro de WEBMIN, aunque si de OpenVPN, no obstante, se podrá manejar y realizar casi las mismas funciones indicadas dentro del terminal de WEBMIN, para ello se pulsará en el panel izquierdo o si no se encuentra abierto sobre las líneas verticales superiores en la parte izquierda, dentro del panel lateral izquierdo se pulsará sobre Tools \ Terminal.







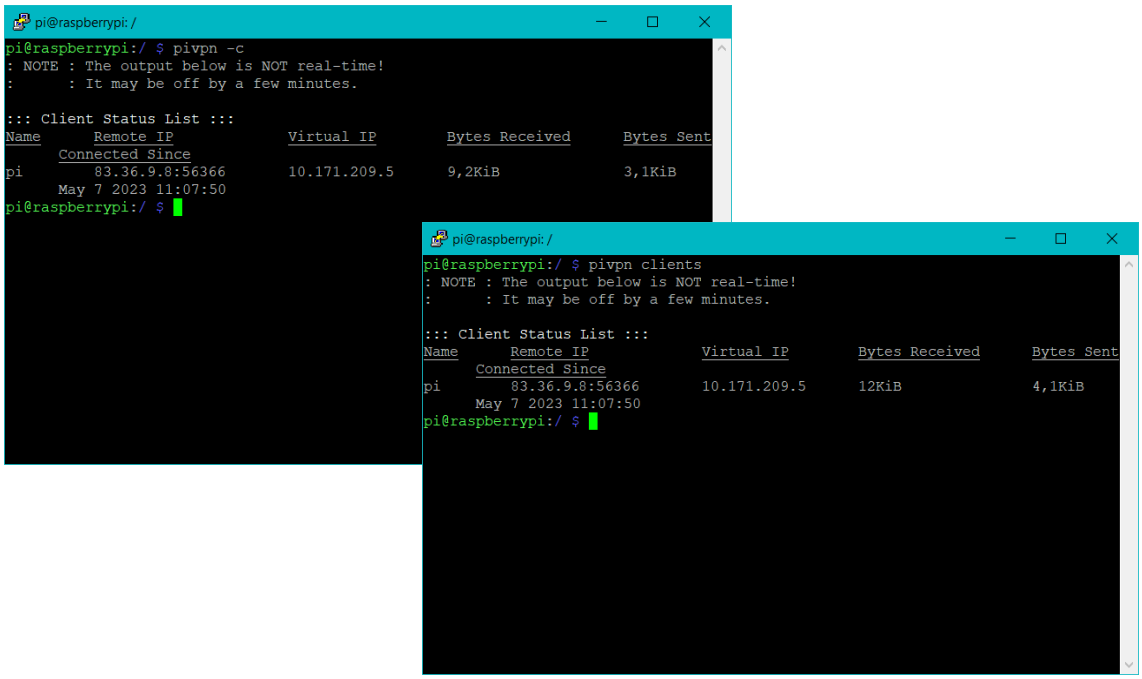
Terminadas las acciones necesarias se saldrá del terminal escribiendo exit y pulsando INTRO.



En el panel derecho para salir, se pulsará sobre el botón superior izquierdo con las letras Webmin  , posteriormente se pulsará en el icono inferior rojo Sign out  .

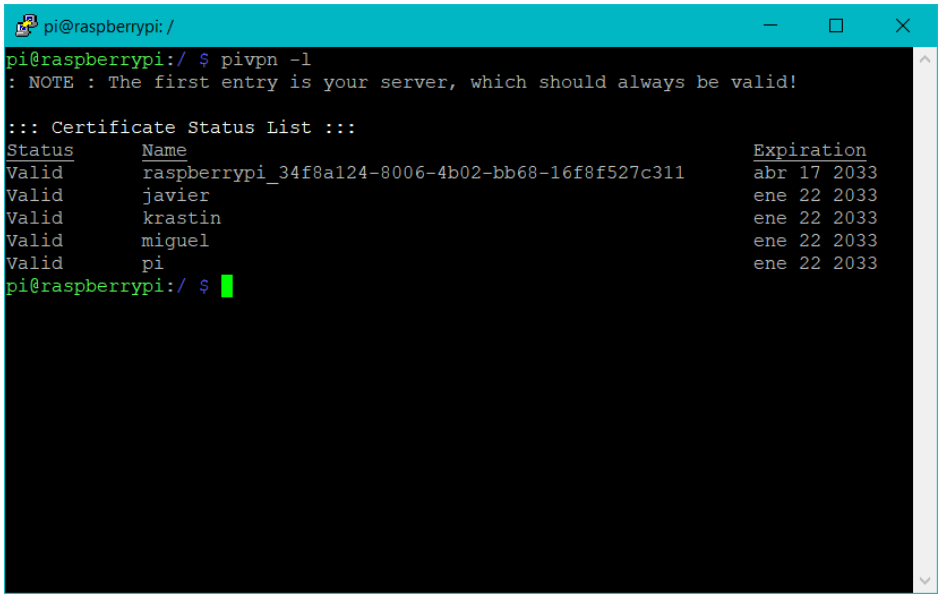
Remotamente conectado al servidor VPN/WOL, se podrán comprobar los clientes conectados a este utilizando los comandos.

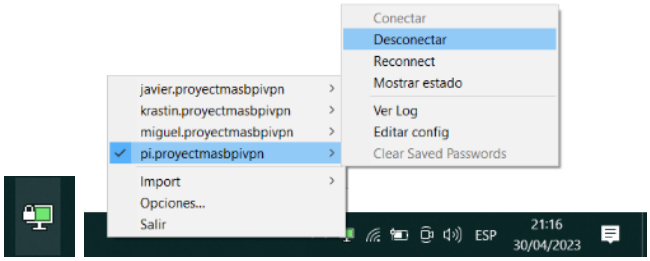
pivpn clients
pivpn -c

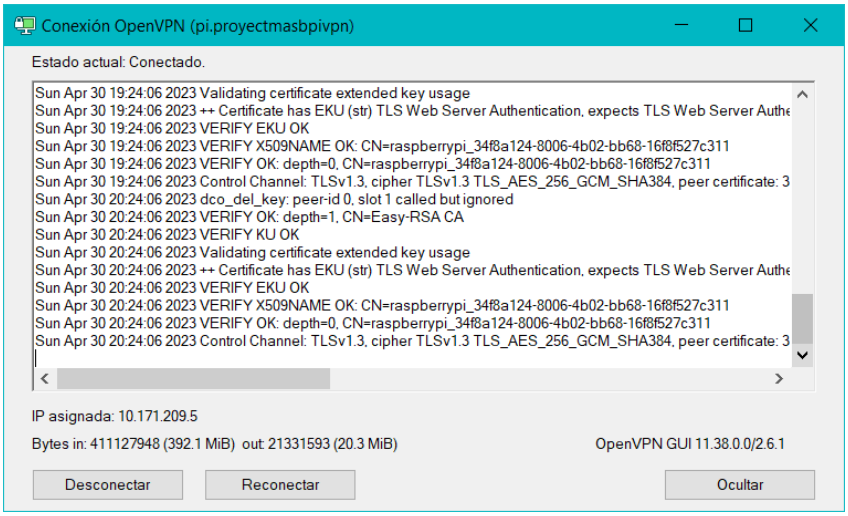


Para comprobar el estado de los clientes se podrá ejecutar el comando.

pivpn -l

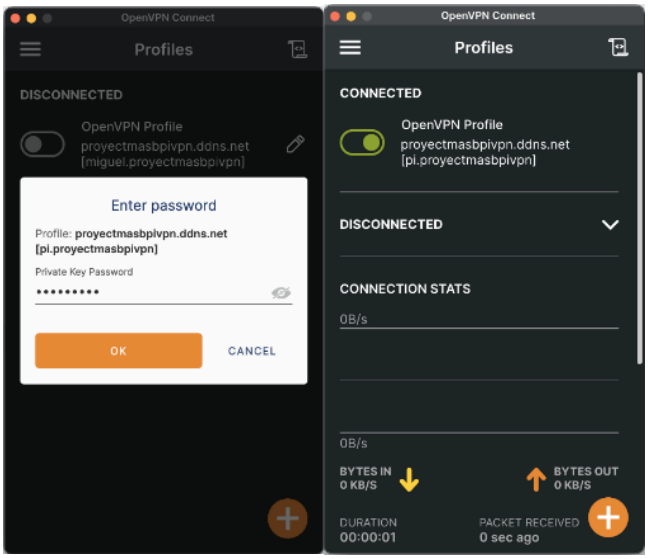






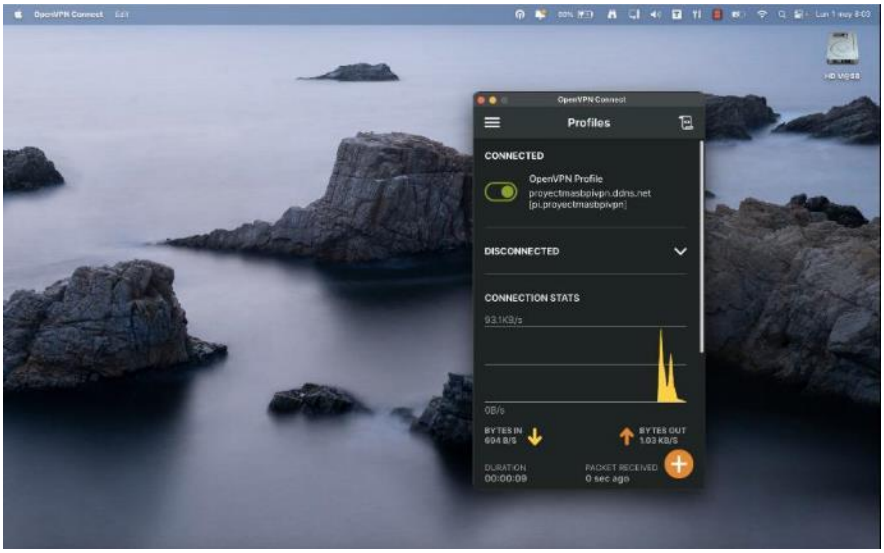
Terminadas todas las acciones de administración, se podrá cerrar las aplicaciones abiertas de control remoto o conexión vía SSH, pudiendo desconectarse de la conexión VPN dentro de la aplicación OpenVPN, como puede apreciarse en la ventana de la captura superior.

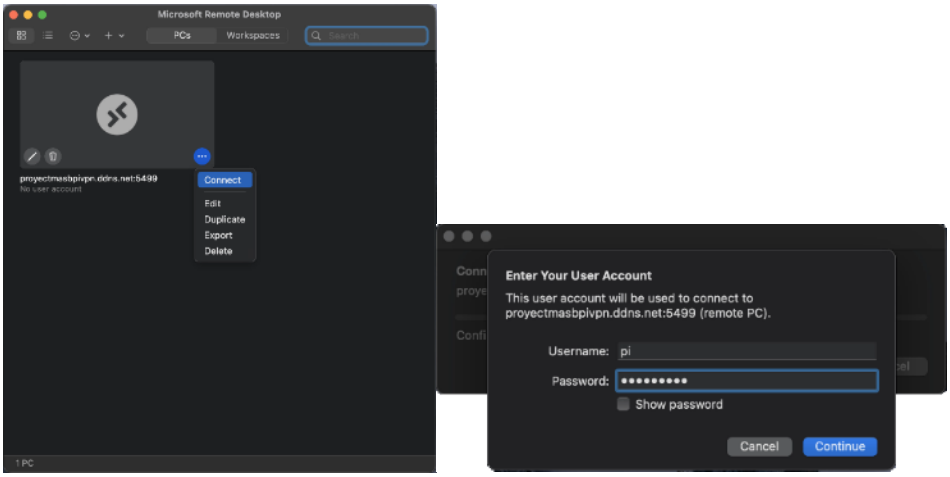
MacOS caso práctico proyecto PiVPN y Wake On LAN WOL.



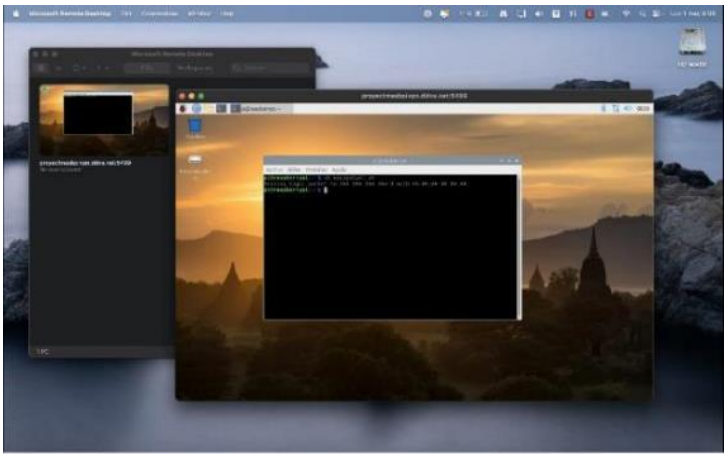
Para este proyecto y en este S.O. es necesario disponer de la aplicación XQuartz instalada, aunque por las pruebas realizadas no es imprescindible que se encuentre en ejecución.

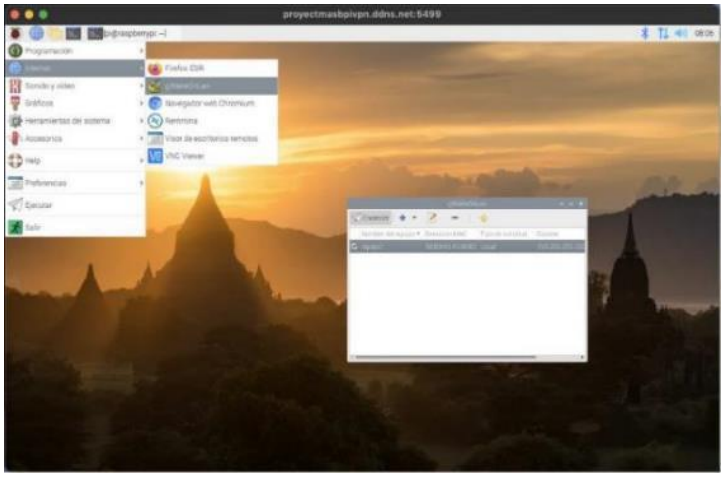
Nuevamente con los ficheros necesarios de conexión creados e importados en la aplicación OpenVPN, se realizará la conexión VPN al servidor VPN/WOL.



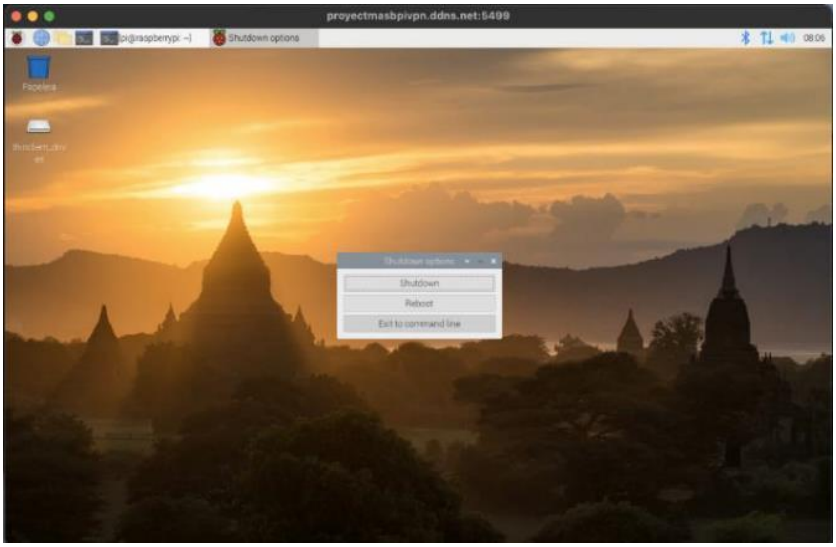


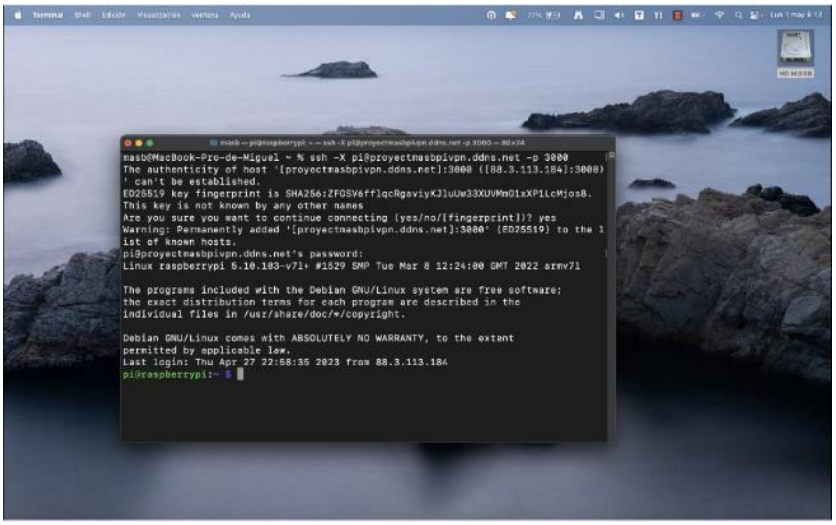
Con la conexión creada dentro Microsoft Remote Desktop se hará doble clic con el botón izquierdo del ratón para iniciar la conexión remota, si no se ha configurado la conexión con el usuario y la contraseña, se solicitará para llevarla a cabo.





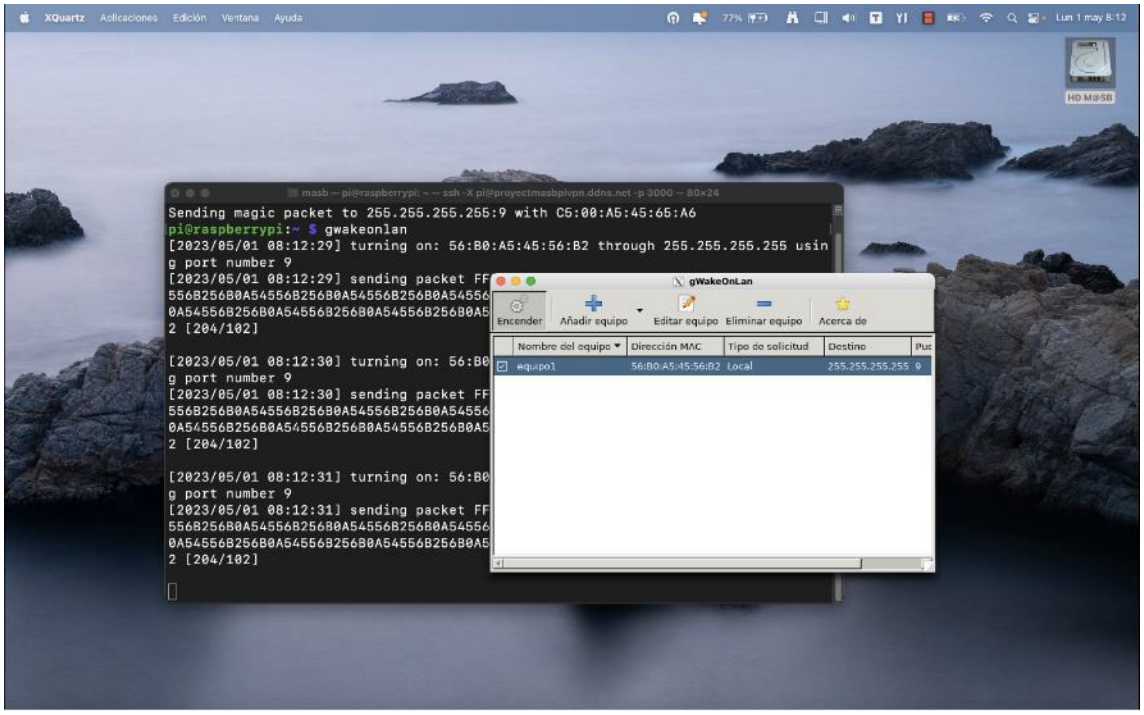
Dentro del escritorio remoto se podrá ejecutar aplicaciones como gwakeonlan, ejecutar los scripts de arranque de los equipos dentro de un terminal.

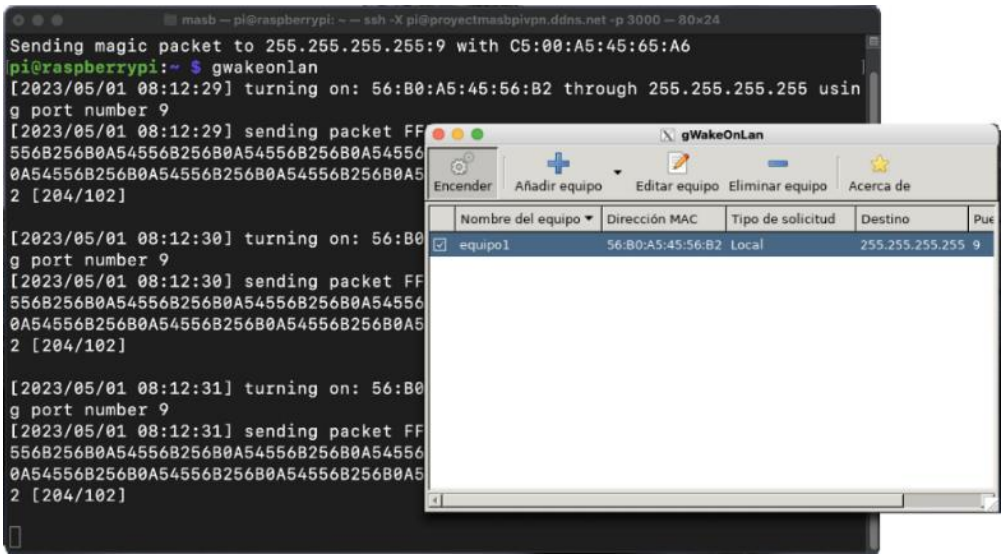




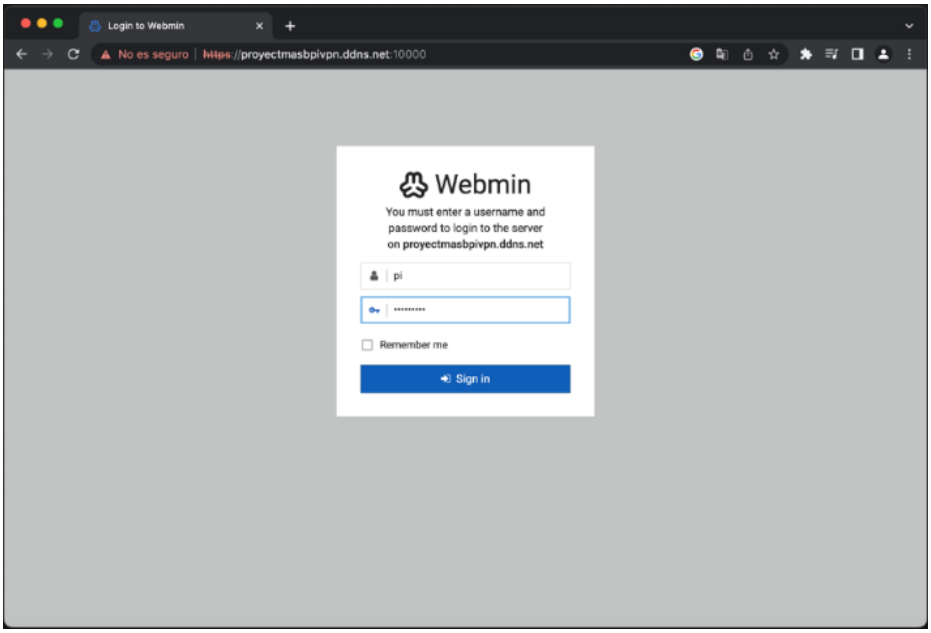


Al conectarse a través de SSH con el comando ssh -X pi@proyectmasbpivpn.ddns.net -p 3000, se podrán ejecutar los scripts de arranque desde ese terminal como si estuviésemos delante del servidor VPN/WOL.





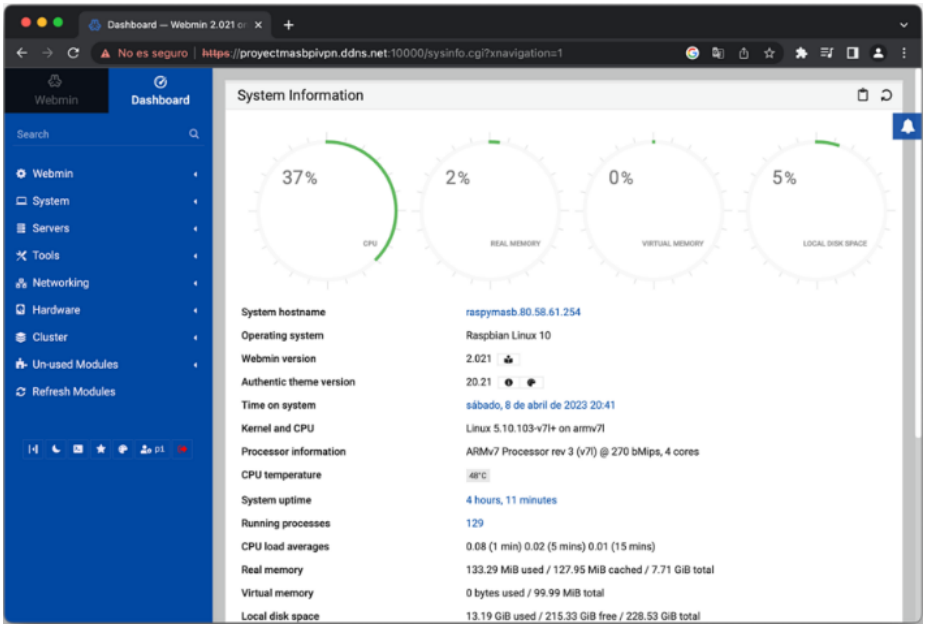
También se podrá iniciar en el equipo remoto aplicaciones graficas al haber ejecutado el comando de conexión SSH con la opción -X

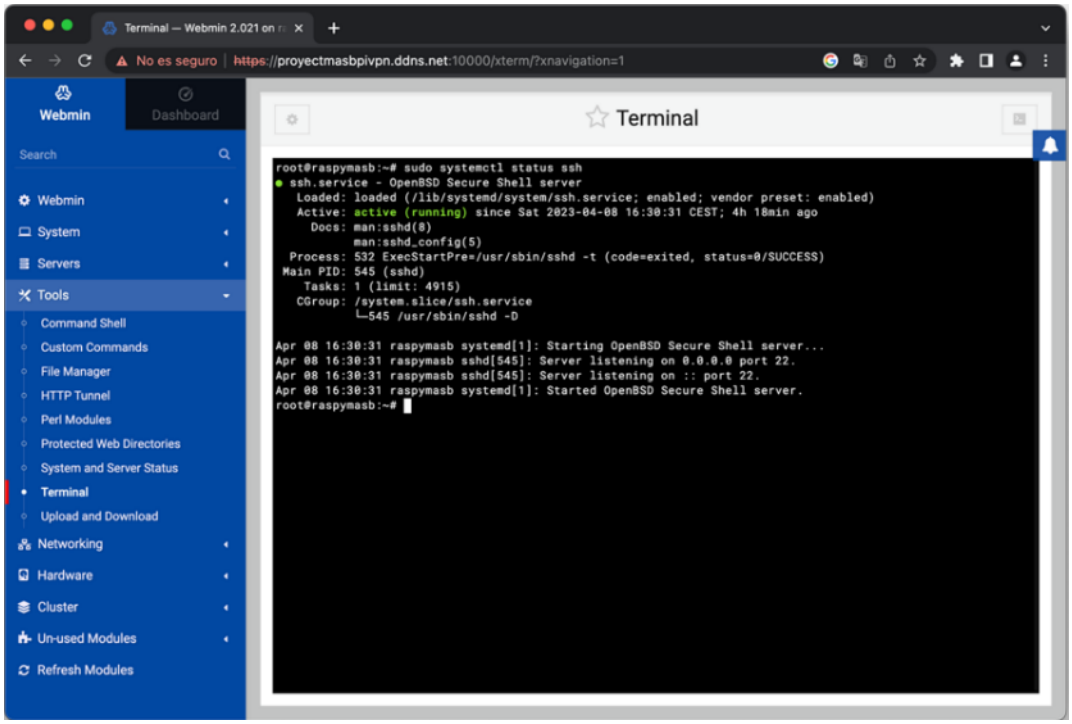


Otra opción será acceder a través del navegador utilizando WEBMIN, colocando como URL el nombre de dominio o host creado en el proveedor de servicios de DDNS, junto con el puerto 10000 abierto en el router separado por ":", y habilitado el tráfico en el cortafuegos en el servidor VPN/WOL.

URL: https://proyectmasbpivpn.ddns.net:10000/

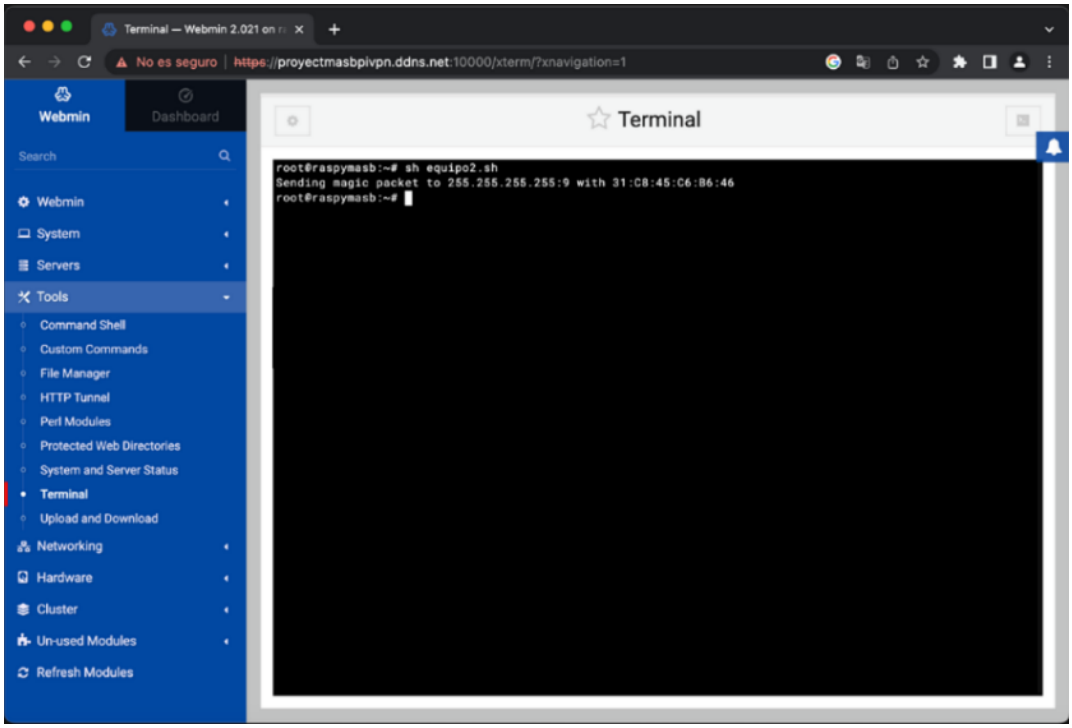
Se facilitarán las credenciales de acceso y se pulsara sobre el botón Sign in.



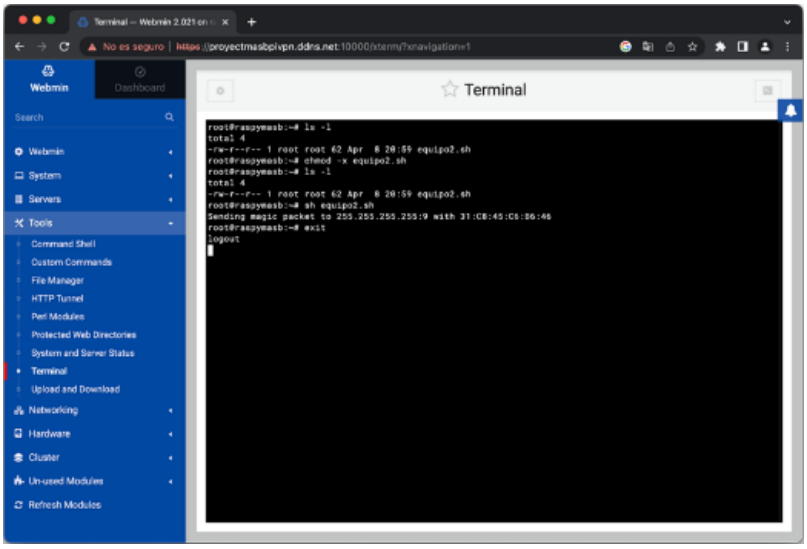


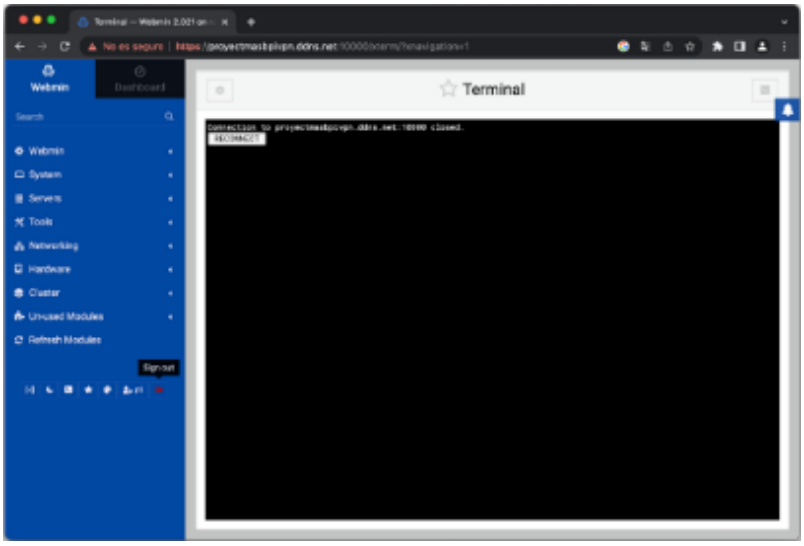
En el panel derecho, se podrá acceder a un terminal ubicado en Tools \ Terminal.

Pudiendo dentro del terminal remoto realizar acciones de administración comprobar, iniciar o parar servicios.



Ejecutar los scripts para iniciar/arrancar los equipos necesarios.

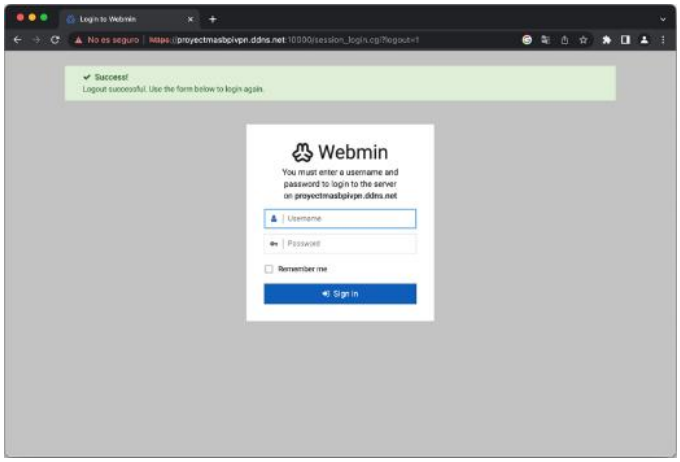




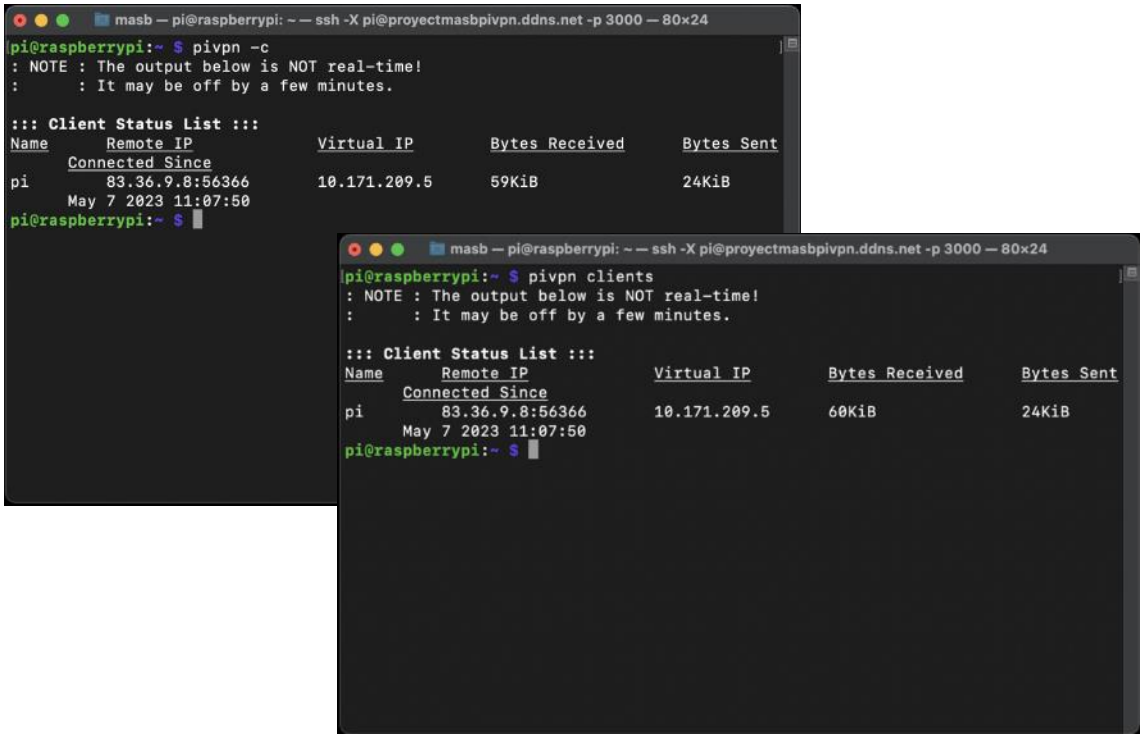
Terminadas las acciones necesarias, se podrá desconectar del terminal remoto escribiendo exit y pulsando INTRO, para salir de WEBMIN, habrá que desconectarse pulsando en el botón superior izquierdo 

, para posteriormente pulsar sobre el icono de color rojo inferior 

.

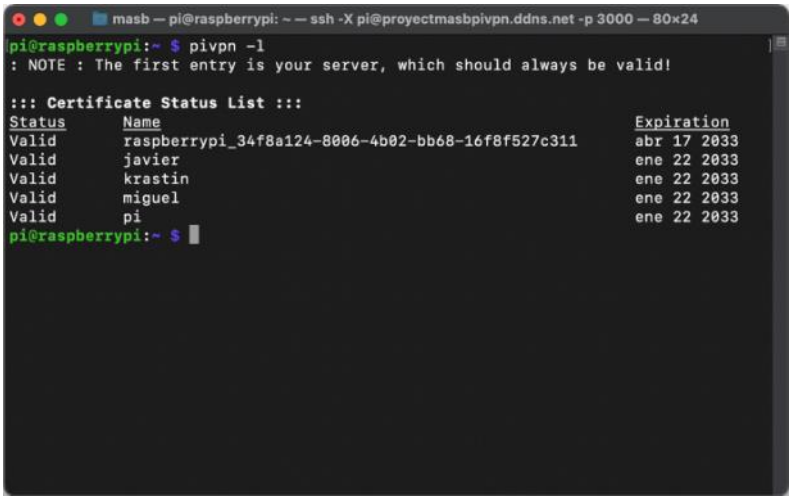


Terminadas las acciones de administración se podrá desconectar de la conexión VPN.



Como usuario administrador y estando conectado al servidor VPN/WOL (Raspberry Pi), vía SSH, se podrá ver los usuarios conectados al servidor con los comandos.

pivpn -c
pivpn clients



Incluso se podrá comprobar el estado de los usuarios creados en el servidor VPN/WOL con el comando.

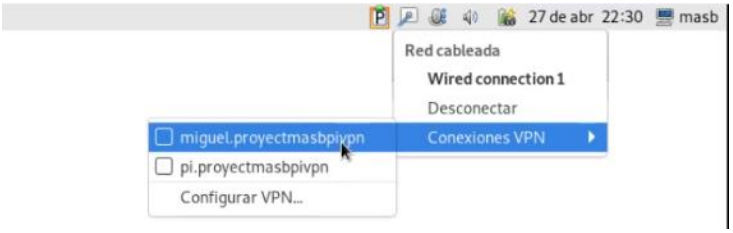
pivpn -l

Terminadas las acciones administrativas se podrá desconectar del servidor VPN/WOL.

Linux caso práctico proyecto PiVPN y Wake On LAN WOL.

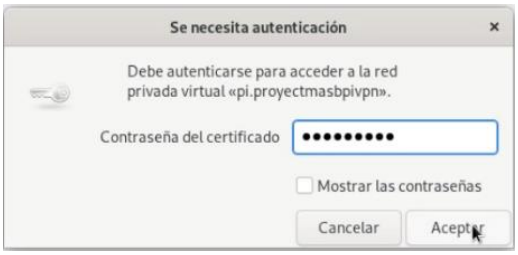
Todas estas explicaciones pueden variar, dependiendo con el tipo de escritorio con el que se acceda a la sesión de usuario, dentro de la distribución de Linux que se esté utilizando, en este caso se trata de la distribución de Linux Debian.



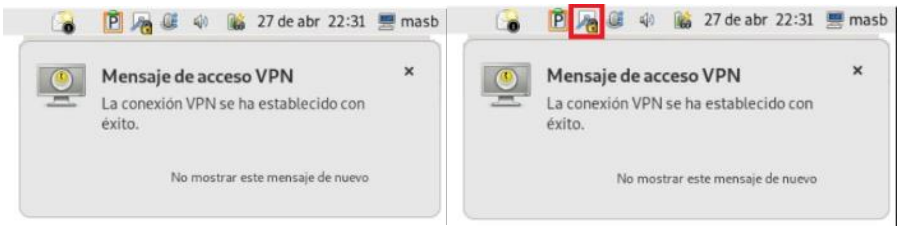


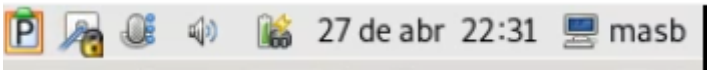
Para realizar la conexión VPN, se pulsará con el botón izquierdo del ratón sobre el icono , ubicado en la barra superior derecha.

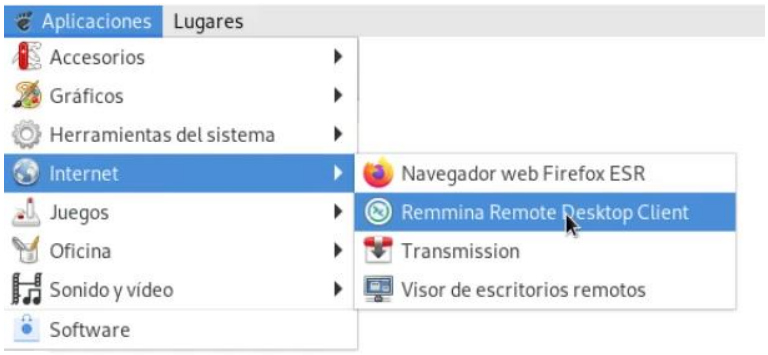




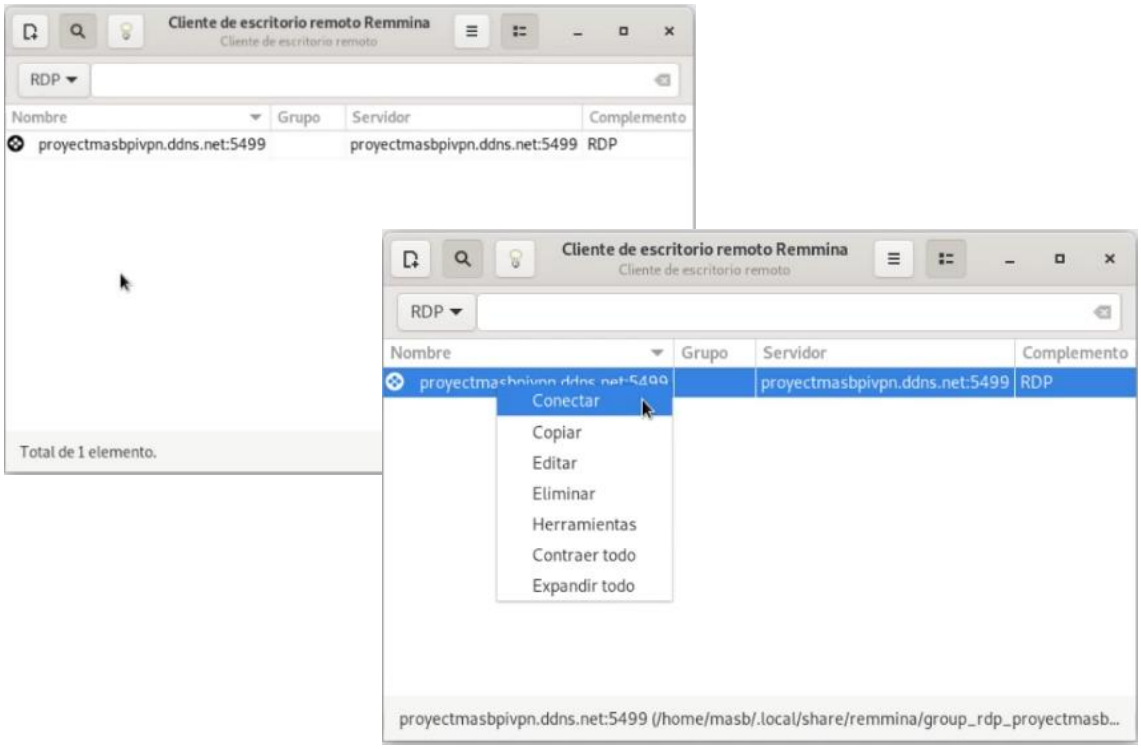
En caso de no haber facilitado la contraseña de conexión, al ir a conectarse con el perfil se solicitará la contraseña de acceso y se pulsará el botón Aceptar.



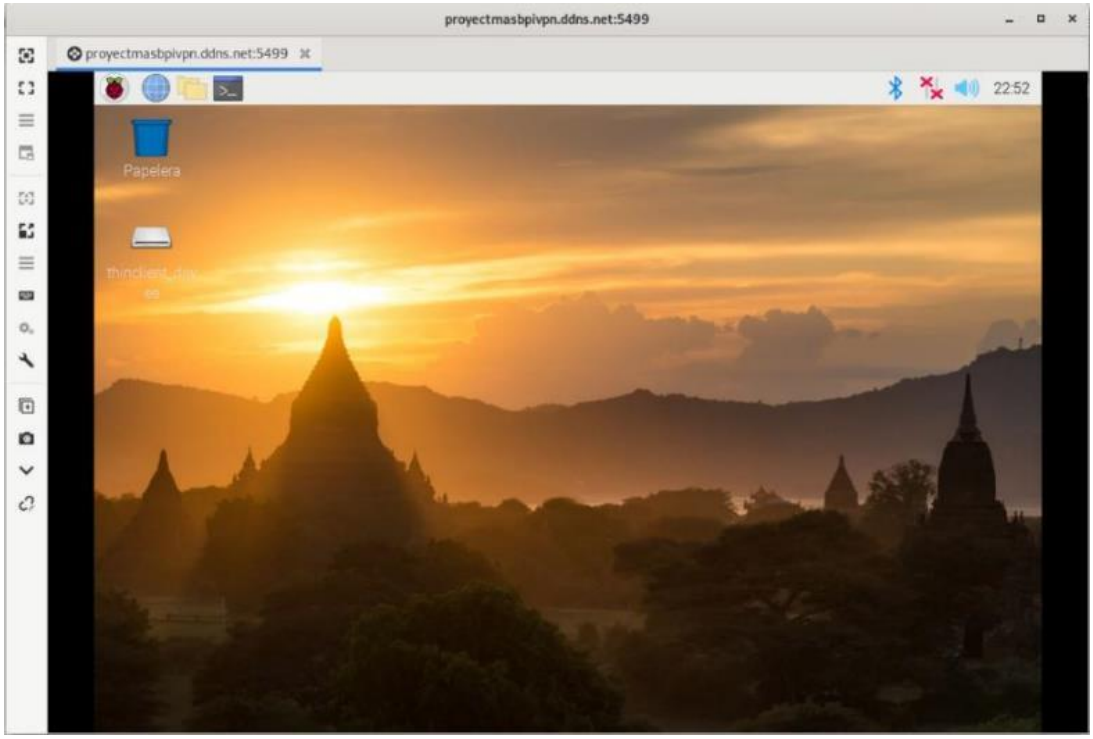




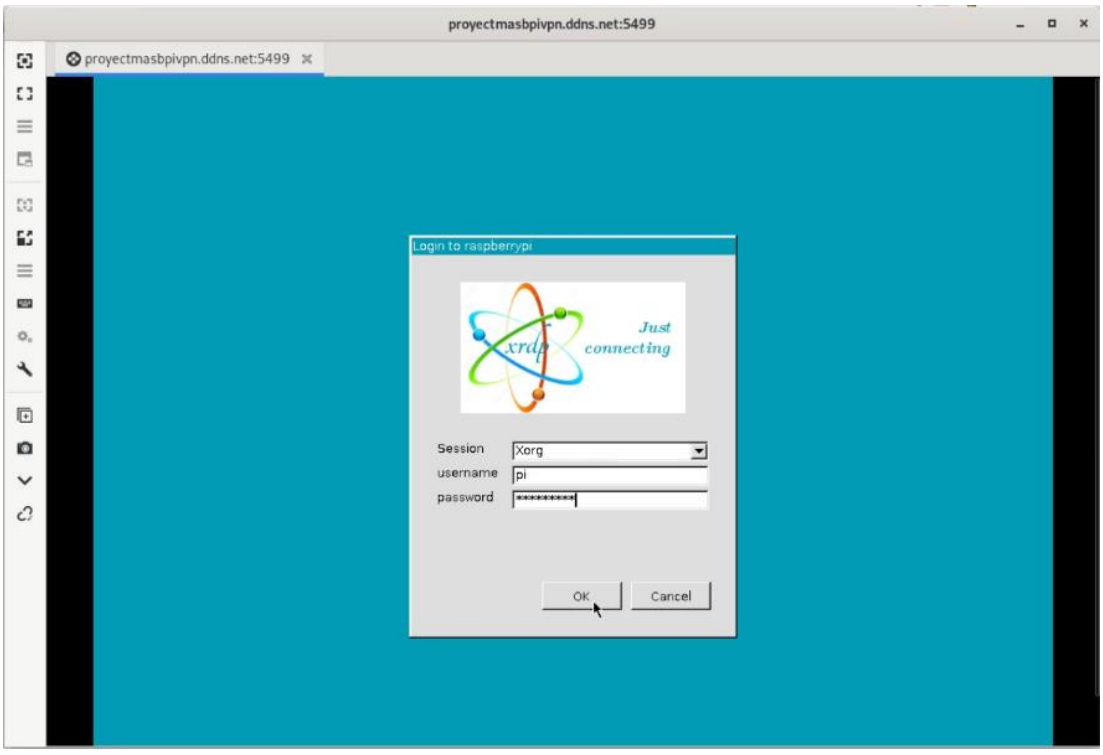
En el menú Aplicaciones ubicado en la barra superior izquierda, se pulsará con el botón izquierdo del ratón sobre el apartado Internet y por último se pulsará sobre Remmina Remote Desktop Client.



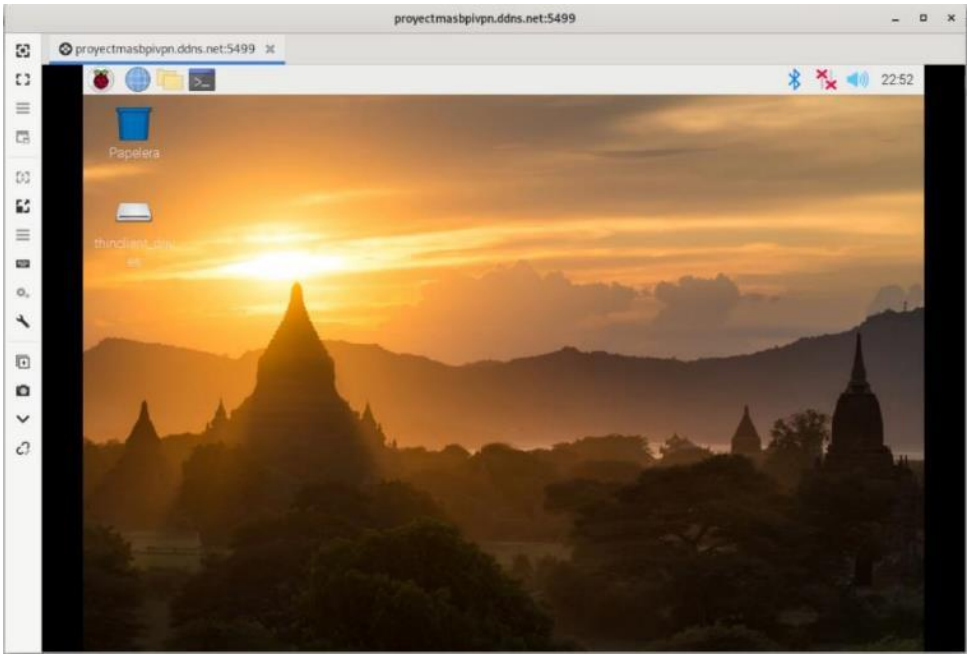
Dentro de la aplicación, se podrá seleccionar con el botón derecho del ratón la conexión creada al servidor VPN/WOL y en el menú emergente se podrá pulsar sobre Conectar, o se podrá hacer doble clic con el botón izquierdo del ratón sobre la miniatura creada a la conexión, para abrir dicha conexión.

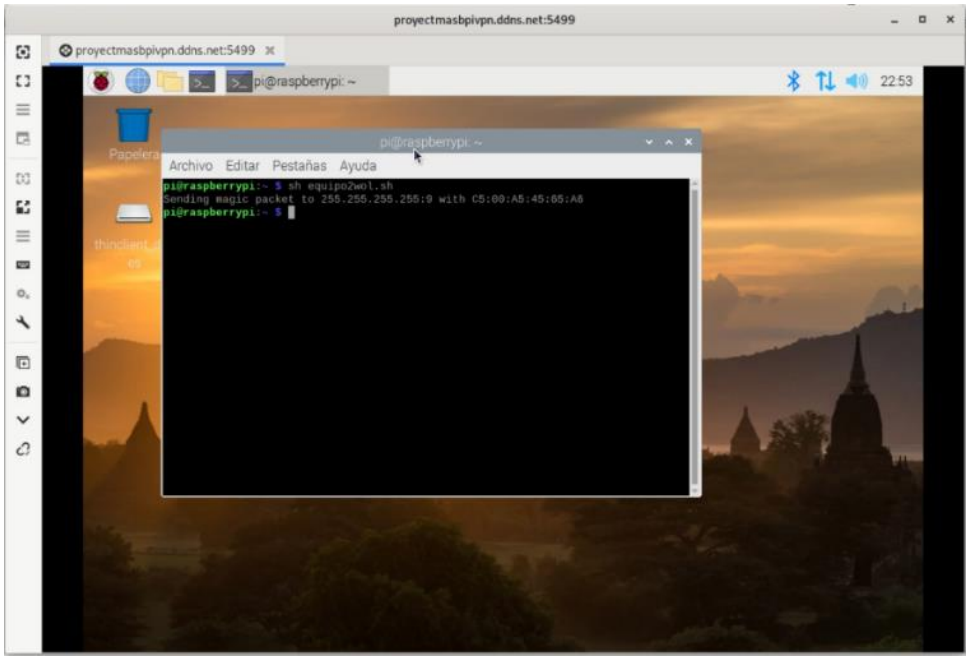


En el caso de haber proporcionado la contraseña de la conexión se realizará sin requerir más intervención.

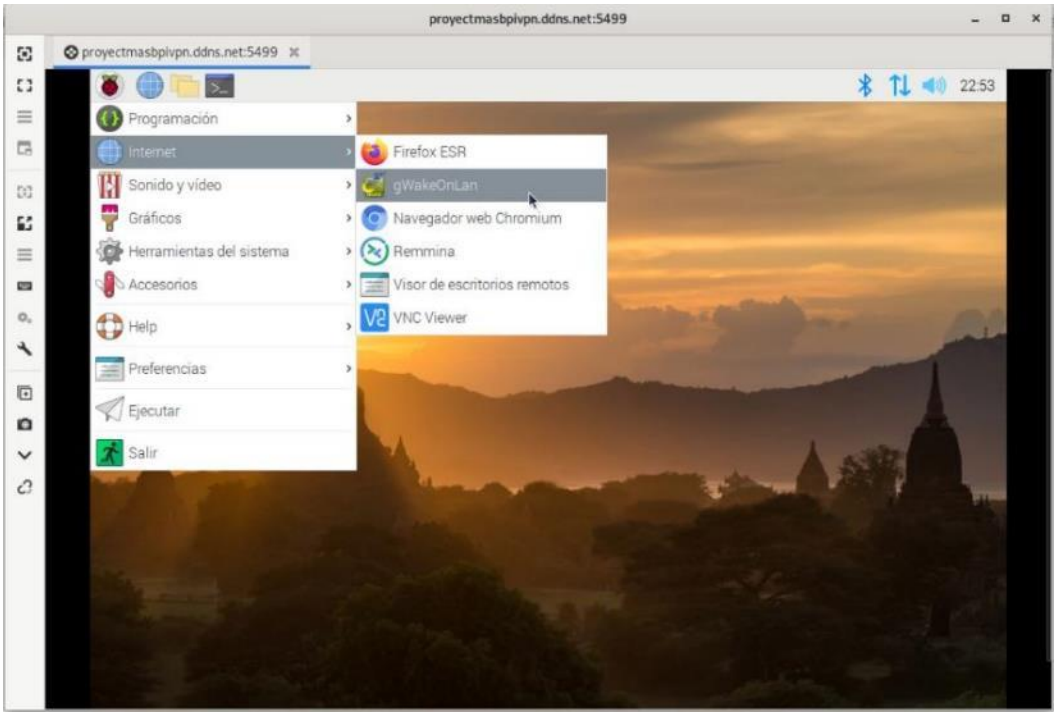


Si no se facilitó la contraseña a la hora de la configuración será necesario proporcionarla para poder llevar a cabo la conexión con el escritorio remoto.

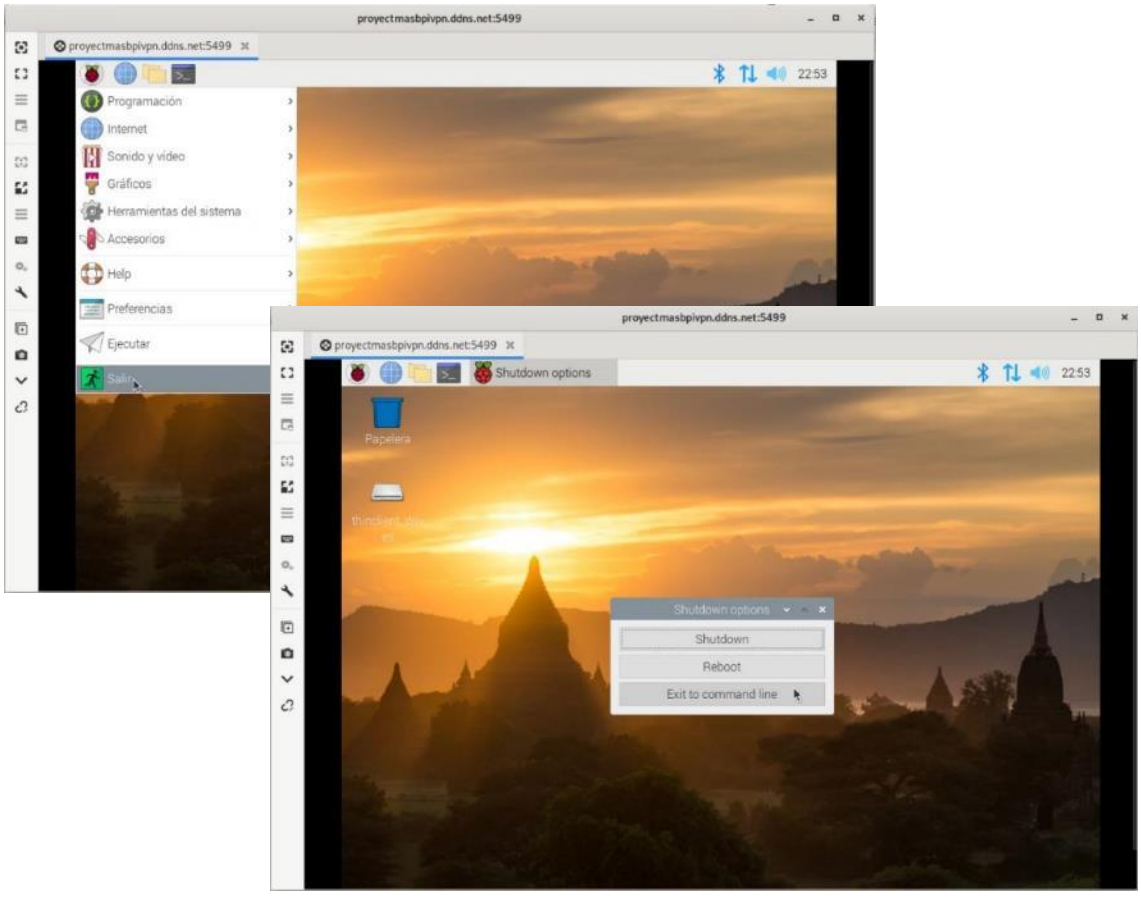


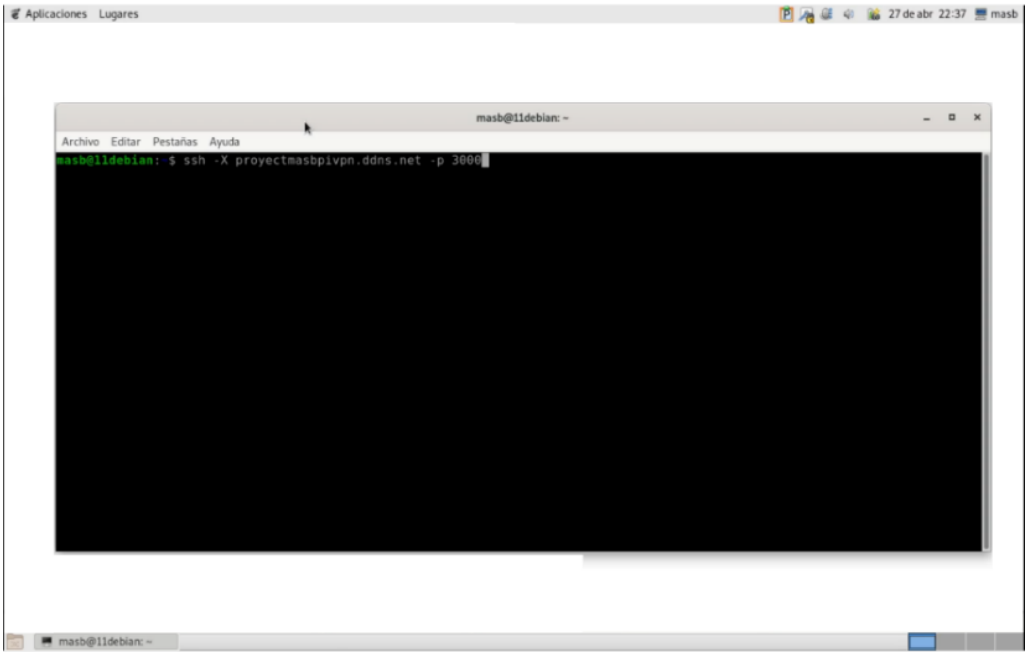


Una vez dentro del escritorio remoto, se podrá abrir un terminal y ejecutar el script o los scripts necesarios para arrancar/encender los equipos.

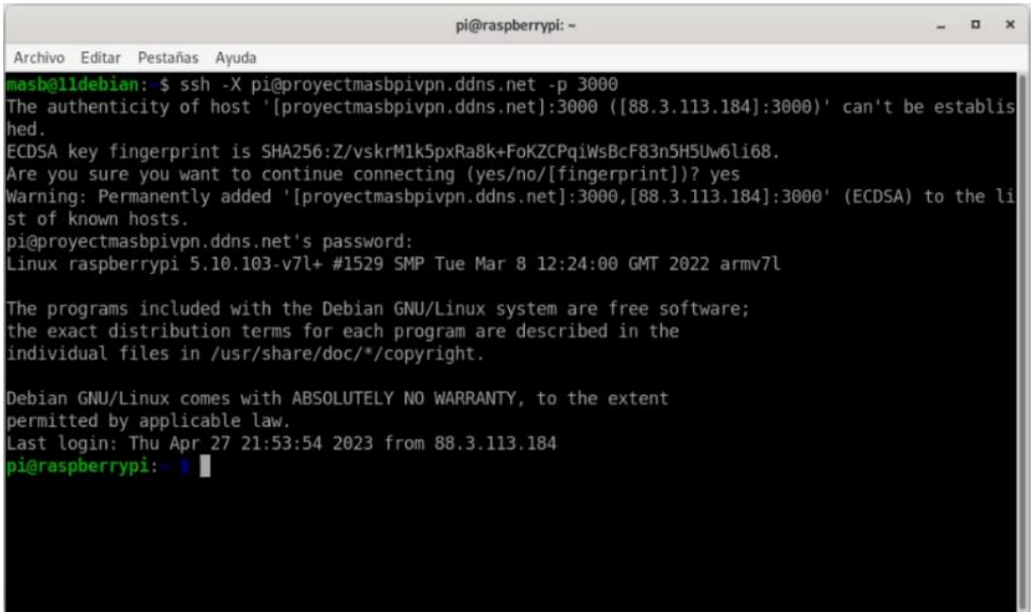


Iniciar la aplicación grafica gwakeonlan para hacerlo de una manera más grafica.





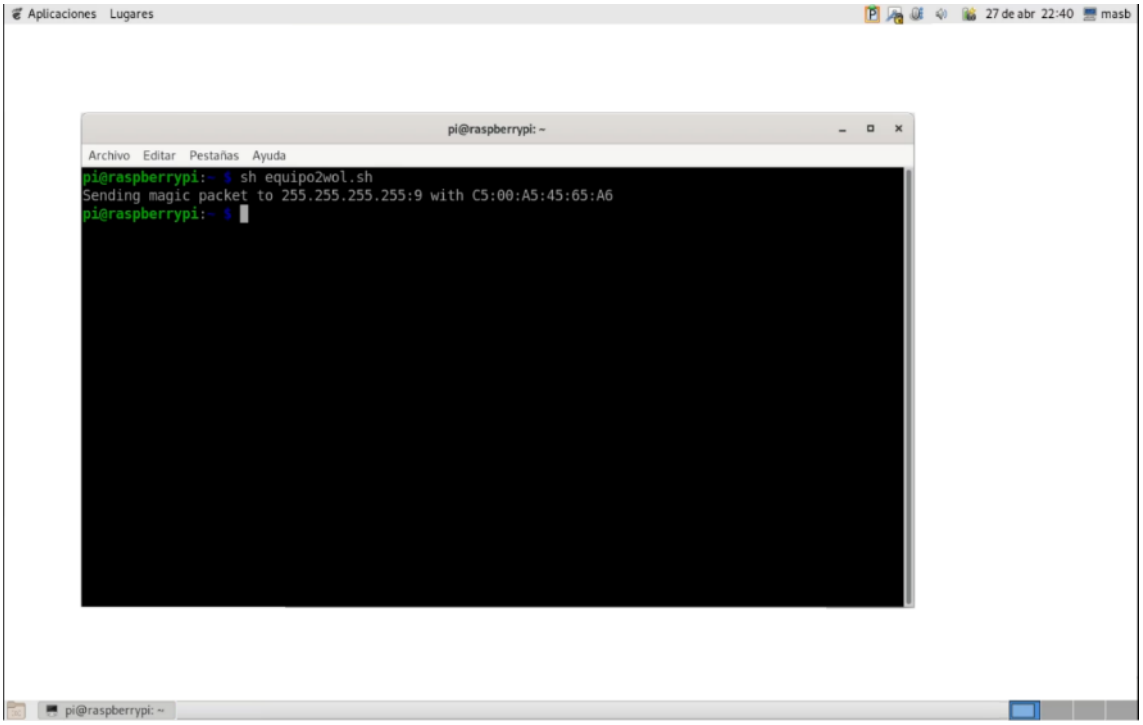
Otra manera como se puede observar en la ventana de la captura superior, dentro de un terminal del cliente Linux, es ejecutar el comando para conectarse vía SSH al servidor VPN/WOL.



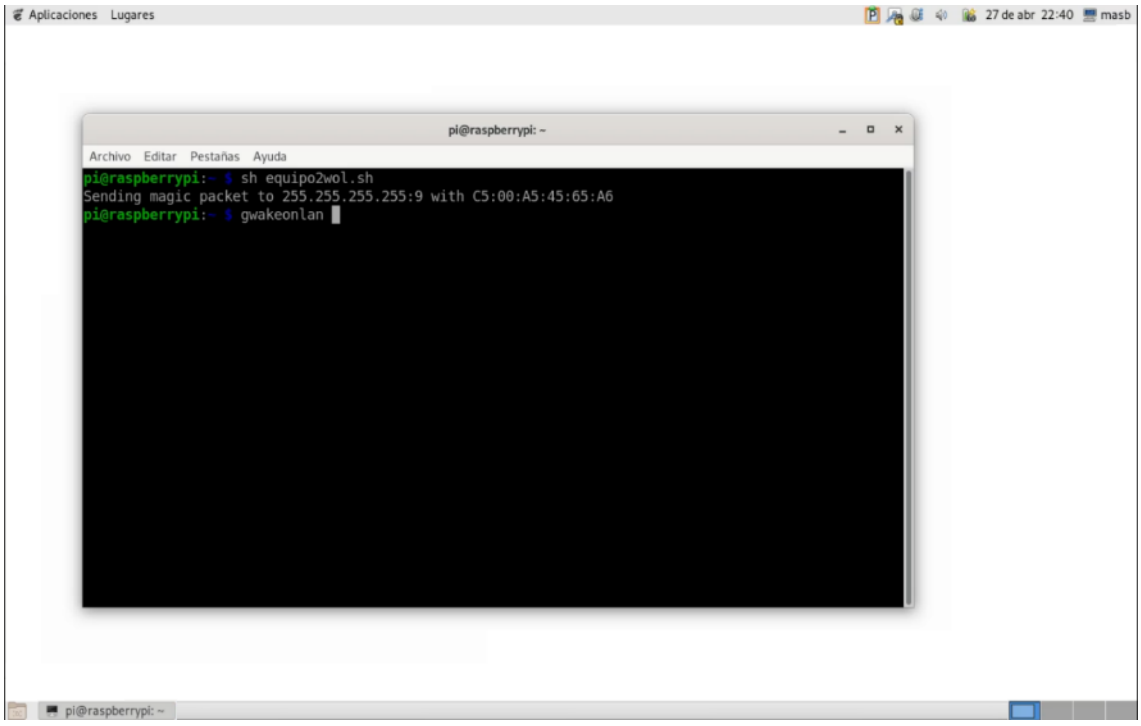
Al ejecutar el comando.

ssh -X proyectmasbpivpn.ddns.net -p 3000

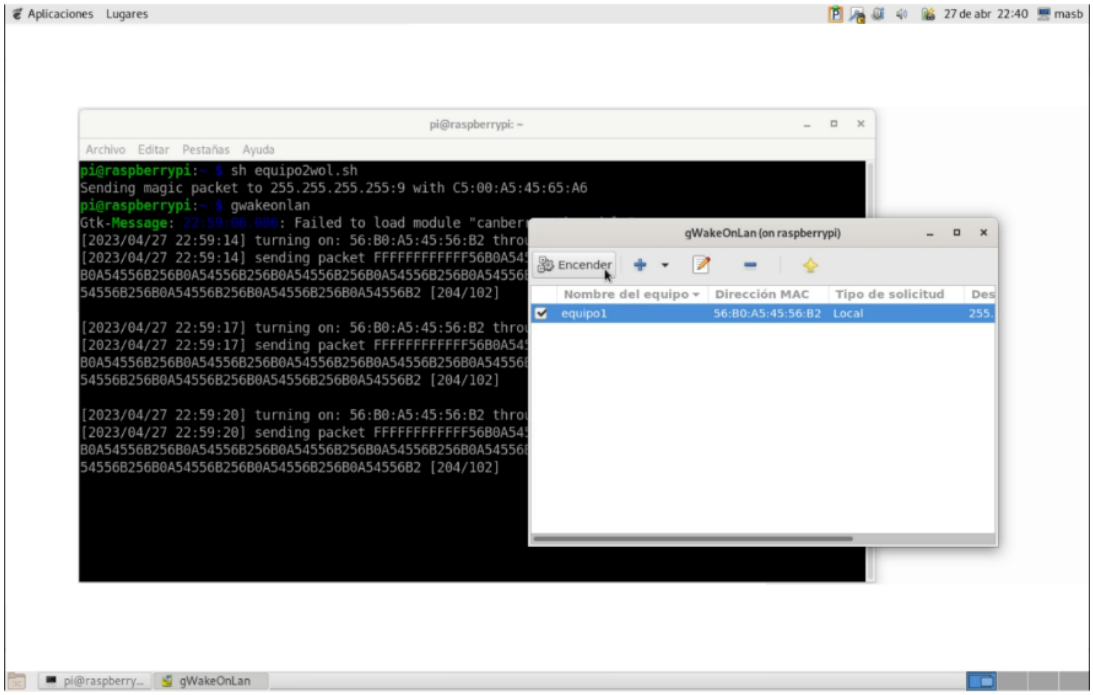
Se conectará al servidor VPN/WOL vía SSH a través del puerto 3000 que fue configurado en el fichero de configuración del protocolo SSH como abierto en el router y habilitado el tráfico en el cortafuegos, todo se indicara en los sucesivos apartados.

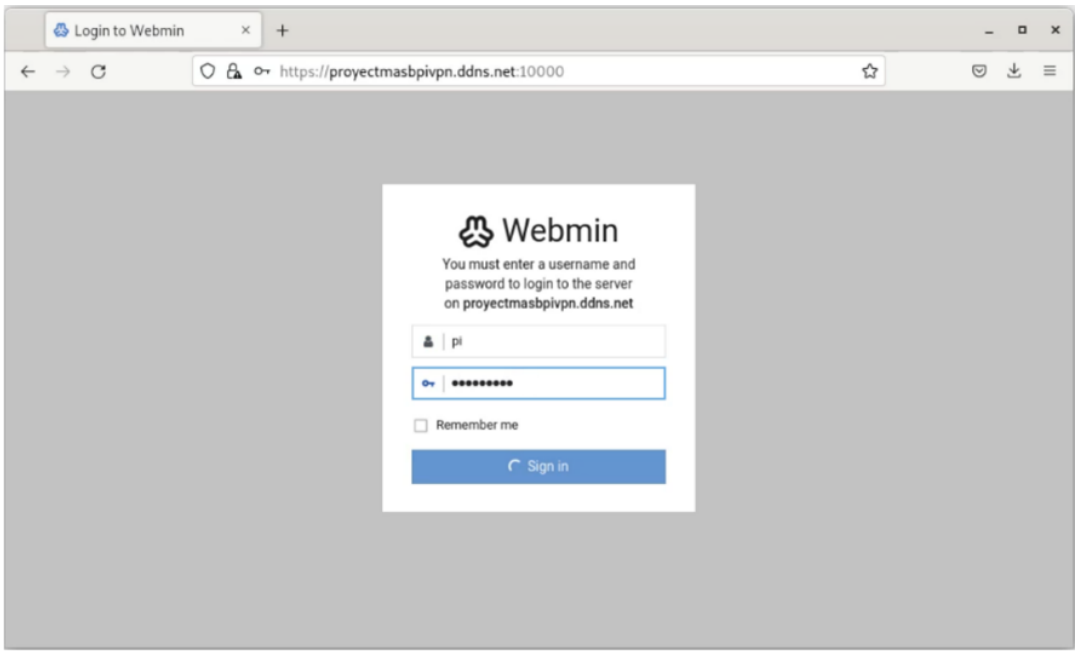


En este caso, nuevamente se podrá ejecutar los scripts para arrancar los equipos dentro de la consola remota.



Sin la necesidad de tener ninguna aplicación instalada, lanzar la aplicación grafica remotamente al haber ejecutado el comando de conexión con la opción (-X).

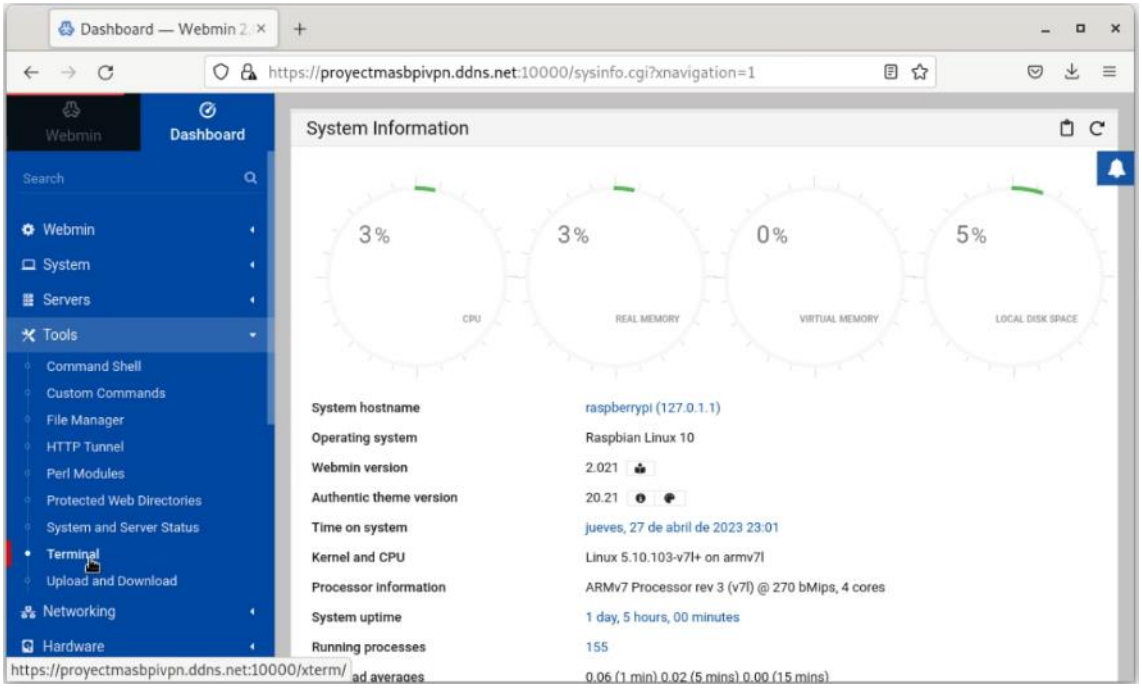




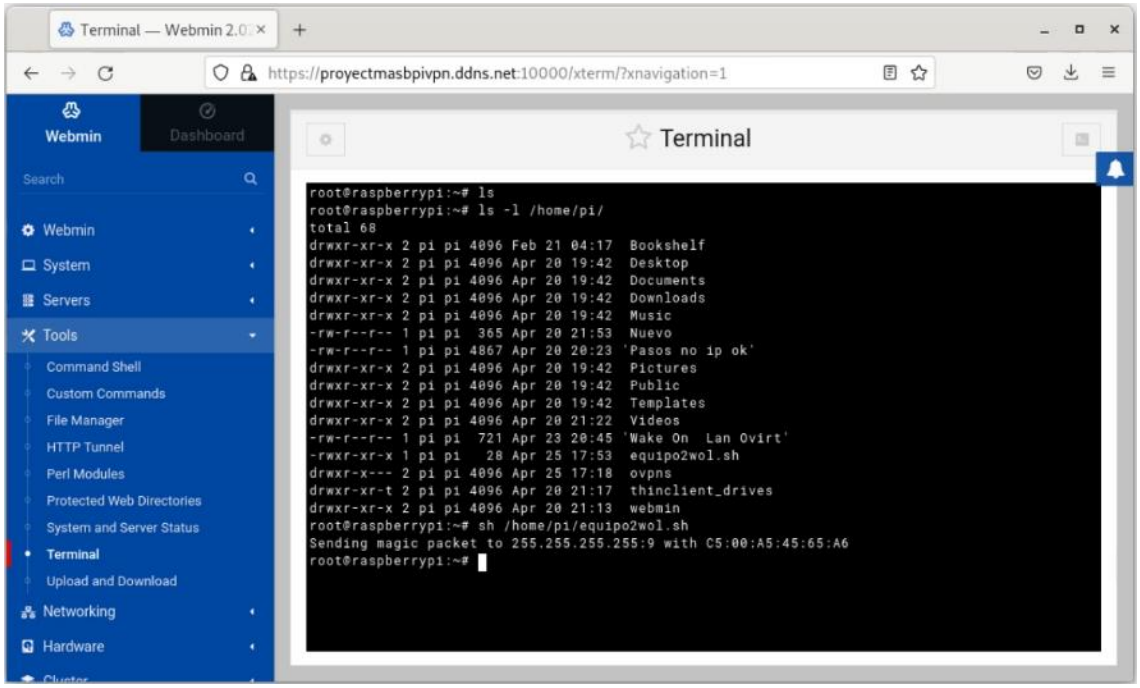
Acceso mediante WEBMIN, dentro del cliente, en un navegador de Internet se colocará como URL: https://proyectmasbpivpn.ddns.net:10000

Coincidiendo la URL con el nombre de dominio o host creado en el proveedor de servicios DDNS y el puerto por defecto de conexión WEBMIN separado por ":".

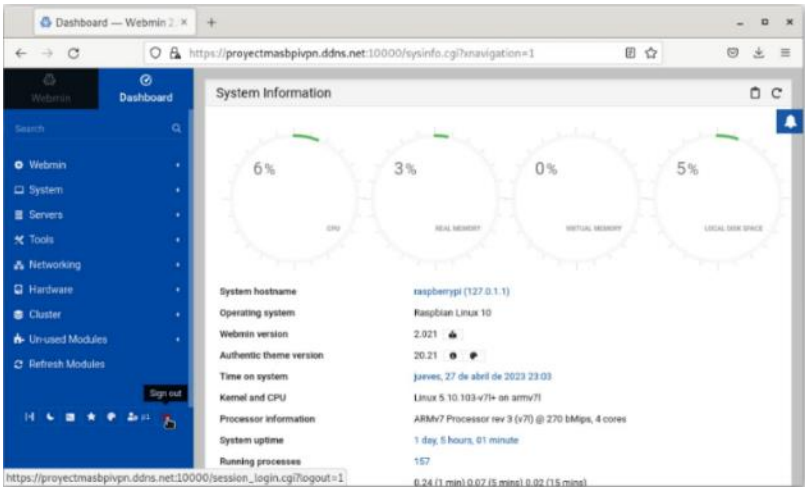
Se facilitarán las credenciales de acceso y se pulsara sobre el botón Sign in.



Para poder acceder al terminal se pulsará en el panel lateral izquierdo sobre Tools y posteriormente sobre Terminal.



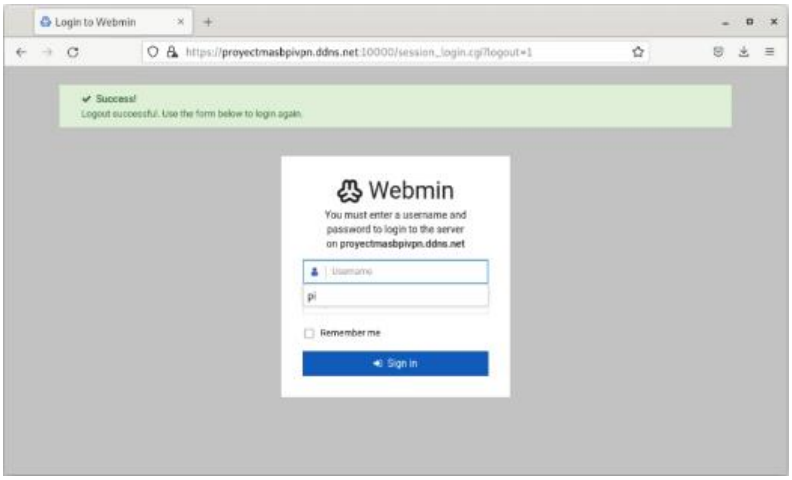
Como se mencionó, se podrá ejecutar remotamente comandos de administración comprobar el estado de servicios, ejecutar los scripts de arranque de los equipos necesarios, por ejemplo.

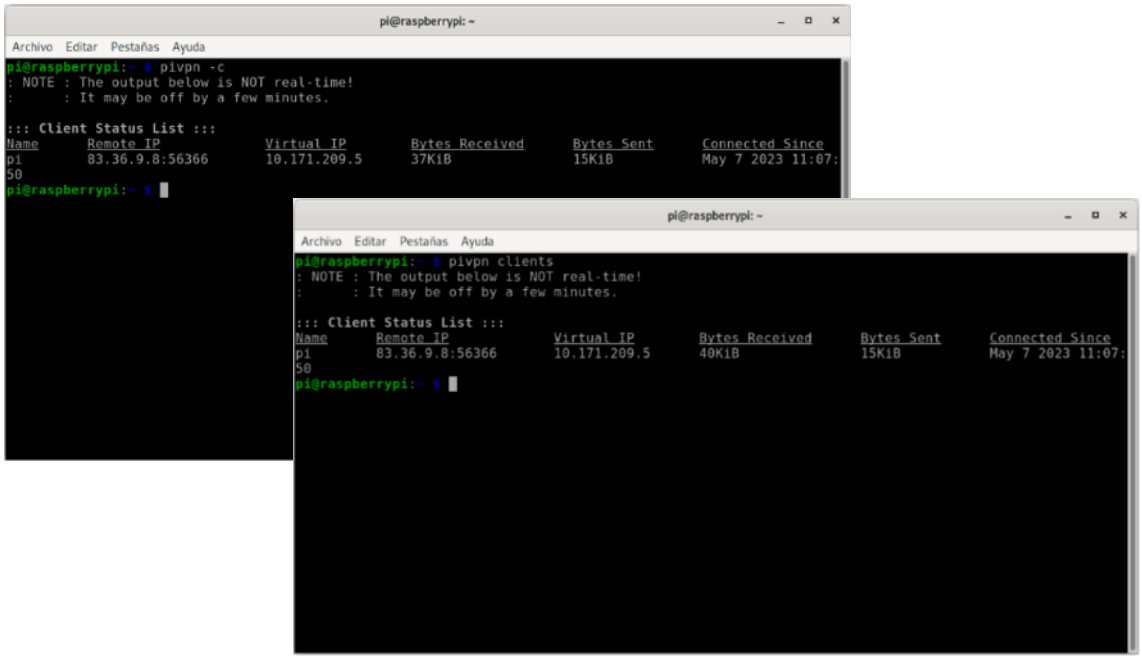


Para finalizar la sesión, habrá que ir a la página de inicio pulsando sobre el botón superior izquierdo 

, y posteriormente pulsar sobre el botón inferior rojo Sign out 

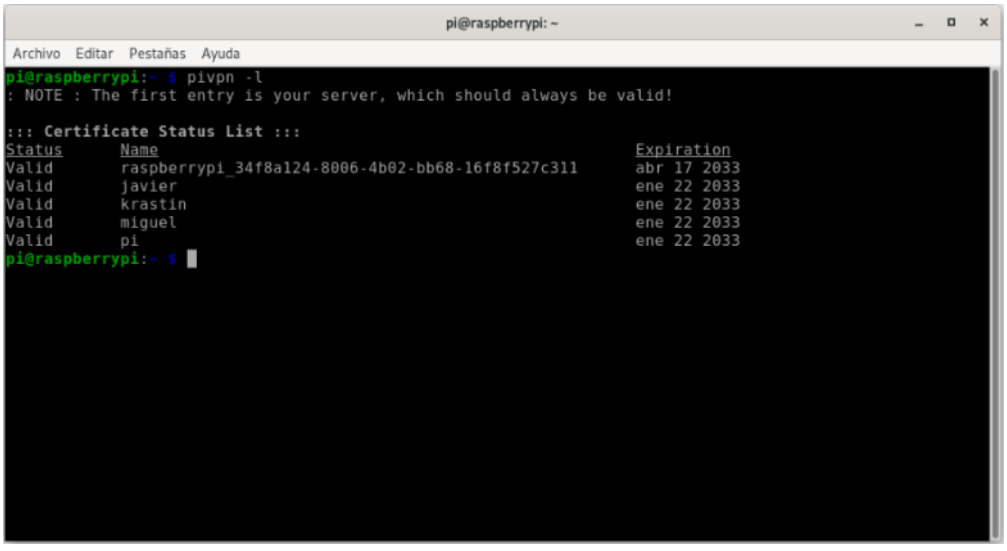
.





Desde el cliente Linux, conectado vía SSH como administrador del servidor, se podrá comprobar los clientes conectados con los comandos.

pivpn -c
pivpn clients



En caso de querer comprobar cómo se encuentran los clientes se utilizará el comando.

pivpn -l



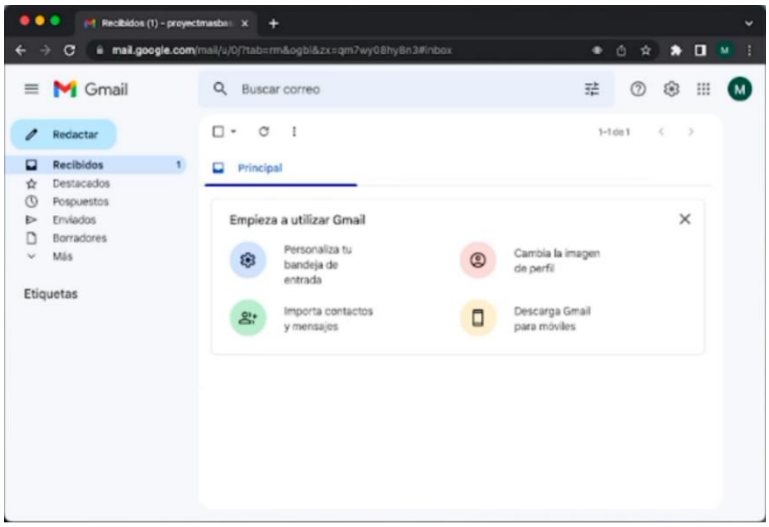
Terminadas las acciones administrativas, se podrán cerrar las aplicaciones abiertas y desconectase de la conexión VPN, pulsando sobre el icono superior derecho  , para acto seguido pulsar en Desconectar cambiando el icono, como se puede apreciar en la captura de la ventana superior derecha.

Llegado a este punto y sin más dilación como diría un compañero de trabajo, comienzo a explicar y desarrollar todo el proceso de este proyecto, muchas gracias por la atención prestada.

Creación de cuenta gratuita en proveedor de servicio DDNS.

Puede existir otra forma de crear la cuenta, esta que se presenta en este documento es una más de las múltiples formas en que se puede crear, o en uno de los muchos proveedores de servicios DDNS donde se puede crear una cuenta.

Para la configuración del servicio DDNS en este caso en No-IP, se puede realizar a través de este router facilitado por el proveedor de servicios de Internet (ISP), esta configuración se explicará más adelante como también la instalación del cliente No-IP en el S.O. de la Raspberry Pi, pudiendo seleccionar uno de los métodos para su uso.



Para poder realizar todo este proyecto, es necesario disponer de una cuenta de correo electrónico con la que habrá que registrarse de forma gratuita en uno de los proveedores de servicios DDNS que existen, y que de algún modo nos permiten crear de alguna forma un nombre de dominio/host asociándolo a la IP pública de la que se dispone, pudiendo conectarnos en vez de a la IP pública que nos facilita nuestro ISP (Proveedor de Servicios de Internet), al nombre de dominio/host que se creará.

Para este proyecto se crea una cuenta específica y dado que las instrucciones que se están detallando son paso a paso, no se dará soporte en esta cuenta puesto que se ha creado explícitamente para la creación de toda la configuración y la documentación de este proyecto.

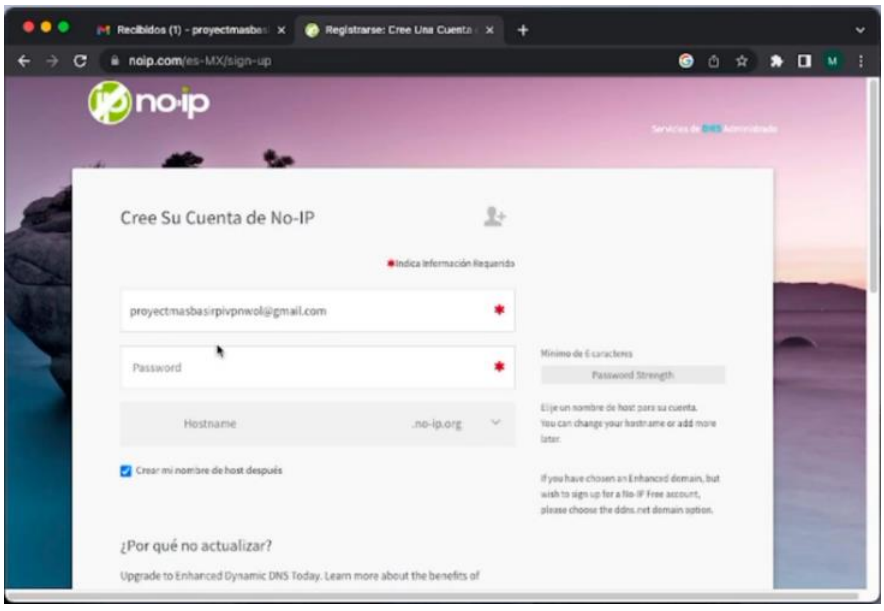
Con una cuenta de correo electrónico, en este caso se trata de una cuenta de correo electrónico gratuita de Google GMAIL, creada expresamente para este proyecto, se explicará a continuación como crear una cuenta en uno de los proveedores de servicios DDNS, en este caso se trata de No-IP.

Esta cuenta puede crearse en cualquier otro proveedor que nos permita la creación de una cuenta gratuita, aunque en este caso, y al encontrarse disponible en el router del ISP la posibilidad de configurar una cuenta de este proveedor de servicios DDNS, es por lo que se utiliza este proveedor.



Dentro de la WEB de No-IP. https://www.noip.com/es-MX

Para crear una cuenta, se pulsará sobre el botón superior derecho: Inscribirse (Sign up).

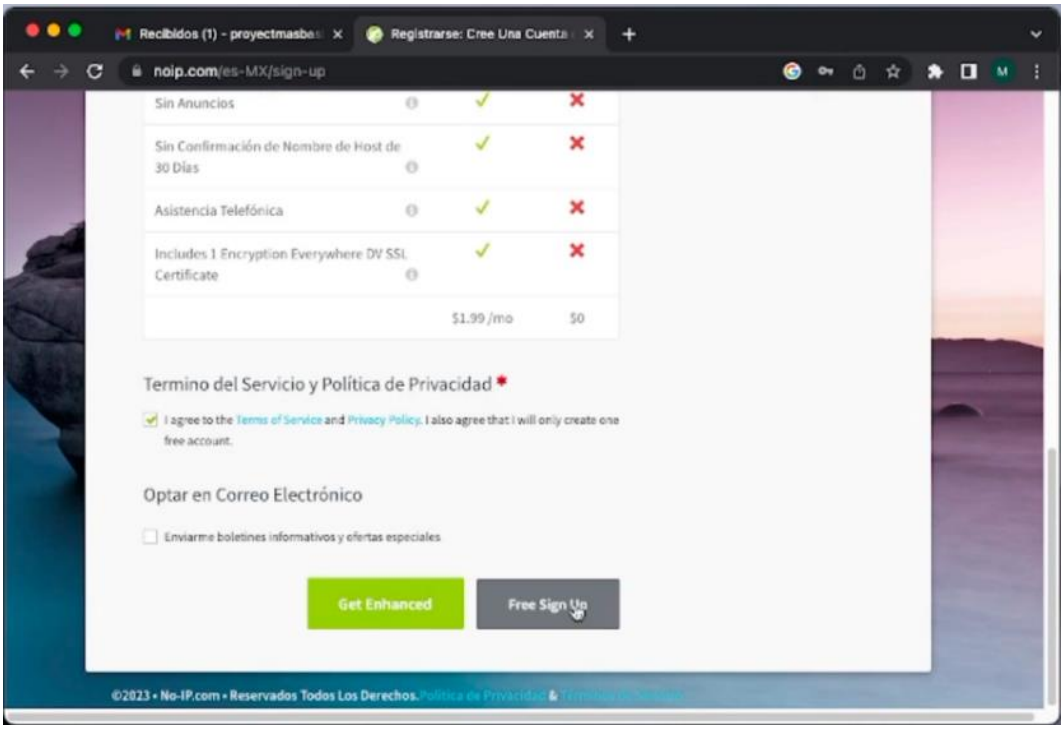


Se utiliza, como se ha mencionado anteriormente la cuenta de correo creada expresamente para la creación de toda la documentación y en la que no se dará soporte.

proyectmasbasirpivpn@gmail.com

Se deja seleccionada la opción. Crear mi nombre de host después.

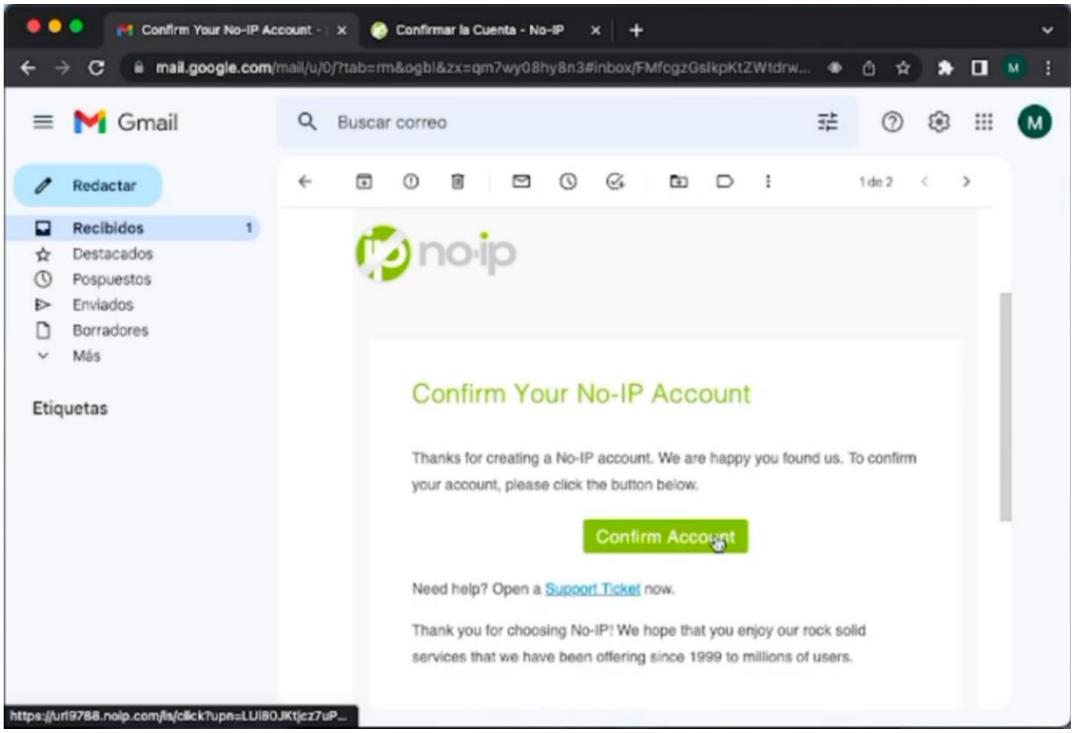
Habrá que introducir una contraseña.



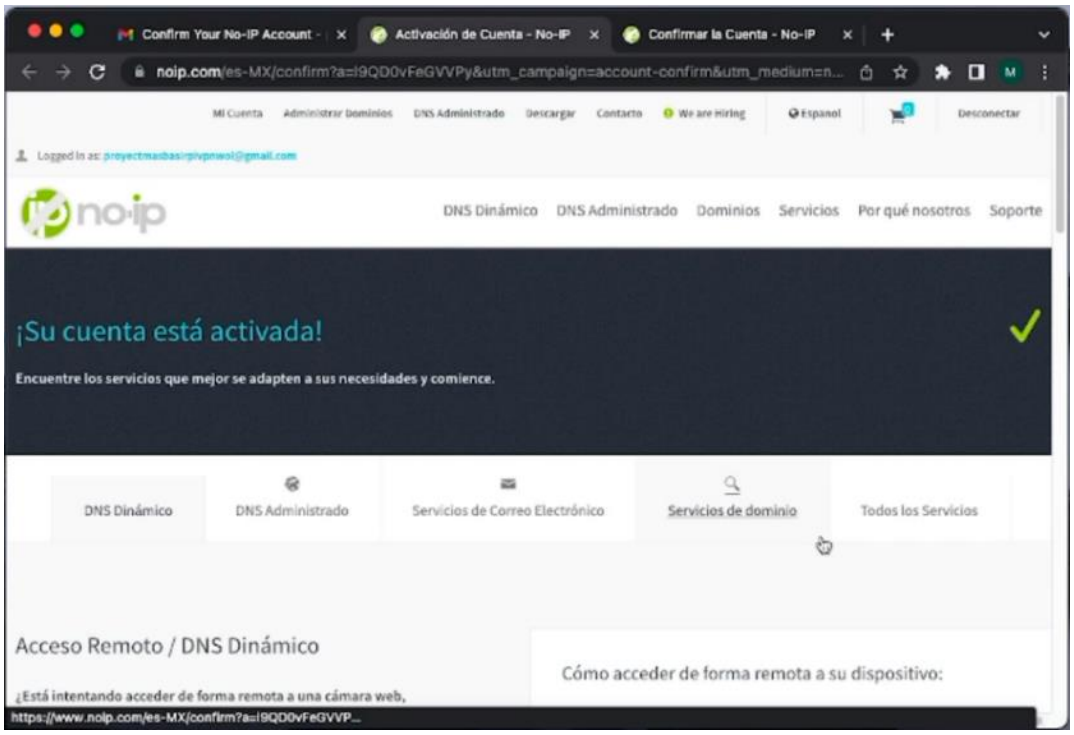
Tras introducir la contraseña, se deslizará la barra de desplazamiento lateral derecha para localizar el botón inferior. Free Sign Up, pulsando sobre él.



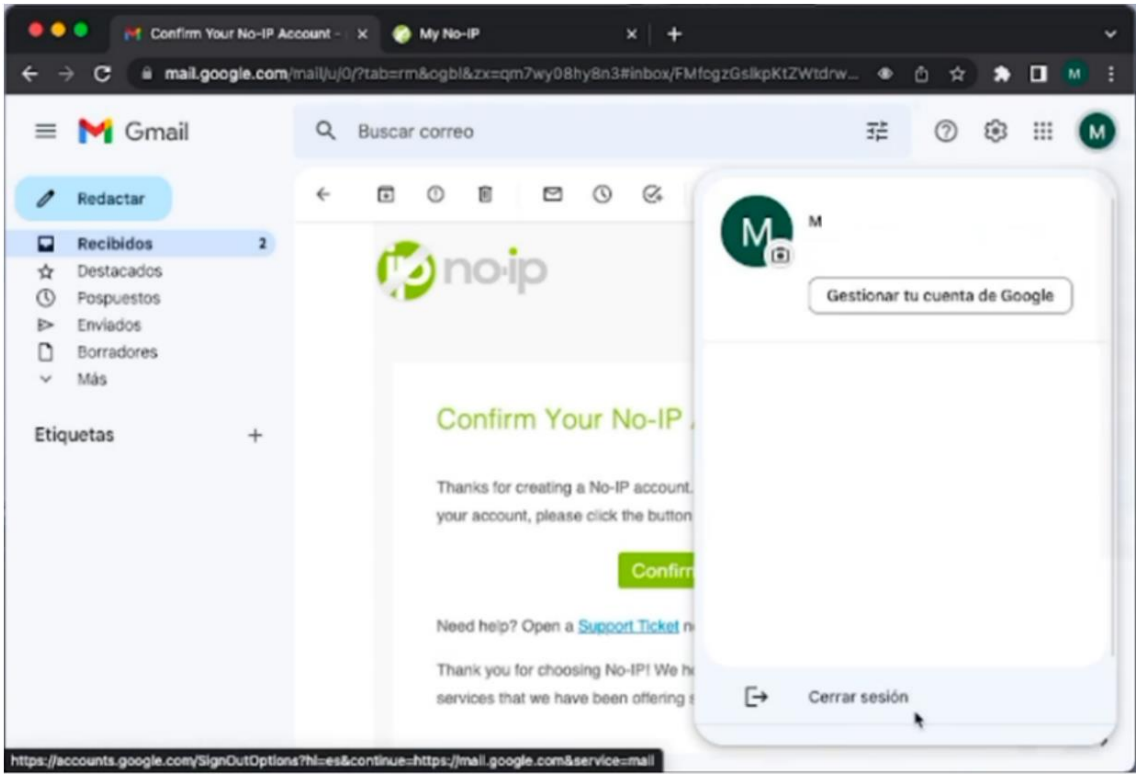
Como se puede apreciar en la ventana de la captura superior, hay que confirmar la cuenta creada en un correo que se enviará al correo utilizado para la creación de la cuenta.



Dentro de la cuenta de correo utilizada para darse de alta en el proveedor de servicios DDNS, habrá llegado un correo del proveedor, en el que, al abrirlo, se tendrá que localizar y pulsar sobre el botón. Confirm Account.

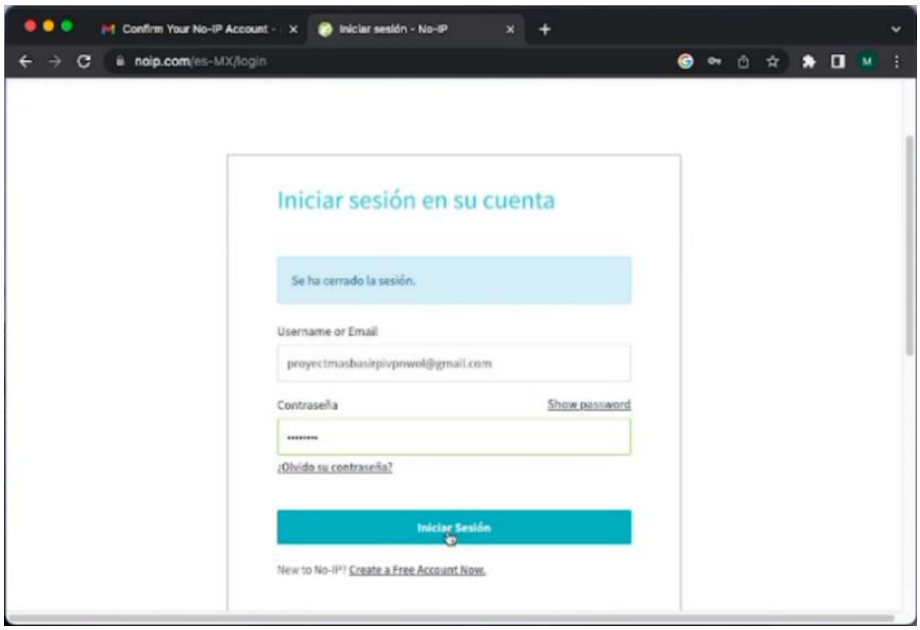


Al haber pulsado sobre el botón. Confirm Account, aparecerá una ventana informando que la cuenta se activó correctamente.



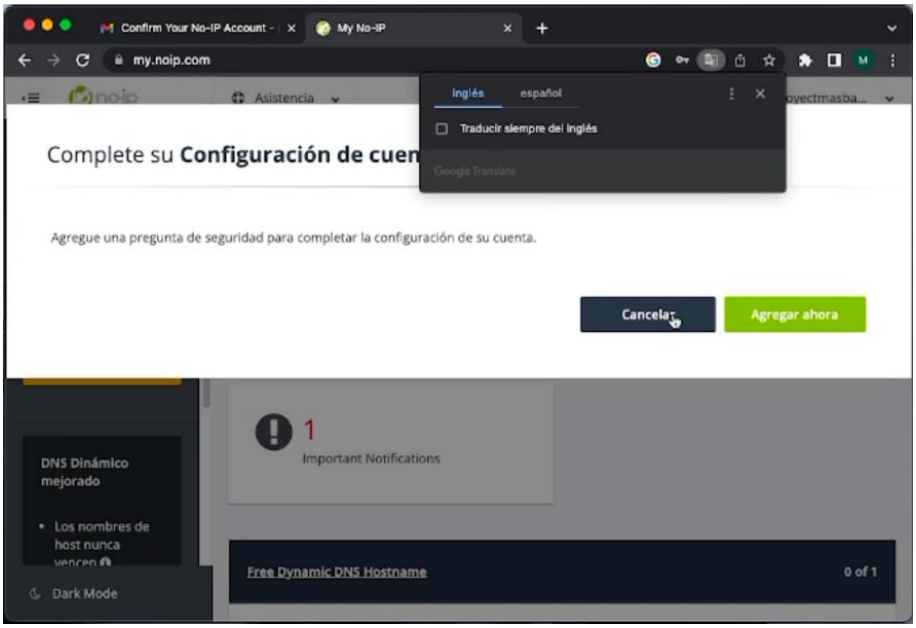
Al activar la cuenta, se podrá proceder a cerrar la sesión dentro de la cuenta de correo, cerrando la sesión.

Creación nombre de dominio en proveedor de servicios DDNS.

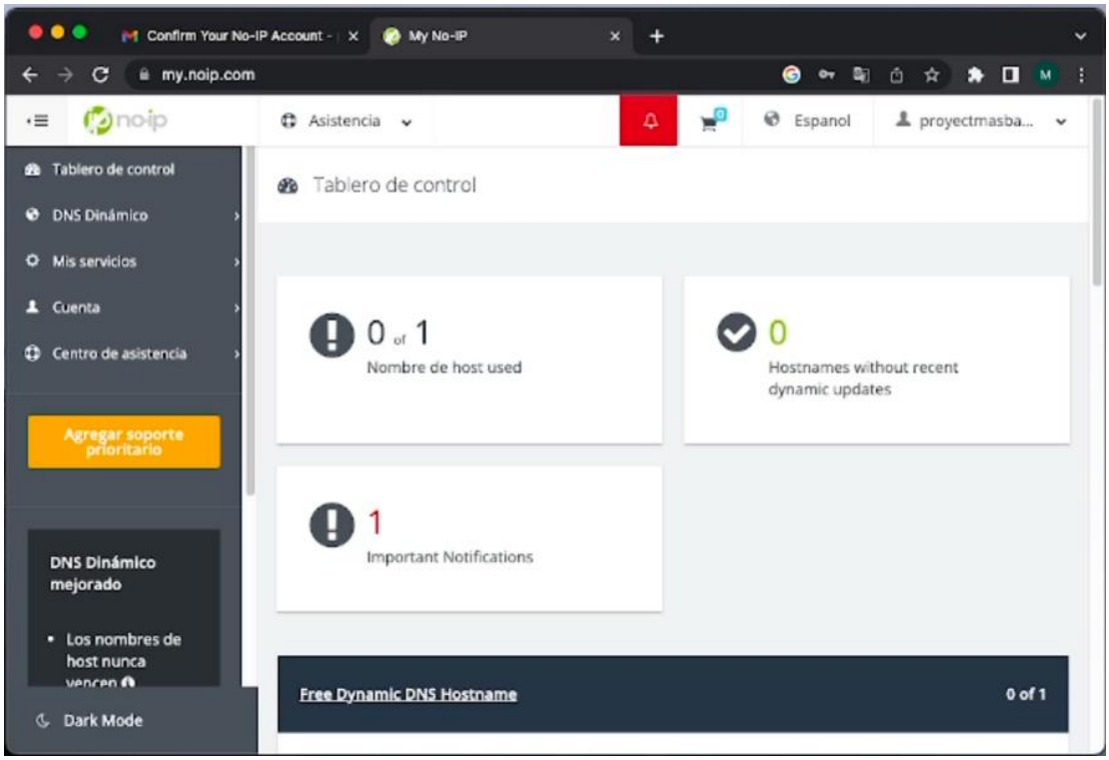


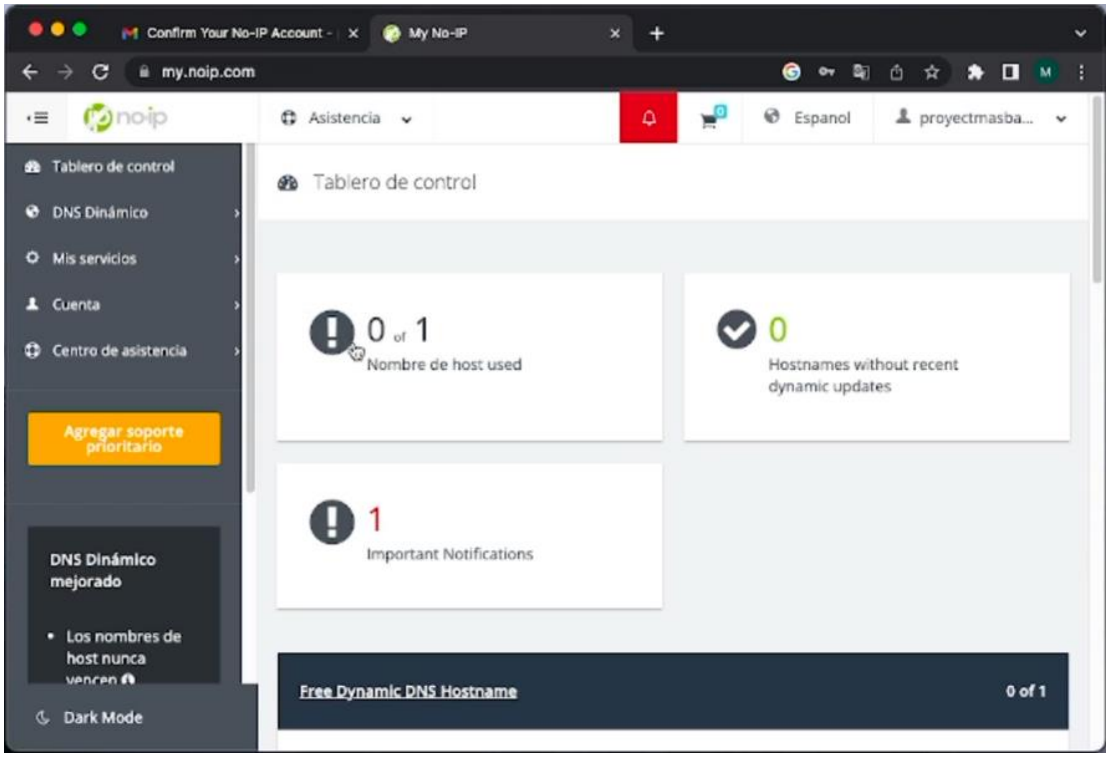
Tras haber creado una cuenta en el proveedor de servicios DDNS, para crear un nombre de dominio o host, se accederá a la cuenta creada en el proveedor de servicios DDNS, en este caso es No-IP en la WEB. https://www.noip.com/es-MX

En la que se localizará y se pulsará sobre el botón superior derecho Iniciar sesión, facilitando el correo utilizado para darse de alta y la contraseña.



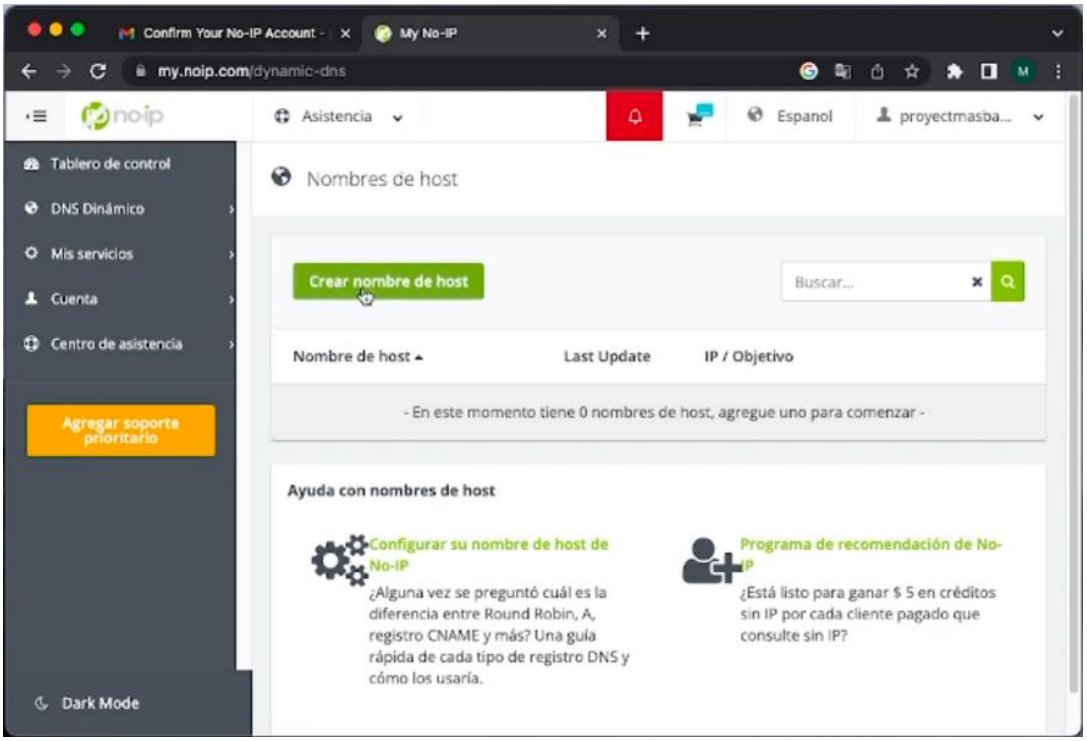
En caso de aparecer el mensaje como el que se muestra en la ventana de la captura superior, se pulsará en. Cancelar.



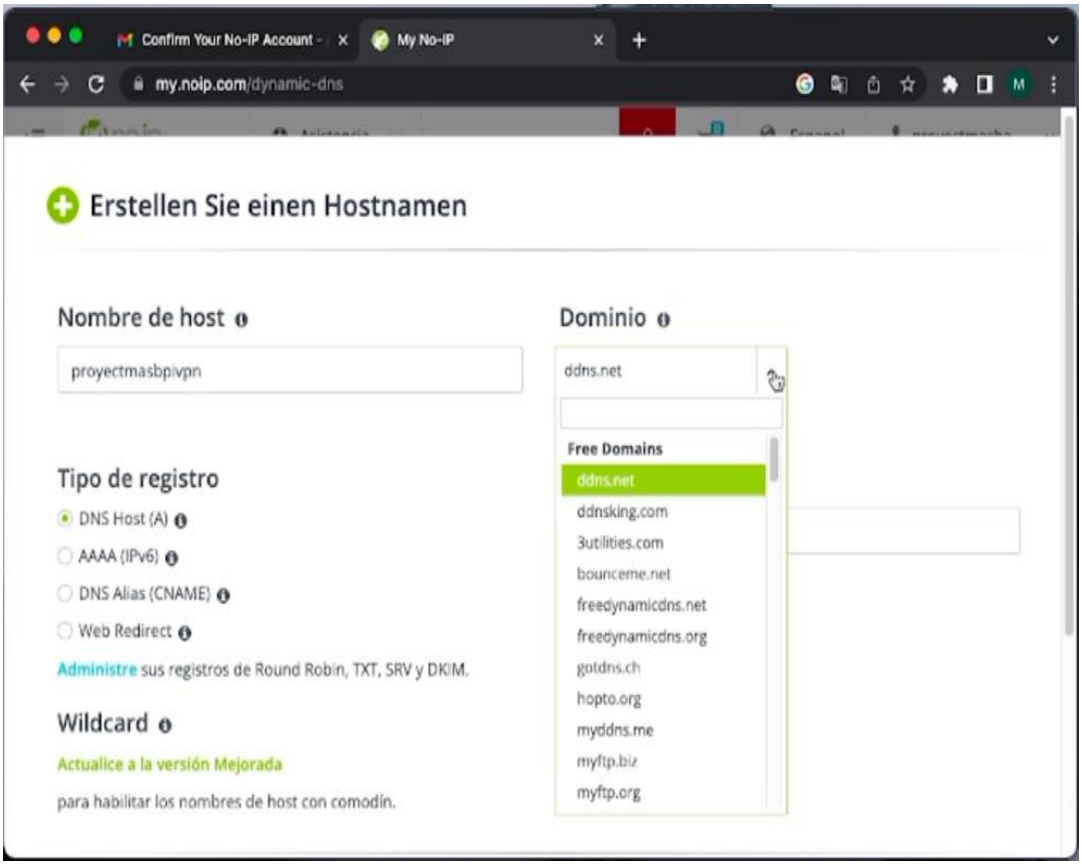


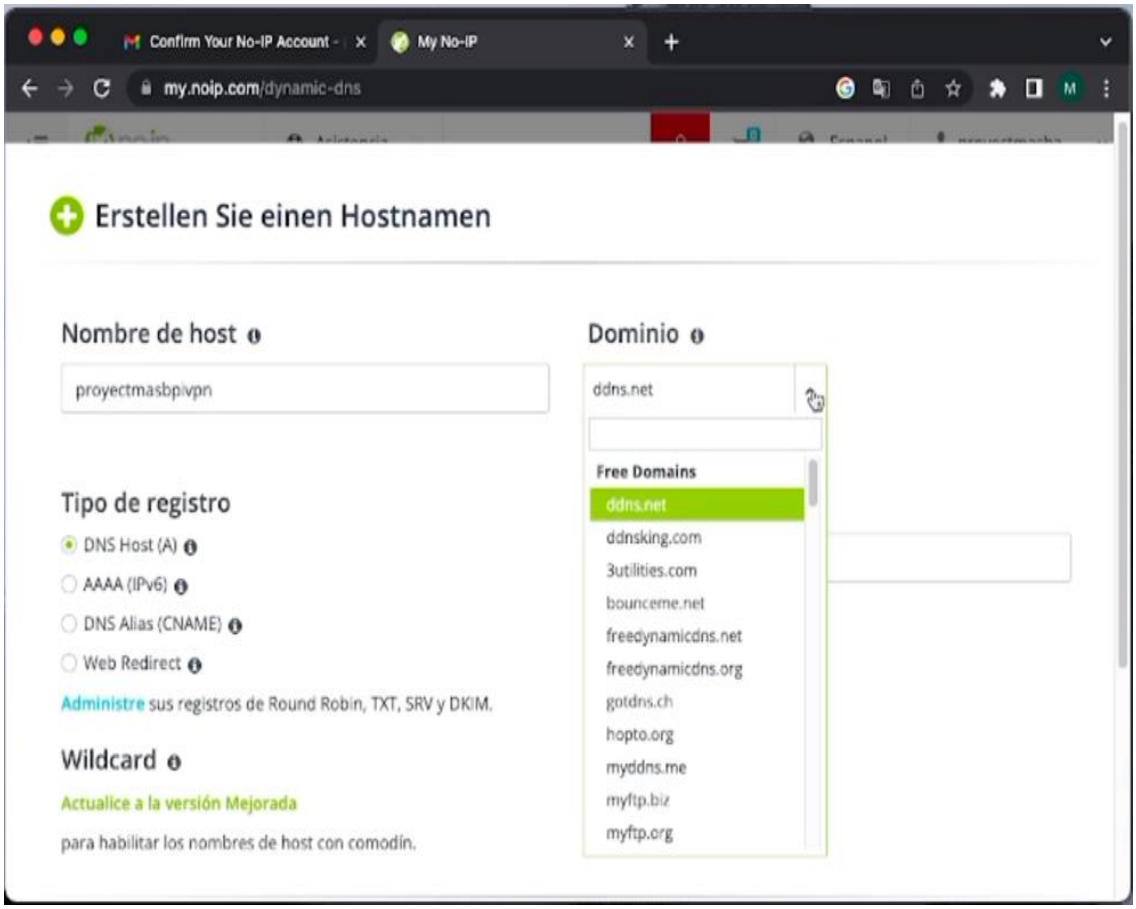
Como se puede observar en la ventana de la captura superior, se pulsará sobre el cuadro superior izquierdo del panel derecho 

, para crear el host.



En esta nueva ventana, se pulsará sobre el botón superior. Crear nombre de host.





En la ventana que se muestra a continuación, habrá que rellenar los apartados:

Apartado superior izquierdo:

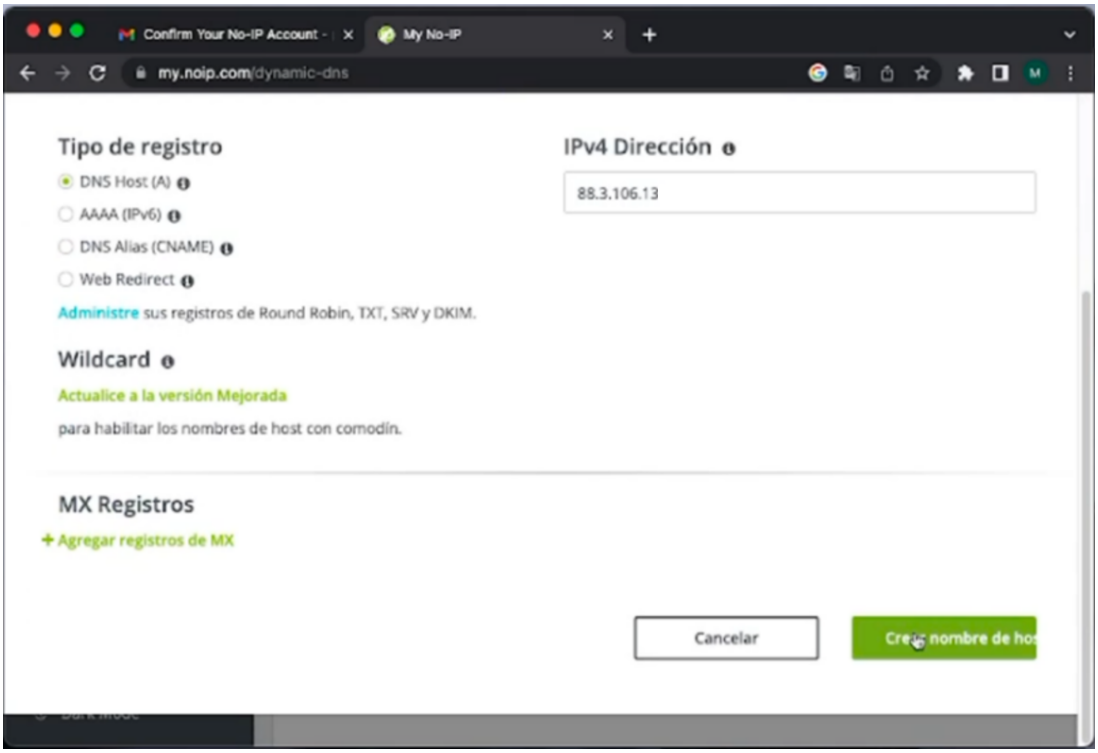
- Nombre de host, se escribirá un nombre descriptivo para utilizar posteriormente, en este caso se utiliza proyectmasbpivpn.

Apartado superior derecho:

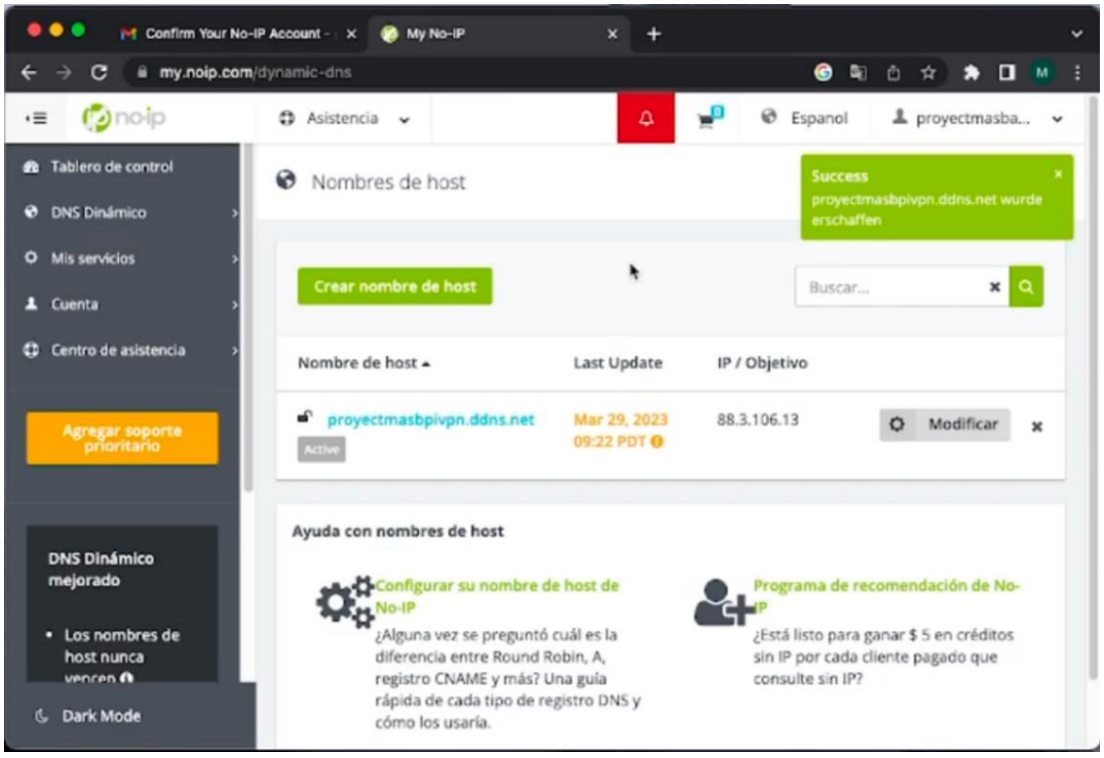
- Dominio: Se podrá desplegar y seleccionar uno de los que se dispone.
- IPv4 Dirección: Esta es la dirección IPv4 que nos facilita nuestro ISP Proveedor de Servicios de Internet, en caso de no disponer de una dirección IP fija y utilizar IP dinámica, que es lo más habitual, cada vez que se apaga, reinicia el router la dirección pública de este cambia y se modifica facilitándose una nueva por el ISP.

Como se observa, los valores elegidos para este proyecto son:
Nombre de host: proyectmasbpivpn, quedando: proyectmasbpivpn.ddns.net

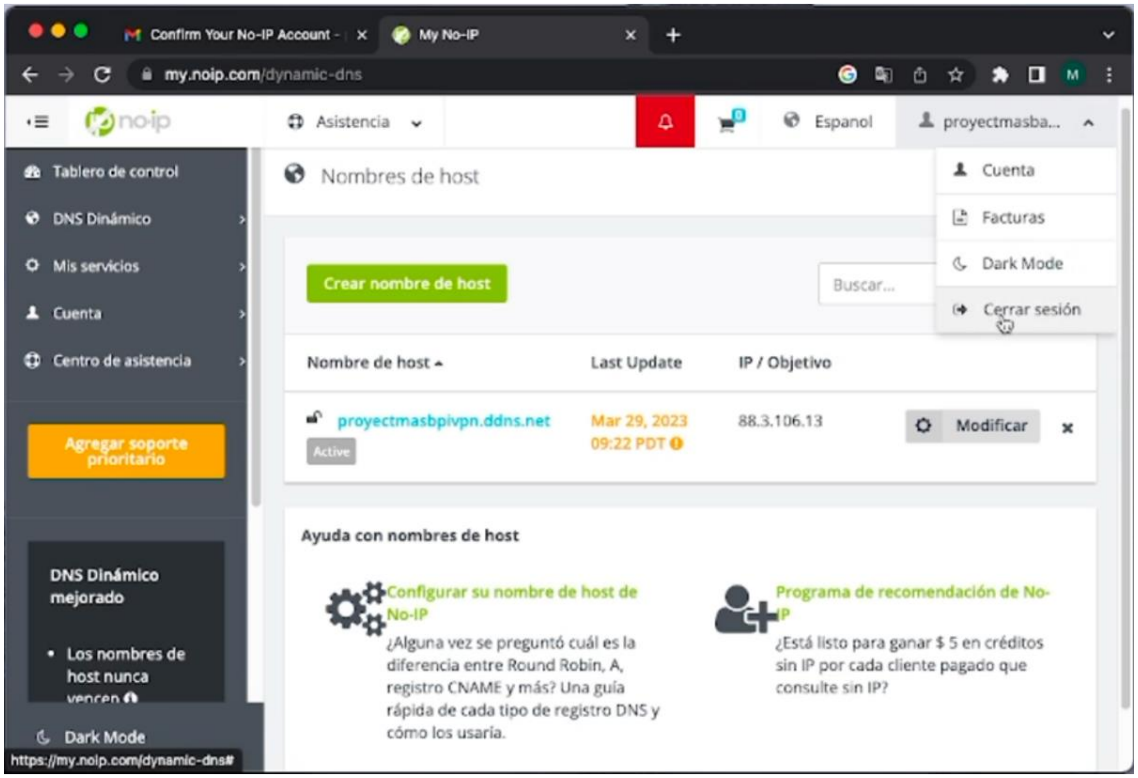
- Domino: ddns.net
- IPv4 Dirección: XXX.XXX.XXX.XXX (esta cambiará con el paso del tiempo).



Rellenados los campos como se necesiten, se deslizará la barra lateral derecha para localizar y pulsar sobre el botón. Crear nombre de host.



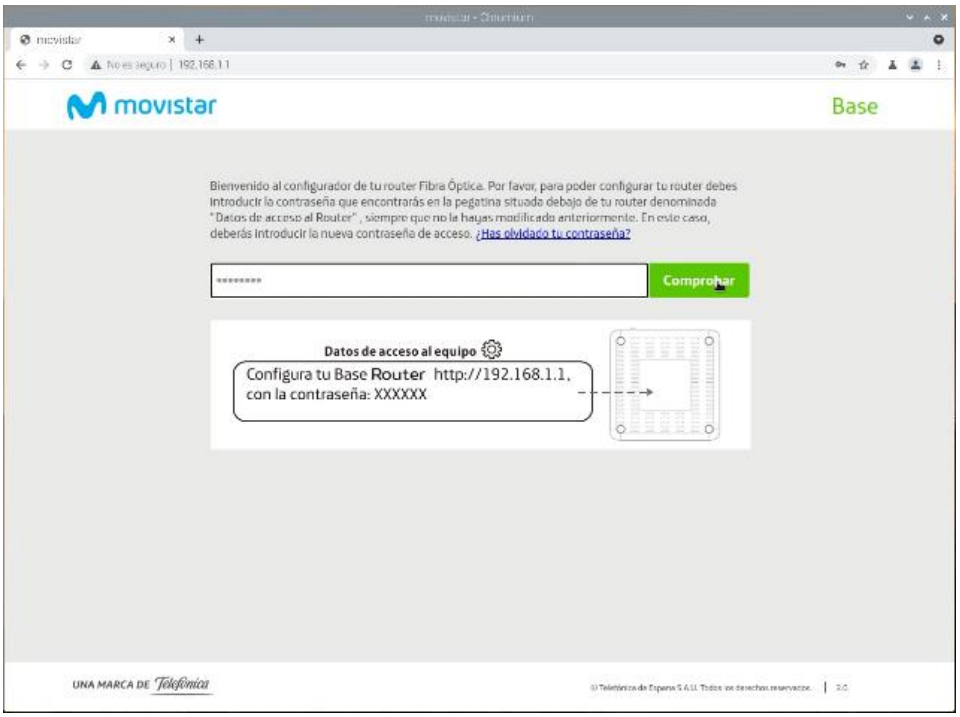
Al pulsar el botón. Crear nombre de host, se puede comprobar que se crea el nombre de dominio o host, con el nombre que se ha facilitado anteriormente.



Creado el nombre de dominio, ya se podrá salir de la sesión creada en el proveedor de servicios DDNS.

Lo único a destacar, es que en la actualidad No-IP ya solo ofrece la ceración de un nombre de dominio o host, en este caso al ser creado como se ha explicado de forma gratuita, se tendrá que actualizar/renovar cada “X” tiempo, siendo este, 30 días, pasados los días indicados, se tendrá que realizar la renovación/actualización del nombre de dominio o host creado, en caso de tener una cuenta antigua, este proveedor facilitaba la creación de tres host.

Configuración proveedor de servicio DDNS No-IP en Router.

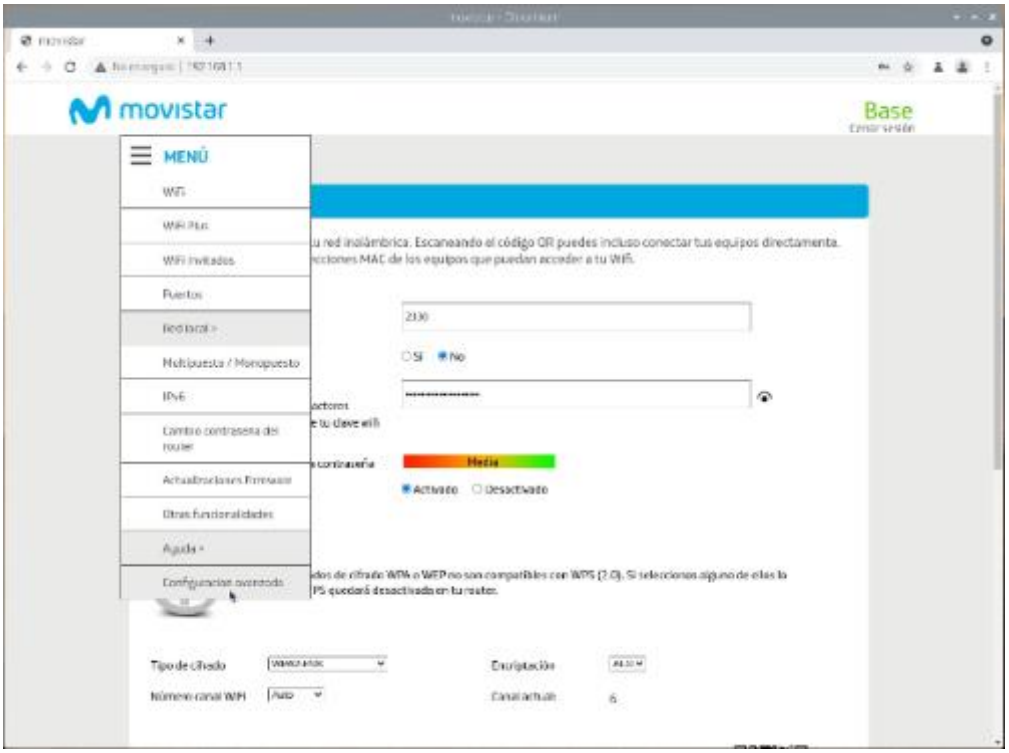


Se muestra cómo realizar la configuración del servicio DDNS del proveedor No-IP, dado que este se puede configurar en este router como algún otro proveedor de DDNS, no es necesario realizar esta configuración si se instala en el servidor VPN en este caso se trata de la Raspberry Pi el software del proveedor de servicio DDNS, o en un equipo cliente de la red, en este router facilitado por el proveedor de servicios de Internet se puede configurar este proveedor de DDNS como otros.

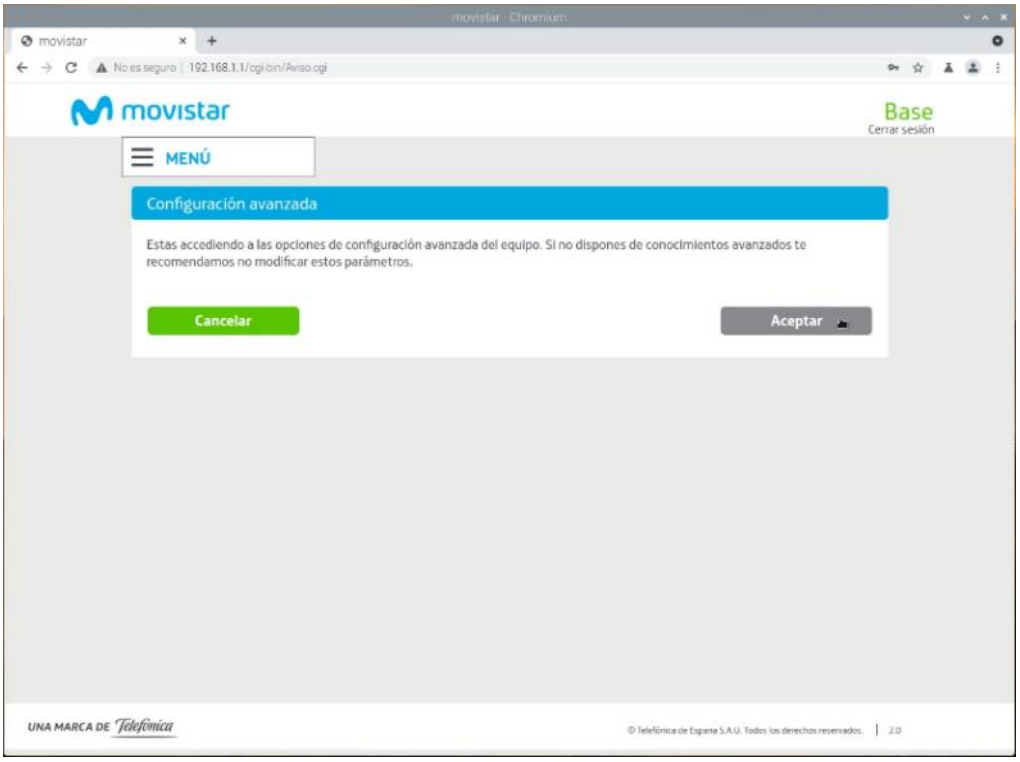
En este caso, habrá que acceder al router por la dirección IP, suele ser la dirección IP que coincide con la puerta de enlace o Gateway, en la configuración IP de los clientes, al poner por ejemplo, en un equipo Windows dentro de un Símbolo del sistema el comando ipconfig /all, se buscará el apartado que indica puerta de enlace o Gateway, siendo la IP en este caso la dirección IP 192.168.1.1

Como se observa en la ventana de la captura superior, se facilitará la contraseña y se pulsará sobre Comprobar.

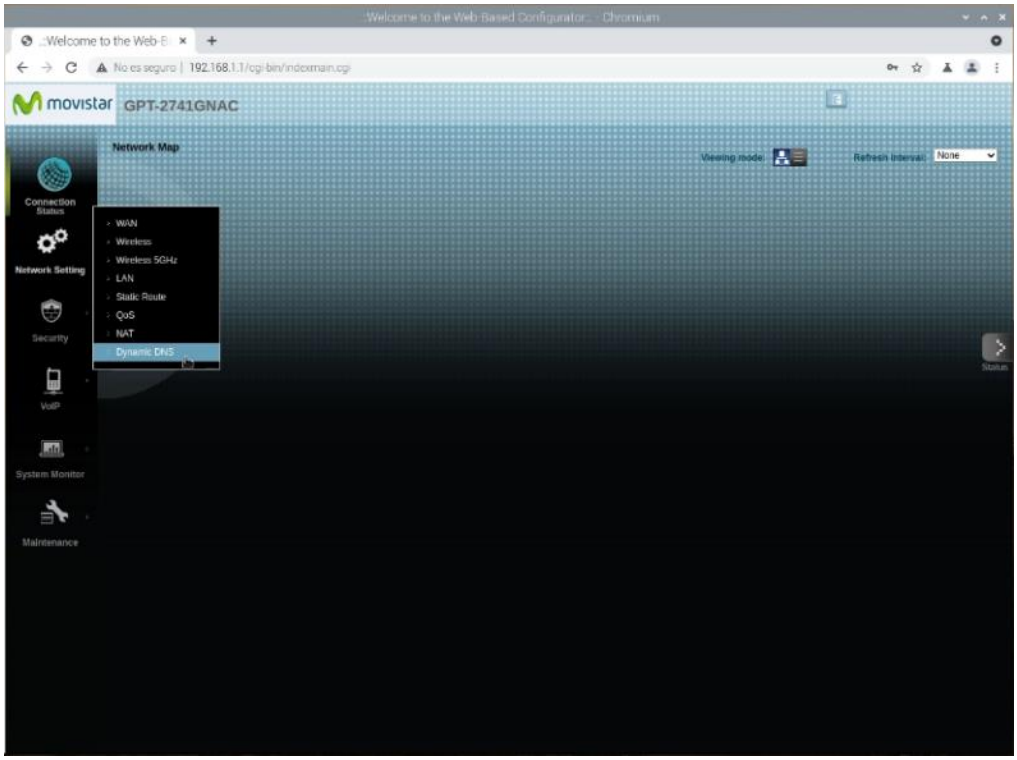
El nombre de dominio o host que se crea en este caso en el proveedor de servicios No-IP, al ser en este proyecto una cuenta gratuita, cada 30 días habrá que actualizarlo/renovarlo, se recibirá un correo en la cuenta utilizada para realizar la actualización/renovación, se explica los pasos a seguir para llevar a buen término este proceso.



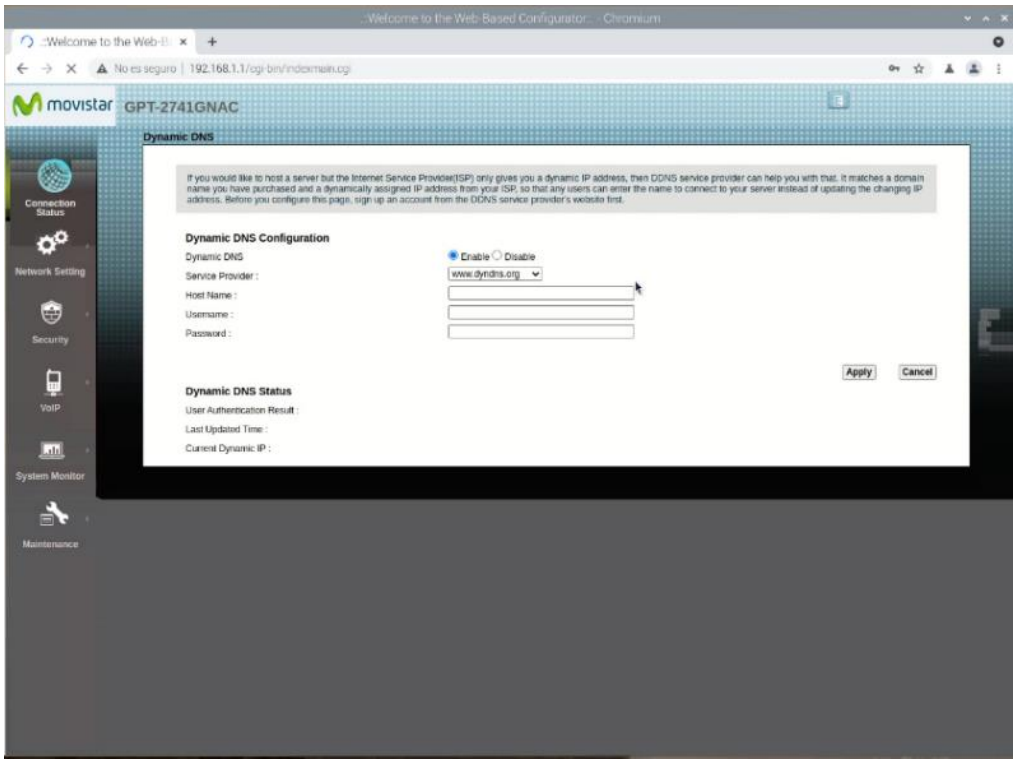
Dentro de la configuración del router, se pulsará sobre Menú \ Configuración avanzada.



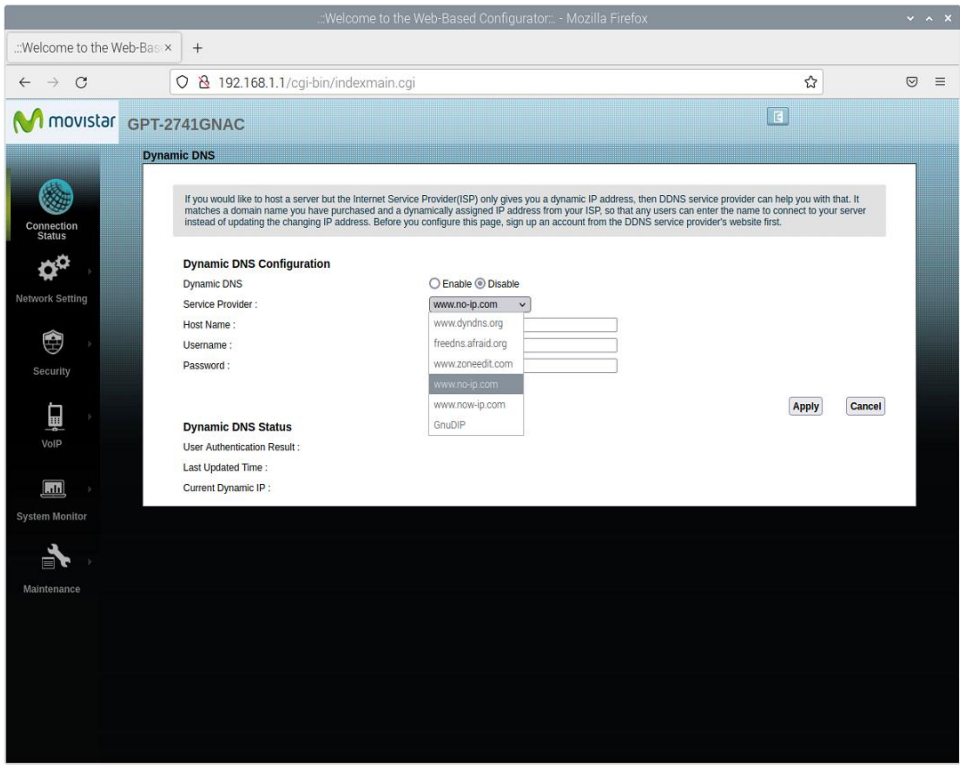
Habrá que pulsar en: Aceptar para poder acceder a la configuración avanzada.



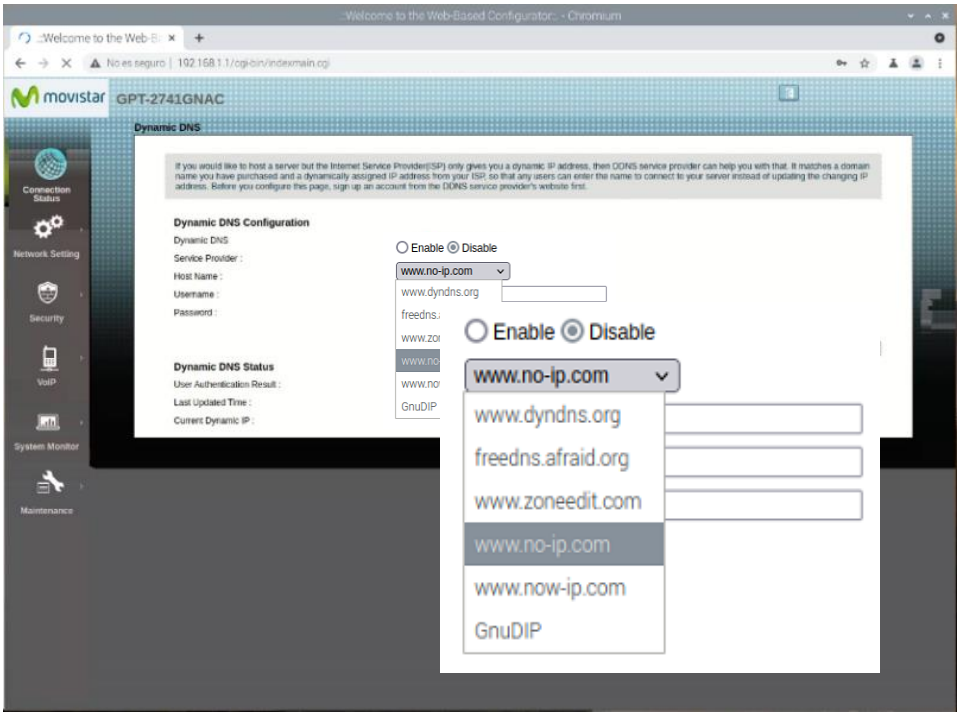
En el menú vertical izquierdo, habrá que pulsar con el botón izquierdo del ratón sobre: Network Setting \ Dynamic DNS.



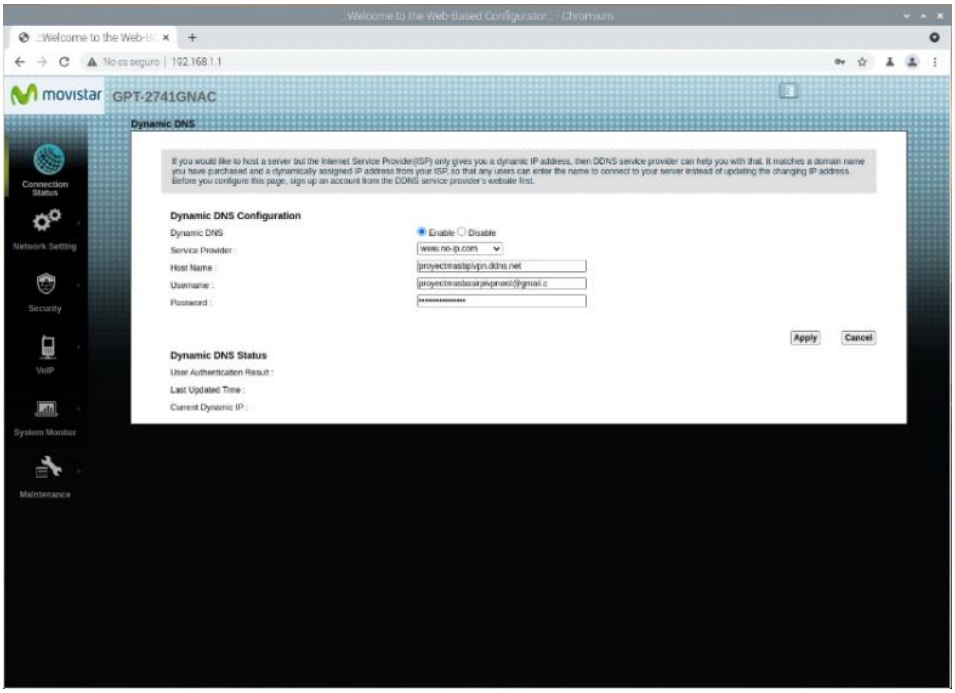
En la ventana: Dynamic DNS Configuration, habrá que seleccionar Enable.



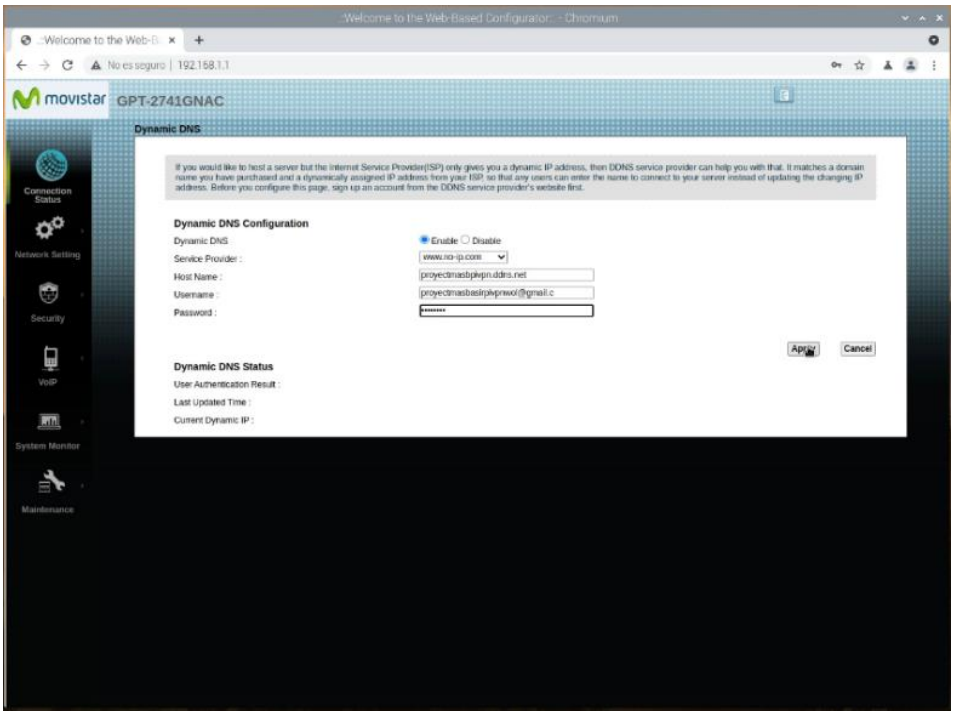
Tras seleccionar Enable, se permitirá seleccionar que proveedor de servicio DDNS se configurará, para este proyecto y según se ha indicado anteriormente, se utiliza www.no-ip.com, por lo que se seleccionará este proveedor.



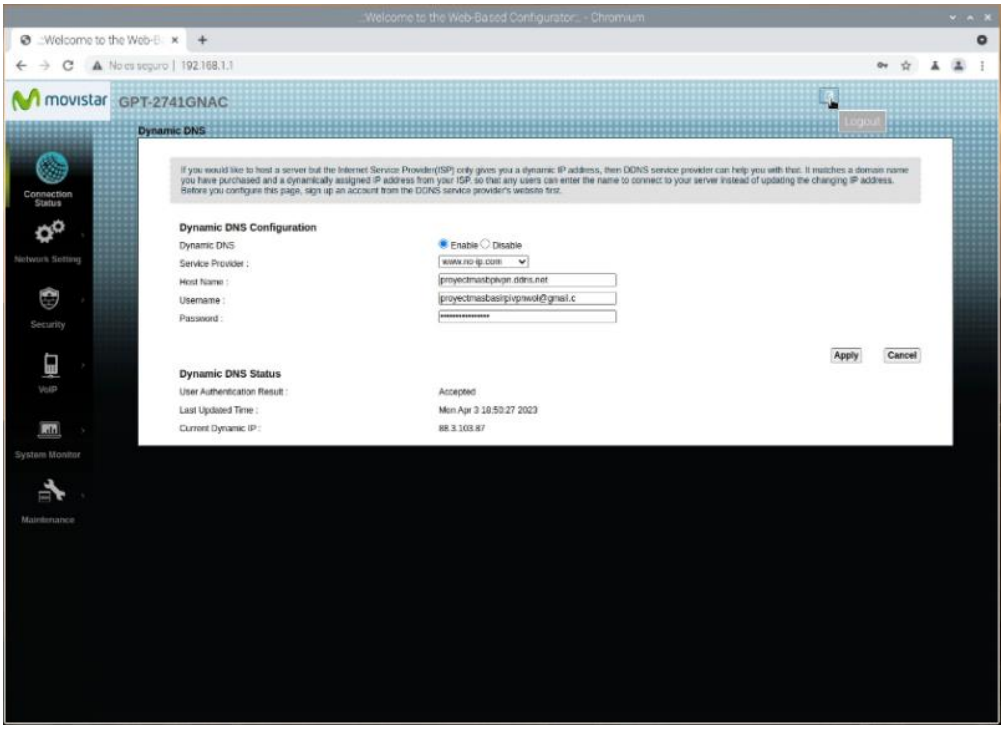
Se muestra la lista de los que se puede utilizar en este router.



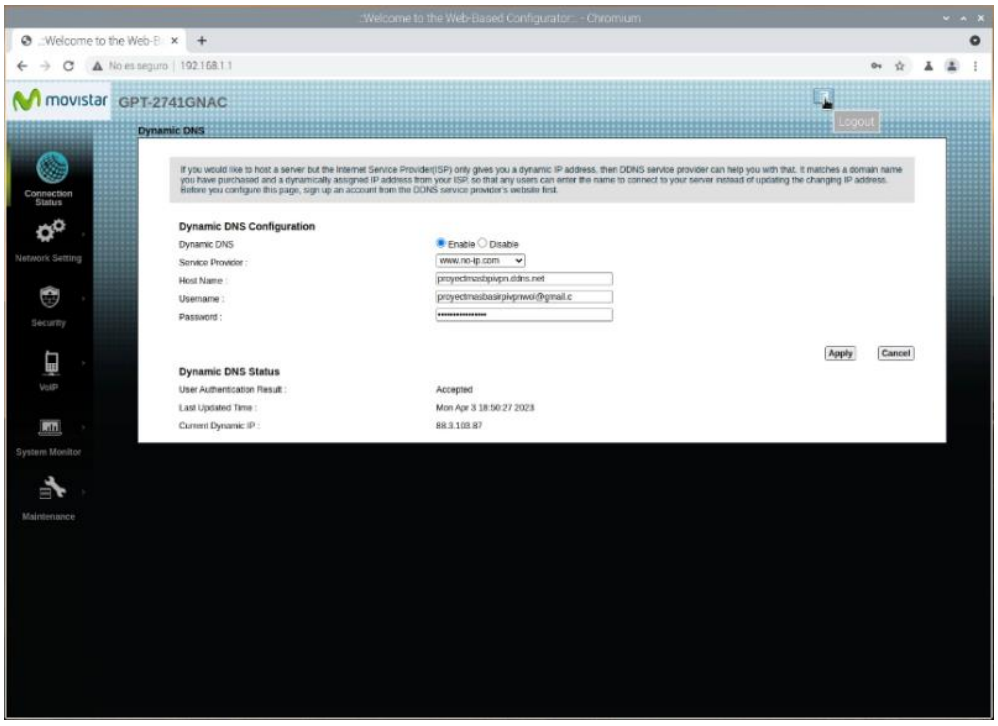
En los apartados, habrá que introducir los datos que correspondan.
Service Provider: www.no-ip.com
Host Name: proyectmasbpivpn.ddns.net
Username: proyectmasbasirpivpnwol@gmail.com
Password: ********



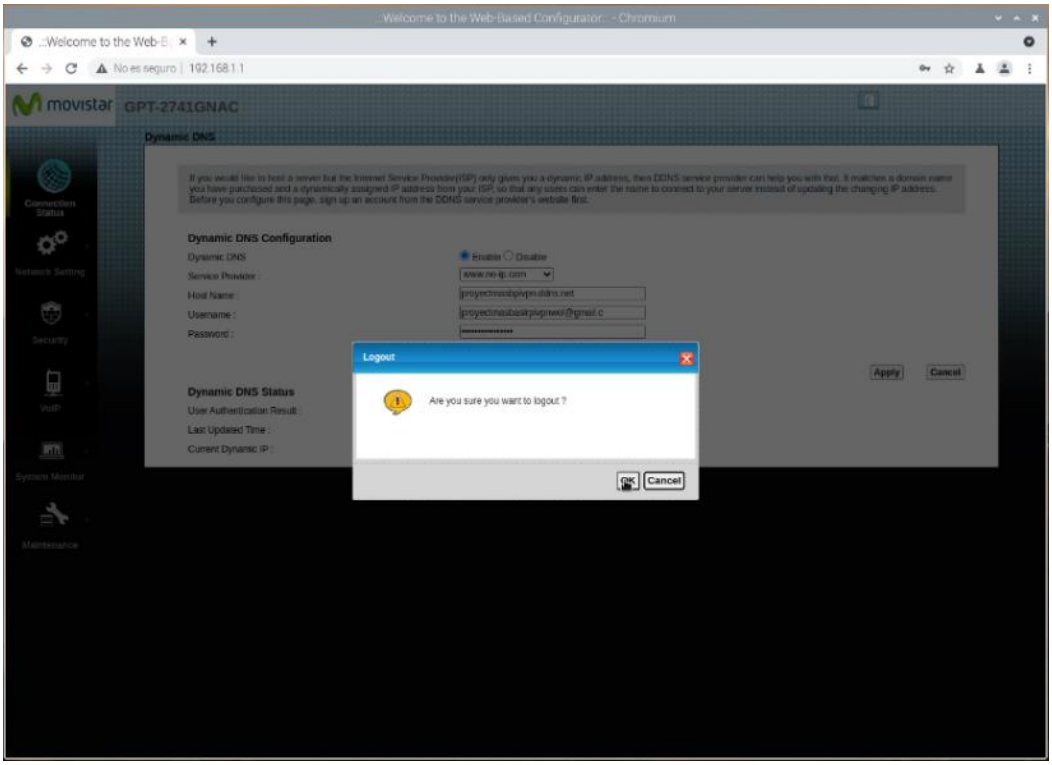
Rellenados los campos necesarios se pulsará sobre: Apply.



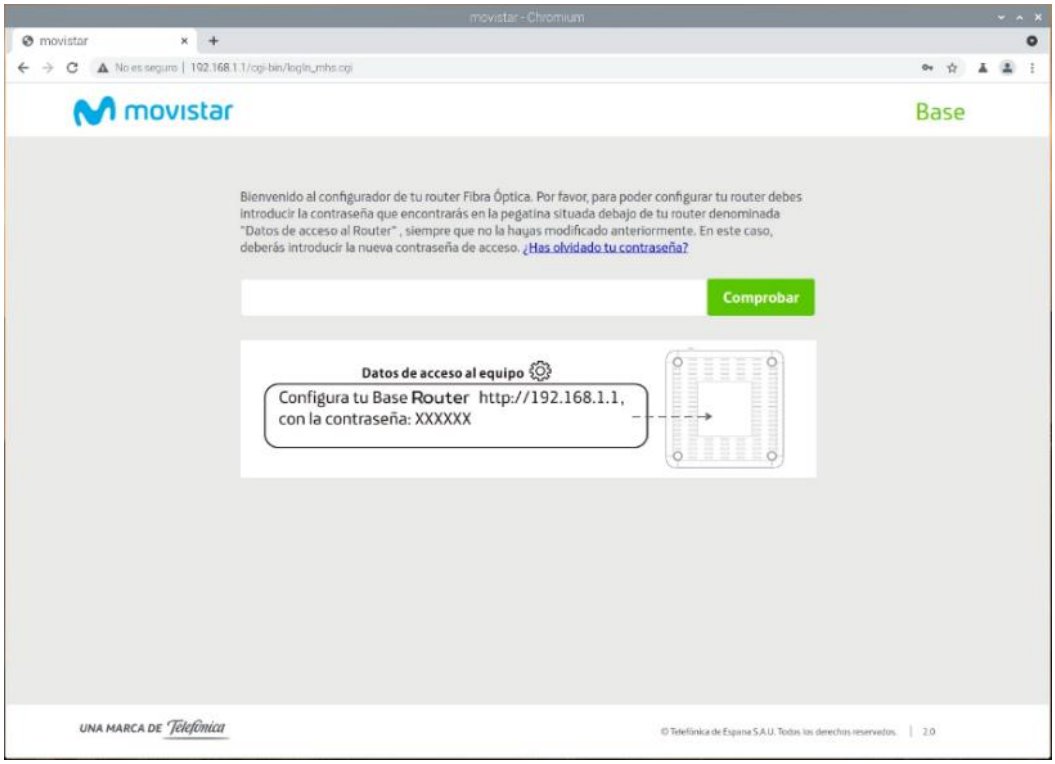
Como se puede apreciar, si se han rellenado correctamente los datos y tras pulsar sobre: Apply, se informa que el resultado de la autentificación del usuario fue aceptado, concretamente se indica: Acepted.



Para finalizar, se pulsará sobre el icono superior derecho para cerrar la sesión como se observa en la ventana de la captura superior.

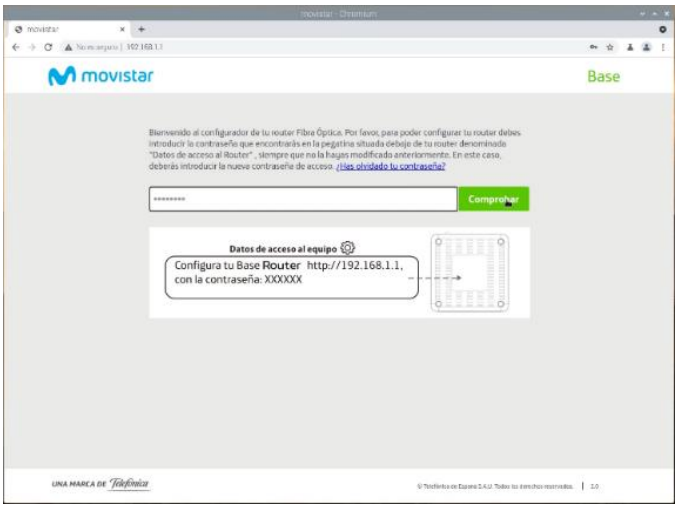


En el cuadro de dialogo que aparece se pulsara sobre: OK.



Finalizando la sesión del router y pudiendo cerrar la ventana del navegador.

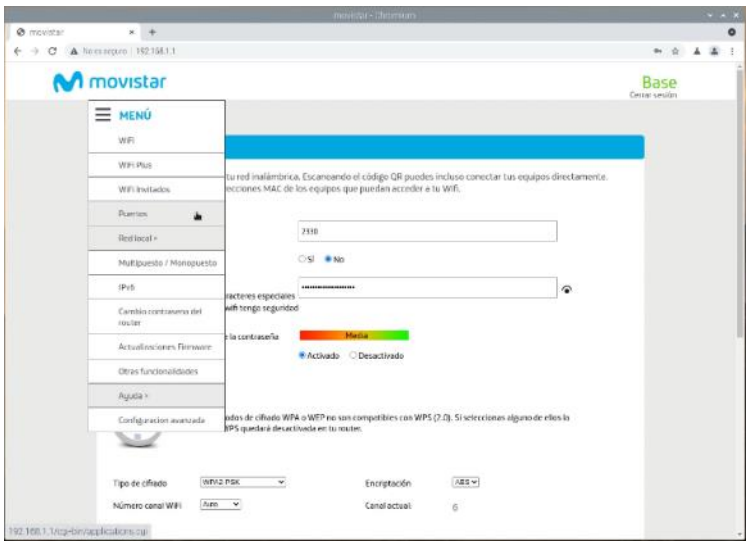
Apertura de puertos en Router.



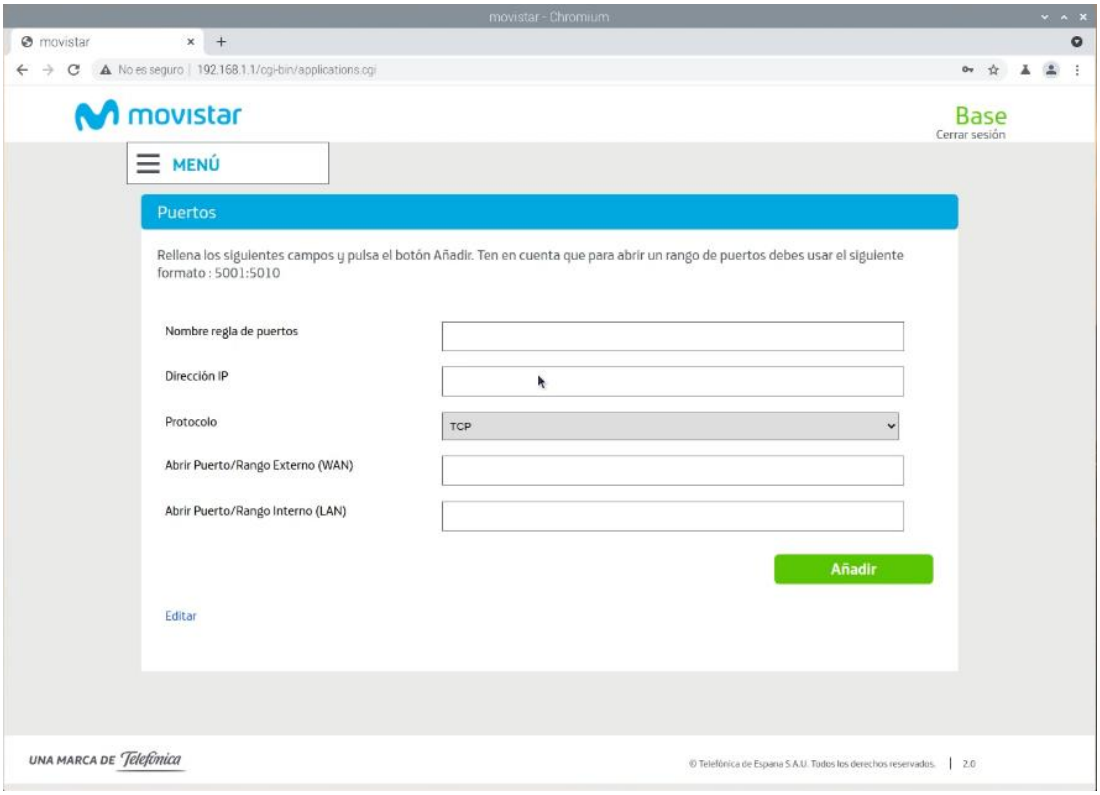
Se muestran las indicaciones de apertura de puertos, en el router que el proveedor de servicios de Internet facilita, este router no permite realizar Wake On LAN (WOL), por lo que es necesario realizar los pasos que se indican para poder disponer de un servidor VPN/WOL.

Para poder realizar la operación de abrir los puertos necesarios del router, habrá que acceder al router por la dirección IP, en este caso se trata de la dirección IP 192.168.1.1, esta dirección IP suele coincidir con la dirección de la puerta de enlace o Gateway en la configuración IP de un cliente, por ejemplo, al ejecutar dentro de un equipo cliente Windows en un Símbolo del sistema el comando ipconfig /all, se buscará el apartado que indica puerta de enlace o Gateway, siendo la IP en este caso la dirección IP 192.168.1.1.

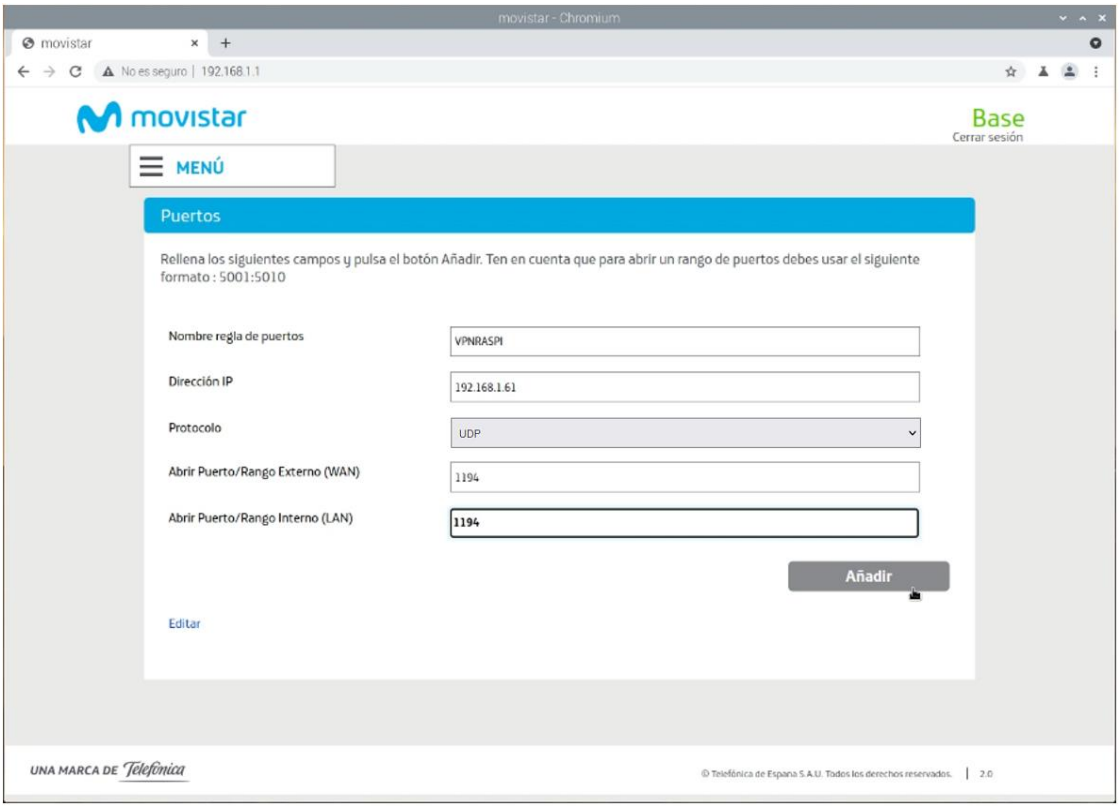
Como se observa en la ventana de la captura superior, se facilitará la contraseña y se pulsará sobre: Comprobar.



Dentro de la configuración del router, se pulsará sobre el botón: Menú \ Puertos.



Estos puertos, son un ejemplo de los que para este proyecto se han abierto, alguno de ellos como por ejemplo para PiVPN, dependiendo de si se selecciona el uso de OpenVPN o WireGuard y el protocolo elegido TCP/UDP, en este proyecto se selecciona un Servidor VPN OpenVPN y el protocolo UDP por lo que el puerto en este caso es el 1194, el cual se puede modificar a la hora de la instalación y su configuración, este puerto habrá que abrirlo en el router y en el caso de que se utilice un cortafuegos como por ejemplo ufw en Linux, habrá que habilitar el tráfico también en el cortafuegos.

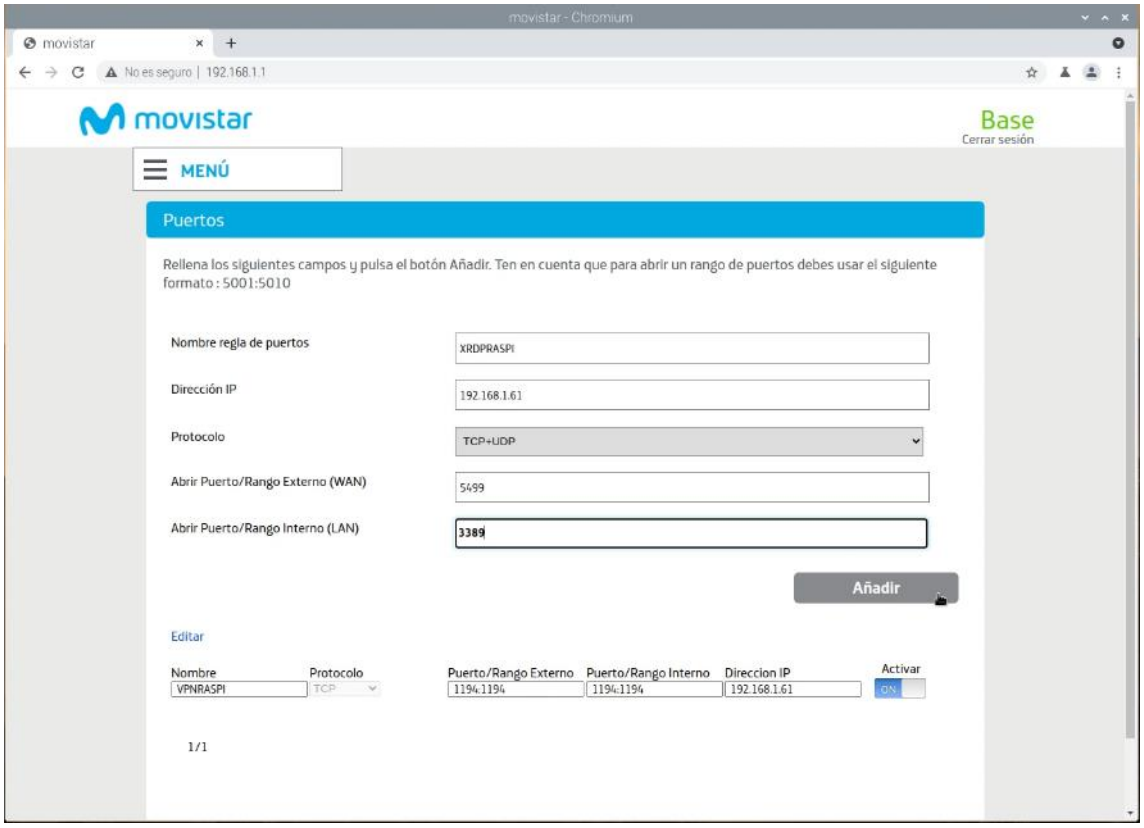


Creación de reglas:

- servicio VPN.
    - Nombre regla de puertos, nombre que se le quiera dar, en este caso VPNRASPI.
    - Dirección IP, dirección IP del dispositivo, en este caso, se trata de una conexión a la Raspberry Pi, por lo que se coloca la IP (dentro de la LAN, dentro de la oficina o residencia), adquirida por la Raspberry Pi, se explicará cómo saberla. (192.168.1.61).
    - Protocolo, en este caso se selecciona UDP, dependiendo del protocolo seria TCP, UDP o incluso ambos.
    - Abrir Puerto/Rango Externo (WAN), nº de puerto a abrir, parte externa de la oficina o residencia, en este ejemplo es el 1194.
    - Abrir Puerto/Rango Interno (LAN), nº de puerto a abrir, parte interna de la oficina o residencia, en este ejemplo es el 1194.

Será necesario habilitar el tráfico en el cortafuegos en el servidor Raspberry Pi (ufw), a través del puerto 1194 y demás puertos necesarios.

Se pulsará sobre Añadir.

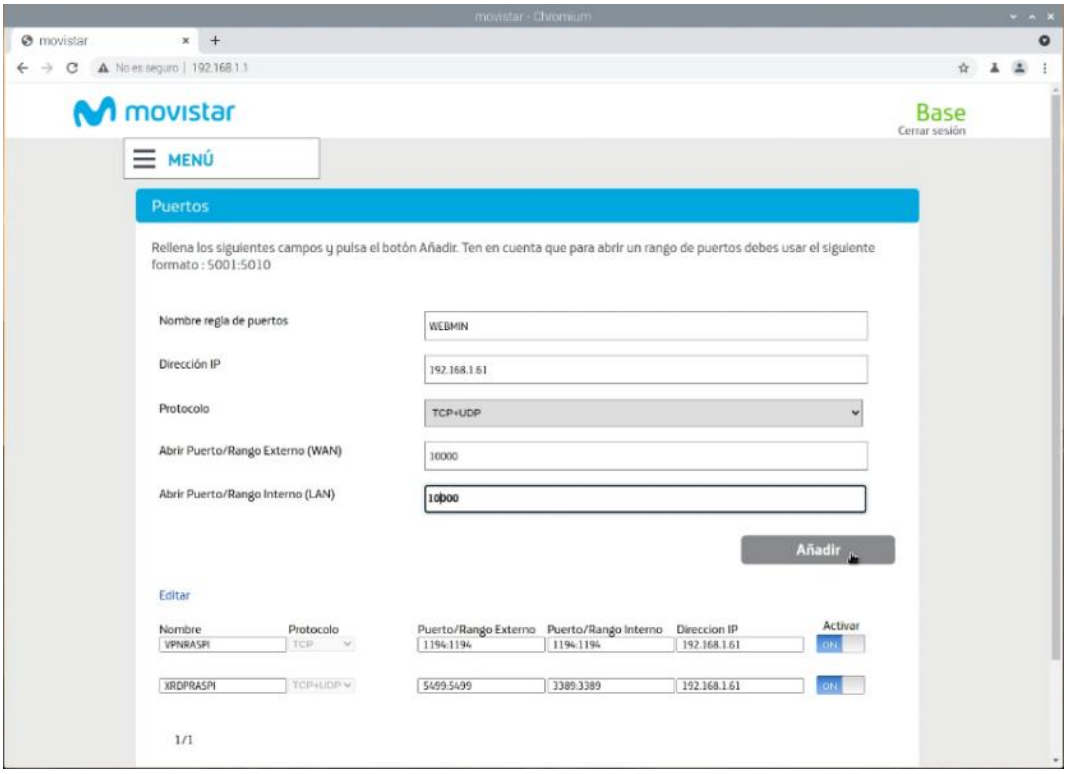


- Protocolo RDP (XRDP), (Para conexión equipo servidor Raspberry Pi).

    - Nombre regla de puertos, nombre que se le quiera dar, en este caso XRDPRASPI.
    - Dirección IP, dirección IP del dispositivo, en este caso, se trata de una conexión a la Raspberry Pi, por lo que se coloca la IP (dentro de la LAN, dentro de la oficina o residencia), adquirida por la Raspberry Pi, se explicará cómo saberla. (192.168.1.61).
    - Protocolo, en este caso se selecciona TCP+UDP, dependiendo del protocolo seria TCP, UDP, o ambos en este ejemplo.
    - Abrir Puerto/Rango Externo (WAN), nº de puerto a abrir, parte externa de la oficina o residencia, en este ejemplo es el 5499.
    - Abrir Puerto/Rango Interno (LAN), nº de puerto a abrir, parte interna de la oficina o residencia, en este ejemplo es el 3389, para conexiones RDP habitualmente es este puerto.

Será necesario habilitar el tráfico en el cortafuegos en el servidor Raspberry Pi (ufw), a través del puerto 3389 y demás puertos necesarios.

Se pulsará sobre Añadir.

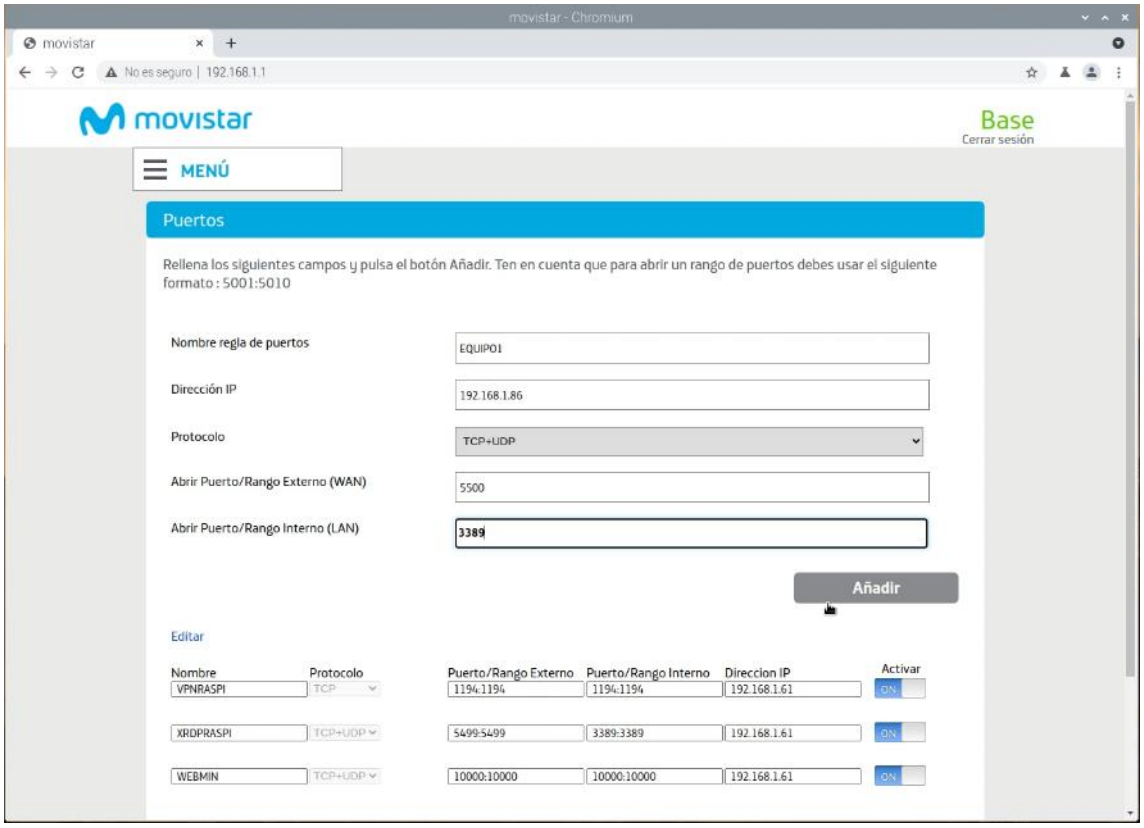


- WEBMIN (Panel de administración vía WEB de servidores Unix).

    - Nombre regla de puertos, nombre que se le quiera dar, en este caso WEBMIN.
    - Dirección IP, dirección IP del dispositivo, en este caso, se trata de una conexión a la Raspberry Pi, por lo que se coloca la IP (dentro de la LAN, dentro de la oficina o residencia), adquirida por la Raspberry Pi, se explicará cómo saberla. (192.168.1.61).
    - Protocolo, en este caso se selecciona TCP+UDP, dependiendo del protocolo seria TCP, UDP, o ambos en este ejemplo.
    - Abrir Puerto/Rango Externo (WAN), nº de puerto a abrir, parte externa de la oficina o residencia, en este ejemplo es el 10000, habitual para WEBMIN.
    - Abrir Puerto/Rango Interno (LAN), nº de puerto a abrir, parte interna de la oficina o residencia, en este ejemplo es el 10000, habitual para WEBMIN.

Será necesario habilitar el tráfico en el cortafuegos en el servidor Raspberry Pi (ufw), a través del puerto 10000 y demás puertos necesarios.

Se pulsará sobre Añadir.

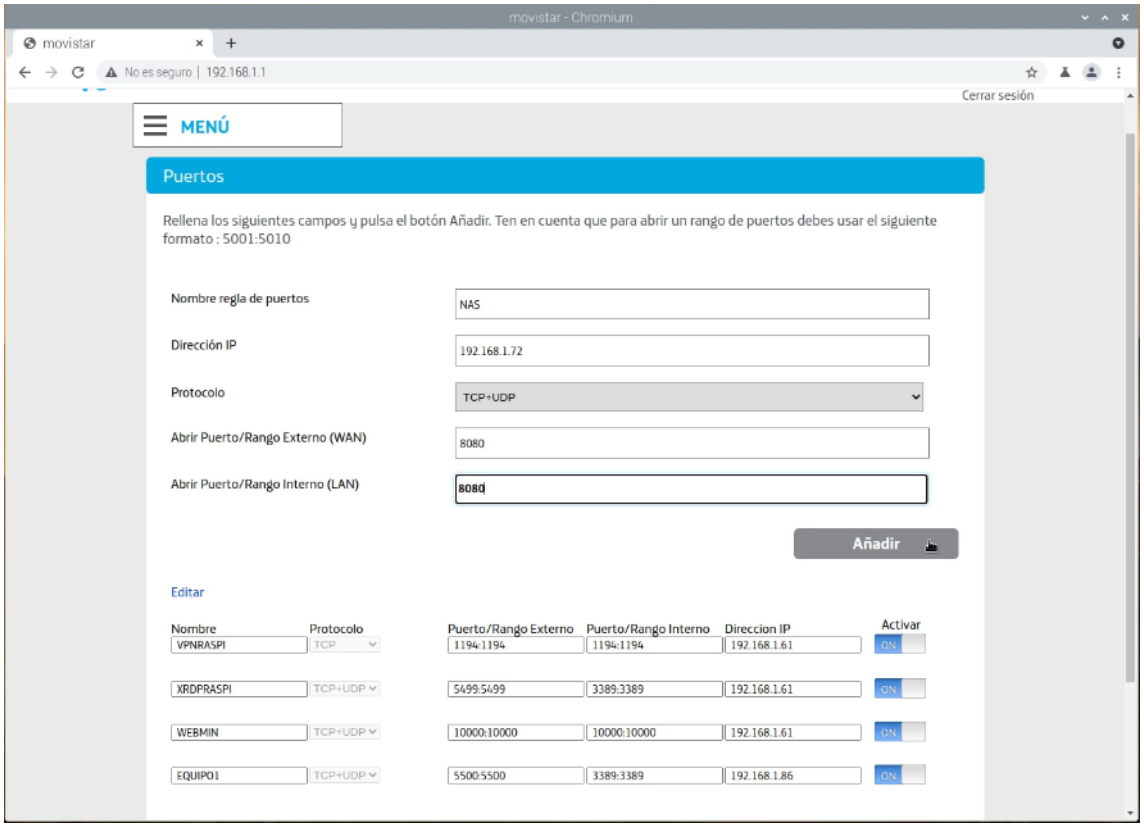


- Protocolo RDP (XRDP), (Para conexión equipo cliente).

    - Nombre regla de puertos, nombre que se le quiera dar, en este caso EQUIPO1.
    - Dirección IP, dirección IP del dispositivo, en este caso, se trata de una conexión a un equipo físico, por lo que se coloca su IP (dentro de la LAN, dentro de la oficina o residencia), adquirida por el equipo, se explicará cómo saberla. (192.168.1.86).
    - Protocolo, en este caso se selecciona TCP+UDP, dependiendo del protocolo seria TCP, UDP, o ambos en este ejemplo.
    - Abrir Puerto/Rango Externo (WAN), nº de puerto a abrir, parte externa de la oficina o residencia, en este ejemplo es el 5500.
    - Abrir Puerto/Rango Interno (LAN), nº de puerto a abrir, parte interna de la oficina o residencia, en este ejemplo es el 3389, para conexiones RDP habitualmente es este puerto.

Será necesario habilitar el tráfico en el cortafuegos en el servidor si es necesario, en el equipo cliente también puede ser necesario abrir el puerto 5500 y demás puertos necesarios para poder realizar la conexión.

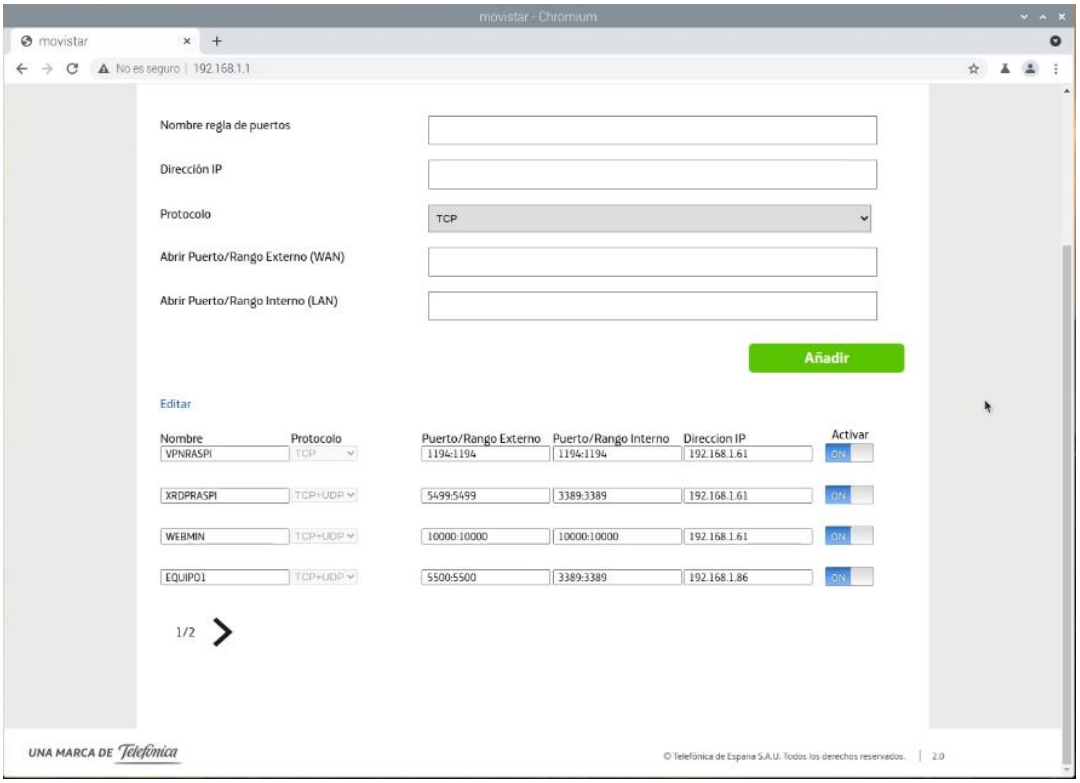
Se pulsará sobre Añadir.

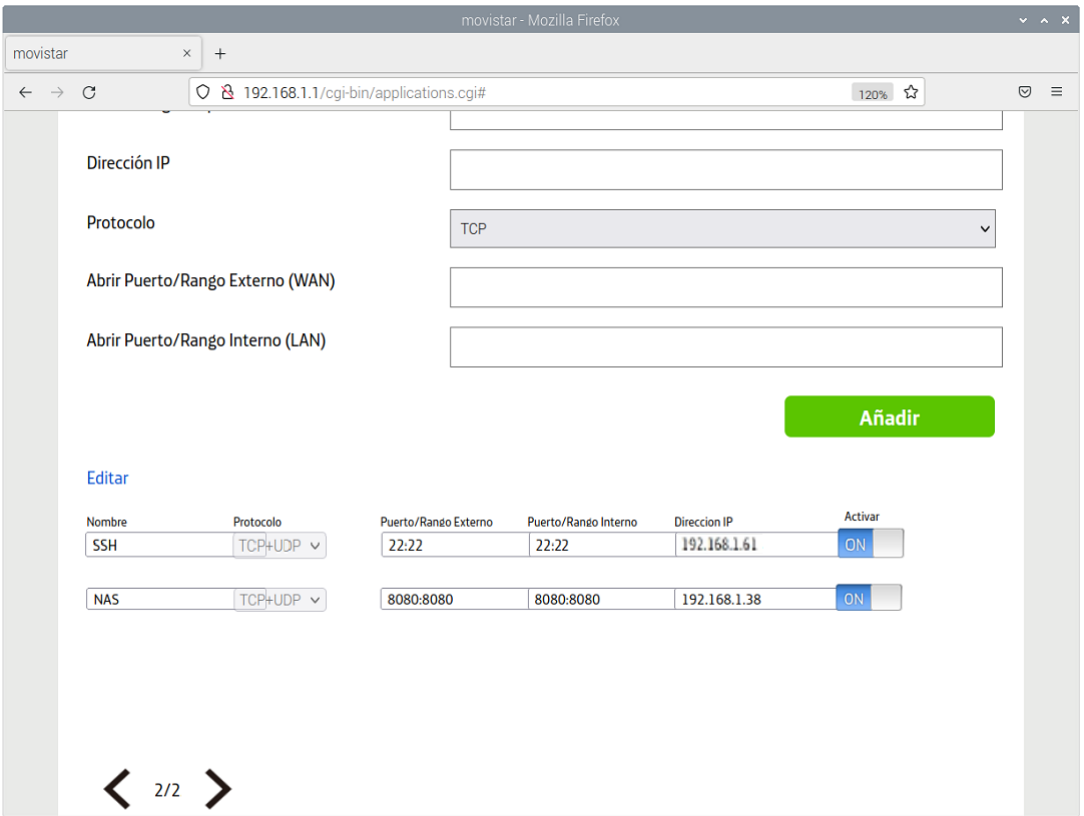


- Puerto para conexión WEB (8080).
    - Nombre regla de puertos, nombre que se le quiera dar, en este caso NAS.
    - Dirección IP, dirección IP del dispositivo, en este caso, se trata de una conexión a un equipo físico, por lo que se coloca su IP (dentro de la LAN, dentro de la oficina o residencia), adquirida por el equipo, se explicará cómo saberla. (192.168.1.72).
    - Protocolo, en este caso se selecciona TCP+UDP, dependiendo del protocolo seria TCP, UDP, o ambos en este ejemplo.
    - Abrir Puerto/Rango Externo (WAN), nº de puerto a abrir, parte externa de la oficina o residencia, en este ejemplo es el 8080.
    - Abrir Puerto/Rango Interno (LAN), nº de puerto a abrir, parte interna de la oficina o residencia, en este ejemplo es el 8080.

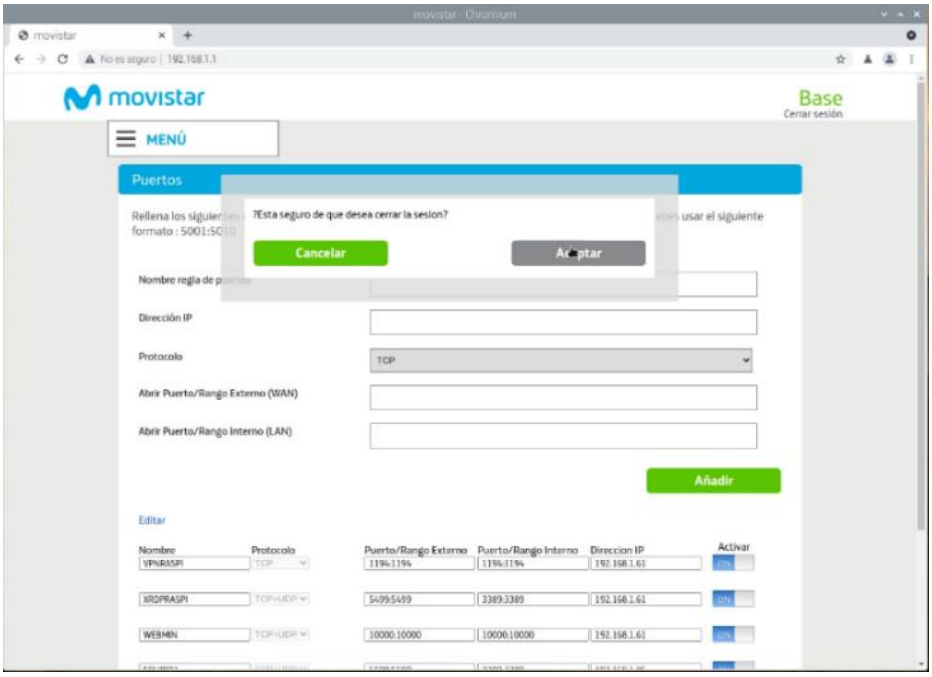
Será necesario habilitar el tráfico en el cortafuegos en el servidor si es necesario, en el equipo cliente también puede ser necesario abrir el puerto 8080 y demás puertos necesarios para poder realizar la conexión.

Se pulsará sobre Añadir.



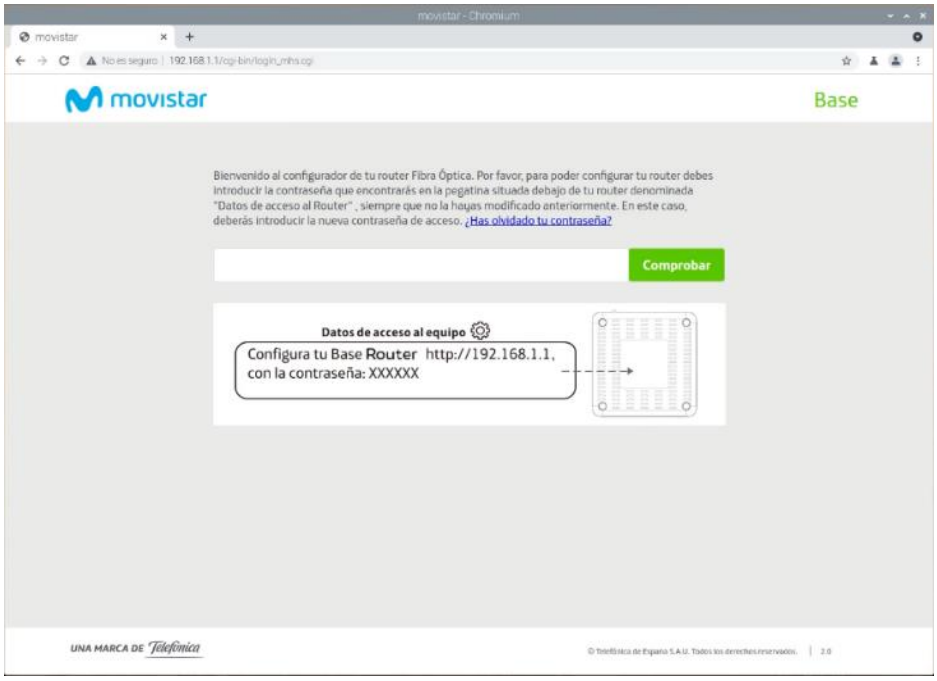


Quedando como se puede observar en las ventanas de las capturas superiores.



Terminada la apertura de puertos, se podrá salir de la configuración del router pulsando sobre Cerrar sesión en la parte superior derecha.

En el cuadro de dialogo que aparece se pulsará sobre Aceptar.



Preparación Tarjeta microSD.

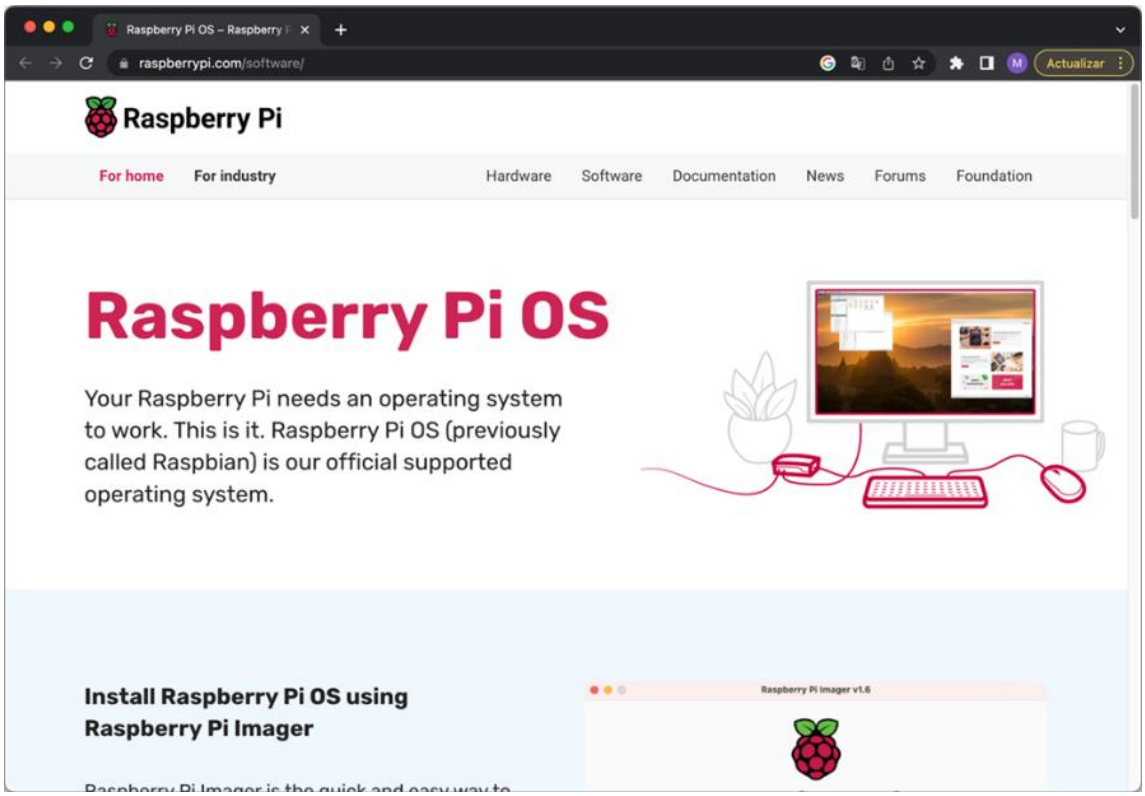
Como se indicó, se pretende explicar todo el proceso de una forma clara y paso a paso, para que cualquier persona sin grandes conocimientos de informática sea capaz de llevar a cabo el mismo, por lo que se explicara ciertos pasos en varios Sistemas Operativos (S.O.), lo único que se tiene que hacer es llevar a cabo los pasos según el S.O. del que se disponga, tanto en la parte servidor que en este proyecto se utiliza una Raspberry Pi con S.O. propio derivado de Linux Debian, como en la parte cliente.

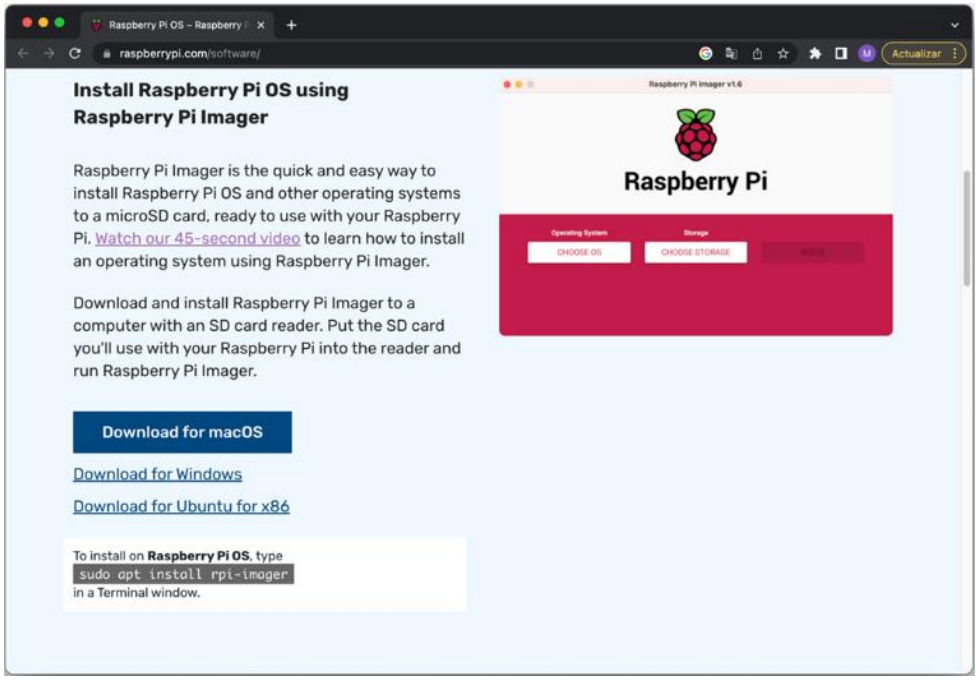
Preparación en Sistema Operativo Apple macOS.

Descarga e instalación de la aplicación Raspberry Pi Imager.

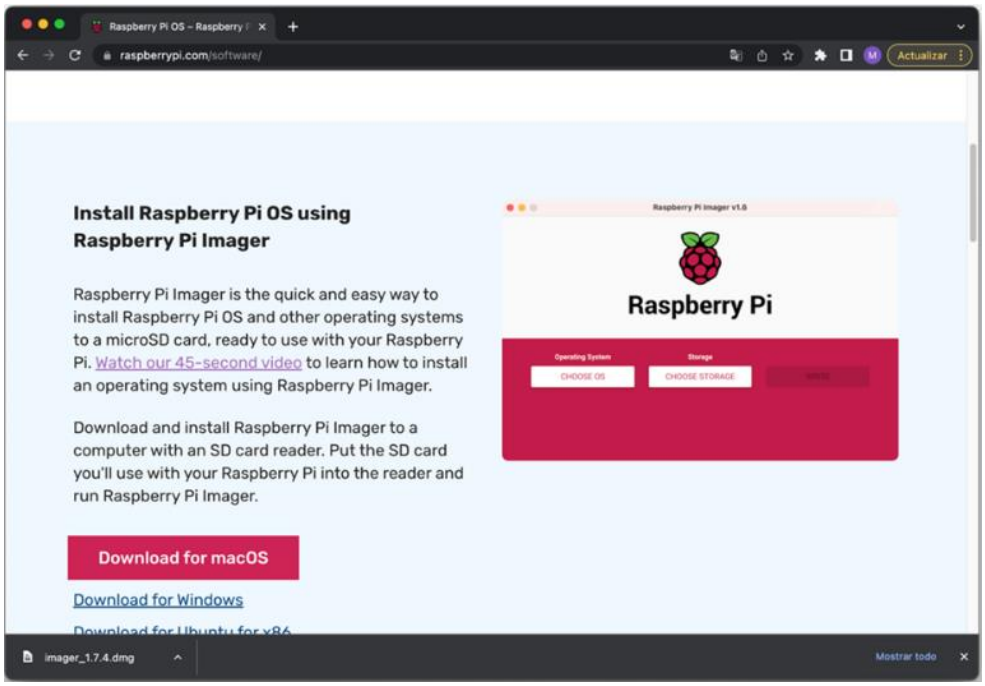
Para comenzar, se tendrá que descargar e instalar la aplicación Raspberry Pi Imager, esta descarga se podrá realizar desde la WEB oficial del proyecto.

URL. https://www.raspberrypi.com/software/

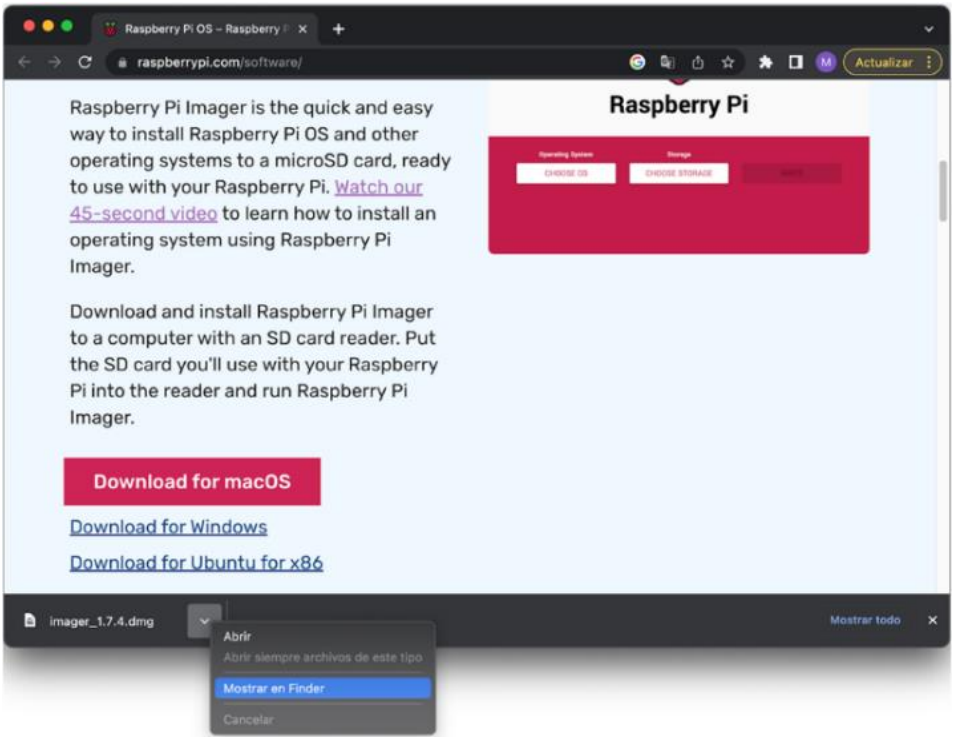




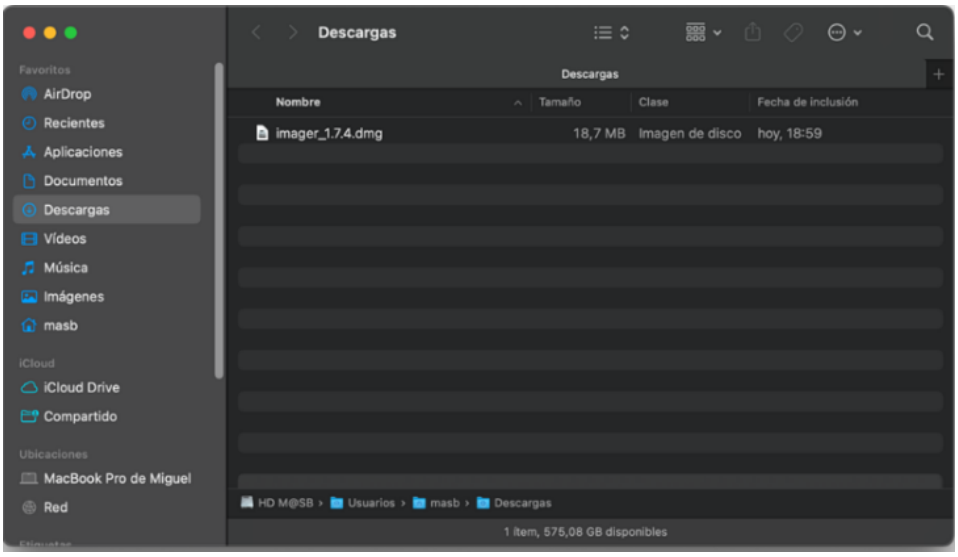
Una vez en la WEB, se deslizará la barra de deslizamiento lateral derecha para localizar el botón: Download for “X”, siendo “X” el S.O. del que se disponga, en este ejemplo es macOS, pulsando sobre el botón: Download for macOS.



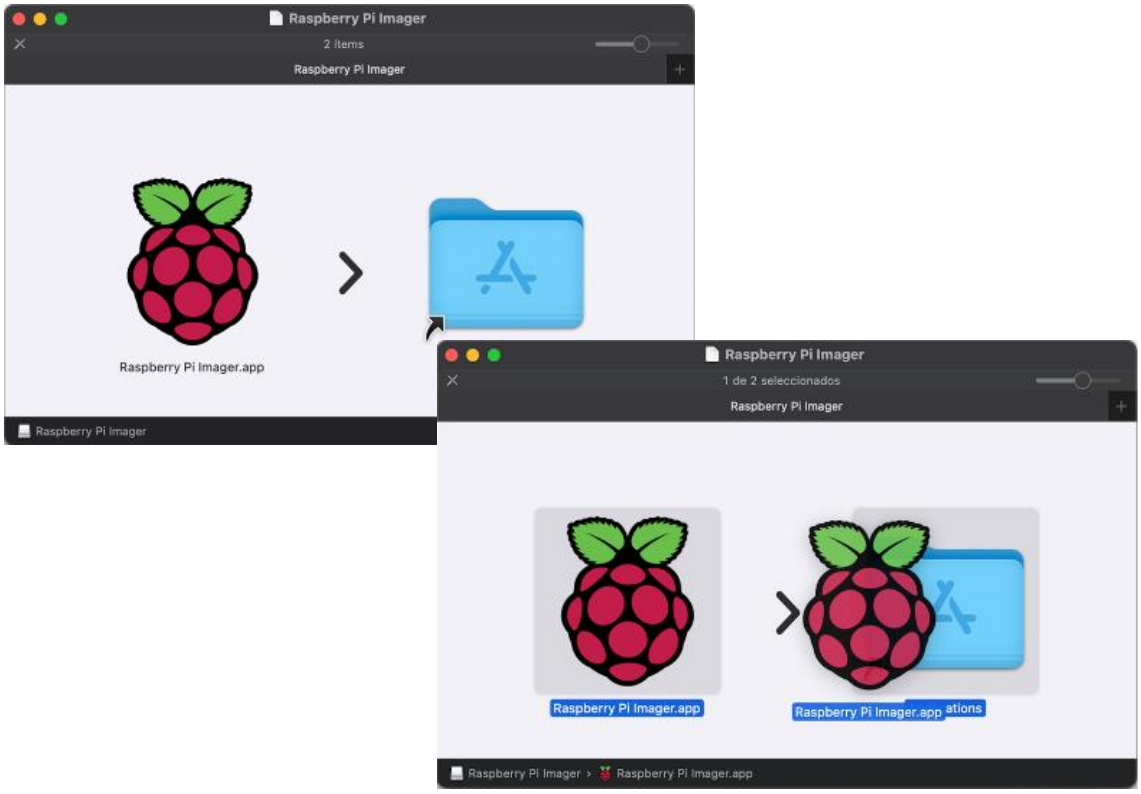
Se pulsará sobre el botón: Download for macOS, recuerda, el S.O. que se disponga puede ser diferente.



Una vez descargada la aplicación, en este caso (la imagen de disco de la aplicación), se accederá a la imagen de disco en este ejemplo desde el navegador Google Chrome, pulsando en la barra inferior del navegador sobre la flecha que apunta hacia abajo, pulsando sobre: Mostrar en Finder, como se muestra en la ventana de la captura superior.

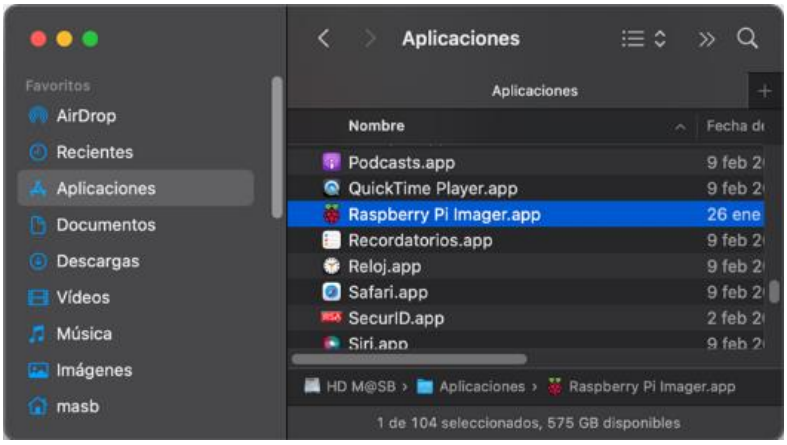


Dentro del Finder, en la ubicación de descarga, a tal efecto carpeta Descargas, se hará doble clic con el botón izquierdo del ratón sobre el fichero descargado imager_1.7.4.dmg, para montar y abrir en este caso la imagen de disco de la aplicación.



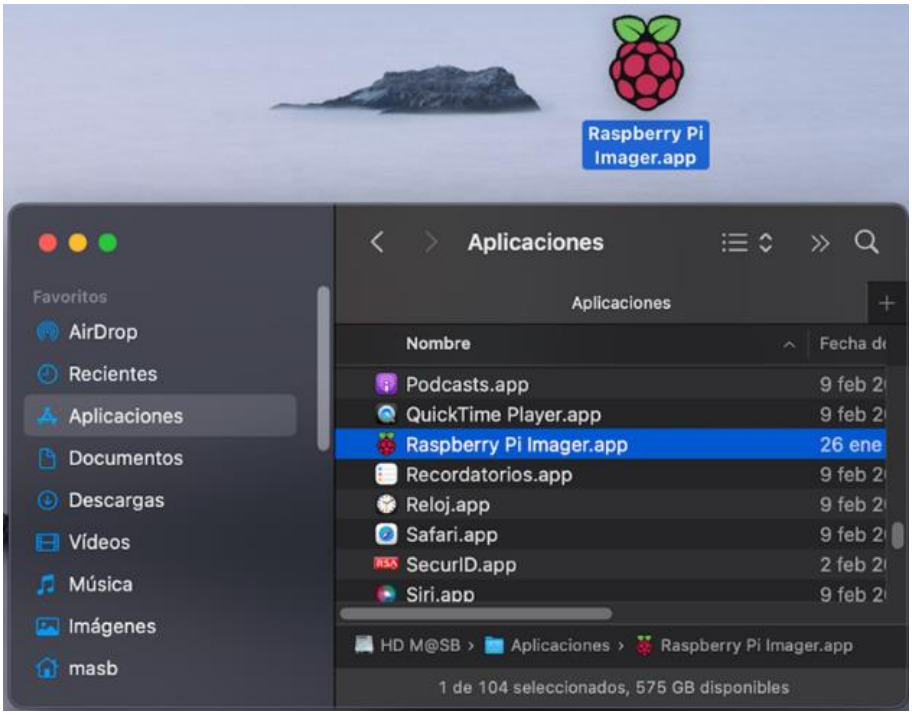
Con el fichero imager_1.7.4.dmg montado y abierto, se pulsará con el botón izquierdo del ratón sobre la aplicación Raspberry Pi Imager.app, en la captura de la ventana superior, el icono de la aplicación izquierda, sin soltarla se arrastrará a la carpeta Applications, icono de la carpeta Applications, derecha.

Copiada la aplicación a la carpeta: Aplicaciones (Applications), se podrá cerrar el fichero imagen de disco abierto de la aplicación descargada anteriormente.



En estos momentos, se tendrá la aplicación: Raspberry Pi Imager.app dentro de la carpeta Aplicaciones (Applications), para abrirla habrá que dirigirse dentro del Finder a la carpeta: Aplicaciones (Applications).

Se podrá crear un alias (Acceso directo a la aplicación), o ejecutarla desde esa misma ubicación.



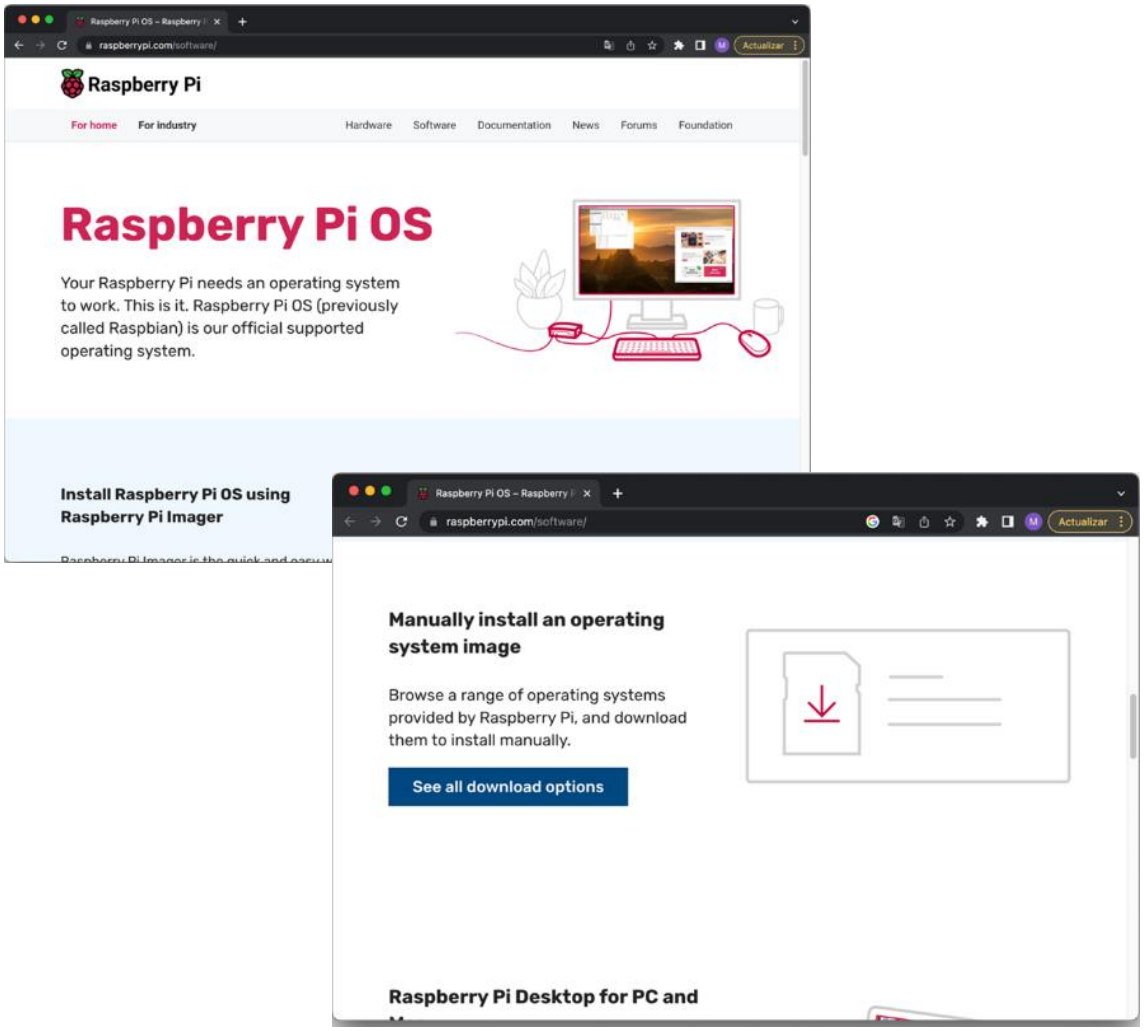
Crear un Alias, es tan sencillo como dentro de la carpeta Aplicaciones en el Finder, pulsar con el botón izquierdo del ratón sobre la aplicación en cuestión, en este ejemplo sobre Raspberry Pi Imager.app, y sin soltar el botón arrastrar hacía por ejemplo una zona libre del escritorio para crear en ese sitio donde se suelte el botón del ratón el Alias, (Acceso directo a la aplicación).

Para ejecutar la aplicación, creado el Alias, o desde la carpeta Aplicaciones, se ejecutada la aplicación, al hacer doble clic sobre la aplicación con el botón izquierdo del ratón.

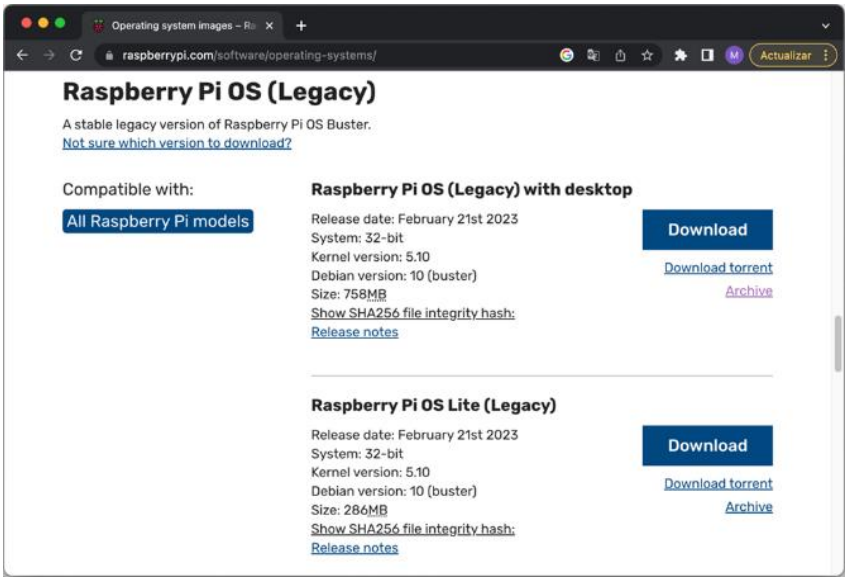
Descarga del fichero imagen del S.O. Raspberry Pi OS.

Para poder continuar y nuevamente en la WEB oficial del proyecto.
URL. https://www.raspberrypi.com/software/

Para la realización de este proyecto junto con la documentación se utiliza un Sistema Operativo (S.O.) en concreto, para facilitar todo el proceso de instalación de las aplicaciones, en caso de querer, se puede descargar y utilizar otro Sistema Operativo (S.O.) aunque en ese caso puede que a la hora de la instalación de ciertas aplicaciones no se llegue a cumplir las dependencias de instalación del paquete, no pudiendo entonces realizar la instalación.



Habrá que deslizar nuevamente la barra de deslizamiento ubicada en la parte lateral derecha hasta localizar el botón See all download options, como se puede observar en la captura de la imagen superior, localizado el botón, se pulsará sobre él.



En esta nueva ventana, habrá que deslizar la barra lateral de deslizamiento hasta llegar a ver el apartado: Raspberry Pi OS (Legacy), como se puede apreciar en la ventana de la captura superior.

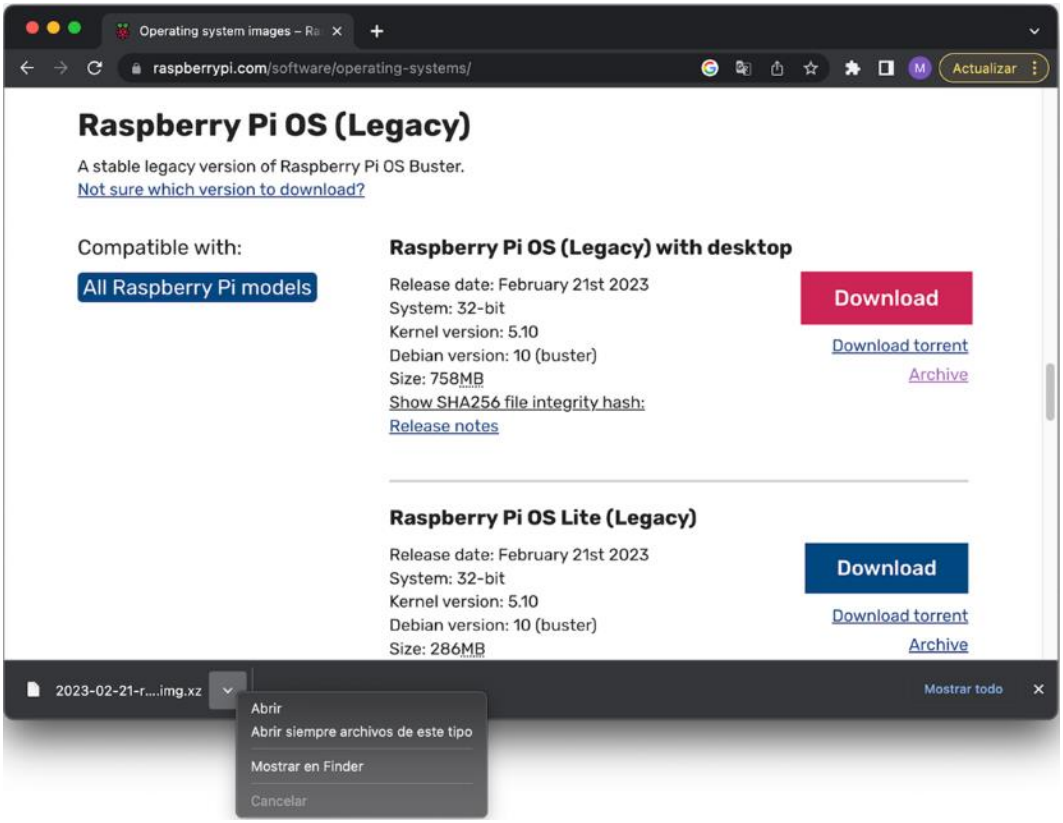
Como se mencionó anteriormente, para la creación de este proyecto, se utiliza una versión del S.O. para facilitar la instalación de ciertas aplicaciones necesarias para la realización del mismo, cualquier persona puede utilizar otra versión del Sistema Operativo (S.O.) que se indica, aunque en esa situación ciertas aplicaciones al proceder a su instalación puede que varíe sutilmente su instalación o no se cumplan las necesidades de instalación al verificar las dependencias del paquete a instalar.



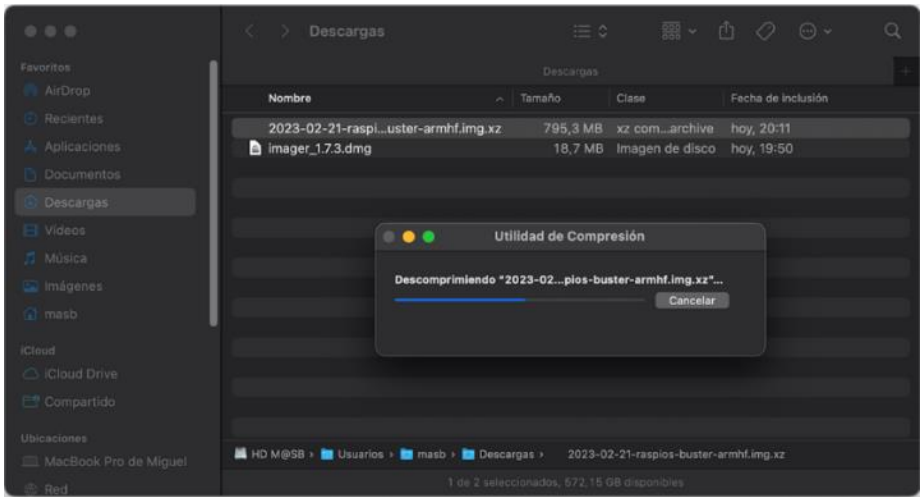
Aunque se puede descargar una de las dos versiones del Sistema Operativo (S.O.).

- Raspberry Pi OS (Legacy) with desktop.
- Raspberry Pi OS Lite (Legacy).

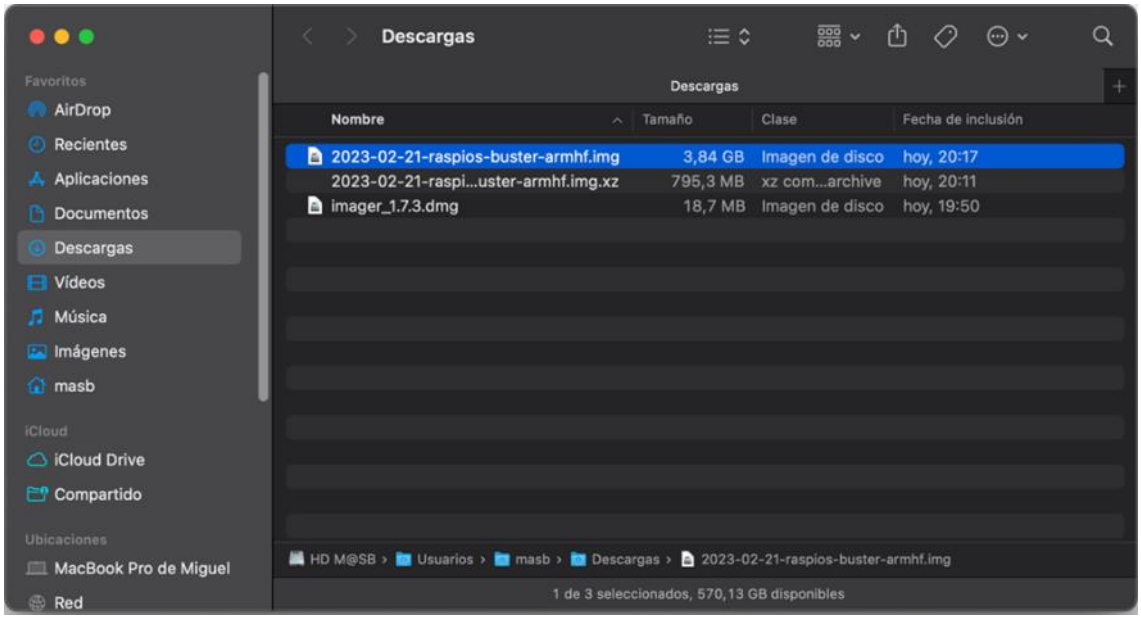
Para este proyecto y para facilitar todo lo posible se realiza la descarga de la versión que se indica en la captura superior con el botón seleccionado en color granate, dicha versión es
Raspberry Pi OS (Legacy) with desktop
Release date February 21st 2023



Descargado el fichero del S.O., en este caso se trata de: Raspberry Pi OS (Legacy) with desktop, se pulsará en la barra inferior del navegador sobre la flecha que apunta hacia abajo y en el menú que se muestra, se tendrá que seleccionar la opción Mostrar en Finder.



En la ubicación de la descarga, en este caso la carpeta Descargas, habrá que hacer doble clic con el botón izquierdo del ratón sobre el fichero descargado, siendo este el fichero: 2023-02-21-raspios-buster-armhf.img.xz



Una vez descomprimido el fichero, se tendrá ahora el fichero: 2023-02-21-raspios-buster-armhf.img

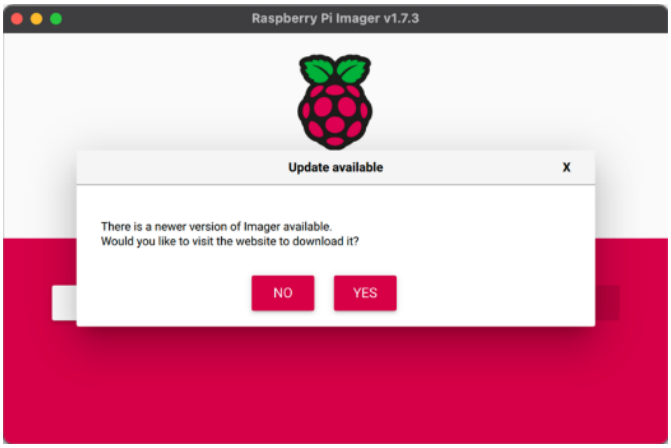
Se ha comprobado que el programa Raspberry Pi Imager, es capaz de manejar la imagen del S.O. descargado incluso sin su descompresión.

Preparación e instalación del S.O. en la tarjeta microSD.

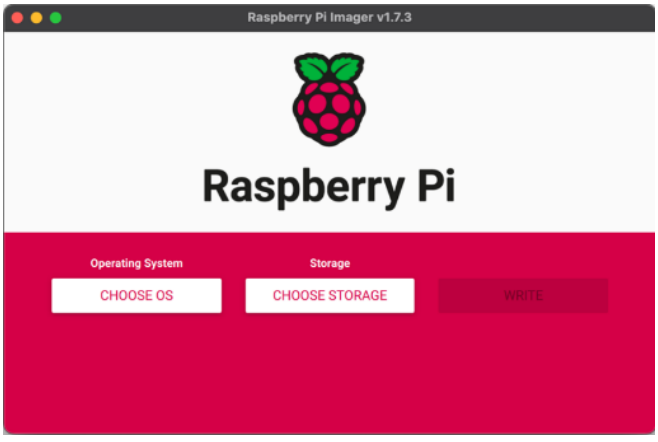
Llegado a este punto en el que tenemos descargada la imagen del S.O. a instalar en la tarjeta de memoria microSD, habrá que introducir la tarjeta en un lector de tarjetas o primero en un adaptador y posteriormente en el lector de tarjetas microSD.



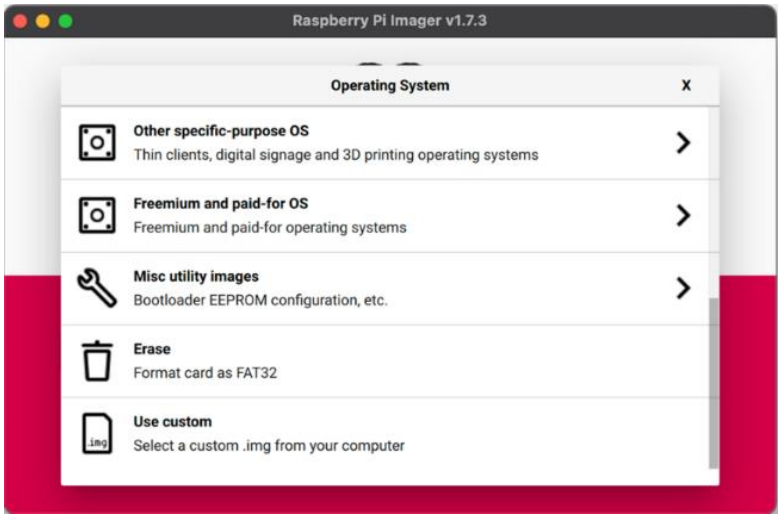
Con la tarjeta introducida y detectada por el S.O., se hará doble clic sobre el Alias (icono de acceso directo a la aplicación), o sobre la aplicación Raspberry Pi Imager.app ubicada en Aplicaciones.



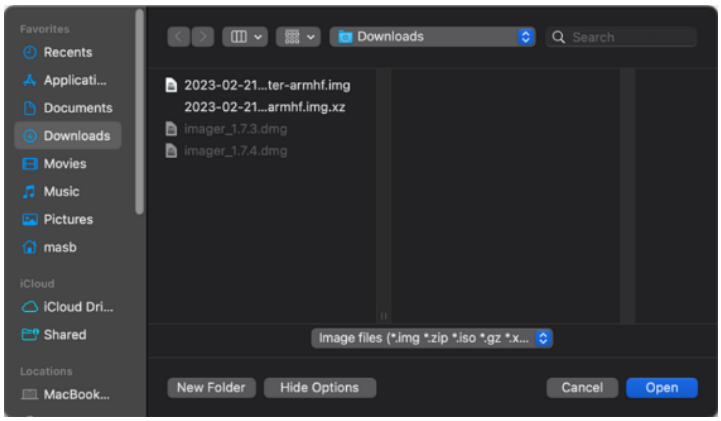
Al abrir la aplicación, en caso de existir alguna versión nueva, se nos informara de si se desea descargar la actualización, en este ejemplo se pulsa sobre: NO.



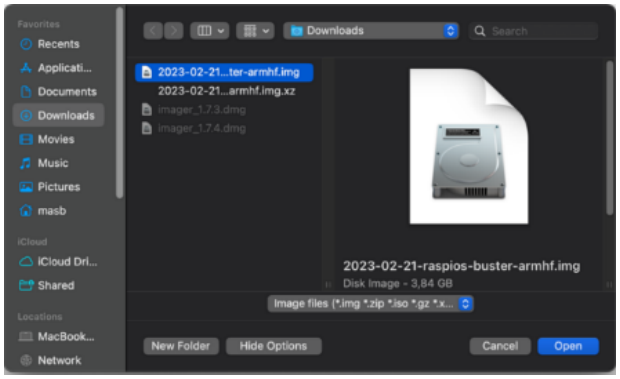
Dentro de la aplicación Raspberry Pi Imager, se pulsará sobre: CHOOSE OS, para seleccionar el S.O. descargado con anterioridad.



Como se mencionó anteriormente, para la realización de este proyecto, se elige una versión en concreto del S.O., por lo que habrá que deslizar la barra de deslizamiento situada en el lateral derecho hasta encontrar la opción inferior: Use custom.



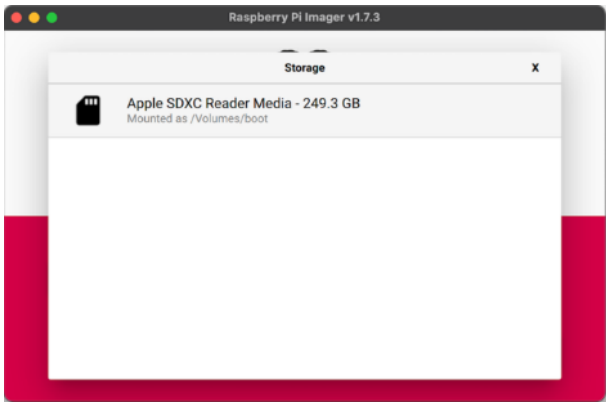
Habiendo pulsado sobre la opción: Use custom, aparecerá un asistente para poder localizar el fichero descargado y descomprimido anteriormente del S.O., en este ejemplo se descargó en la carpeta Descargas, concretamente el fichero descargado es el 2023-02-21-raspios-buster-armhf.img.xz y descomprimido es el fichero 2023-02-21-raspios-buster-armhf.img.



Se seleccionará el fichero en cuestión, en este caso el fichero 2023-02-21-raspios-buster-armhf.img y posteriormente se pulsará sobre el botón: Open.



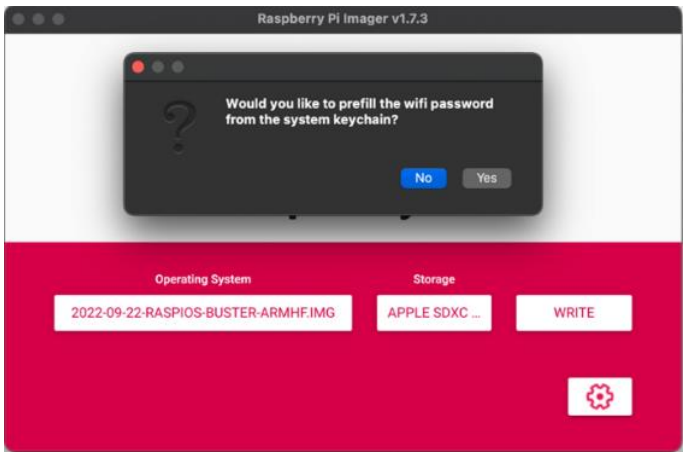
En este momento, si no se ha insertado la tarjeta microSD, habrá que insertarla en el adaptador y posteriormente en el lector de tarjetas, con la tarjeta microSD introducida en el adaptador, se insertará en el lector para su preparación, en este momento, al pulsar sobre: CHOOSE STO…, ya tendría que estar introducida y detectada por el S.O., en caso contrario se introducirá antes de pulsar sobre: CHOOSE STO…



Introducida la tarjeta de memoria microSD y habiendo pulsado sobre: CHOOSE STO…, se nos mostrara la tarjeta disponible, como se muestra en la ventana de la captura izquierda.
En la ventana que se muestra, se informa que disponemos montada una tarjeta de memoria en /Volumes/boot, se seleccionara, pulsando sobre ella.



Ya se podría pulsar sobre el botón WRITE para comenzar el proceso, sin embargo, si se quiere personalizar aún más la instalación, se podrá pulsar sobre el icono con aspecto de rueda dentada, situado en la parte inferior derecha: .



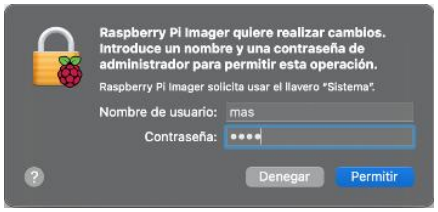
En este manual se explican si no todas, algunas de las opciones que podemos personalizar, para ello se pulsa sobre el icono: ⚙ .

En caso de aparecer la pregunta:

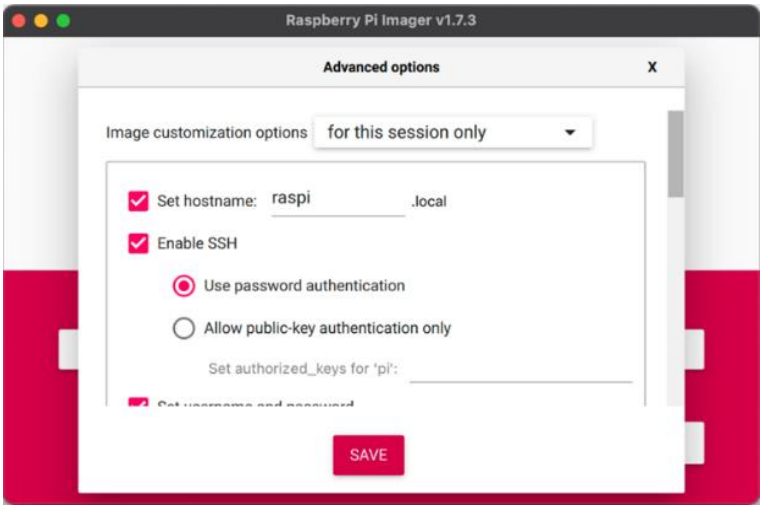
“” Would you like to prefill the wifi password from the system keychain?,
“” ¿Te gustaría prellenar la contraseña wifi del llavero del sistema? “”.

En caso de querer utilizar la contraseña/configuración de la conexión WIFI se pulsará sobre: Yes.





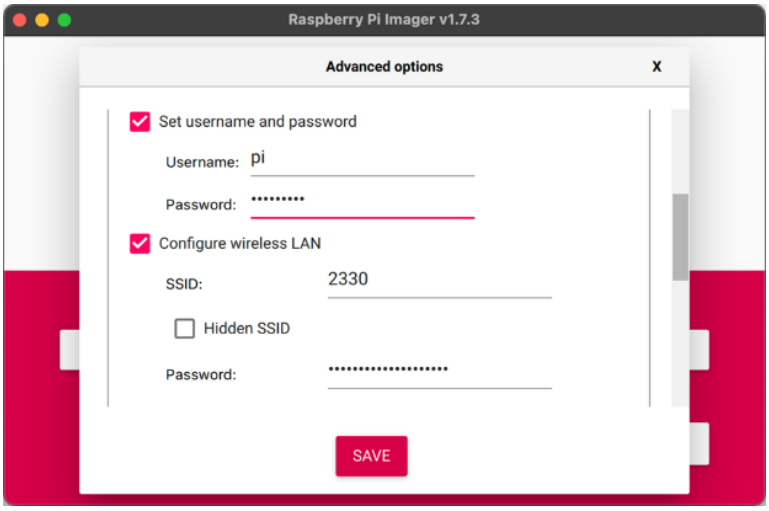
Puede que se solicite un usuario con permisos de administrador, en este ejemplo se solicita un usuario con permisos, se tendrá que proporcionar el nombre de un usuario con permisos y su contraseña.



Se puede seleccionar para que sesión se configuran estas opciones, en este caso se deja seleccionada la configuración para solo esta sesión, en la opción superior: Image customization Options: for this sesión only.

Como se puede apreciar en la ventana de la captura superior, se podrá modificar el nombre del host, habilitando la opción: Set hostname, nombre que se le dará al equipo, en este caso a la Raspberry Pi.

Al marcar la opción Enable SSH, se habilitará el acceso por SSH, seleccionando dicho acceso a través del uso de autenticación por contraseña o con llave pública.

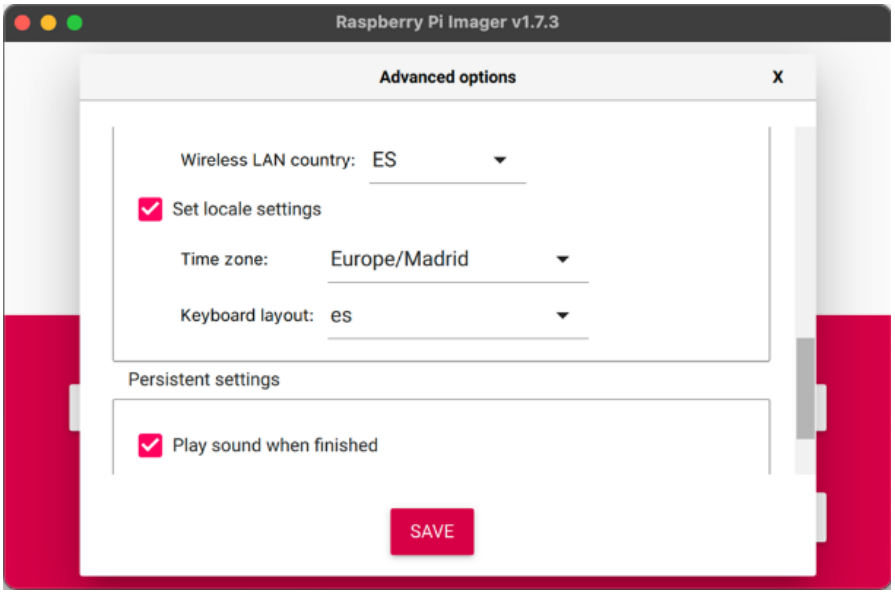


Rellenados o modificados los campos anteriores como se desee, se podrá deslizar la barra de deslizamiento lateral derecha para continuar con las modificaciones.

En este caso se podrá cambiar el nombre del usuario por defecto.

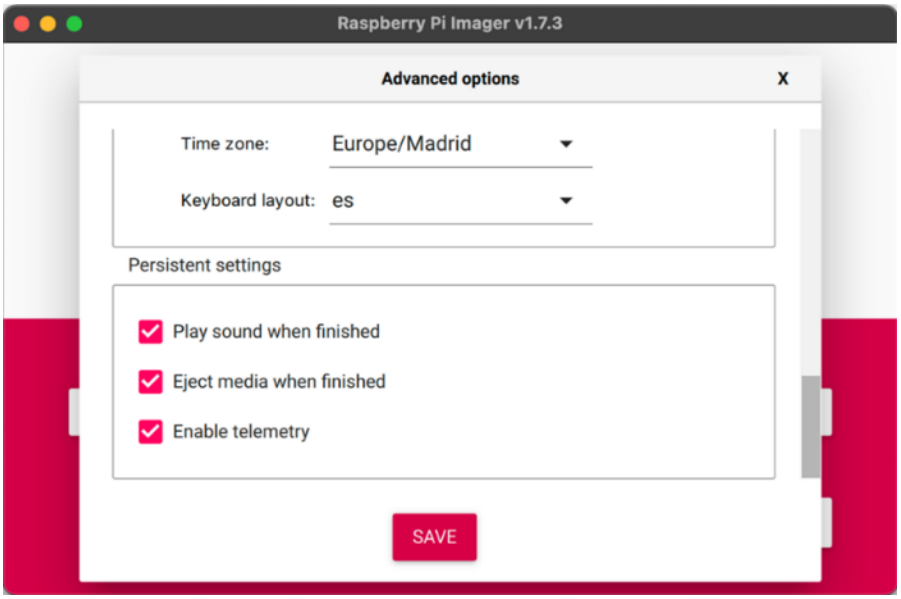
(usuario que será root, superusuario, por lo que se tendrá que recordar la contraseña que se facilite).

Como se aprecia en la ventana de la captura superior, se podrá configurar o se podrá dejar la configuración adquirida desde el S.O. al haber contestado anteriormente si se quería “autorrellenar” la contraseña WIFI.



Deslizando más la barra de deslizamiento ubicada en el lateral derecho, se podrá indicar la localización de la ubicación WIFI.

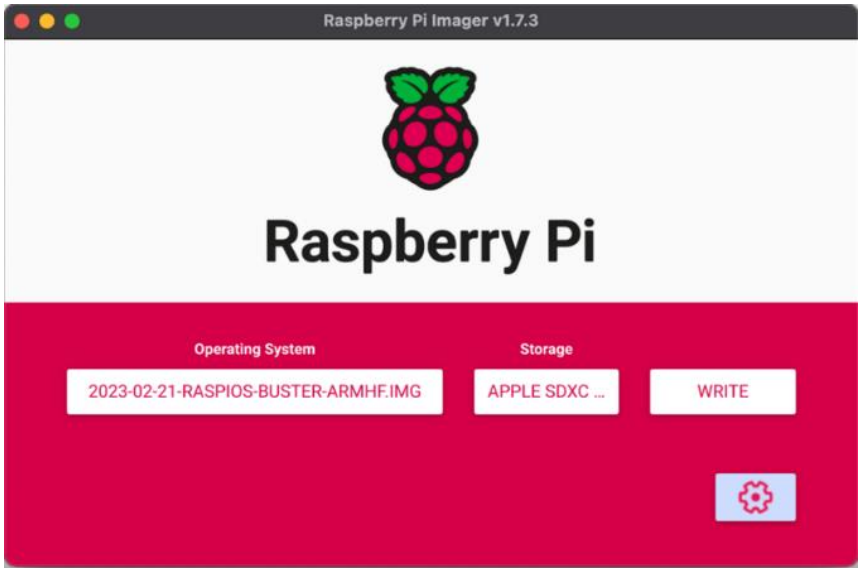
Acto seguido, al seleccionar la opción Set locale settings, si no se encuentra ya seleccionada bien la zona a la que se pertenece, se podrá modificar dichas opciones, Time zone y Keyboard layout tras seleccionar la mencionada opción Set locale settings.



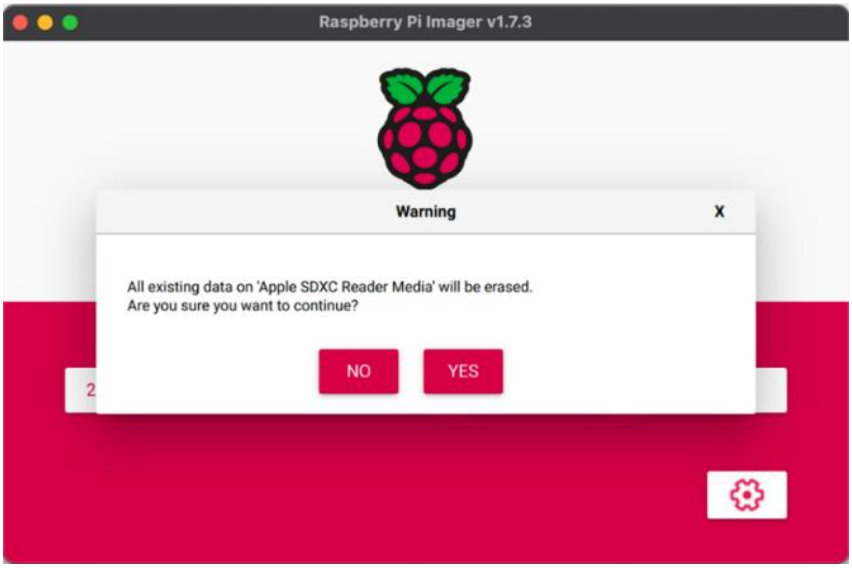
En este caso se modifican las opciones:

- Time zone (Zona horaria): Europe/Madrid
- keyboard layoud (Diseño del teclado): es

Modificadas las opciones como se necesiten, se pulsará sobre el botón: SAVE.



Terminadas todas las modificaciones, se podrá pulsar sobre el botón: WRITE para comenzar la instalación del S.O. en la tarjeta de memoria microSD.



Se mostrará la pregunta.

“All existing data on `Apple SDXC Reader Media` will be erased. Are you sure you want to continue?”

“Se borrarán todos los datos existentes en `Apple SDXC Reader Media`. ¿Está seguro de que desea continuar?”

Si se está Seguro de que la tarjeta de memoria introducida es la correcta se podrá proceder a pulsar sobre: YES.





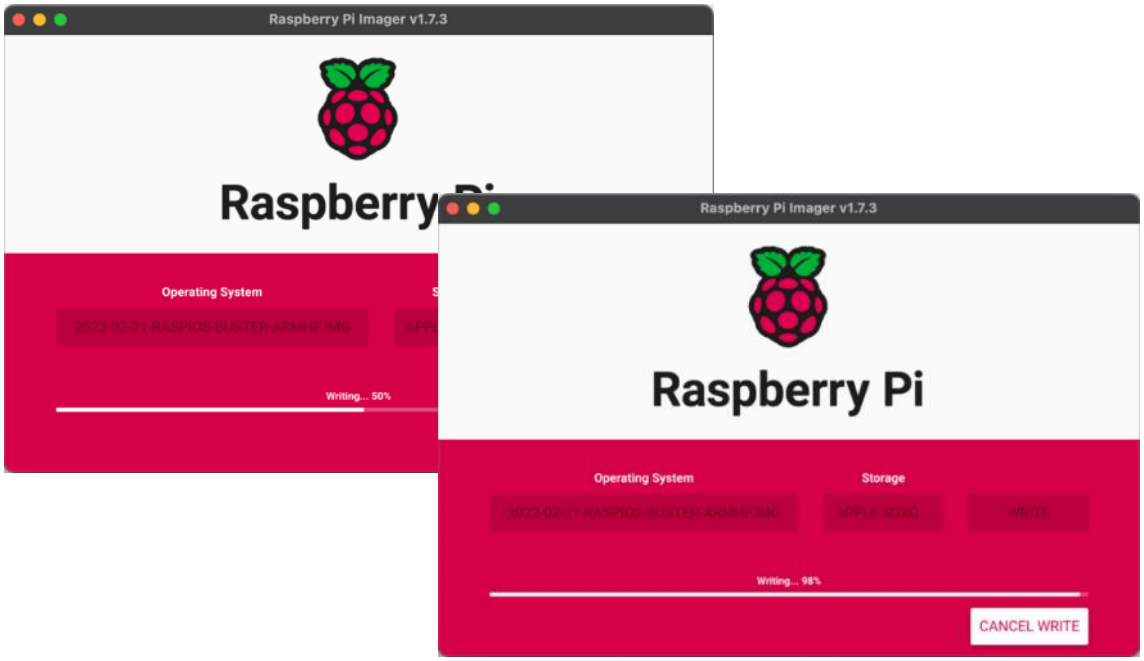
Dependiendo como se encuentre configurado el S.O., puede que aparezca la ventana de la captura izquierda solicitando las credenciales de un usuario con permisos, en la que habrá que proporcionar las credenciales de un usuario con permisos y se pulsará: Aceptar.



Comenzando la preparación para la escritura en la tarjeta.

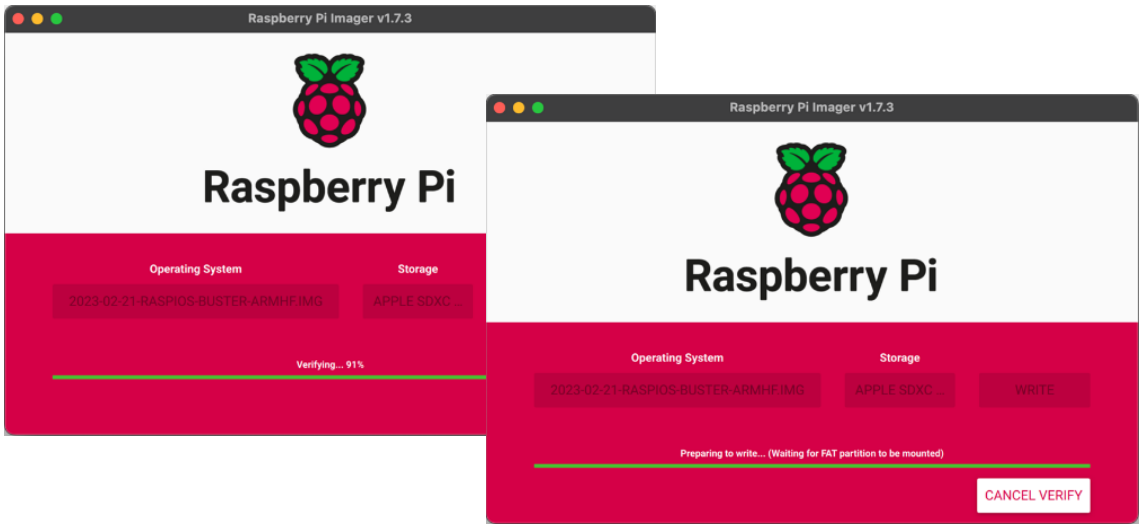


Posteriormente, comienza la escritura en la tarjeta de memoria.

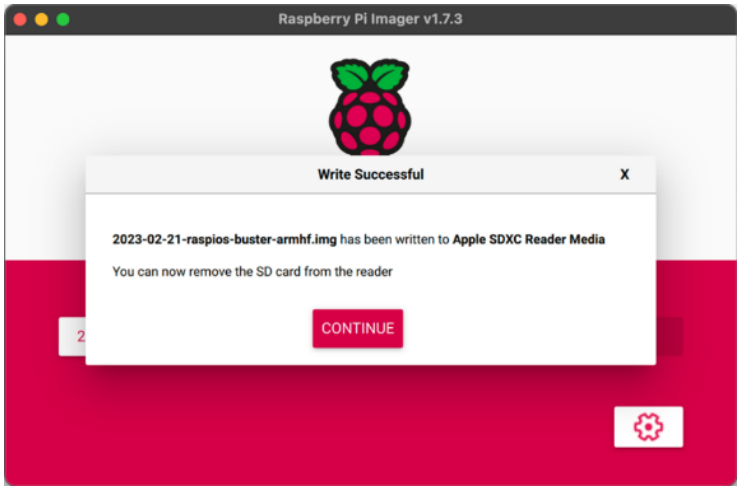




Posterior a la escritura, comienza el proceso de verificación, el cual se podrá detener pulsando sobre: CANCEL VERIFY.







Terminado el proceso se podrá pulsar sobre el botón: CONTINUE.



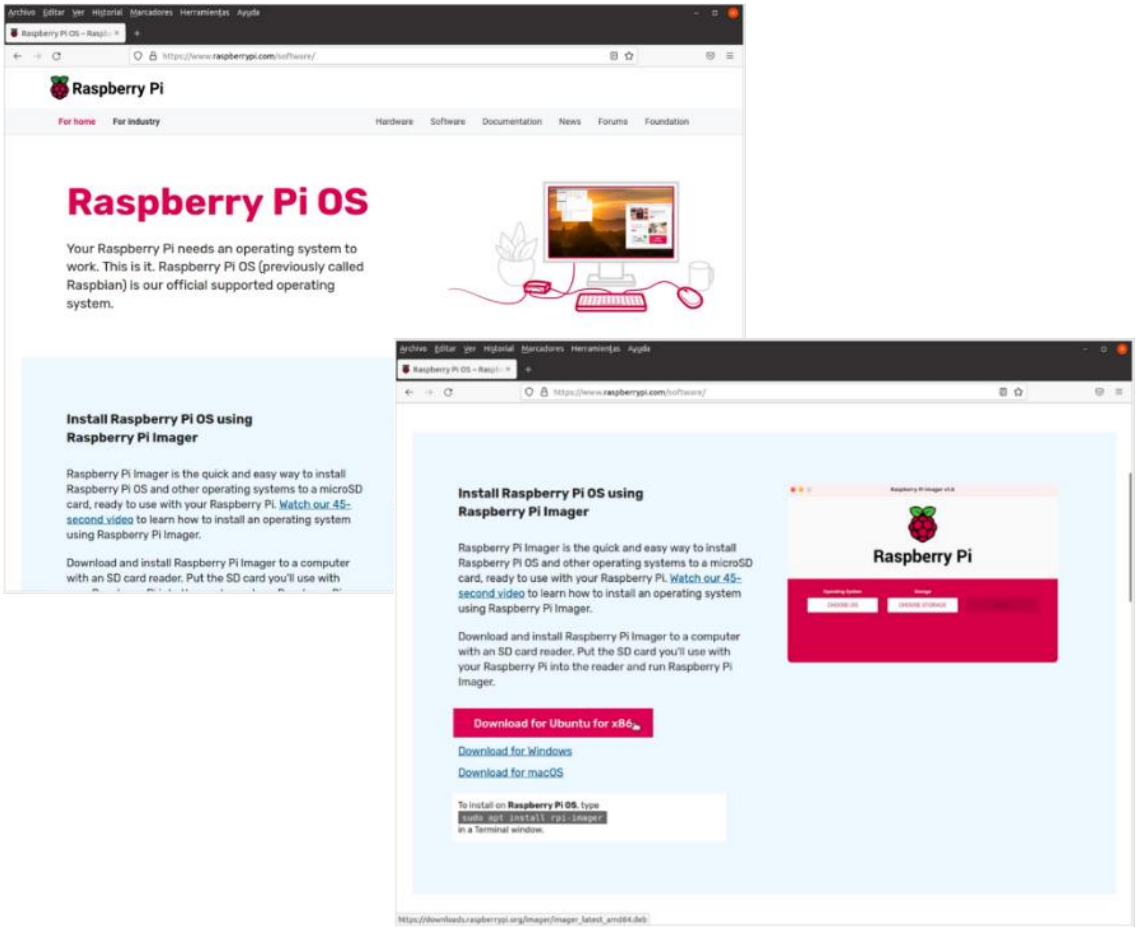
Pudiendo cerrar la aplicación, quitando la tarjeta del lector y se podrá insertar la tarjeta microSD en la Raspberry Pi, donde se continuará más adelante ya con el primer inicio del S.O. su configuración y la instalación de todas las aplicaciones necesarias para este proyecto.

Preparación en Sistema Operativo Linux.

Descarga e instalación de la aplicación Raspberry Pi Imager.

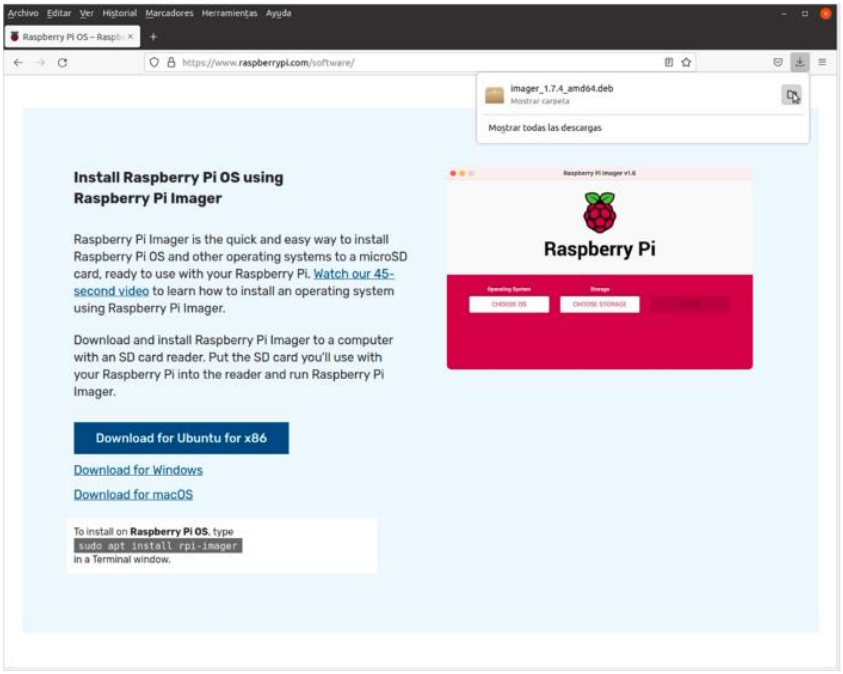
Como en el caso anterior, se comenzará con la descarga e instalación de la aplicación Raspberry Pi Imager, pudiendo realizar la descarga desde la WEB oficial.

URL. https://www.raspberrypi.com/software/

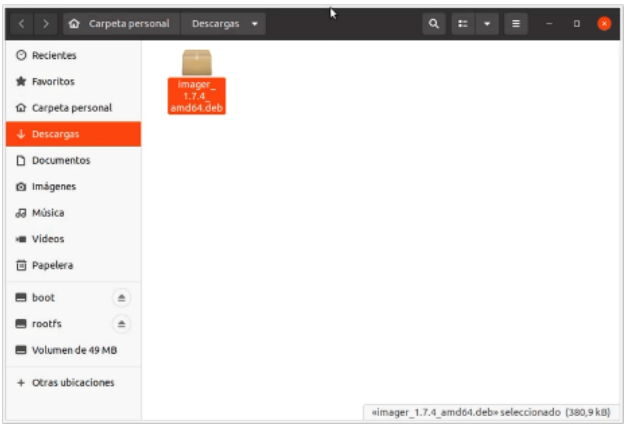


Una vez en la WEB, se deslizará la barra de deslizamiento lateral derecha para localizar el botón Download for “X”, siendo “X” el Sistema Operativo (S.O.) del que se disponga, en este nuevo ejemplo se trata de Linux Ubuntu, pulsando sobre el botón Download for Ubuntu for x86.

Recuerda que el S.O. que se esté utilizando puede ser diferente al que se indica en este apartado.

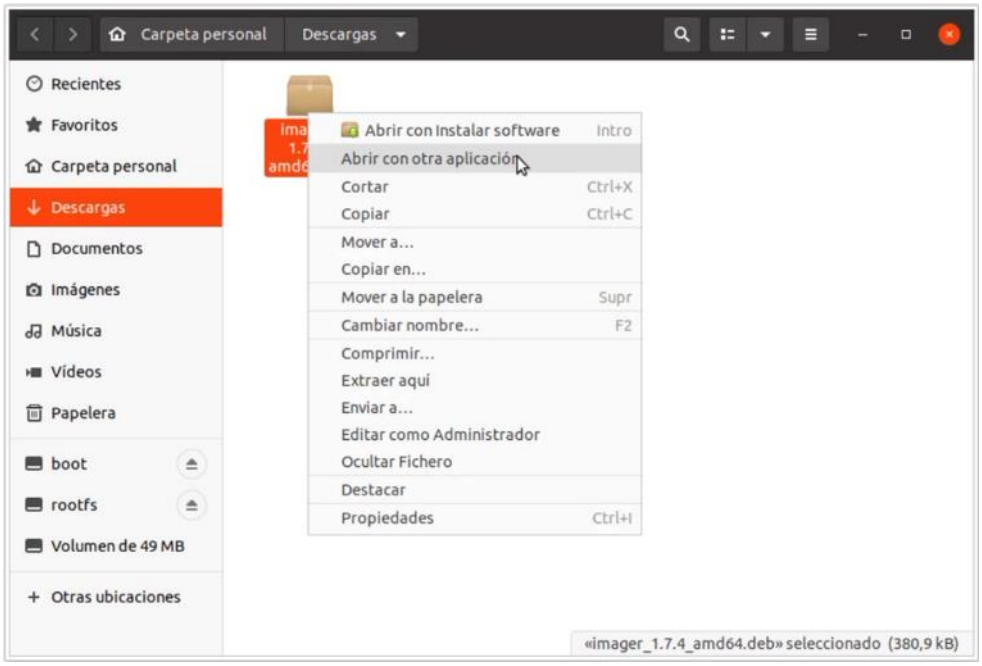


Tras la descarga, en este caso el fichero imager_1.7.4_amd64.deb, se accederá al mismo en este ejemplo desde el navegador Chromium, pulsando en la flecha que apunta hacia abajo en la parte superior derecha en el cuadro de dialogo tras finalizar la descarga.

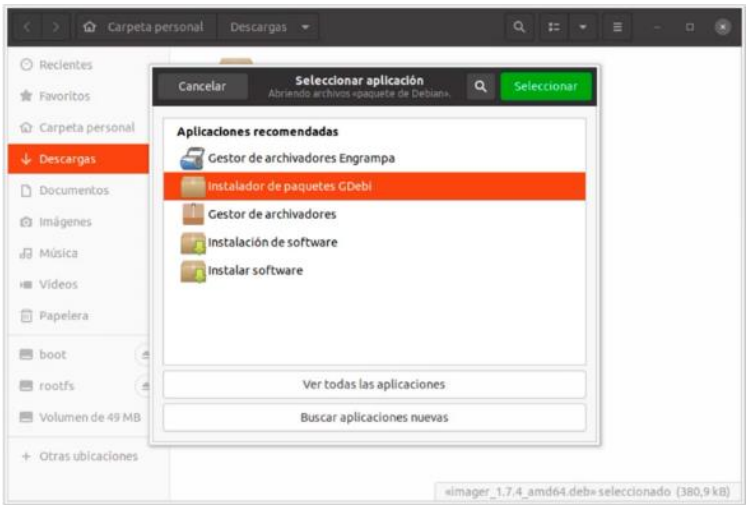


En la ubicación de la descarga del fichero, dentro de la carpeta Descargas, se encuentra el fichero Imager_1.7.4_amd64.deb.

En este ejemplo, se utiliza un equipo con Linux Ubuntu, para la instalación se utiliza la aplicación gdebi instalada, en caso de necesitar instalar la aplicación gdebi, esta aplicación se puede instalar dentro de un terminal ejecutando el comando (sin las comillas), “sudo dpkg –i Imager_1.7.4_amd64.deb”, en caso de aparecernos dependencias incumplidas se utilizará el comando (sin las comillas), “sudo apt-get install -f” y posteriormente el comando (sin las comillas), “sudo dpkg –i Imager_1.7.4_amd64.deb”.



Al pulsar con el botón derecho del ratón sobre el fichero Imager_1.7.4_amd64.deb, se seleccionará la opción Abrir con otra aplicación.

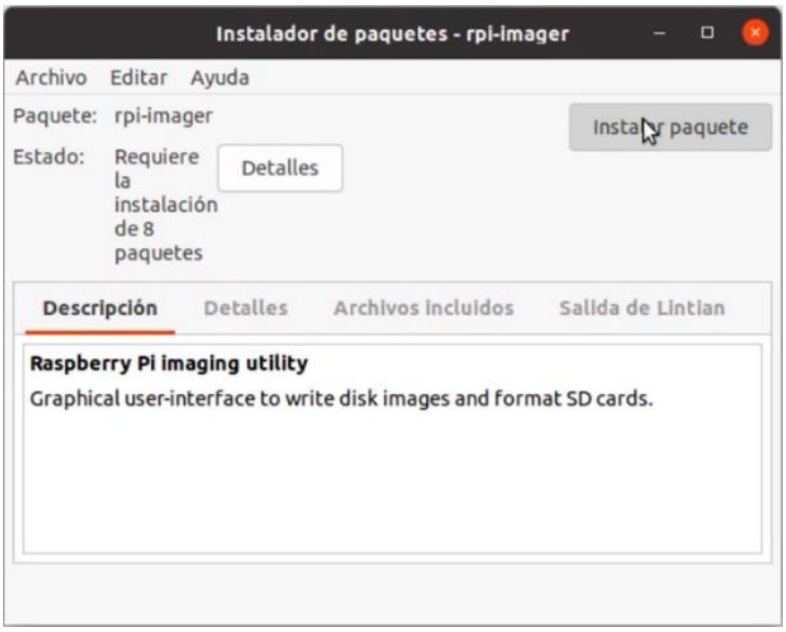


Dependiendo como se encuentre configurado el S.O., o que no se encuentre instalada la aplicación GDebi, para lo que se procederá con el apartado de las instalaciones bajo el terminal de Linux, puede que no nos aparezca la aplicación en la lista de esta ventana.

Se puede instalar la aplicación entonces, dentro de un terminal ejecutando el comando (sin las comillas), “sudo dpkg –i Imager_1.7.4_amd64.deb”, en caso de aparecernos dependencias incumplidas se utilizará el comando (sin las comillas), “sudo apt-get install -f” y posteriormente el comando (sin las comillas), “sudo dpkg –i Imager_1.7.4_amd64.deb”.



En este caso, al seleccionar la aplicación Instalador de paquetes GDebi.



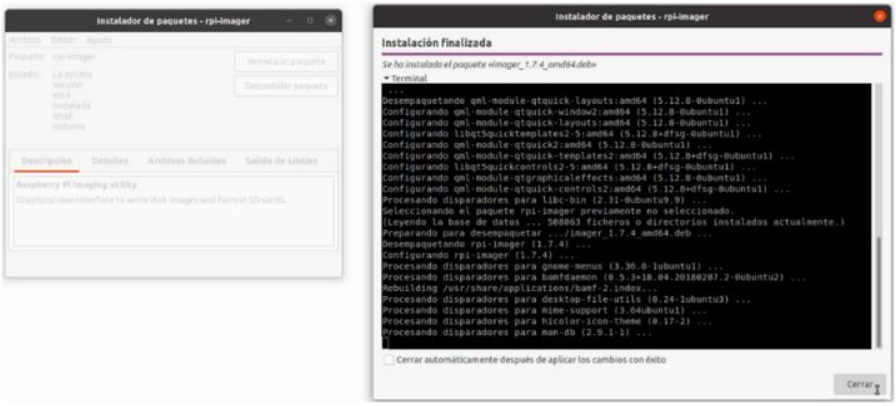
Se abre la aplicación y se tendrá que pulsar sobre el botón Instalar paquete, ubicado en la parte superior derecha.

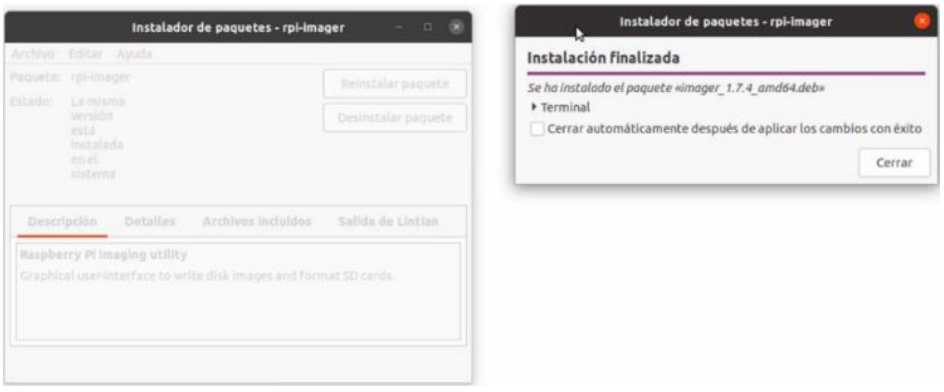


En caso de solicitarse las credenciales de un usuario con permisos, se facilitarán y se pulsara sobre Autenticar.

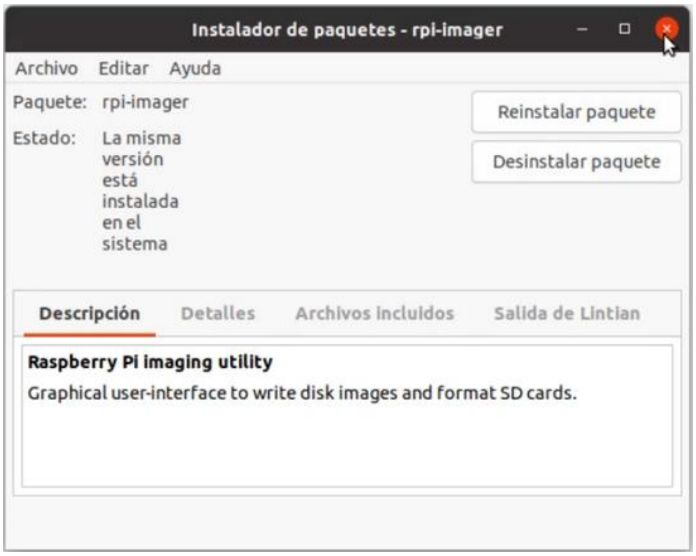


Comenzando el proceso de instalación de las dependencias necesarias como el de la propia aplicación.





Terminada la instalación, se podrá cerrar la ventana instalador de paquetes - rpi-imager, pulsando en Cerrar, ventana de la captura superior derecha

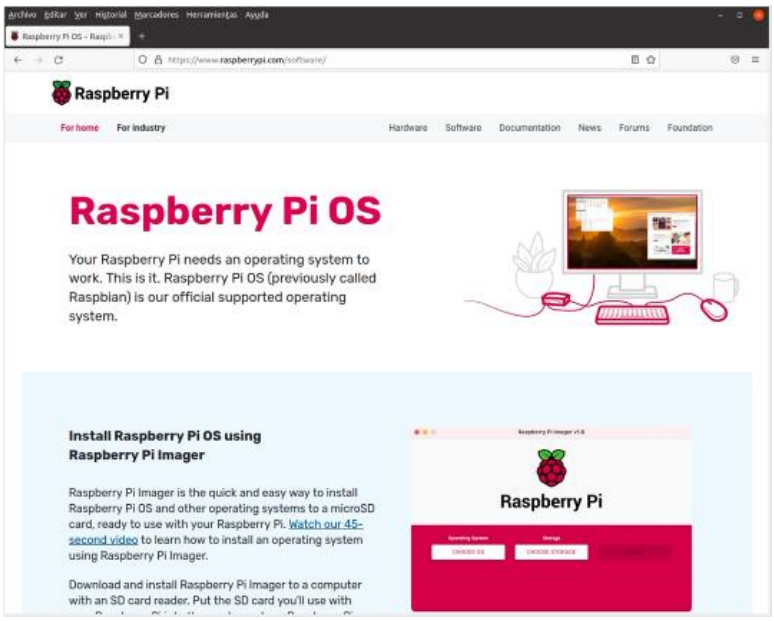


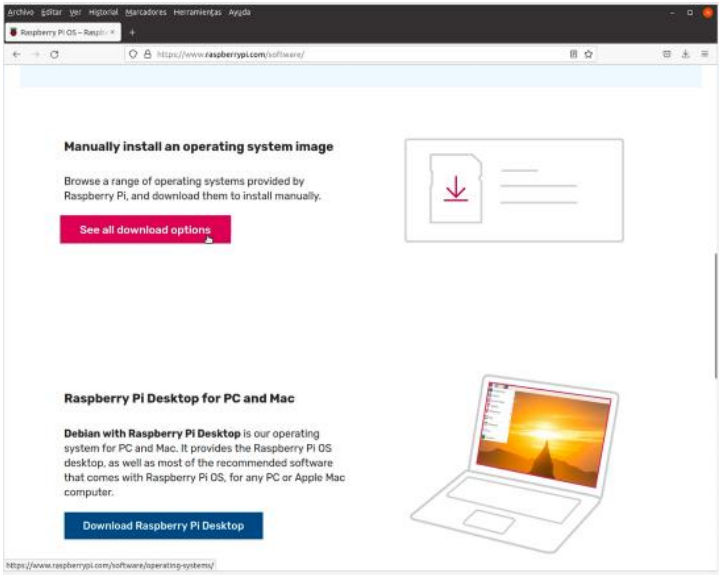
Posteriormente se podrá cerrar la ventana de la aplicación Gdebi: instalador de paquetes - rpi-imager.

Descarga del fichero imagen del S.O. Raspberry Pi OS.

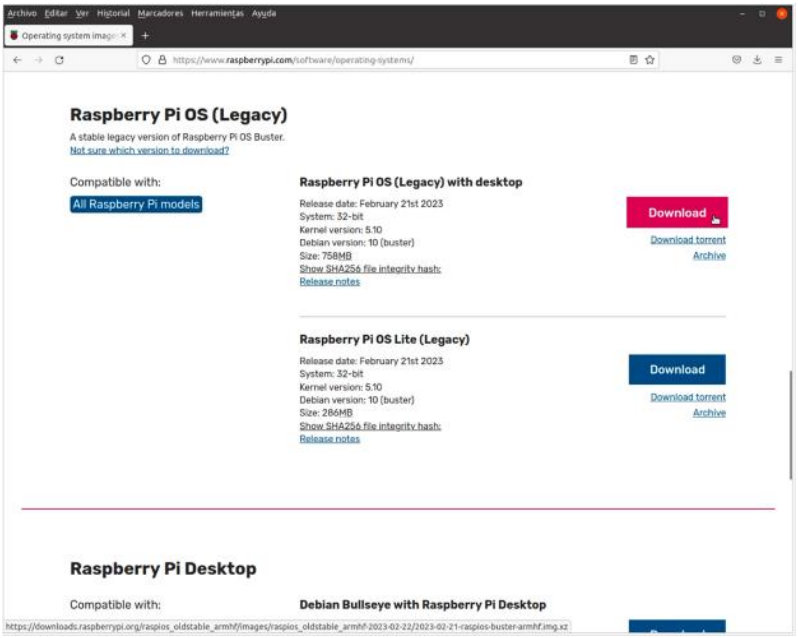
Para la realización de este proyecto junto con la documentación, se utiliza un Sistema Operativo (S.O.) en concreto, para facilitar todo el proceso de instalación de las aplicaciones, en caso de querer, se puede descargar y utilizar otro Sistema Operativo (S.O.), aunque en ese caso puede que a la hora de la instalación de ciertas aplicaciones no se llegue a cumplir las dependencias de instalación del paquete, no pudiendo entonces realizar la instalación.

Nuevamente habrá que descargar el fichero del S.O en la WEB oficial.
URL. https://www.raspberrypi.com/software/





Habrá que deslizar la barra de deslizamiento ubicada en la parte lateral derecha hasta localizar el botón See all download options, como se puede observar en la captura de la imagen izquierda, localizado el botón, se pulsará sobre él.



En esta nueva ventana, habrá que deslizar la barra lateral de deslizamiento hasta llegar a ver el apartado Raspberry Pi OS (Legacy), como se puede apreciar en la ventana de la captura superior.

Se mencionó anteriormente, que para la creación de este proyecto, se utiliza una versión del S.O. para facilitar la instalación de ciertas aplicaciones necesarias para la realización del mismo, cualquier persona puede utilizar otra versión del Sistema Operativo (S.O.) que se indica, aunque en esa situación ciertas aplicaciones al proceder a su instalación puede que varie sutilmente su instalación o no se cumplan las necesidades de instalación al verificar las dependencias del paquete a instalar.

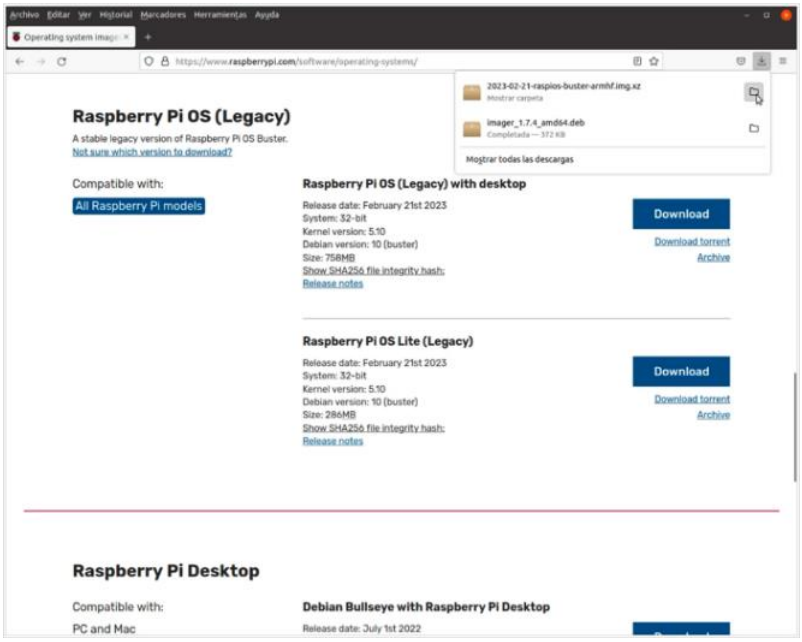


Aunque se puede descargar una de las dos versiones del Sistema Operativo (S.O.).

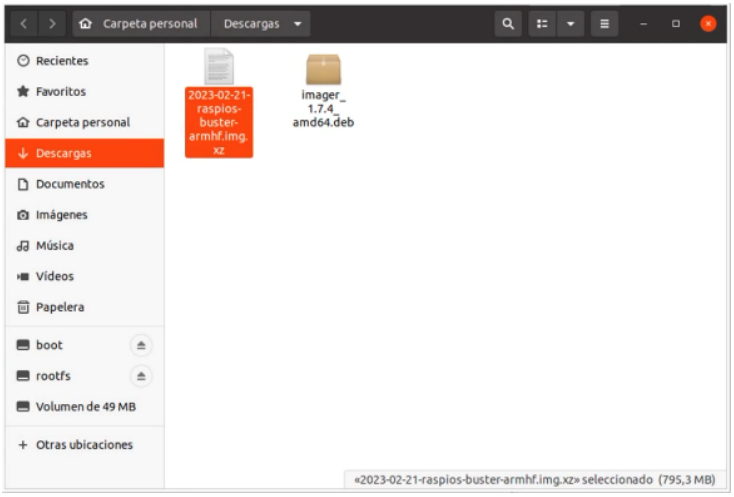
- Raspberry Pi OS (Legacy) with desktop.
- Raspberry Pi OS Lite (Legacy).

Para este proyecto y para facilitar en la medida de lo posible, se realiza la descarga de la versión que se indica en la captura superior con el botón seleccionado en color granate, dicha versión es:

Raspberry Pi OS (Legacy) with desktop
Release date: February 21st 2023



Descargado el fichero del S.O., en este caso se trata de Raspberry Pi OS (Legacy) with desktop, se pulsará en el icono de la carpeta que aparece en la ventana superior derecha del navegador.

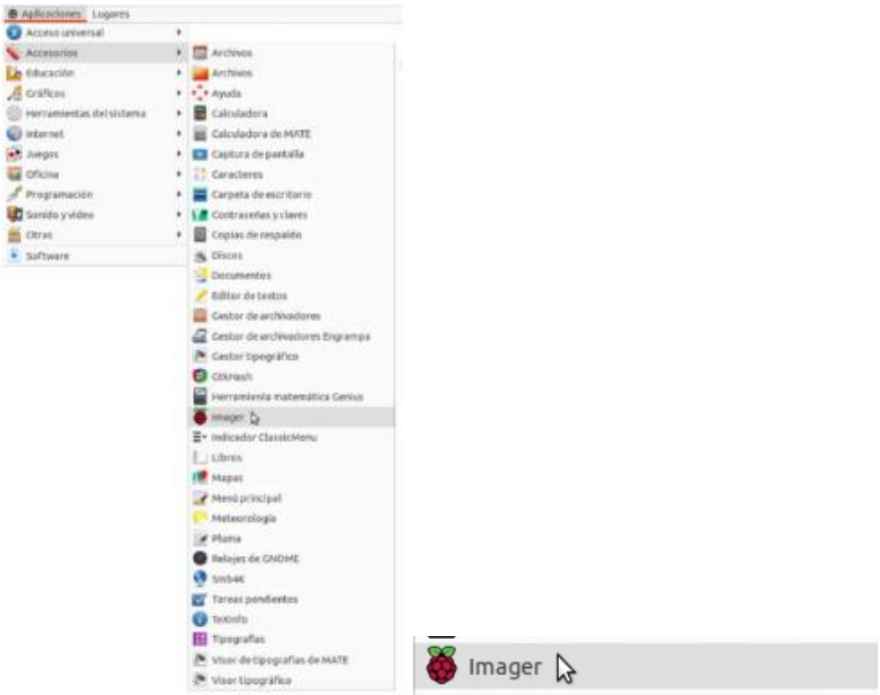


En la ubicación de la descarga, carpeta Descargas, como se puede observar en la ventana de la captura superior, se habrá descargado el fichero 2023-02-21-raspios-buster-armhf.img.xz.

Una vez descomprimido el fichero, se tendrá ahora el fichero: 2023-02-21-raspios-buster-armhf.img

Se ha comprobado que el programa Raspberry Pi Imager, es capaz de manejar la imagen del S.O. descargado incluso sin su descompresión, por lo que no se descomprime.

Preparación e Instalación del S.O. en la tarjeta microSD.



Este proceso se realiza en una distribución de Linux siendo esta Ubuntu, aunque se ha comprobado que se puede hacer en otras distribuciones donde se puede instalar la aplicación Imager.

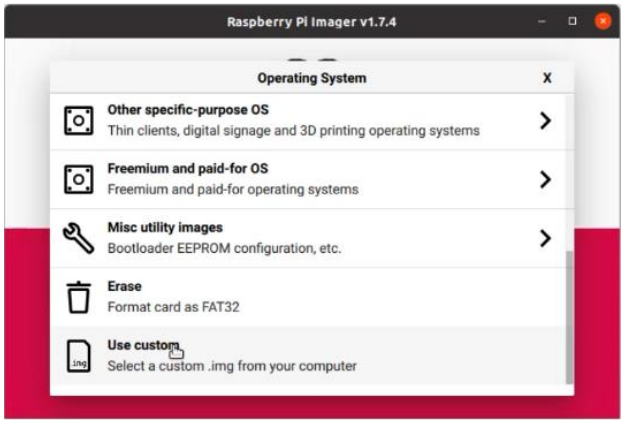
Se pulsará sobre el menú superior izquierdo Aplicaciones \ Accesorios \ dentro del menú Accesorios, se pulsará con el botón izquierdo del ratón sobre Imager.



Llegado a este punto, en el que tenemos descargada la imagen del S.O. a instalar en la tarjeta de memoria microSD, habrá que tener introducida o introducir la tarjeta en el lector de tarjetas o primero en el adaptador y posteriormente en el lector de tarjetas microSD.

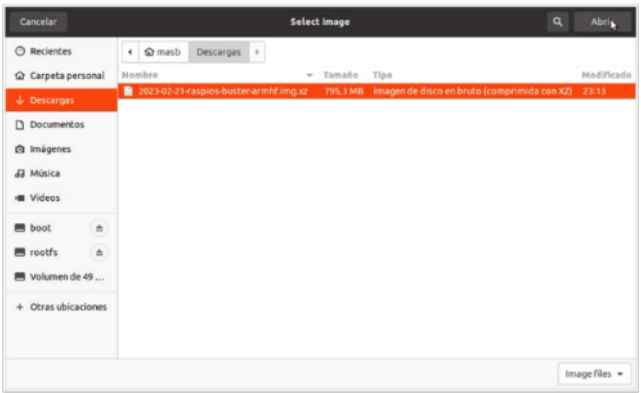


Dentro de la aplicación, se pulsará sobre CHOOSE OS, para seleccionar el S.O. descargado con anterioridad.



Anteriormente, se mencionó que para la realización de este proyecto, se elige una versión en concreto del S.O., por lo que habrá que deslizar la barra de deslizamiento situada en el lateral derecho hacia abajo, hasta encontrar la opción inferior Use custom.

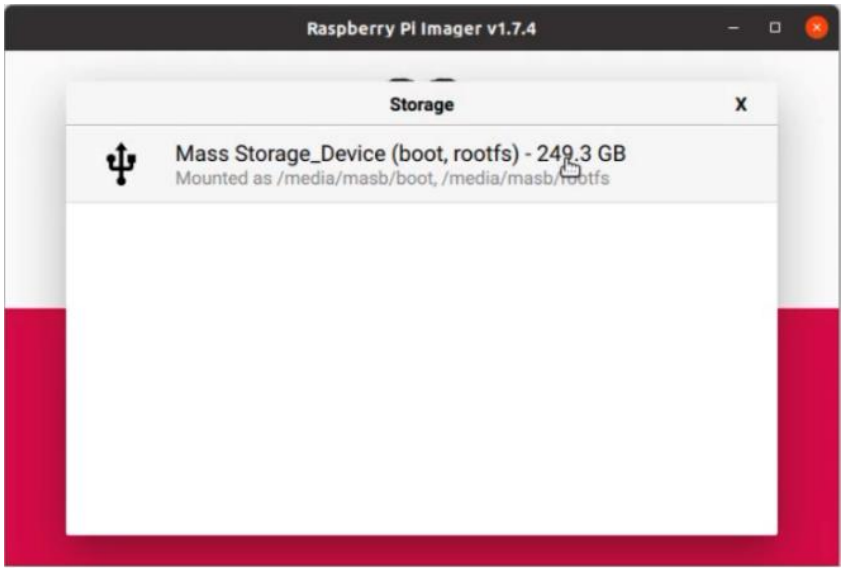
Habiendo pulsado sobre la opción Use custom, aparecerá un asistente para poder localizar el fichero descargado anteriormente del S.O., en este ejemplo se descargó en la carpeta Descargas, concretamente el fichero descargado es el 2023-02-21-raspios-buster-armhf.img.xz



Se seleccionará el fichero en cuestión, en este caso el fichero 2023-02-21-raspios-buster-armhf.img.xz y se pulsará sobre el botón superior derecho Abrir.

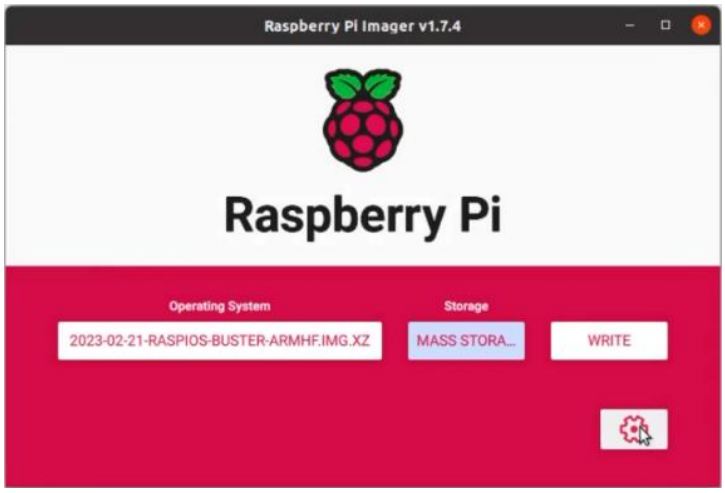


En este momento, si no se tenía insertada la tarjeta microSD, habrá que insertarla en el adaptador y posteriormente en el lector de tarjetas, con la tarjeta microSD introducida en el adaptador, se insertará en el lector para su preparación, en este momento al pulsar sobre: CHOOSE STO…, ya tendría que estar introducida en caso contrario se introducirá antes de pulsar sobre: CHOOSE STO…

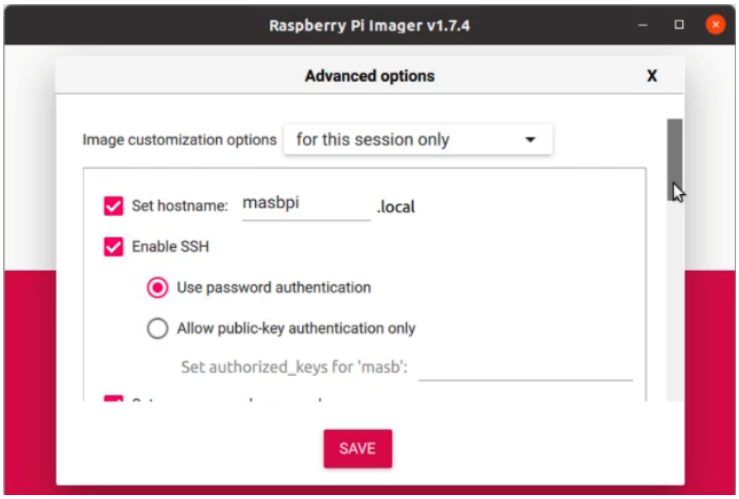


Introducida la tarjeta de memoria microSD y detectada por la aplicación, al pulsar sobre: CHOOSE STO…, se nos mostrara la tarjeta disponible, como se muestra en la ventana de la captura superior.

En la ventana que se muestra, se informa que se tiene montada una tarjeta de memoria /media/masb/boot, montada en: /media/masb/…, se seleccionara, pulsando sobre ella.



Ya se podría pulsar sobre el botón WRITE, para comenzar el proceso, sin embargo, si se quiere personalizar aún más la instalación, se podrá pulsar sobre el icono con aspecto de rueda dentada situado en la parte inferior derecha: .



En este proyecto se explican si no todas, algunas de las opciones que podemos personalizar, para ello se pulsa sobre el icono: .

Se podrá seleccionar para que sesión se configuran estas opciones, en este caso se deja seleccionada la configuración para solo esta sesión, en la opción superior Image customization Options: for this sesión only.

Como se puede apreciar en la ventana de la captura superior, se podrá modificar el nombre del host, habilitando la opción Set hostname, nombre que se le dará al equipo, en este caso a la Raspberry Pi.

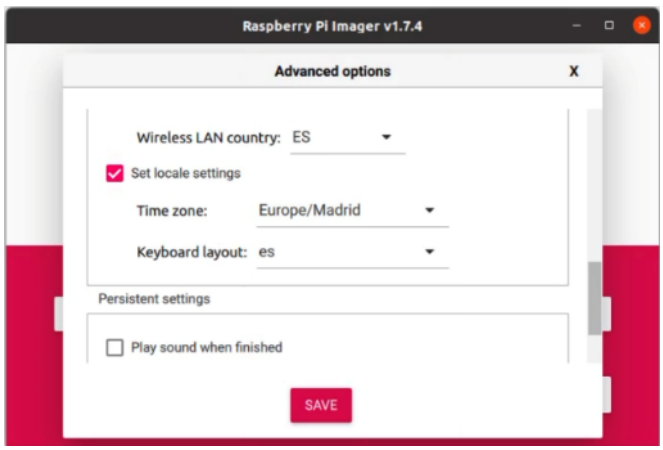
Al marcar la opción Enable SSH, se habilitará el acceso por SSH, seleccionando dicho acceso a través del uso de autenticación por contraseña o con llave pública.

Rellenados o modificados los campos anteriores como se necesiten, se podrá deslizar la barra de deslizamiento lateral derecha para continuar con las modificaciones.



En este caso se podrá cambiar el nombre del usuario por defecto, **(usuario que será root, superusuario, por lo que se tendrá que recordar la contraseña que se facilite)**.

Como se aprecia, se podrá dejar configurados los datos de la red wireless en caso de que se encuentren autorrellenados los apartados SSID y Password rellenos o se podrán colocar los valores que correspondan.



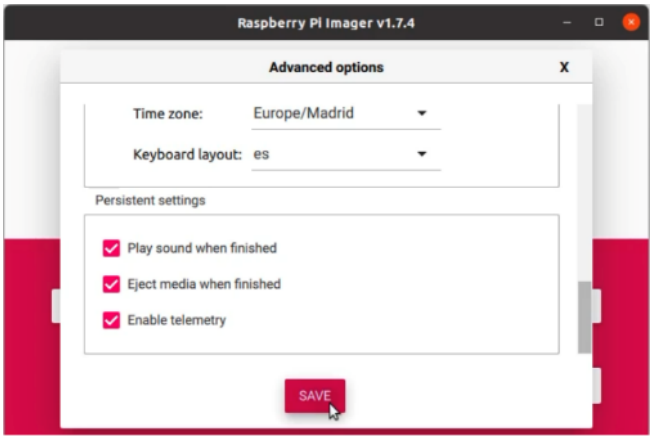
Deslizando más la barra de deslizamiento ubicada en el lateral derecho.

Se podrá indicar la localización de la ubicación WIFI opción Wireless LAN country.

Acto seguido, al seleccionar la opción: Set locale settings, si no se encuentra la zona a la que se pertenece se podrá seleccionar.

En este caso se modifican las opciones:

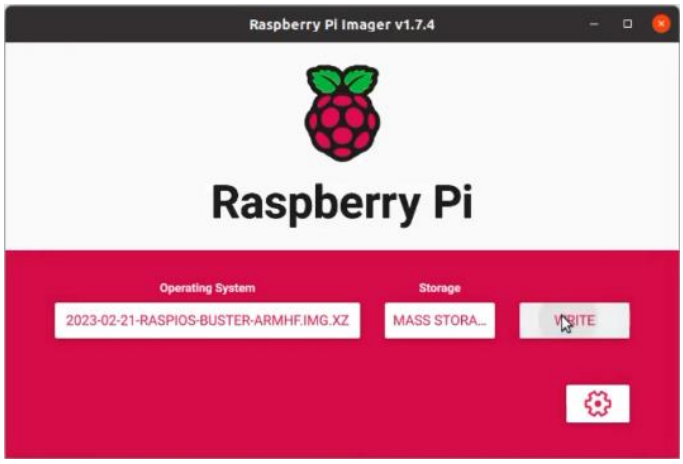
- Time Zone (Zona horaria): Europe/Madrid
- keyboard layoud (Diseño del teclado): es

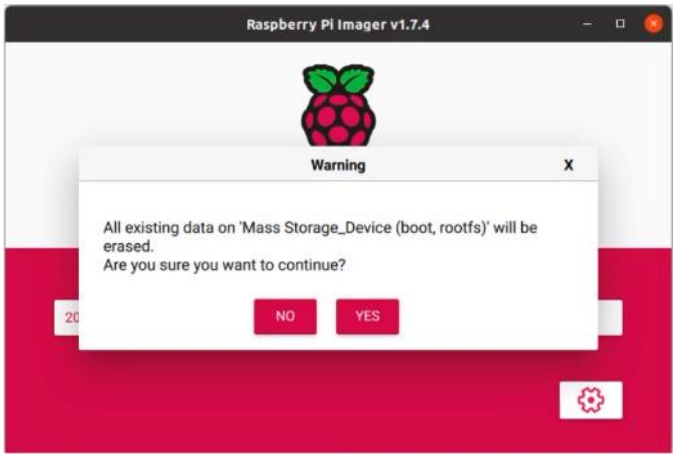


Modificadas las opciones como se necesiten, se pulsará sobre el botón SAVE.



Terminadas las modificaciones, se podrá pulsar sobre el botón: WRITE, para comenzar la instalación del S.O. en la tarjeta de memoria microSD.





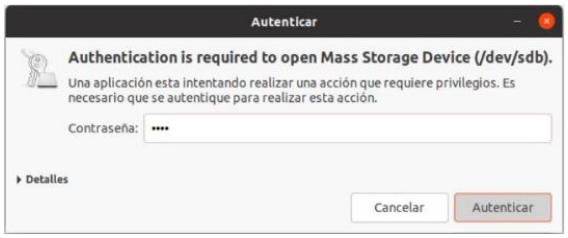
En caso de aparecer la pregunta:

“All existing data on ‘Mass Storage_Device (boot, rootfs)’ will be erased. Are you sure you want to continue?”

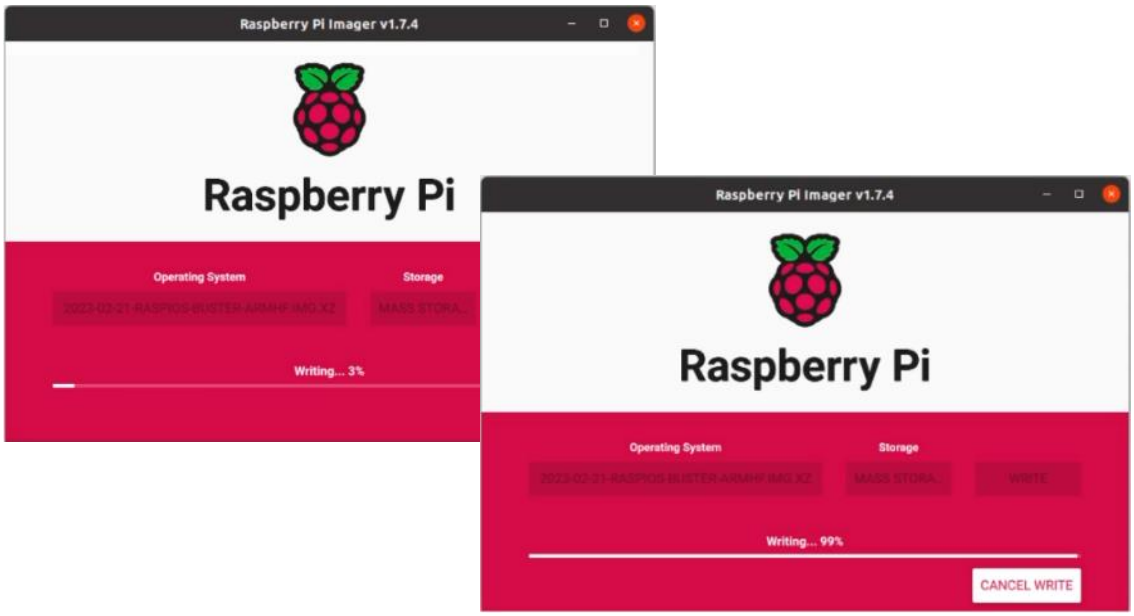
“Se borrarán todos los datos existentes en ‘Mass Storage_Device (boot, rootfs)’. ¿Está seguro de que desea continuar?”

Si se está Seguro de que la tarjeta de memoria introducida es la correcta, se podrá proceder a pulsar sobre YES.

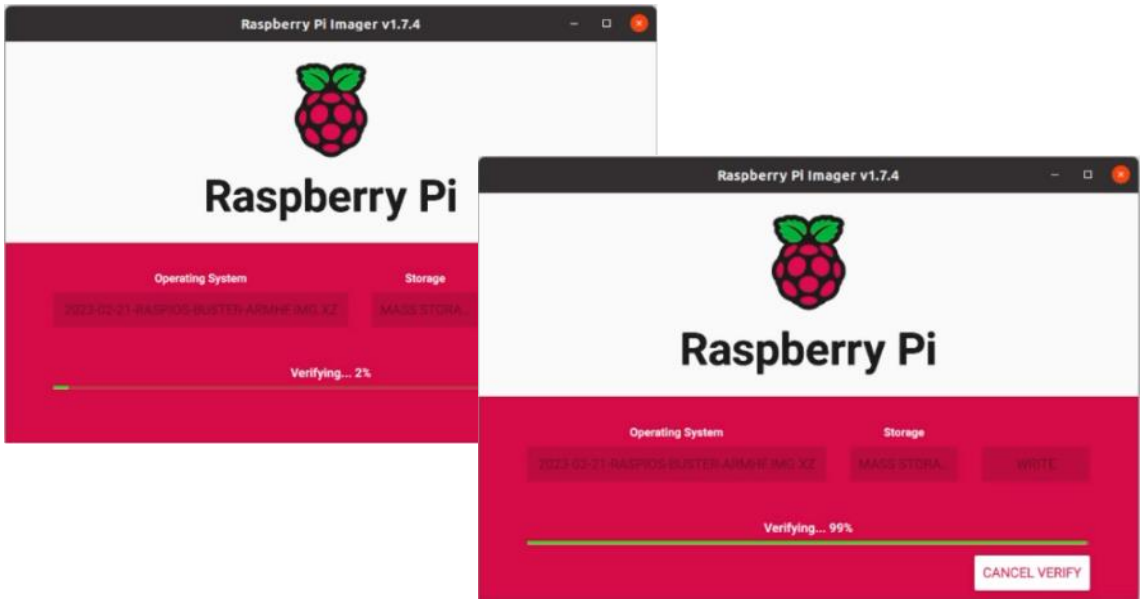




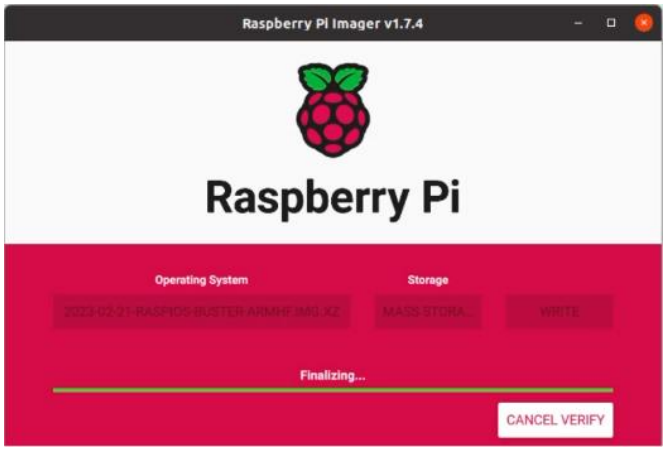
Dependiendo como se encuentre configurado el S.O. que se esté utilizando, para la creación, puede que nos aparezca la ventana de la captura superior solicitando las credenciales de un usuario con permisos, habrá que proporcionar las credenciales de un usuario con permisos, tras lo que se pulsara el botón inferior derecho Autenticar.

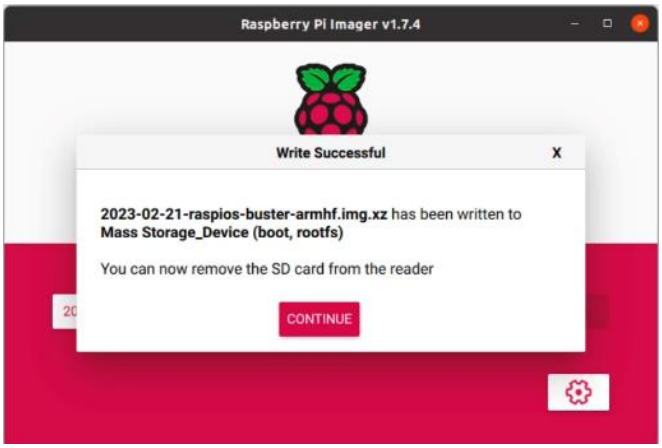


Comenzando la preparación para la escritura en la tarjeta y la escritura propiamente dicha.

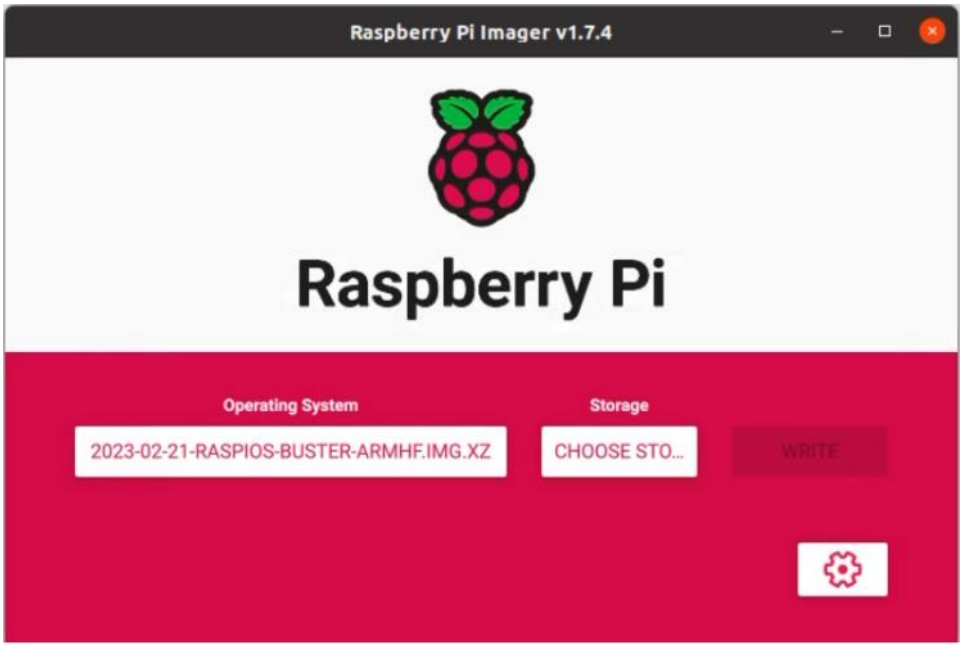


Finalizada la escritura, comienza el proceso de verificación, el cual se podrá detener pulsando sobre CANCEL VERIFY.





Terminado el proceso, se podrá pulsar sobre el botón: CONTINUE.



Pudiendo cerrar la aplicación, quitando la tarjeta del lector y se podrá insertar la tarjeta microSD en la Raspberry Pi, donde se continuará más adelante ya con el primer inicio del S.O., su configuración y la instalación de todas las aplicaciones necesarias para este proyecto.

Preparación en Sistema Operativo Windows.

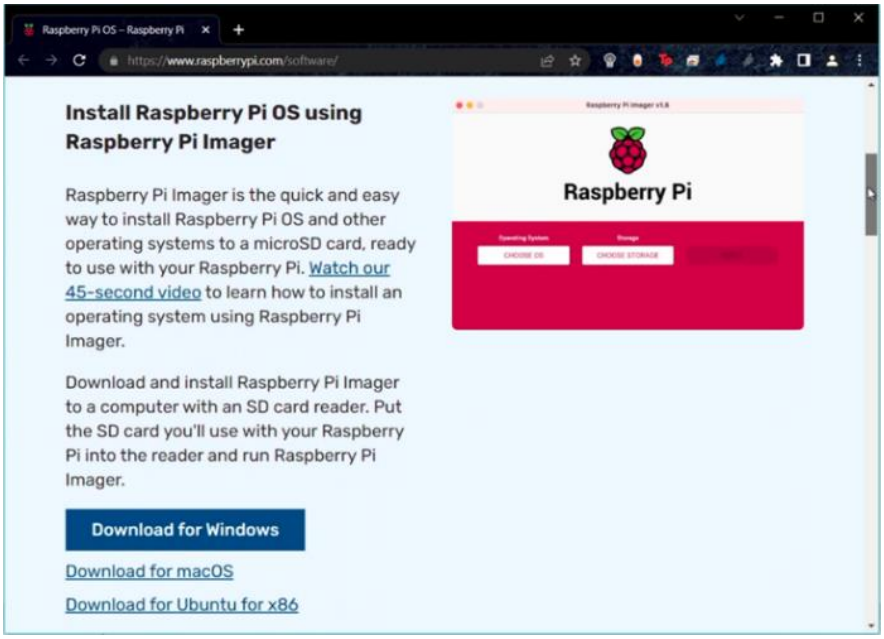
Descarga e instalación de la aplicación Raspberry Pi Imager.

Para finalizar esta parte de la explicación, se hará con el S.O. Windows, como en las anteriores explicaciones se tendrá que descargar e instalar la aplicación Raspberry Pi Imager, pudiendo realizar la descarga desde la WEB oficial.

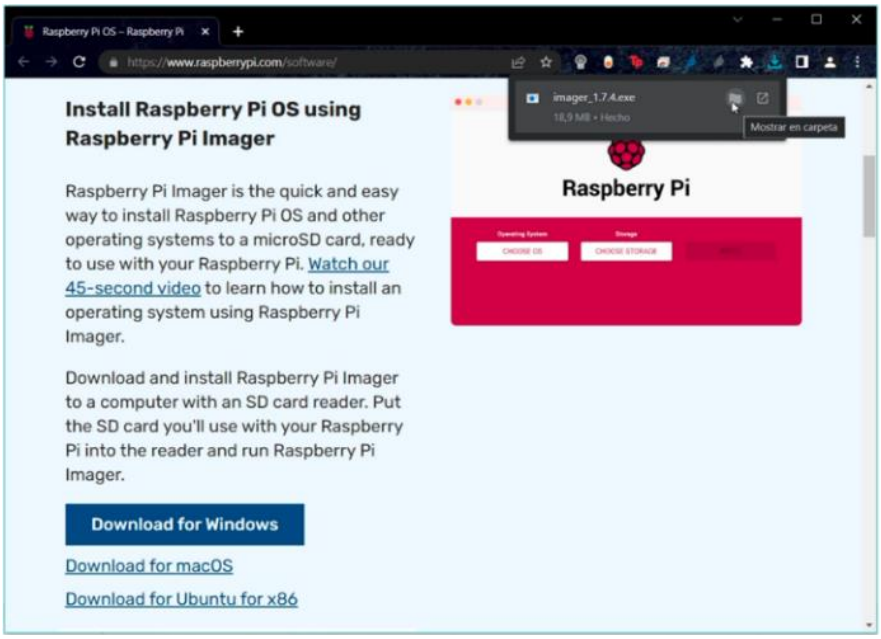
URL. https://www.raspberrypi.com/software/

Para la realización de este proyecto junto con la documentación, se utiliza un Sistema Operativo (S.O.) en concreto, para así facilitar todo el proceso de instalación de las aplicaciones, en caso de querer, se puede utilizar la descarga y utilización de otro Sistema Operativo (S.O.), aunque en ese caso puede que a la hora de la instalación de ciertas aplicaciones no se llegue a cumplir las dependencias de instalación del paquete.

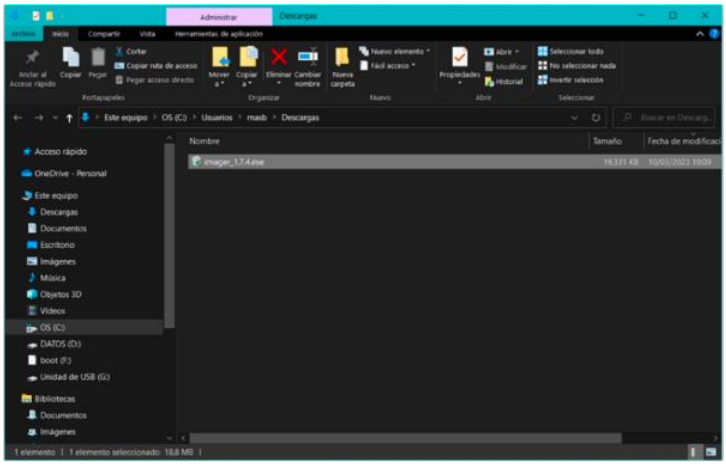




Una vez en la WEB, deslizaremos la barra de deslizamiento lateral derecha para localizar el botón: Download for “X”, siendo “X” el S.O. del que se disponga, en este último ejemplo se trata de Windows, pulsando sobre el botón: Download for Windows.

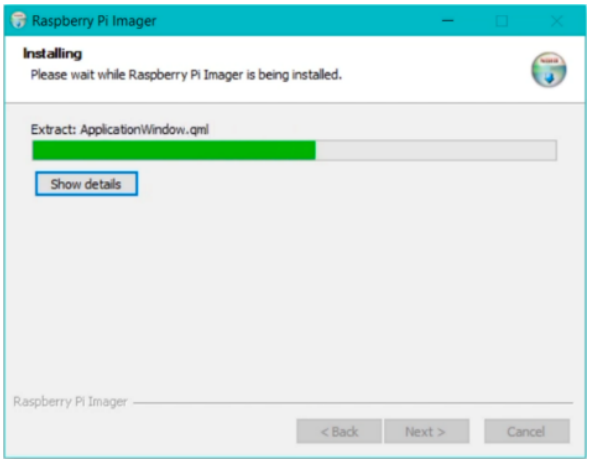


Una vez descargada la aplicación, en este caso el fichero imager_1.7.4.exe, se accederá a la ubicación donde se ha descargado el fichero pulsando sobre el icono de la carpeta “Mostrar en carpeta” en el cuadro de dialogo tras la descarga, como se puede apreciar en la captura de la ventana superior.

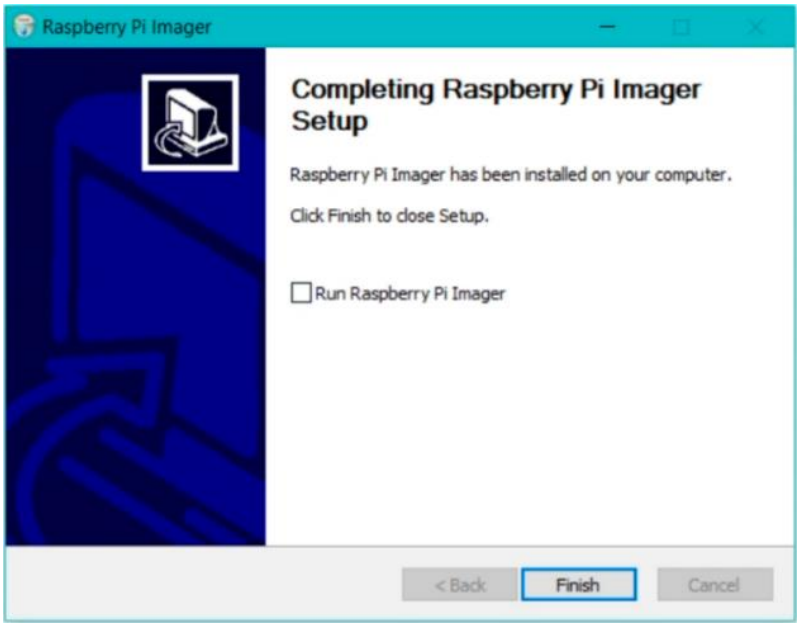


Dentro del explorador de archivos y en la ubicación de la descarga, dependiendo como se tenga configurado el navegador, en este ejemplo la descarga se realiza en la carpeta Descargas, se hará doble clic con el botón izquierdo del ratón sobre el fichero descargado imager_1.7.4.exe, en caso de aparecer la ventana Control de cuentas de usuario, se pulsará Sí.





Para comenzar el proceso de instalación, se pulsará sobre el botón Install.



Terminada la instalación, se desmarcará la opción: Run Raspberry Pi Imager, posteriormente se pulsará sobre el botón Finish.

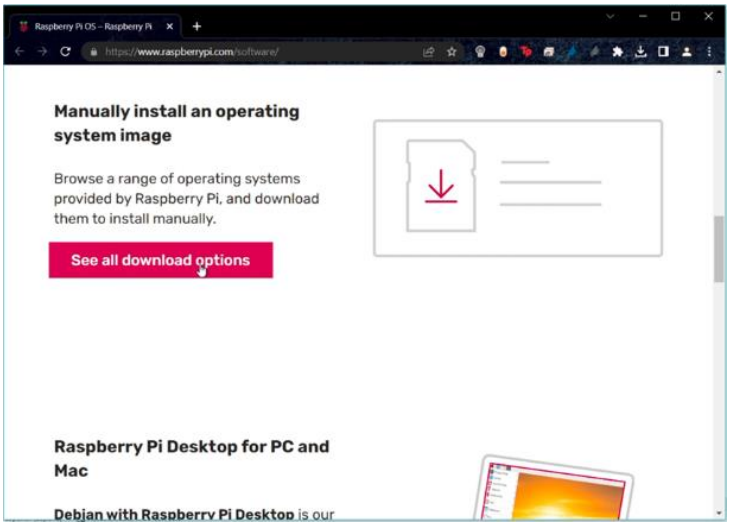
Descarga del fichero imagen del S.O. Raspberry Pi OS.

Para poder continuar y nuevamente en la WEB oficial del proyecto.

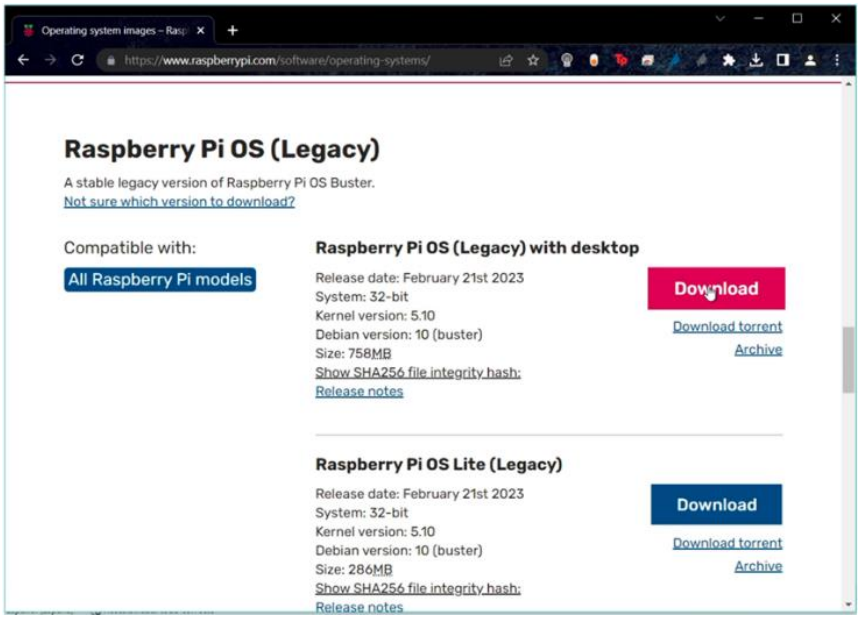
URL. https://www.raspberrypi.com/software/

Para la realización de este proyecto junto con la documentación, se utiliza un Sistema Operativo (S.O.) en concreto, facilitando todo el proceso de instalación de las aplicaciones, en caso de querer, se puede utilizar la descarga y utilización de otro Sistema Operativo (S.O.), aunque en ese caso puede que a la hora de la instalación de ciertas aplicaciones, no se llegue a cumplir las dependencias de instalación del paquete a instalar.



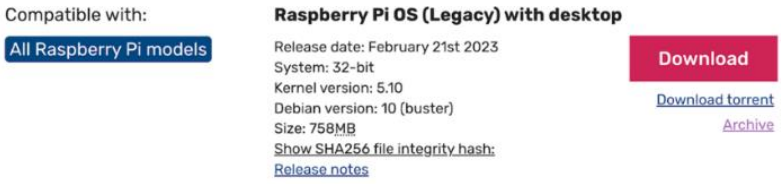


Habrá que deslizar la barra de deslizamiento ubicada en la parte lateral derecha hasta localizar el botón: See all download options, como se puede observar en la ventana de la captura superior, localizado el botón, se pulsará sobre él.



En esta nueva ventana, habrá que deslizar la barra lateral de deslizamiento hasta llegar a ver el apartado Raspberry Pi OS (Legacy), como se puede apreciar en la ventana de la captura superior.

Recordar que para la creación de este proyecto, se utiliza una versión en concreto del S.O. facilitando de esta forma la instalación de ciertas aplicaciones necesarias para la realización del mismo, cualquier persona puede utilizar otra versión del Sistema Operativo (S.O.) que se indica, aunque, en esa situación ciertas aplicaciones al proceder a su instalación puede que varie sutilmente su instalación o no se cumplan las necesidades de instalación al verificar las dependencias del paquete a instalar.

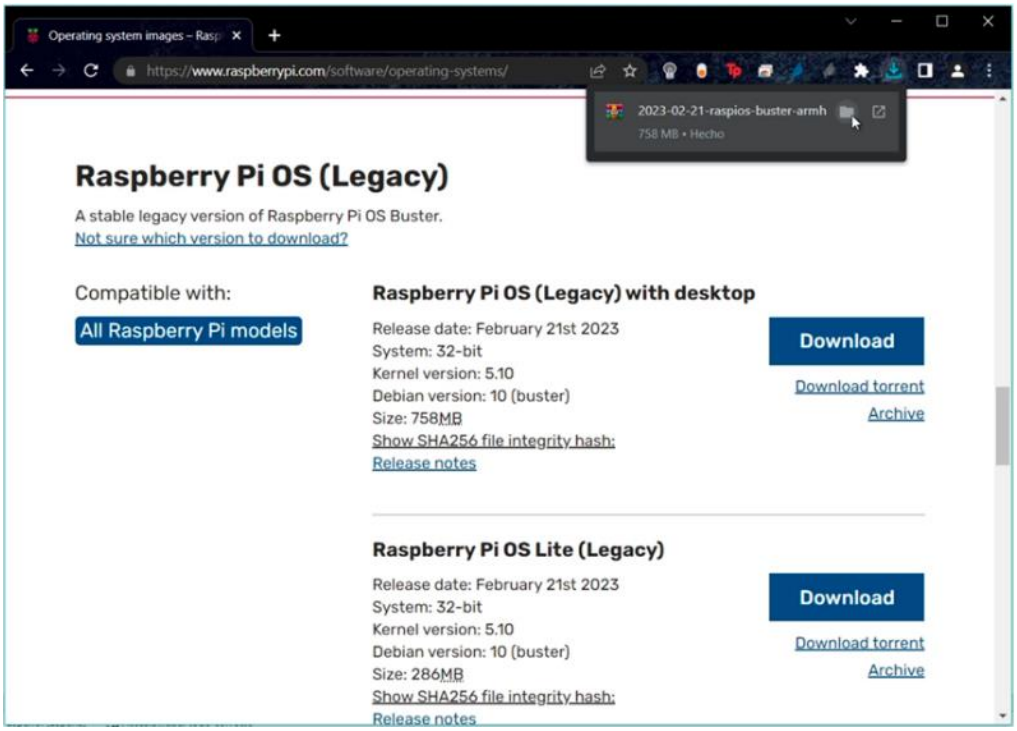


Aunque se puede descargar una de las dos versiones del Sistema Operativo S.O.

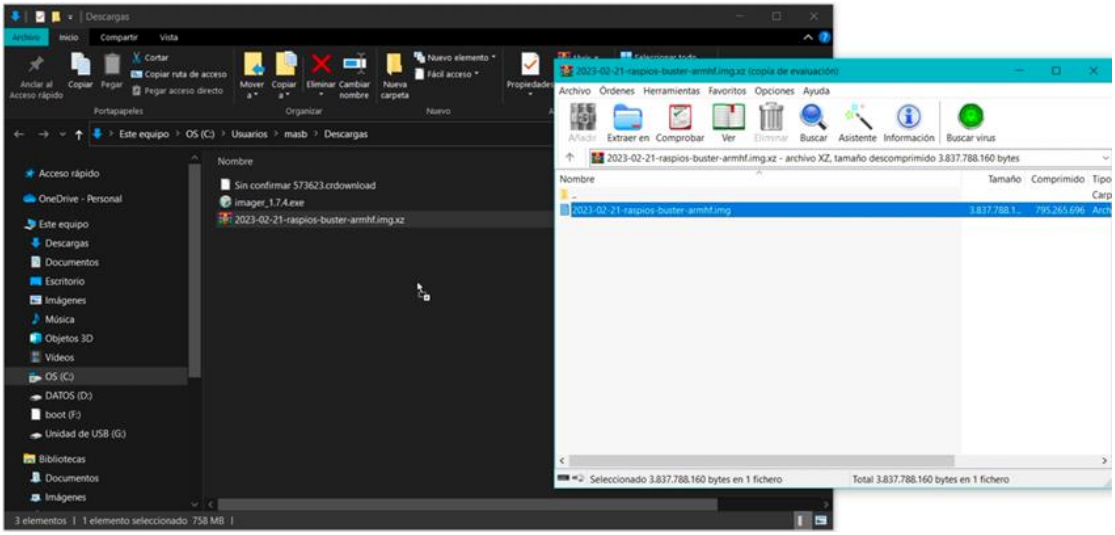
- Raspberry Pi OS (Legacy) with desktop.
- Raspberry Pi OS Lite (Legacy).

Para este proyecto, y para facilitar en la medida de lo posible, se realiza la descarga de la versión que se indica en la captura superior con el botón seleccionado en color granate, dicha versión es:

Raspberry Pi OS (Legacy) with desktop
Release date: February 21st 2023



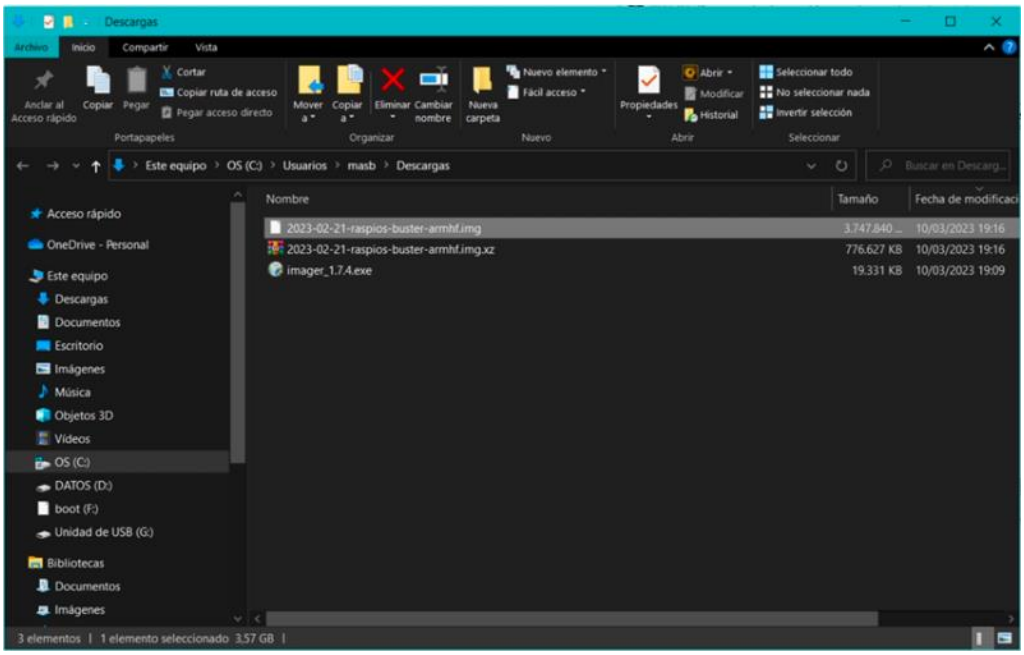
En el explorador de Internet y descargado el fichero, se accederá a la ubicación donde se ha descargado el fichero, pulsando sobre el icono de la carpeta “Mostrar en carpeta”, en el cuadro de dialogo tras la descarga, como se puede apreciar en la captura de la ventana superior.



Dentro de Descargas, se puede observar el fichero descargado 2023-02-21-raspios-buster-armhf.img.xz

Sobre el fichero 2023-02-21-raspios-buster-armhf.img.xz, se hará doble clic con el botón izquierdo del ratón para su descompresión.

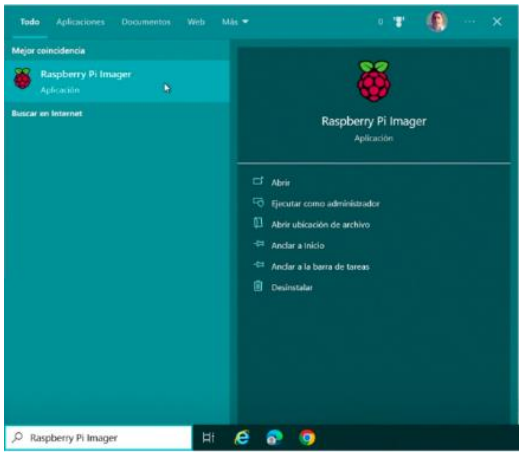




Tras la descompresión se tendrá también el fichero 2023-02-21-raspios-buster-armhf.img

Se ha comprobado que el programa Raspberry Pi Imager, es capaz de manejar la imagen del S.O. descargado incluso sin su descompresión.

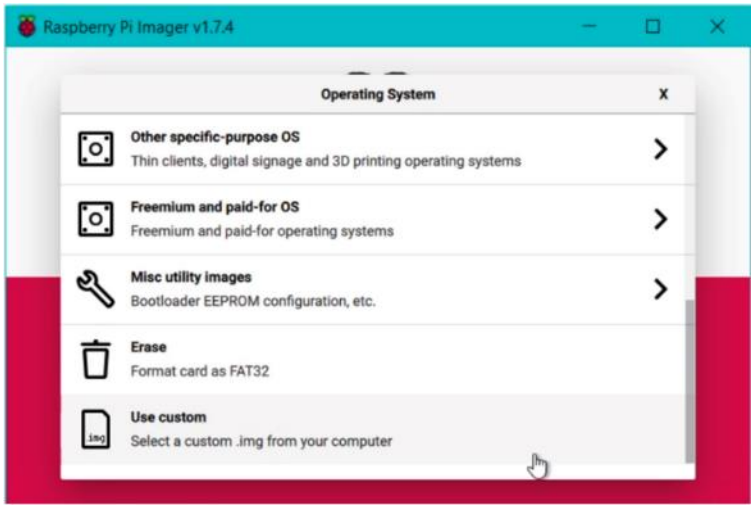
Preparación e Instalación del S.O. en la tarjeta microSD.



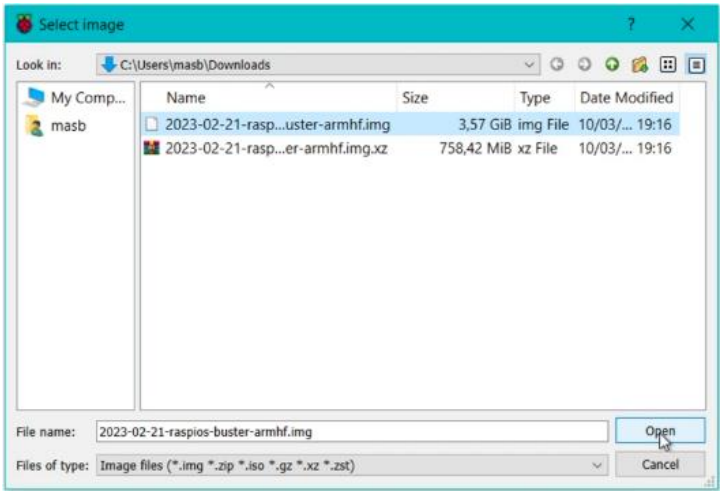
Se localizará la aplicación instalada, Raspberry Pi Imager, para abrirla pulsando sobre el icono de la misma con el botón izquierdo del ratón.



Dentro de la aplicación, se pulsará sobre: CHOOSE OS, para seleccionar el S.O. descargado con anterioridad.



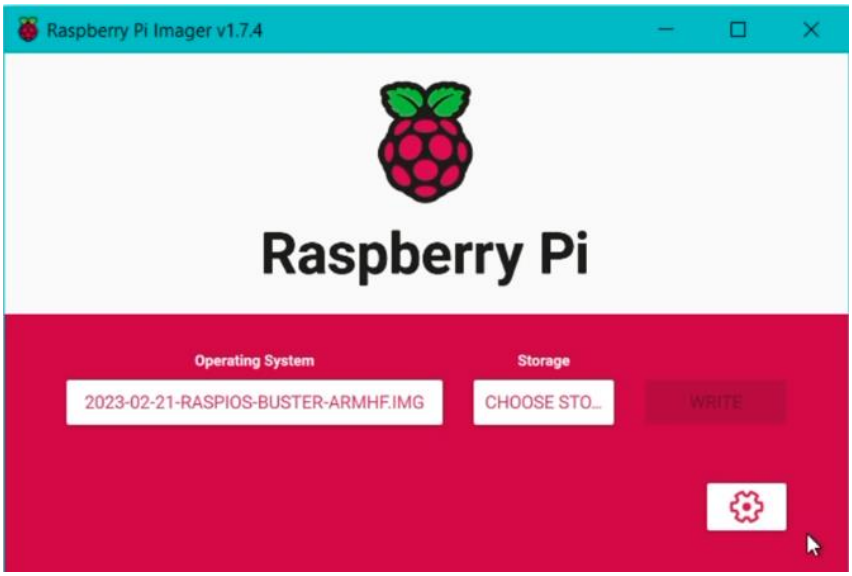
Como se mencionó, para la realización de este proyecto, se elige una versión en concreto del S.O., por lo que habrá que deslizar la barra de deslizamiento situada en el lateral derecho hacia abajo hasta encontrar la opción inferior Use custom.



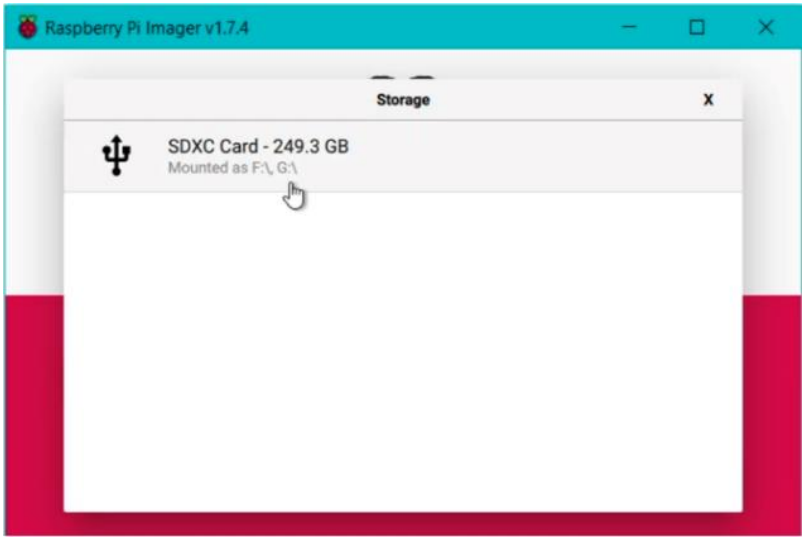
Habiendo pulsado sobre la opción Use custom, aparecerá un asistente para poder localizar el fichero descargado y descomprimido del S.O., en este ejemplo se descargó en la carpeta Descargas, concretamente el fichero descargado es el 2023-02-21-raspios-buster-armhf.img.

Se seleccionará el fichero en cuestión, en este caso el fichero 2023-02-21-raspios-buster-armhf.img y se pulsará sobre el botón Open.

Se ha podido comprobar que el programa Raspberry Pi Imager, es capaz de manejar la imagen del S.O. descargado incluso sin su descompresión.

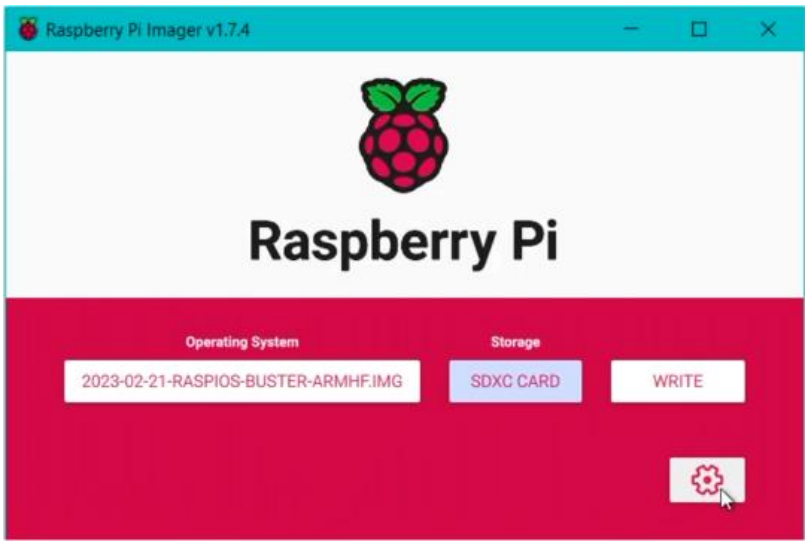


En este momento si no se ha insertado la tarjeta microSD, habrá que insertarla en el adaptador y posteriormente en el lector de tarjetas, con la tarjeta microSD introducida en el adaptador, se insertará en el lector para su preparación, al pulsar sobre CHOOSE STO…, ya tendría que estar introducida para que sea reconocida por la aplicación, en caso contrario se introducirá antes de pulsar sobre: CHOOSE STO…



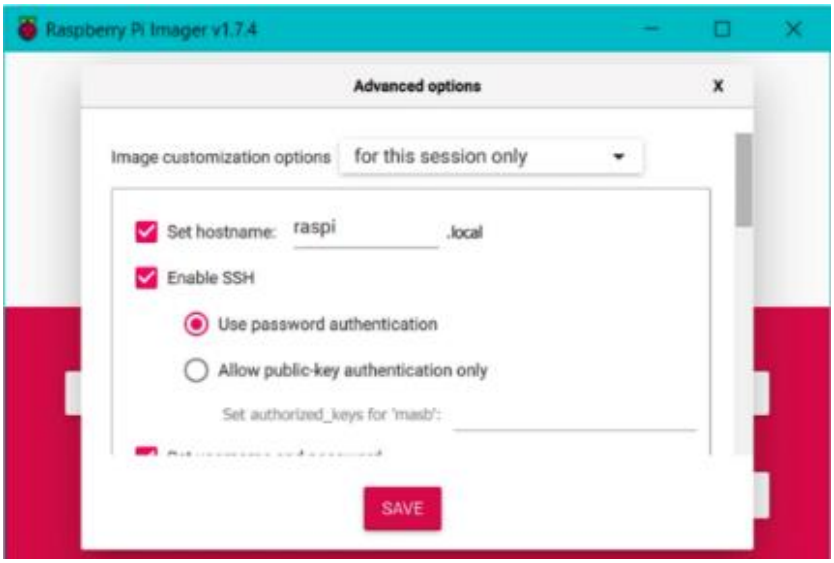
Introducida la tarjeta de memoria microSD y habiendo pulsado sobre CHOOSE STO…, se nos mostrara la tarjeta disponible, como se muestra en la ventana de la captura superior.

En la ventana que se muestra, se informa que se dispone de una tarjeta de memoria en las unidades F: y G:, se seleccionará pulsando sobre la tarjeta.



Ya se podría pulsar sobre el botón WRITE, para comenzar el proceso, sin embargo, si se quiere personalizar aún más la instalación, se podrá pulsar sobre el icono con aspecto de rueda dentada situado en la parte inferior derecha: .

En este manual se explican si no todas, algunas de las opciones que podemos personalizar, para ello se pulsa sobre el icono: .



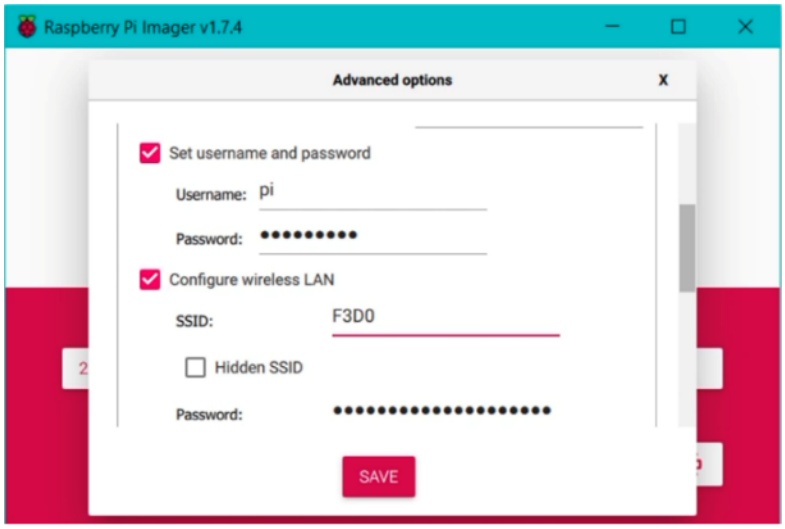
Se podrá seleccionar para que sesión se configuran estas opciones, en este caso se deja seleccionada la configuración para solo esta sesión, en la opción superior Image customization Options: for this sesión only.

Como se puede observar en la ventana de la captura superior, se podrá modificar el nombre del host, habilitando la opción Set hostname, nombre que se le dará al equipo, en este caso a la Raspberry Pi.

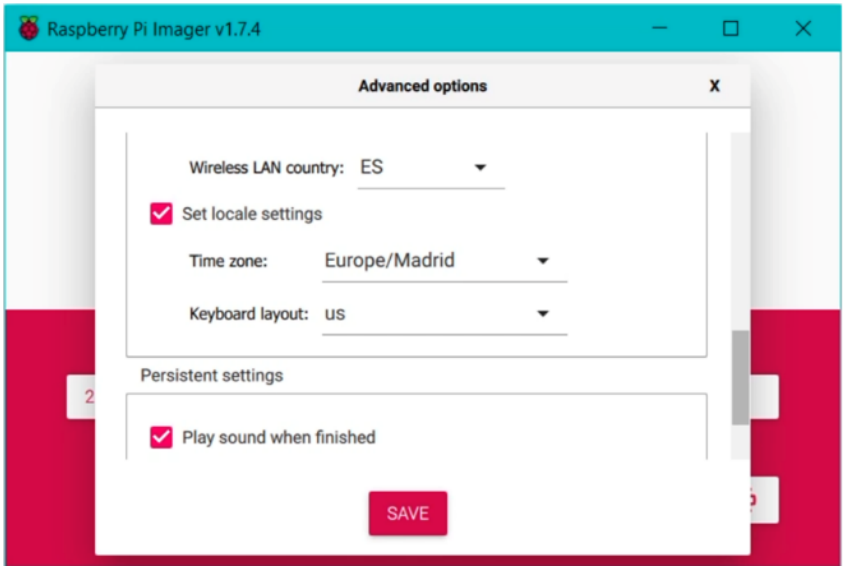
Al marcar la opción Enable SSH, se habilitará el acceso por SSH, seleccionando dicho acceso a través del uso de autenticación por contraseña o con llave pública.

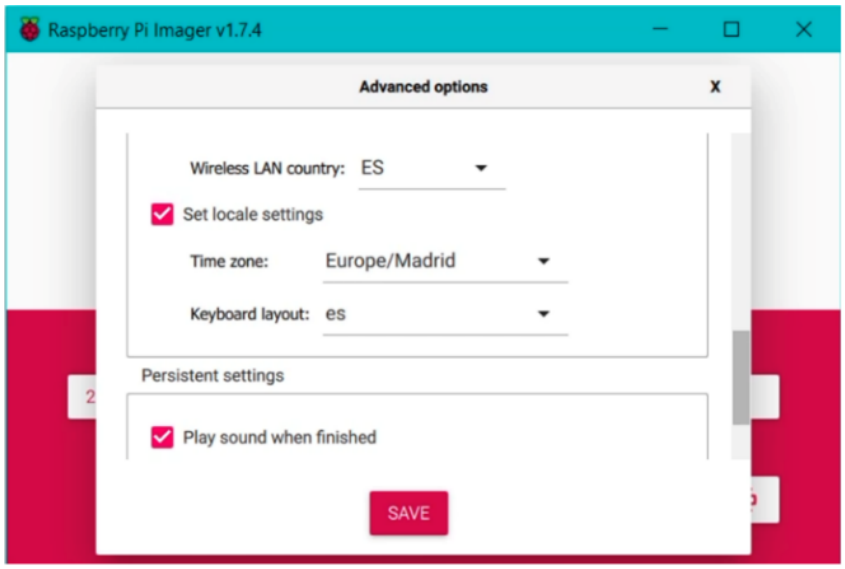
Rellenados o modificados los campos anteriores como se necesiten, se podrá deslizar la barra de deslizamiento lateral derecha para continuar con las modificaciones.

A continuación, se podrá cambiar el nombre del usuario por defecto, **(usuario que será root, superusuario, por lo que se tendrá que recordar la contraseña que se facilite)**.



Como se aprecia, se podrá configurar o se podrá dejar la configuración adquirida desde el S.O. en referencia a la configuración WIFI en la opción Configure wireless LAN.





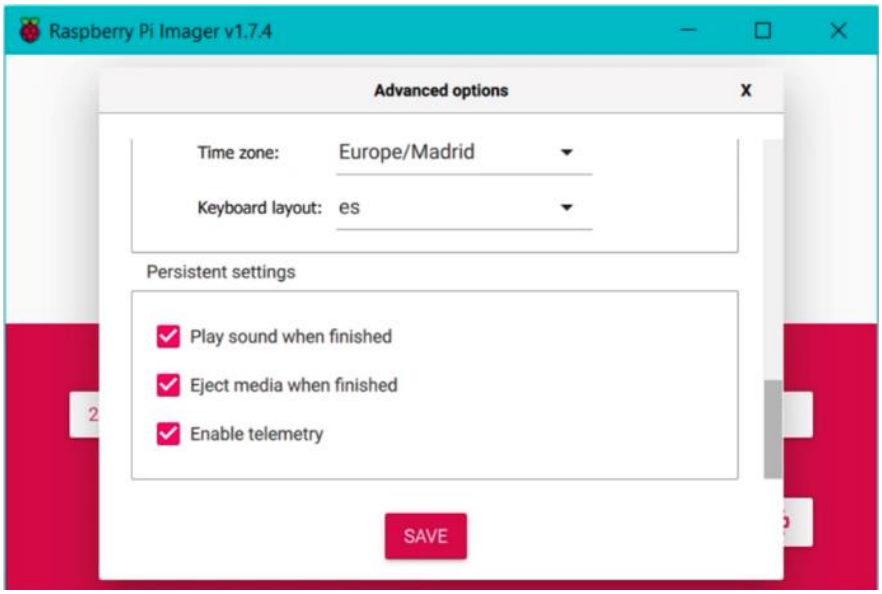
Deslizando más la barra de deslizamiento ubicada en el lateral derecho.

Se podrá indicar la localización de la ubicación WIFI en caso de no estar correctamente el valor en la opción Wireless LAN country.

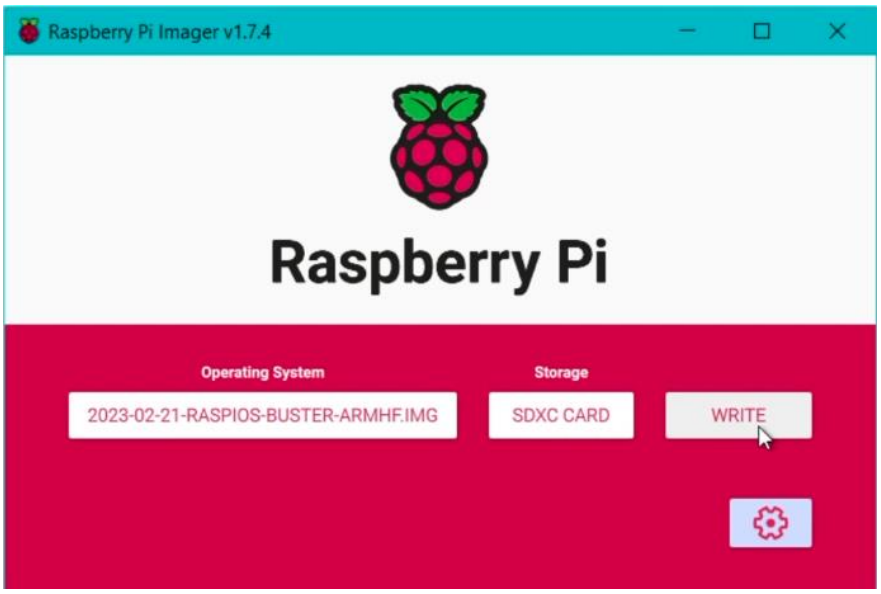
Acto seguido, al seleccionar la opción Set locale settings, si no se encuentra ya seleccionada bien la zona a la que se pertenece, se podrá modificar dichas opciones Time zone y Keyboard layout tras seleccionar la mencionada opción Set locale settings.

En este caso se modifican las opciones:

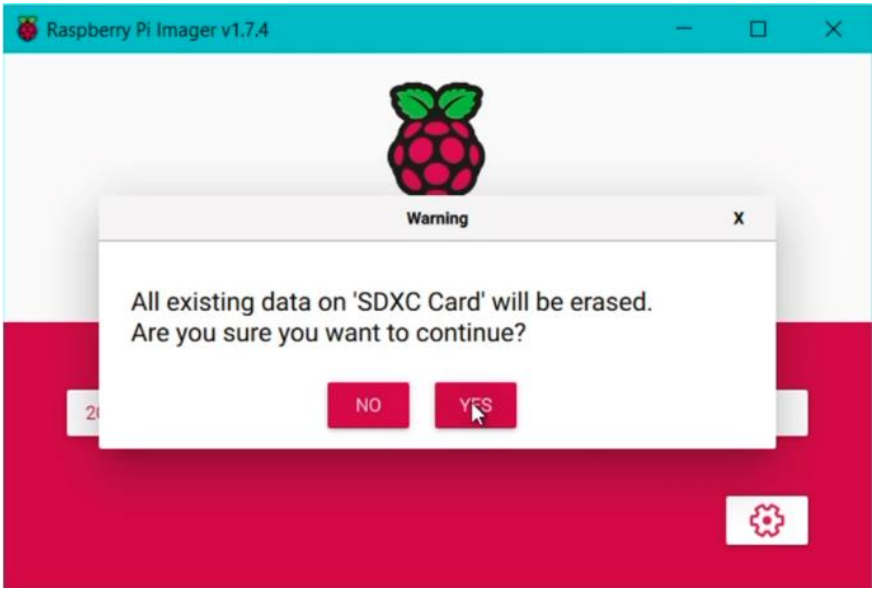
- keyboard layoud (Diseño del teclado): es
- Time Zone (Zona horaria): Europe/Madrid



Modificadas las opciones como se necesiten, se pulsará sobre el botón: SAVE.



Terminadas las modificaciones, se podrá pulsar sobre el botón: WRITE para comenzar la instalación del S.O. en la tarjeta de memoria microSD.



Al mostrarse la pregunta.

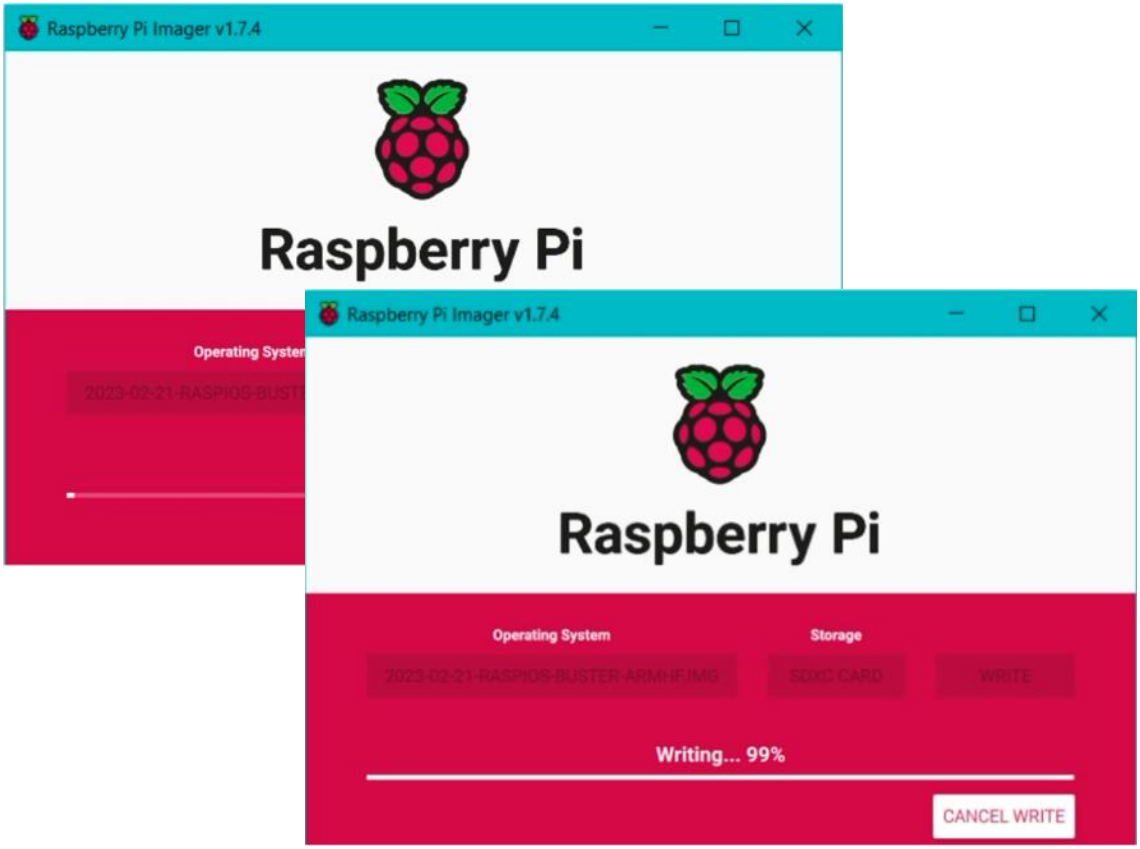
“All existing data on ‘SDXC Card’ will be erased. Are you sure you want to continue?”

“Se borrarán todos los datos existentes en ‘SDXC Card’. ¿Está seguro de que desea continuar?”

Si se está Seguro de que la tarjeta de memoria introducida es la correcta, se podrá proceder a pulsar sobre: YES.

En caso de aparecer la ventana Control de cuentas de usuario se pulsará sobre: Sí





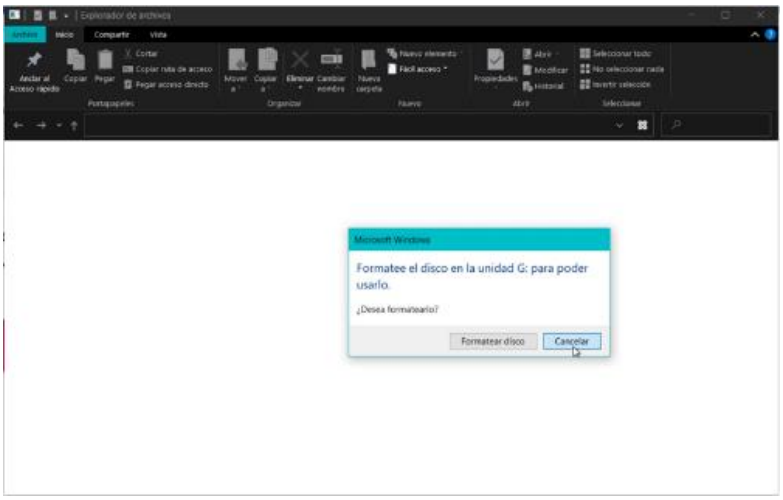


Comenzando el proceso de preparación de la tarjeta y la posterior escritura en la misma.

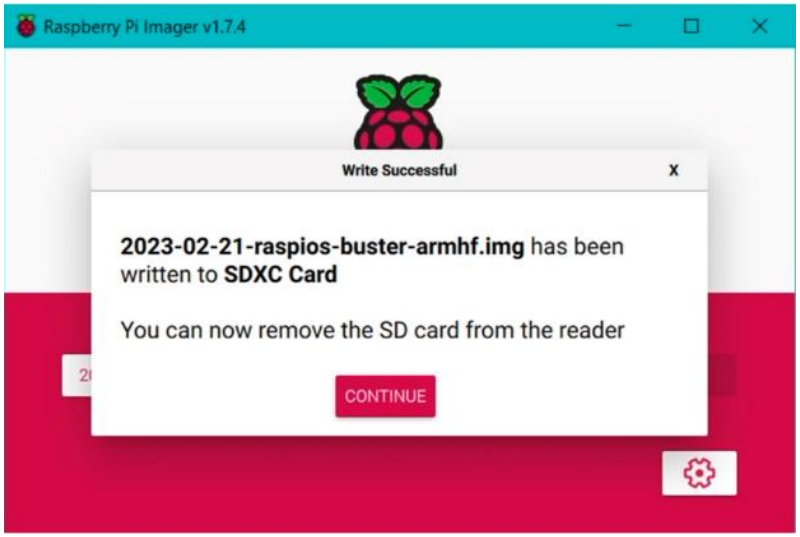
Terminada la escritura, comienza el proceso de verificación, el cual se podrá detener pulsando sobre: CANCEL VERIFY.







Antes de mostrarse el mensaje de finalización, puede que aparezcan algunas ventanas informando de que se Formatee el disco en la unidad X: (unidad X: esta unidad puede variar), para poder usarlo. ¿Desea formatearlo?, se pulsará sobre Cancelar.



Terminado el proceso, se podrá pulsar sobre el botón: CONTINUE.



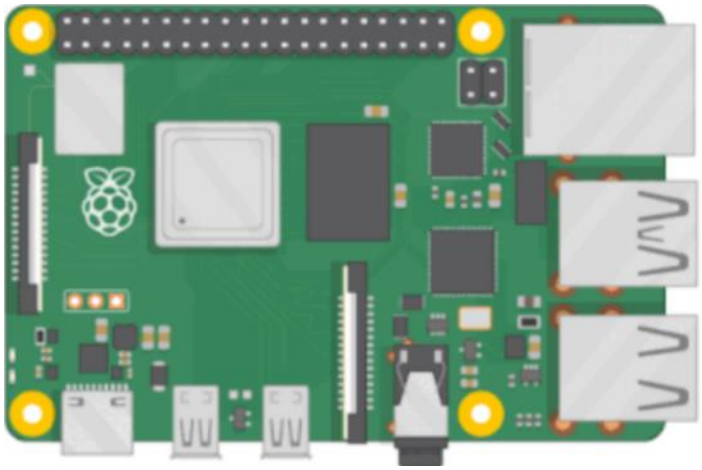
Pudiendo cerrar la aplicación, quitando la tarjeta del lector y se podrá insertar la tarjeta microSD en la Raspberry Pi, donde se continuará más adelante ya con el primer inicio del S.O. su configuración y la instalación de todas las aplicaciones necesarias para este proyecto.

Primer arranque Raspberry Pi.

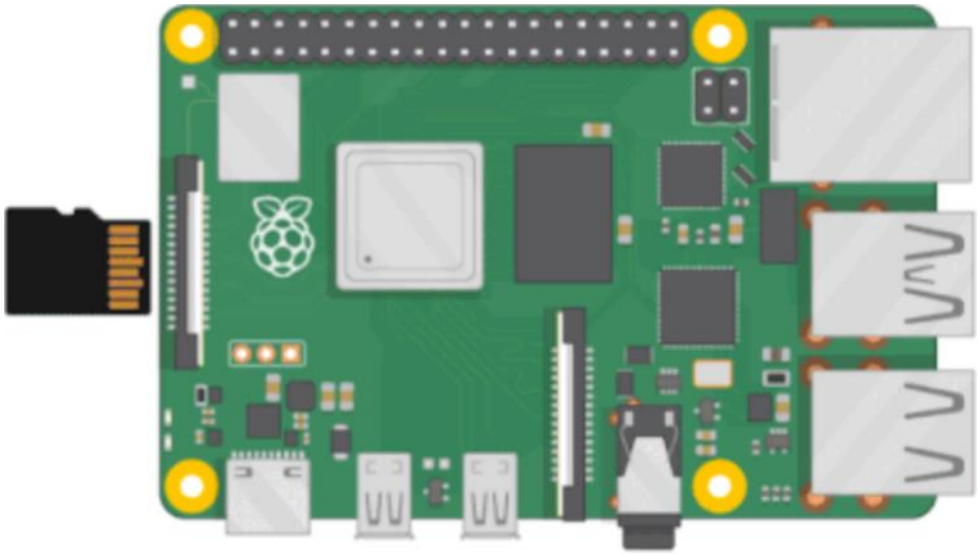
Capturas adquiridas desde la WEB oficial de documentación sobre Raspberry Pi, en la WEB.

URL. https://www.raspberrypi.org/help/

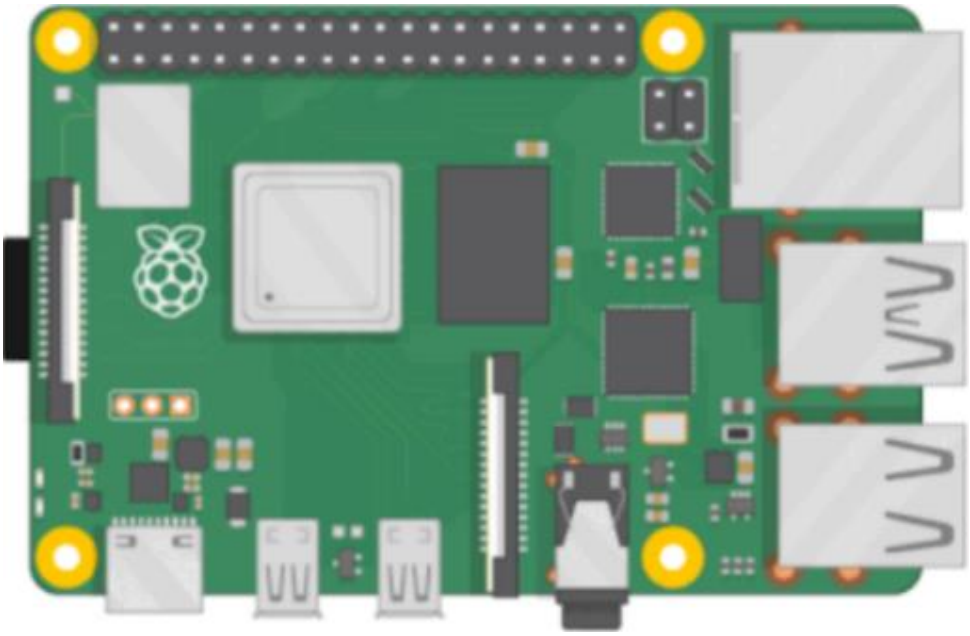
Tras haber realizado la descarga de la aplicación, como del fichero imagen del S.O. y haber preparado la tarjeta de memoria microSD, con el S.O. Raspberry Pi OS (RaspiOS).



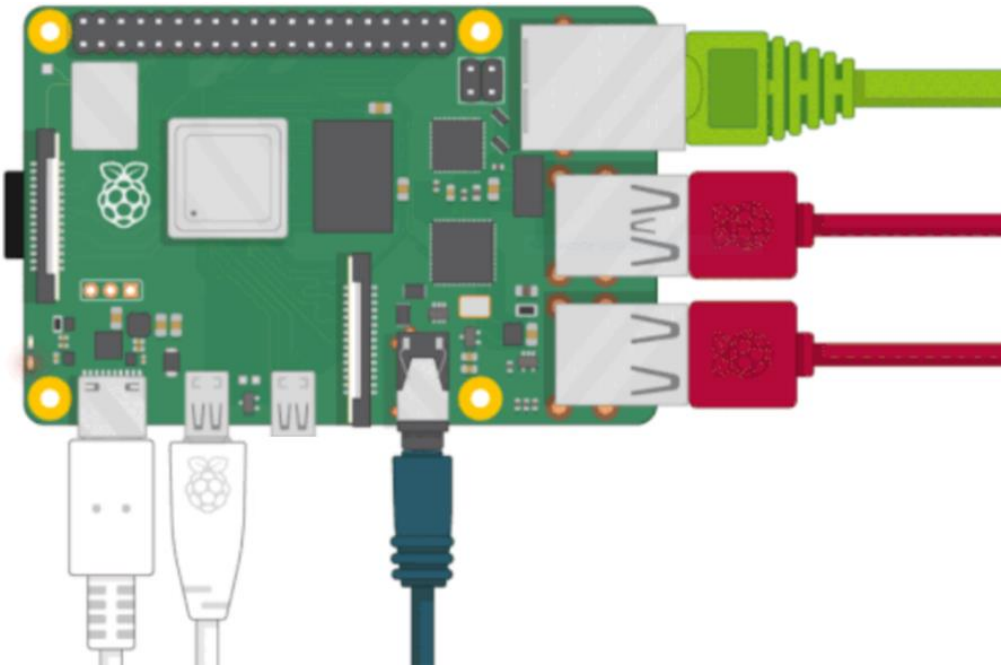
Se tendrá que introducir la tarjeta en la Raspberry Pi, para ello si no se tiene mucha práctica, como primera medida, se puede colocar todos los cables necesarios y la propia tarjeta microSD sin antes haber colocado la placa de la Raspberry Pi en la caja.



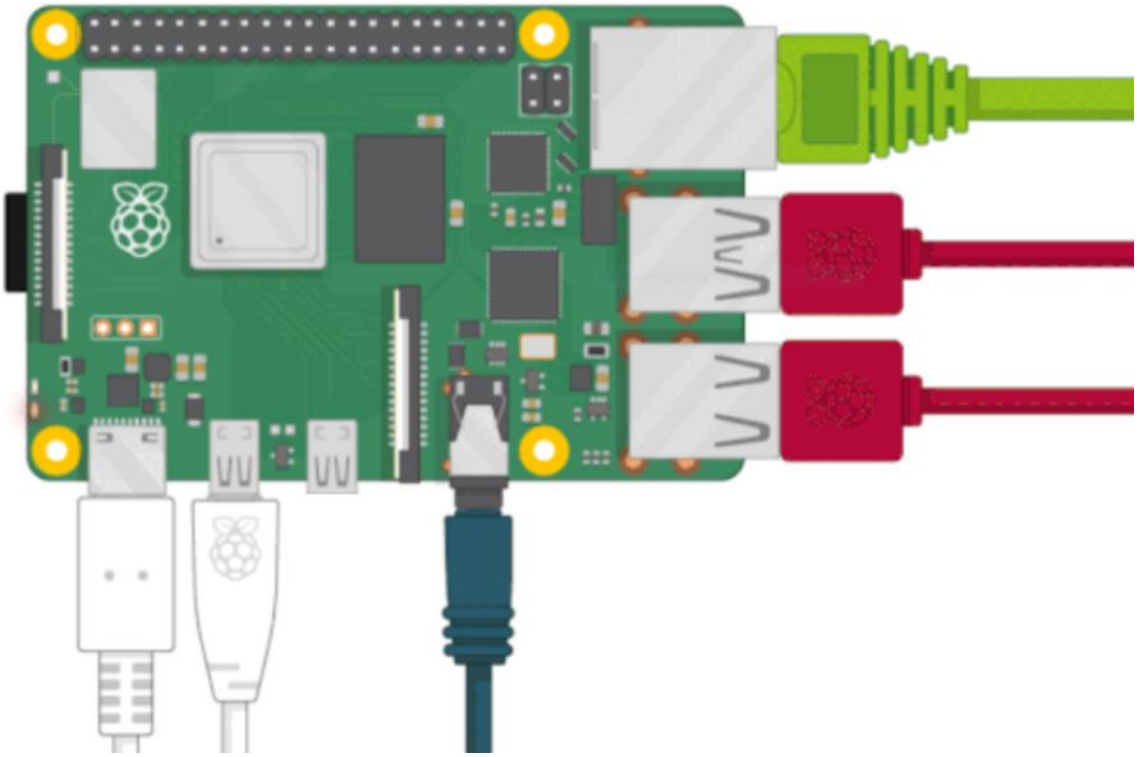
Para introducir la tarjeta microSD, como se puede observar en la ventana de la captura superior, los contactos se posicionarán hacia arriba y se introducirá la tarjeta con los contactos hacia arriba y hacia delante, como se observa en la captura de la ventana superior.



Se tendrá que tener especial cuidado para introducirla correctamente, sin forzarla, solo se puede introducir de una forma, por lo que, si no se introduce, habrá que intentarlo de otra forma, (solo se puede introducir con los contactos hacia arriba, como se muestra en las capturas de las ventanas superiores).



A continuación, se podrá conectar los cables de los dispositivos que se necesiten.



Introducida la tarjeta micro SD, se tendrá que introducir los cables de los dispositivos necesarios, según se observa en la captura de la imagen superior, (los colores y su posición pueden variar), dependiendo del modelo de Raspberry Pi que se utilice.

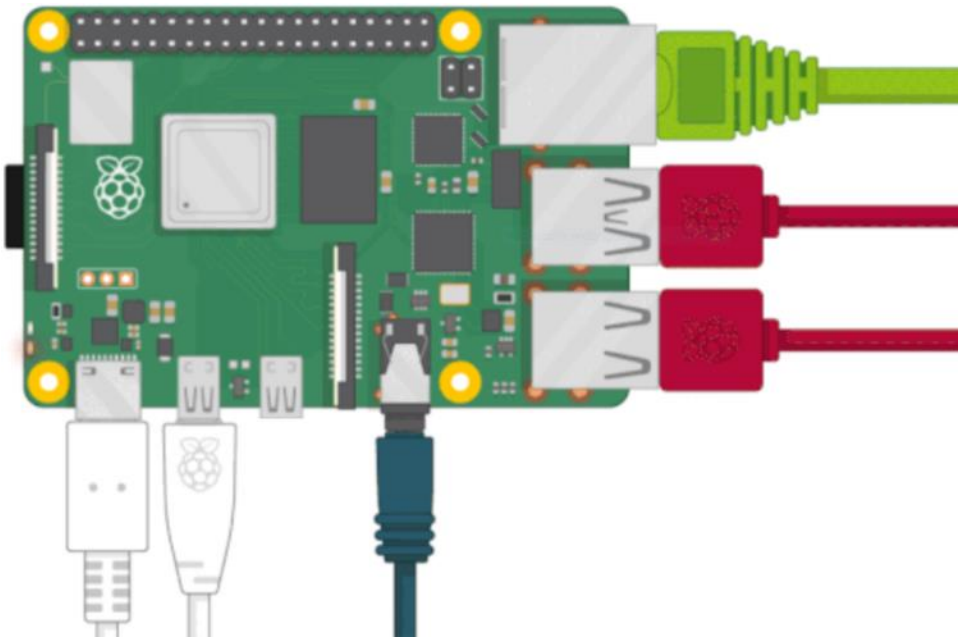
- Cable color verde claro: (conector RJ45), Cable Ethernet, en caso de conectarse a la red por WIFI no sería necesario.

- Cables de color rojo: (conectores USB), Pueden ser cables para el teclado y ratón, puede utilizarse un teclado por bluetooth por lo que se tendría que colocar el enlazador USB solamente.

- Cable color verde oscuro: Conector para audio, no necesario.

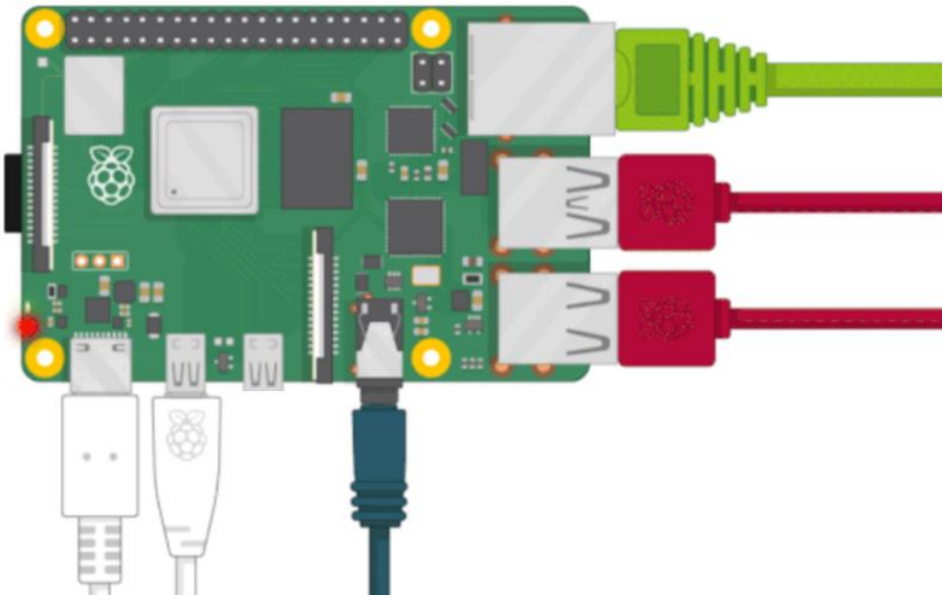
- Cables de video: Según la imagen de la captura superior, es el cable blanco a la izquierda del cable verde oscuro en la parte inferior, son dos conectores, solo es necesario uno de ellos, en caso de no disponer de pantalla integrada y ser necesario conectar un monitor externo.

- Cable alimentación eléctrica: Cable blanco (puede variar), en la captura de la imagen superior es blanco, cable inferior izquierda, el primero.

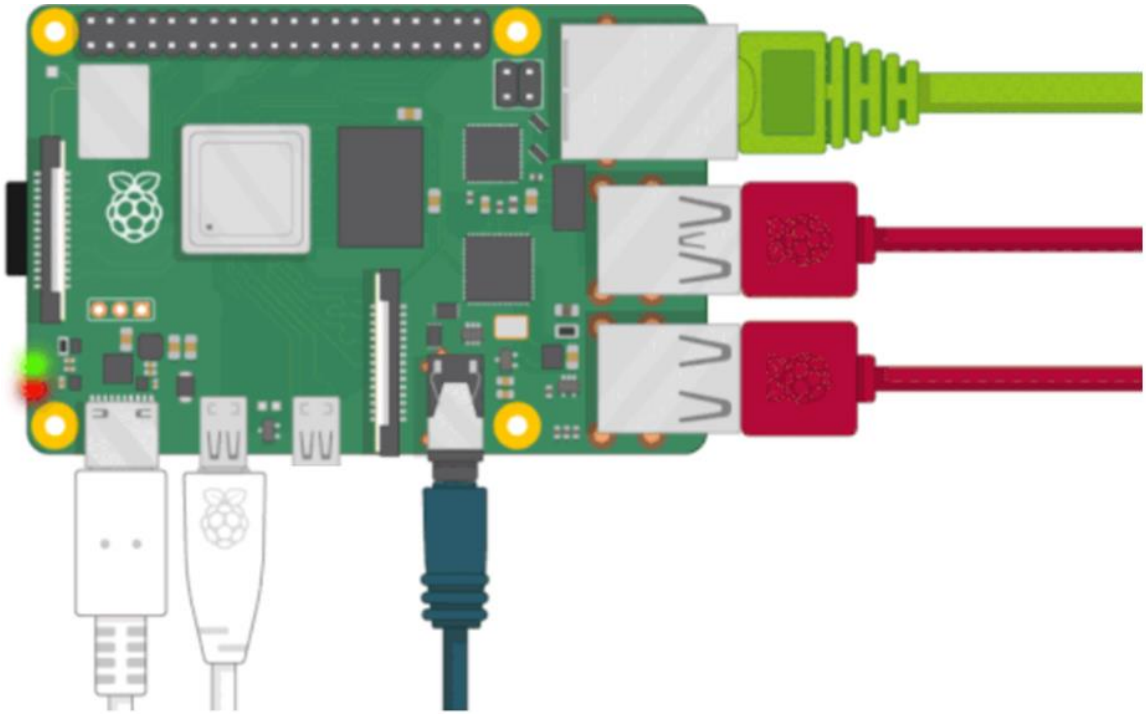


Se tendrán que conectar lo necesario para poder manipular la Raspberry Pi como, por ejemplo:

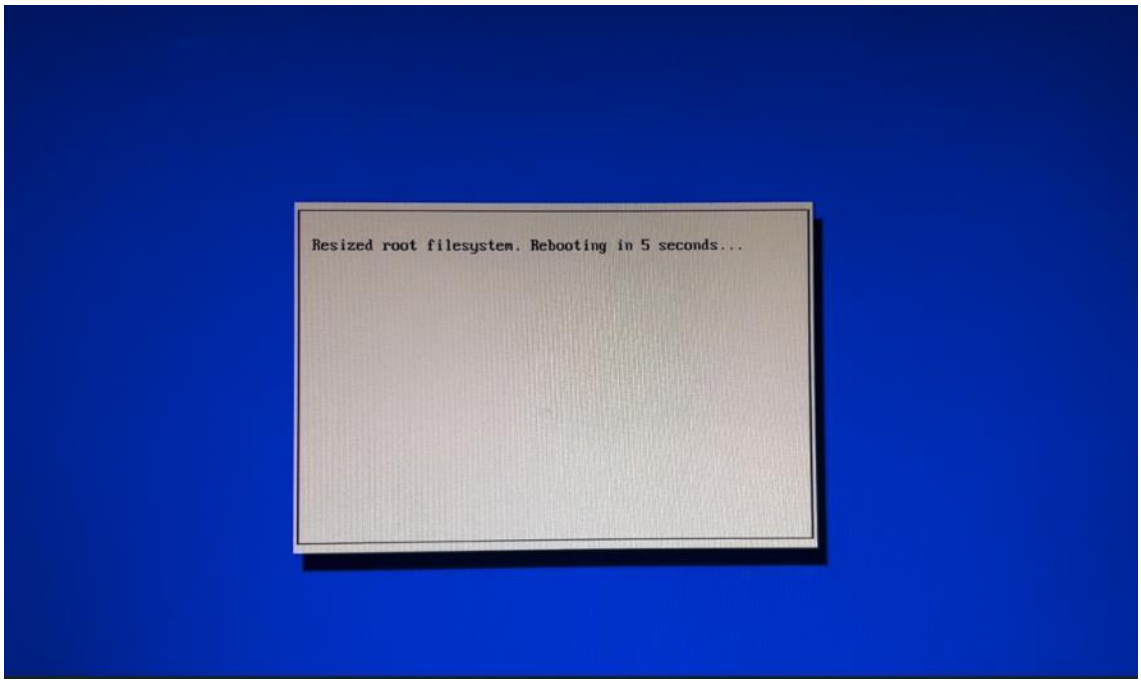
- Teclado, (tras la configuración de la Raspberry Pi no sería necesario).
- Ratón, (tras la configuración de la Raspberry Pi no sería necesario).
- Cable para conectar un monitor externo. (tras la configuración de la Raspberry Pi no sería necesario monitor externo).
- Cable de alimentación eléctrica.



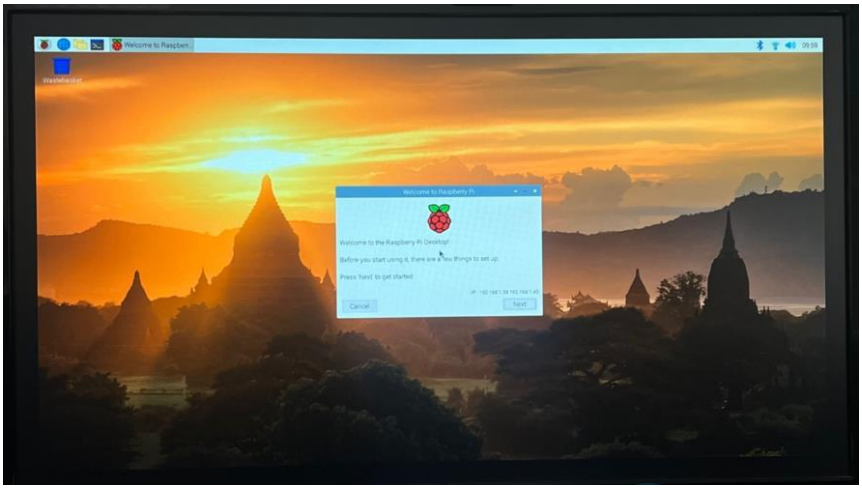
Una vez conectados los cables necesarios y conectar el cable de alimentación eléctrica, se encenderá un led de color rojo, como se puede observar en la ventana de la captura superior.



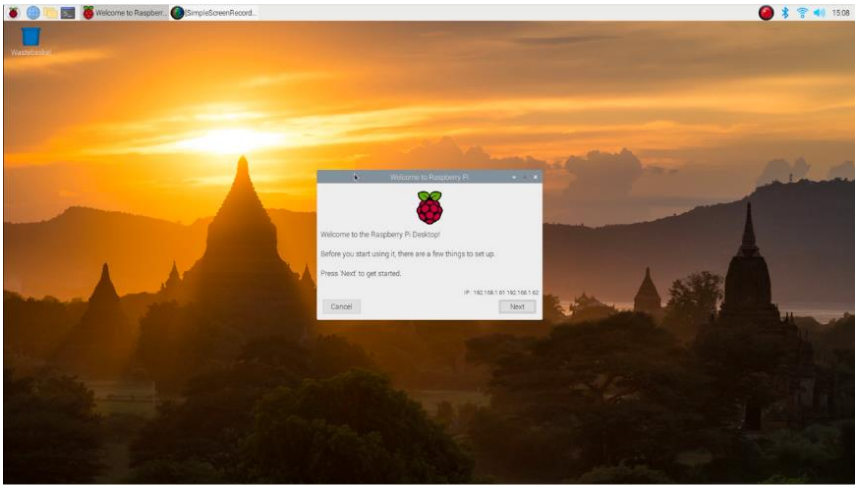
Si se ha colocado la tarjeta microSD correctamente y con el S.O., comenzará la carga del mismo, pudiendo observarse como el led de color verde comienza a parpadear, hasta la carga del S.O., pude que se reinicie varias veces hasta finalizar el proceso y llegar al escritorio, no apagar la Raspberry Pi hasta llegar al escritorio.



Uno de los reinicios se producirá al redimensionar el sistema de archivos, el espacio de la tarjeta microSD.



Llegado al escritorio, puede que se muestre como se aprecia en la ventana de la captura superior, un marco negro alrededor del escritorio, no llegando a cubrir este toda la superficie del monitor, con las opciones que se indicaran a modificar más adelante en la configuración de la Raspberry Pi este problema desaparece.



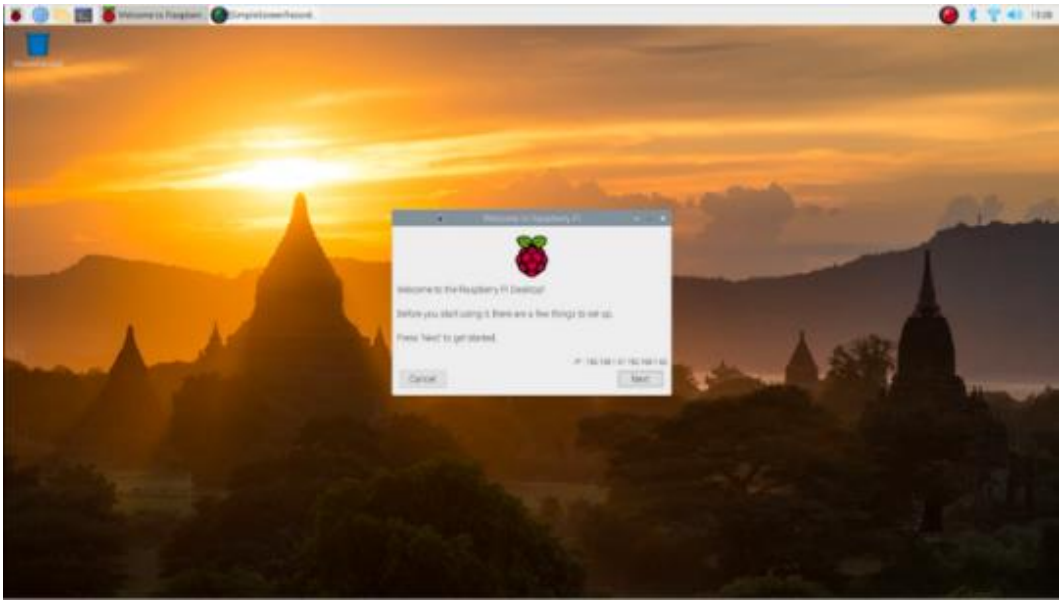


Aspecto de la ventana al inicio del S.O. en modo texto.

Primer inicio configuración Raspberry PI.

Primer inicio y asistente de configuración.

En el primer inicio de la Raspberry Pi, podrá observar varias pantallas que se mostrarán y se ocultarán rápidamente hasta llegar al escritorio, llegando a mostrarse el asistente de configuración, el cual se muestra a continuación, otro asistente de configuración se puede iniciar más tarde mediante terminal o entorno gráfico, se indica más adelante, aunque no todas las opciones.



Escritorio de la Raspberry Pi por primera vez, tras la carga del S.O. desde la tarjeta microSD.

Este asistente puede que se muestre aun habiendo configurado la instalación al realizar el proceso de preparación de la tarjeta microSD.



Se puede observar que se nos muestra la IP de la que dispone nuestro dispositivo, en este caso al estar conectado por WIFI y por la tarjeta ethernet, se muestran dos direcciones IP en la parte inferior derecha.
Habrá que pulsar sobre Next para comenzar el asistente.



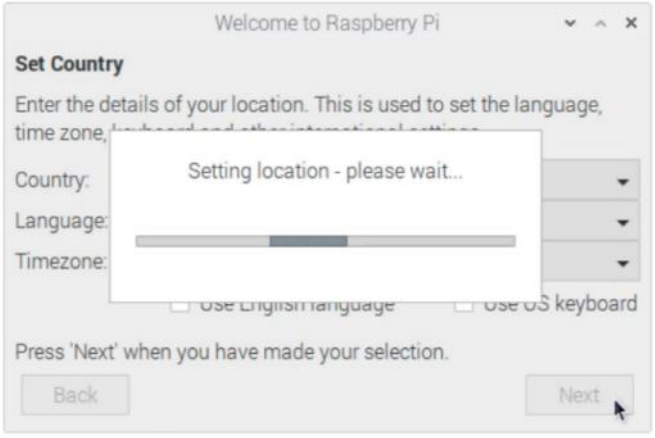
En la Ventana Set Country, habrá que seleccionar los valores que correspondan.



En este caso se modifican las opciones:

- Apartado Country, se despliega y se selecciona el país España (Spain).
- Apartado Language, se selecciona el lenguaje European Spanish.

Por último, en el apartado Timezone, se selecciona la zona horaria Madrid y se pulsa en el botón Next.



Tras haber seleccionado la zona horaria y haber pulsado Next, como se puede apreciar en la ventana de la captura izquierda, se comienza a realizar los cambios en la configuración.

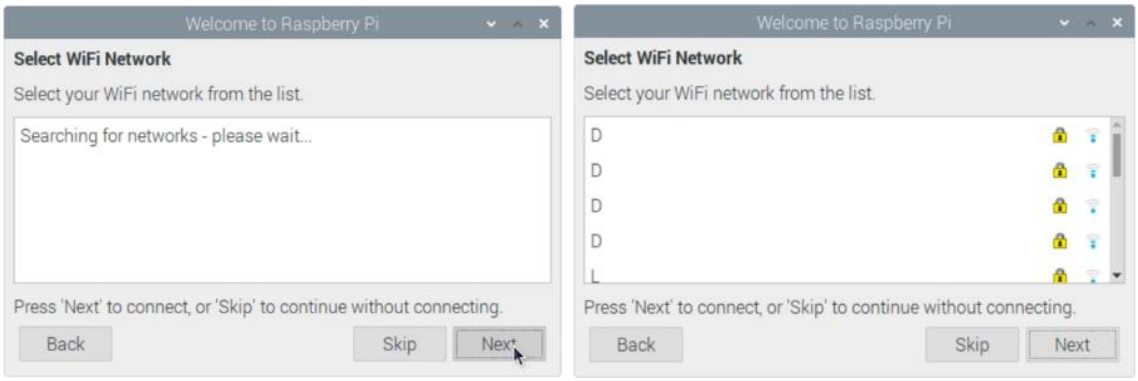


En la nueva ventana que muestra el asistente, Change Password, se facilita la opción de modificar el password (contraseña), por lo que se procederá a sustituirlo y se pulsará sobre Next, esta contraseña es importante recordarla, puesto que el usuario será root (superusuario), teniendo que facilitarla para por ejemplo realizar instalaciones de software.



Ventana Set Up Screen, al seleccionar la opción This screen shows a black border around the desktop, tras el reinicio posterior, en el monitor desaparecerán los marcos negros alrededor de la imagen del escritorio.

Para continuar con el asistente se pulsará en el botón Next.

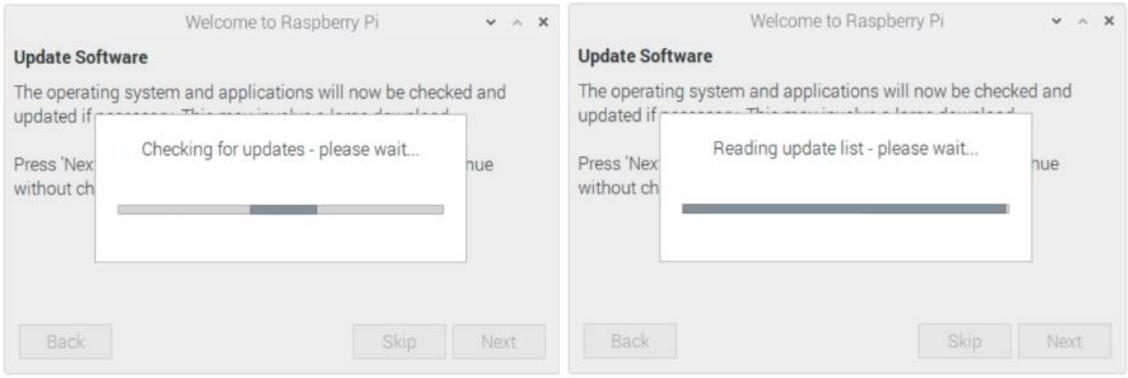


En la ventana Select WiFi Network, en el caso de no haber realizado la configuración previa al preparar la tarjeta, ahora se podrá conectar si es necesario a una red WIFI, se tendrá que esperar a que se muestren todos los SSID (Identificadores de todas las redes), y tras seleccionar una de ellas, se tendrá que seguir el asistente para la configuración, en caso contrario se pulsará en: Next.

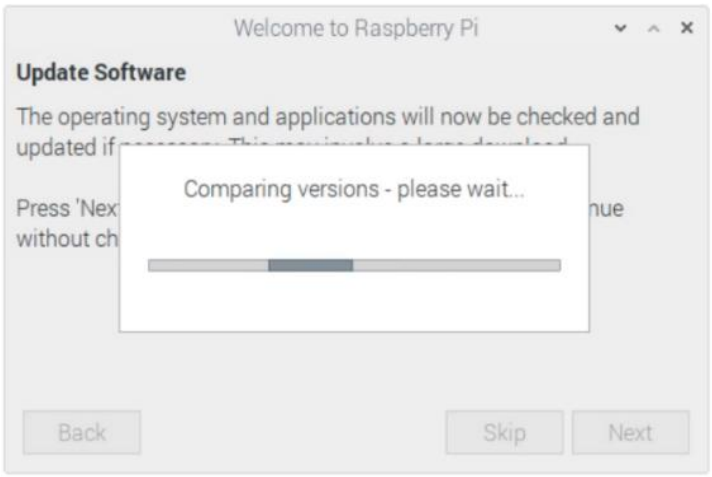
Para conectarse a una red WIFI se seleccionará el SSID de la misma y se seguirá el asistente de conexión en la que habrá que facilitar la contraseña de conexión.

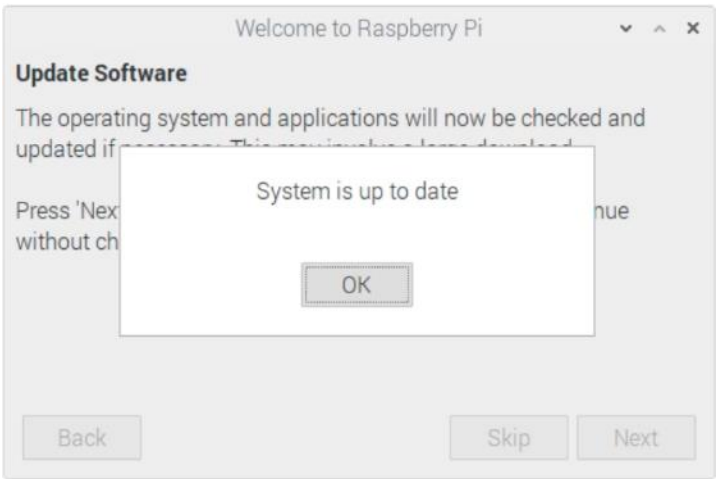


En esta nueva ventana, se pulsará sobre Next para comprobar e instalar las actualizaciones si existiesen, en caso contrario se pulsará sobre Skip, en este caso se pulsa sobre Next.



Llegado a este punto, en la ventana Update Software al pulsar sobre Next, comenzaran los procesos de comprobación de actualizaciones y comparaciones de las versiones, habrá que esperar a que termine el proceso.



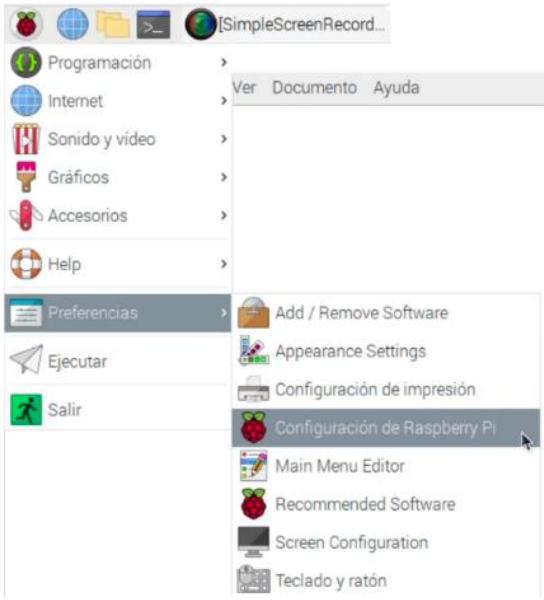


Terminada la instalación de las actualizaciones, se notificará como se puede ver en la ventana de la captura superior, teniendo que presionar en OK.

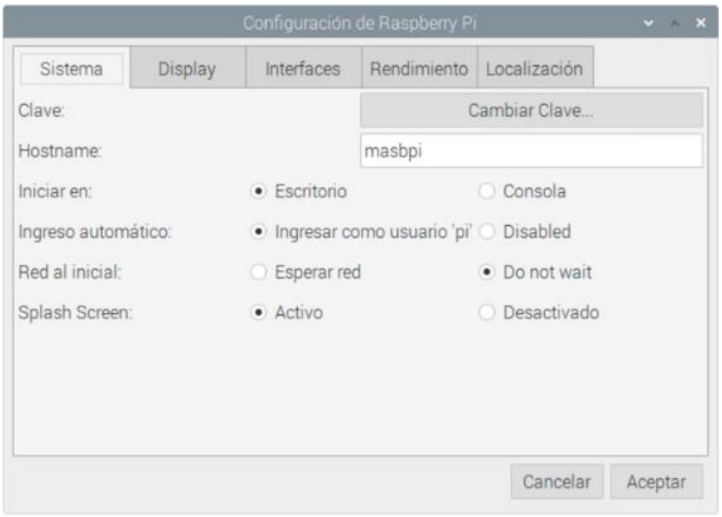


En caso de ser necesario el reinicio de la Raspberry Pi, se reiniciará pulsando sobre: Restart.

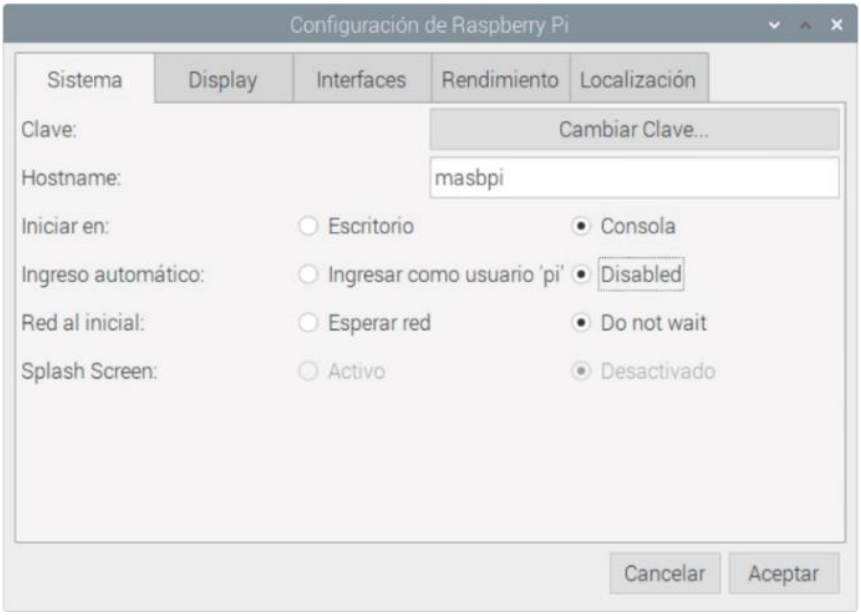
Asistente de configuración gráfico Raspberry Pi.



En el caso de no haber realizado la configuración del entorno al realizar la preparación de la tarjeta microSD, o necesitar configurar nuevamente alguna opción del sistema, para configurar el entorno de trabajo, se podrá acceder al menú pulsando sobre el icono superior izquierdo , en el desplegable que se muestra se pulsará sobre Preferencias \ Configuración de Raspberry Pi.

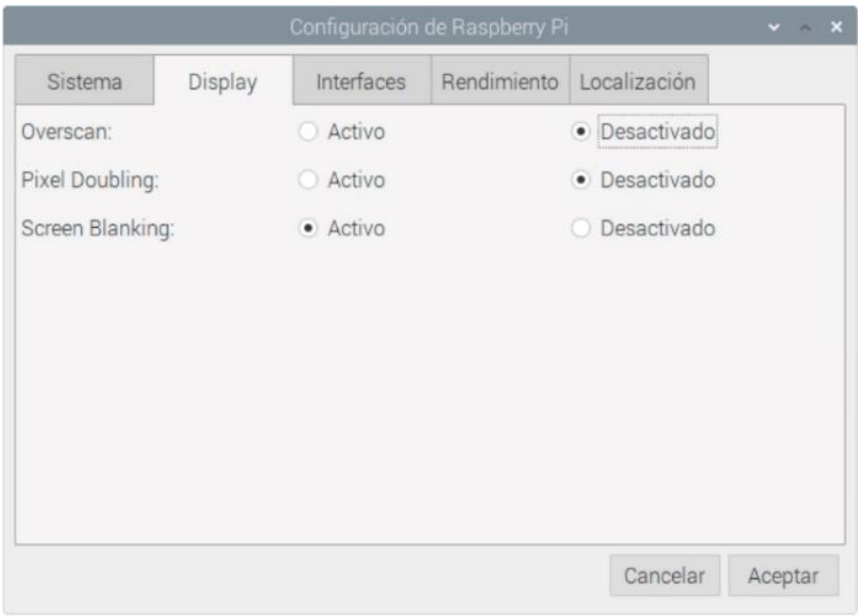


Apareciendo el asistente de configuración.



Para continuar con este proyecto, se seleccionarán las siguientes opciones en los apartados correspondiente a la pestaña Sistema.

- Iniciar en Consola, tras el reinicio se accederá en modo consola y habrá que autenticarnos con un usuario y su contraseña, para poder acceder al entorno grafico se escribirá el comando startx (startx), dentro de la sesión de consola iniciada.
- Ingreso automático Disabled, tras el reinicio cada vez que se reinicie o se apague y se encienda la Raspberry Pi, habrá que autenticarse con un usuario y su contraseña valida.

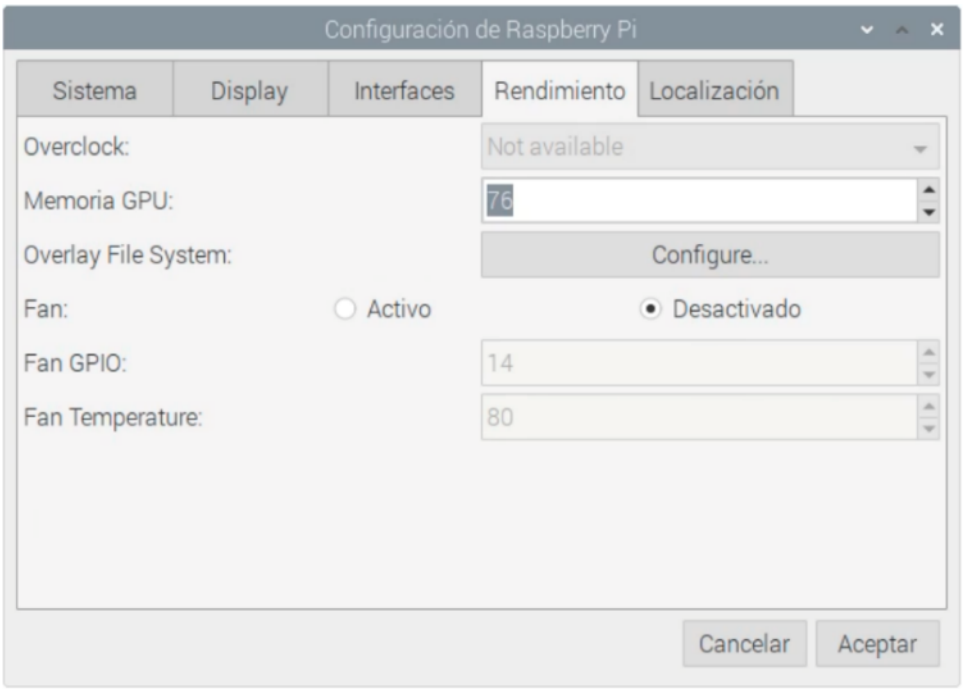


Pestaña Display, no se realiza ninguna modificación.

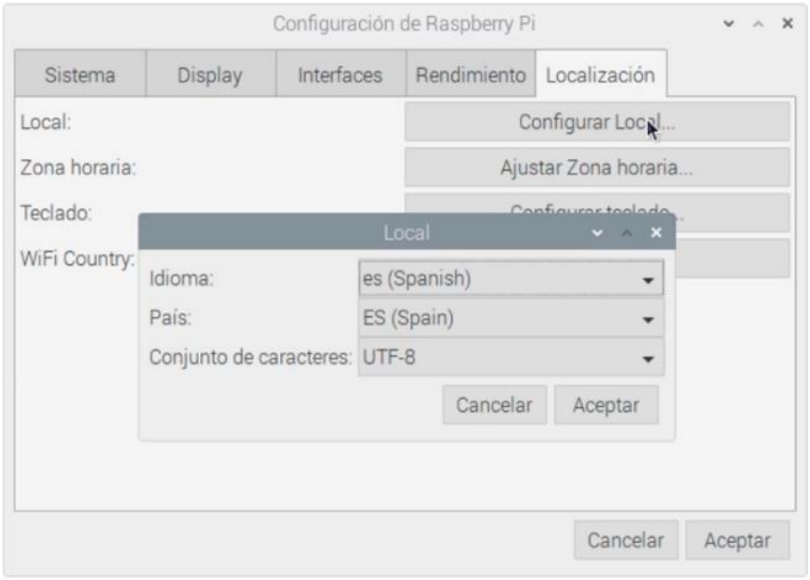


Pestaña Interfaces, para este proyecto se realizan las siguientes modificaciones.

- SSH, en caso de encontrarse desactivado, se activará.
- VNC, se activa.

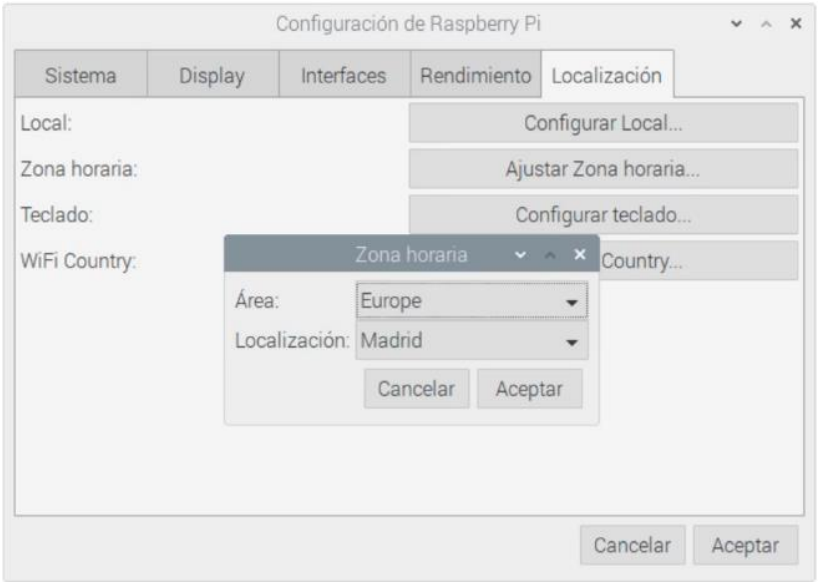


Pestaña Rendimiento, no se realiza ninguna modificación.

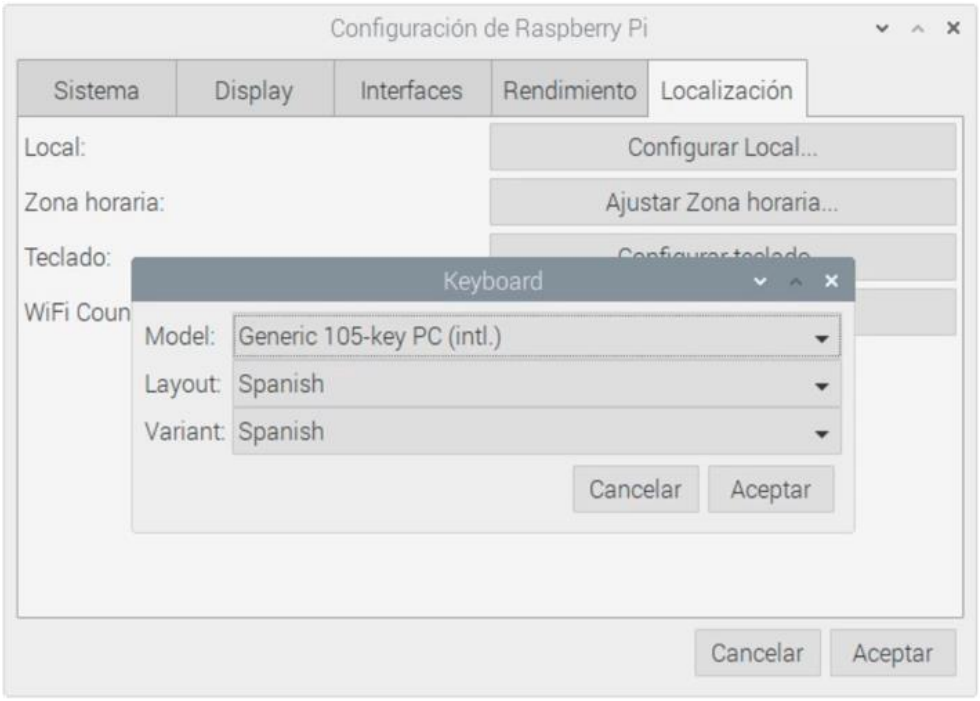


Pestaña Localización.
En esta pestaña, se puede configurar en el apartado:

- Local (Configurar Local …), pudiendo configurar el idioma, el país y el conjunto de caracteres.



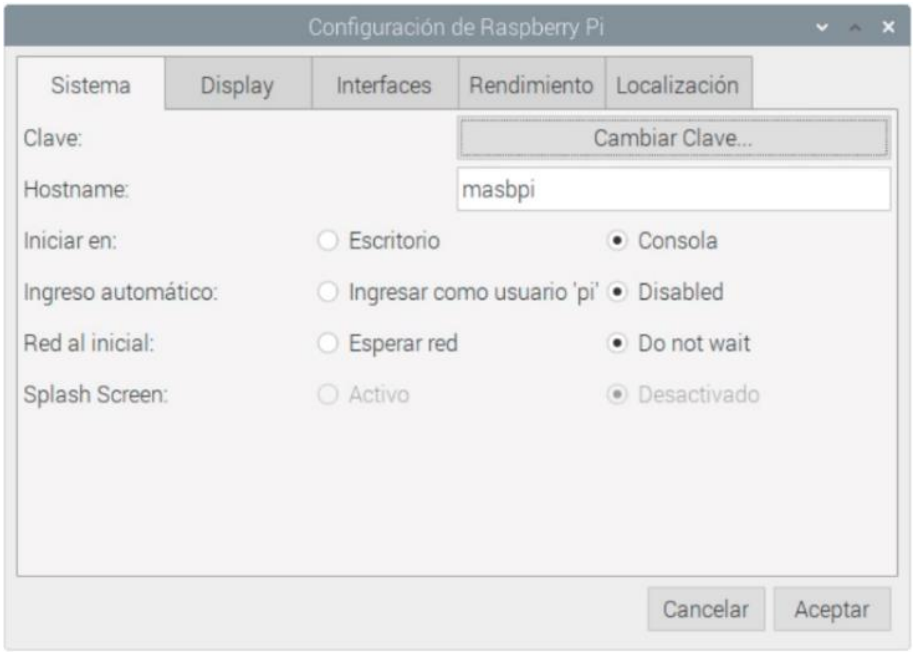
- Zona horaria (Ajustar Zona horaria), donde se podrá seleccionar el área y la localización.



- Teclado (Configurar teclado …), se podrá configurar el modelo de teclado, su disposición y la variante del mismo.



- WiFi Country (Set WiFi Country …), en este apartado se puede configurar el país o la localización de la WIFI.



Tras realizar las modificaciones propuestas, puede que sea necesario reiniciar, en caso de no ser necesario, la próxima vez que se reinicie o se apague y se encienda el sistema, se iniciará en modo consola (modo texto), habrá que validarse con un usuario valido y su contraseña.



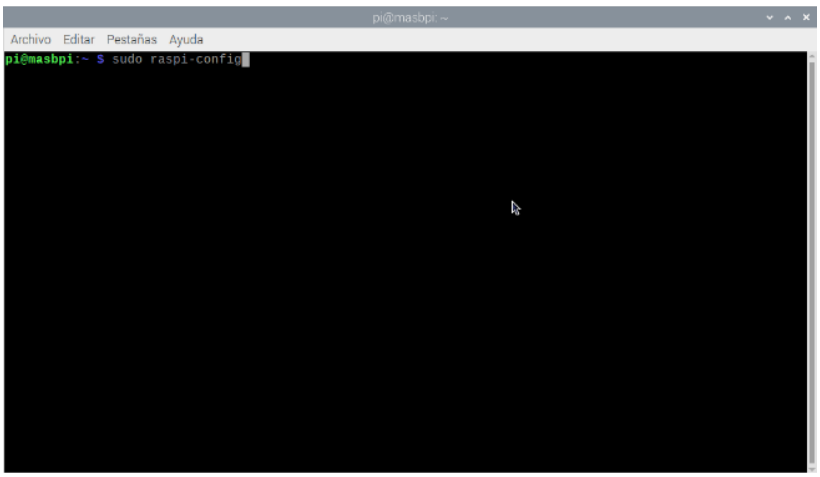
Aspecto de la ventana tras el reinicio y habiendo modificado las opciones indicadas.

Para poder acceder al entorno gráfico dentro de la sesión del usuario y encontrándonos en el terminal, se escribirá el comando startx (solo startx), comando que iniciará las "X", el entorno gráfico.

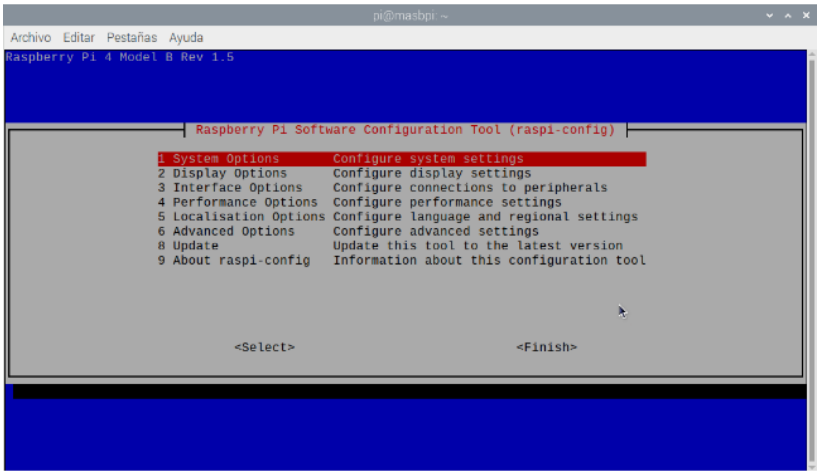


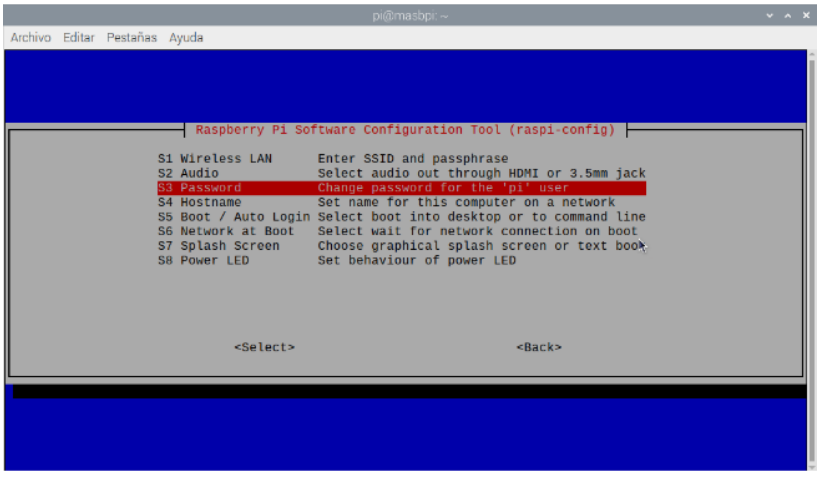
Resultado después de inicio en modo consola, autenticación con un usuario valido y ejecución del comando para iniciar las “X”, iniciar el entorno gráfico, comando startx

Asistente de configuración en terminal.

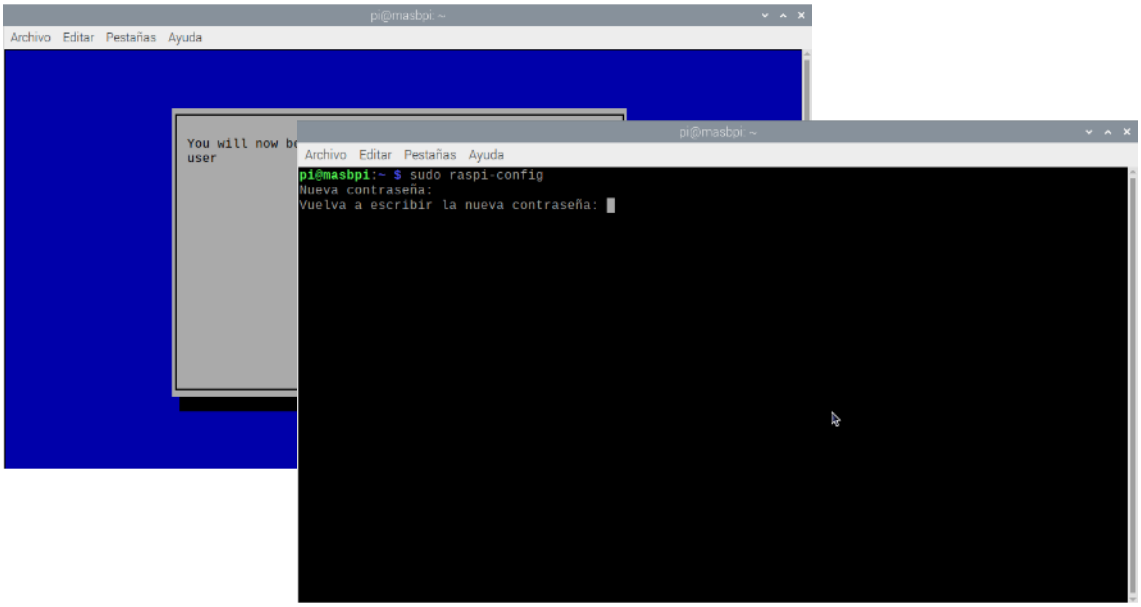


Para acceder a este asistente, dentro de un terminal se ejecutará el comando.
sudo raspy-config

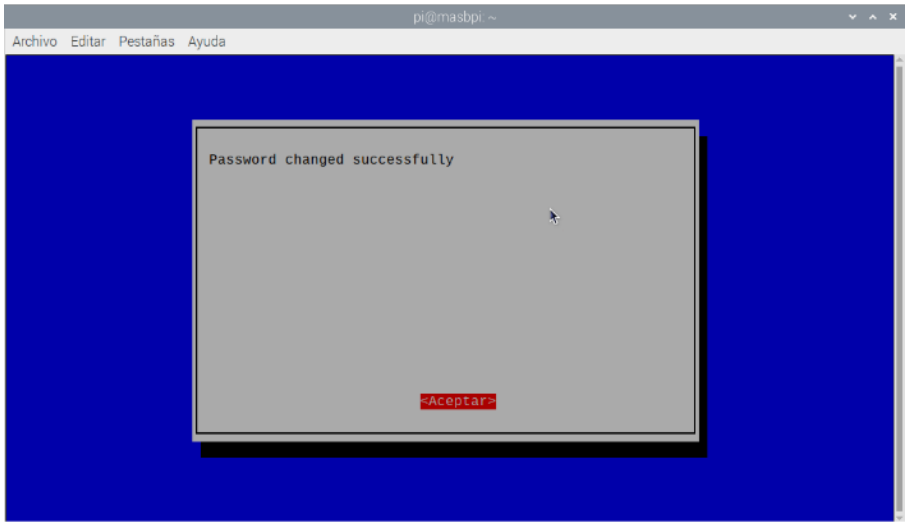




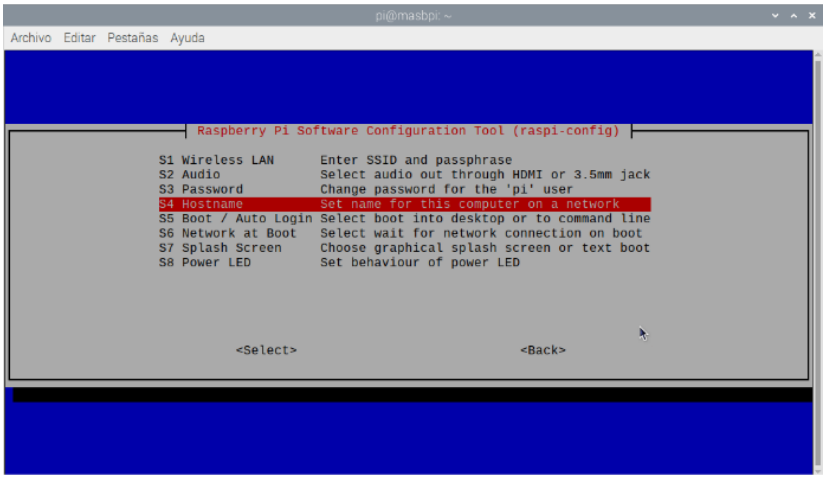
Dentro de System Options \ Password, se podrá modificar el password.



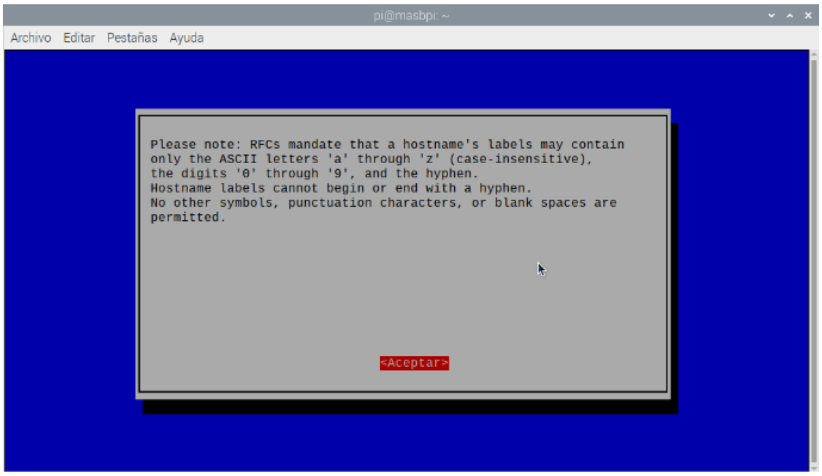
Habrá que proporcionar una nueva contraseña como repetirla por segunda vez.



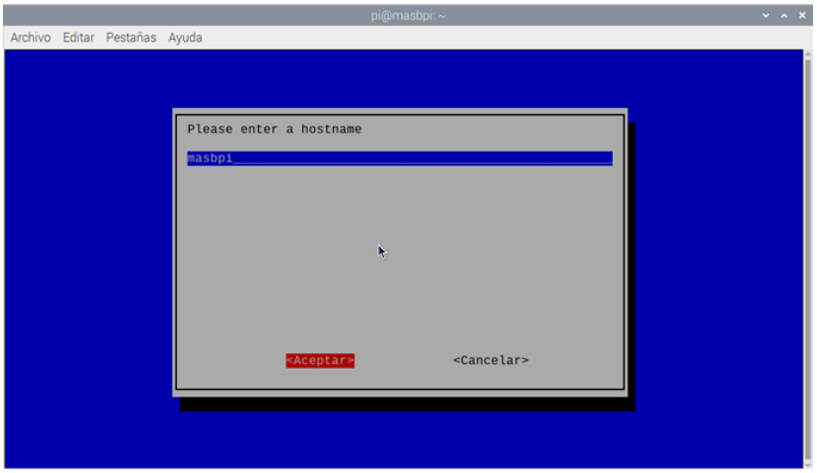
Finalizado este proceso se pulsará sobre Aceptar.



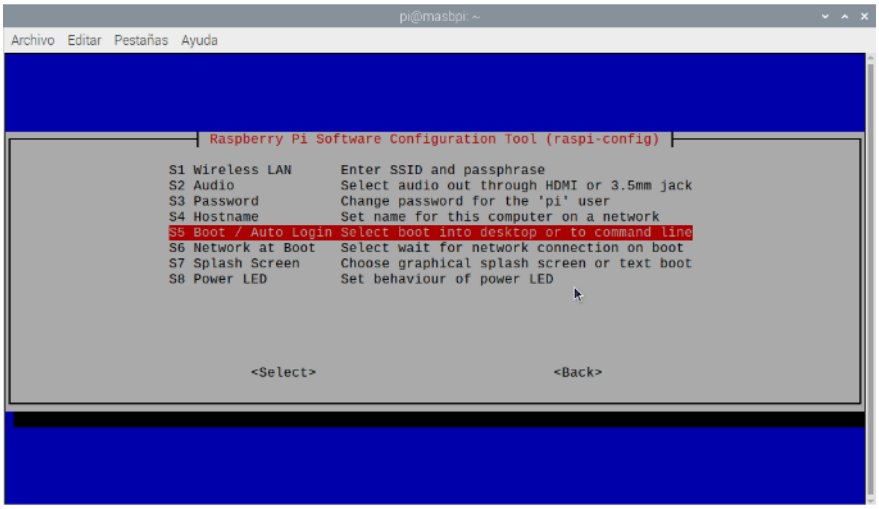
Opción, System Options \ Hostname.



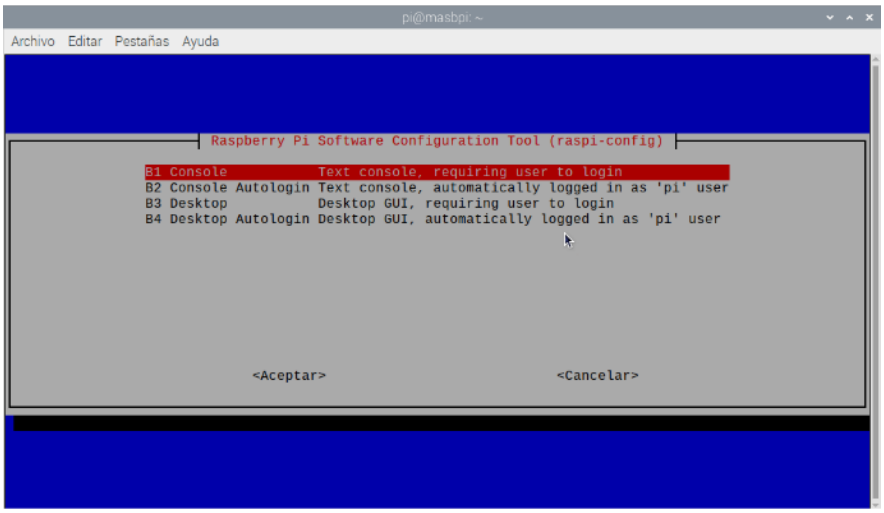
Se pulsará Aceptar.



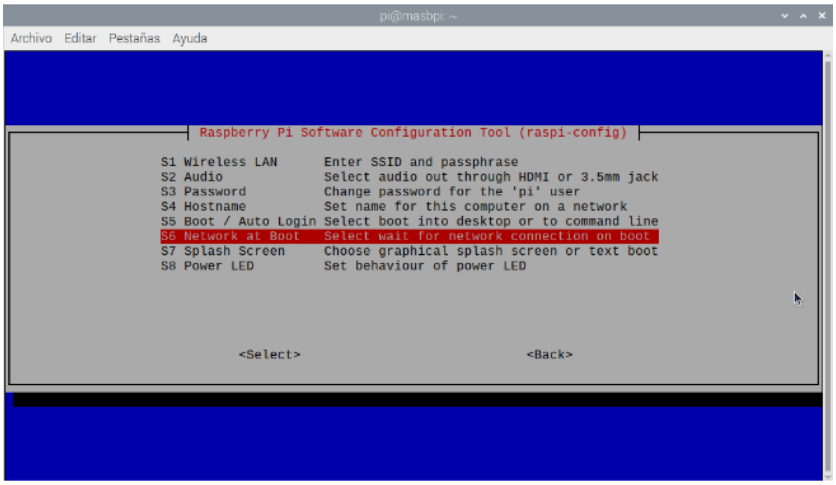
En la nueva ventana que se muestra, se podrá modificar el nombre de la Raspberry Pi, dispositivo que será el servidor VPN/WOL.



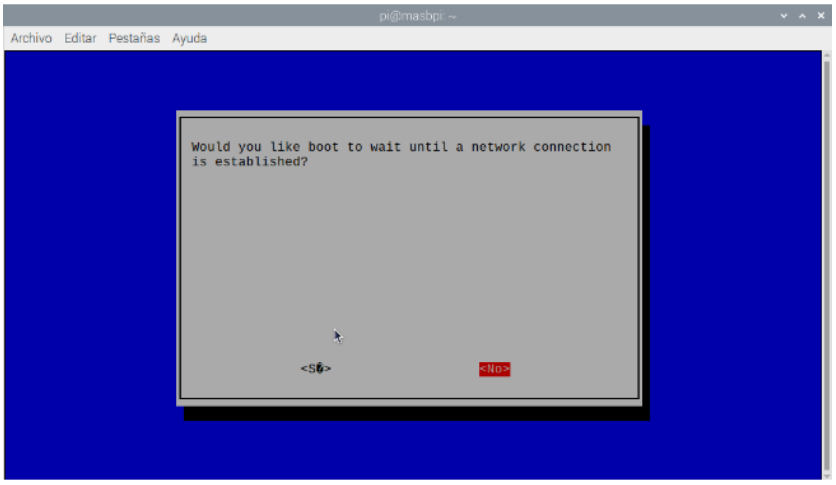
System Options \ Boot / Auto Login select boot into desktop or to command line.

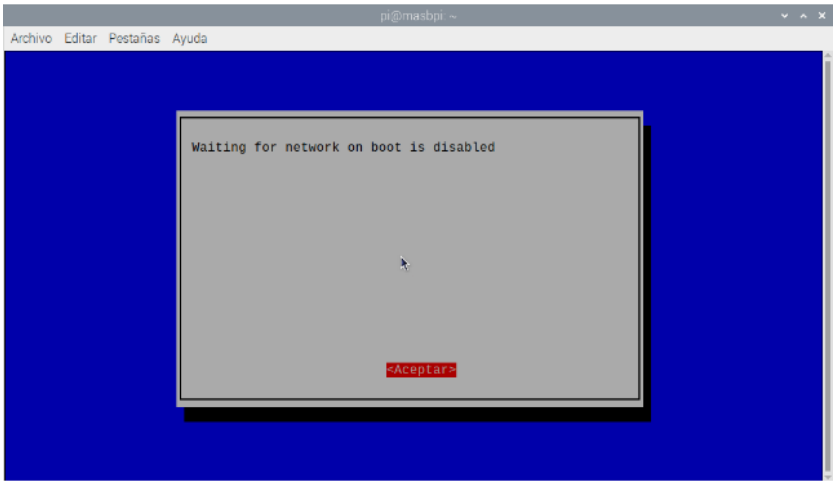


Se seleccionará B1 Console Text console, requiring user to login y se pulsará INTRO. Esta opción hará que la Raspberry Pi al arrancar o reiniciar, arrancara en modo consola, teniendo que autenticarse para poder acceder, y en caso de necesitar acceder al entorno gráfico, será necesario ejecutar el comando. **startx**

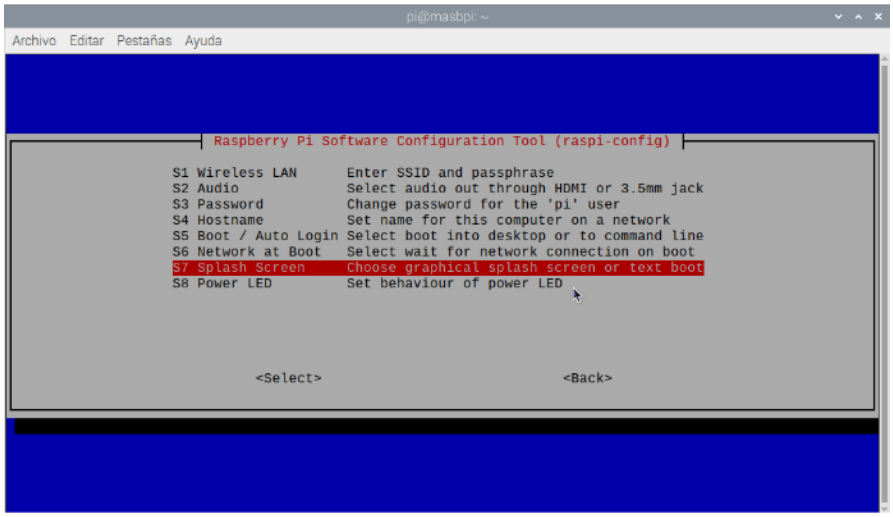


Opción, System Options \ Network at boot.

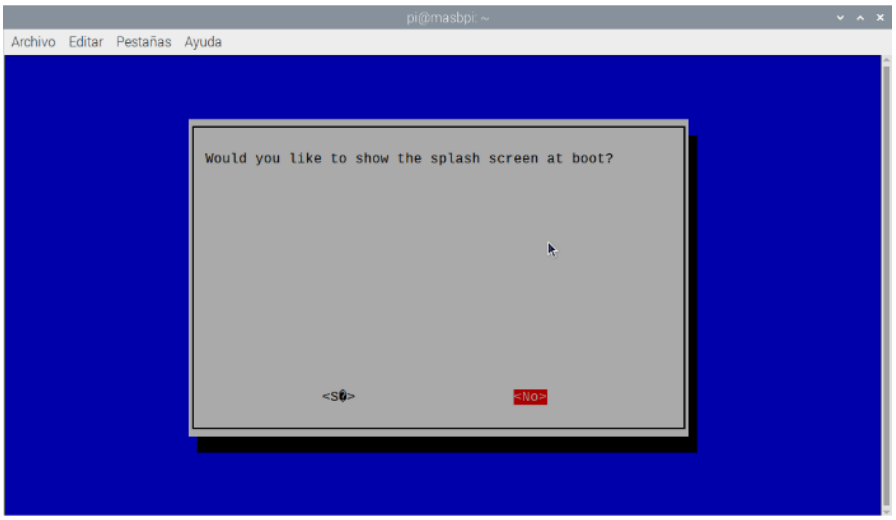


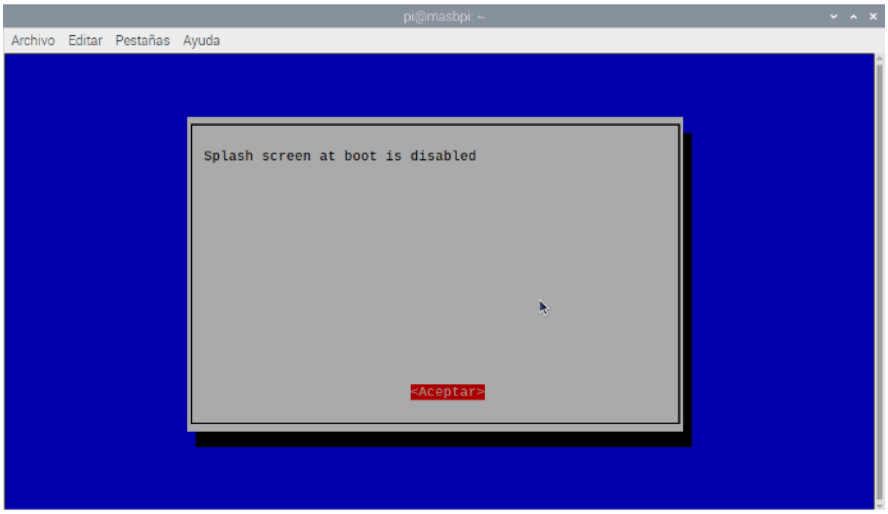


Se selecciona No, para evitar que la Raspberry Pi se quede a la espera de red al arrancar o tras un reinicio.

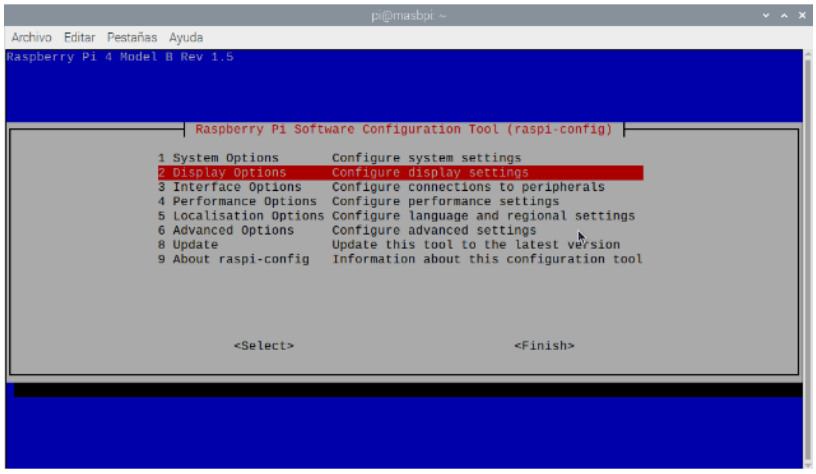


System Options \ Splash Screen.

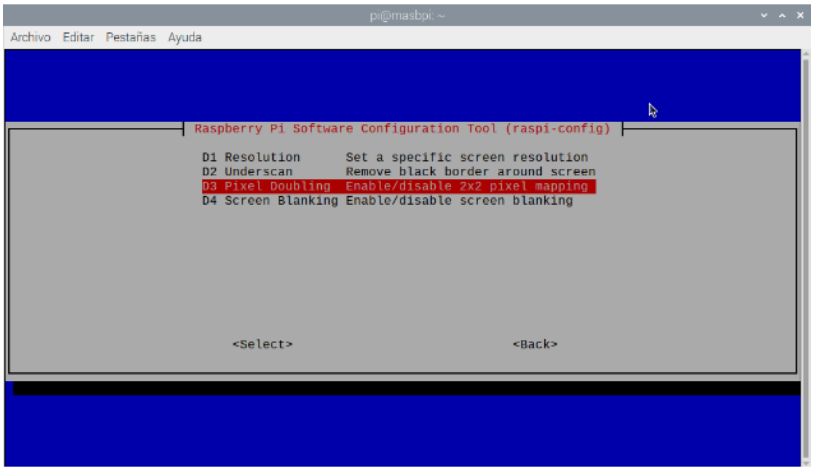


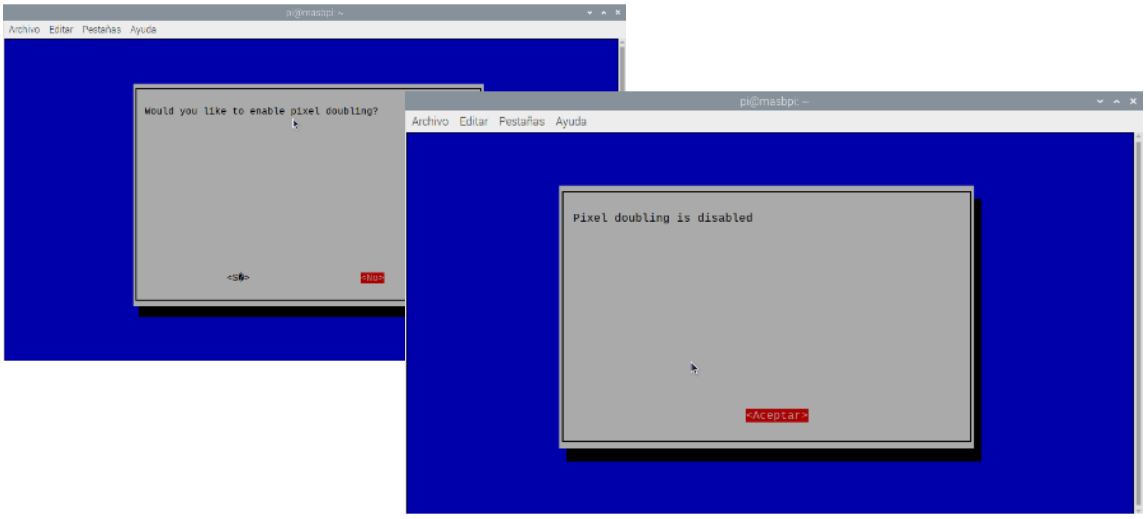


Se selecciona No y tras pulsar No, se pulsará sobre Aceptar.

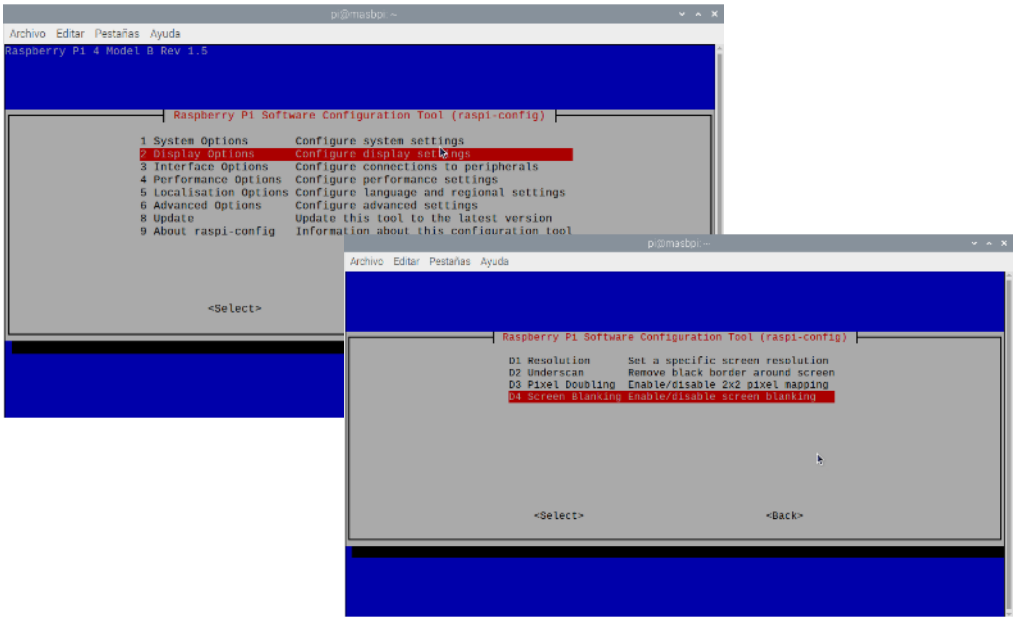


System Options \ Display Options.

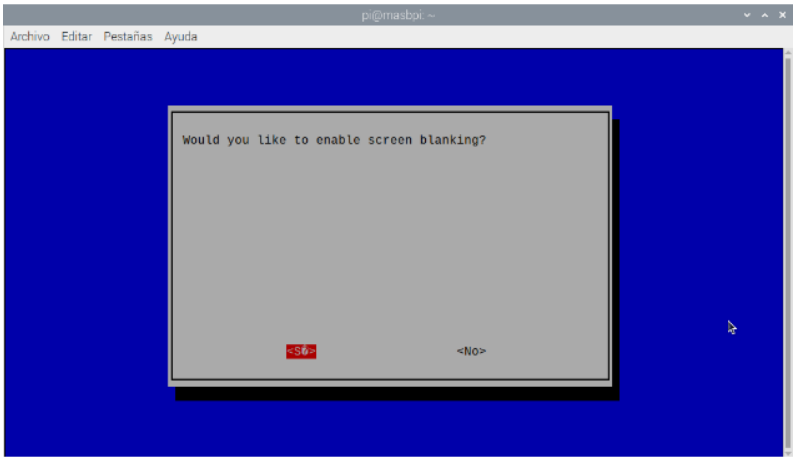


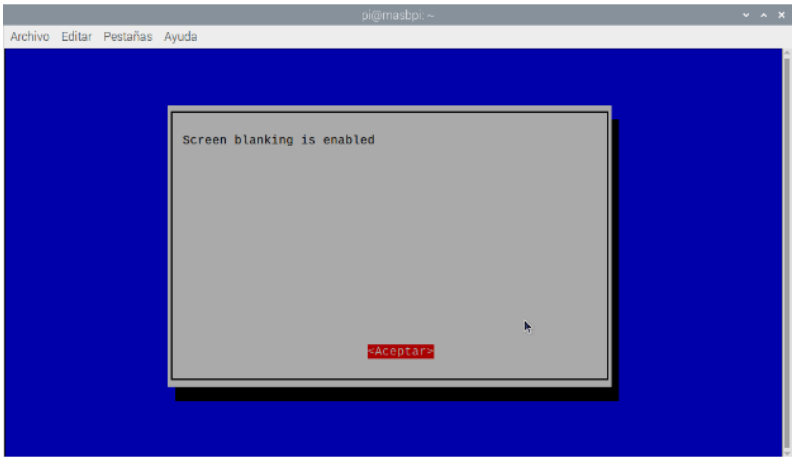


Se selecciona No y tras pulsar No, se pulsará sobre Aceptar.

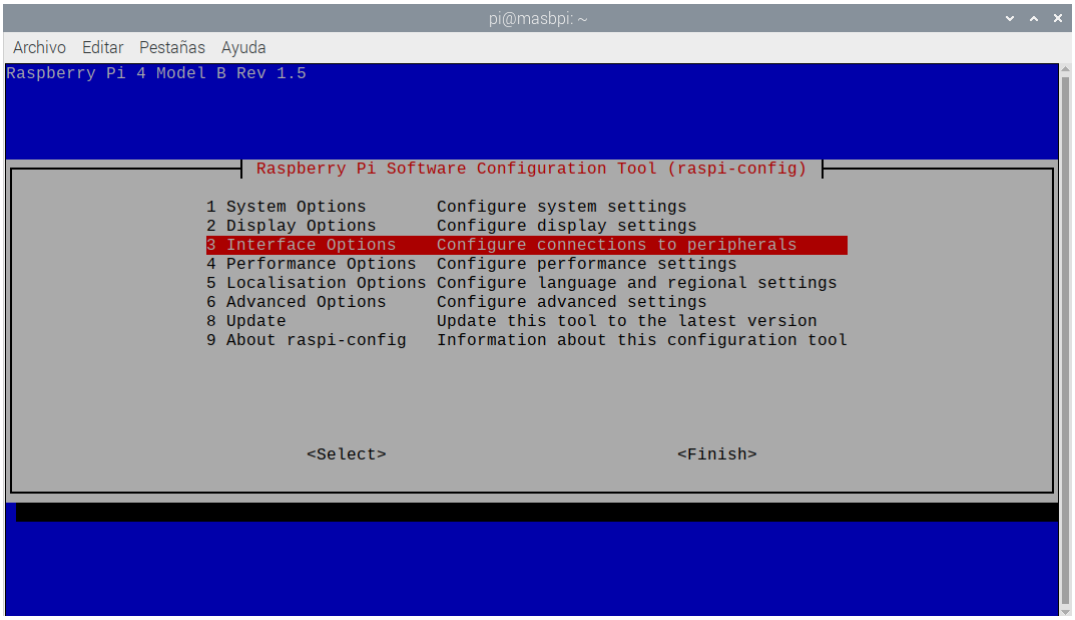


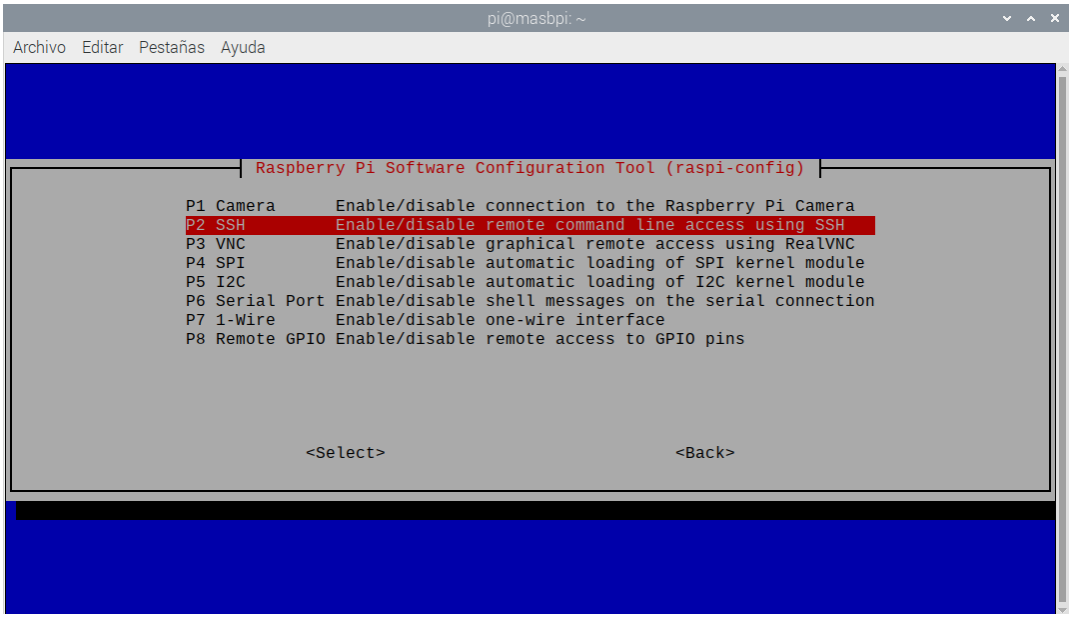
Display Options \ Screen Blanking.

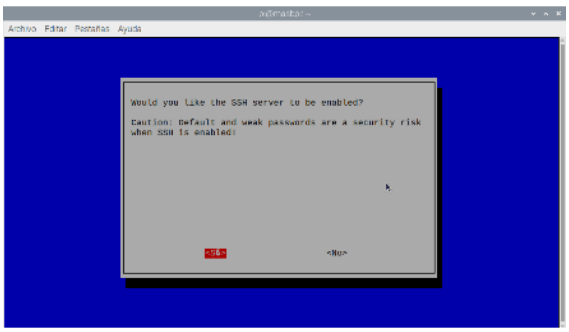


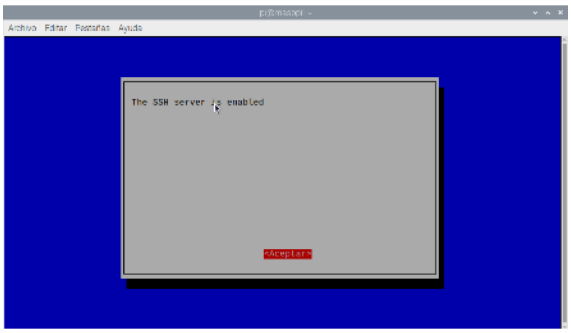


Se selecciona Sí, tras pulsar Sí, se pulsará sobre Aceptar.

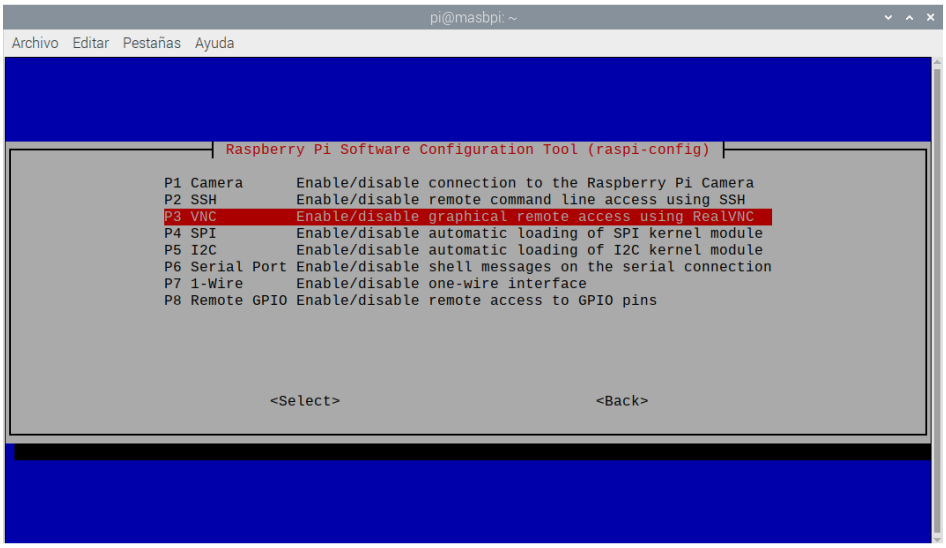


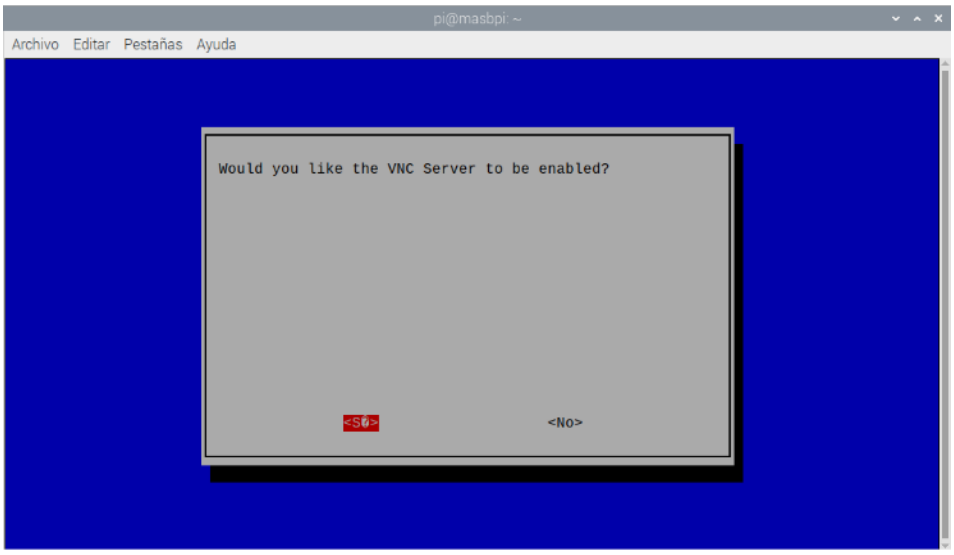


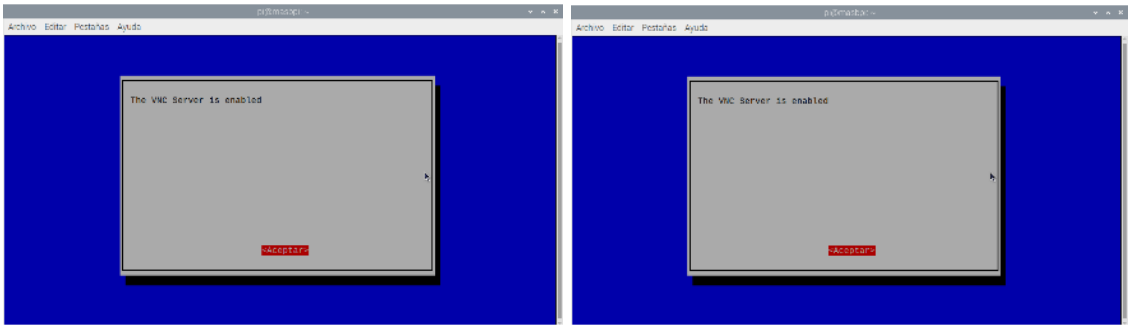




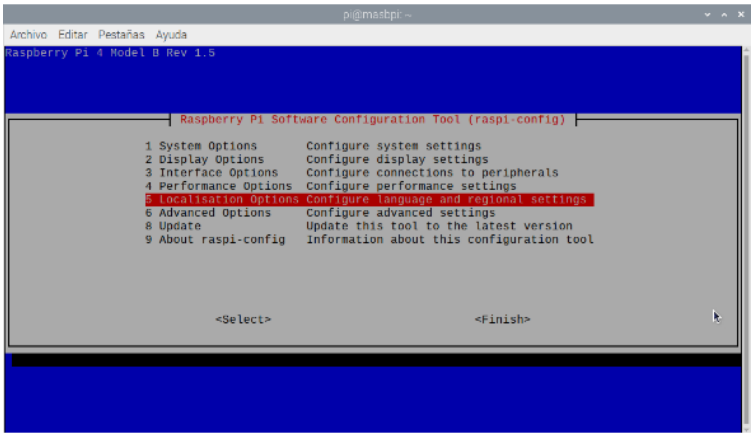
Apartado Interface Options \ SSH, se seleccionará Sí, tras lo que en la siguiente Ventana se pulsará en Aceptar.



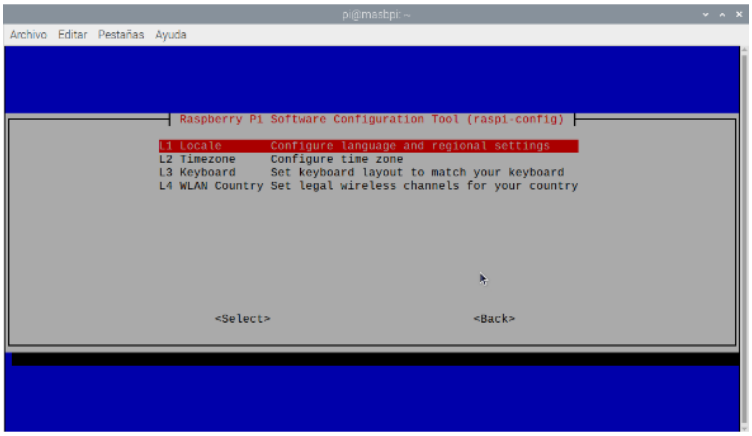




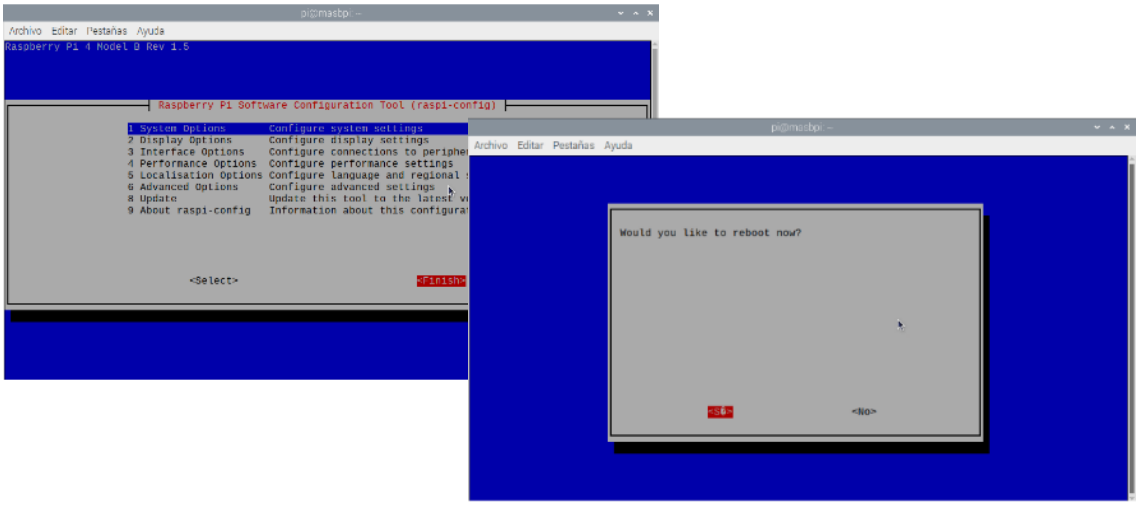
Apartado Interface Options \ VNC, se seleccionará Sí, tras lo que en la siguiente Ventana se pulsará en Aceptar.



Opción, Localization Options.



Locale, se podrá configurar el lenguaje y la configuración regional, zona horaria, el teclado y la configuración regional “”WLAN””.



Terminadas las modificaciones en la ventana System Options se pulsará sobre Finish, posteriormente puede ser necesario reiniciar el dispositivo pulsando sobre Sí, para reiniciar la Raspberry Pi.

Instalación parte servidor.

Instalación local.

Instalación No-IP.

El nombre de dominio o host que se creó en este caso en el proveedor de servicios DDNS No-IP, al ser en este proyecto una cuenta gratuita, cada 30 días habrá que actualizarlo/renovarlo, se recibirá un correo en la cuenta utilizada para realizar la actualización/renovación, se explica los pasos a seguir para llevar a buen término este proceso.

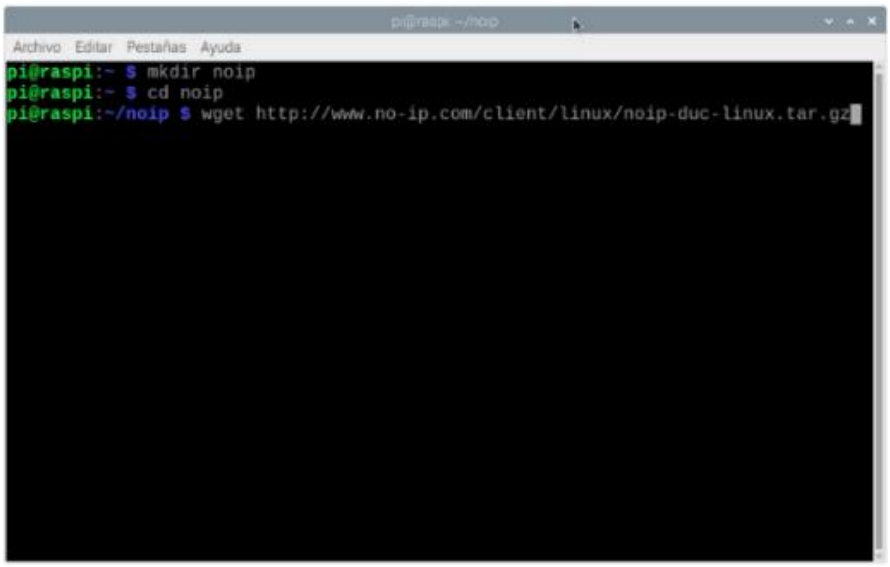
Puede ser necesario instalar dentro de un terminal ciertas aplicaciones y sus dependencias, estas aplicaciones pueden ser make y build-essential, esto será en el caso de que el instalador de No-IP lo indique, en ese caso se ejecutará dentro de un terminal el comando.

sudo apt-get install make build-essential

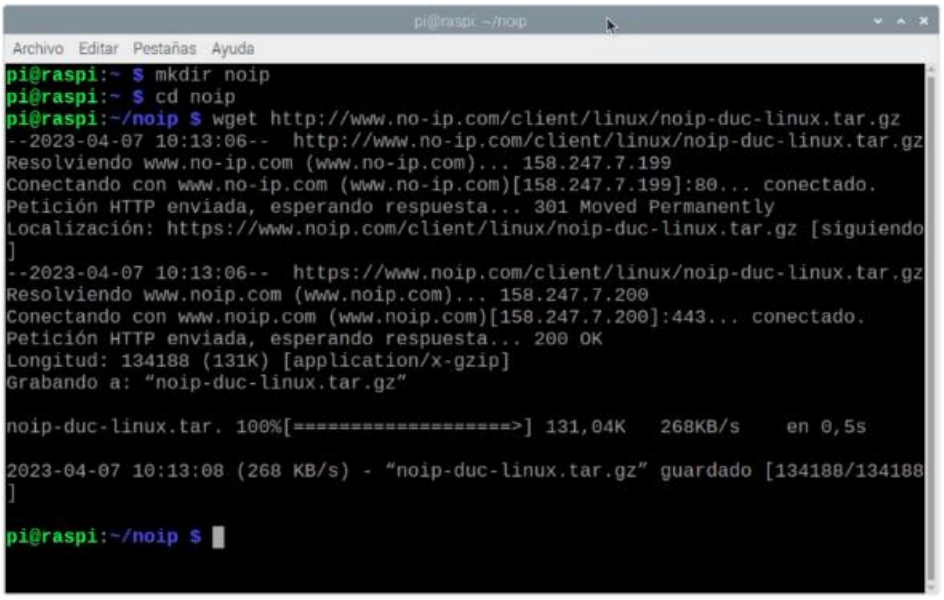
Se muestra cómo realizar la instalación del servicio DDNS del proveedor No-IP, no siendo necesario entonces llevar a cabo la configuración en el router si se instala en el servidor VPN, en este caso se instala el software del proveedor de servicio DDNS en la Raspberry Pi.

Información respecto de la instalación en la WEB oficial.

URL. https://www.noip.com/support/knowledgebase/install-ip-duc-onto-raspberry-pi/



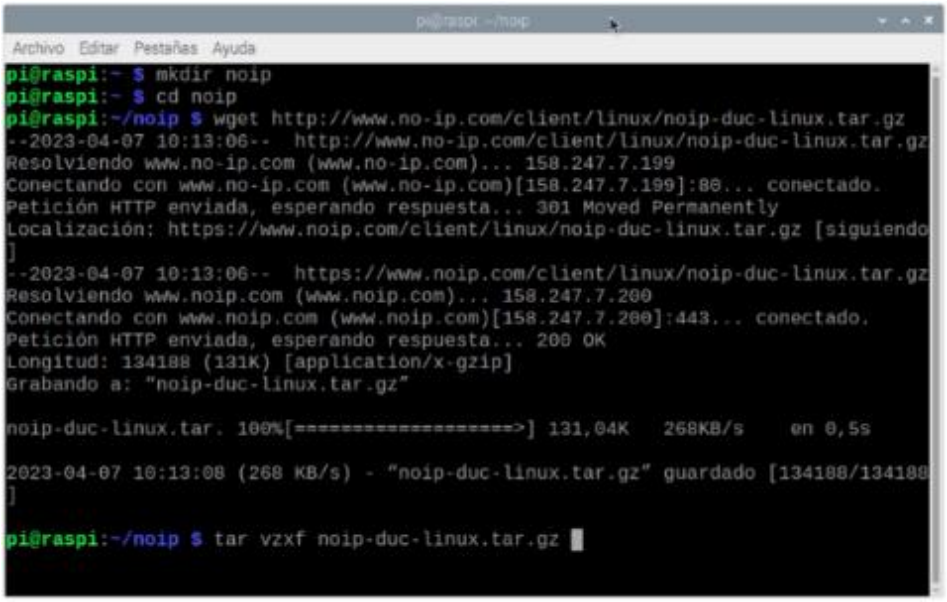
Dentro de un terminal, se actualizarán los repositorios de software y se creará una carpeta llamada noip, en la ubicación donde nos encontramos y se accederá a ella con los comandos indicados a continuación.



Actualización repositorios de software, sudo apt-get update
Creación carpeta noip, mkdir noip
Acceder a la carpeta creada, cd noip

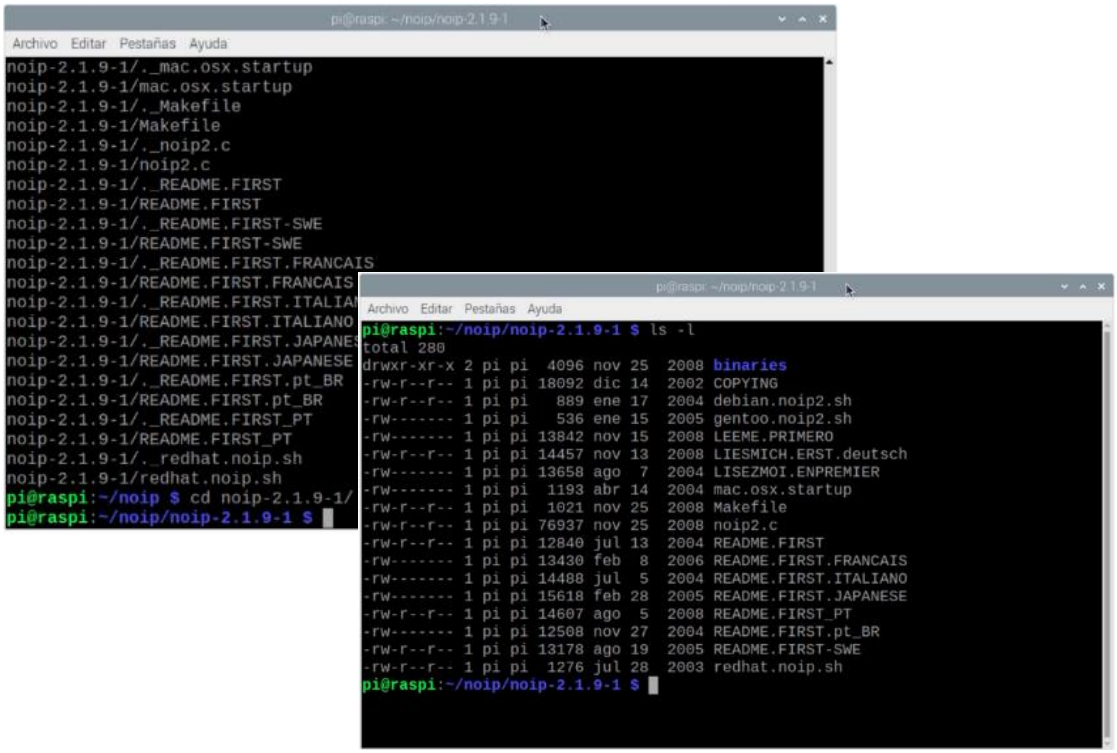
Se utilizará el comando siguiente para la descarga.

wget http://www.no.ip.com/client/linux/noip-duc-linux.tar.gz



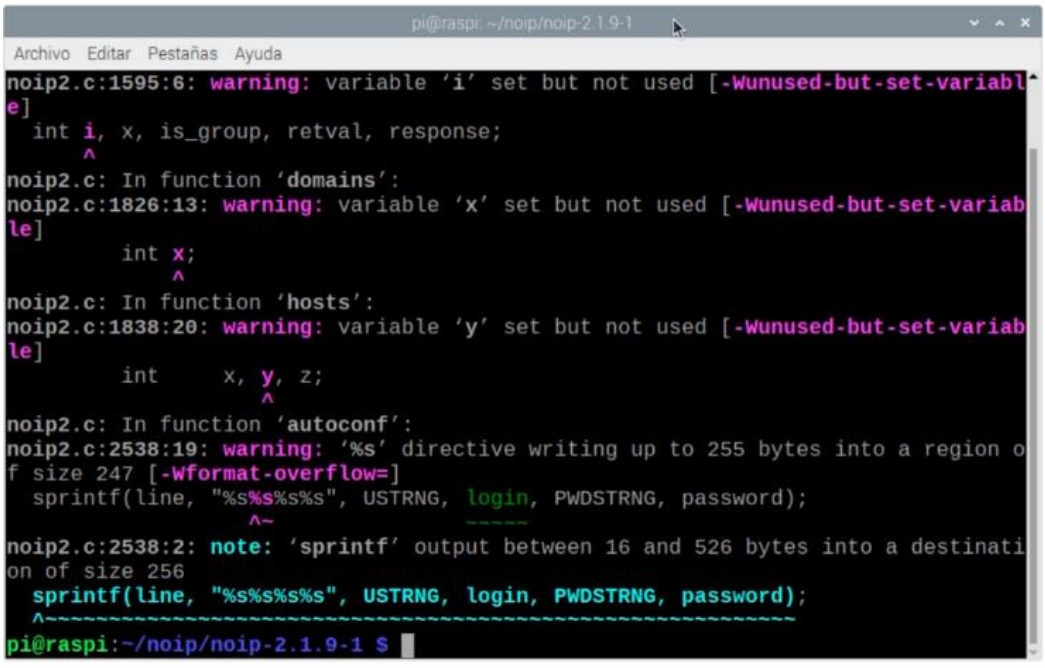
Acto seguido, se desempaquetará y descomprimirá el fichero descargado con el comando.

tar vzxf noip-duc-linux.tar.gz



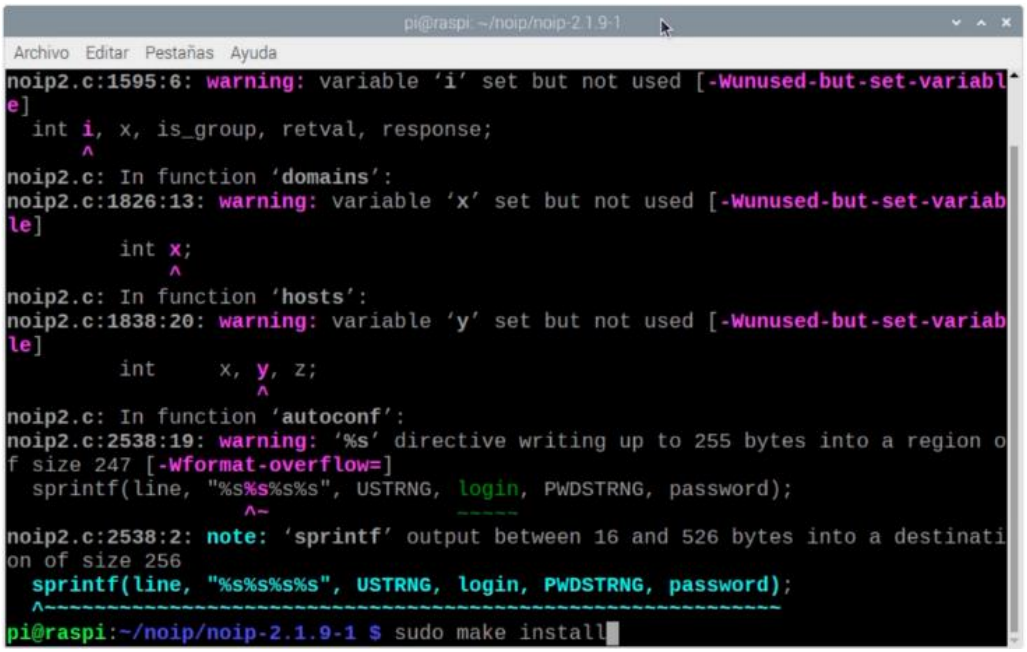
Se accederá al nuevo directorio noip-2.1.9-1, con el comando. cd noip-2.1.9-1

En caso de querer ver el contenido del directorio, se ejecutará el comando. ls -l



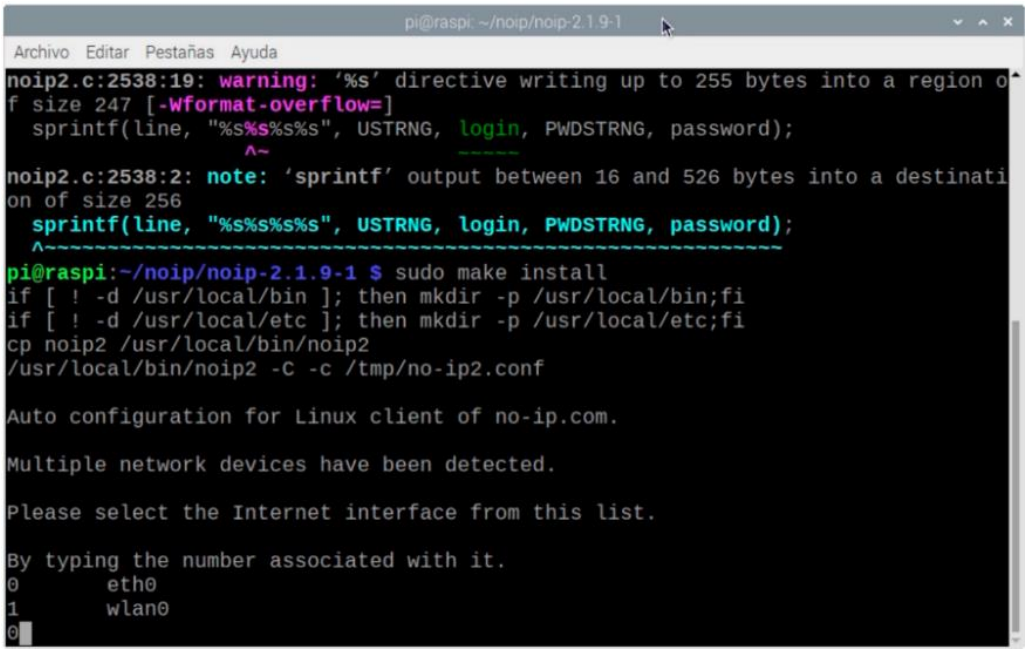
Para comenzar la instalación se ejecutará el comando.

sudo make

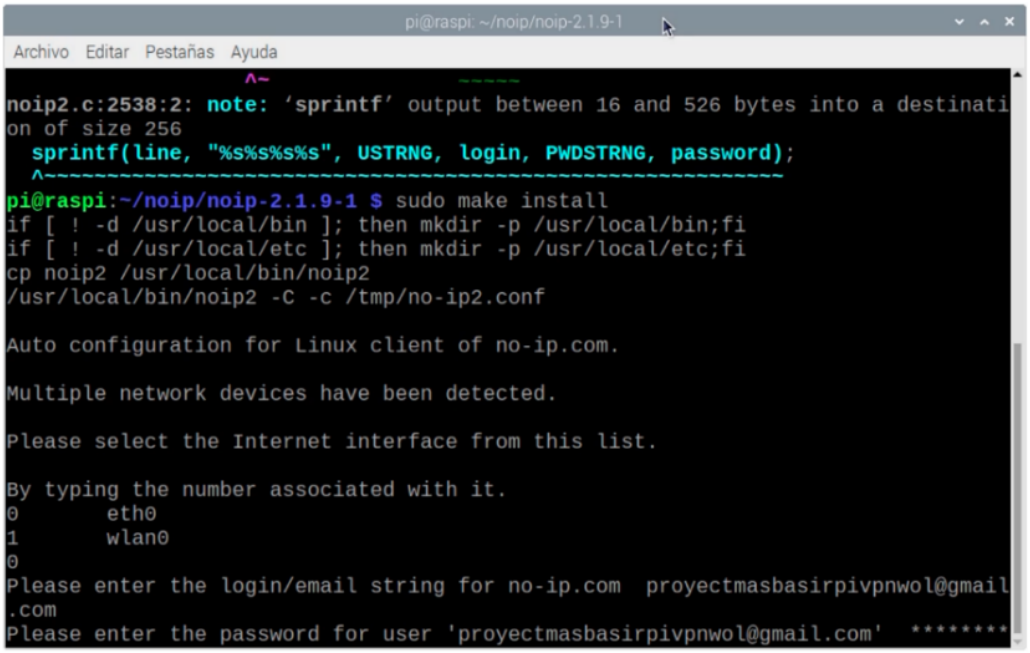


Tras la ejecución del comando sudo make y si no se informa de algún error, se ejecutará el comando para comenzar con la instalación.

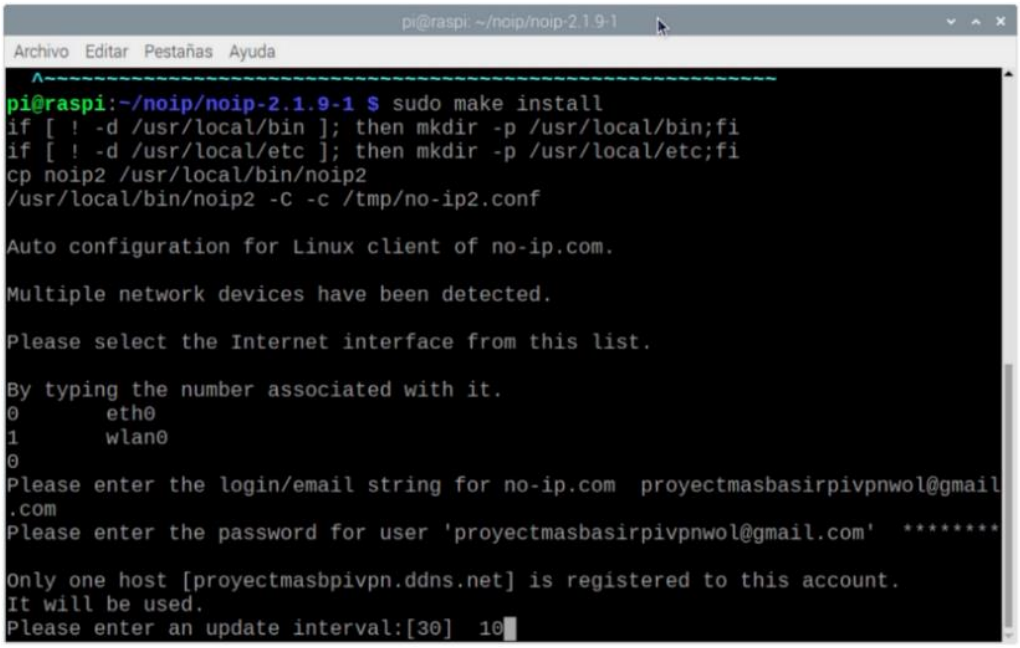
sudo make install



En este paso de la instalación, se indicará la interfaz de red a utilizar, teniendo que indicar el número ubicado a la izquierda, correspondiente a la interfaz de red que se utilizara, para la creación de este proyecto se selecciona 0 “cero”, correspondiente a la interfaz ethernet eth0, se ha comprobado que si se selecciona la interfaz WIFI wlan0 funciona correctamente, seleccionada la interfaz de red, se pulsará INTRO.

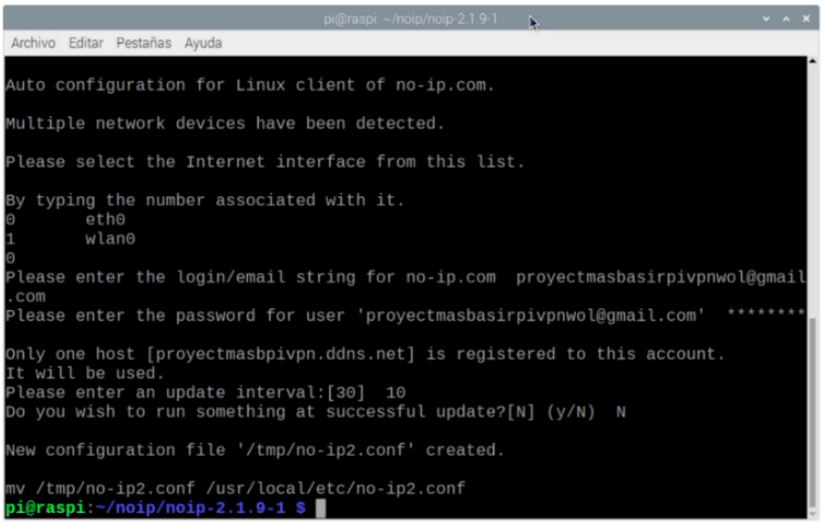


A continuación, se pregunta la cuenta que se utilizará para el servicio no-ip.com, se facilitará la cuenta de correo utilizada para la creación de la cuenta en este ejemplo en No-IP, posteriormente habrá que introducir la contraseña.



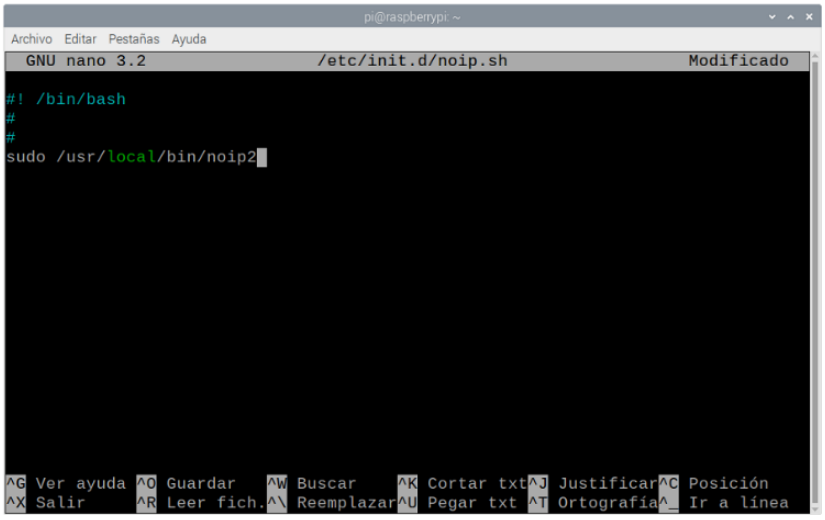
“”Please enter an update Interval””
“”Introduzca un intervalo de actualización””

Ahora se pregunta con que intervalo se realizará la actualización con el servicio DDNS, intervalo de actualización para la asociación de la IP pública con el nombre de dominio o host creado, en este caso se selecciona 10 minutos y se pulsa INTRO.



“”Do you wish to run something at successful update? [N] (y/N)”” N
“”¿Desea ejecutar algo en una actualización exitosa? [N] (y/N)”” N

Se presiona N e INTRO para finalizar la instalación.

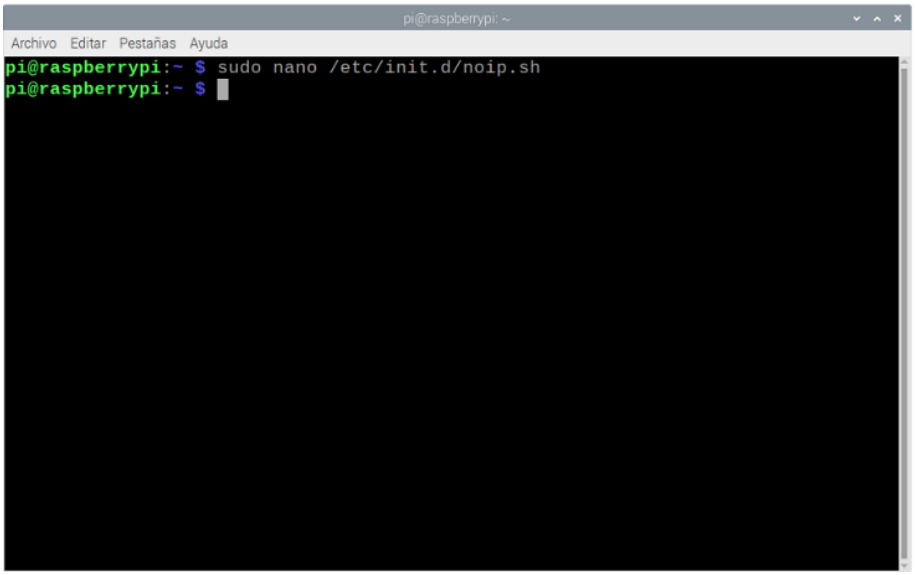


Ahora, se creará el fichero noip.sh, el cual, tras la actualización de los enlaces de scripts, iniciará noip cada vez que se reinicie/se apague y se encienda el servidor VPN/WOL, se utilizará el comando.

sudo nano /etc/init.d/noip.sh

En este fichero se escribirá:

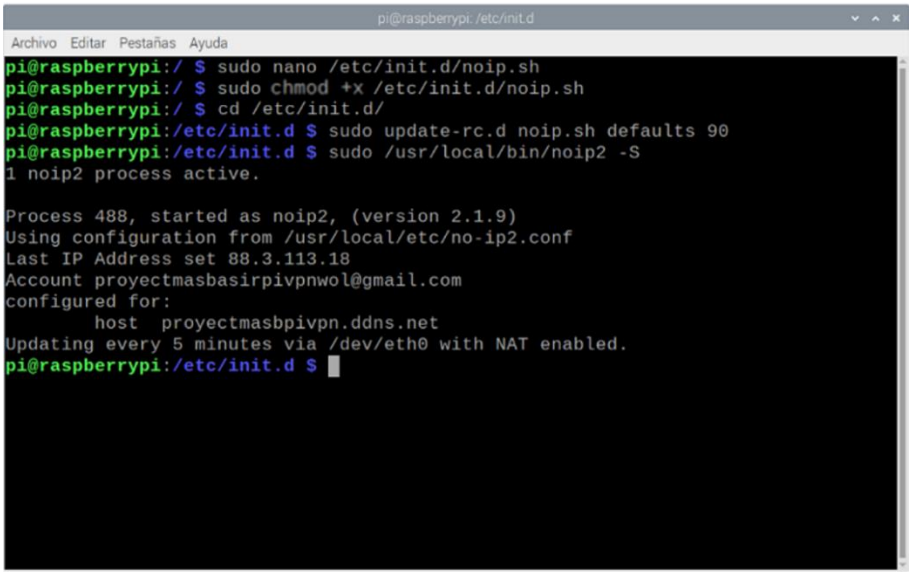
#! /bin/bash
#
#
sudo /usr/local/bin/noip2



Habrá que pulsar la combinación de teclas Ctrl+O (Control y sin soltar pulsar O), para guardar el contenido y para salir se pulsará Ctrl+X (Control y sin soltar pulsar X).

Una vez creado el fichero, para que sea un fichero ejecutable, se ejecutara el comando

sudo chmod +x /etc/init.d/noip.sh y posteriormente se pulsará INTRO.



Para iniciar el servicio, habrá que actualizar automáticamente los enlaces a los scripts de init tipo System V, se ejecutarán los comandos:

cd /etc/init.d/	(acceder al directorio /etc/init.d/)
sudo update-rc.d noip.sh defaults 90	(actualización enlaces scripts).
sudo /usr/local/bin/noip2 -S	(Se mostrarà el estado y los datos de la cuenta NO-IP configurada).

```
pi@raspberrypi:/etc/init.d $ sudo /usr/local/bin/noip2 -S
1 noip2 process active.

Process 488, started as noip2, (version 2.1.9)
Using configuration from /usr/local/etc/no-ip2.conf
Last IP Address set 88.3.113.18
Account proyectmasbasirpivpnwol@gmail.com
configured for:
        host  proyectmasbpivpn.ddns.net
Updating every 5 minutes via /dev/eth0 with NAT enabled.
```

Como se observa en la ventana de la captura superior, tras la ejecución del comando.

sudo /usr/local/bin/noip2 –S

Se muestra cómo se mencionó anteriormente, la configuración, el estado y los datos de la cuenta No-IP configurada.

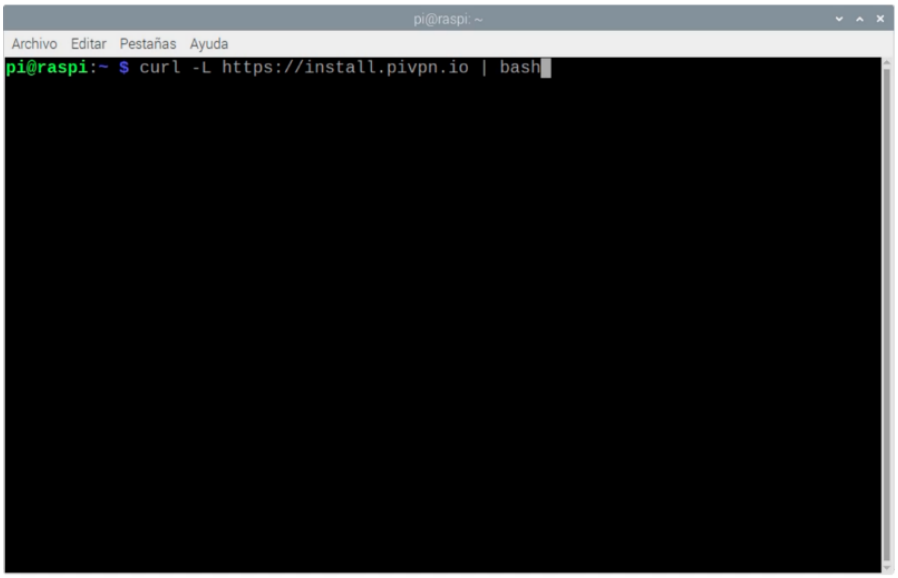
Instalación PiVPN.

Información respecto a la instalación, en la WEB oficial.

URL. https://docs.pivpn.io/install/

En esta instalación podemos encontrarnos según las opciones que se elijan múltiples tipos de configuraciones, para este proyecto se indican los pasos más rápidos y sencillos para poder realizar la instalación y la configuración.

Debido a la traducción online, es posible que al trascribir el texto se pueda haber cometido algún error tipográfico, sin embargo, tras múltiples pruebas realizadas en ningún momento se ha tenido problemas con el hardware por haber elegido una u otra configuración.



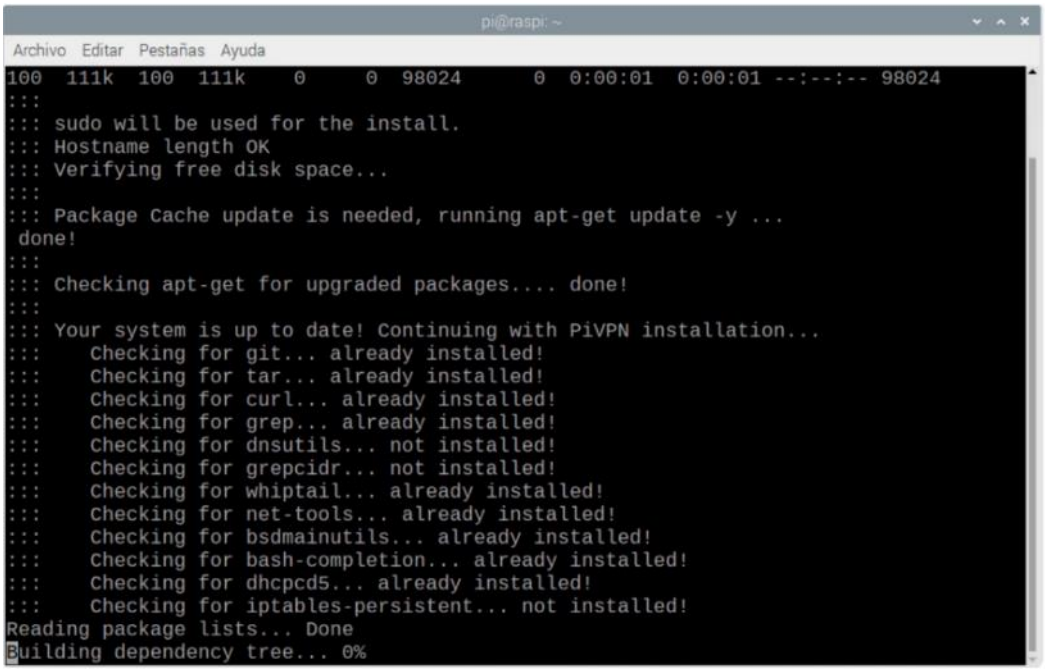
Para comenzar con la instalación y según la WEB del desarrollador del proyecto PiVPN
URL. https://pivpn.io/

La instalación se puede realizar simplemente con ejecutar dentro de un terminal el comando.

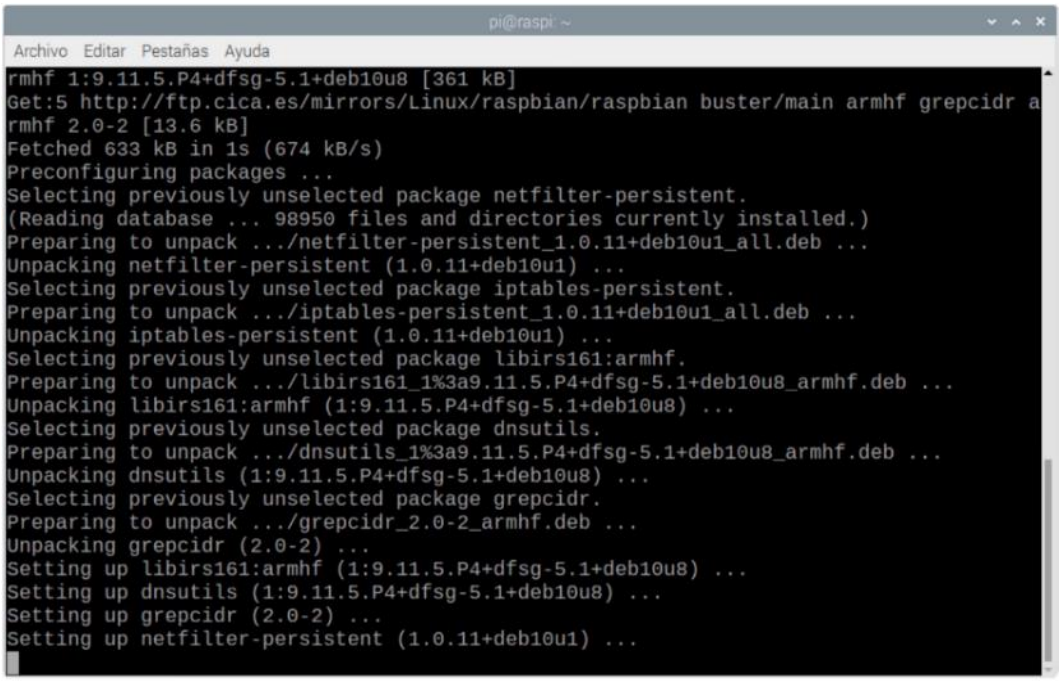
curl -L https://install.pivpn.io | bash

Tras pulsar la tecla INTRO, comenzará la instalación como podrá observar en sucesivas captaras de pantalla.

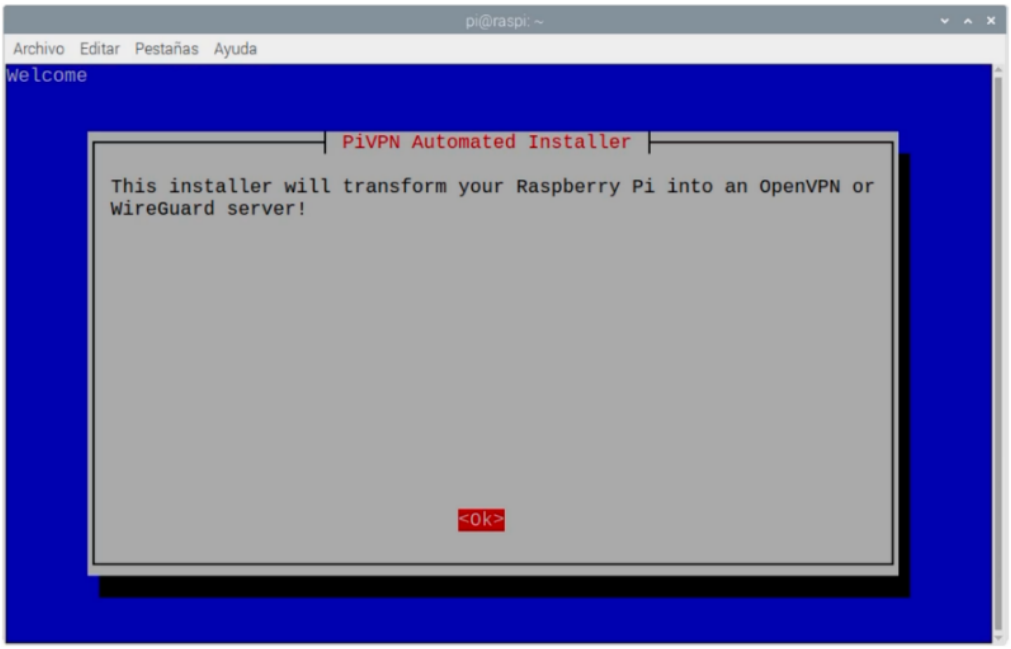
Durante el proceso de instalación, se intercalarán ventanas en las que se puede observar las acciones que se están llevando a cabo, desapareciendo estas rápidamente.



Como se puede apreciar en la captura de la ventana superior, tras la ejecución del comando. curl -L https://install.pivpn.io | bash
La primera acción en realizarse es la comprobación de la existencia de ciertas aplicaciones instaladas.



En el proceso aparecerán ventanas en las que se va indicando lo que se realiza, estas desaparecerán rápidamente, continuando con el asistente.

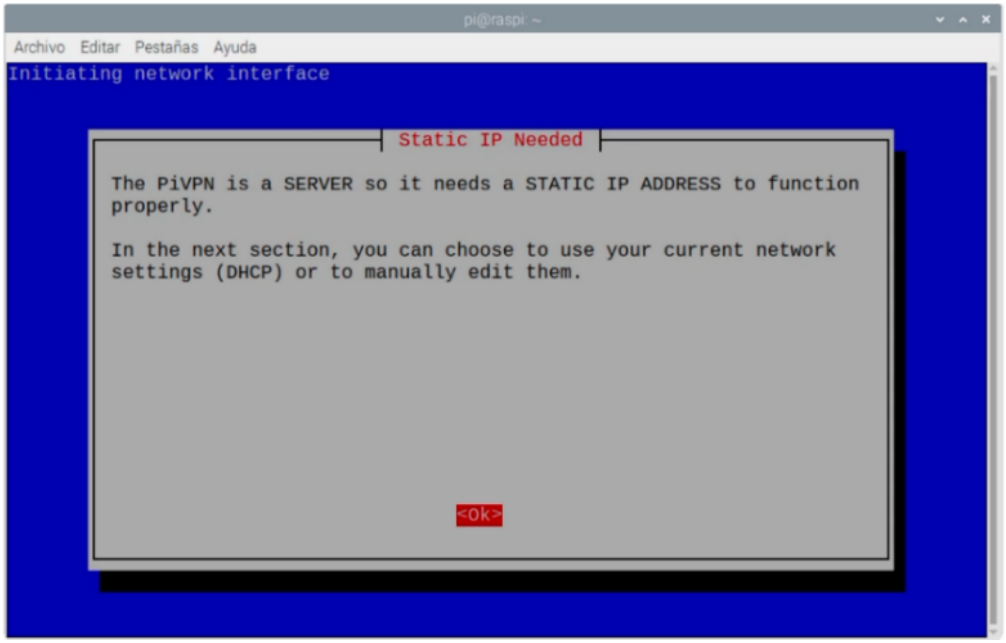


Pantalla de bienvenida (PiVPN Automated Installer)

“”This installer will transform your Raspberry Pi into an OpenVPN or WireGuard Server””

“”Este instalador transformará su Raspberry Pi en un servidor OpenVPN o WireGuard””

En caso de querer continuar al encontrarse seleccionado OK, se pulsará INTRO



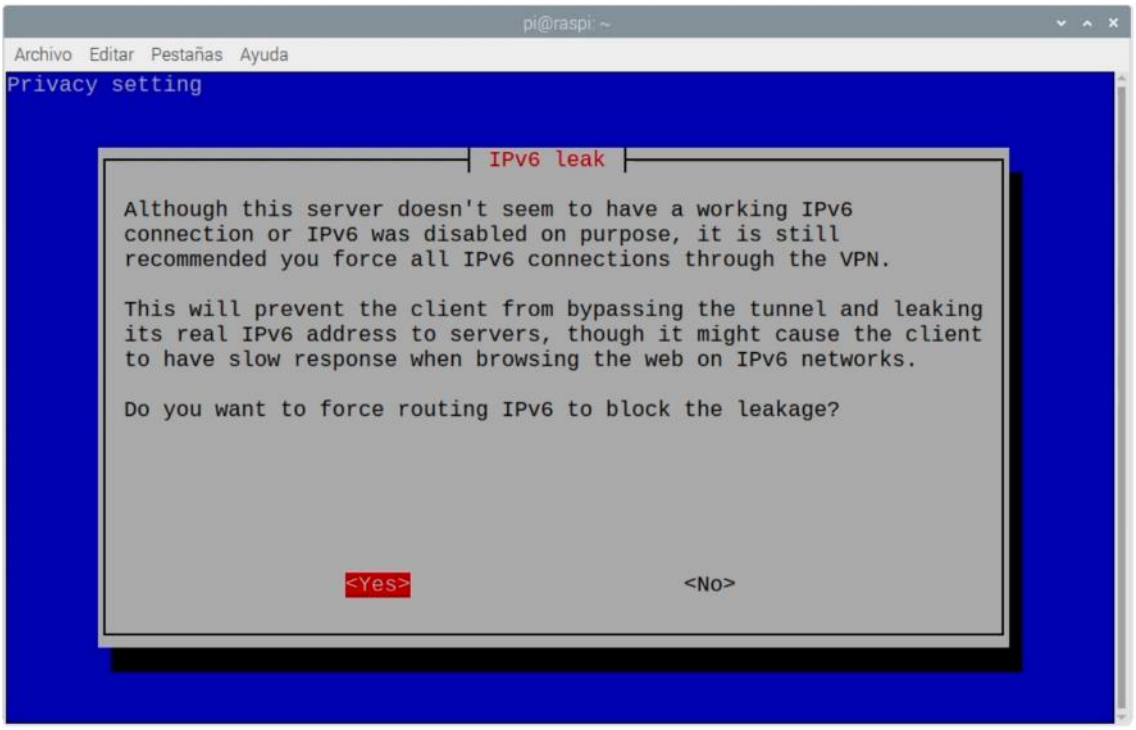
A continuación, en la ventana Initialing network interface (Static IP Needed).

“”The PiVPN is a SERVER so it needs a STATIC IP ADDRESS to function properly.
In the next section. you can choose to use your current network settings (DHCP) or to manually edit them.“”

“”El PiVPN es un SERVIDOR por lo que necesita una DIRECCIÓN IP ESTÁTICA para funcionar correctamente.
En la siguiente sección. puede optar por utilizar su configuración de red actual (DHCP) o editarla manualmente.“”

“”Se puede colocar una IP fija a la Raspberry PI, o se puede asignar a través de la MAC de la tarjeta de red/WIFI de la Raspberry Pi, una IP en el router de nuestro ISP si se tiene esa posibilidad””

Se pulsará INTRO al encontrarse seleccionado OK.



Ventana Privacy setting (IPv6 leak).

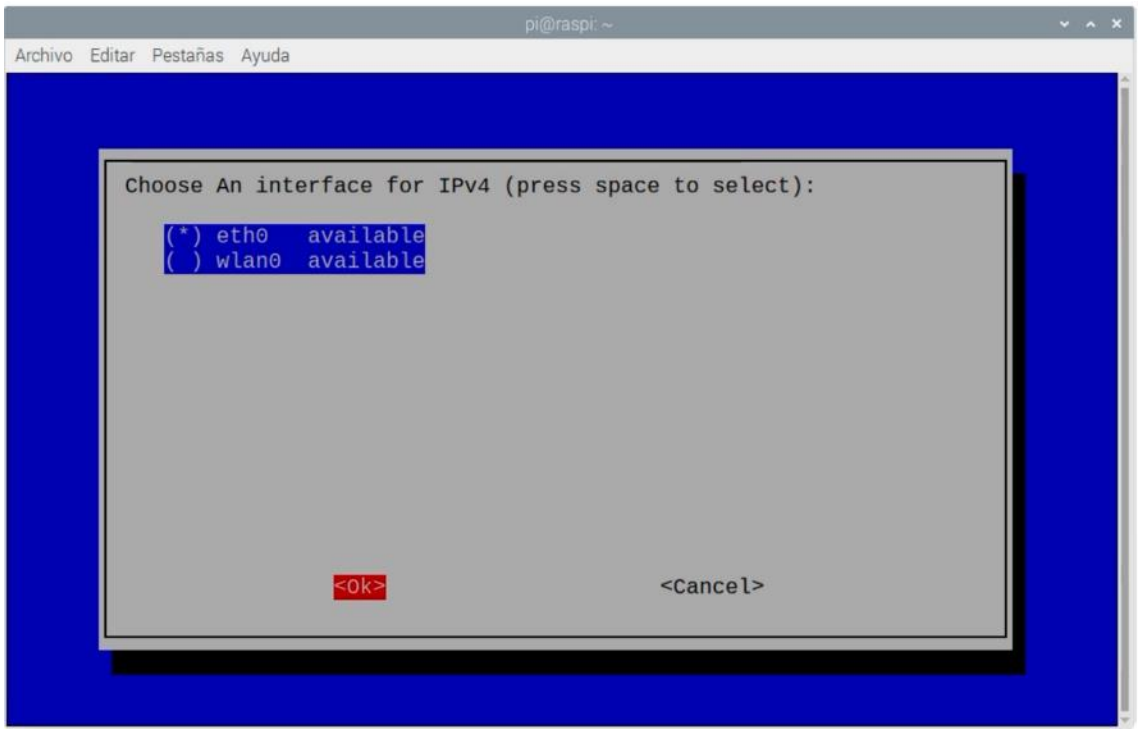
“”Although this server doesn`t seem to have a working IPV6 connection or IPv6 was disabled on purpose, it is still recommended you force all IPv6 connections through the VPN.
This will prevent the client from bypassing the tunnel and leaking its real IPv6 address to servers, though it might cause the client to have slow response when browsing the web on IPv6 networks.

Do you want to force routing IPv6 to block the leakage?“”

“”Aunque este servidor no parece tener una conexión IPV6 que funcione o IPv6 se deshabilitó a propósito, se recomienda forzar todas las conexiones IPv6 a través de la VPN.
Esto evitará que el cliente eluda el túnel y filtre su dirección IPv6 real a los servidores, aunque podría causar que el cliente tenga una respuesta lenta al navegar por la web en redes IPv6.

¿Quiere forzar el enrutamiento IPv6 para bloquear la fuga?“”

Se seleccionará Yes y se pulsará INTRO.



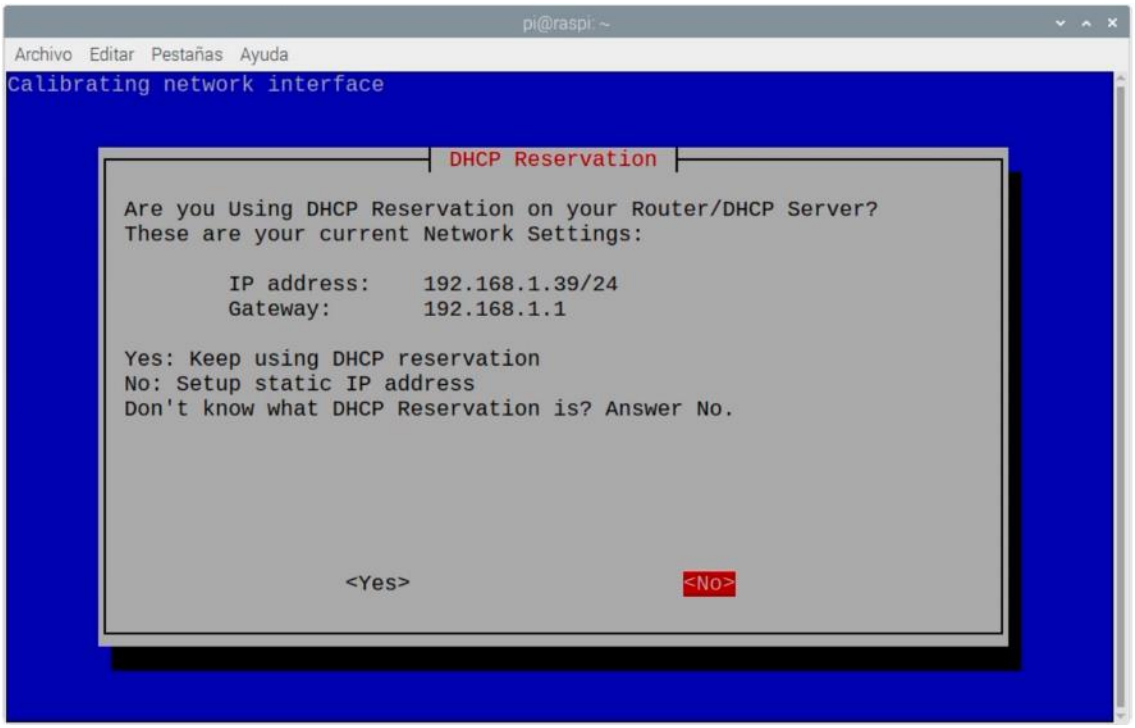
“”Choose An interface for IPv4 (press space to select):
(*) eth0 available
( ) wlan0 available””

“”Elija una interfaz para IPv4 (presione espacio para seleccionar):
(*) eth0 disponible
( ) wlan0 disponible“”

Se ha probado a realizar esta configuración tanto seleccionando eth0 (conexión Ethernet RJ45), como wlan0 (conexión a través de WIFI), en ambos casos el resultado es satisfactorio.

Para la realización de este proyecto, se selecciona la conexión eth0, conexión ethernet RJ45, pulsando la barra espaciadora para seleccionar la mencionada opción, para desplazarnos entre las opciones se pulsarán las teclas con los dibujos de las flechas de dirección (arriba, abajo, izquierda o derecha), la tecla tabuladora nos posiciona en la siguiente opción de selección (<OK> <- -> <Cancel>).

Posteriormente se seleccionará OK y se pulsará INTRO.



Ventana Calibrating network interface (DHCP Reservation).
“”Are you Using DHCP Reservation on your Router/DHCP Server?
These are your current Network Settings:

IP address: 192.168.1.61/24
Gateway: 192.168.1.1

Yes: Keep using DHCP reservation
No: Setup static IP address
Don`t know what DHCP Reservation is? Answer No.“”

“”¿Está utilizando la reserva DHCP en su enrutador/servidor DHCP?
Estas son sus configuraciones de red actuales:

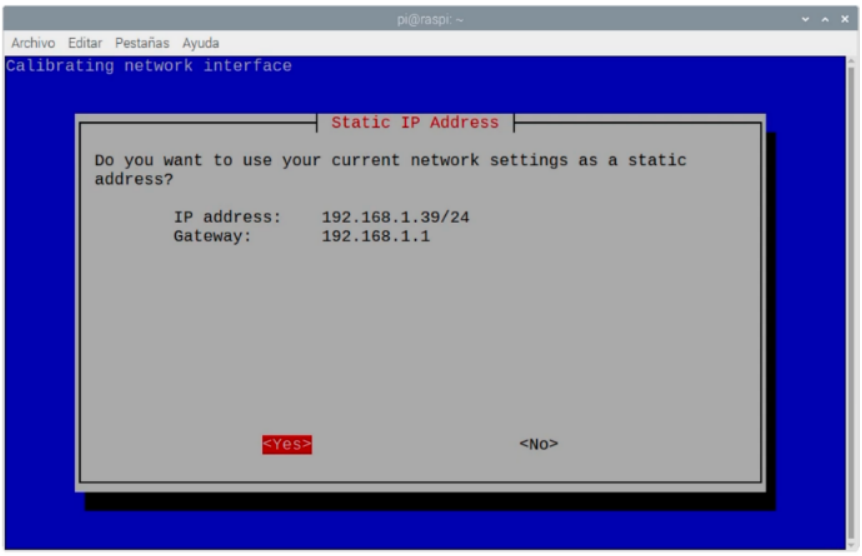
Dirección IP: 192.168.1.61/24
Puerta de enlace: 192.168.1.1

Sí: seguir usando la reserva de DHCP
No: Configurar dirección IP estática
¿No sabe qué es la reserva DHCP? respuesta no“”

Aclaración: Las IP que se muestran son facilitadas por un router como se puede tener en cualquier oficina o residencia, el cual tiene configurado y habilitado un servicio de DHCP, facilitando una dirección IP (IPv4) a cada dispositivo que se conecta para poder comunicarse con él y él con el resto de equipos o dispositivos en la red, en caso de tratarse de una pequeña red, no es necesario que sea la configuración de la dirección IP como la que se muestra en la captura superior, puede variar según la configuración de la que se disponga.

Aunque no se está utilizando reserva de IP, es decir, la Raspberry Pi adquiere una IP del router a través del servicio de DHCP, al encontrarse está conectada las 24 horas los 365 días del año, puesto que este dispositivo no consume casi, esta no pierde la IP que adquiere, la perdería si al encontrarse apagada al conectarse otro dispositivo se le facilitase la IP que tuviese la Raspberry Pi, con lo que se tendría que realizar ciertas modificaciones para que todo el proyecto volviese a funcionar.

Se seleccionará No y se pulsará INTRO.



Ventana Calibrating network interface (Static IP Address).

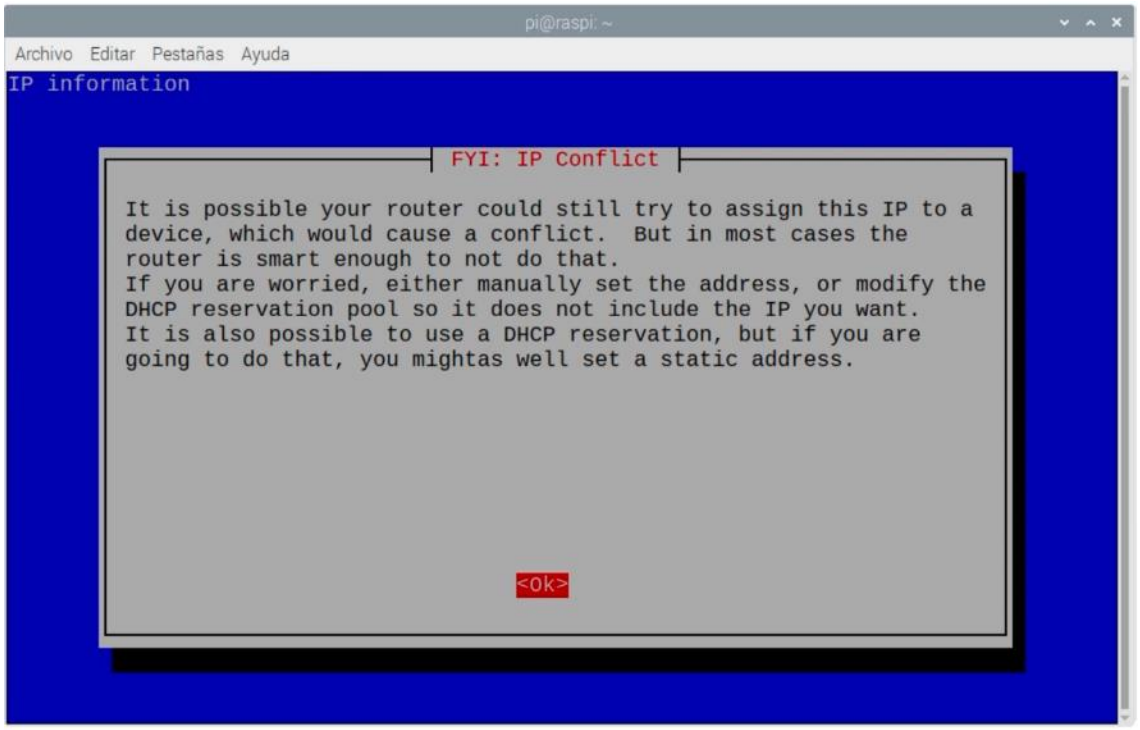
“”Do you want to use your current network settings as a static address?

IP adress: 192.168.1.61/24
Gateway: 192.168.1.1“”

“”¿Desea utilizar su configuración de red actual como una dirección estática?

Dirección IP: 192.168.1.61/24
Puerta de enlace: 192.168.1.1“”

Se seleccionará Yes y se pulsará INTRO.



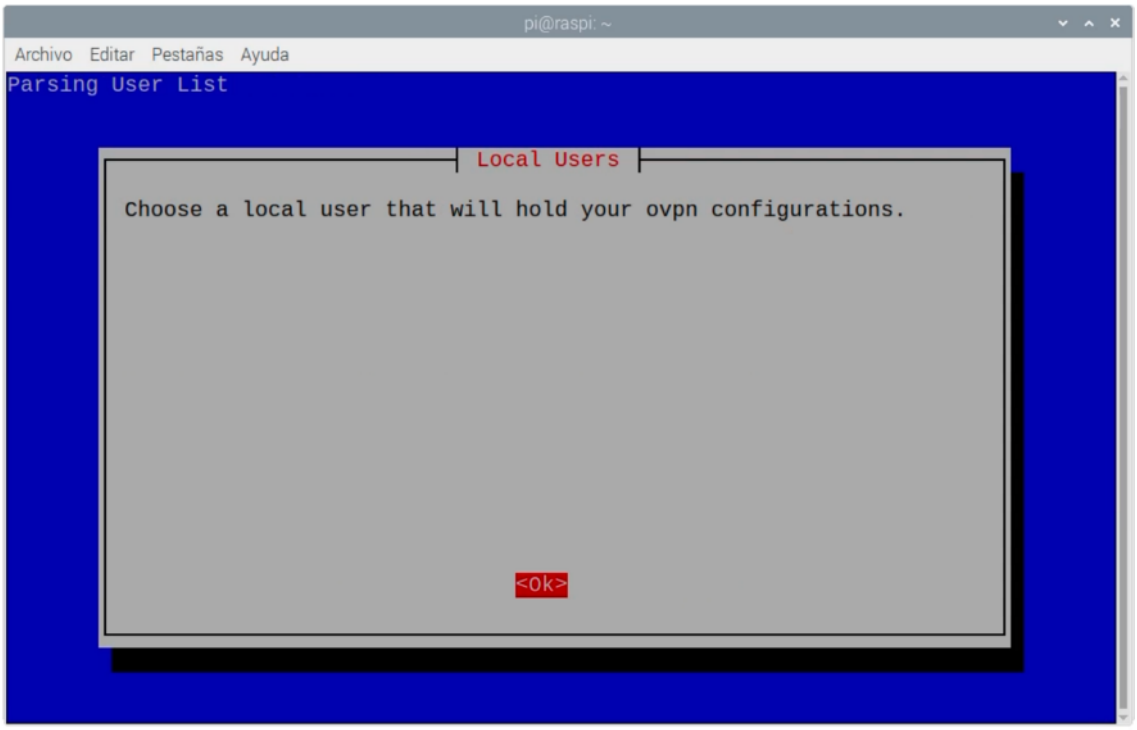
Ventana IP information (FYI: IP Conflict).

“”It is possible your router could still try to assign this IP to a device, which would cause a conflict. But in most cases the router is smart enough to not do that.
If you are worried, either manually set the address, or modify the DHCP reservation pool so it does not include the IP you want.
It is also possible to use a DHCP reservation, but if you are going to do that, you mightas well set a static address.“”

“”Es posible que su enrutador aún intente asignar esta IP a un dispositivo, lo que podría causar un conflicto. Pero en la mayoría de los casos, el enrutador es lo suficientemente inteligente como para no hacer eso.
Si está preocupado, configure manualmente la dirección o modifique el grupo de reservas de DHCP para que no incluya la IP que desea.
También es posible utilizar una reserva de DHCP, pero si va a hacerlo, también puede establecer una dirección estática. “”

Por la experiencia en la realización de la documentación de este proyecto y como se ha mencionado anteriormente, al encontrarse encendida la Raspberry Pi las 24 h., los 365 días del año, no se ha producido este problema.

En la realización de este proyecto, se pulsa INTRO al encontrarse seleccionado OK.

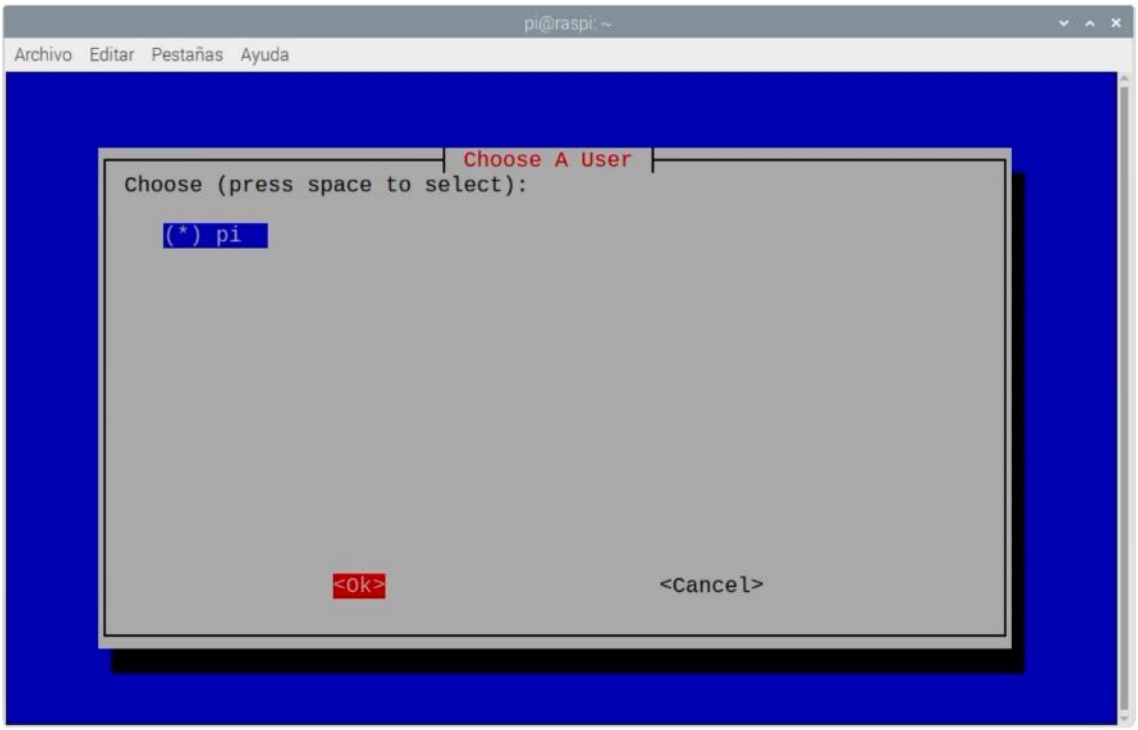


Ventana Parsing User List (Local Users).

“”Choose a local user that will hold your ovpn configurations.“”

“”Elija un usuario local que contendrá sus configuraciones de ovpn.“”

Se pulsará INTRO para seleccionar un usuario.

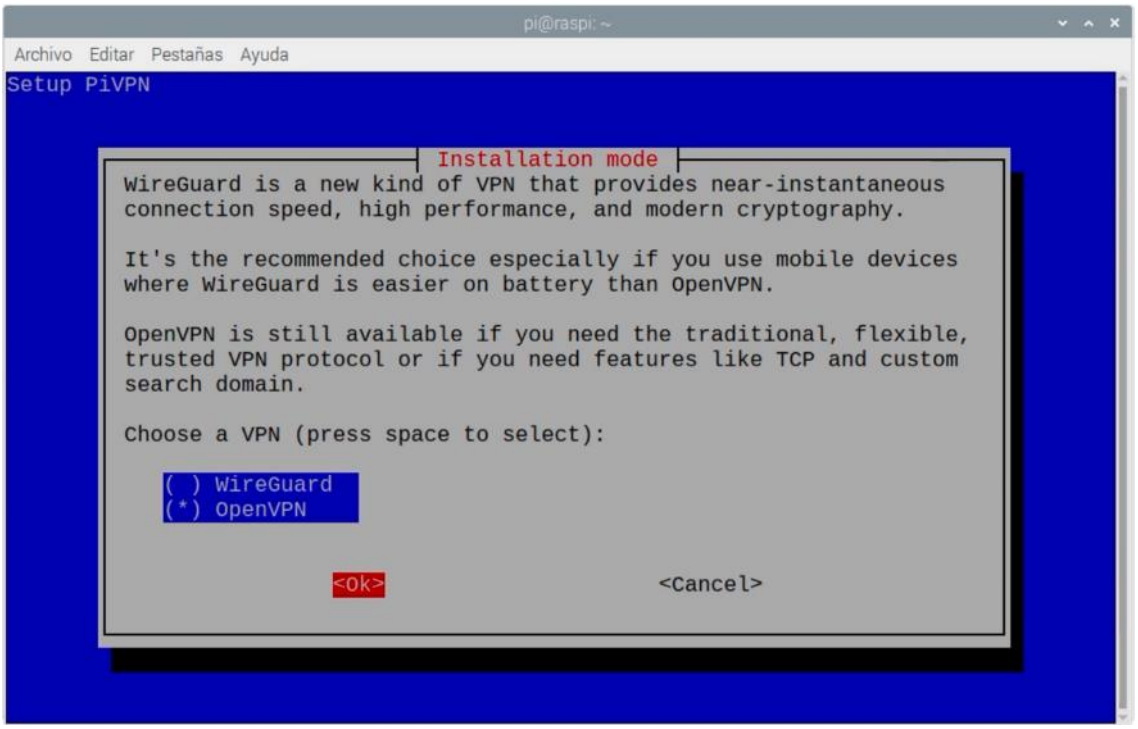


(Choose A User).

“”Choose (press space to select):
(*) pi””

“”Elija (presione espacio para seleccionar):
(*) Pi""

Para la realización de este proyecto, solo se dispone de un usuario, en este caso se trata del usuario por defecto “pi”, aunque modificada su contraseña, si se hubiese utilizado el comando adduser para añadir más usuarios, aparecerían más usuarios en la ventana de la captura superior, pudiendo seleccionar uno de ellos pulsando la tecla “barra espaciadora” y posteriormente se seleccionaría Ok y se pulsaría INTRO.

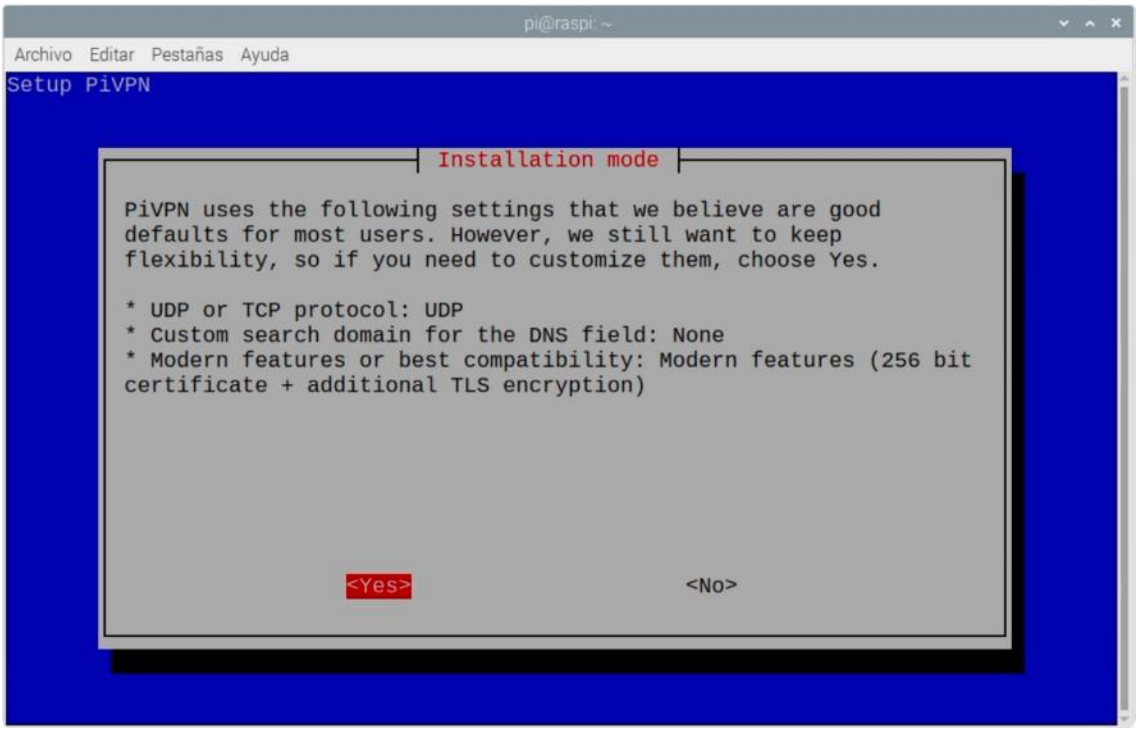


Ventana Setup PiVPN (Installation mode).

“”WireGuard is a new kind of VPN that provides near-instantaneous connection speed, high performance, and modern cryptography.
It's the recommended choise especially if you use mobile devices WireGuard is easier on battery than OpenVPN.
OpenVPN is still available if you need the traditional, flexible, trusted VPN protocol or if you need features like TCP and custom search domain.
Choose a VPN (press space to select):“”

“”WireGuard es un nuevo tipo de VPN que proporciona una velocidad de conexión casi instantánea, alto rendimiento y criptografía moderna.
Es la opción recomendada, especialmente si usa dispositivos móviles. WireGuard es más fácil con la batería que OpenVPN.
OpenVPN todavía está disponible si necesita el protocolo VPN tradicional, flexible y confiable o si necesita funciones como TCP y un dominio de búsqueda personalizado.
Elija una VPN (presione espacio para seleccionar):“”

Nuevamente, para la realización de este proyecto, y aunque la configuración no difiere mucho se selecciona OpenVPN y tras seleccionar Ok se pulsa INTRO.



Ventana Setup PiVPN (Installation mode).

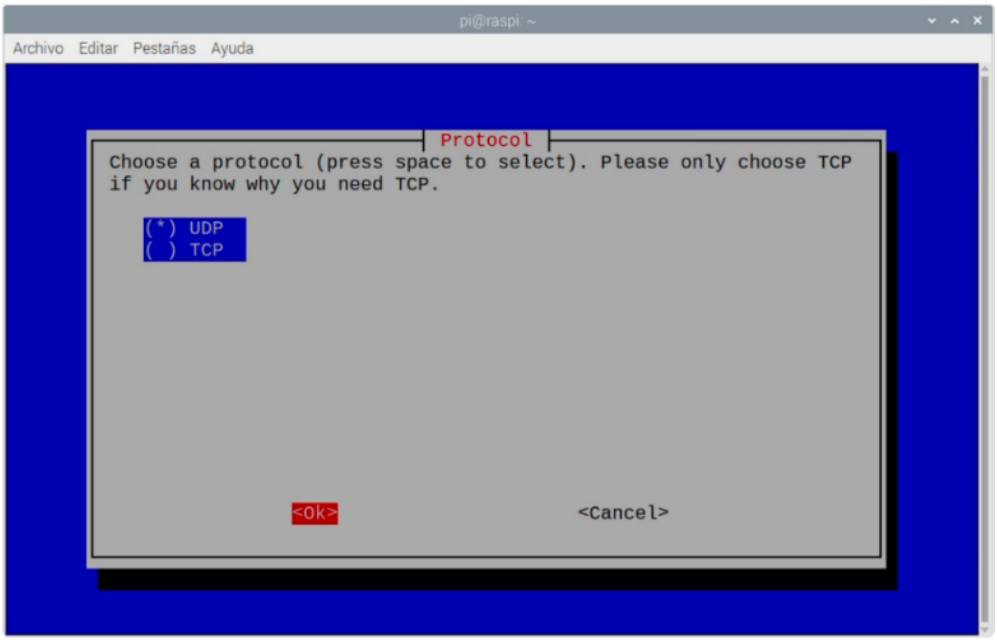
“”PiVPN uses the following settings that we believe are good defaults for most users. However, we still want to keep flexibility, so if you need to customize them, choose Yes.

* UDP or TCP protocol: UDP
* Custom search domain for the DNS field: None
* Modern features or best compatibility: Modern features (256 bit certificate + additional TL5 encryption)“”

“”PiVPN usa las siguientes configuraciones que creemos que son buenos valores predeterminados para la mayoría de los usuarios. Sin embargo, aún queremos mantener la flexibilidad, por lo que, si necesita personalizarlos, elija Sí.

* Protocolo UDP o TCP: UDP
* Dominio de búsqueda personalizado para el campo DNS: Ninguno
* Funciones modernas o mejor compatibilidad: Funciones modernas (certificado de 256 bits + cifrado TL5 adicional)“”

Se seleccionará Yes y se pulsará INTRO.



Ventana (Protocol).

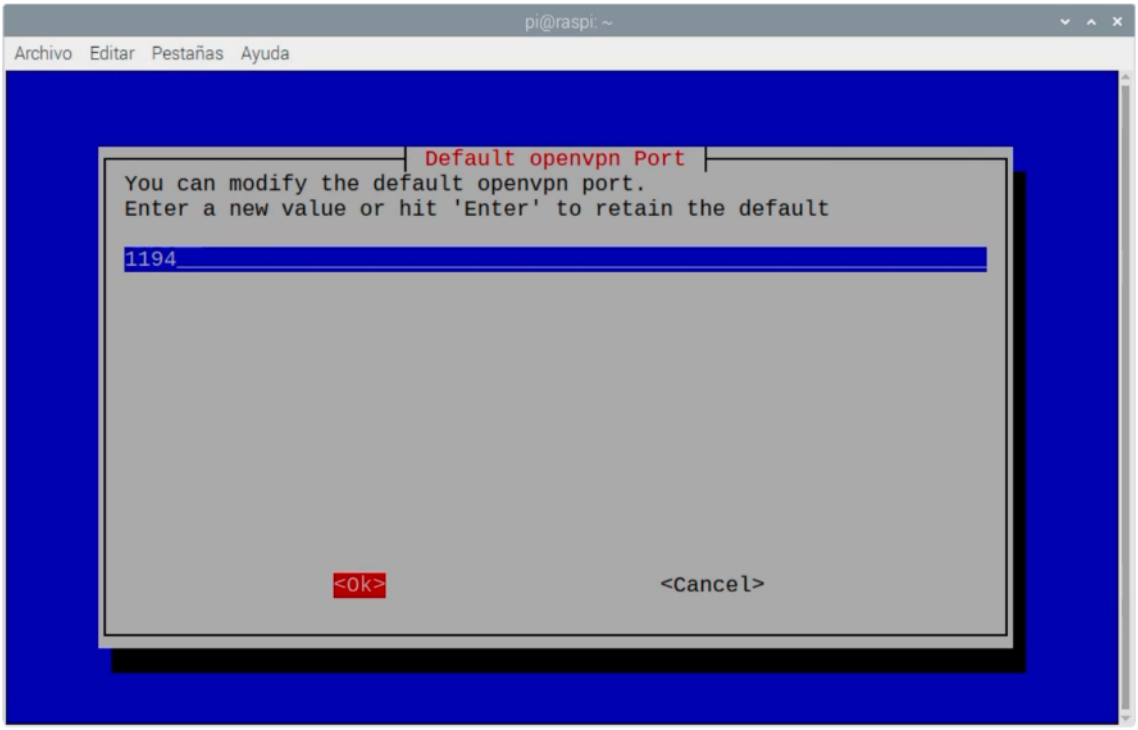
“”Choose a protocol (press space to select). Please only choose TCP if you know why you need TCP.
(*) UDP
( ) TCP“”

“”Elija un protocolo (presione espacio para seleccionar). Elija TCP solo si sabe por qué necesita TCP.
(*) UDP
( ) TCP “”

Se deja seleccionado el protocolo UDP y se pulsa INTRO.

En principio, y desde que uso este servidor VPN, no se ha tenido ningún tipo de problema con la configuración que se está proporcionando.

En caso de modificar el número del puerto por defecto (UDP/1194), se apuntará para modificar la apertura de puerto en el router y si es necesario habilitar el tráfico en el cortafuegos, se tendrá que tomar nota de los puertos que se modifiquen para como se ha indicado, abrir los puertos en el router y habilitar el tráfico en el cortafuegos.



Ventana (Default openvpn port).

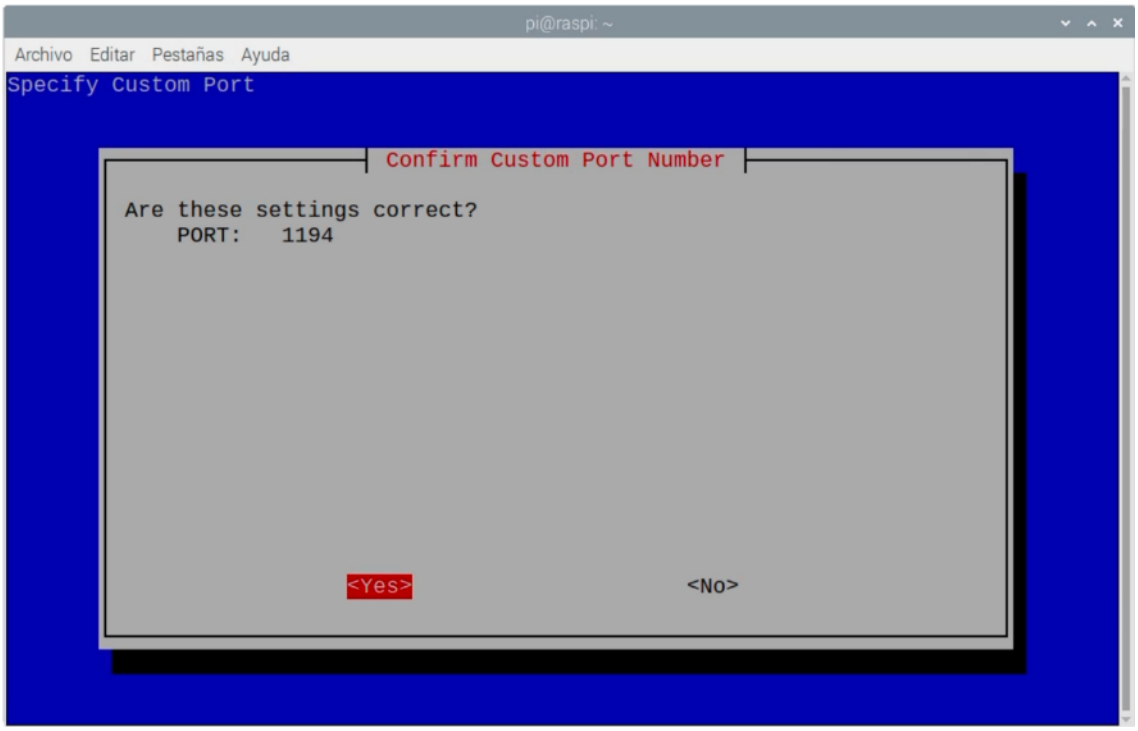
“”You can modify the default openvpn port.
Enter a new value or hit 'ENTER' to retain the default.“”

“”Puede modificar el puerto openvpn predeterminado.
Ingrese un nuevo valor o presione 'ENTER' para conservar el valor predeterminado.“”

Al haber elegido el protocolo UDP se nos indica el puerto 1194.
Si se hubiese elegido TCP se sugeriría el 443.

Estos números de puerto, se pueden modificar, para la realización de este proyecto se deja el protocolo UDP y el número de puerto 1194.

En caso de modificar el número del puerto por defecto (UDP/1194), se apuntará para modificar la apertura de puerto en el router y si es necesario habilitar el tráfico en el cortafuegos.

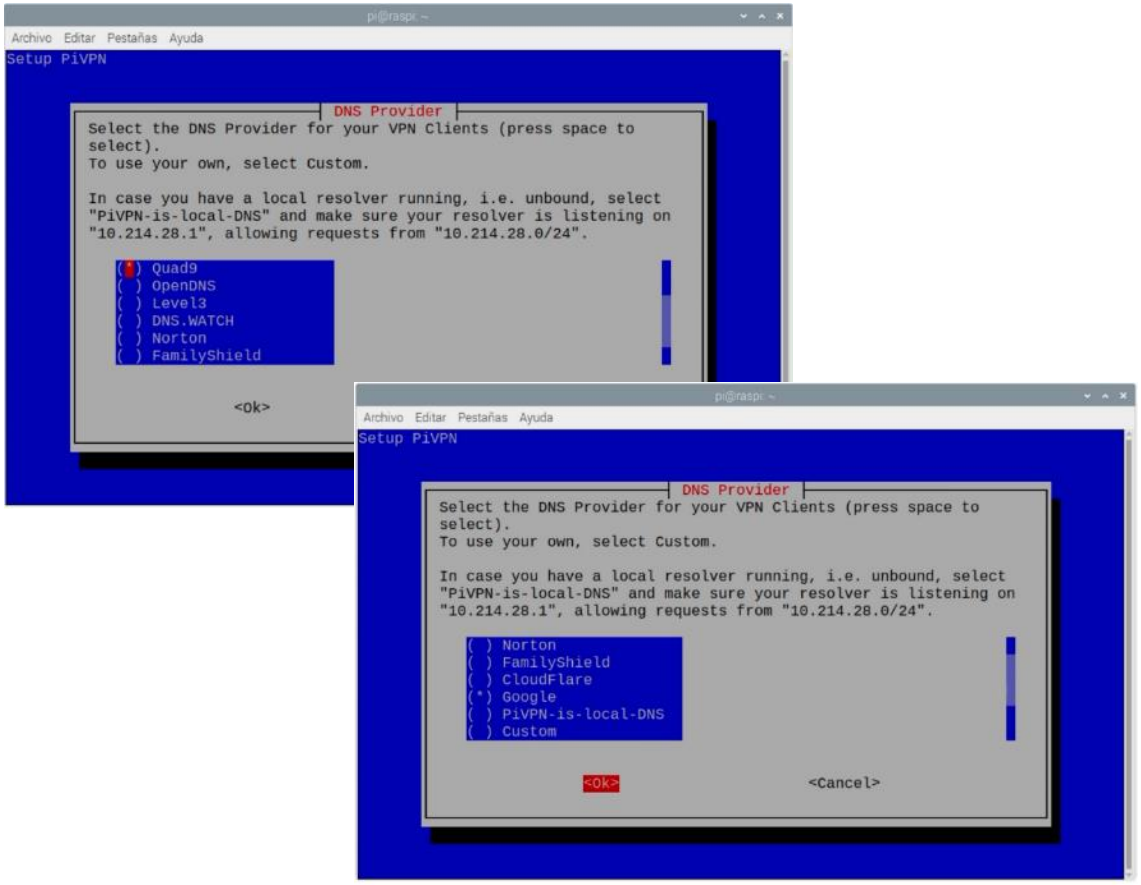


Ventana (Confirm Custom Port Number).

“”Are these settings correct?
PORT: 1194””

“”¿Son correctas estas configuraciones?
PUERTO: 1194””

Se seleccionará Yes y se pulsará INTRO.



Ventana Setup PiVPN (DNS Provider).

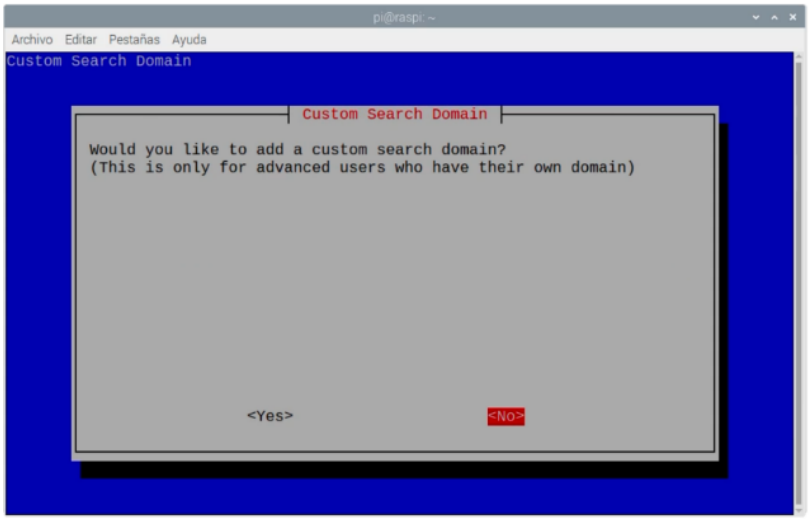
“”Select the DNS Provider for your VPN Clients (press space to select).
To use your own, select Custom.

In case you a local resolver running. i.e. unbound, select "PiVPN-is-local-DNS" and make sure your resolver is listening on "10.198.83.1", allowing requests from "10.198.83.0/24".””

“”Seleccione el proveedor de DNS para sus clientes VPN (presione espacio para seleccionar).
Para usar uno propio, seleccione Personalizado.

En caso de que se esté ejecutando un solucionador local. es decir, sin vincular, seleccione "PiVPN-is-local-DNS" y asegúrese de que su resolución esté escuchando en "10.198.83.1", permitiendo solicitudes de "10.198.83.0/24".“”

En este caso como proveedor de DNS se selecciona Google, y se pulsara INTRO si se encuentra seleccionado Ok.

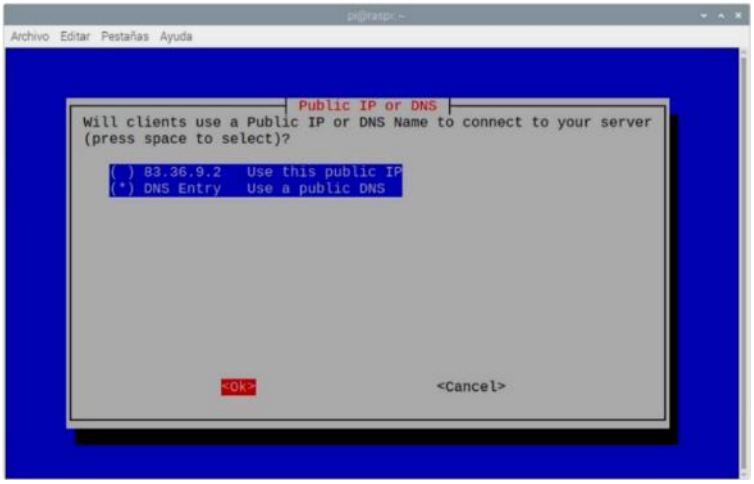


Ventana (Custom Search Domain).

“”Would you like to add a custom search?
(This is only for advanced users who have their own domain)“”

“”¿Le gustaría agregar una búsqueda personalizada?
(Esto es solo para usuarios avanzados que tienen su propio dominio)“”

Para este proyecto se selecciona NO y se pulsa INTRO.



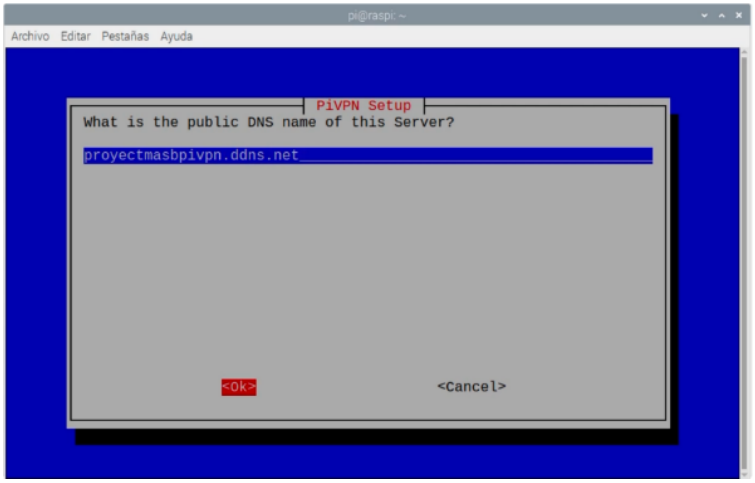
Ventana (Public IP or DNS).

“”Will clients use a public IP or DNS Name to connect to your server (press space to select)?“”

“”¿Usarán los clientes una IP pública o un nombre DNS para conectarse a su servidor (presione la barra espaciadora para seleccionar)?“”

Como nombre de dominio, se utiliza el nombre de dominio o host creado en No-IP, que más adelante se explicará para que sirve, en este caso, se escribirá el nombre de host que corresponde a: proyectmasbpivpn.ddns.net

Se selecciona DNS Entry Use a public DNS y se pulsará INTRO.



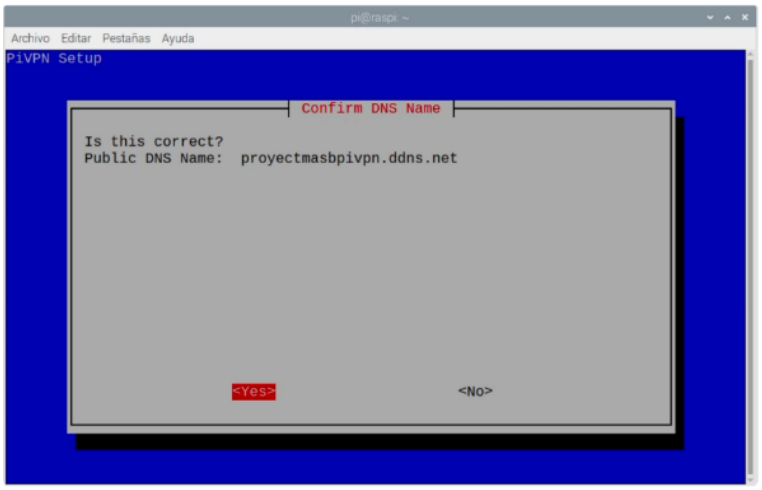
Ventana (PiVPN Setup).

“”What is the public DNS name of this Server?“”

“”¿Cuál es el nombre DNS público de este servidor?“”

Se proporciona como nombre DNS público: proyectmasbpivpn.ddns.net

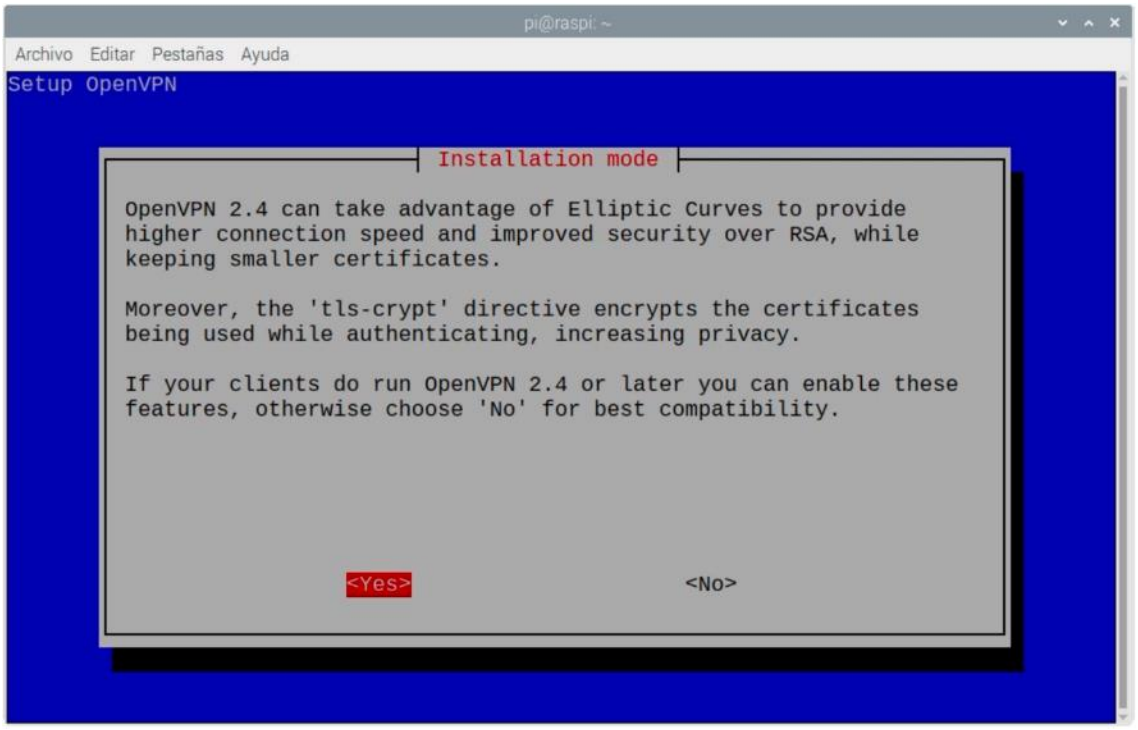
Se seleccionará OK y se pulsa INTRO.



Ventana PiVPN Setup (Confirm DNS Name).
“”Is this correct?
Public DNS Name: proyectmasbpivpn.ddns.net””

“”¿Es esto correcto?
Nombre DNS público: proyectmasbpivpn.ddns.net “”

Se seleccionará Yes y se pulsará INTRO.



Ventana: Setup OpenVPN (Installation mode)

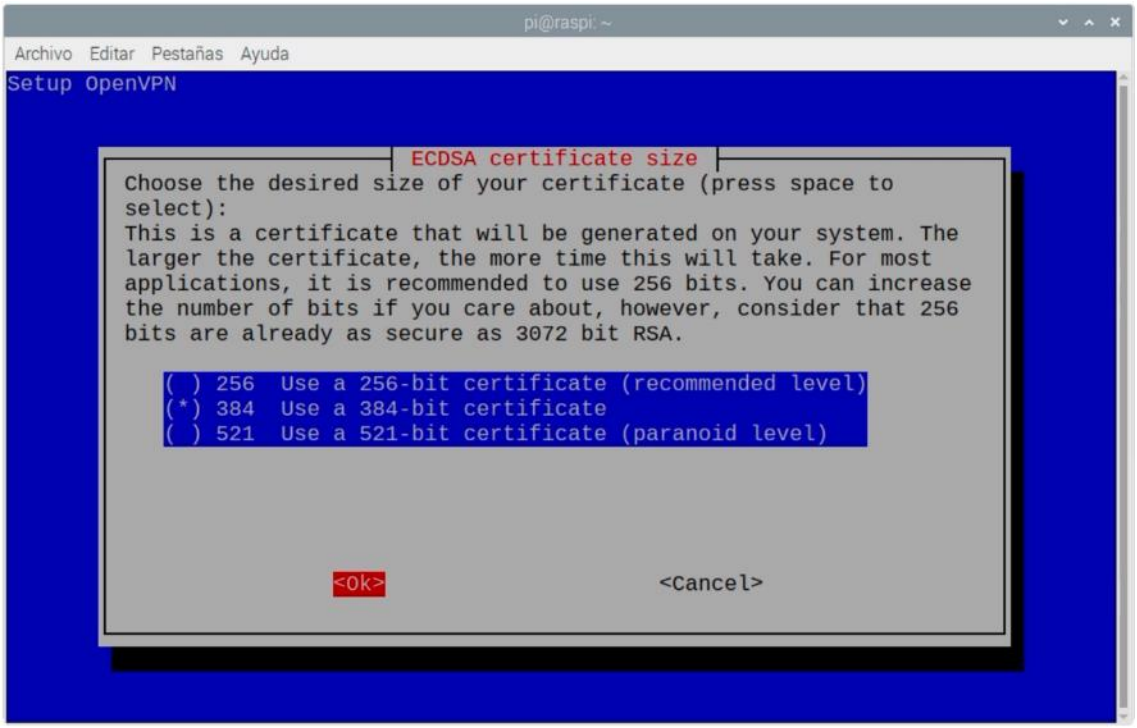
“”OpenVPN 2.4 can take advantage of Eliptic Curves to provide higher connection speed and improved security over RSA, while keeping smaller certificates.

Moreover, the 'tls-crypt' directive encrypts the certificates being used while authenticating, increasing privacy.
If your clients do run OpenVPN 2.4 or later you can enable these features, otherwise choose 'No' for best compatibility.“”

“”OpenVPN 2.4 puede aprovechar Eliptic Curves para proporcionar una mayor velocidad de conexión y una seguridad mejorada sobre RSA, manteniendo certificados más pequeños.

Además, la directiva 'tls-crypt' cifra los certificados que se utilizan durante la autenticación, lo que aumenta la privacidad.
Si sus clientes ejecutan OpenVPN 2.4 o posterior, puede habilitar estas funciones; de lo contrario, elija 'No' para obtener la mejor compatibilidad.””

Se seleccionará Yes y se pulsará INTRO.



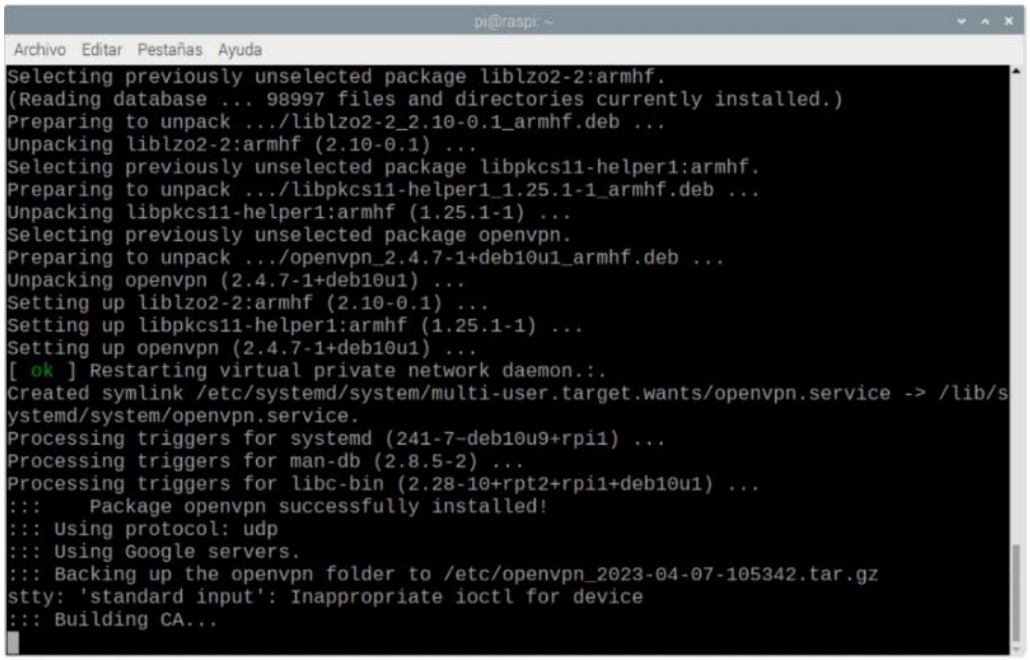
Ventana Setup OpenVPN (ECDSA certificate size).

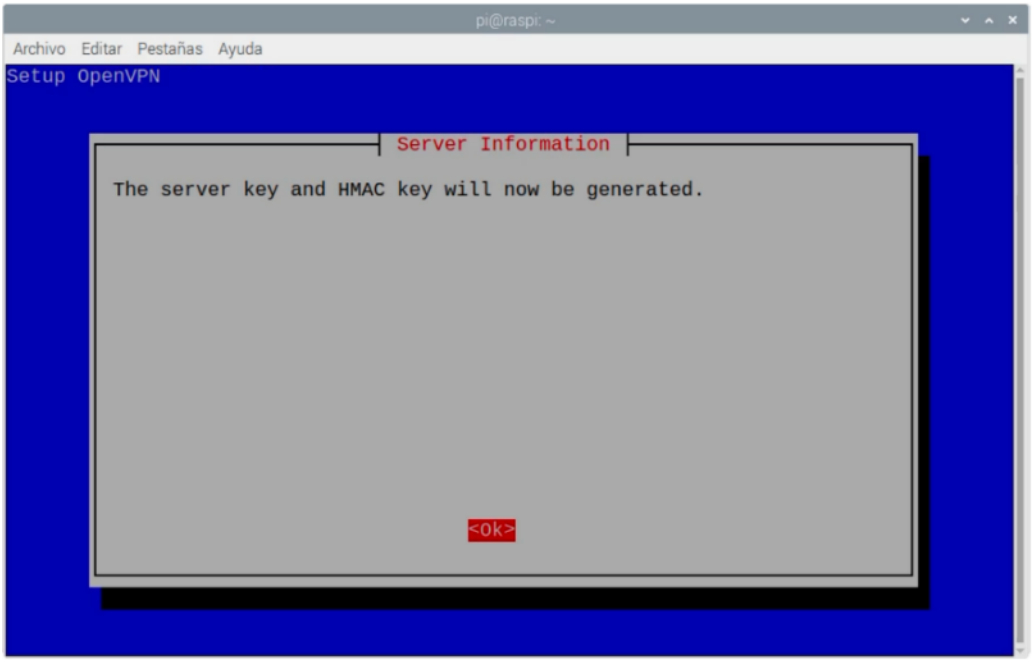
“”Choose the desired size of your certificate (press space to selectet):
This is a certificate that will be generated on your system. The larger the certificate, the more time this will take. For most applicatons, it is recommended to use 256 bits. You can increase the number of bits if you care about, however, consider that 256 bits are already as secure as 3072 bit RSA.””

“”Elija el tamaño deseado de su certificado (presione espacio para seleccionar):
Este es un certificado que se generará en su sistema. Cuanto más grande sea el certificado, más tiempo llevará. Para la mayoría de las aplicaciones, se recomienda utilizar 256 bits. Puede aumentar la cantidad de bits si lo desea, sin embargo, tenga en cuenta que 256 bits ya son tan seguros como RSA de 3072 bits.“”

Se ha probado con la opción correspondiente a 256 bit y con la de 384 bit sin ningún problema, para este proyecto, se selecciona la opción intermedia 384 bit.

Posteriormente se selecciona Ok y se pulsa INTRO.



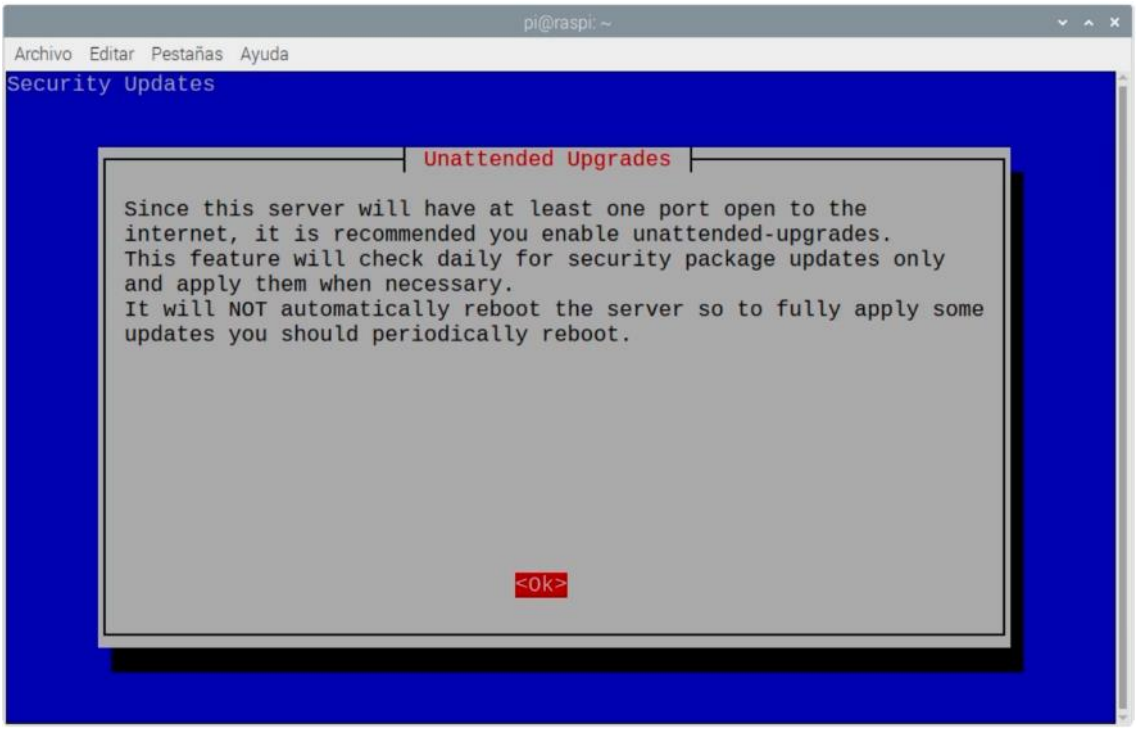


Ventana Setup OpenVPN (Server Information).

“”The server Key and HMAC Key will now be generated.””

“”La clave del servidor y la clave HMAC ahora se generarán.””

Se selecciona OK y se pulsa INTRO.

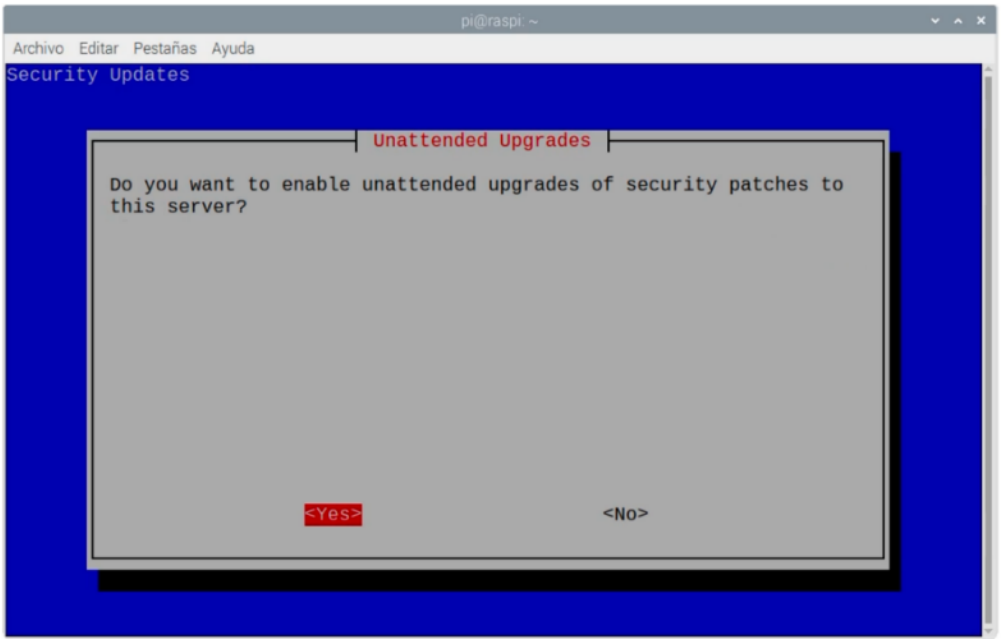


Ventana Security Updates (Unattended Upgrades).

“”Since this server will have at least one port open to the internet, it is recommended you enable unattended-upgrades.
This feature will check daily for security package updates only and apply them when necesary.
It will NOT automatically reboot the server so to fully apply some updates you should periodically reboot.“”

“”Dado que este servidor tendrá al menos un puerto abierto a Internet, se recomienda habilitar las actualizaciones desatendidas.
Esta característica verificará diariamente solo las actualizaciones del paquete de seguridad y las aplicará cuando sea necesario.
NO reiniciará automáticamente el servidor, por lo que, para aplicar completamente algunas actualizaciones, debe reiniciar periódicamente.“”

En la elaboración de este proyecto se selecciona OK y se pulsa INTRO.

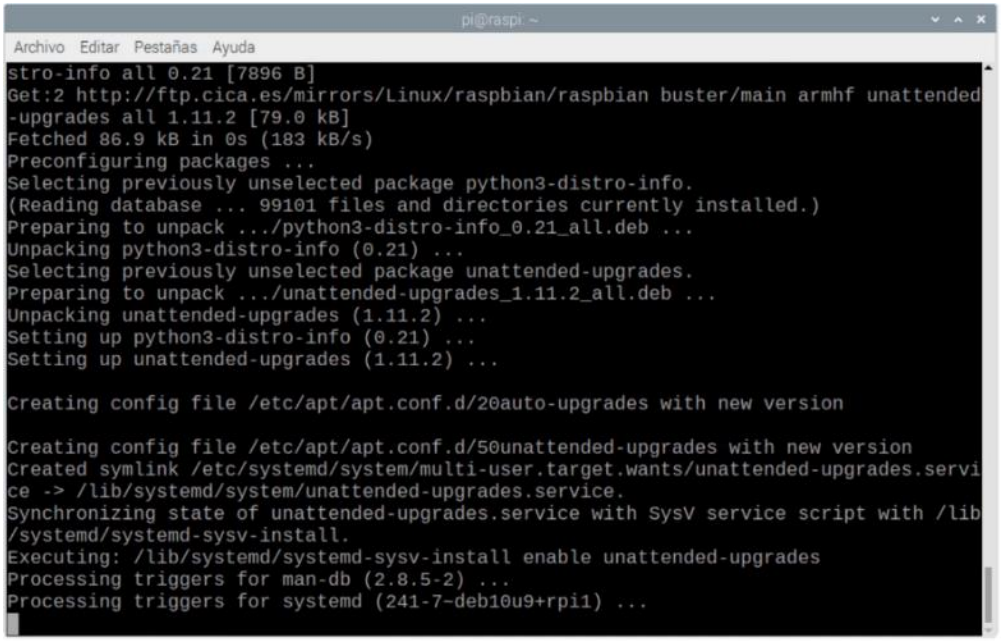


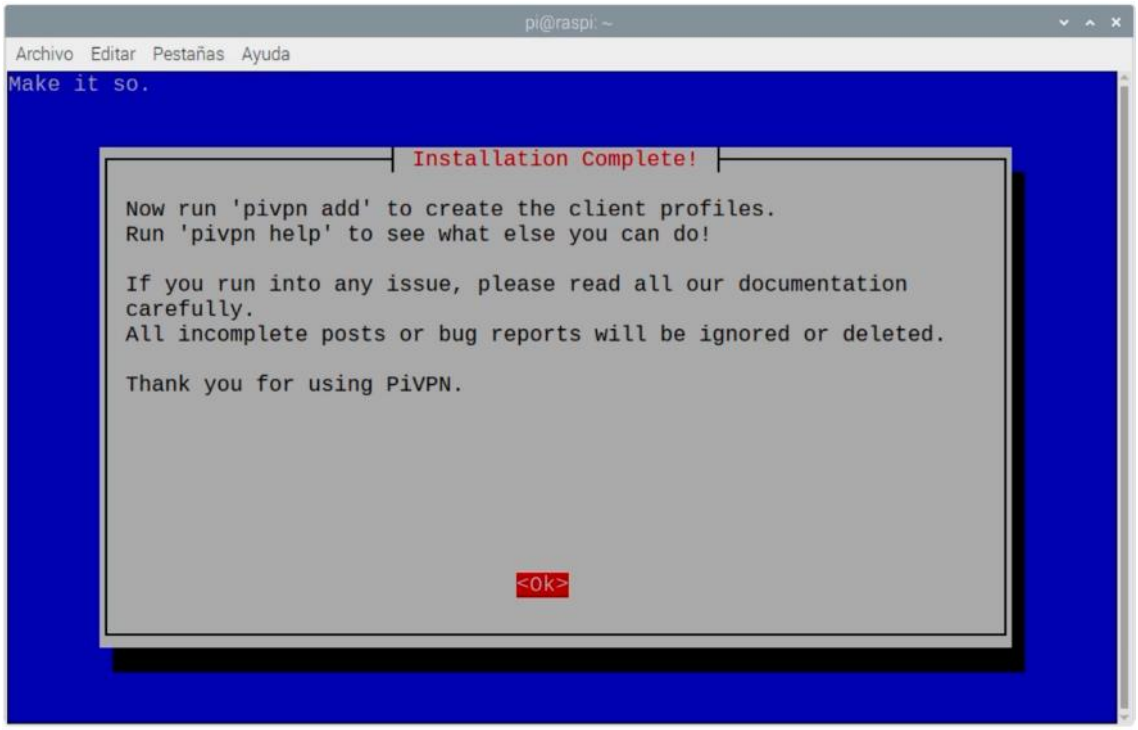
Ventana Security Updates (Unattended Upgrades).

“”Do you want to enable unattended upgrades of security patches to this server?“”

“”¿Desea habilitar actualizaciones desatendidas de parches de seguridad para este servidor?“”

En esta ventana, en la que se informa sobre las actualizaciones de seguridad, se selecciona Yes y se pulsa INTRO.





Ventana Make it so (Installation Complete!).

“”Now run ‘pivpn add’ to create the client profiles.
Run ‘pivpn help’ to see what else you can do!

If you run into any issue, please read all our documentation carefully
All incomplete posts or bug reports will be ignored or deleted.

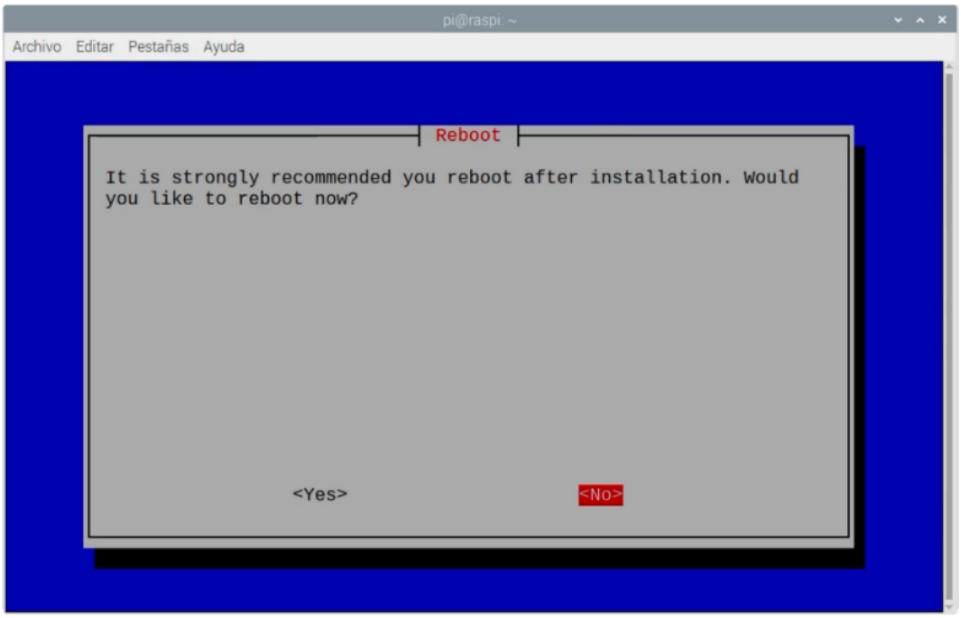
Thank you for using PiVPN””

“”Ahora ejecute 'pivpn add' para crear los perfiles de cliente.
¡Ejecute 'pivpn help' para ver qué más puede hacer!

Si tiene algún problema, lea atentamente toda nuestra documentación.
Todas las publicaciones incompletas o informes de errores serán ignorados o eliminados.

Gracias por usar PiVPN“”

Al encontrarse seleccionada la opción OK, se pulsa INTRO.



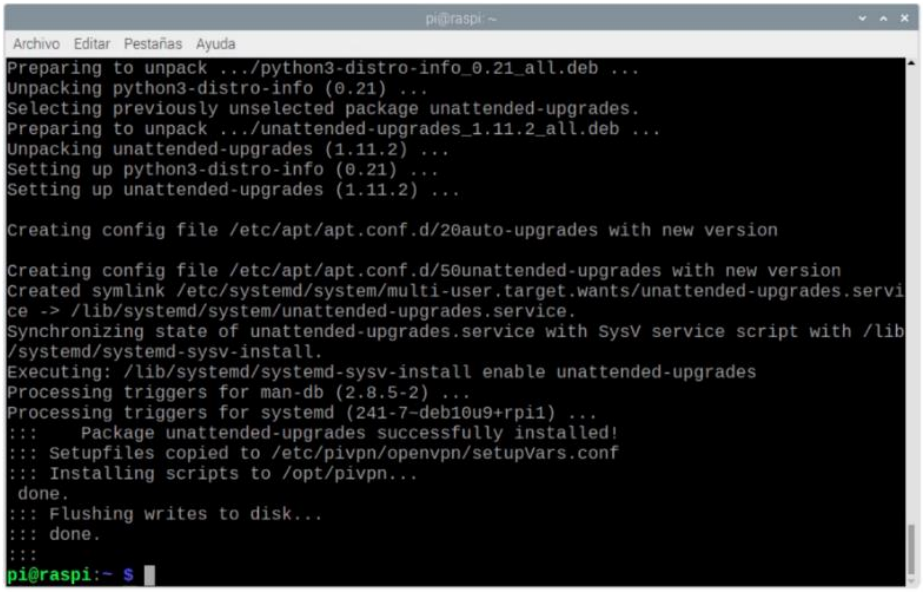
Ventana Reboot.

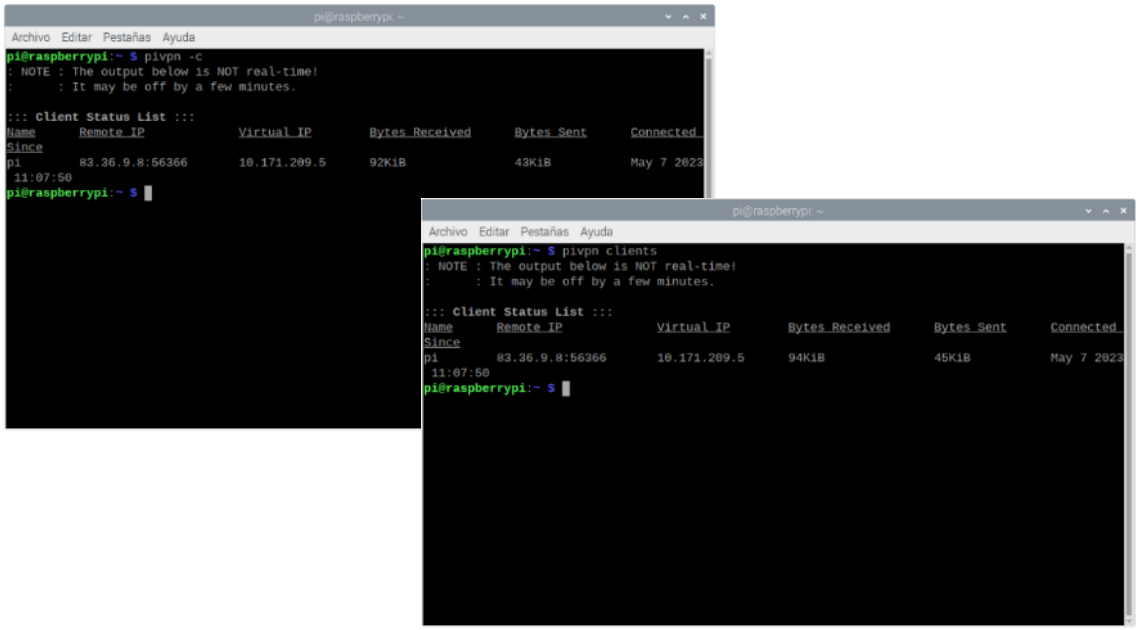
“”It is strongly recommended you reboot after installation. Would you like to reboot now?“”

“”Se recomienda encarecidamente que reinicie después de la instalación. ¿Le gustaría reiniciar ahora?""

Se selecciona Yes para realizar el reinicio de la Raspberry Pi.

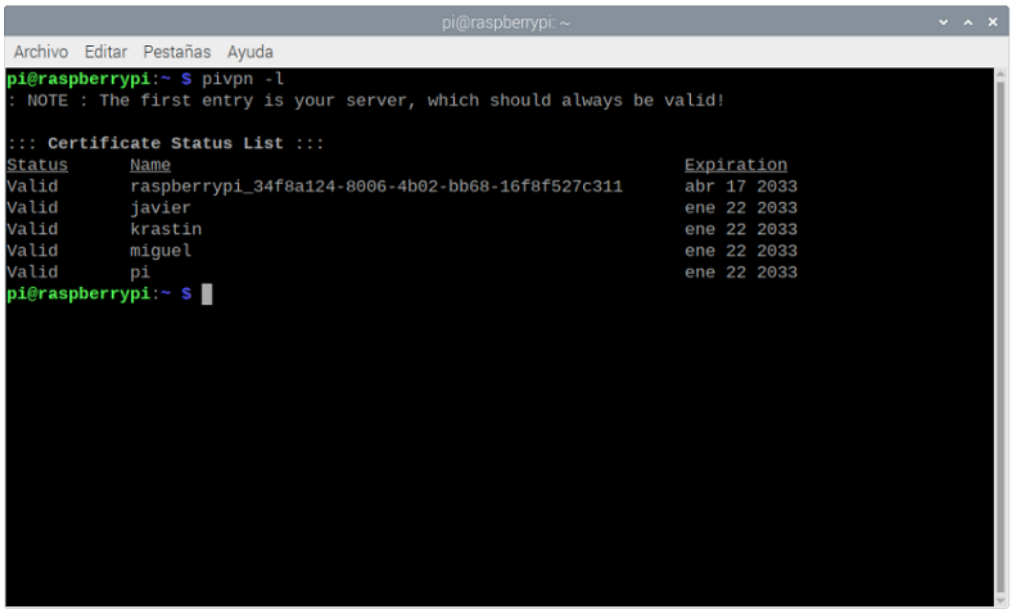
En todas las instalaciones de prueba, la opción por defecto ha sido siempre No, aunque como se indica es necesario el reinicio.





Terminada la instalación de PiVPN y tras la creación de los usuarios con el comando pivpn add, se podrá comprobar los usuarios conectados al servidor VPN/WOL, con los comandos.

pivpn -c
pivpn clients



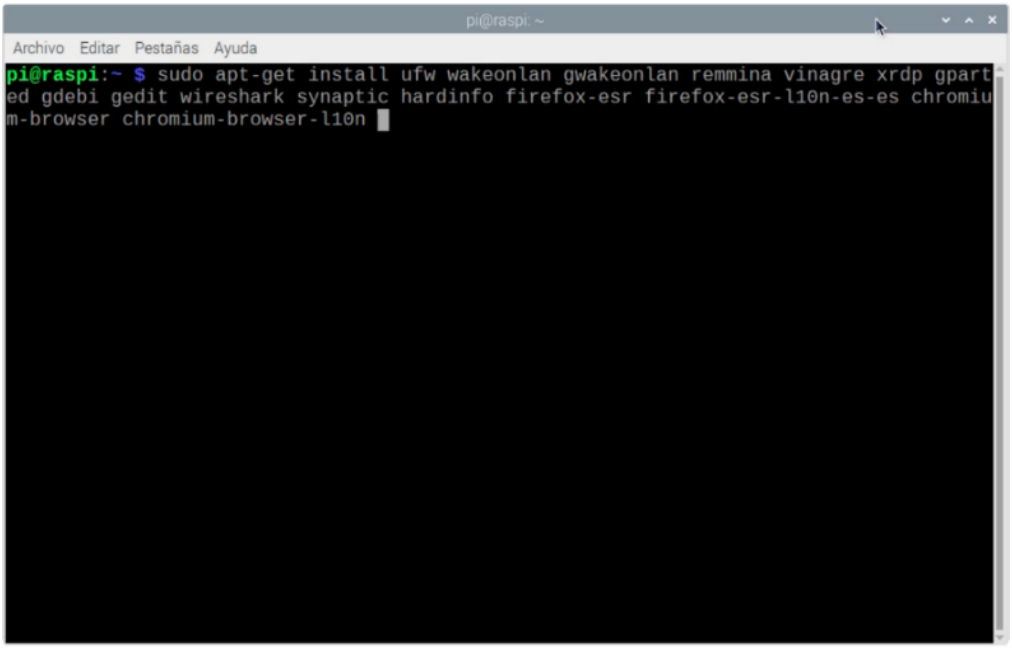
Para comprobar cómo se encuentran los usuarios creados se tendrá que utilizar el comando.

pivpn -l

Instalación aplicaciones necesarias a través de terminal en local.

No es necesario realizar la instalación de todas las aplicaciones que aquí se indican, como por ejemplo gparted, wireshark, synaptic, firefox y chromium.

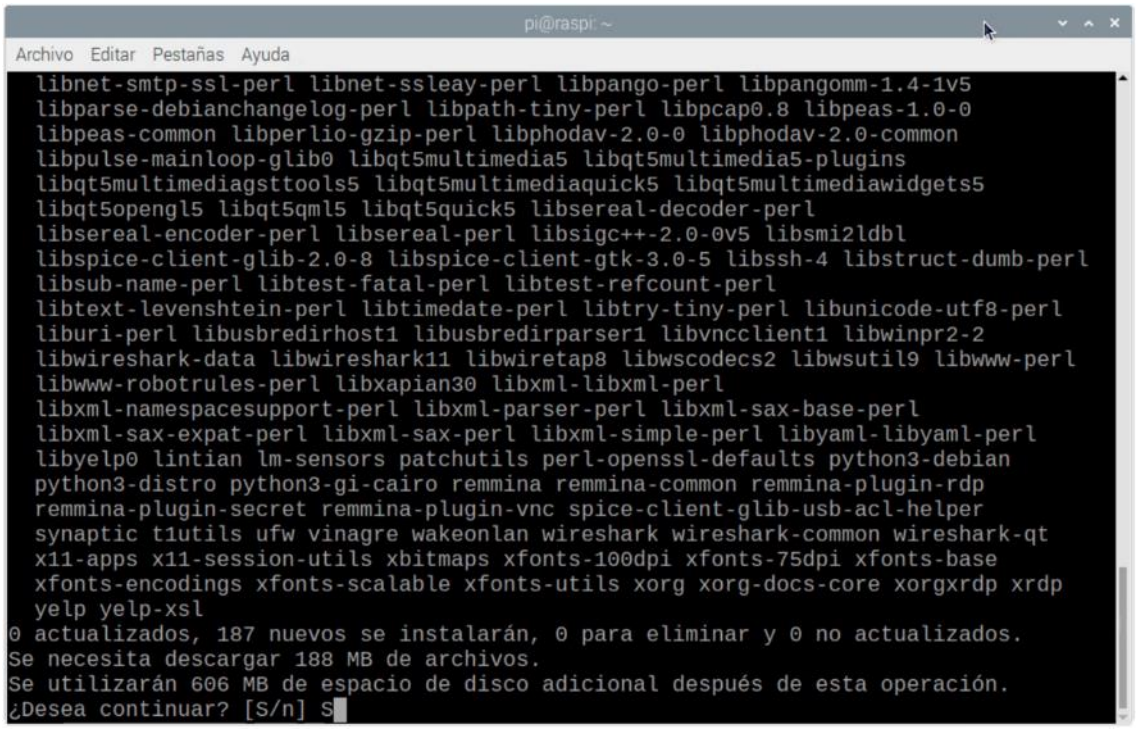
Dependiendo de las aplicaciones que se instalen, esta instalación durara más o menos tiempo puesto que también se tendrán que instalar todas las dependencias necesarias de todas las aplicaciones a instalar.



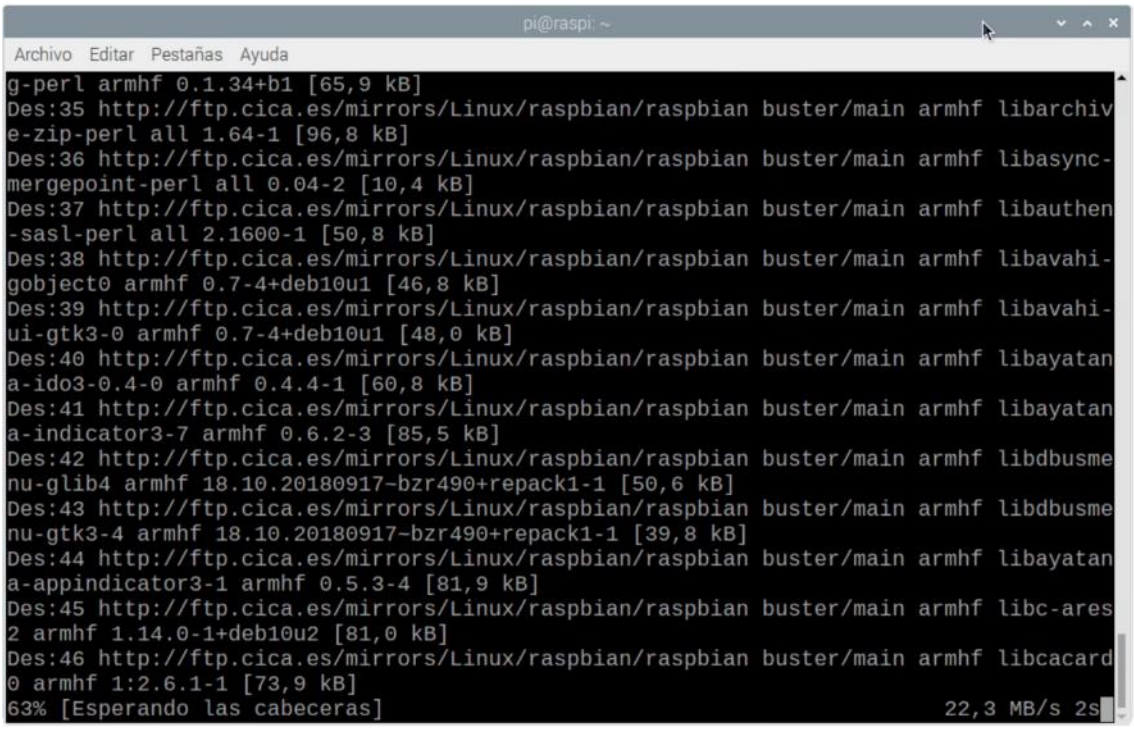
Para este proyecto, se realiza la instalación de ciertas aplicaciones y otras utilizadas por ejemplo para realizar las capturas de pantalla o la realización de capturas en video, las aplicaciones imprescindibles para este proyecto en el servidor se instalan con el comando.

sudo apt-get install ufw wakeonlan gwakeonlan remmina vinagre xrdp gparted gdebi gedit wireshark synaptic hardinfo firefox-esr firefox-esr-l10n-es-es chromium-browser chromium-browser-l10n

Las aplicaciones opnssh-server, openssh-client, real-vnc-server y real-vnc-viewer, no serían necesarias instalarlas puesto que al realizar la configuración de la Raspberry Pi y haber seleccionado o habilitar SSH y VNC, ya se instala o se habilita en el S.O., no siendo necesaria ya su instalación, aun así, se pueden instalar.



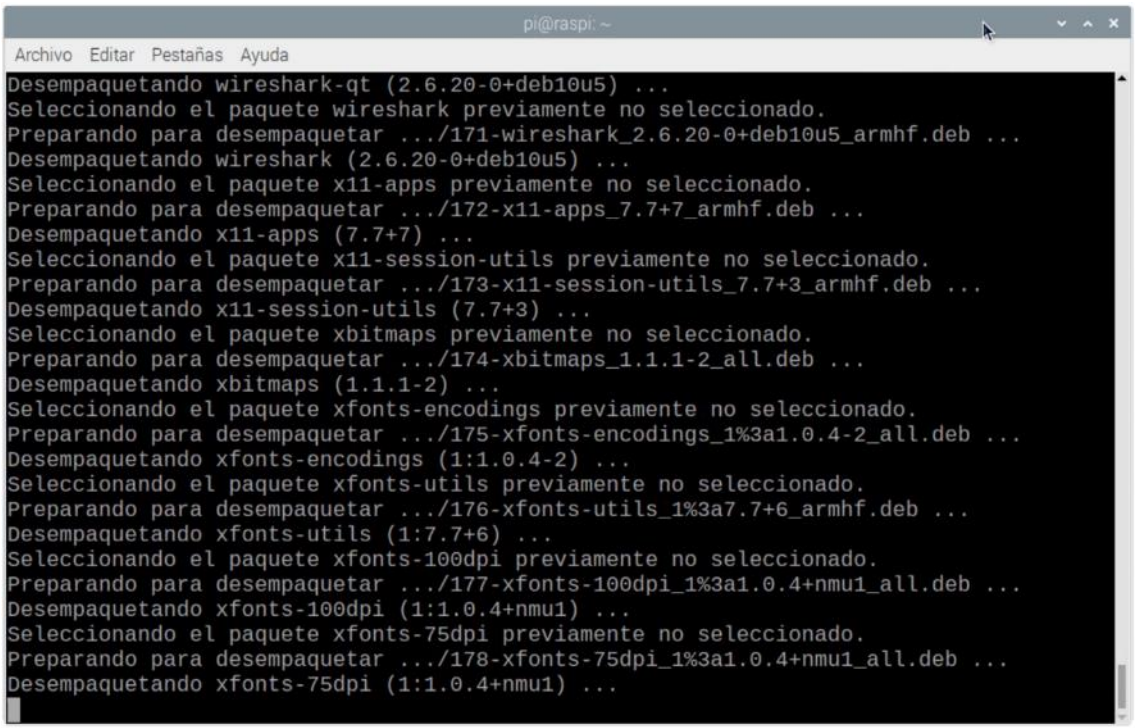
Una vez comprobadas las dependencias, será necesario pulsar la tecla S e INTRO, para que se instalen las aplicaciones indicadas y todas sus dependencias.

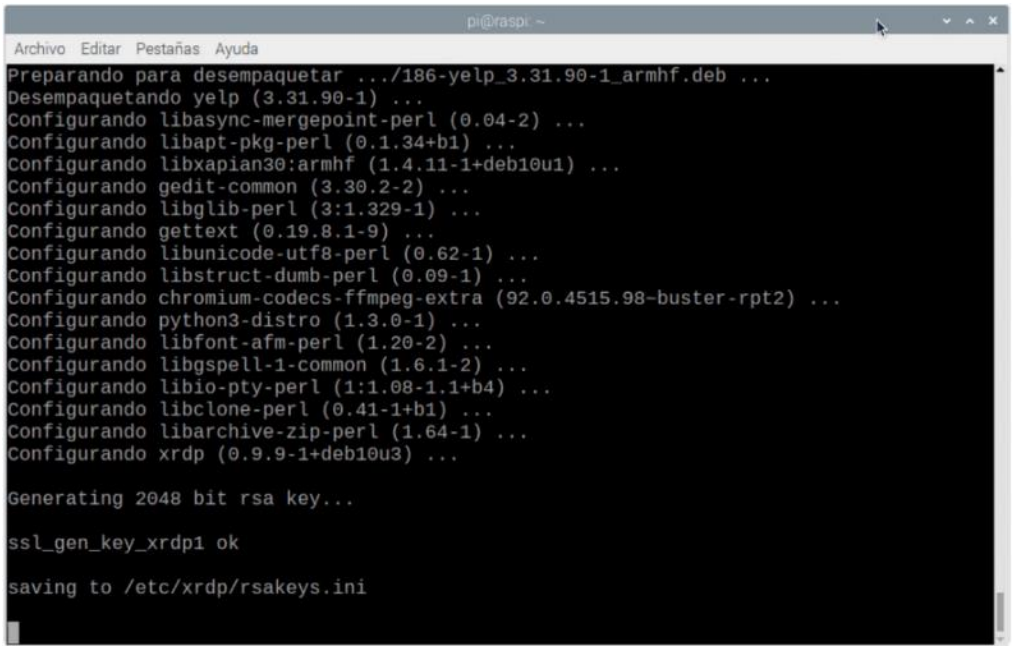


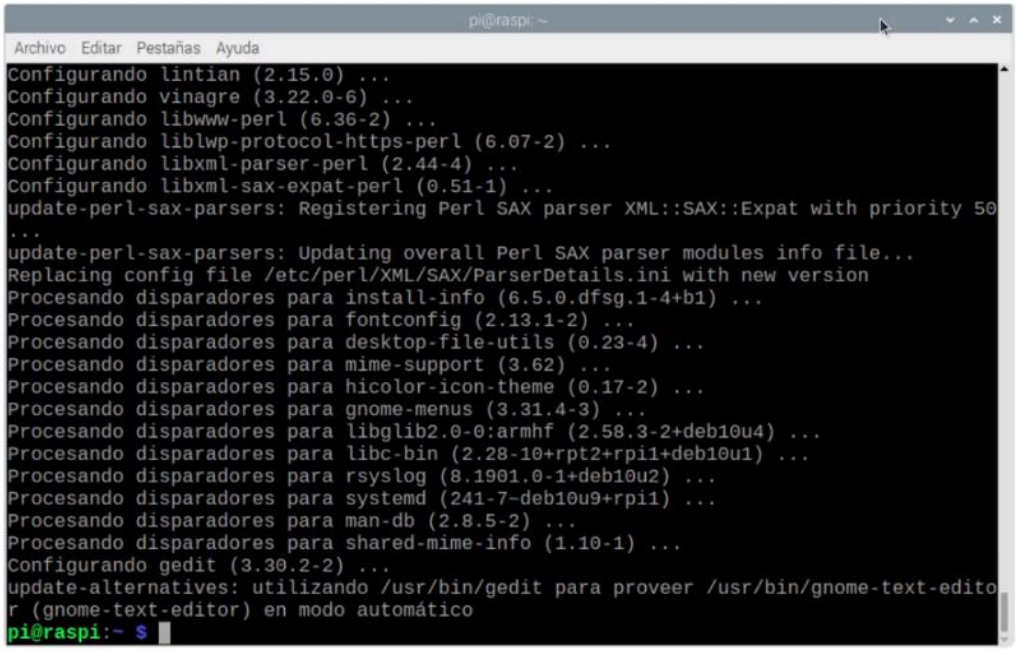
Al pulsar INTRO, comenzará el proceso de instalación.



En caso de instalar la aplicación Wireshark, y se quiera permitir realizar capturas a usuarios sin privilegios de administración se seleccionará Si, en caso contrario como es este, se selecciona NO y se pulsa INTRO.







Aplicaciones utilizadas dentro del S.O. de la Raspberry Pi, para las capturas de pantalla y la grabación de video, gnome-screenshot y simplescreenrecorder respectivamente.

Se ejecutará el comando.

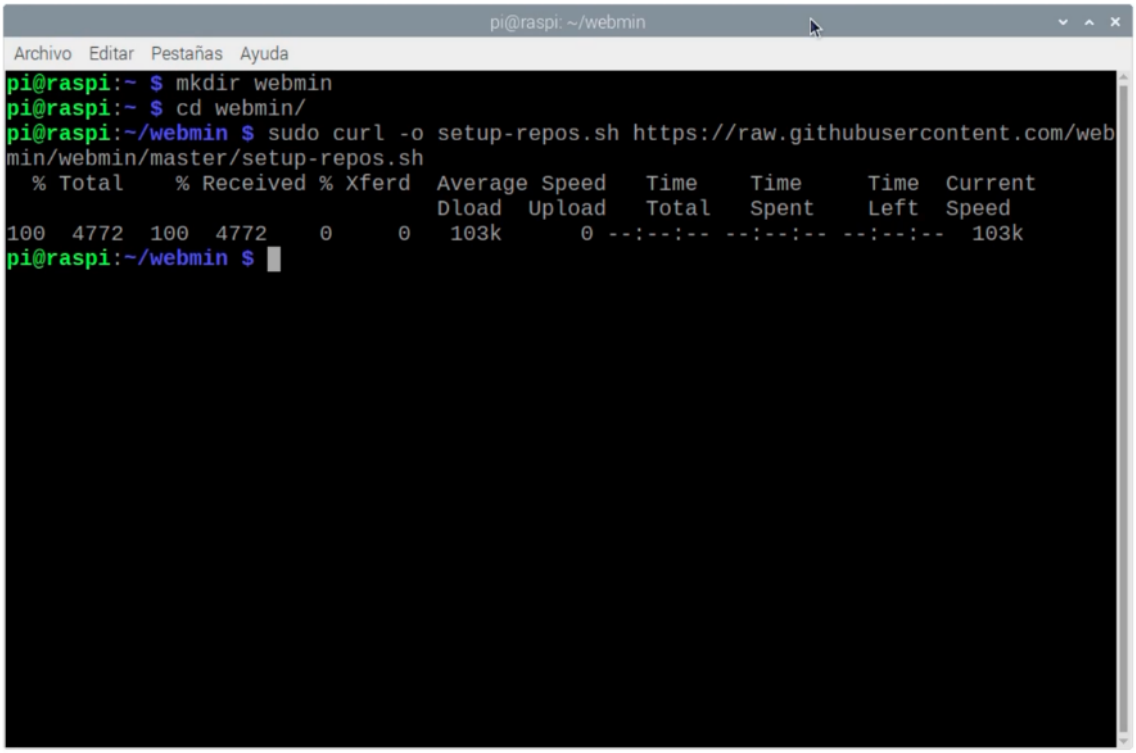
sudo apt-get install gnome-screenshot simplescreenrecorder

En el caso de la existencia de dependencias será necesario contestar afirmativamente para realizar la instalación de las aplicaciones y sus dependencias.

Instalación WEBMIN.

Según las últimas indicaciones en la WEB oficial del proyecto.

URL. https://webmin.com/download/

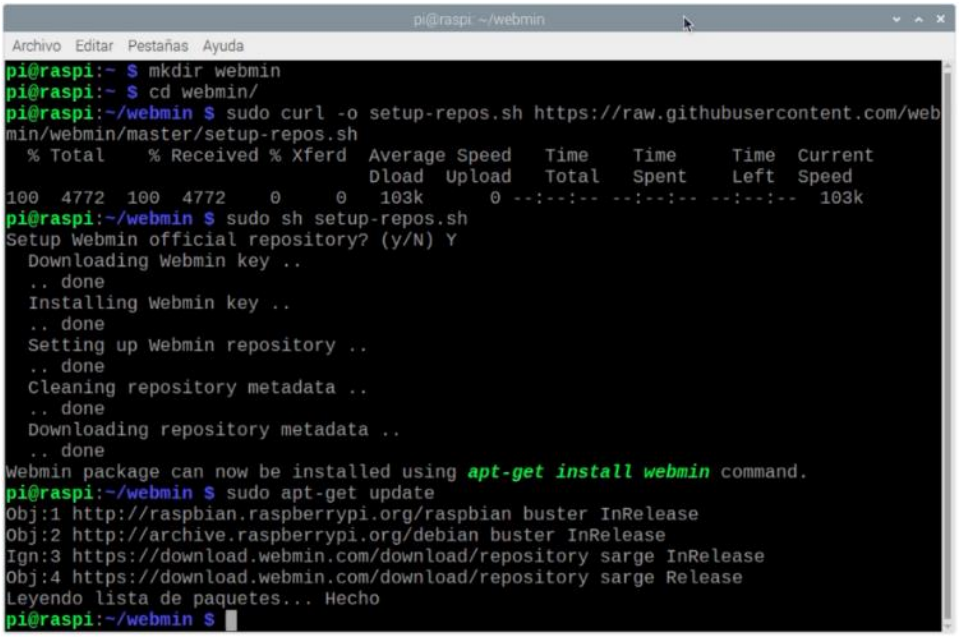


En este caso, se crea una carpeta llamada webmin y se accede a ella con los comandos.

Creación de la carpeta, mkdir webmin
Acceder a la carpeta, cd webmin

Posteriormente se ejecuta el comando

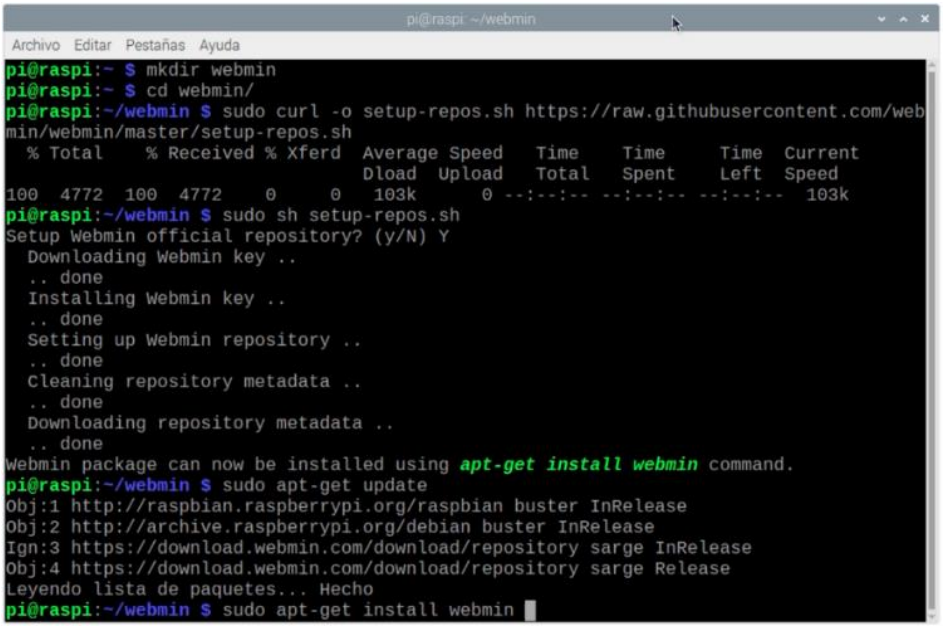
sudo curl -o setup-repos.sh
https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh



Para poder agregar los repositorios de WEBMIN, se ejecutará el comando.

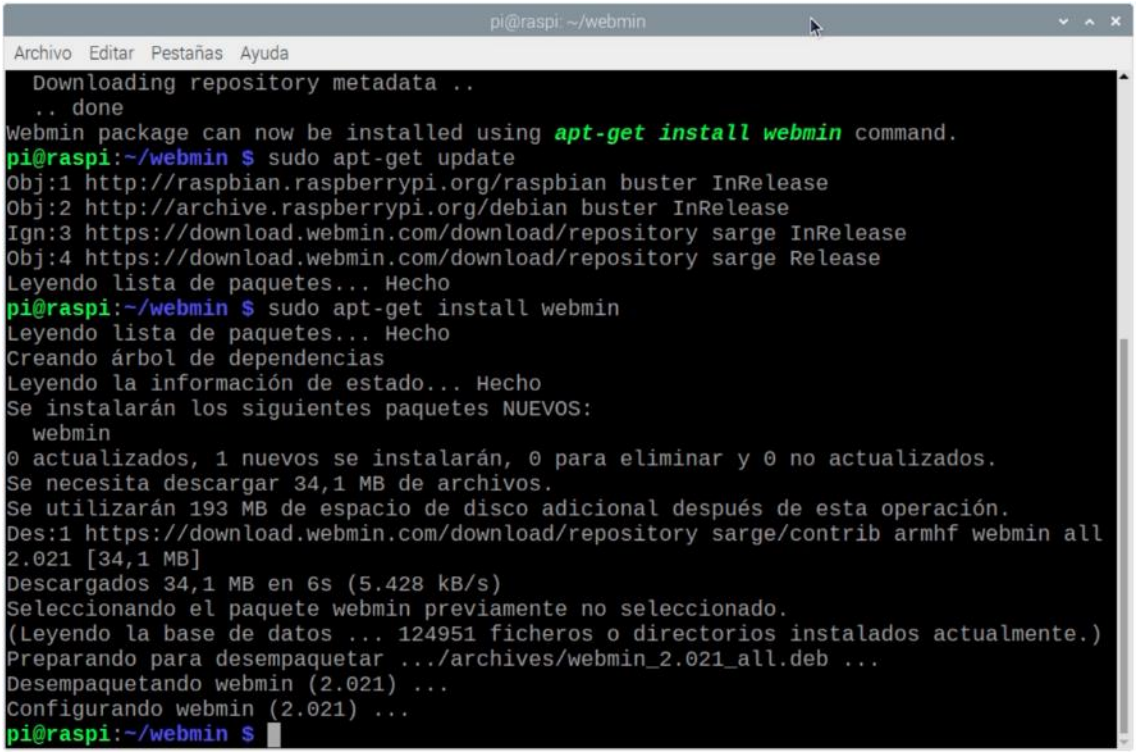
sudo sh setup-repos.sh

Como se puede observar en la captura de la ventana superior, a la pregunta, Setup Webmin oficial repository? (y/N), se escribirá la letra “Y”, posteriormente se pulsará INTRO.



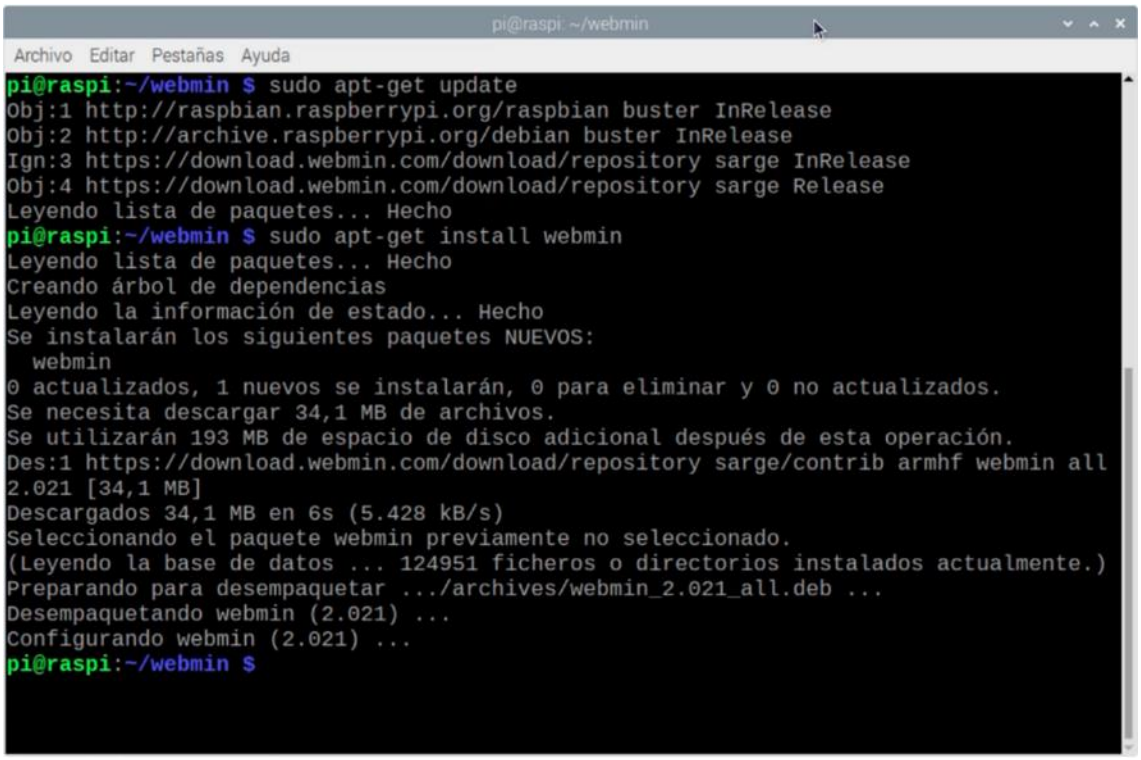
Agregado el repositorio, se actualizarán las fuentes con el comando.

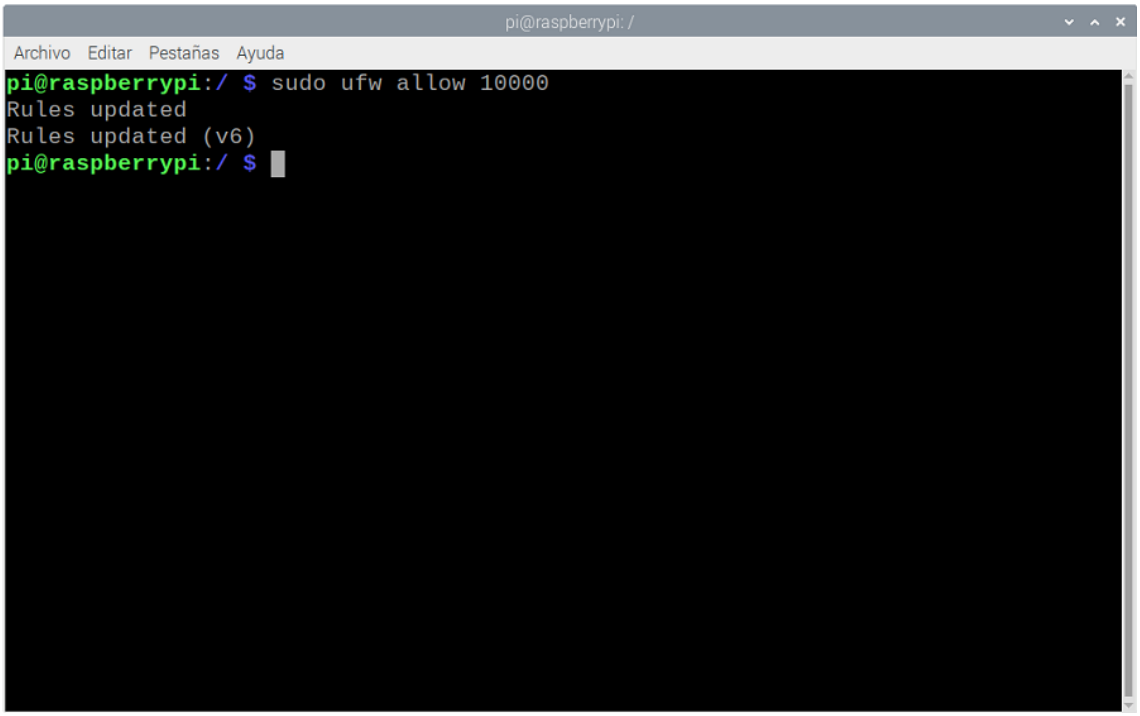
sudo apt-get update



Terminada la actualización de los repositorios, se instalará WEBMIN ejecutando el comando.

sudo apt-get install webmin





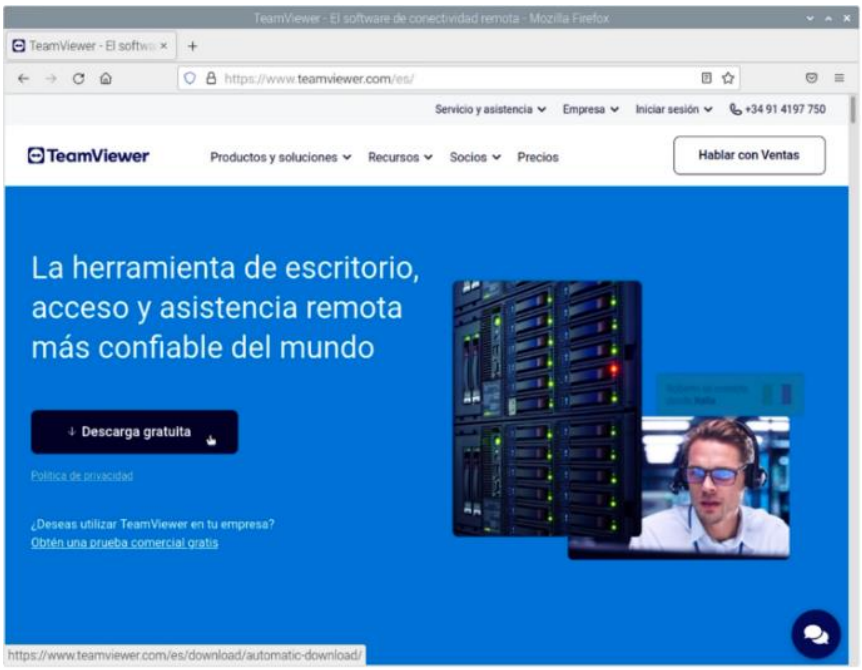
Por último, en la instalación de WEBMIN, para crear una regla en el firewall, siendo el cortafuegos la aplicación ufw, el cual tendrá que estar instalado e iniciado, se explicará estas cuestiones, se ejecutará el comando.

sudo ufw allow 10000

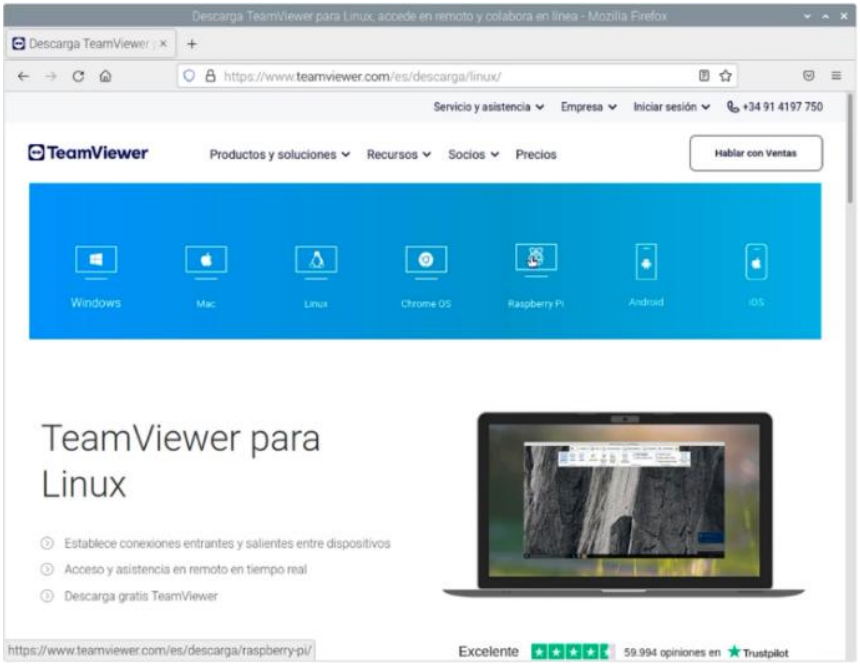
Instalación aplicación TeamViewer en Raspberry Pi.

Se accederá a la WEB oficial.

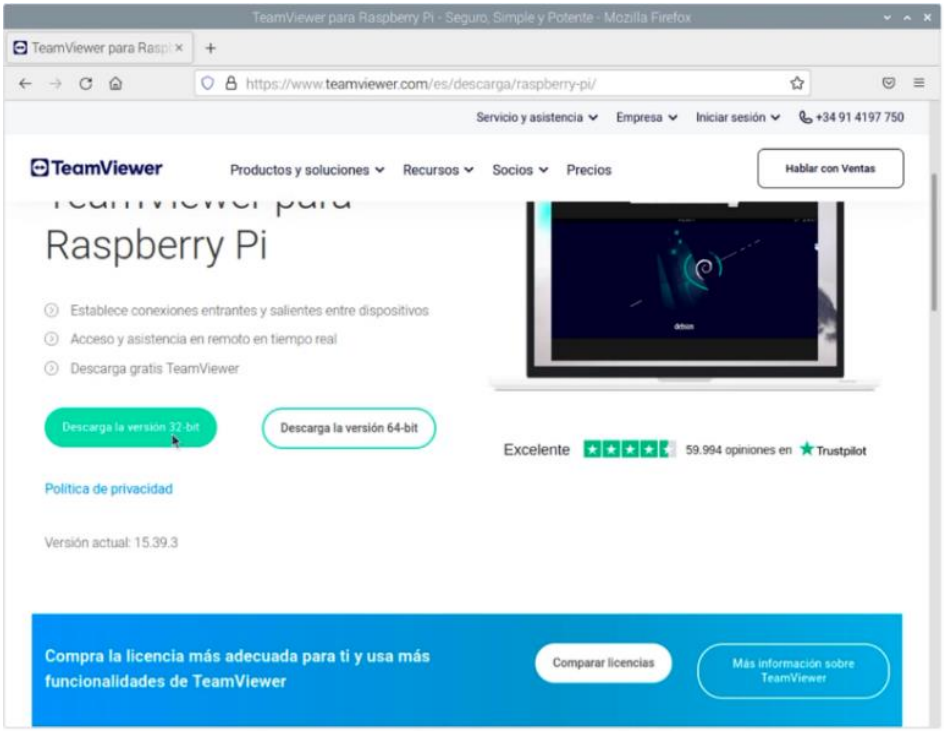
URL. https://www.teamviewer.com/es/descarga/windows/



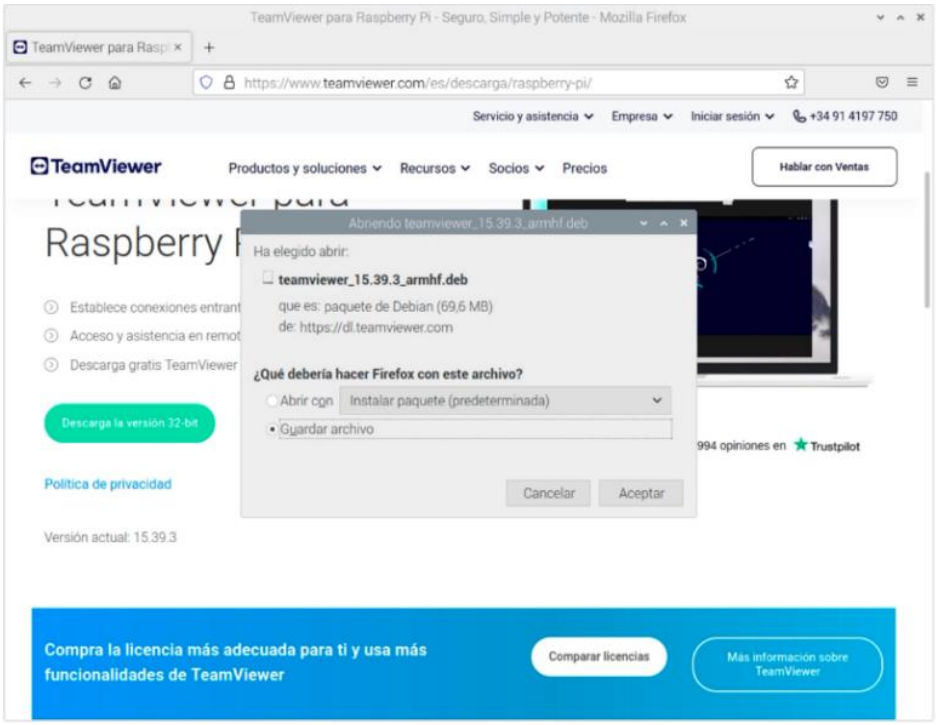
Se pulsará sobre el botón Descarga gratuita.



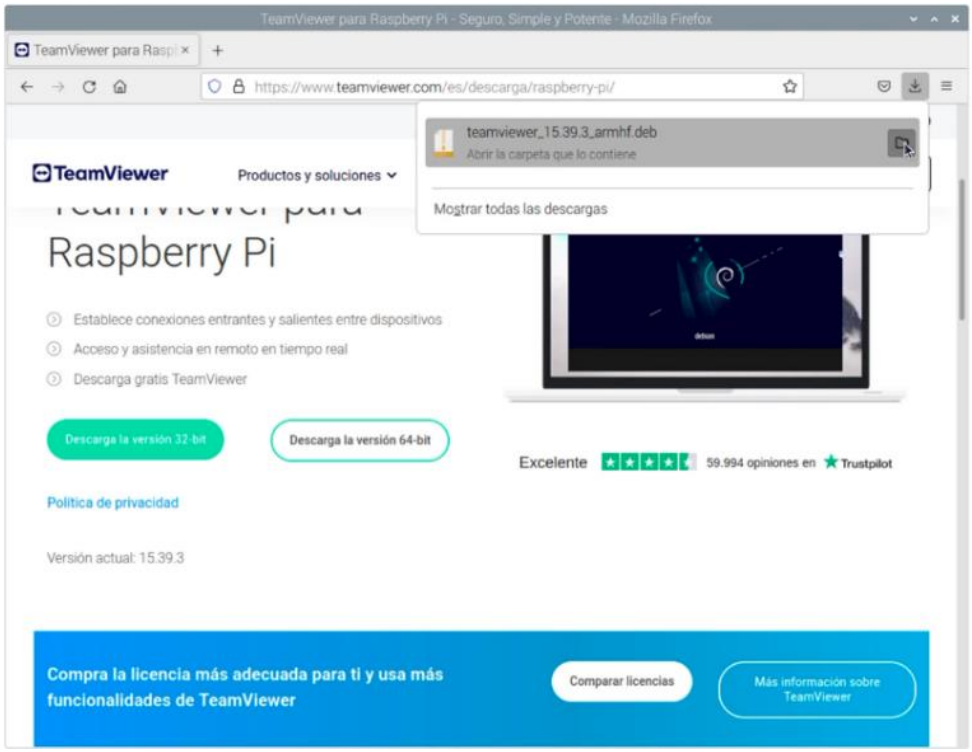
En esta nueva ventana, habrá que pulsar sobre el botón Raspberry Pi.



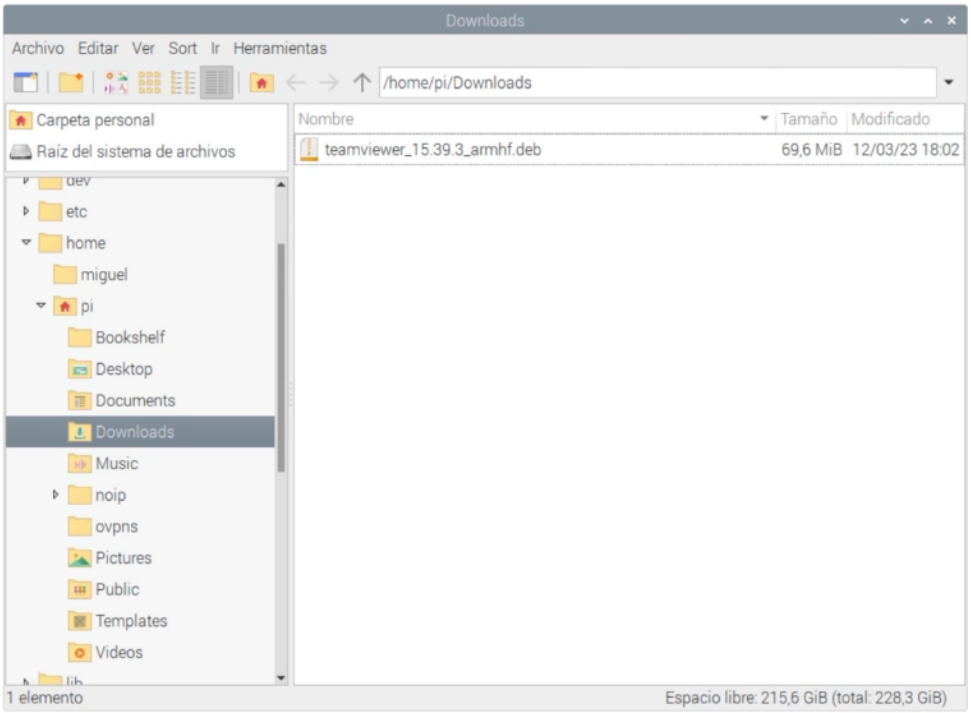
Habrá que seleccionar la arquitectura del S.O., en este caso se trata de 32 Bits, por lo que se pulsa sobre el botón Descarga la versión 32-bit.



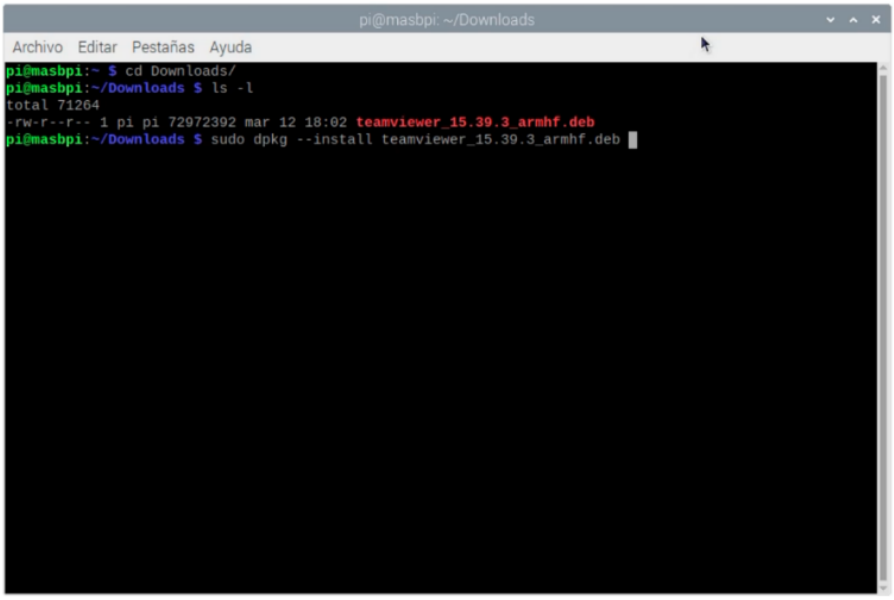
Dependiendo como se tenga configurado el navegador a la hora de realizar las descargas, aparecerá este mensaje o no, en este caso se selecciona en el cuadro de descarga que el fichero se guarde y se pulsa sobre Aceptar.



Una vez descargado el fichero, se pulsará en el icono con forma de carpeta que aparece tras finalizar la descarga en la parte superior derecha.



Como se puede apreciar en la ventana de la captura superior, la descarga del fichero se encuentra en la carpeta Descargas.

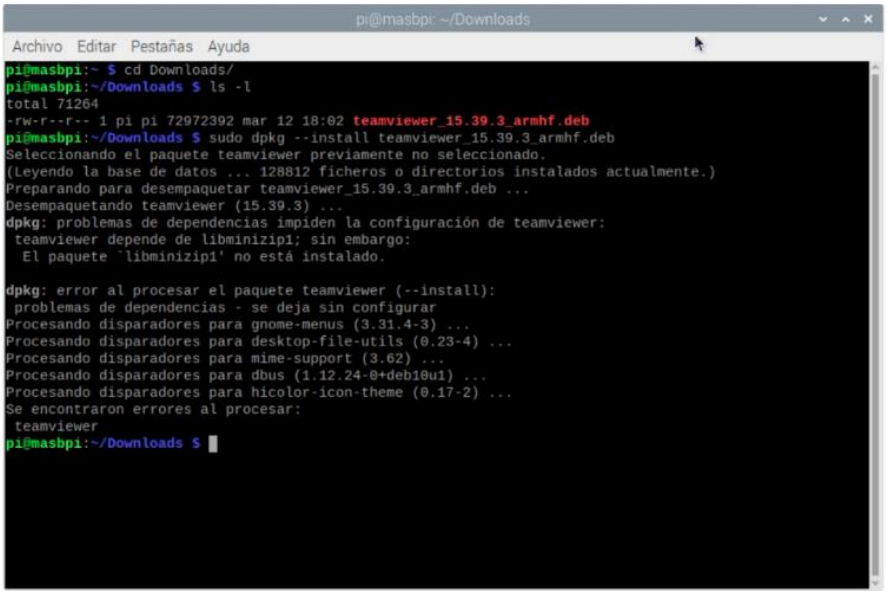


Dentro de un terminal, habrá que dirigirse a la ubicación de la descarga, en este caso es el directorio Descargas, ejecutando el comando.

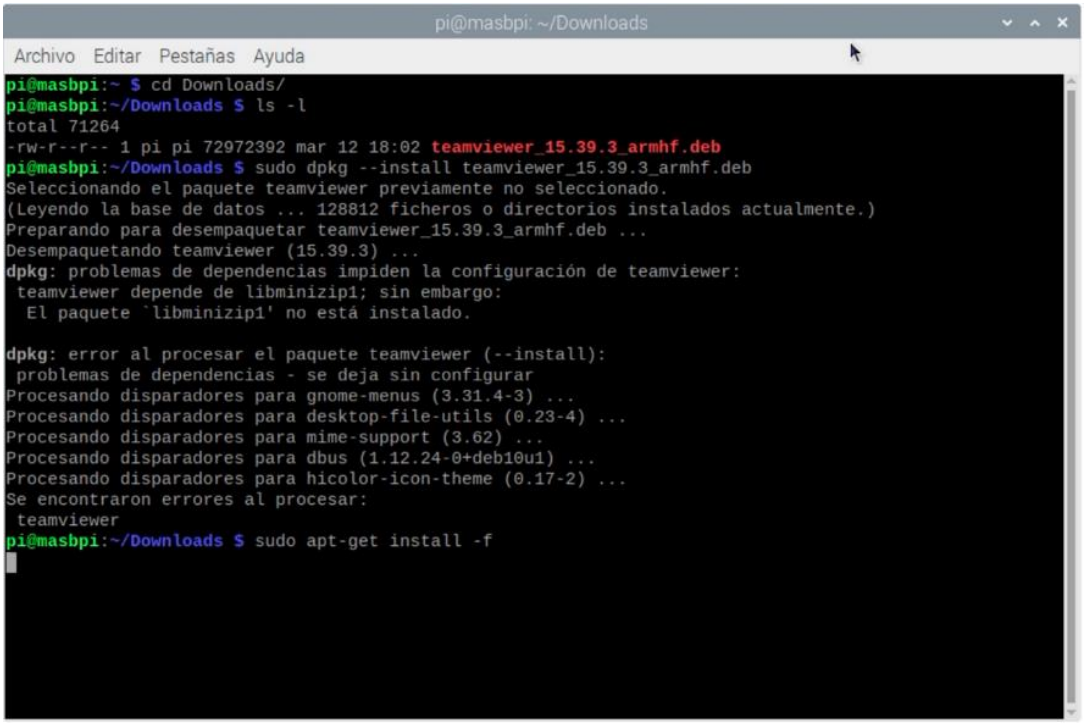
cd Downloads

Para comprobar el nombre del fichero o visualizar el contenido de la carpeta, se ejecuta el comando.
ls -l
Por último, para comenzar la instalación habrá que ejecutar el comando

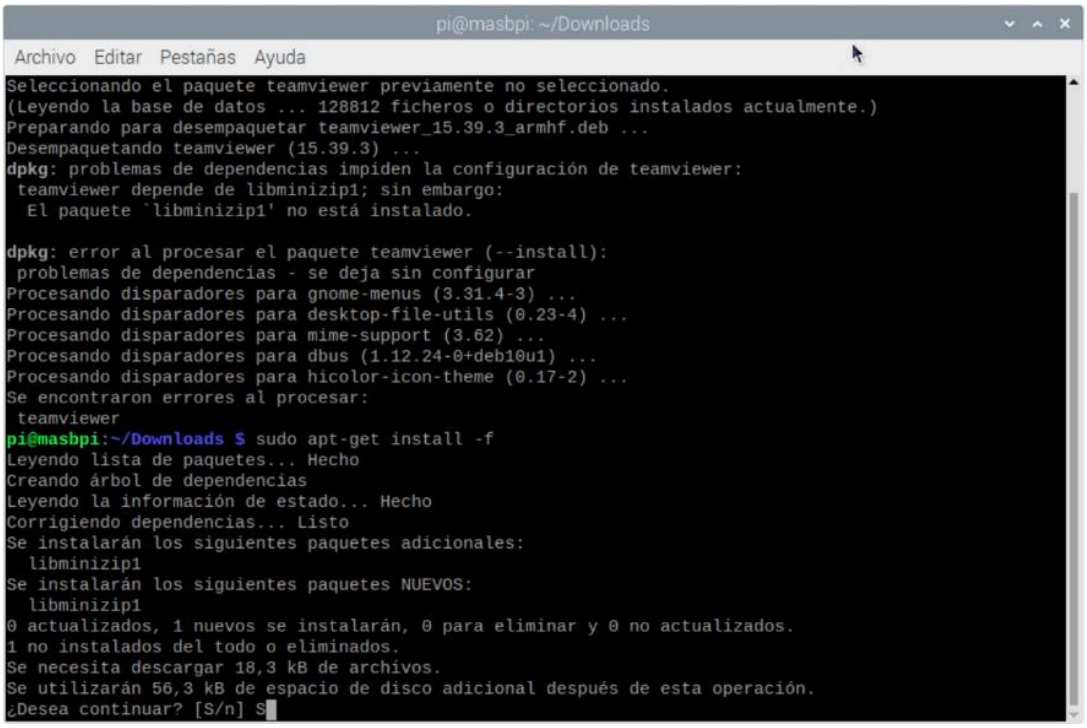
sudo dpkg –install teamviewer_15.39.3_armhf.deb



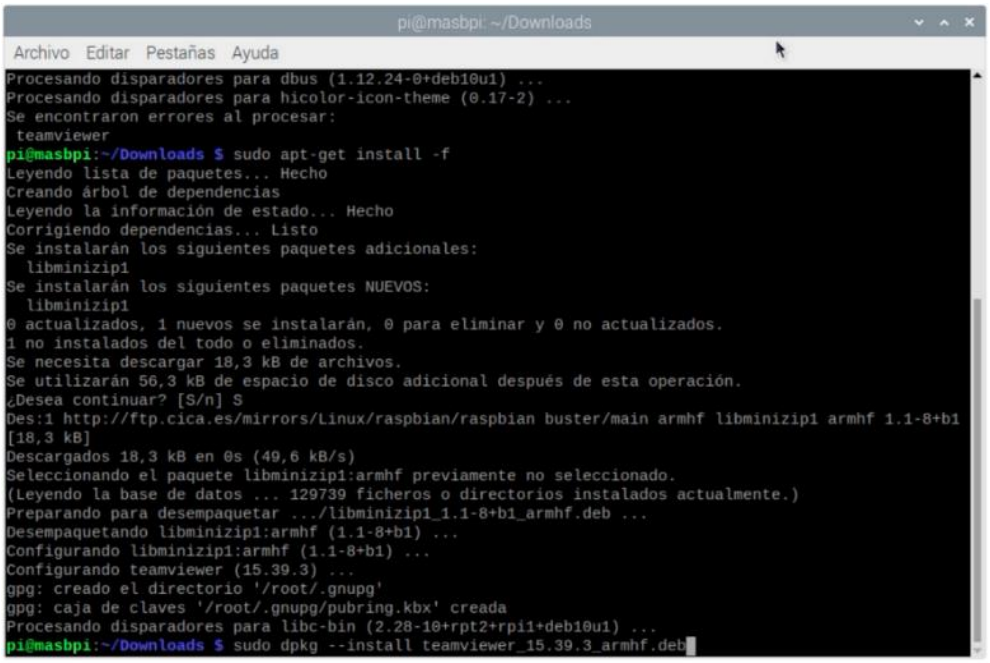
Puede que aparezcan problemas o errores a la hora de instalar la aplicación.



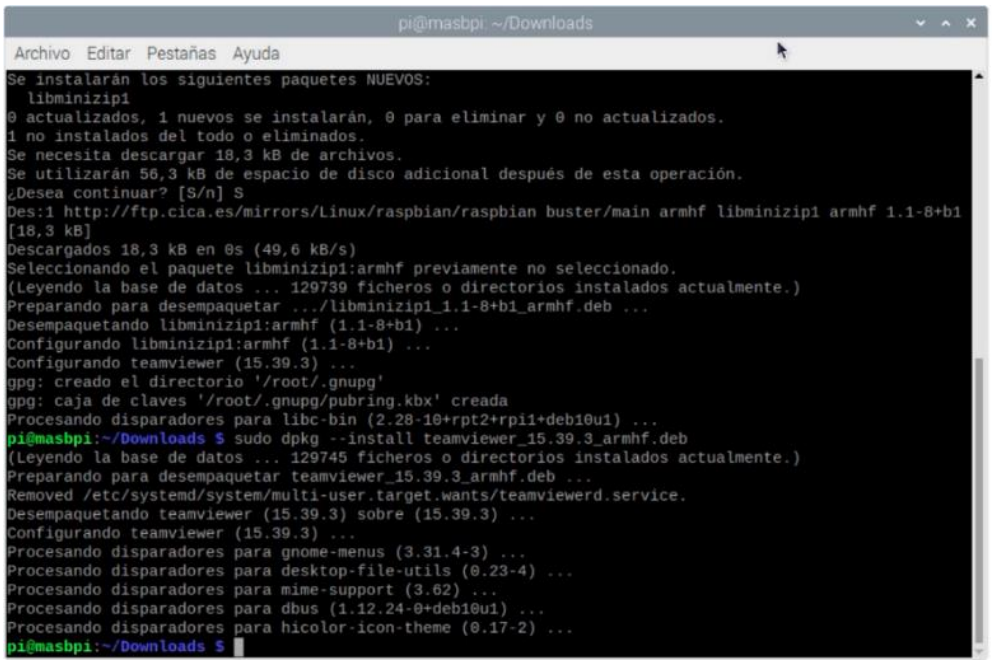
Si ese es el caso, para solventar el problema se ejecutará el comando.
sudo apt-get install -f



Como se aprecia en la ventana de la captura superior, al encontrase dependencias incumplidas y ejecutar el mencionado comando, para solventar el problema se escribirá “S” y se pulsará INTRO.

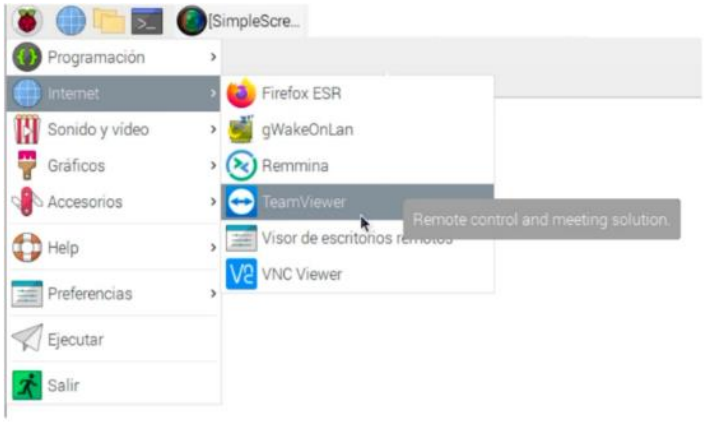


Terminada la instalación de las dependencias, nuevamente se ejecutará el comando sudo dpkg –install teamviewer_15.39.3_armhf.deb

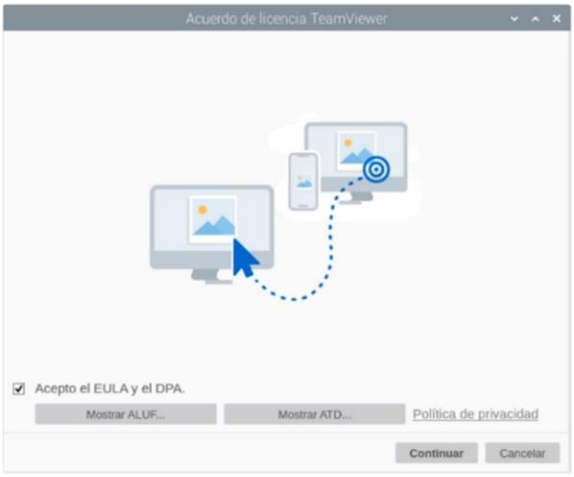


Comprobando más tarde que la instalación de la aplicación TeamViewer se termina correctamente.

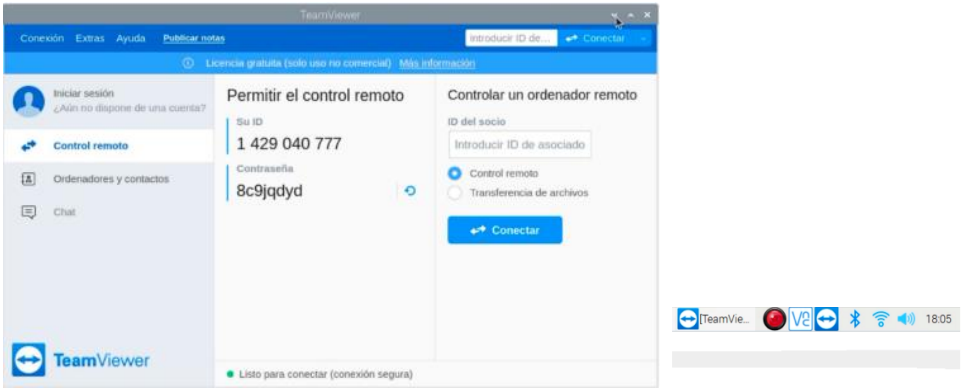
Puede ser necesario la apertura del puerto de conexión TCP/UDP 5938, el cual, habrá que abrirlo en el router y habilitar el tráfico TCP/UDP puerto 5938 en el cortafuegos del servidor VPN/WOL, aunque en las pruebas realizadas no fue necesario.



Una vez terminada la instalación, se pulsará sobre el icono , ubicado en la barra superior izquierda, se pulsará sobre Internet \ TeamViewer.



Se tendrá que marcar la opción Acepto el EULA y el DPA. pulsando a continuación sobre Continuar.



Por último, se mostrará la ventana de la aplicación, encontrándose está preparada para las conexiones remotas, si se minimiza la aplicación, esta mostrará un icono en la barra superior derecha, como se aprecia en la ventana de la captura superior derecha, informando que la aplicación se encuentra iniciada.

Activación instalación VNC.



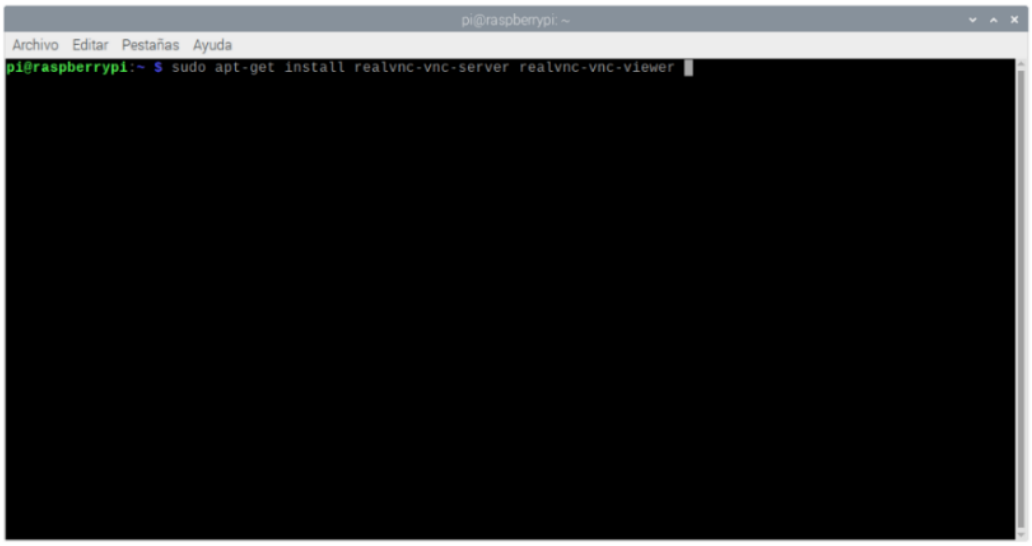
La instalación o activación de la aplicación VNC en la Raspberry Pi, se puede realizar a través de la propia configuración, como instalar la aplicación en un terminal bajo línea de comando.

Mediante la aplicación de configuración gráfica, la cual se indicó tras el primer inicio de la Raspberry Pi, este es un ejemplo rápido de cómo llevarlo a cabo.

En el menú superior izquierdo se pulsará sobre  , posteriormente sobre Preferencias \ Configuración de Raspberry Pi, abriéndose la aplicación de configuración.



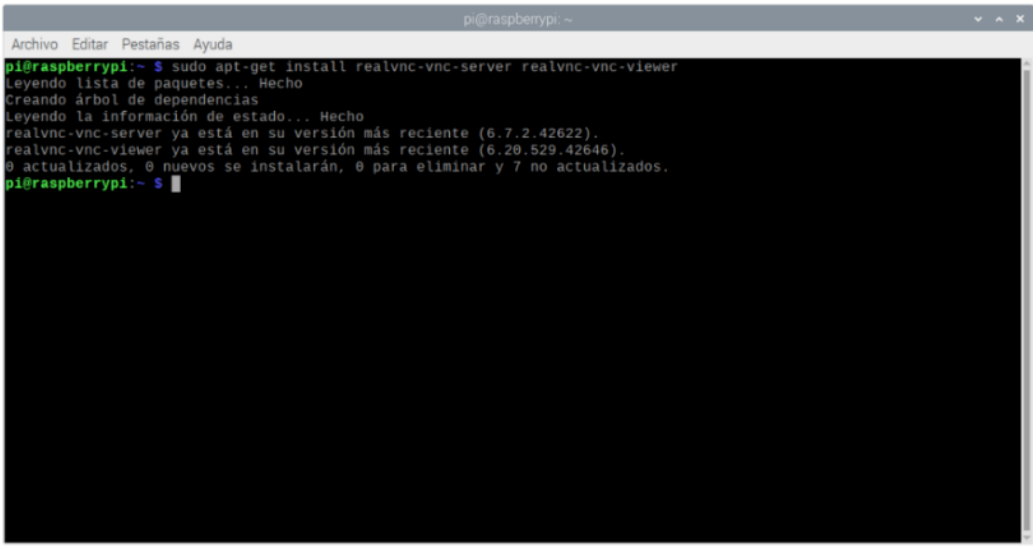
Dentro de la aplicación de configuración, en la pestaña Interfaces, se tendrá que tener activada la interfaz VNC, como se puede apreciar en la ventana de la captura superior, en caso de activarla al pulsar sobre Aceptar, puede ser necesario el reinicio de la Raspberry Pi.



Otra opción, es instalar la aplicación a través de un terminal con el comando.

sudo apt-get install realvnc-vnc-server realvnc-vnc-viewer

Al pulsar INTRO, para comenzar la instalación puede que se solicite credenciales de un usuario con permisos para realizar instalaciones, se facilitaran y en el caso de indicar que es necesario la instalación de dependencias se tendrán que instalar todas las dependencias.



Puede que al encontrarse ya activada la interfaz VNC en la configuración de la Raspberry Pi, no sea necesaria la instalación, mostrándose el mensaje de la ventana de la captura superior.

El puerto de conexión por defecto es el TCP 5900, el cual habrá que abrirlo en el router y habilitar el tráfico TCP puerto 5900 en el cortafuegos del servidor VPN/WOL.

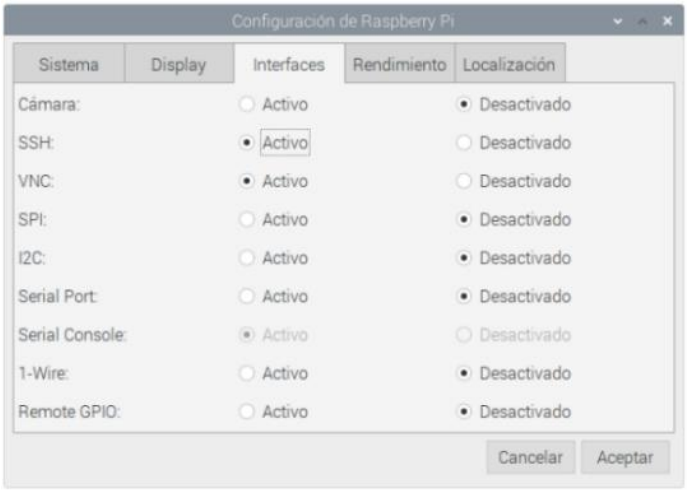
Activación instalación SSH.



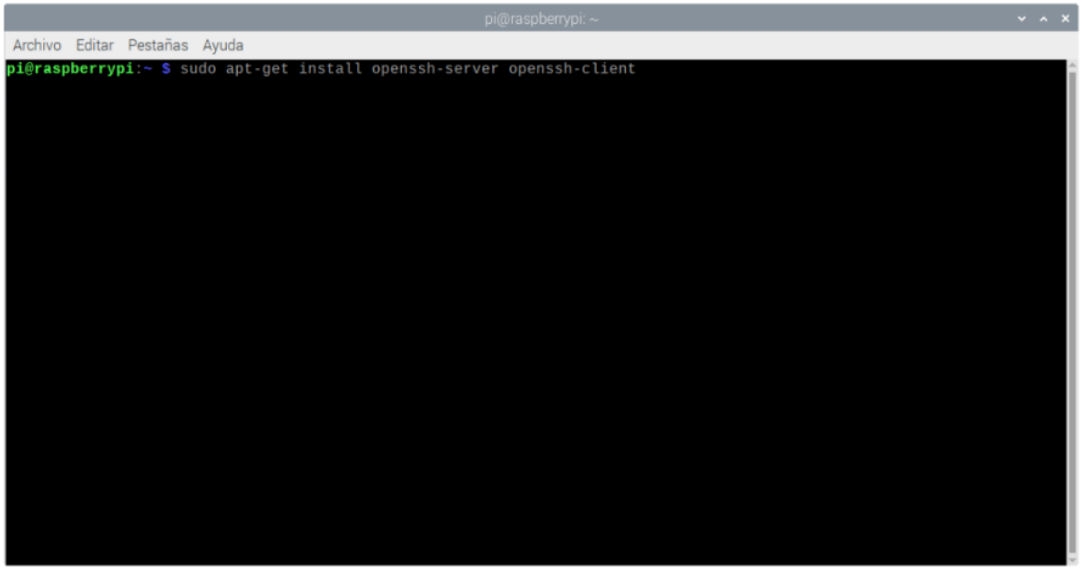
La instalación o activación del protocolo SSH en la Raspberry Pi, se puede realizar a través de la propia configuración, como instalar el protocolo en un terminal bajo la línea de comando.

Mediante la aplicación de configuración gráfica, la cual se indicó tras el primer inicio de la Raspberry Pi, este es un ejemplo rápido de cómo llevarlo a cabo.

En el menú superior izquierdo se pulsará sobre  , posteriormente sobre Preferencias \ Configuración de Raspberry Pi, abriéndose la aplicación de configuración.



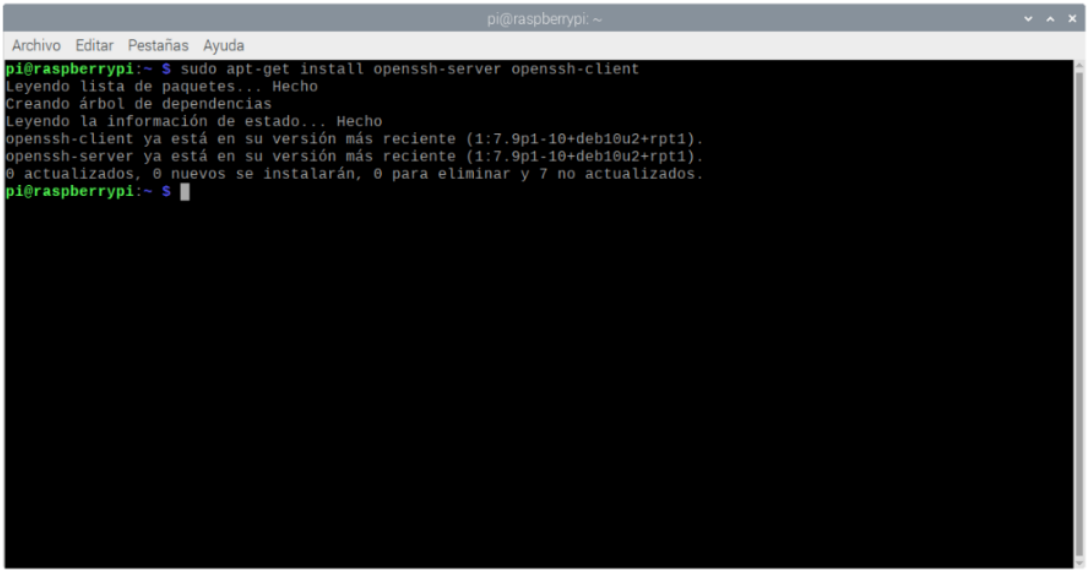
Dentro de la aplicación de configuración, en la pestaña Interfaces, se tendrá que tener activada la interfaz SSH, como se puede apreciar en la ventana de la captura superior, en caso de activarla al pulsar sobre Aceptar, puede ser necesario el reinicio de la Raspberry Pi.



Otra opción, es la instalación a través de un terminal con el comando.

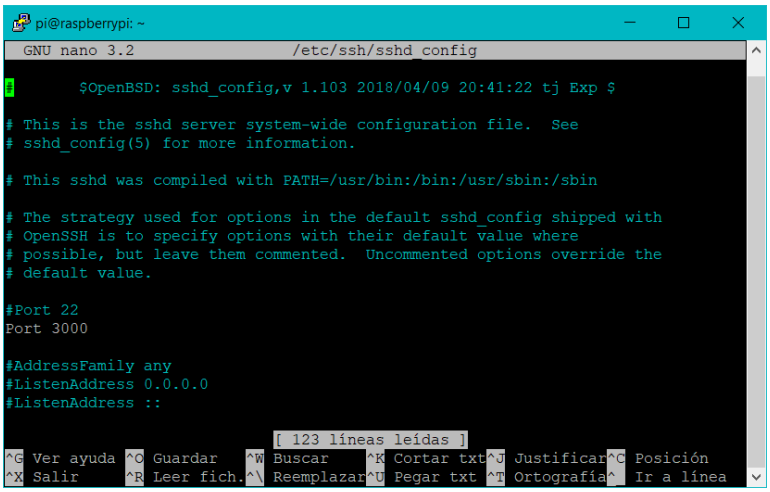
sudo apt-get install openssh-server openssh-client

Al pulsar INTRO para comenzar la instalación, puede que se solicita credenciales de un usuario con permisos para realizar instalaciones, se facilitaran y en el caso de indicar que es necesario la instalación de dependencias, se tendrán que instalar todas las dependencias.



Puede que al encontrarse ya activada la interfaz SSH en la configuración de la Raspberry Pi, no sea necesaria la instalación, mostrándose el mensaje de la ventana de la captura superior.

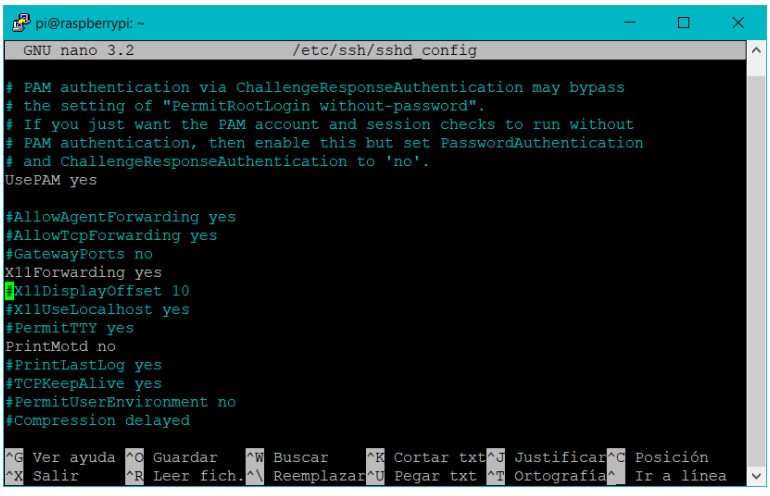
Habilitar X11Forwarding.



Este paso se puede hacer tanto localmente como a través de SSH, en ambos casos, estando dentro de un terminal, se escribirá el comando.
sudo nano /etc/ssh/sshd_config

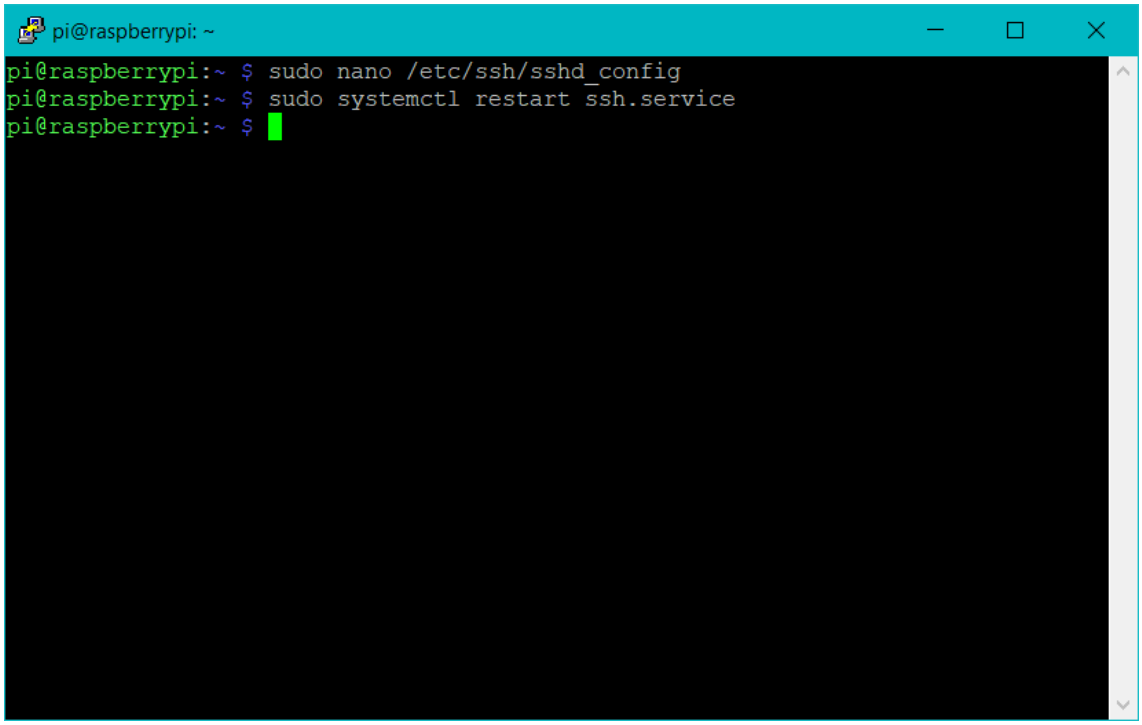
Habrá que localizar la línea comentada.
X11Forwarding no

Quedando.
X11Forwarding yes



Se quitará la almohadilla “#”, situada al principio de la línea y tendrá que quedar como se muestra en la ventana de la captura superior, también se puede escribir en la parte inferior del fichero.

Realizados los cambios necesarios, se pulsará Ctrl+O (Ctrl y sin soltar pulsar O), para grabar y Ctrl+X (Ctrl y sin soltar pulsar X), para salir del fichero.



Para finalizar, se ejecutará el comando para reiniciar el servicio SSH.

sudo systemctl restart ssh.service

Fichero configuración servicio SSH.

Si se quiere modificar el puerto de conexión del protocolo SSH, es posible editando el fichero de configuración del servicio SSH en el servidor.

Fichero sshd_config ubicado en /etc/ssh

```
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

Para modificar el puerto por defecto del protocolo SSH, habrá que editar con un editor de textos el fichero sshd_config, ubicado en /etc/ssh con el comando.

sudo nano /etc/ssh/sshd_config

Una vez dentro, habrá que quitar la almohadilla en la línea # port 22

```
#Port 22
```

```
#Port 22
Port 2222
```

Pudiendo modificar el número de puerto, por ejemplo, donde se sustituye el 22 por 2222

```
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

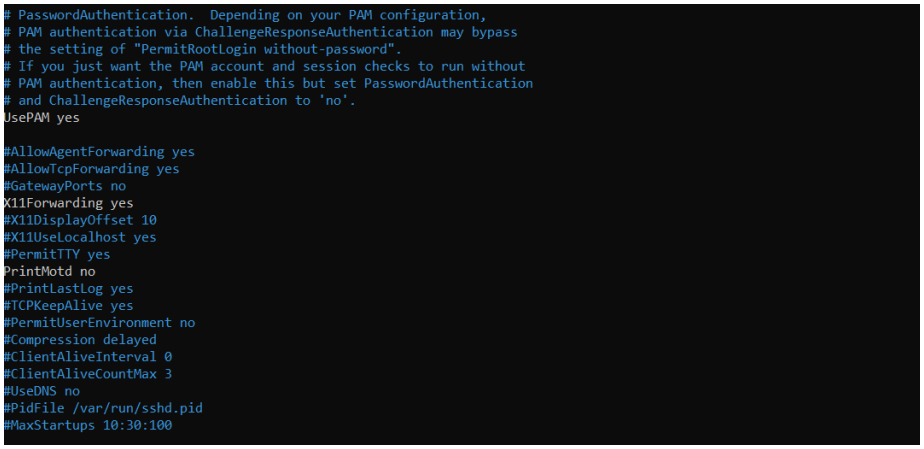
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
Port 2222

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
```



Realizados los cambios necesarios, se pulsará Ctrl+O (Ctrl y sin soltar pulsar O), para grabar y Ctrl+X (Ctrl y sin soltar pulsar X), para salir del fichero.

Se muestra parte del contenido del fichero de configuración en el servidor del servicio SSH.

Fichero /etc/ssh/sshd_config (contenido no integro).

```
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
```
(Puerto por defecto por donde escucha el servicio SSH para cambiarlo quitar almohadilla y poner nº Puerto diferente, Habrá que habilitarlo en el cortafuegos del servidor VPN/WOL y en el Router).
```
#AddressFamily any

#ListenAddress 0.0.0.0
#ListenAddress ::
.
.

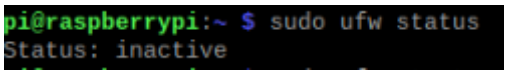
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
```
(Para habilitar X11Forwarding, redirección X, se quitará la almohadilla y habrá que sustituir el no por yes, X11Forwarding yes).
```
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
```

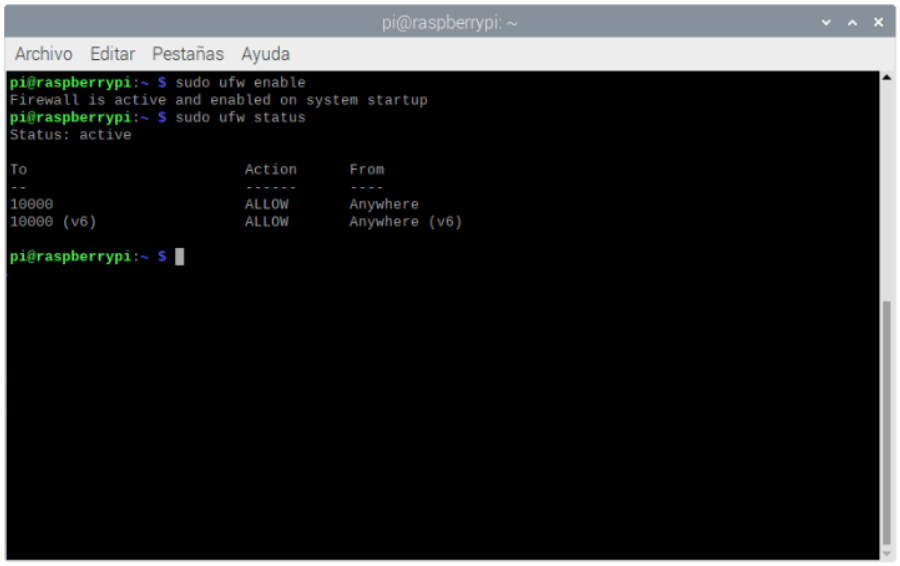
Habilitar tráfico en cortafuegos Linux ufw.

Para que ciertas características en este proyecto funcionen correctamente, es necesario como se explicó anteriormente, la apertura de ciertos puertos en el router, este dispositivo es el facilitado por el proveedor de servicios de Internet (ISP), otra cosa importante es habilitar el tráfico dentro del servidor Linux VPN/WOL, al tratarse este de un S.O. Linux, Raspberry Pi OS, más concretamente una variante de Debian, en este proyecto se instala y se utiliza el cortafuegos ufw.

Para comprobar el estado del cortafuegos, si se encuentra activo o no, se podrá utilizar el comando.

sudo ufw status

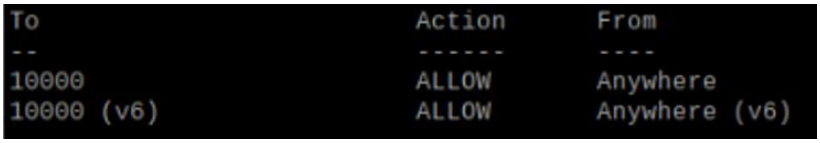




Si se encuentra inactivo, se podrá ejecutar el comando.

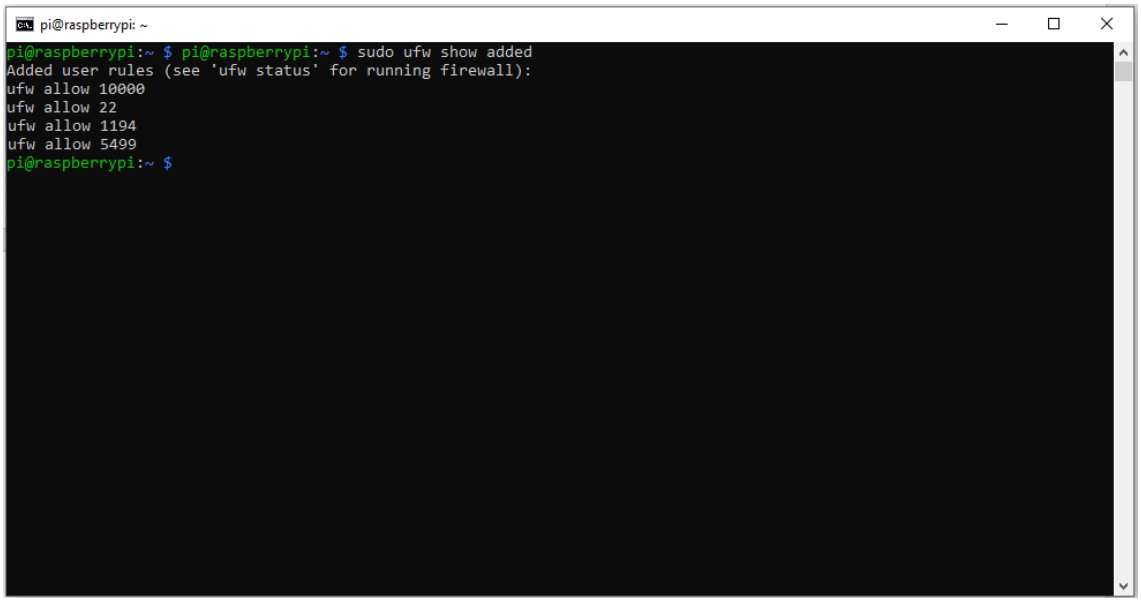
sudo ufw enable

Con el comando sudo ufw status, sudo ufw status verbose o sudo systemctl status ufw, se muestra el estado del cortafuegos como las reglas, en el último comando no se muestran las reglas.



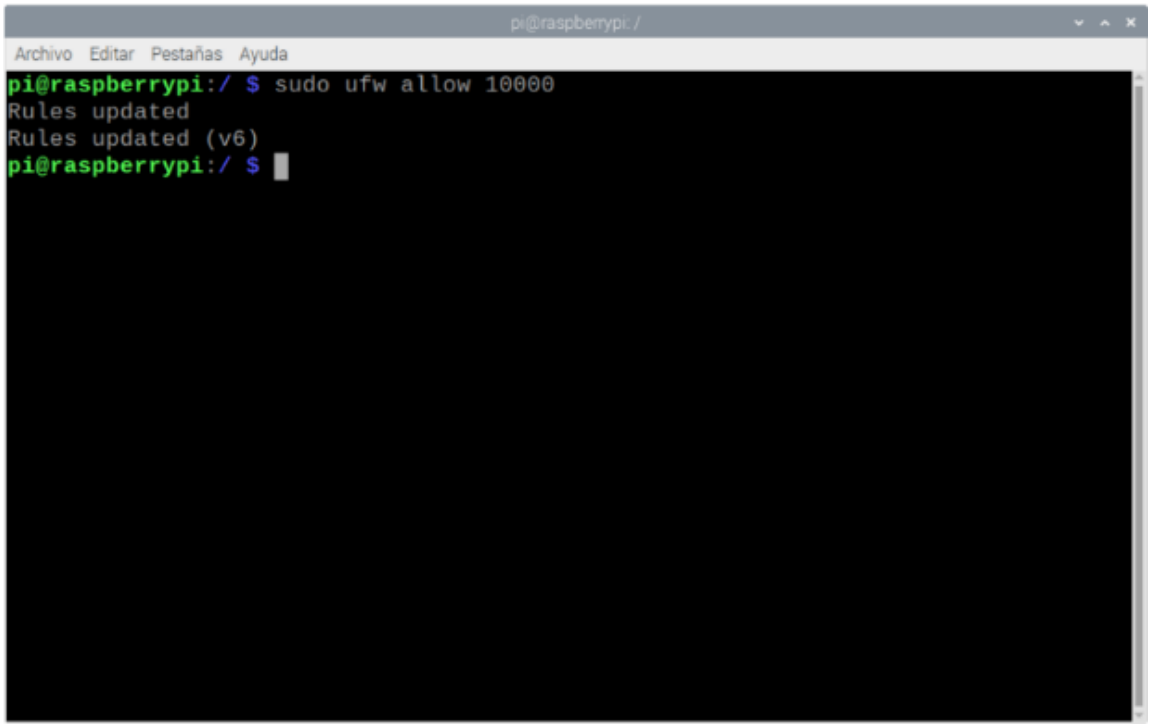
Según se puede apreciar en la ventana de la captura superior.

En este ejemplo, solo se permitió “Action” ALLOW, el tráfico al puerto “to” 10000, desde cualquier red “From“ Anywhere, habitualmente WEBMIN utiliza el puerto 10000.



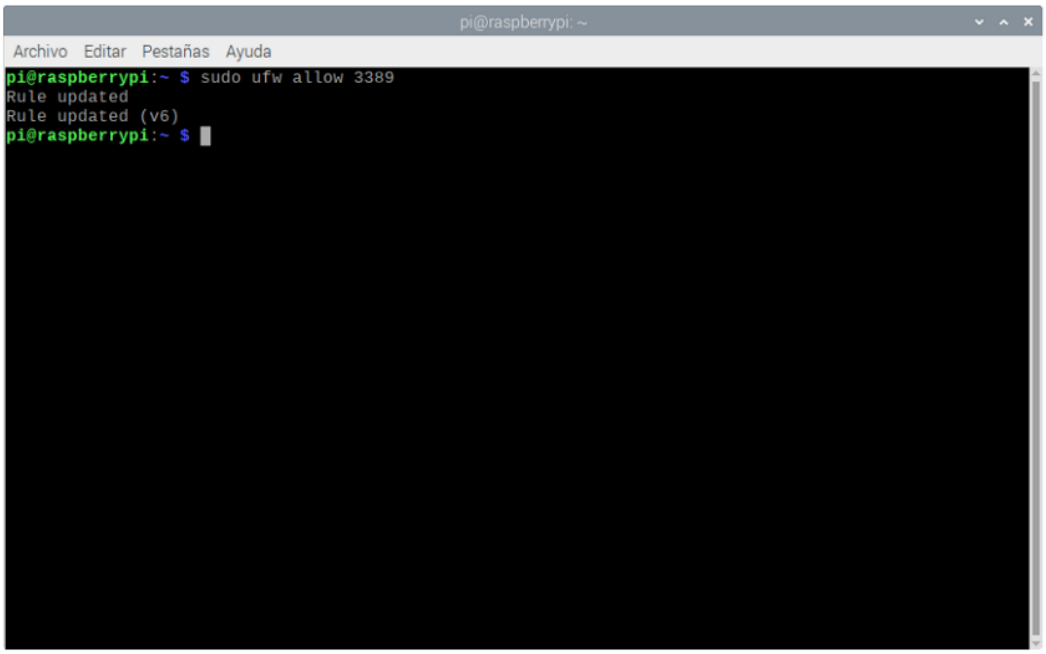
De usuario comando.
sudo ufw show added

Ejemplo de uso básico, habilitar tráfico para conexión WEBMIN.



Dentro del terminal, se ejecutará con el comando.

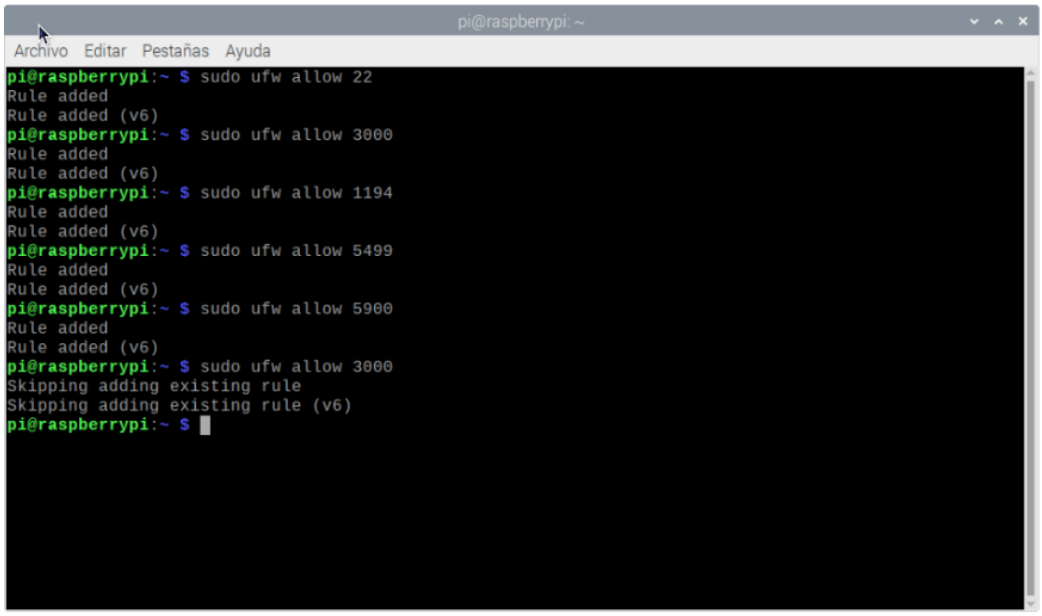
sudo ufw allow 10000



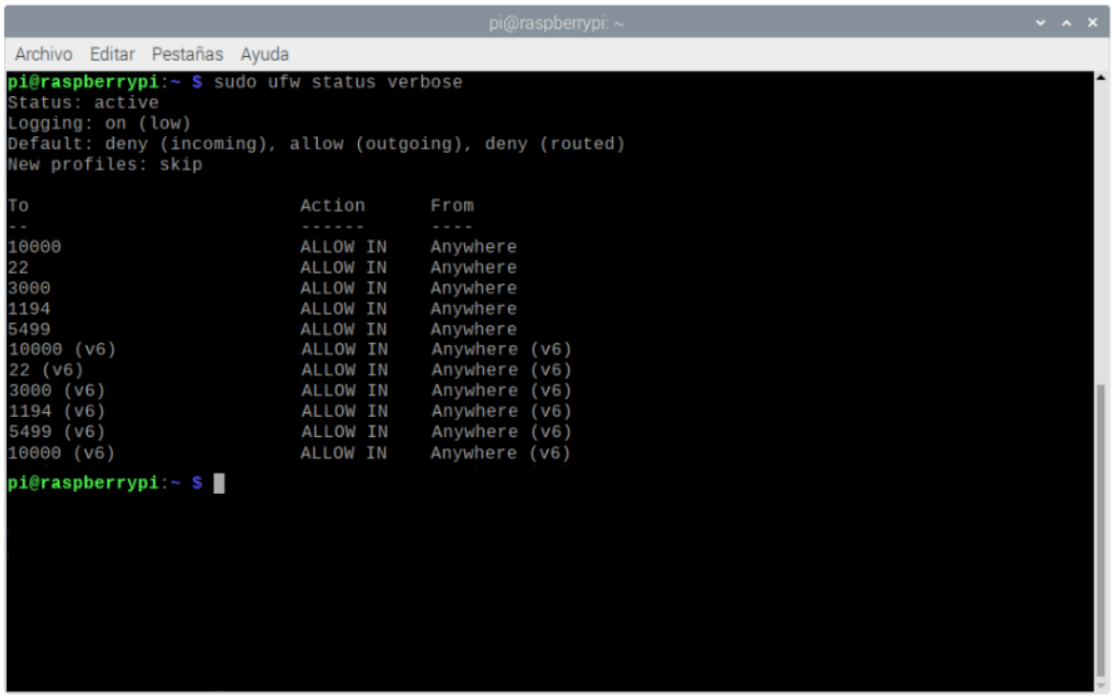
Ejemplo de uso básico, apertura tráfico para conexión RDP en el servidor VPN/WOL, se ejecutará el comando.

sudo ufw allow 3389

En la captura de la imagen superior, se muestra el resultado de ejecutar el comando sudo ufw allow 3389, tras haberlo ejecutado previamente.



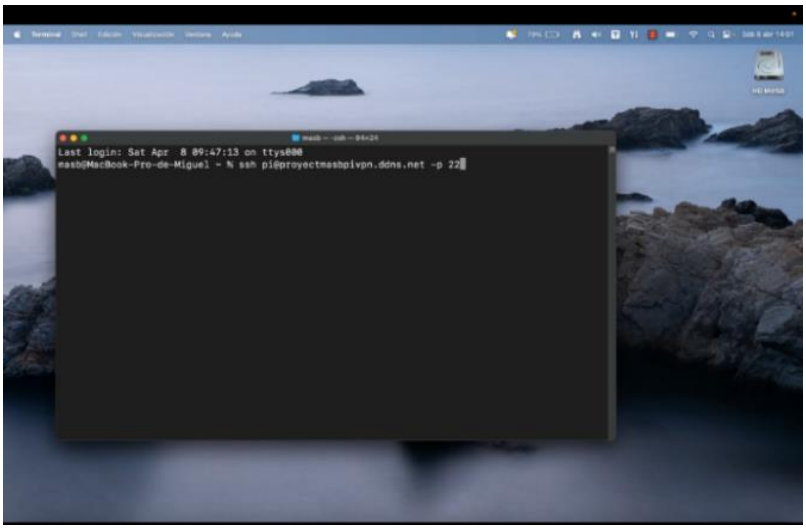
Como se puede observar en la ventana de la captura superior, se habilita el tráfico con el comando básico a los puertos 22, 3000, 1194, 5499, si se ejecuta el comando sobre una regla ya establecida, se informará como se puede apreciar en el último intento.



Habrá que habilitar el tráfico por tantos puertos/protocolos etc, como sea necesario, en este ejemplo se muestra un ejemplo básico de cómo llevarlo a cabo.

Instalación remota vía SSH.

Conexión vía SSH.



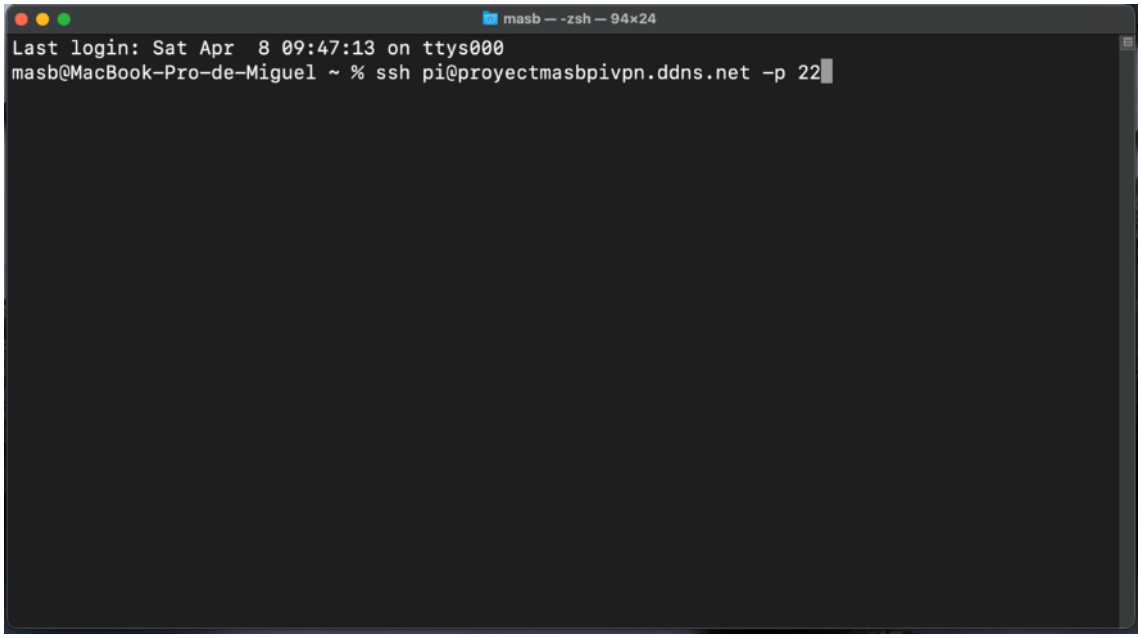
Para realizar este tipo de instalación, lo primero es establecer una conexión SSH.

Este método de instalación vía SSH, nos permite realizar la instalación no estando en la misma ubicación de la Raspberry Pi, por lo que, por lo menos en el dispositivo se tendrá que tener habilitada la conexión por medio del protocolo SSH y en este caso al disponer de direccionamiento dinámico a través del proveedor de servicios de Internet, es necesario disponer de un servicio DDNS, el cual se explicó anteriormente como crear una cuenta, un nombre de dominio o host, y como configurarlo en un router o en su defecto como instalar el software del proveedor de servicios DDNS en el S.O. de la Raspberry Pi.

Para poder conectarnos remotamente a la Raspberry Pi a través de SSH, se tendrá que disponer de la IP pública de la conexión facilitada por el proveedor de servicios de Internet, habilitada la conexión vía SSH en el router y además se habrá habilitado el tráfico en el cortafuegos del S.O. de la Raspberry Pi, o en su defecto, teniendo como mínimo instalado y funcionando el servicio de un proveedor DDNS, en este ejemplo se dispone del software No-IP configurado en el router, habilitado el acceso por SSH y abiertos los puertos adecuados en el router como también habilitado el tráfico en el cortafuegos del S.O.

Es decir, para poder tener la posibilidad de realizar la instalación a través de SSH, será necesario

- Tener configurado el servicio DDNS en el router o instalado y funcionando el software en la Raspberry Pi o en un equipo cliente.
- Habilitada la conexión vía SSH en la Raspberry Pi.
- Abiertos los puertos adecuados en el router.
- Habilitado el tráfico a través del cortafuegos del servidor VPN/WOL.



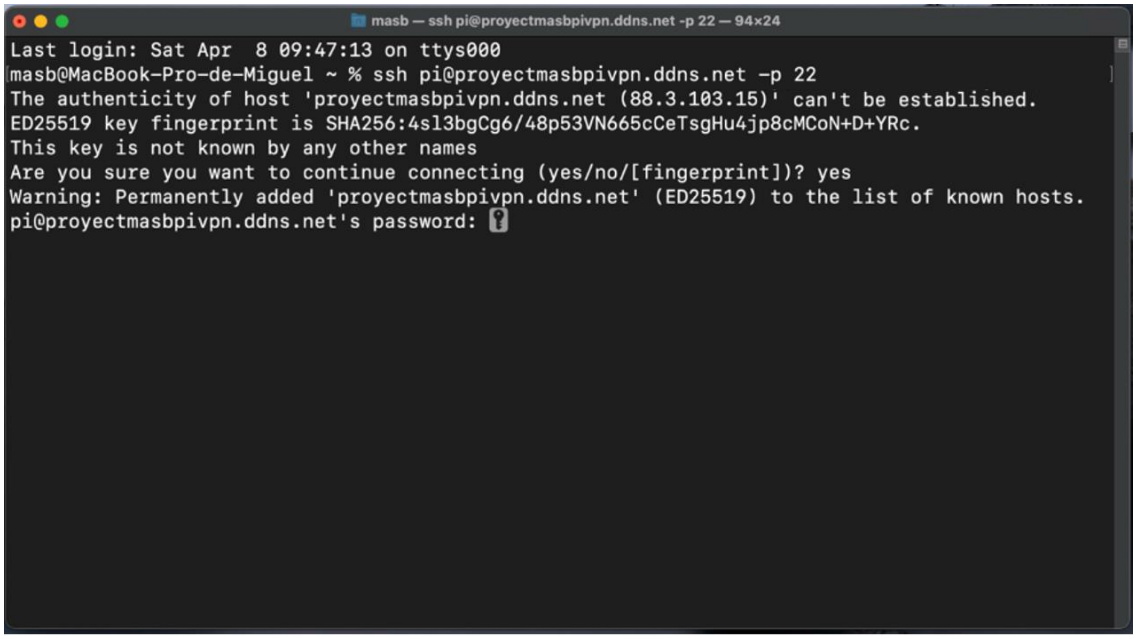
Estas instalaciones a través de SSH no se explicarán tanto, puesto que serían los mismos pasos como si nos encontrásemos frente a la Raspberry Pi.

Disponiendo de las todas las cosas necesarias mencionadas anteriormente, se establecerá conexión vía SSH con el comando.

ssh “nombre de usuario”@”dirección_IP o nombre de dominio o host” “opciones”

En caso de no haber modificado el puerto por defecto para el acceso vía SSH, no es necesario indicar el puerto como se observa en la ventana de la captura superior con la opción “-p 22”, puesto que el puerto por defecto del protocolo SSH es el 22.

ssh pi@proyectmasbpivpn.ddns.net -p 22



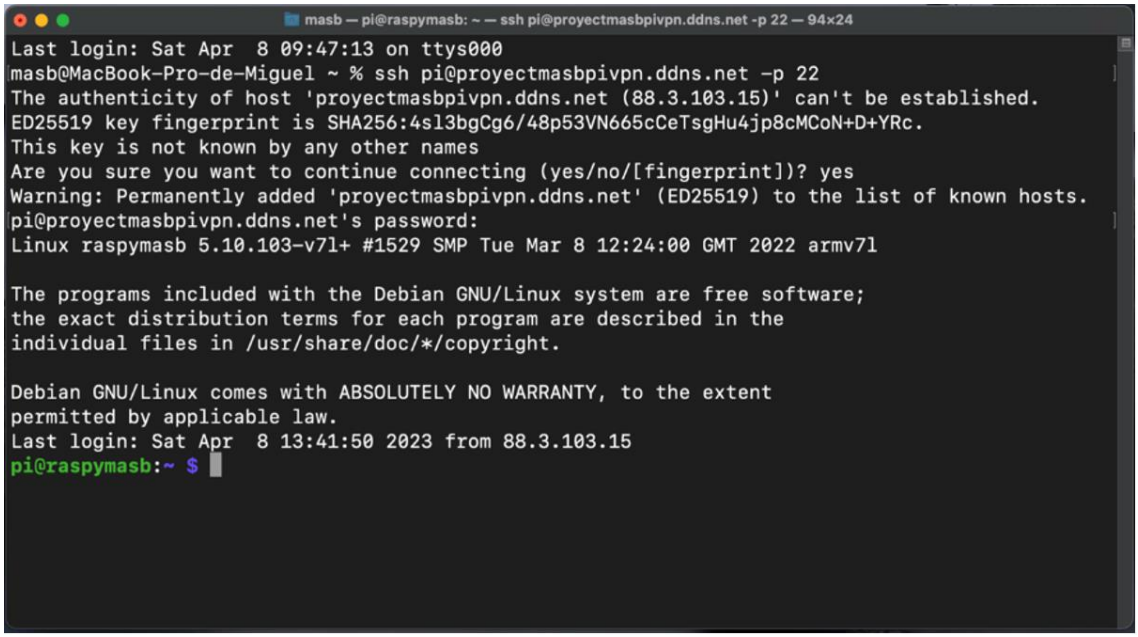
Si como se muestra en la ventana de la captura superior, es la primera vez que se establece la conexión, se mostraran estos mensajes que aparecen en la captura.

“The authenticity of host ‘proyectmasbpivpn.ddns.net (88.3.103.15)’ can´t be established.
ED25519 key fingerprint is `SHA256:4sl3bgCg6/48p53VN665cCeTsgHu4jp8cMCoN+D+YRc`
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?”

“No se puede establecer la autenticidad del host ‘proyectmasbpivpn.ddns.net (88.3.103.15)’.
La huella dactilar de la llave ED25519 es `SHA256:4sl3bgCg6/48p53VN665cCeTsgHu4jp8cMCoN+D+YRc`
Esta clave no es conocida por ningún otro nombre.
¿Está seguro de que desea continuar con la conexión (sí/no/[huella digital])?”

Se escribirá yes y se pulsará la tecla INTRO para poder acceder vía SSH al dispositivo remoto.

Se solicitará la password del usuario con el que se está intentando acceder, en este caso se trata del usuario “pi”.

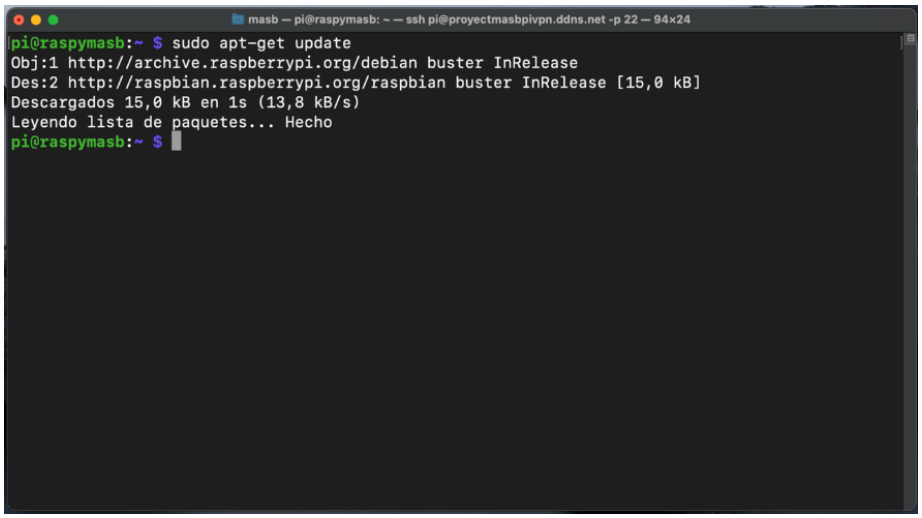


Una vez proporcionada la contraseña, se habrá iniciado sesión remota al dispositivo vía SSH.

En este caso es como si nos encontrásemos sentado delante del monitor localmente y en el terminal de la Raspberry Pi.

Instalación PiVPN a través de SSH.

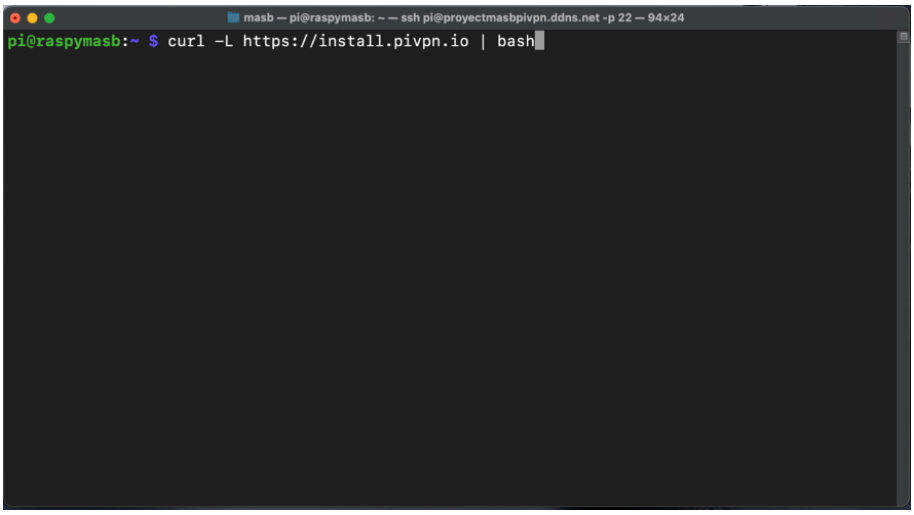
URL. https://docs.pivpn.io/install/



Para la instalación de PiVPN vía SSH no se explicará tan detalladamente, puesto que en caso de necesitar algún tipo de explicación, se encuentra explicado en la instalación local de PiVPN, en este caso se indican las opciones elegidas para realizar este proyecto.

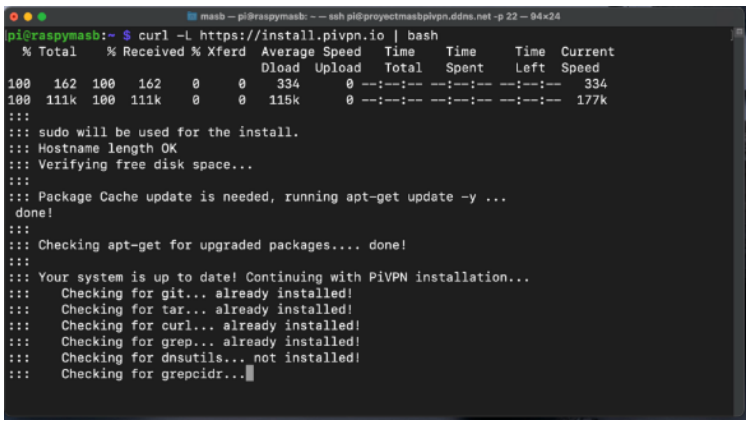
Se actualizarán los repositorios con el comando.

sudo apt-get update

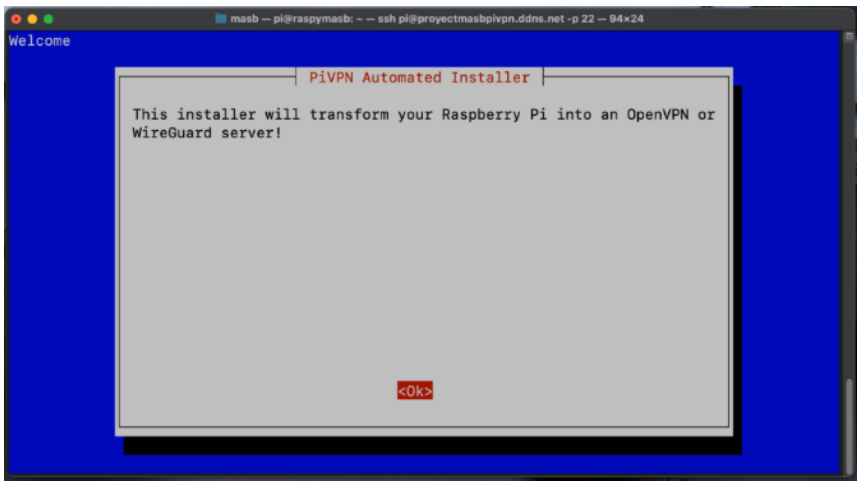


Tras la actualización de los repositorios, se ejecuta el comando para la instalación de PiVPN, comando.

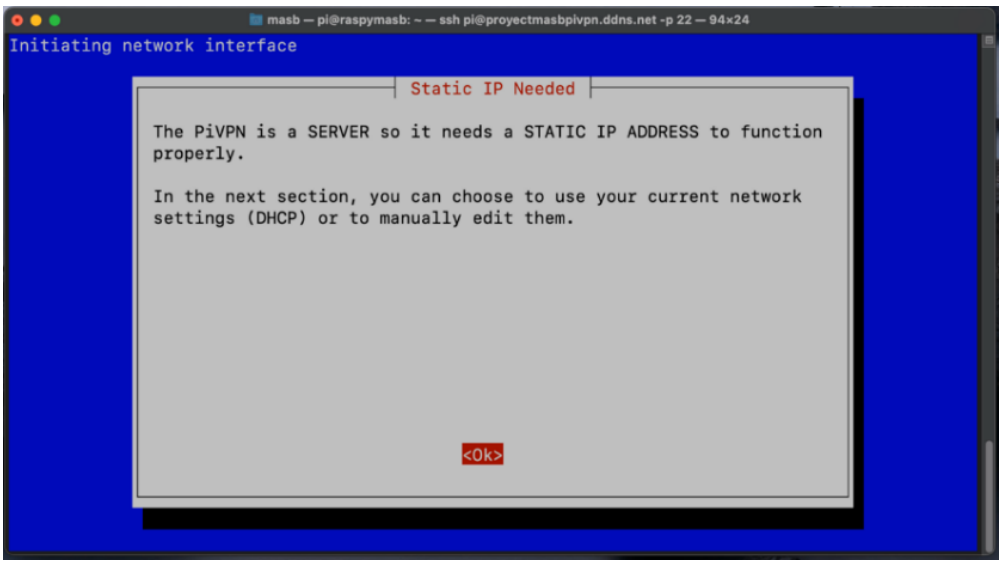
curl -L https://install.pivpn.io | bash



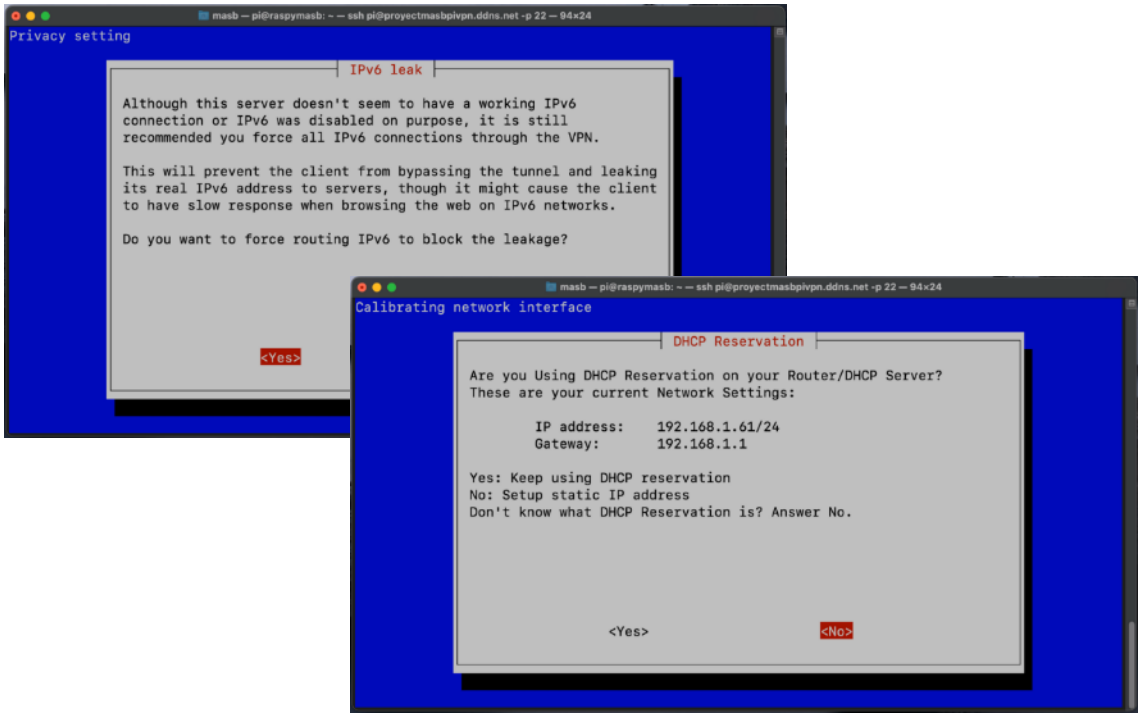
El programa de instalación comprobará si es necesario la instalación de aplicaciones.



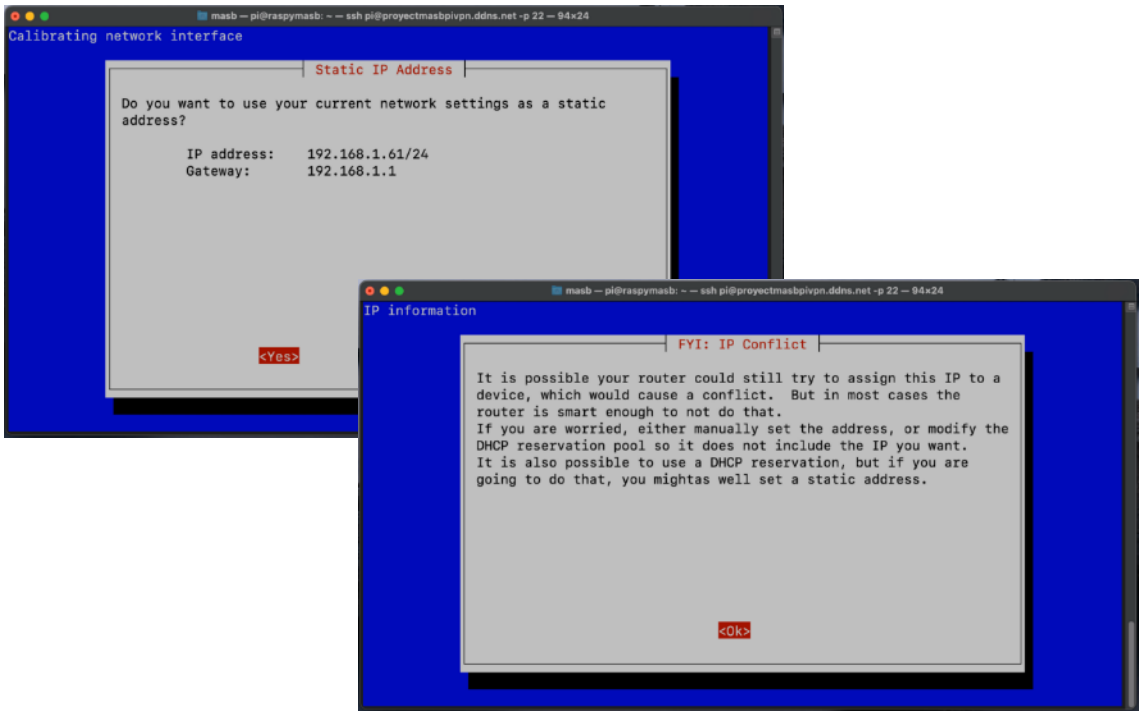
Se pulsará INTRO al encontrarse seleccionado OK.



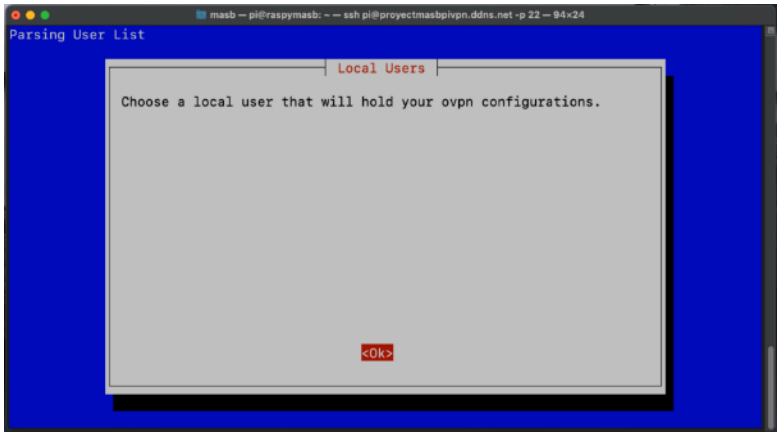
Nuevamente se pulsará INTRO al encontrarse seleccionado OK.



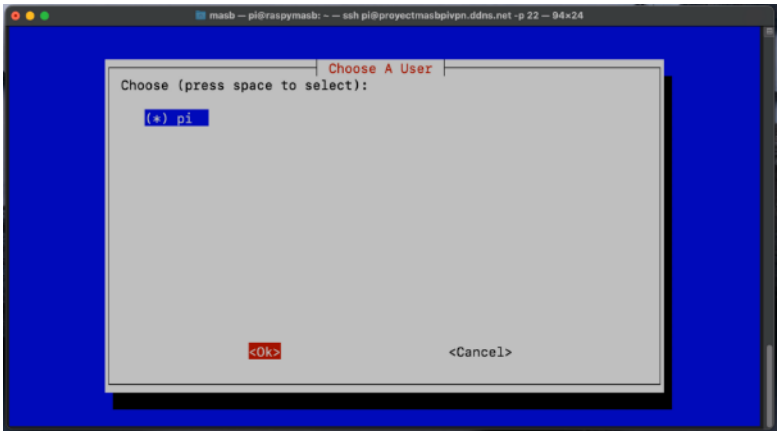
En las siguientes ventanas, se seleccionará Yes y posteriormente No, pulsando INTRO.



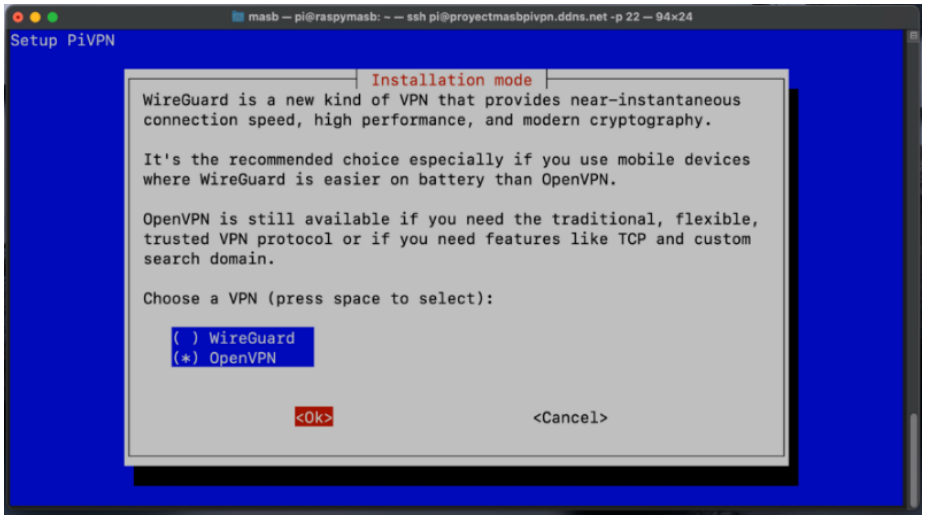
A continuación, se seleccionará Yes y posteriormente al encontrarse OK seleccionado habrá que pulsar INTRO.



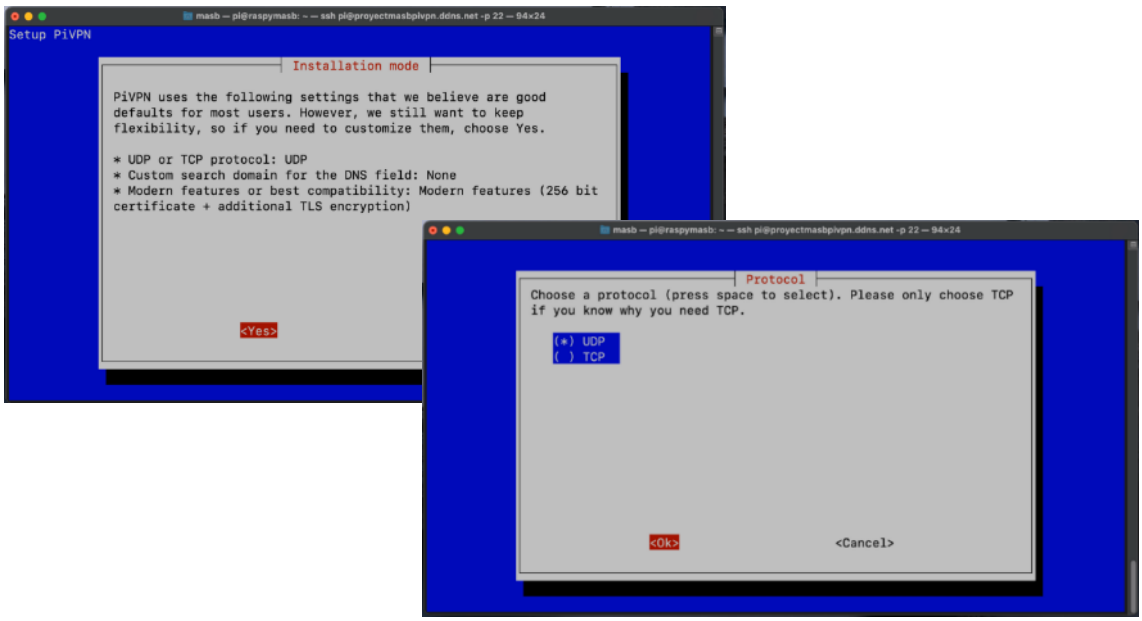
Se pulsará INTRO al encontrarse seleccionado OK.



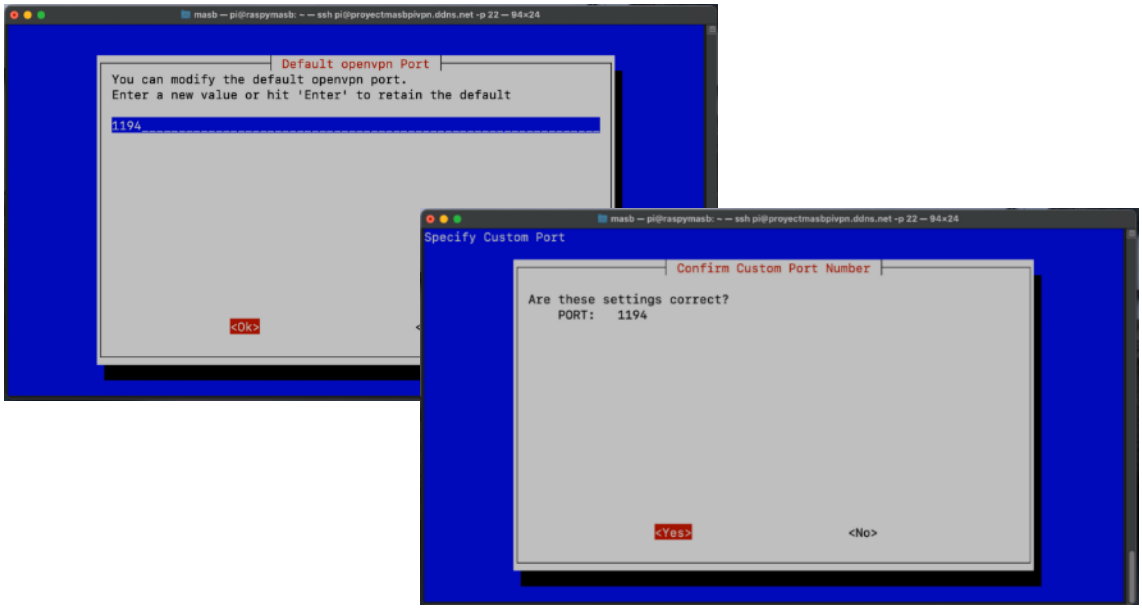
Al solo existir en el servidor VPN/WOL el usuario pi, solo se podrá seleccionar este usuario, teniendo que seleccionar a continuación Ok y pulsar INTRO.



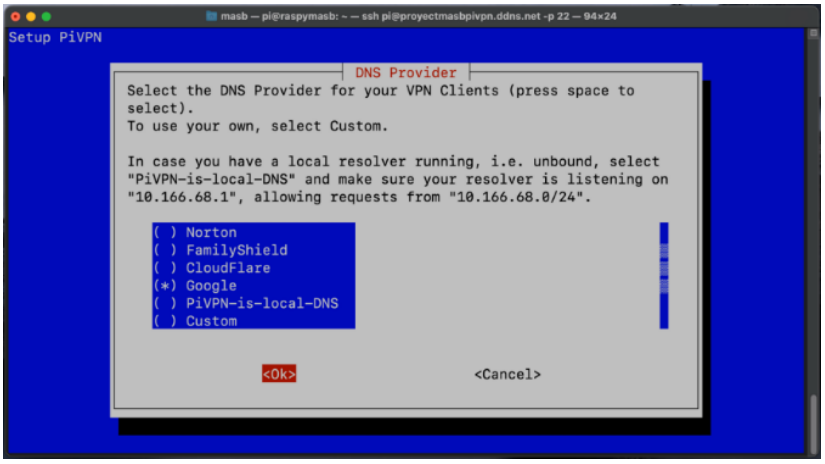
Para este proyecto se selecciona la opción OpenVPN, se selecciona Ok y se pulsará INTRO.



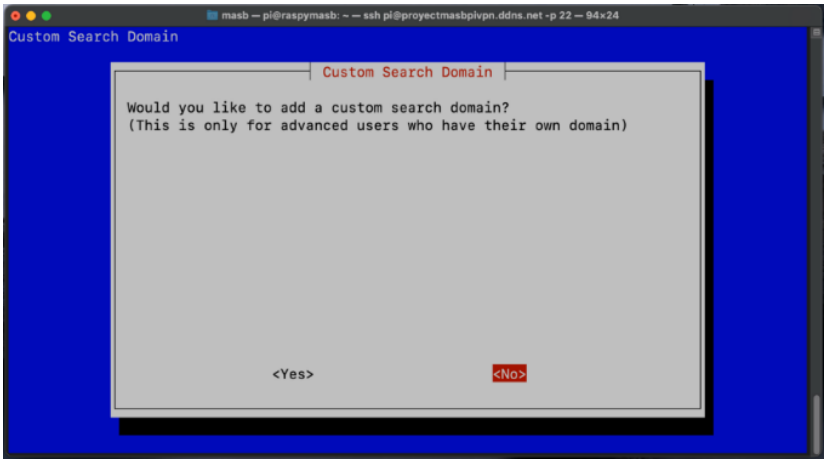
Se dejará la opción seleccionada por defecto (protocolo UDP), seleccionando OK y pulsando INTRO.



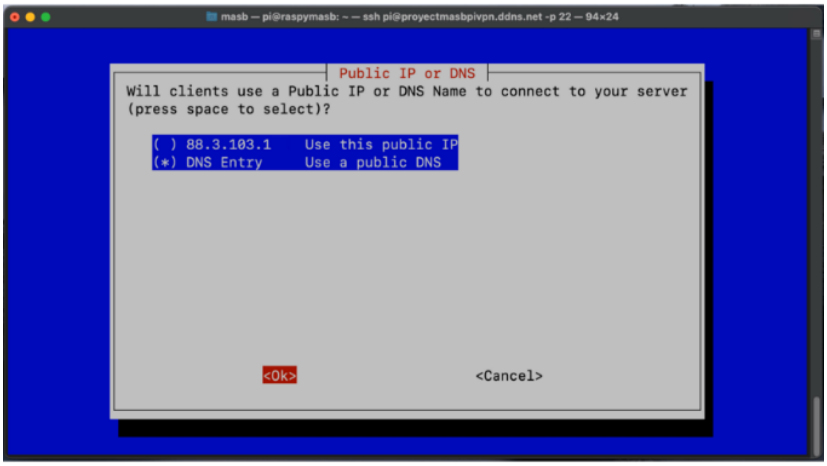
En la siguiente pantalla, se deja el puerto de conexión por defecto como el que se indica en la captura de la ventana superior (puerto 1194), tras lo que a continuación en la ventana siguiente, se confirmará seleccionando Yes y se pulsará INTRO.



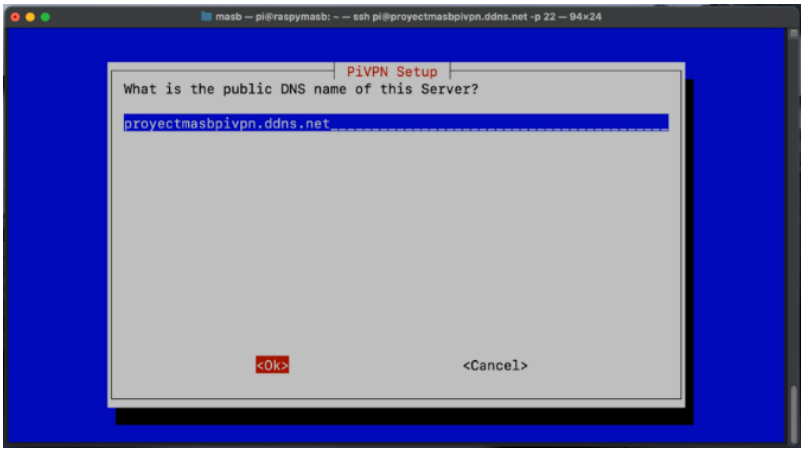
Para este proyecto, se elige como proveedor de DNS Google, seleccionando posteriormente OK y pulsando INTRO.



En esta ventana, se seleccionará No, a continuación se pulsará INTRO.



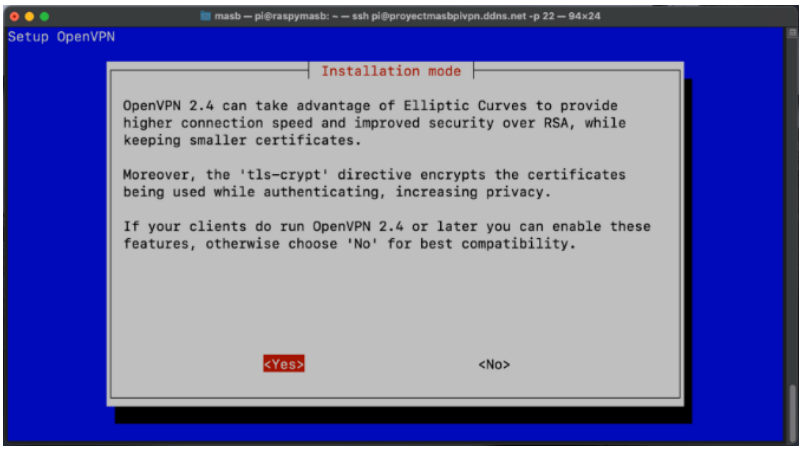
En la ventana de la captura superior se selecciona “DNS Entry Use a public DNS”, pulsando posteriormente sobre Ok.



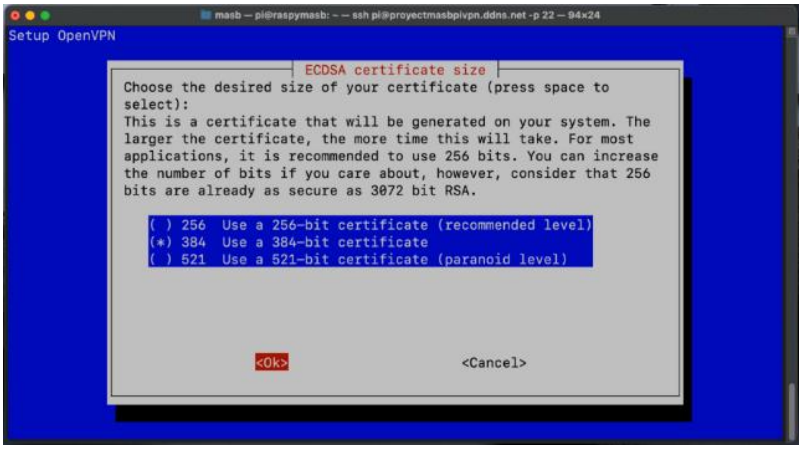
Como nombre DNS público, se escribirá en este caso, el nombre de dominio o host creado en el proveedor de servicios DDNS, siendo este nombre de host proyectmasbpivpn.ddns.net, acto seguido se seleccionará Ok y se pulsará INTRO.



En la ventana de confirmación, si se escribió correctamente el host, se seleccionará Yes y habrá que pulsar INTRO.

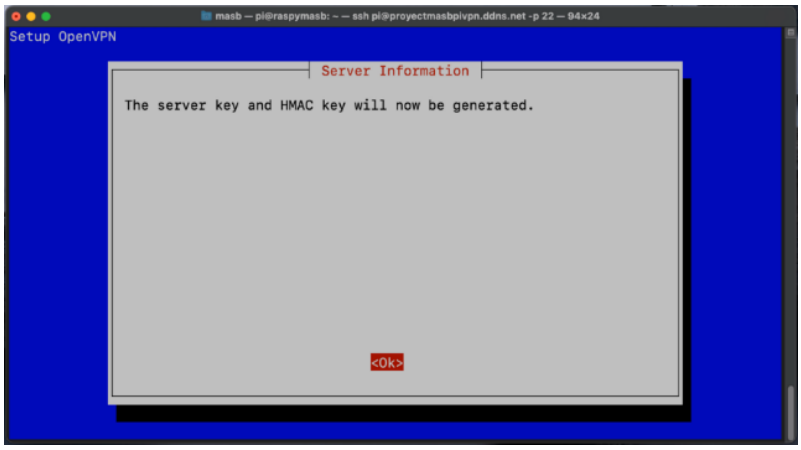


Se seleccionará Yes y se pulsará INTRO.

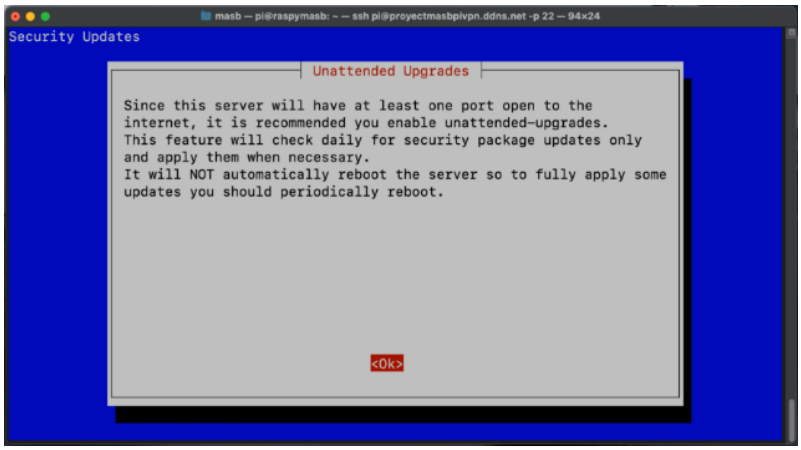


Aunque con la opción de 256, Use a 256-bit certificate …. podría valer, para el proyecto se selecciona la opción 384, Use a 384-bit certificate …

Seleccionando OK y pulsando a continuación INTRO.



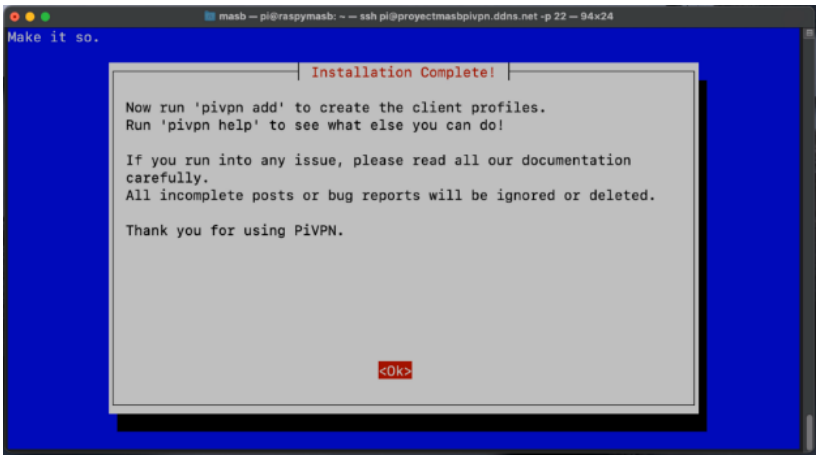
Al encontrarse seleccionado OK, se pulsará INTRO.



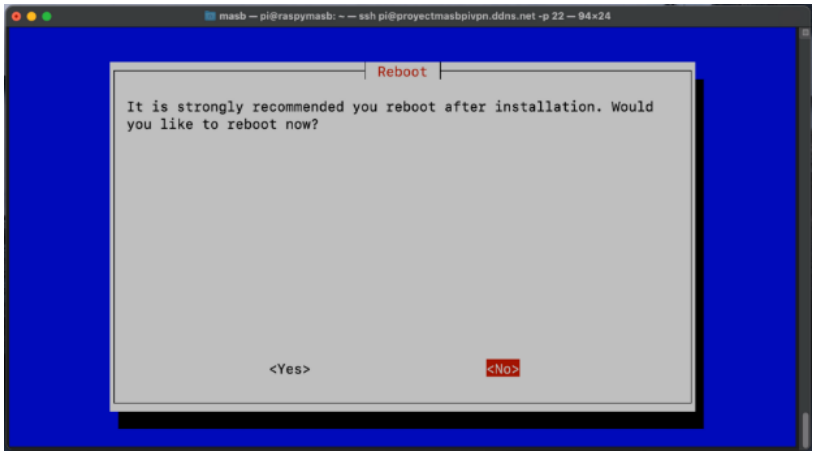
En esta nueva ventana, al encontrarse seleccionado OK, se pulsará INTRO.



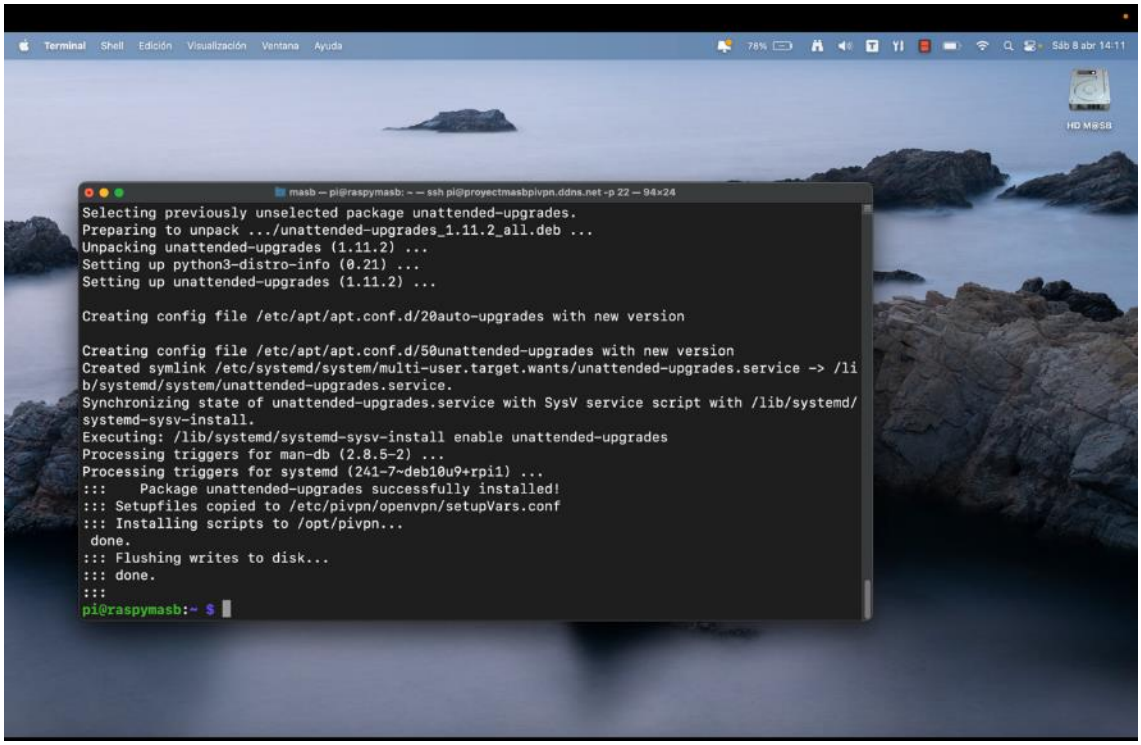
Se podrá habilitar las actualizaciones o parches de seguridad o negarlas, en este caso se habilitan, seleccionando Yes y pulsando INTRO.



Habrá que pulsar en esta ventana INTRO al encontrarse seleccionado Ok.



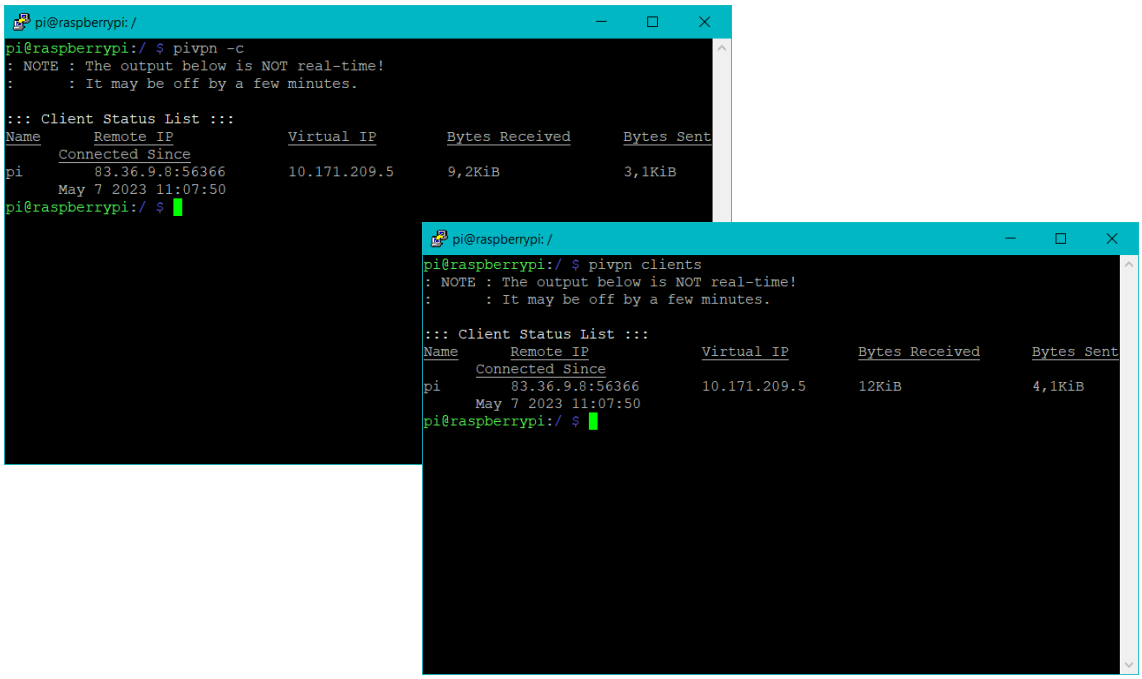
En todas las instalaciones de pruebas realizadas, nunca se activó la opción Yes para reiniciar la Raspberry Pi, por lo que se seleccionará Yes y se pulsará INTRO.



Finalmente, tras la instalación, el programa terminará dejando el prompt en el terminal como se puede observar en la ventana de la captura superior.

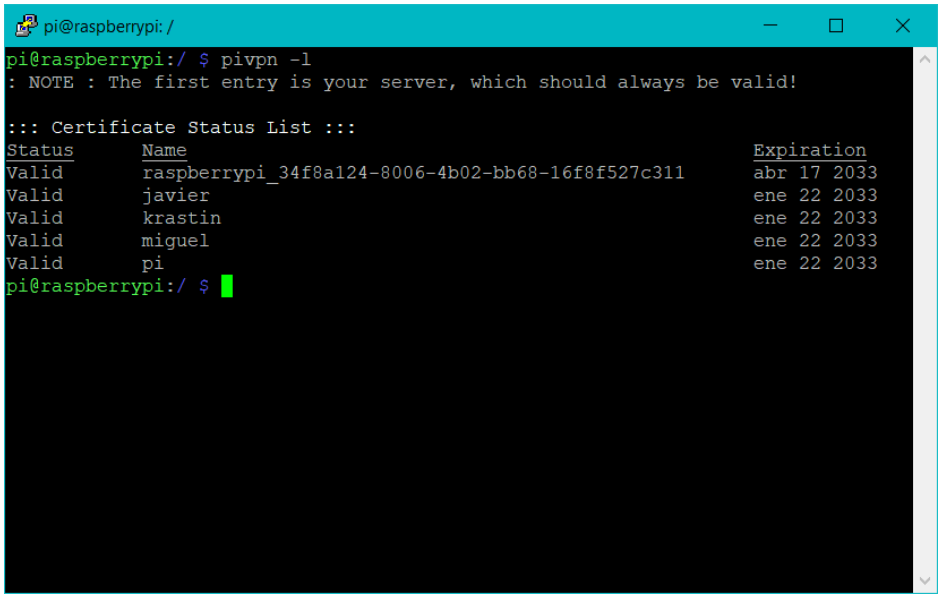
Una vez instalado PiVPN en el servidor VPN/WOL, para comprobar los clientes conectados, se podrá utilizar los comandos.

pivpn clients
pivpn -c



Para comprobar el estado de los clientes se podrá ejecutar el comando.

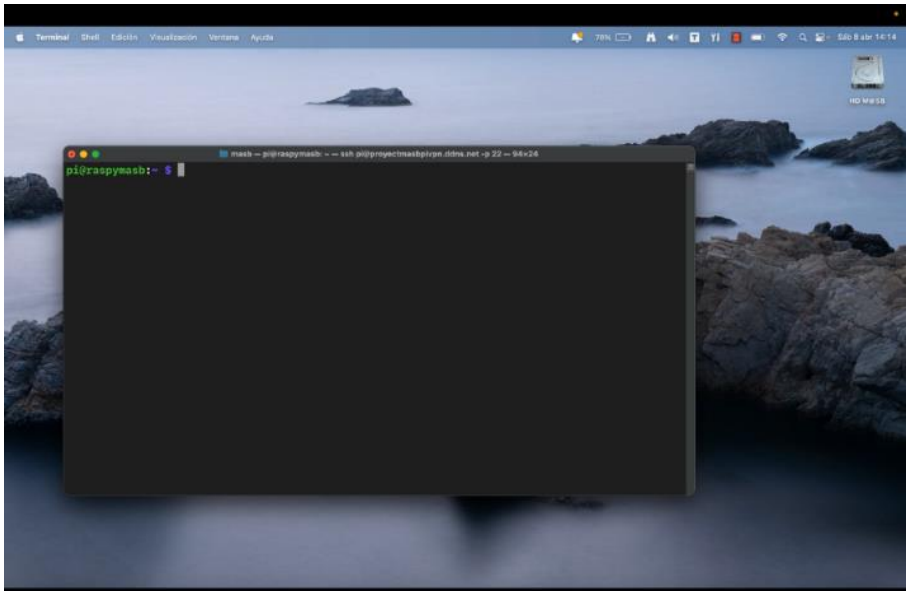
pivpn -l



Instalación WEBMIN vía SSH.

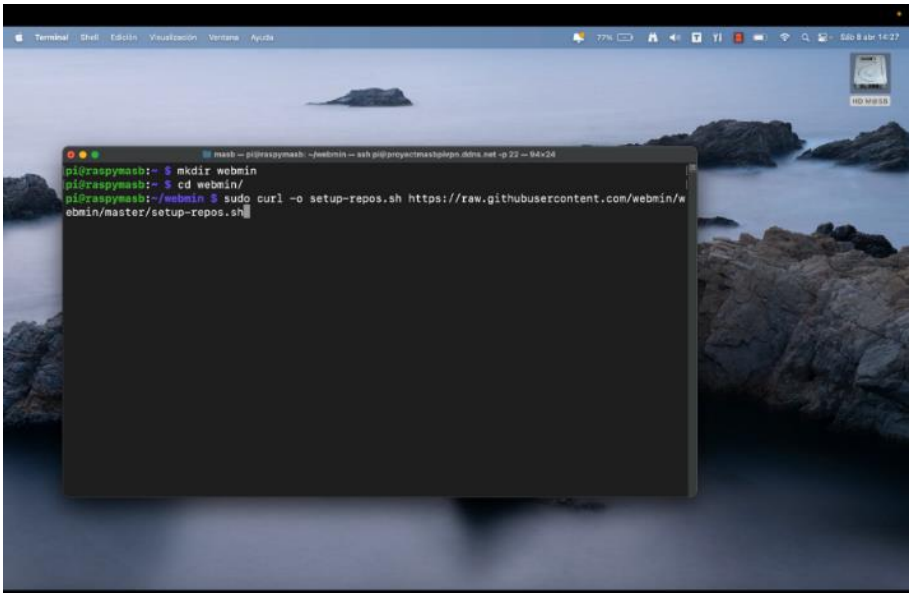
Según las últimas indicaciones en la WEB oficial del proyecto.

URL. https://webmin.com/download/

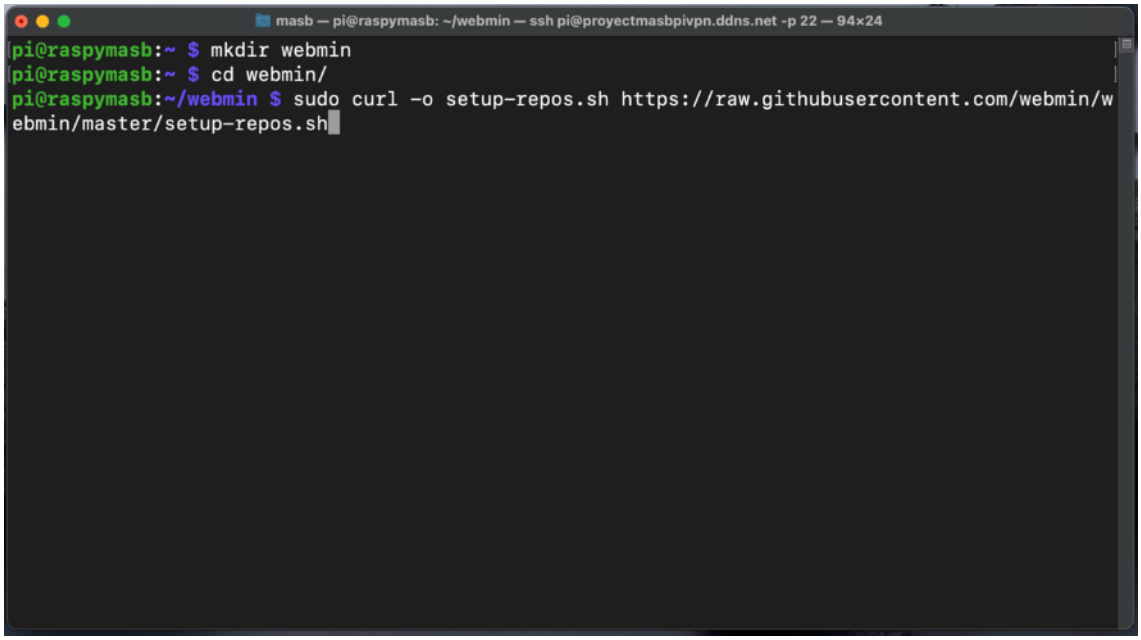


Estando conectado al servidor VPN/WOL a través del protocolo SSH con el comando.

ssh pi@proyectmasbpivpn.ddns.net -p 22

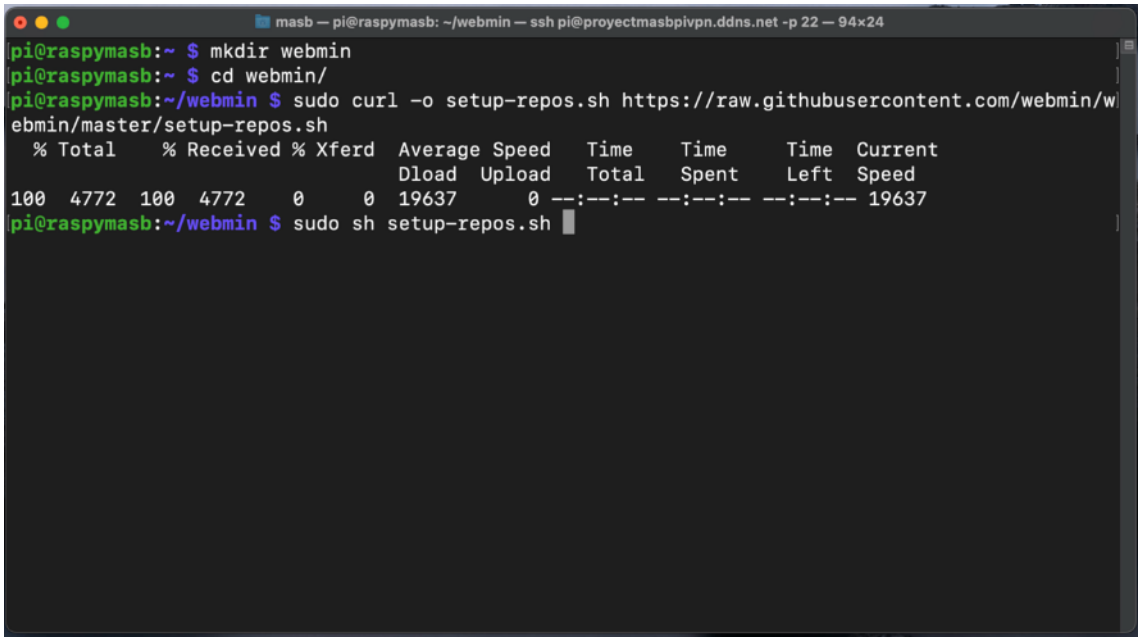


Se crea la carpeta webmin y se accede a ella con los comandos
Creación carpeta webmin, mkdir webim
Acceder a la carpeta creada, cd webmin



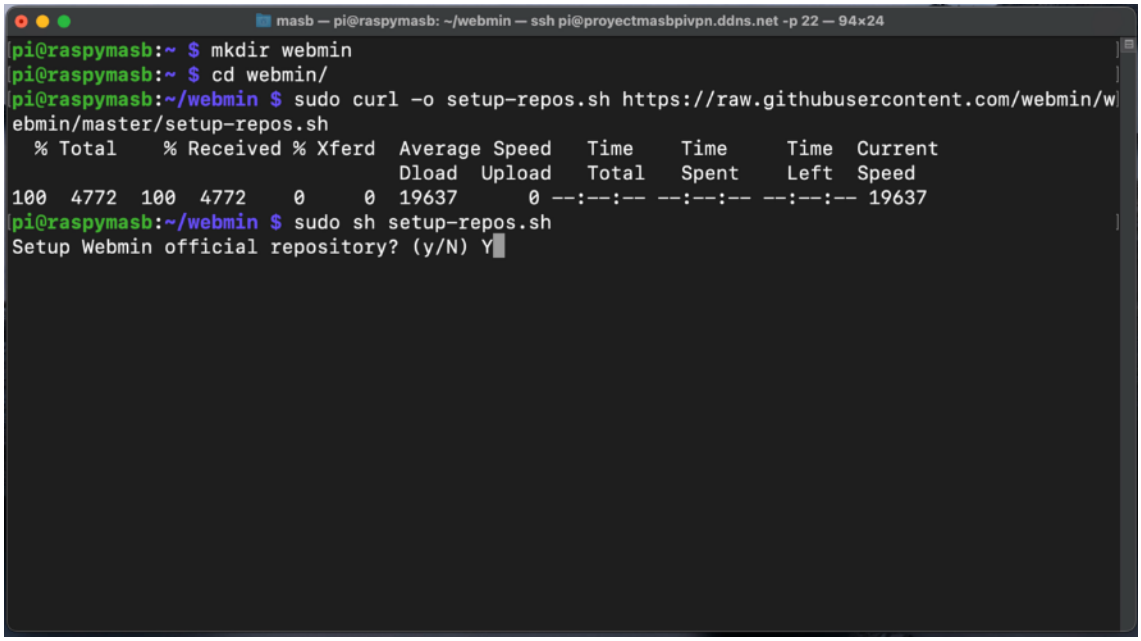
Se ejecutará el comando.

sudo curl -o setup-repos.sh
ttps://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh

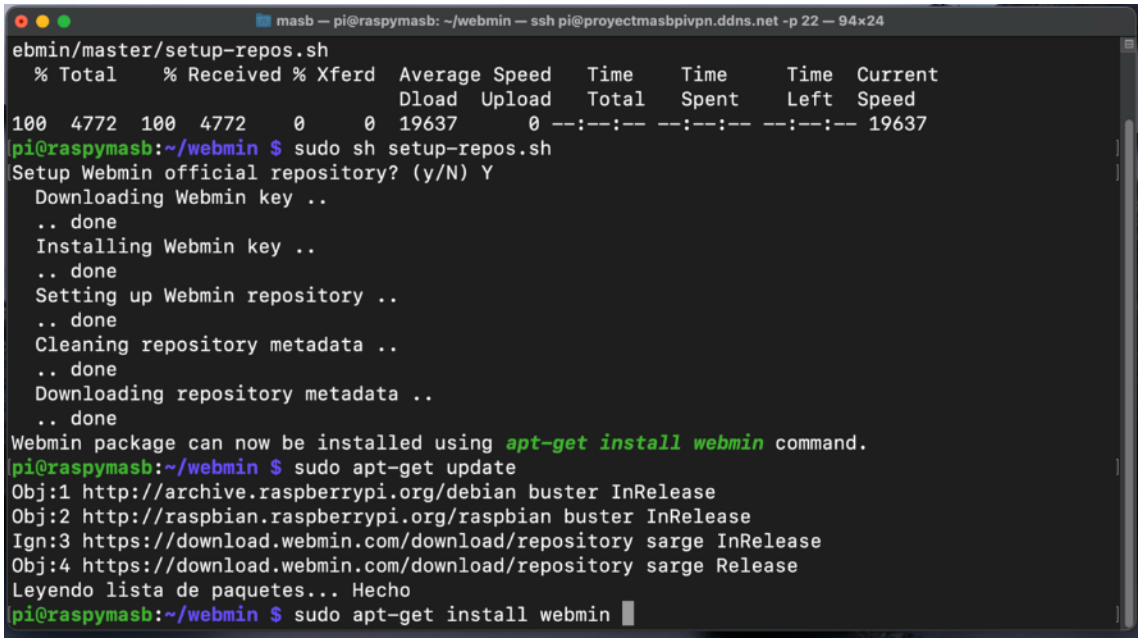


Descargado el fichero, se ejecutará el comando.

sudo sh setup-repos.sh

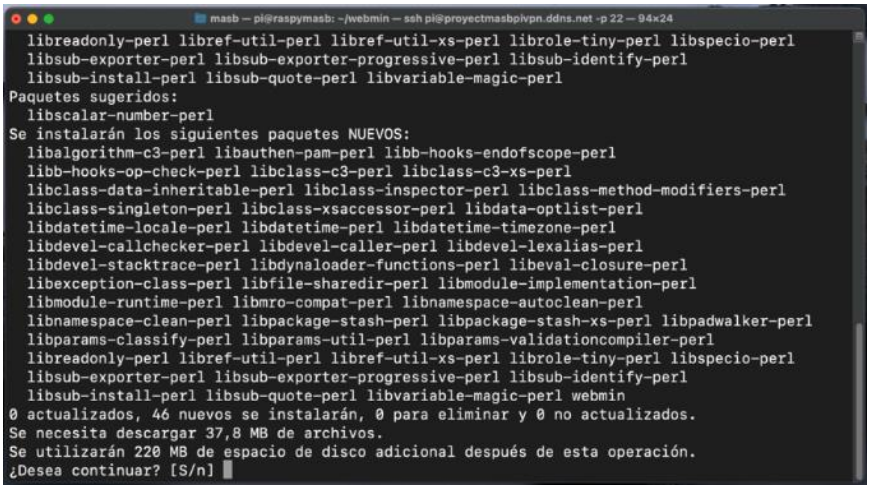


Se pulsará la tecla “Y”, pulsando a continuación INTRO.

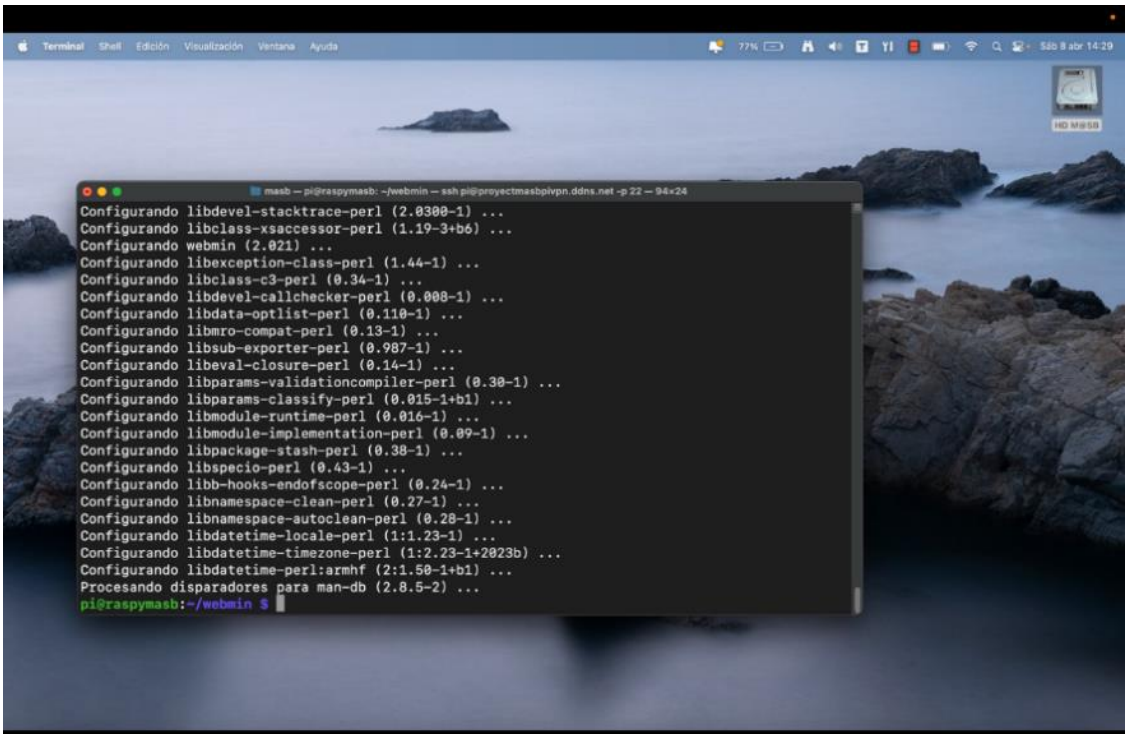


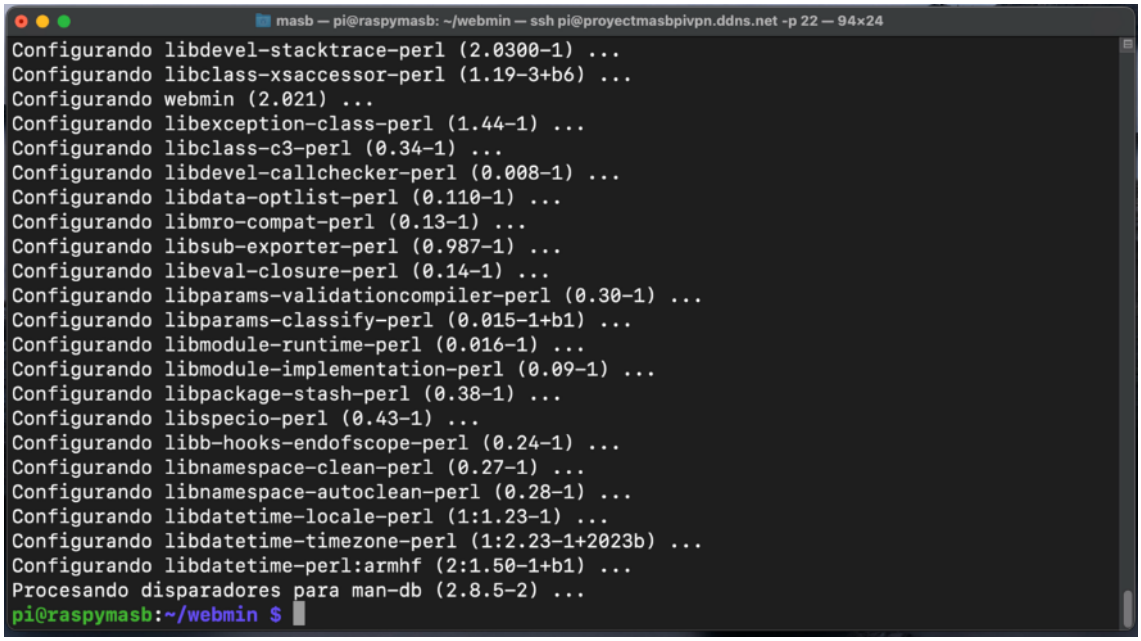
Se actualizarán los repositorios y se procederá con la instalación respectivamente con los comandos.

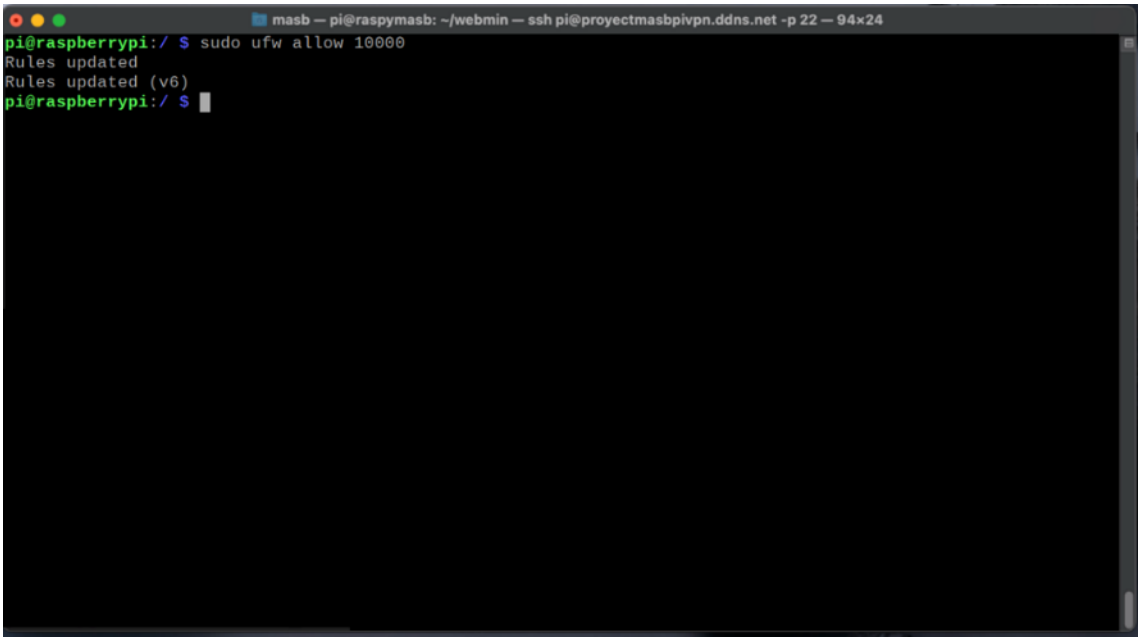
sudo apt-get update
sudo apt-get install webmin



Habrá que pulsar la tecla “S” para continuar con la instalación de todas las aplicaciones necesarias, tras pulsar la tecla “S”, posteriormente se pulsará INTRO.





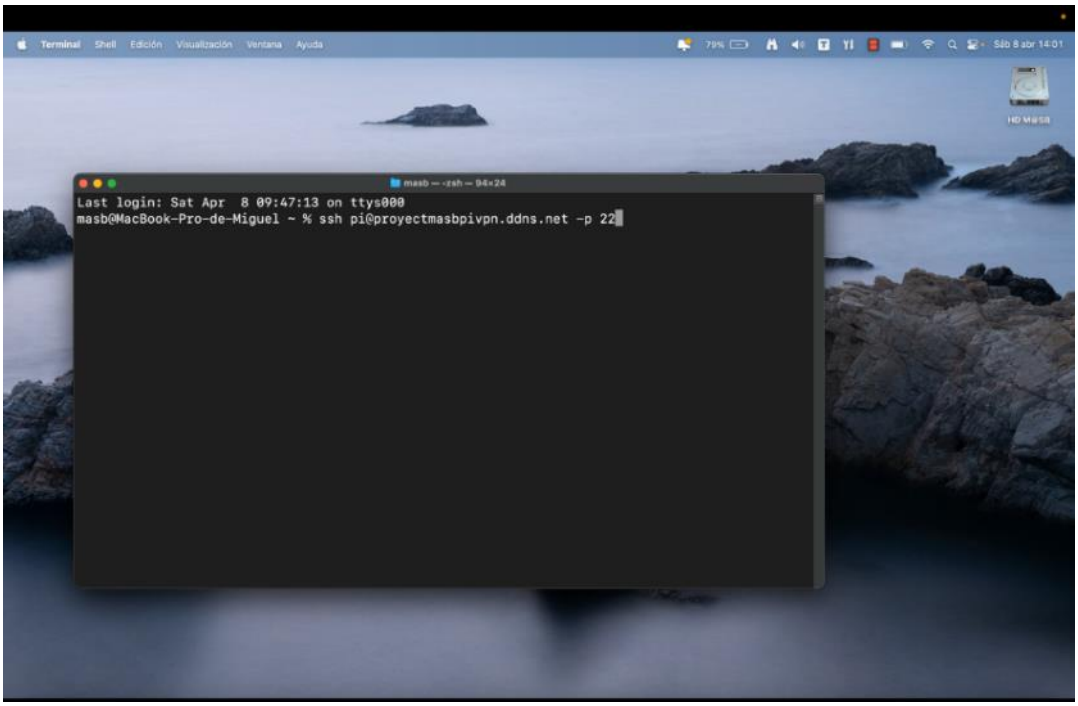


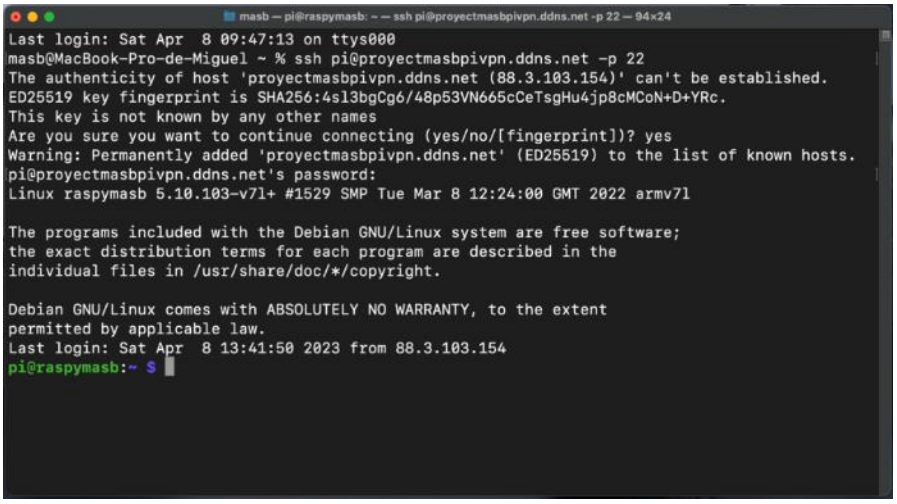
Finalizada la instalación, y para la apertura del tráfico en el cortafuegos, se ejecutará el comando

sudo ufw allow 10000

Con este comando, se permite la conexión a través del puerto 10000, que se abrió en el router y corresponde al puerto de conexión habitual de WEBMIN.

Instalación aplicaciones necesarias vía SSH.

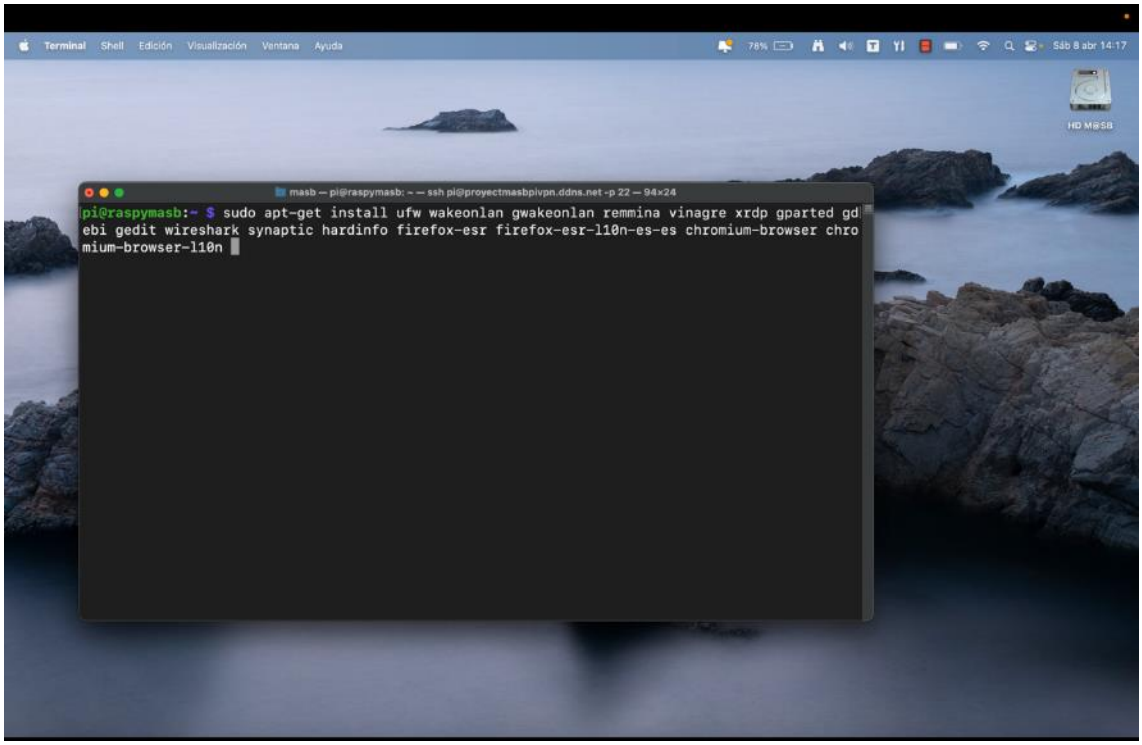


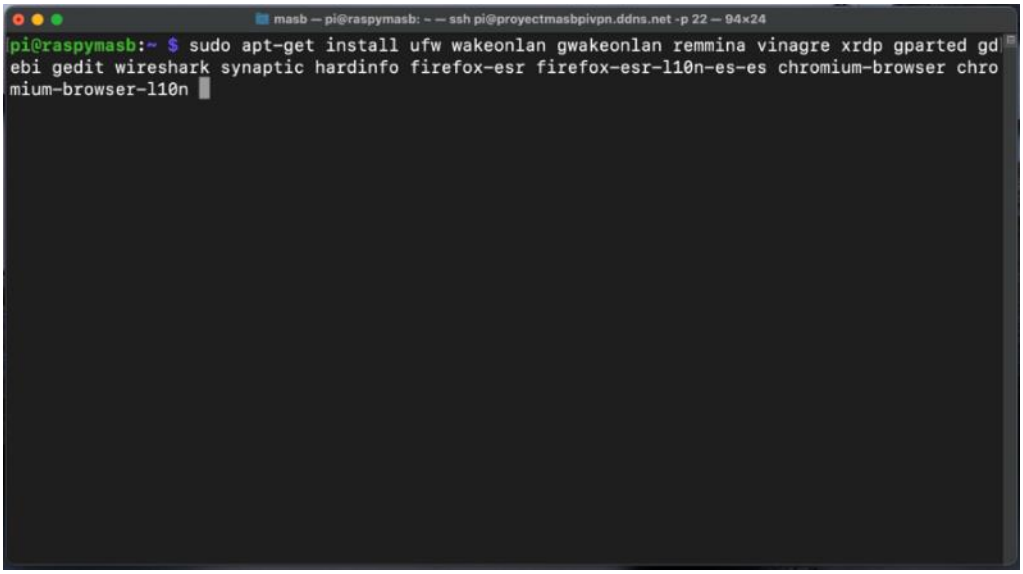


Una vez conectado remotamente al servidor VPN/WOL vía SSH con el comando.

ssh pi@proyectmasbpivpn.ddns.net -p 22

Se podrá llevar a cabo la instalación de las aplicaciones necesarias remotamente a través de SSH.

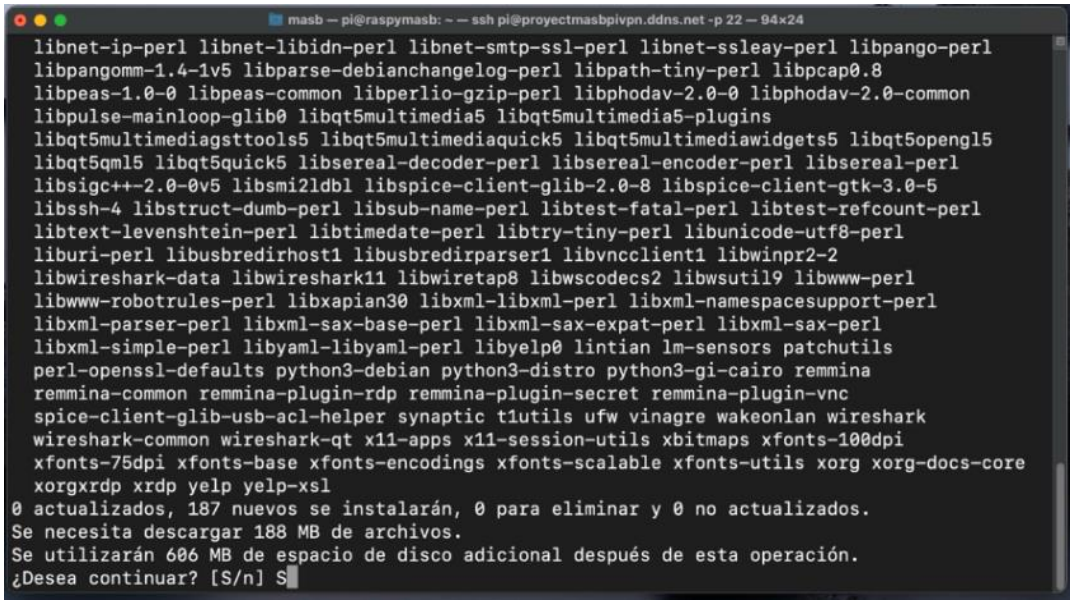




Comando para realizar la instalación.

sudo apt-get install ufw wakeonlan gwakeonlan remmina vinagre xrdp gparted gdebi gedit wireshark synaptic hardinfo firefox-esr firefox-esr-l10n-es-es chromium-browser chromium-browser-l10n

Anteriormente, se informó que no es necesaria la instalación de todas las aplicaciones como gparted, gedit, wireshark, firefox y chromium.

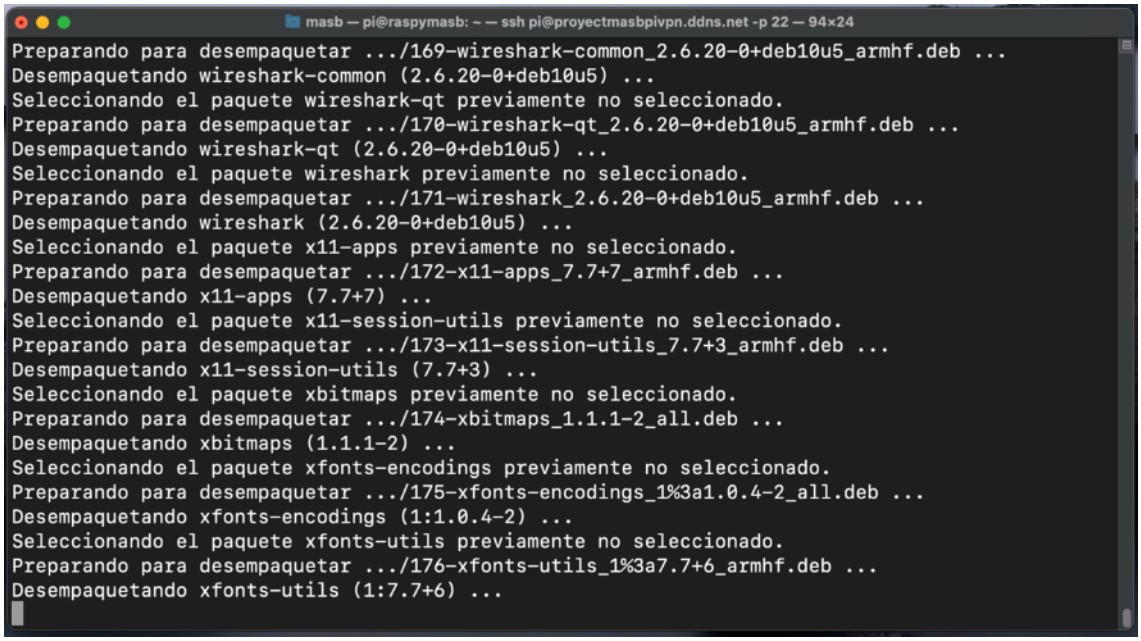


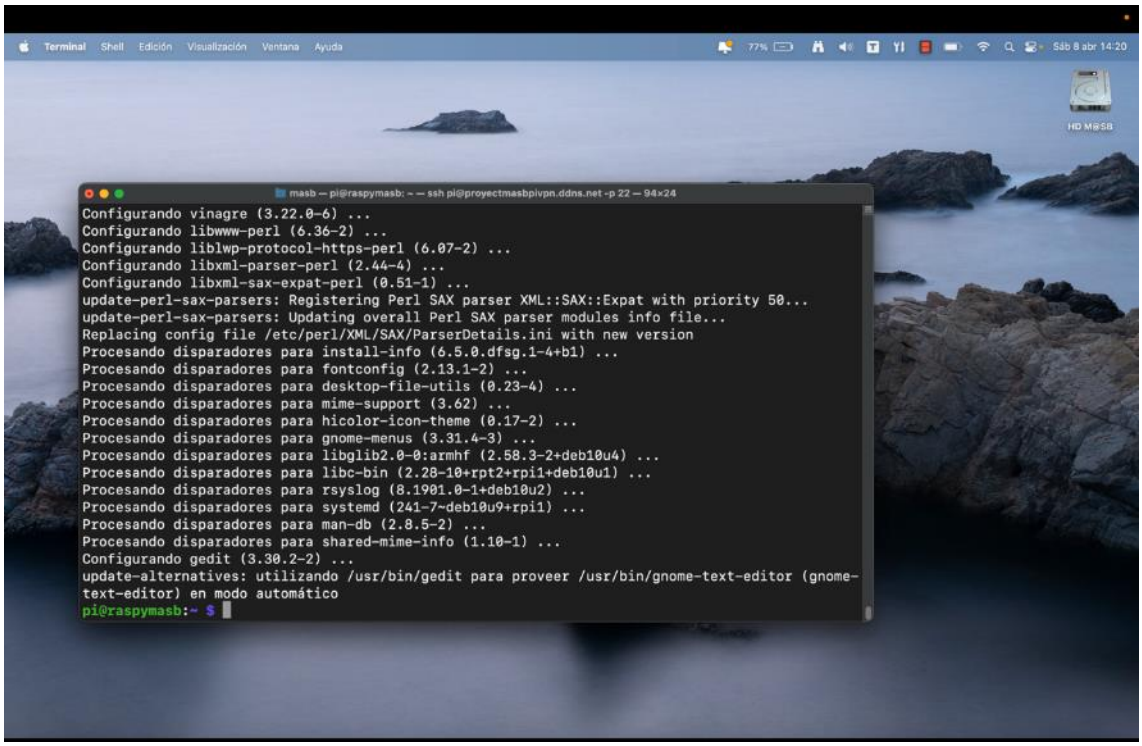
Se tendrá que teclear/escribir la tecla “S”, en este caso para proceder con la instalación de las aplicaciones y todas sus dependencias y pulsar INTRO.



Comenzando el proceso de instalación.

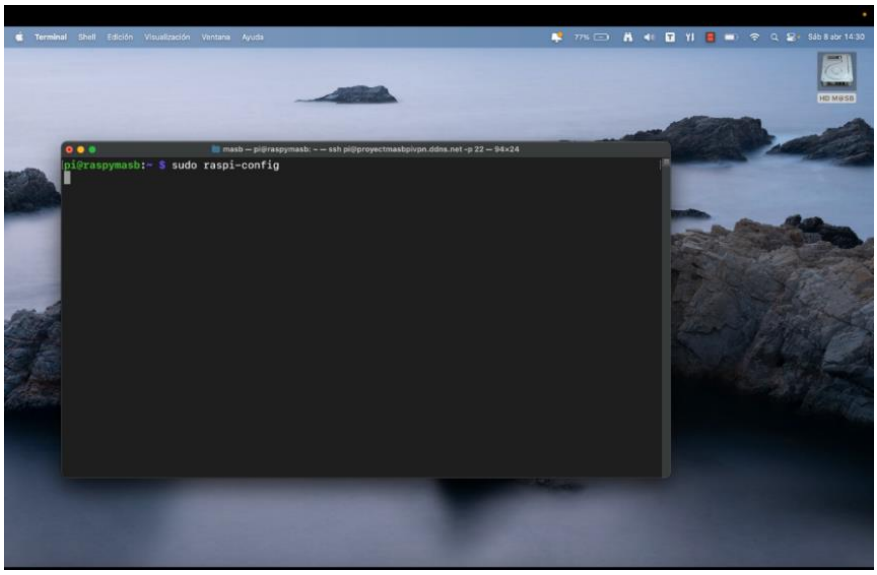
Como en este ejemplo se instala la aplicación wireshark, se pregunta si se quiere dejar a los usuarios sin permisos de administrador poder realizar capturas, en este caso se selecciona No y se pulsa INTRO.



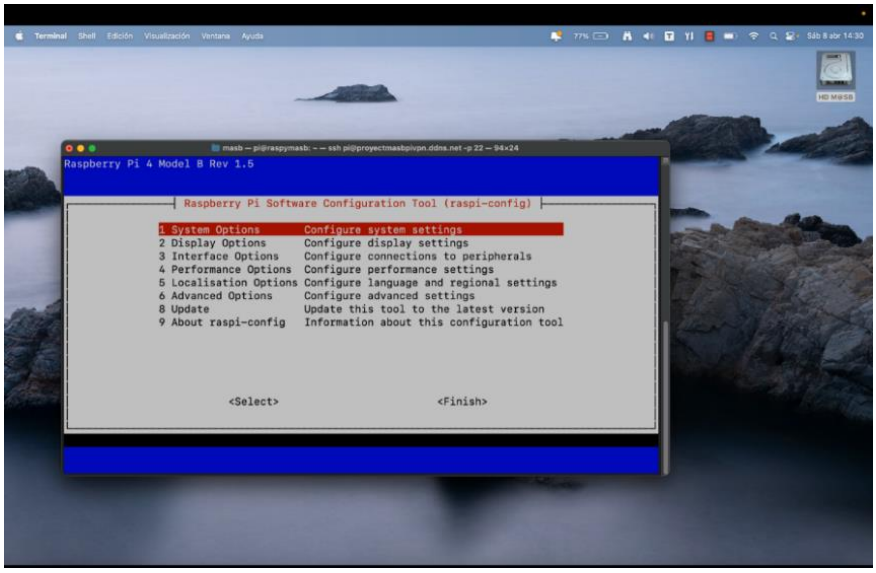


Terminada la instalación de las aplicaciones se continuará con las demás acciones a realizar.

Configuración Raspberry Pi vía remota a través de SSH.



Al encontrarse ya explicado anteriormente en la configuración local, en esta ocasión se indicarán las opciones y no se detallará tanto las explicaciones, en caso de necesitarse, habrá que acudir al apartado mencionado, “Asistente de configuración en terminal”.

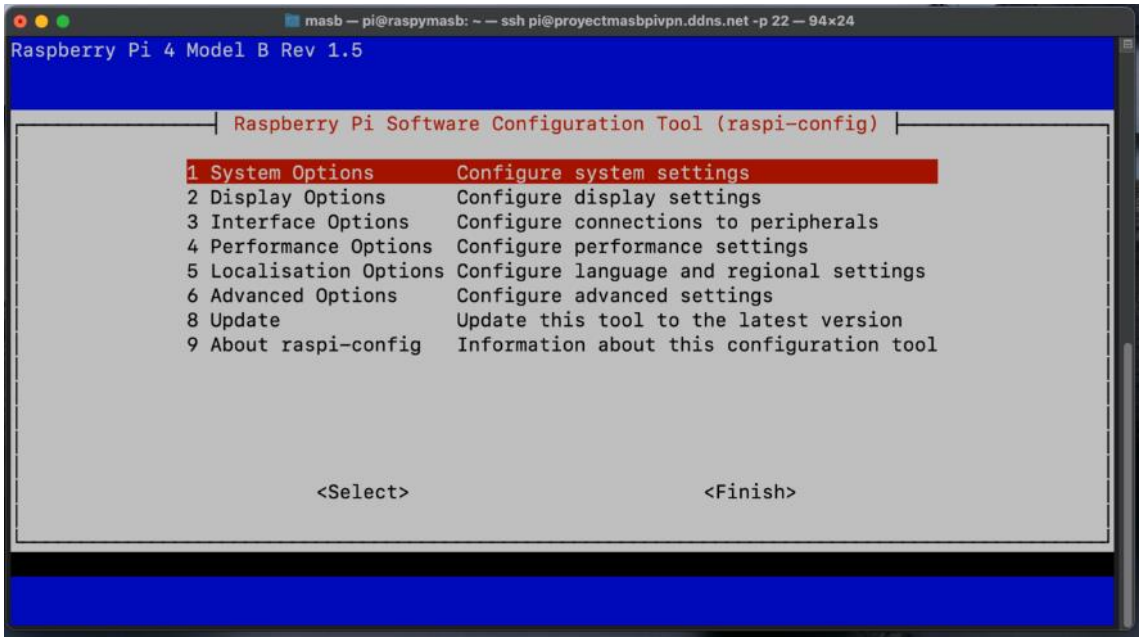


Para iniciar la configuración de la Raspberry Pi remotamente, estando conectado a través de SSH al servidor VPN/WOL con el comando.

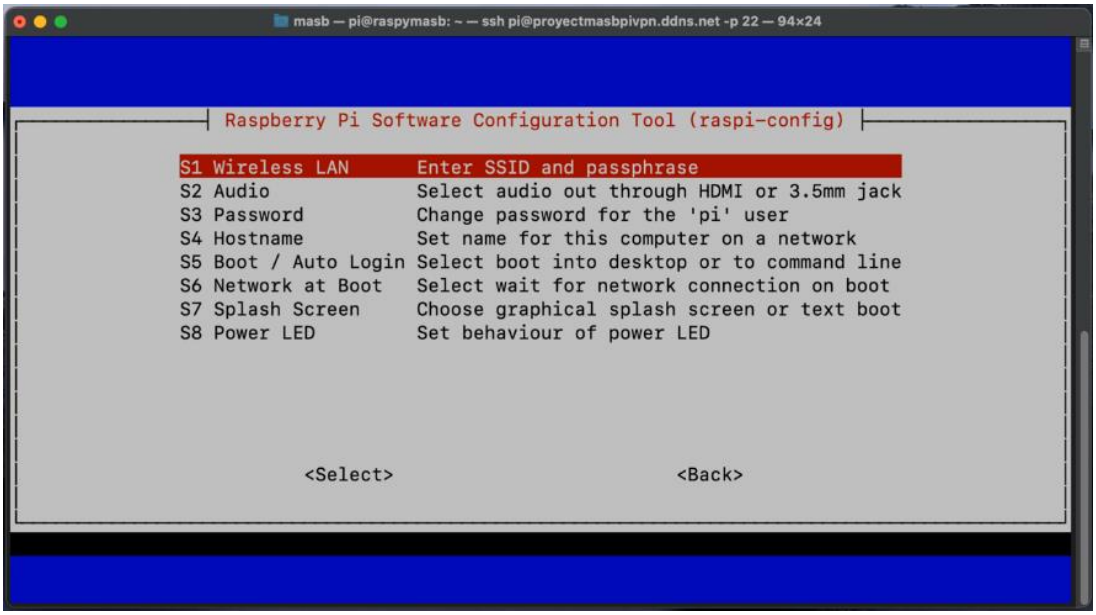
ssh pi@proyectmasbpivpn.ddns.net -p 22

Habrá que ejecutar dentro de un terminal remoto el comando.

sudo raspi-config

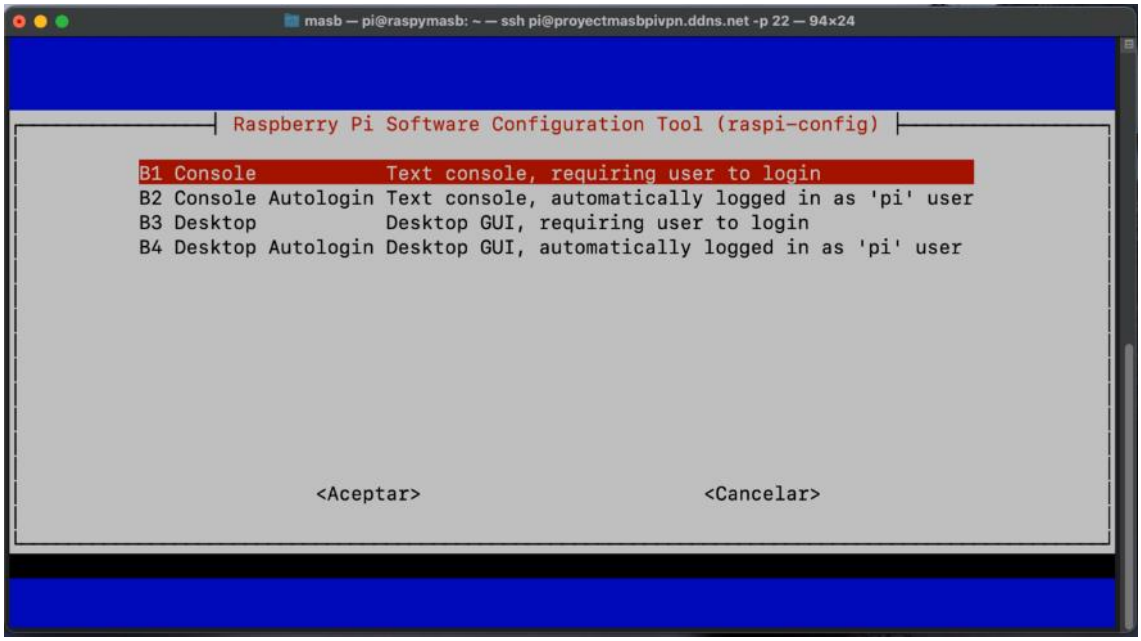


Apartado System Options.

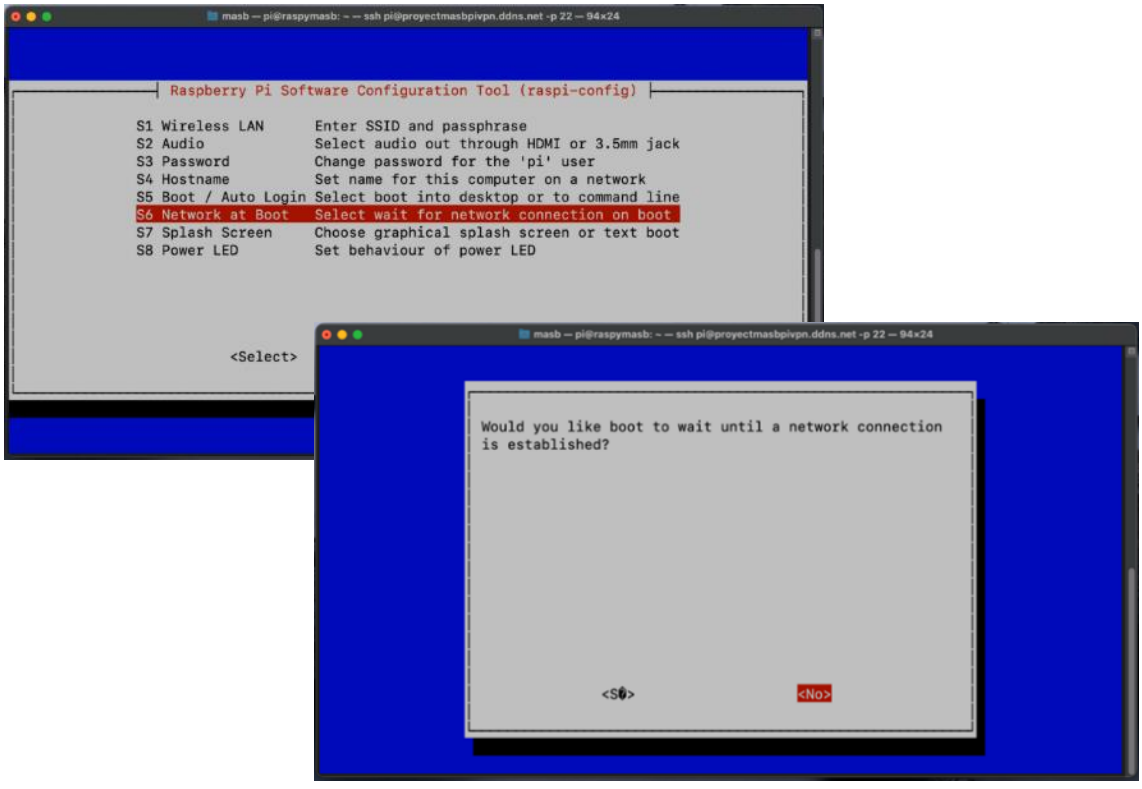


System Options.

- Wireless LAN, se podrá conectar a una red WIFI.
- Password, cambiar la contraseña del usuario en este caso “pi” (root).
- Hostname, modificar el nombre de Host (nombre del equipo Raspberry Pi).
- Boot / Auto Login, se podrá modificar como se accede al equipo, para este proyecto se selecciona inicio en modo texto y requerir usuario y contraseña para acceder.
- Network at Boot, requerir si se espera a la red en el inicio o no.
- Splash Screen.

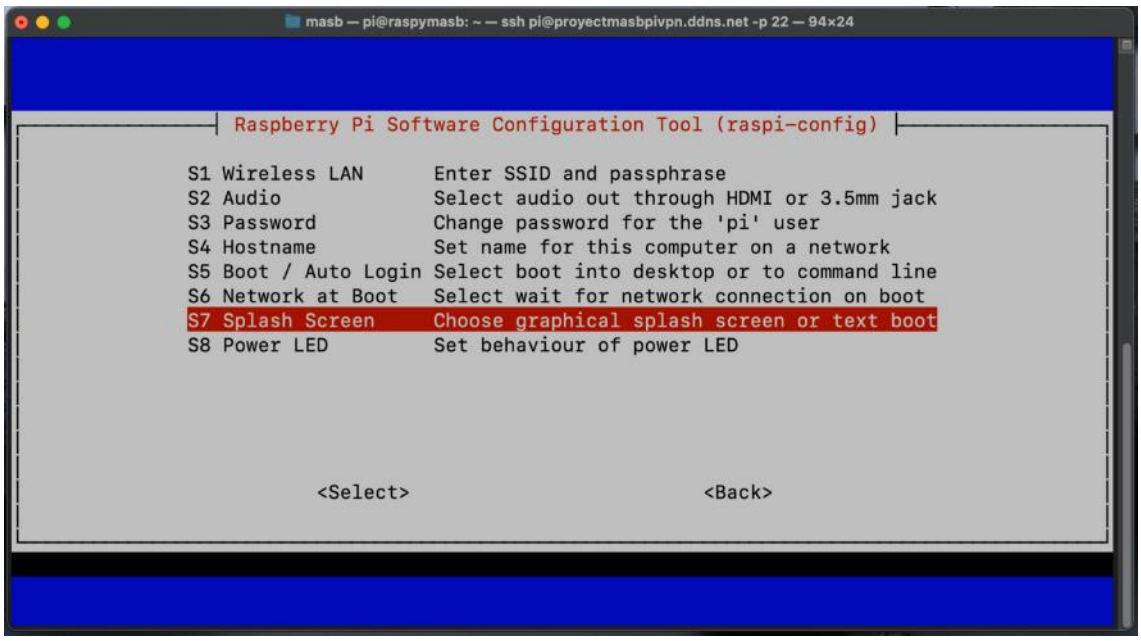


System Options \ Boot / Auto Login, para este proyecto se selecciona inicio en modo texto y requerir usuario y contraseña para acceder.

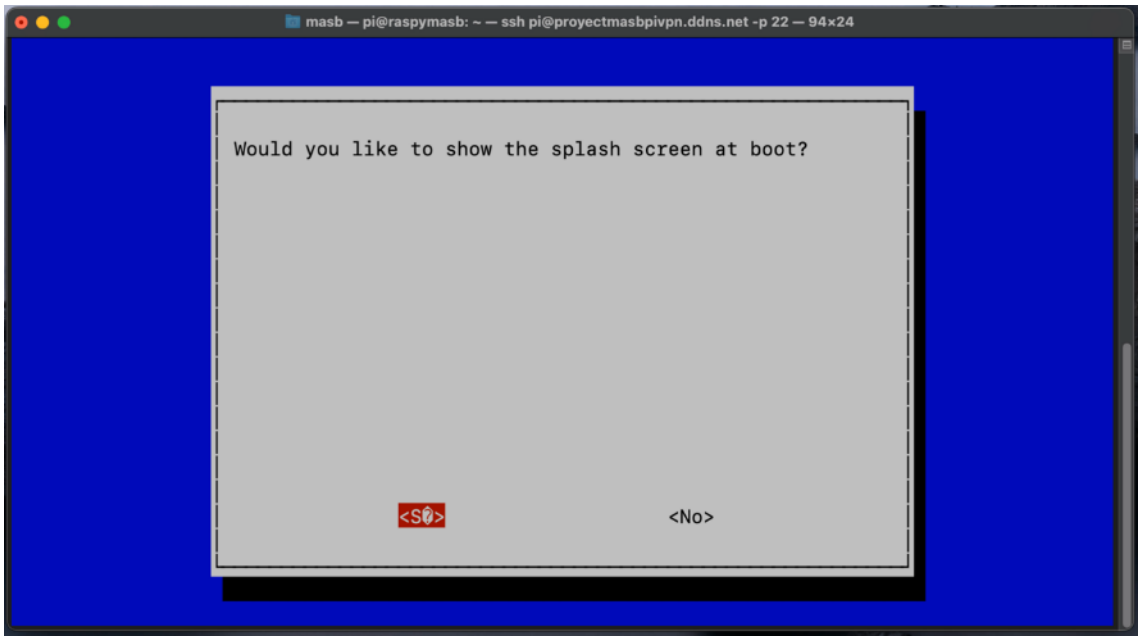


System Options \ Network al Boot.

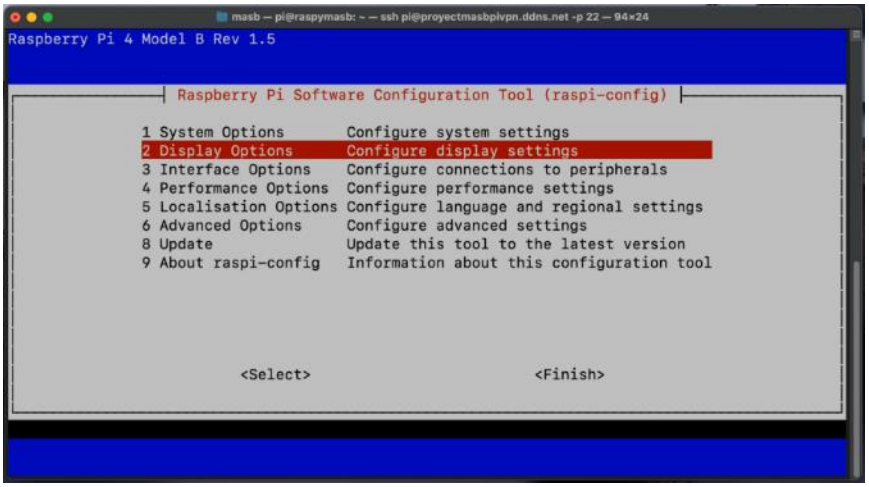
Se seleccionará No y se pulsará INTRO.



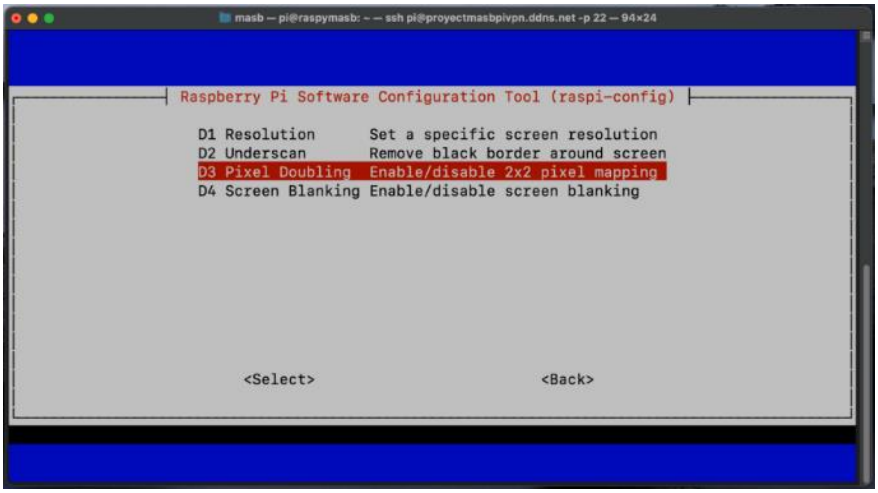
System Options \ Splash Screen.



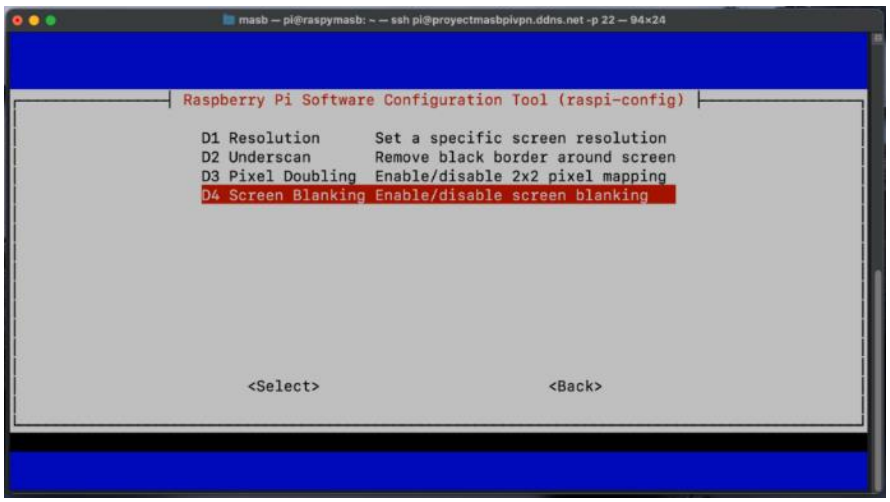
Se selecciona Si y se pulsará INTRO.



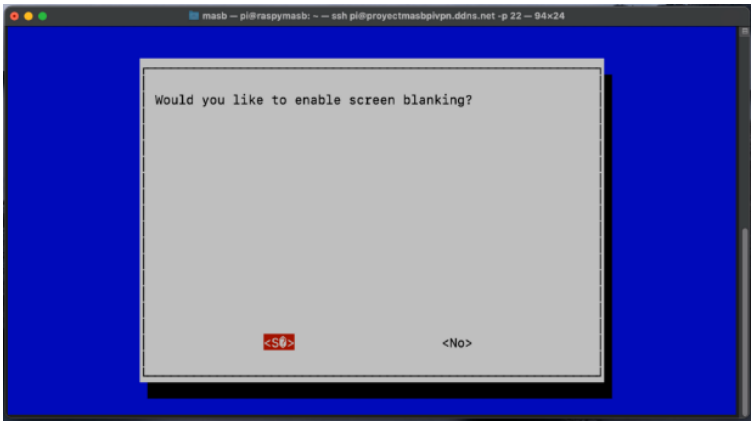
Sección Display Options.



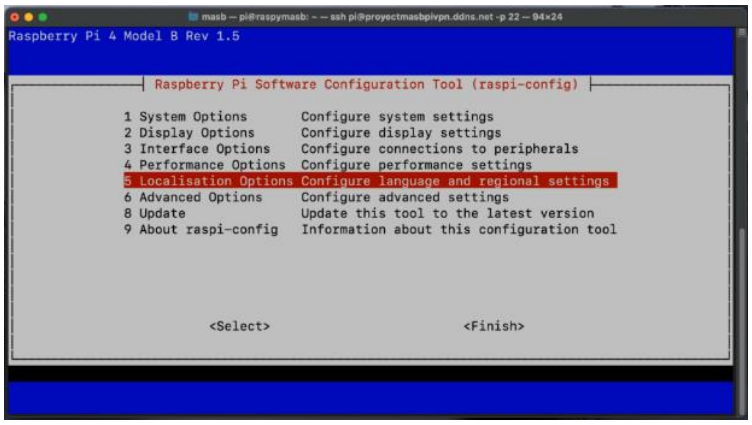
Opción Display Options \ Pixel Doubling, se seleccionará No.



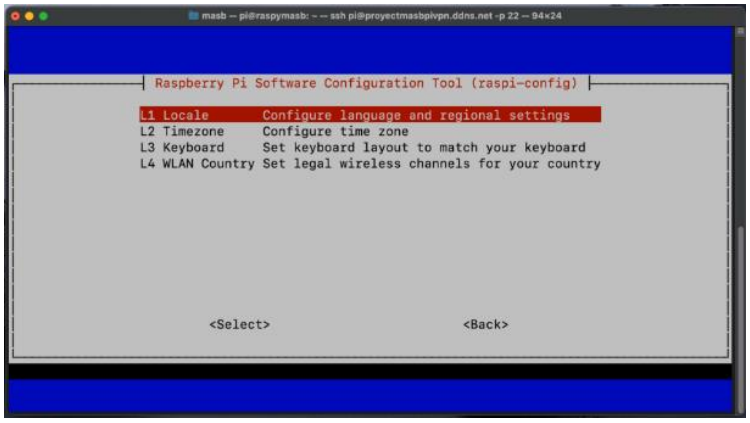
Display Options \ Screen Blanking.



Se seleccionará Si y se pulsará INTRO.

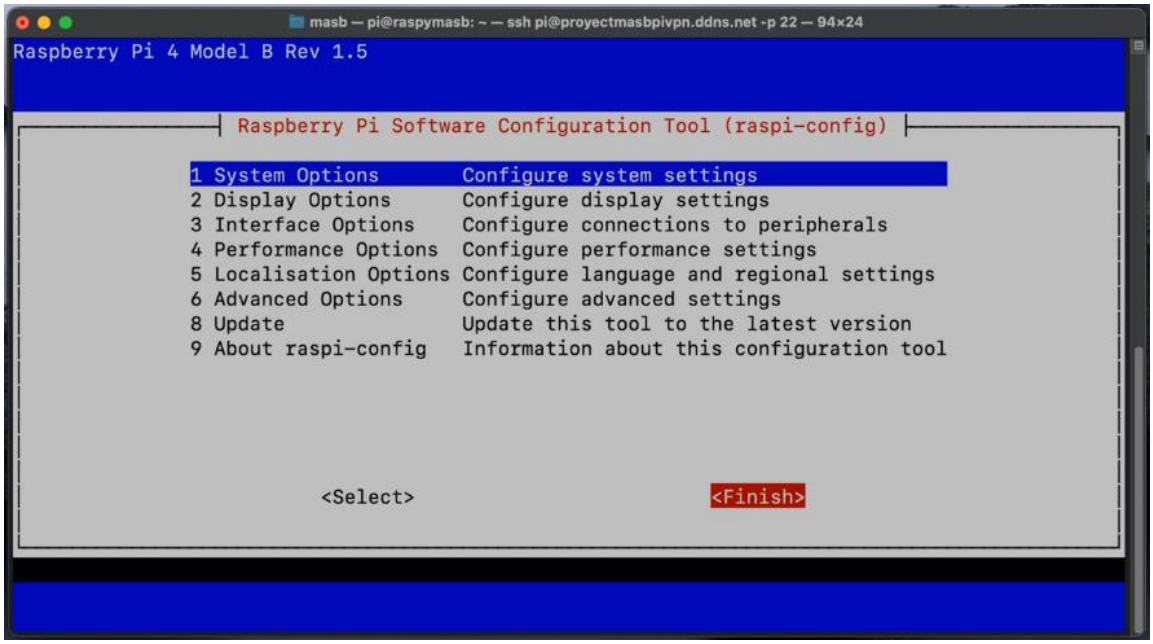


Apartado Localisation Options.

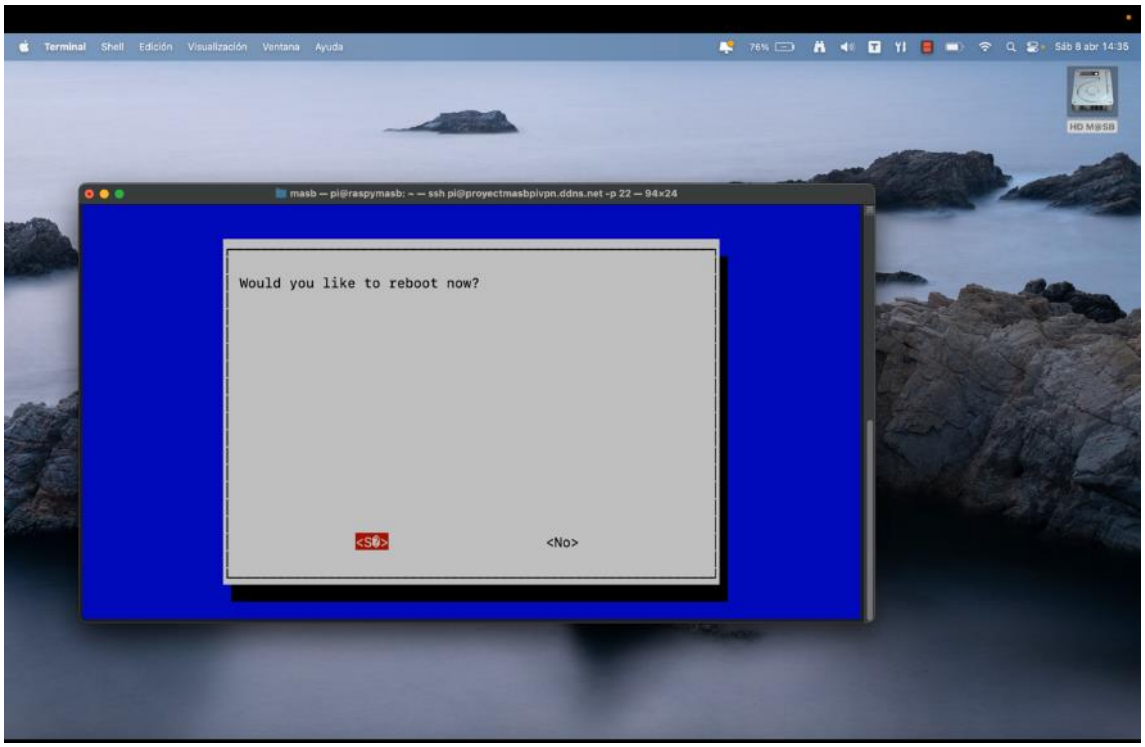


Pudiendo configurar las opciones.

- Locale Configure language and regional settings.
- Timezone Configure time zone.
- Keyboard Set Keyboard layout to match your keyboard.
- WLAN Country Set legal wireless channels for your country.

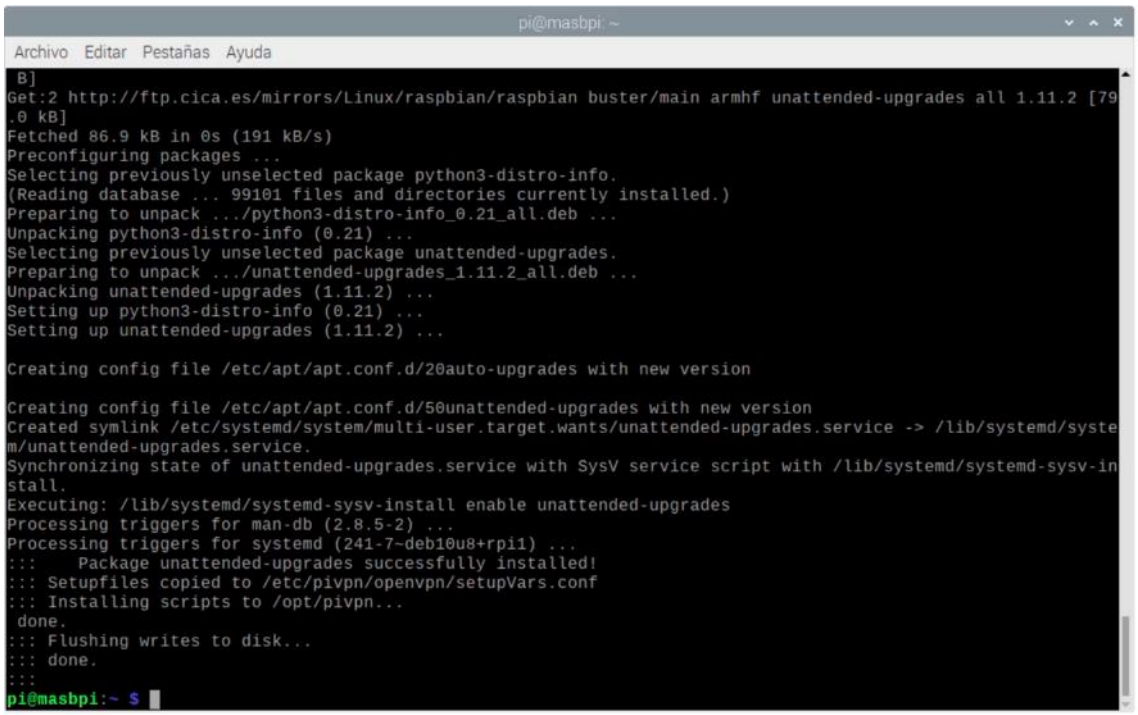


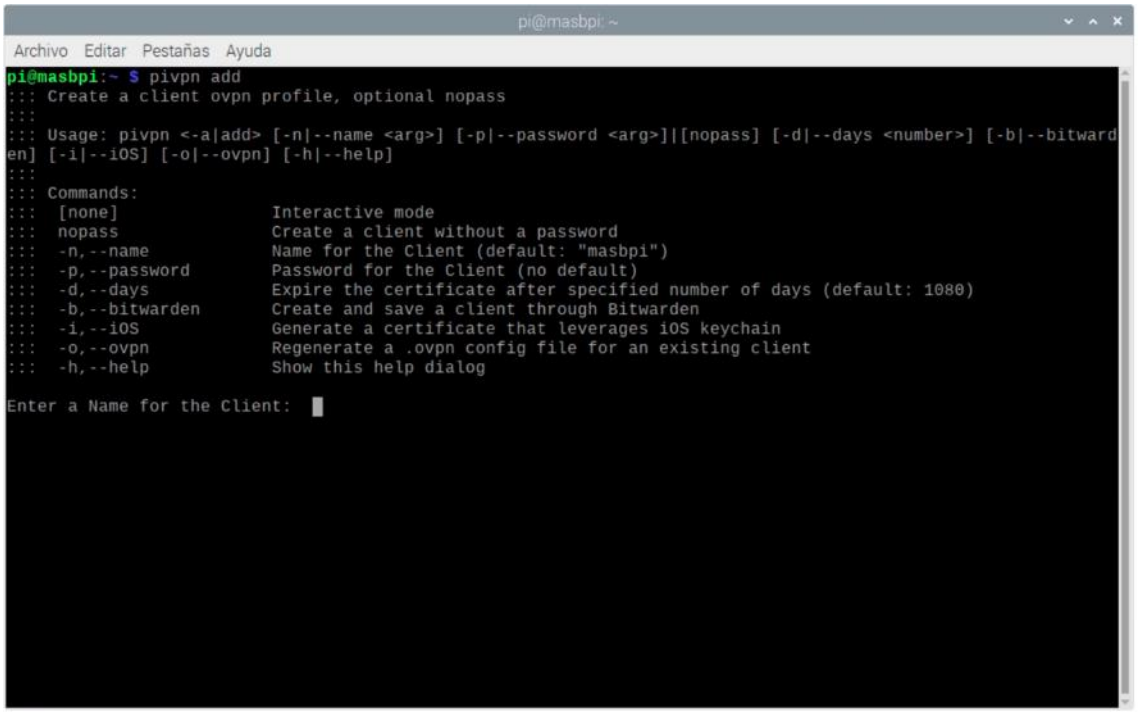
Realizadas las modificaciones necesarias, se seleccionará Finish y se pulsará INTRO.



En caso de ser necesario el reinicio de la Raspberry Pi, se seleccionará Si y se pulsará INTRO para reiniciar.

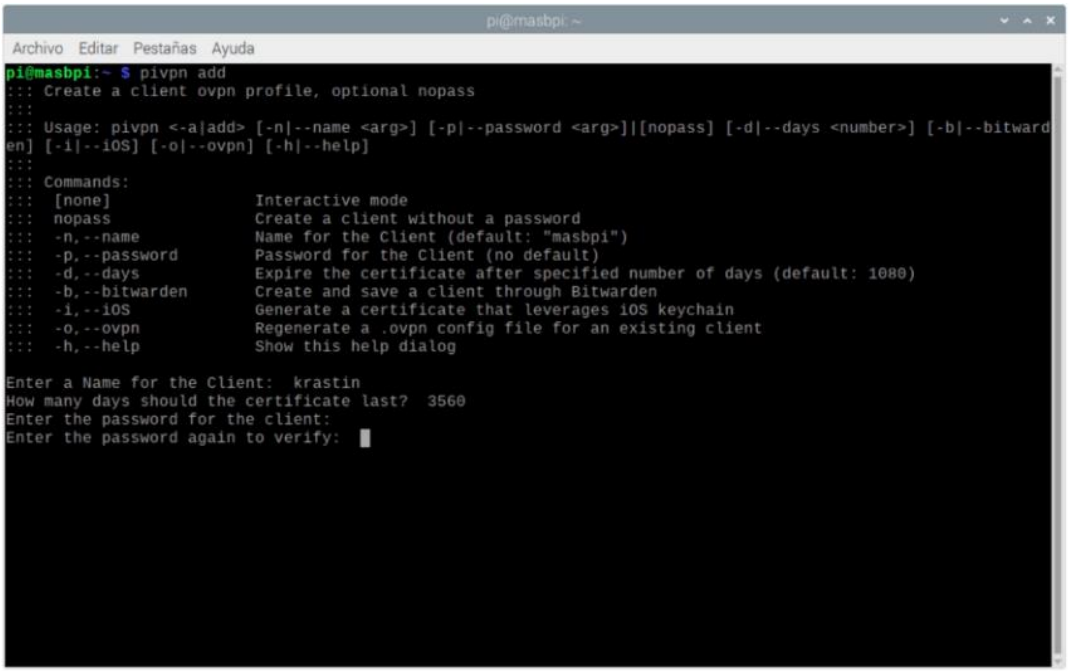
Creación usuarios conexión remota PiVPN.





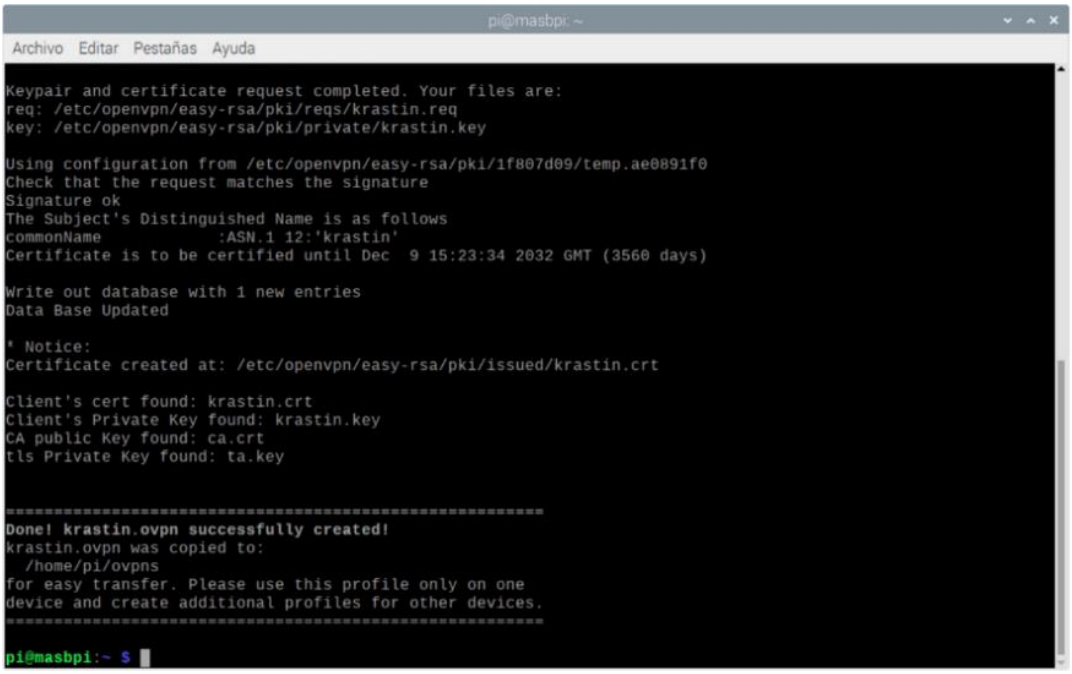
Finalizada la instalación de PiVPN, para la creación de los usuarios, se ejecutará el comando.

pivpn add

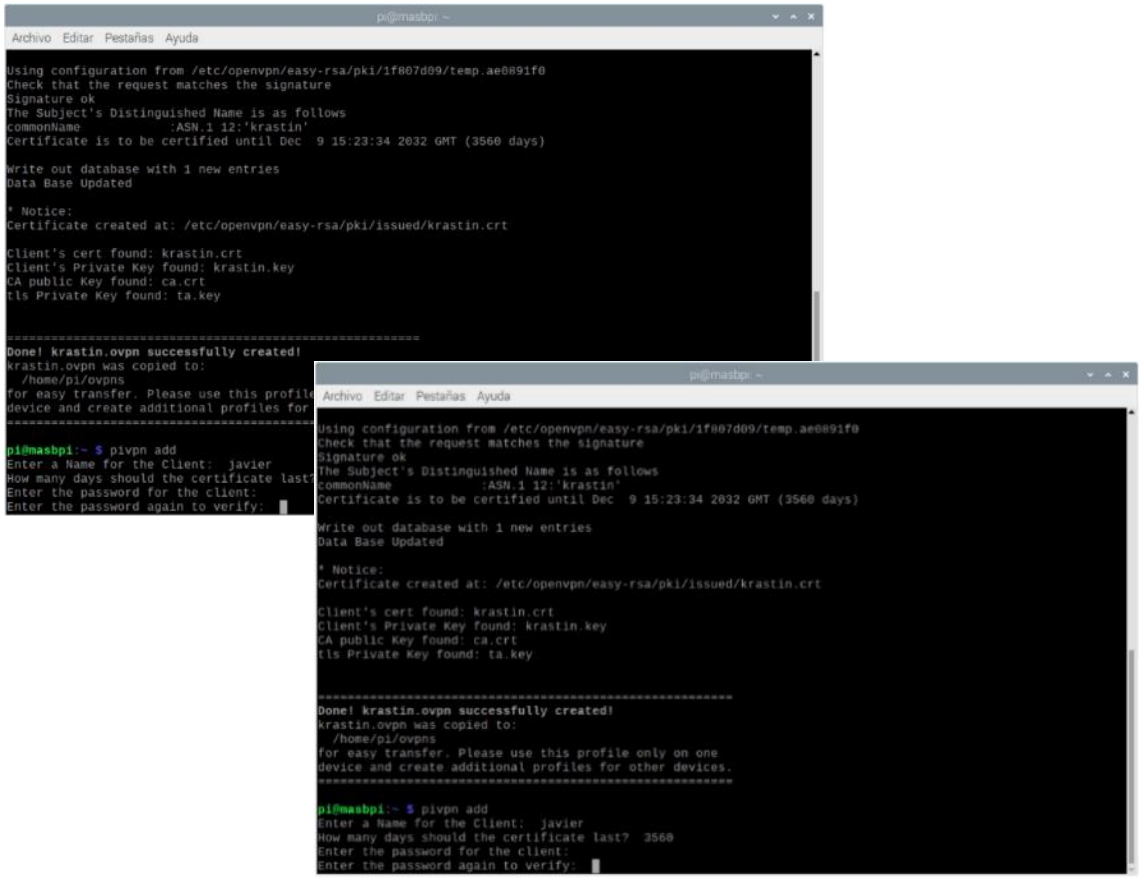


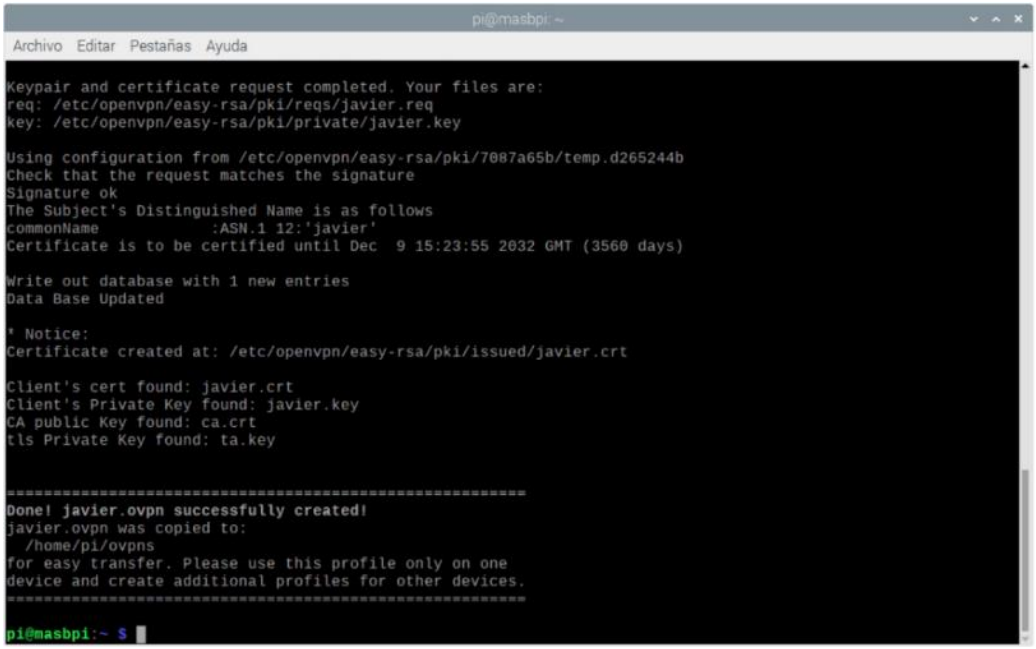
Cuestiones a facilitar en la creación del usuario con el comando pivpn add.

Habrá que facilitar el nombre de usuario a crear, como en este caso krastin.
Fecha válida para el certificado, se define el máximo, siendo este de 3560 días.
Se facilitará una contraseña y se tendrá que repetir la contraseña para su verificación.

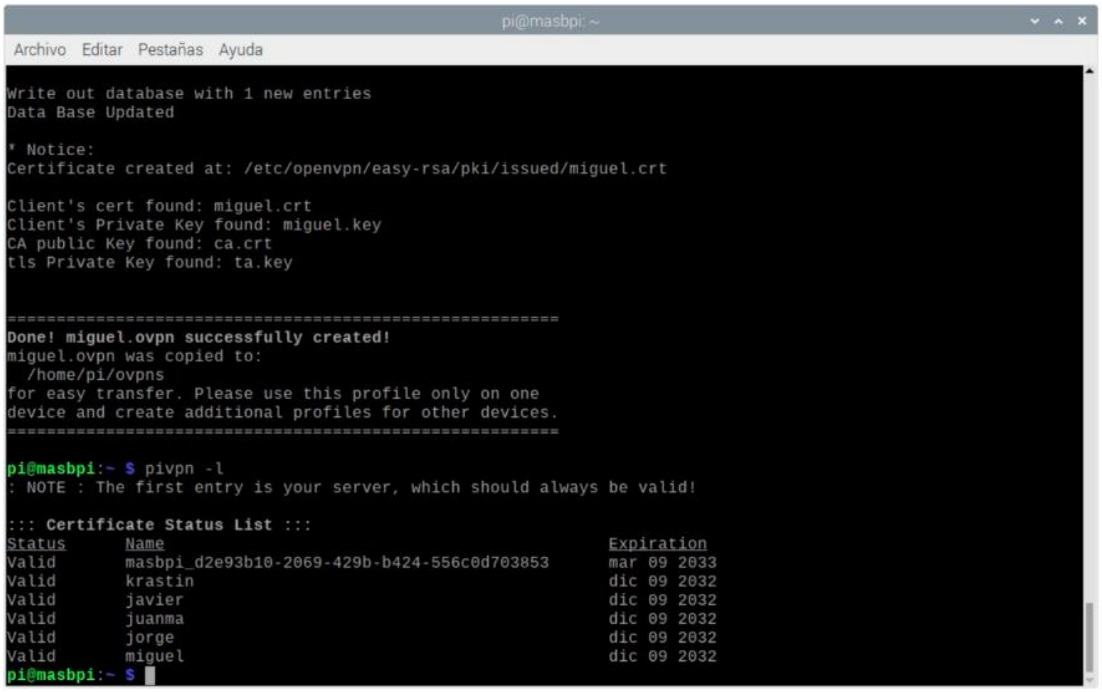


Facilitados los datos necesarios, se puede observar que el fichero de configuración creado para el usuario krastin se ubica en la ruta /home/pi/ovpns

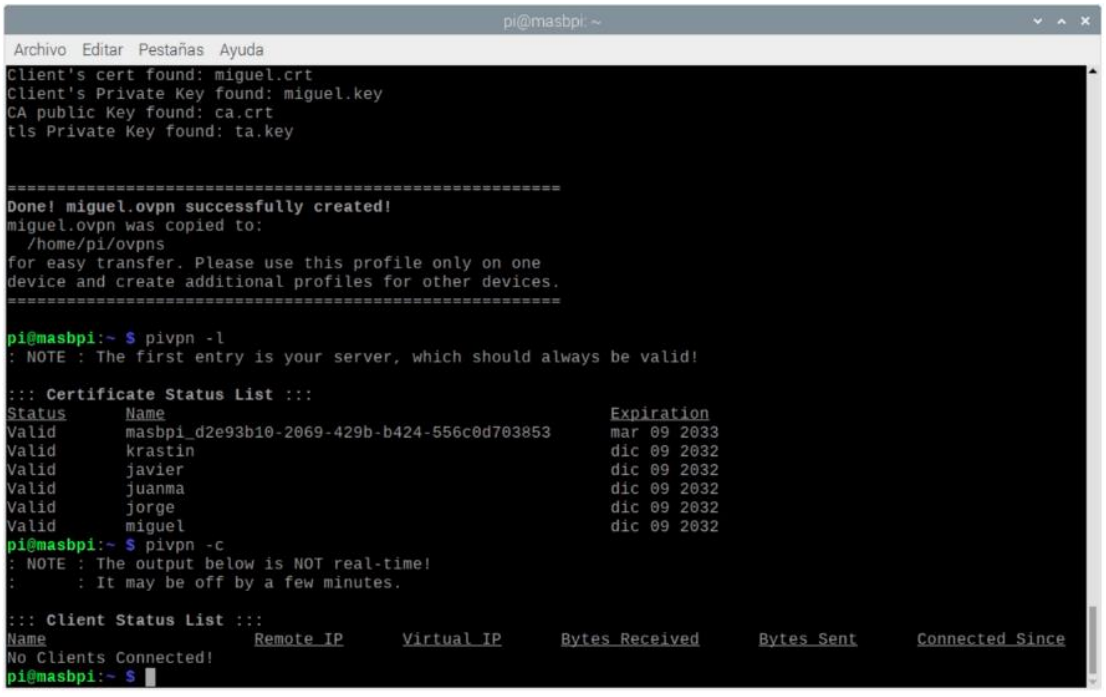




Nuevamente con el comando pivpn add se crea el usuario javier, facilitando los datos necesarios.

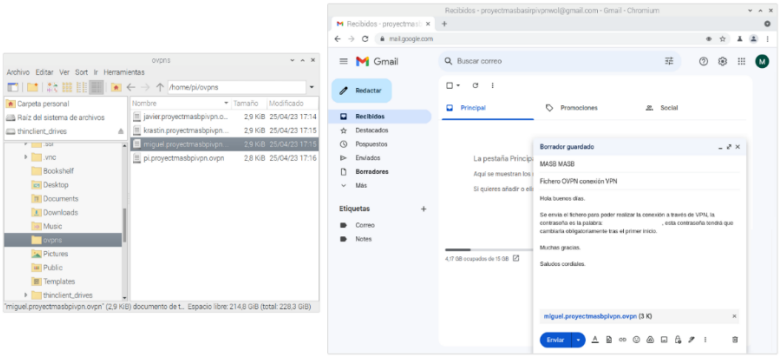


Para comprobar el estado de los usuarios creados se utilizará el comando.
pivpn -l



Mientras que, si se desea ver las conexiones activas de los usuarios, se podrá utilizar uno de los comandos.
pivpn -c
pivpn clients

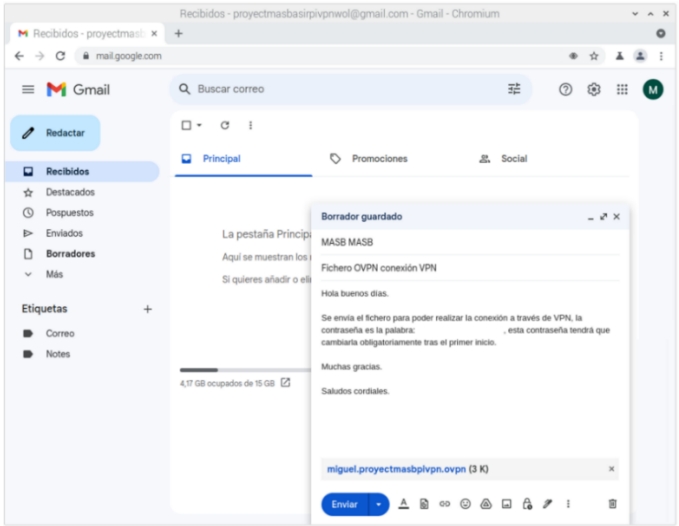
Envió de los ficheros de configuración OVPN creados por correo.



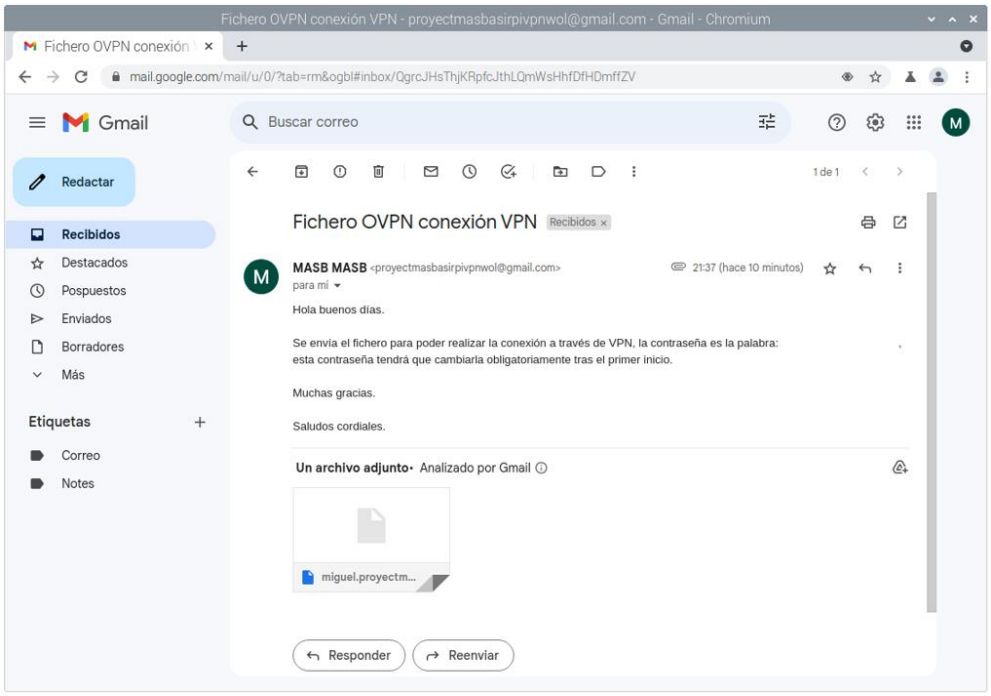
Los ficheros creados en el servidor VPN/WOL, se podrán mandar a los usuarios por ejemplo a través del correo electrónico.

Para lo que se accederá a la ubicación donde se encuentran los ficheros de configuración de las conexiones para cada usuario creado, pudiendo como administrador, sacar los ficheros en un pendrive o en cualquier otro medio de almacenamiento, posteriormente se puede mandar a cada usuario su fichero correspondiente a la conexión con el servidor VPN/WOL, mediante correo electrónico por ejemplo, o a través de algún otro medio con la suficiente seguridad para su entrega.

Se creará un correo, en el que se anexará el fichero correspondiente al usuario que se encuentre en el apartado superior Para, se escribirá lo que corresponda tanto en el apartado Asunto como en el cuerpo del mensaje del correo electrónico.



En este ejemplo, se realiza él envió a través de correo electrónico, con el fichero de configuración para un usuario en el correo, creado el correo, se pulsará sobre el botón Enviar.



Como se puede observar en la ventana de la captura superior, con el fichero recibido se podrán descargar e importar al programa OpenVPN para la posterior conexión.

Puede que exista algún otro método de envió, aunque el que aquí se explica, solo es un ejemplo de cómo exportar los ficheros de conexión de cada usuario y su envió, en este caso, habrá que enviar un correo electrónico con su correspondiente fichero de configuración por cada usuario existente.

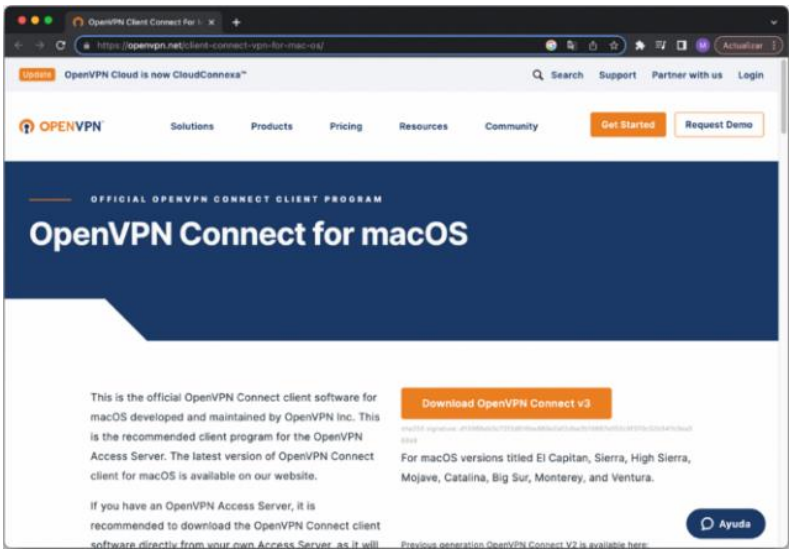
Instalación parte cliente.

Descarga e instalación aplicación OpenVPN.

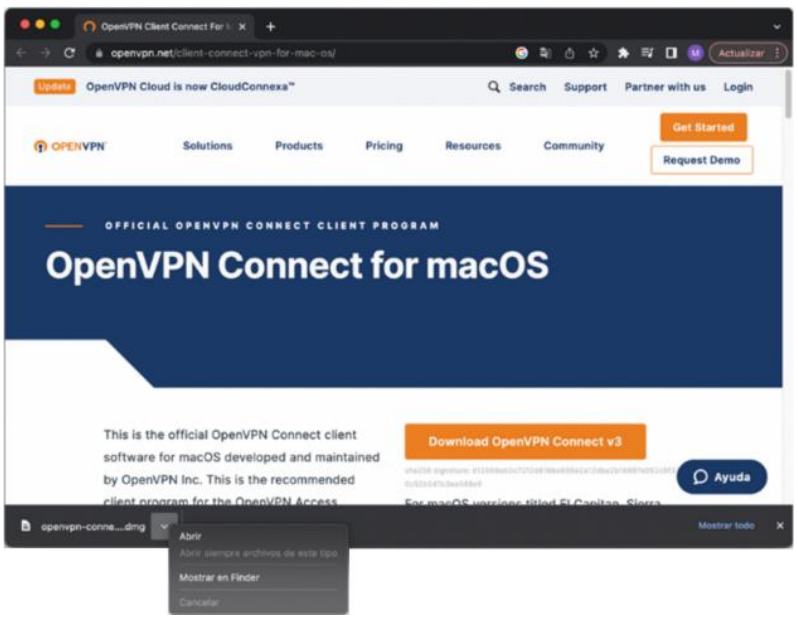
Descarga en S.O. Apple macOS.

Habrá que dirigirse a la WEB oficial.

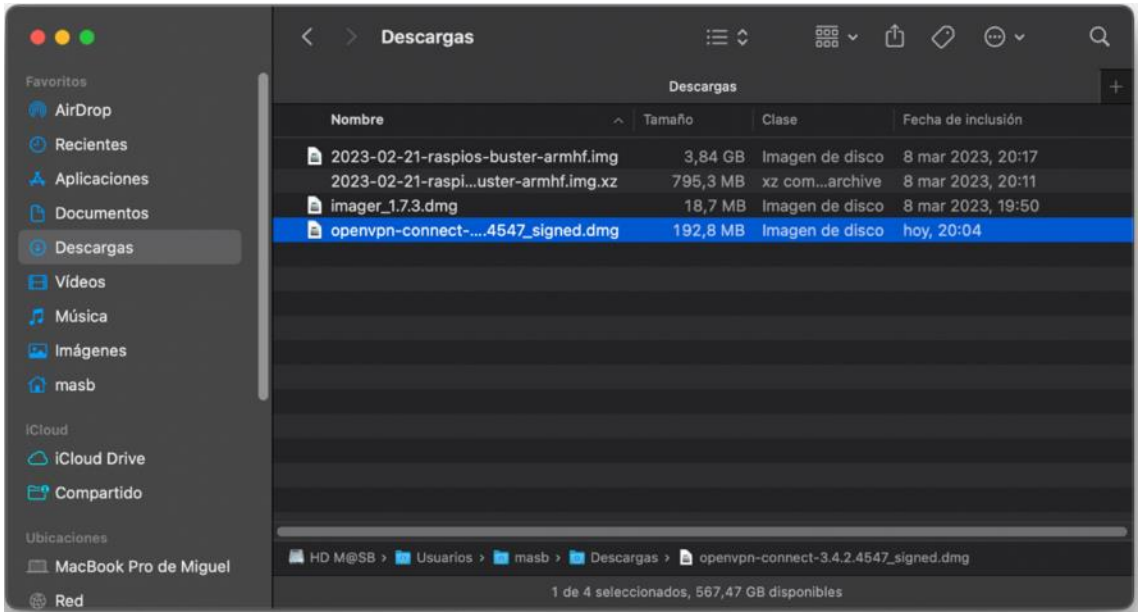
URL. https://openvpn.net/client-connect-vpn-for-mac-os/



Dentro de la WEB, se pulsará sobre el botón Download OpenVPN Connect v3.

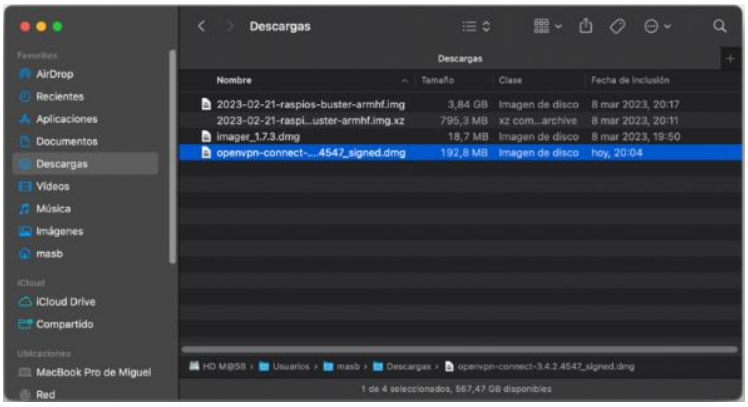


Finalizada la descarga, se pulsará en el icono en forma de flecha que apunta hacia abajo, en el menú que aparece, se tendrá que pulsar sobre Mostrar en Finder.



Una vez en el Finder, en la ubicación donde se encuentra el fichero descargado openvpn-connect-3.4.2.4547_signed.dmg, se hará doble clic con el botón izquierdo del ratón para montar la imagen de disco de la aplicación descargada.

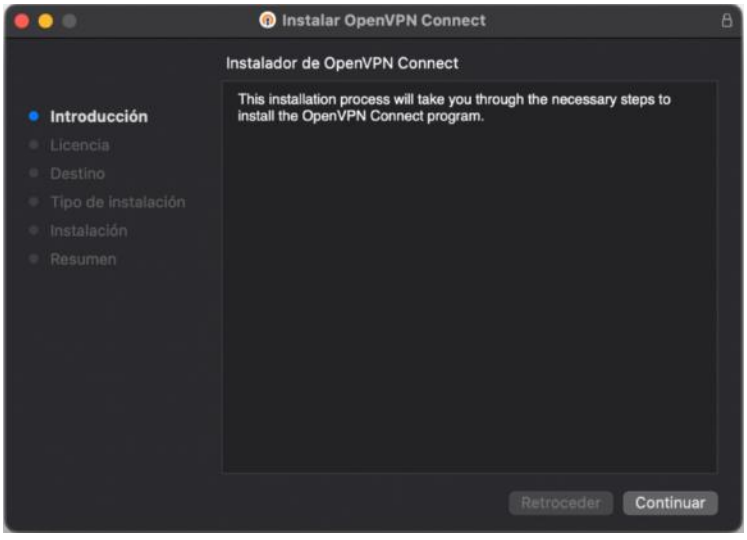
Instalación en S.O. Apple macOS.



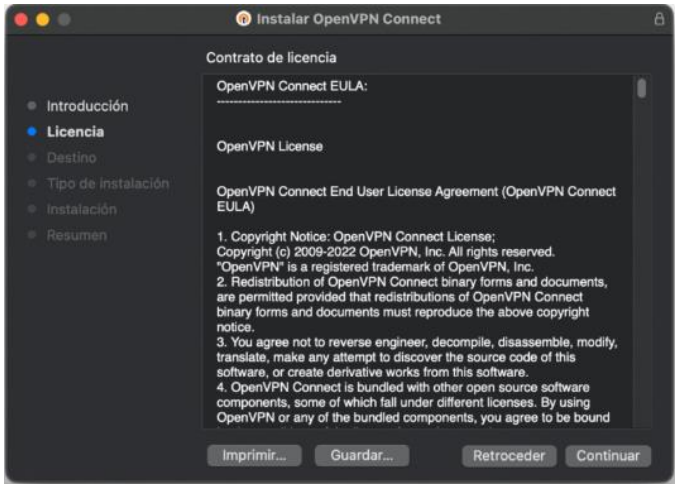
Dentro del Finder, y tras la descarga en la ubicación donde se encuentra el fichero descargado openvpn-connect-3.4.2.4547_signed.dmg, se hará doble clic con el botón izquierdo del ratón para montar la imagen de disco de la aplicación descargada.



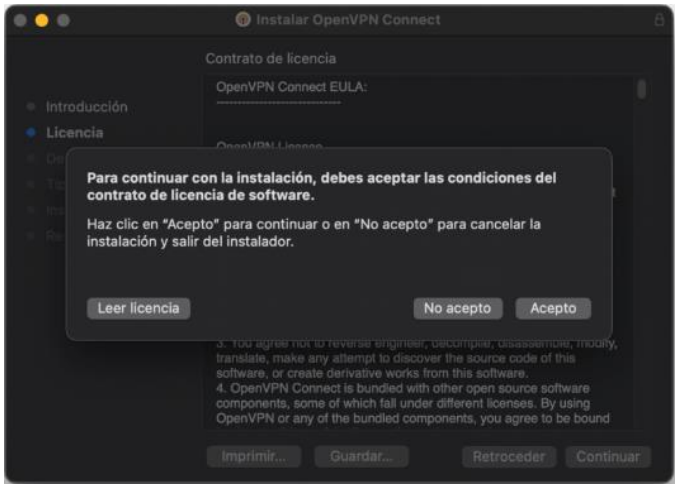
Dependiendo del chip del que disponga nuestro equipo Apple, se hará doble clic con el botón izquierdo del ratón sobre uno u otro fichero pkg,
en este caso se dispone de chip Apple M, por lo que se hace doble clic sobre el fichero pkg con chip Silicon.



Para comenzar el asistente de instalación, se pulsará sobre Continuar.



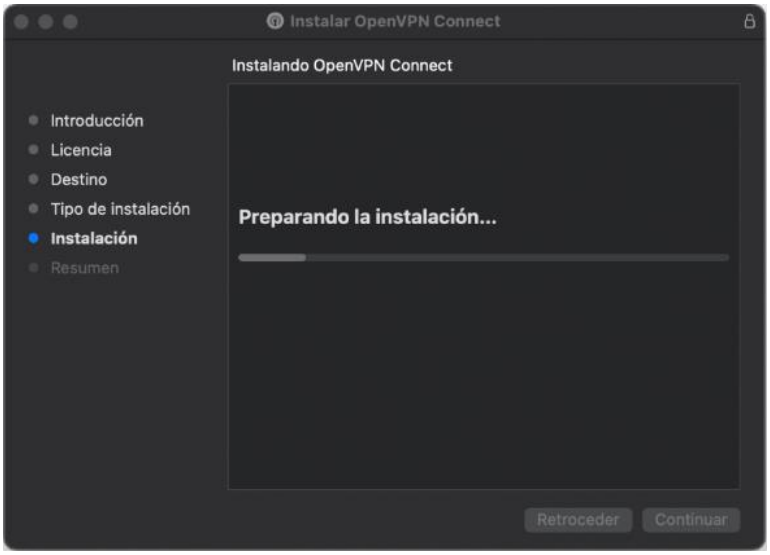
En la ventana Contrato de licencia, se pulsará en el botón Continuar.



Se pulsará el botón Aceptar para aceptar las condiciones del contrato de licencia de software.

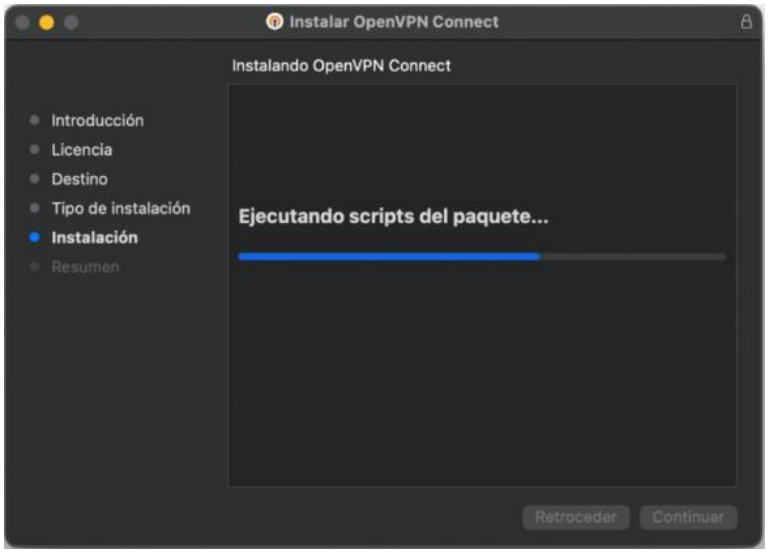


Para comenzar la instalación, habrá que pulsar el botón Instalar.

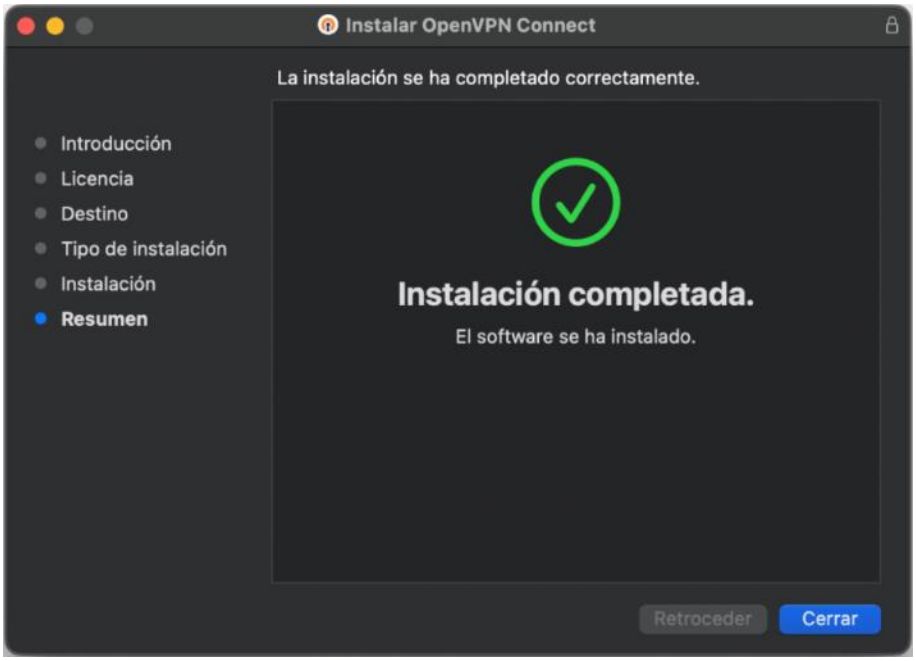




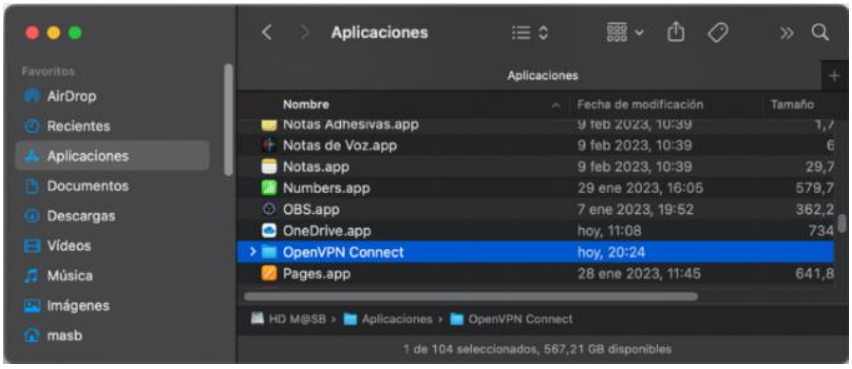
En caso de aparecer un cuadro de dialogo solicitando autenticación con una cuenta con permisos para la instalación, se proporcionará el usuario y la contraseña, pulsando posteriormente sobre el botón Instalar software.



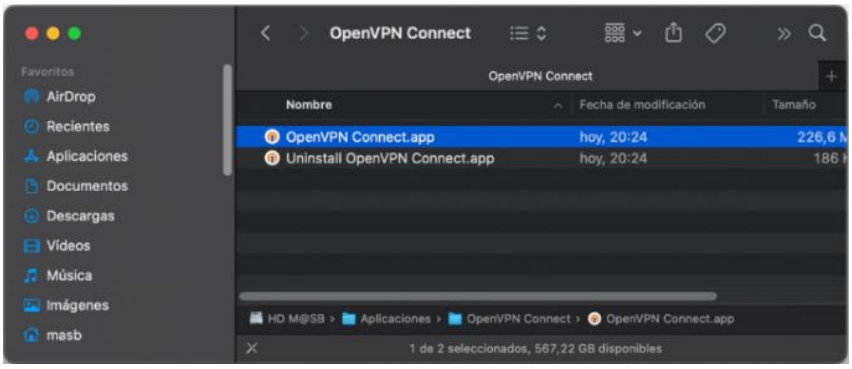
Comenzando la instalación del programa OpenVPN.



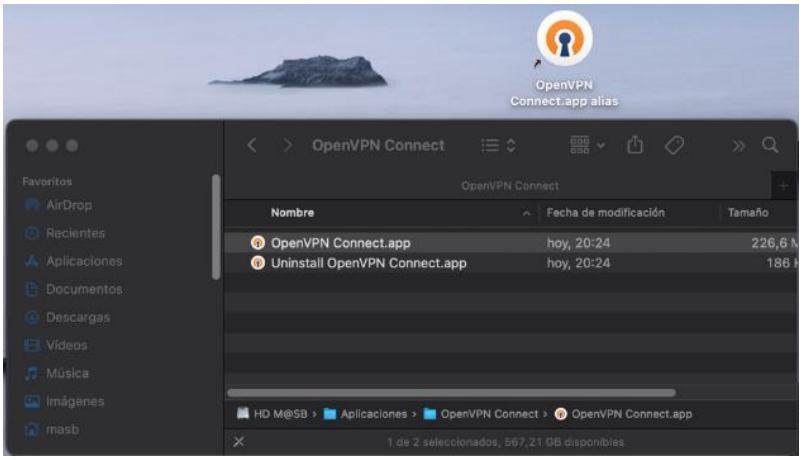
Terminada la instalación, se pulsará sobre Cerrar.



Como se puede observar en la ventana de la captura superior, dentro de la carpeta Aplicaciones, se habrá creado la carpeta: OpenVPN Connect.



Al acceder a ella, se encuentra la aplicación: OpenVPN Connect.app.

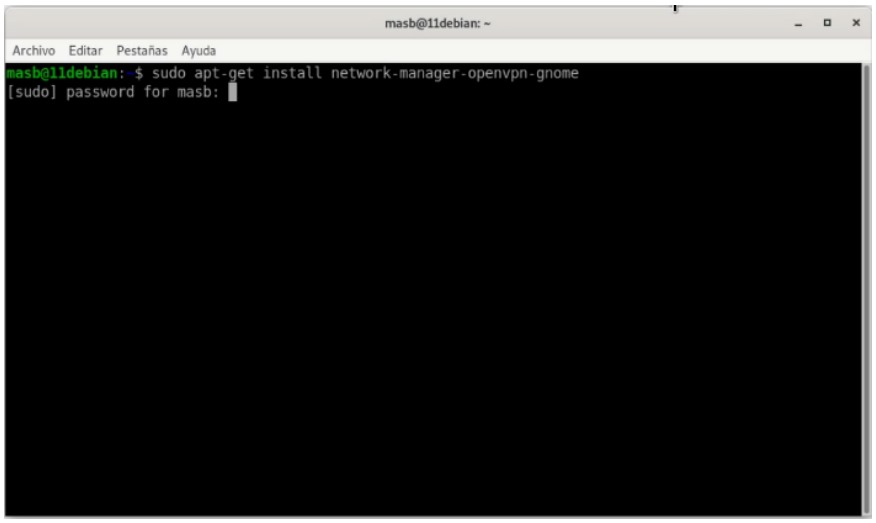


Anteriormente se explicó cómo crear un alias, dentro de la carpeta OpenVPN Connect se seleccionará con el botón izquierdo del ratón la aplicación OpenVPN Connect.app y sin soltarla, se arrastrará hasta un lugar libre en el escritorio, al soltar el botón del ratón, se creará un alias de la aplicación en esa ubicación.

Descarga e instalación en S.O. Linux.

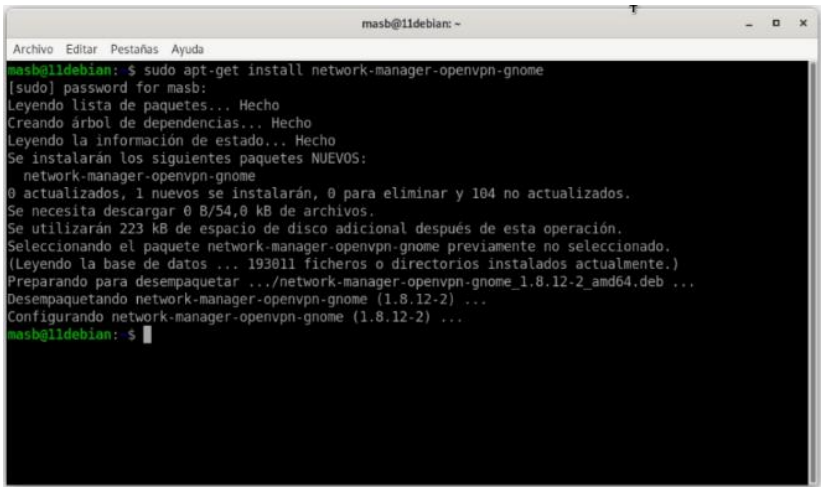
Como se podrá comprobar, en distribuciones Linux como Debian, puede ser necesario la instalación de un paquete para poder importar o utilizar los ficheros de configuración creados para las conexiones al servidor VPN/WOL, en Ubuntu, según las últimas versiones utilizadas para las pruebas, no fue necesario la descarga ni instalación de la aplicación OpenVPN, pudiendo realizar una conexión con los ficheros de configuración que se enseñó anteriormente a crearlos dentro de la aplicación PiVPN en el servidor Raspberry Pi.

Instalación de la aplicación en distribución Linux Debian, puede que en Ubuntu sea necesario, por las pruebas realizadas, en las últimas versiones no fue necesario, en caso de ser necesario, se seguirán los mismos pasos indicados.



Dentro de un terminal, se ejecutará el comando.

sudo apt-get install network-manager-openvpn-gnome



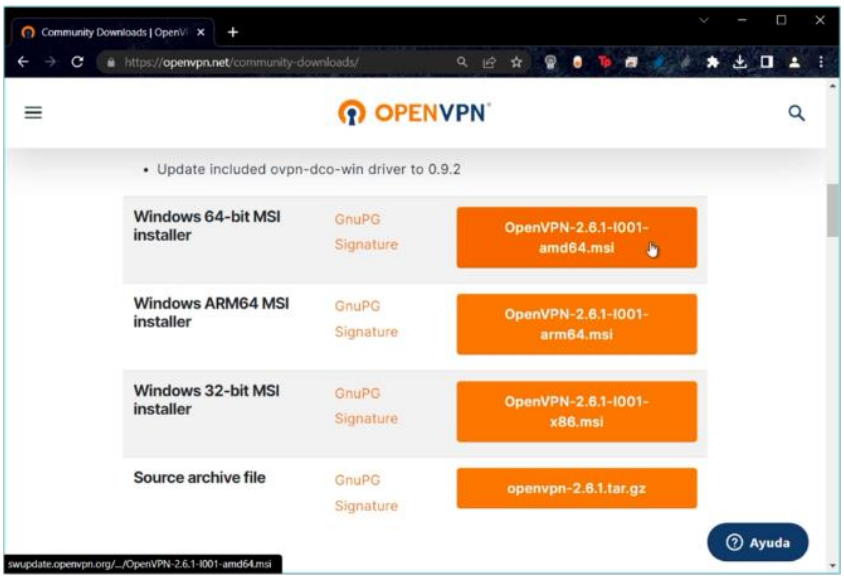
Terminada la instalación en Debian se podrán utilizar los ficheros de configuración para las conexiones.

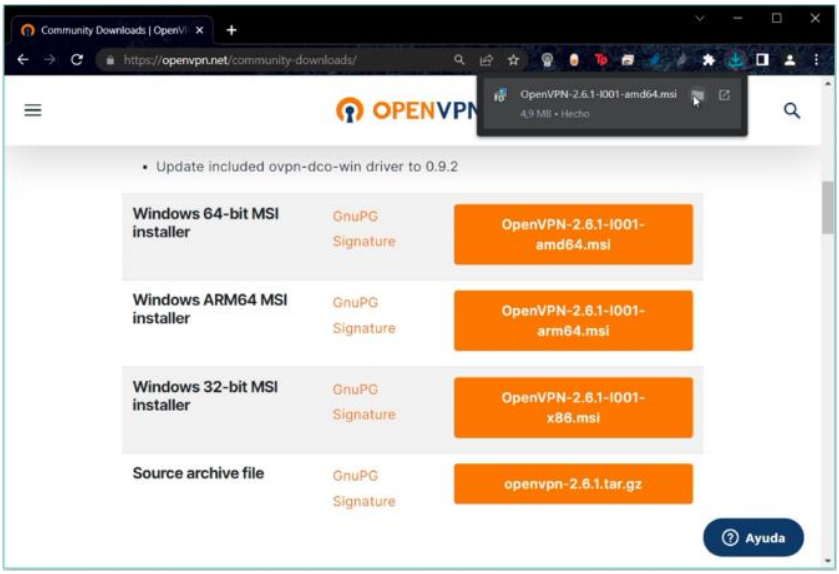
Descarga e instalación en S.O. Windows.

Descarga en S.O. Windows.

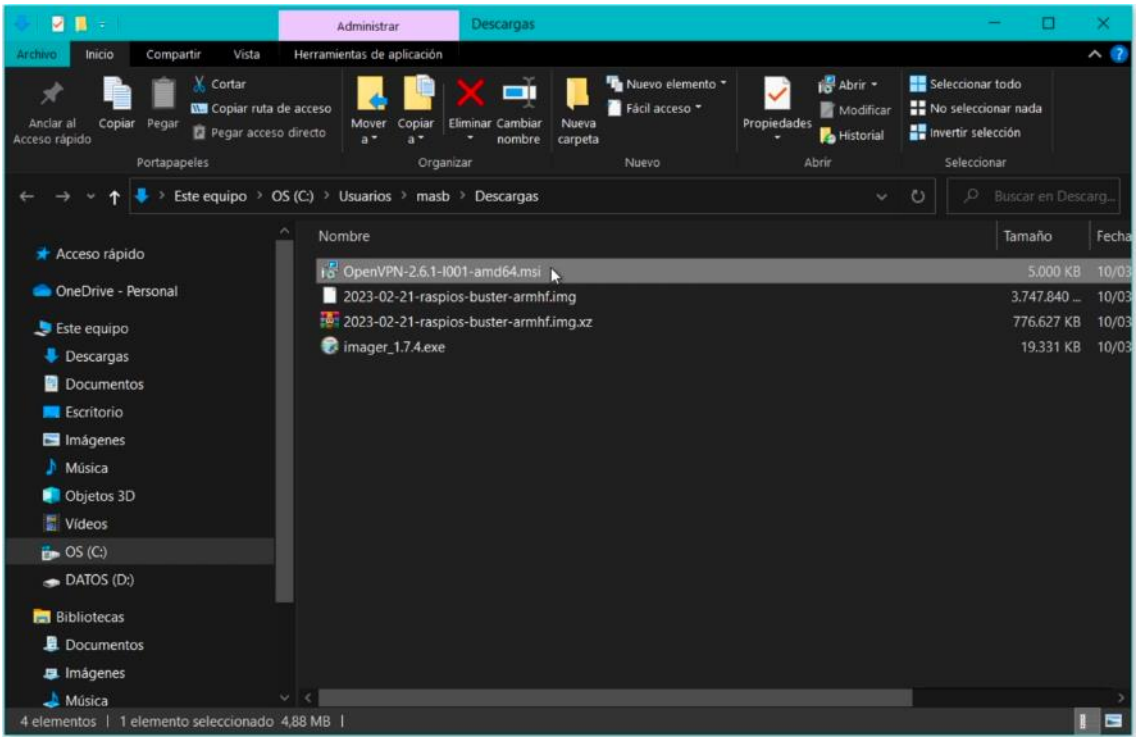
Habrá que dirigirse a la WEB oficial.

URL. https://openvpn.net/community-downloads/



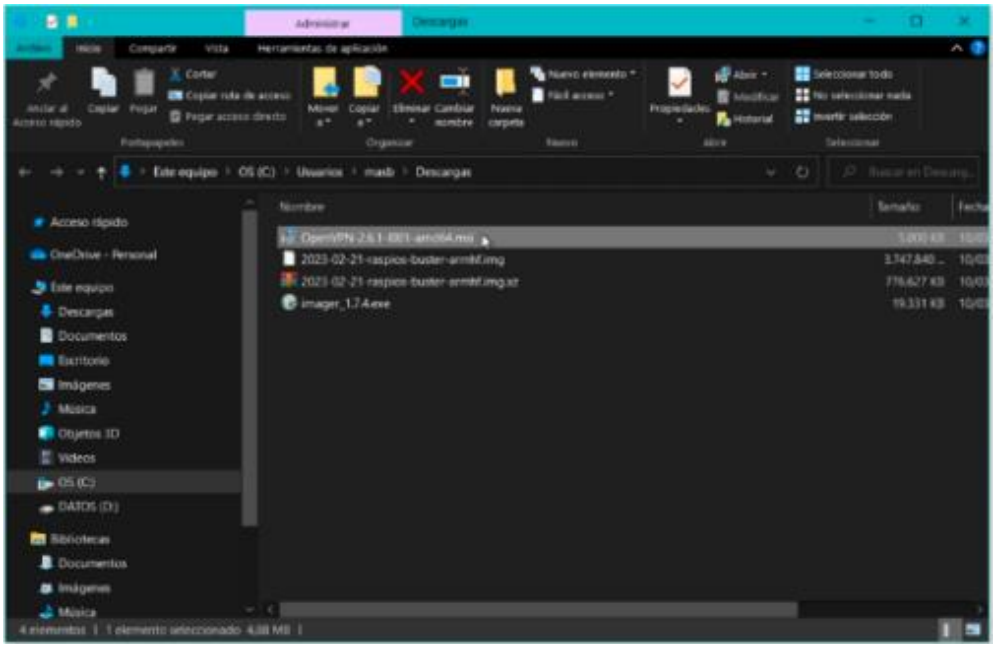


Dentro de la WEB, se deslizará la barra ubicada en la parte lateral derecha hasta localizar el botón, en este caso el S.O. Windows, es de 64 Bits, por lo que se pulsará en el botón OpenVPN-2.6.1-I001-amd64.msi, versión que puede diferir respecto a la que se disponga dependiendo de la arquitectura del S.O., se pulsará sobre este o sobre el fichero OpenVPN-2.6.1-I001-x86.msi en caso de disponer de un S.O. Windows de 32 Bits.

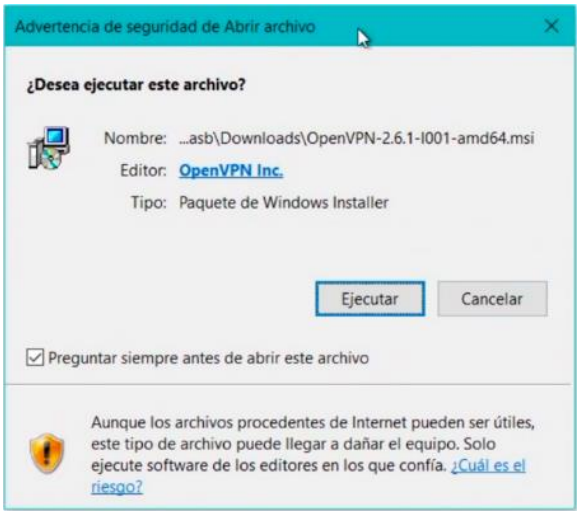


Una vez descargado el fichero, dentro del navegador de Internet, si se pulsa en la flecha que apunta hacia abajo en la parte superior derecha y posteriormente en el icono de la carpeta, se abrirá el explorador de archivos en la ubicación donde se descargó el fichero.

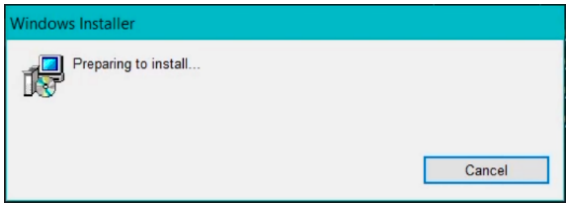
Instalación en S.O. Windows.

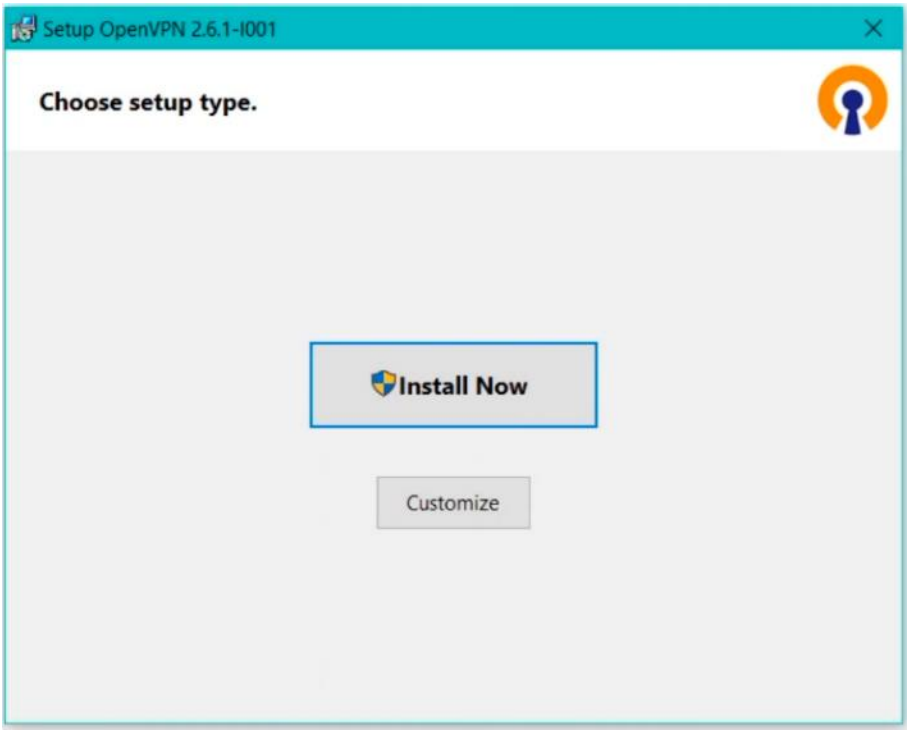


Una vez descargado el fichero, en este caso se trata del fichero OpenVPN-2.6.1-I001-amd64.msi, dentro de la carpeta Descargas, se hará doble clic sobre el fichero con el botón izquierdo del ratón.



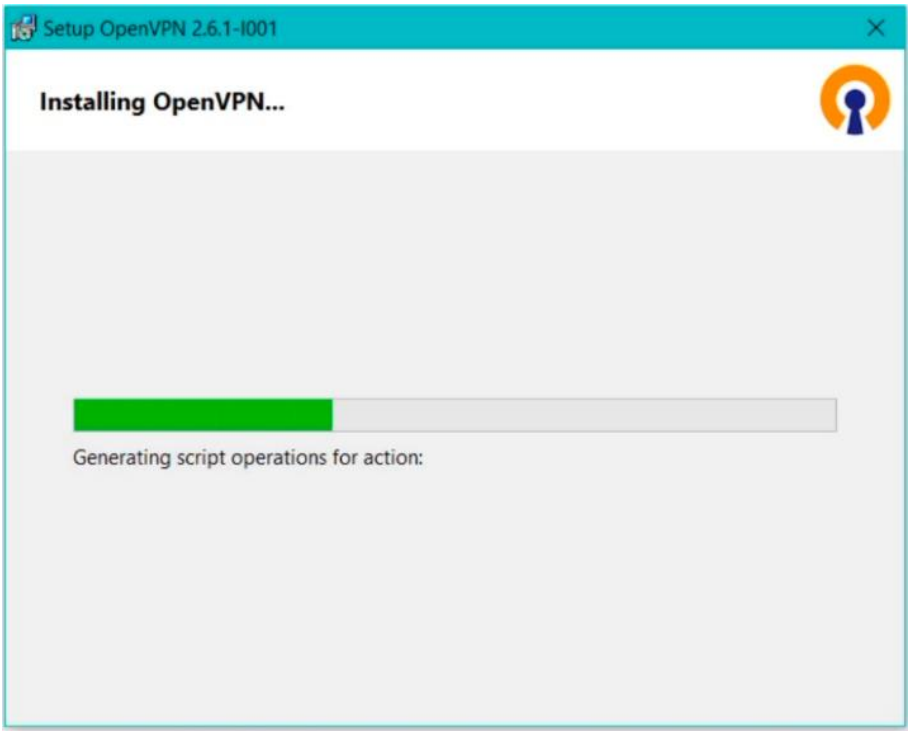
En la ventana, Advertencia de seguridad de Abrir archivo, se pulsará sobre Ejecutar.

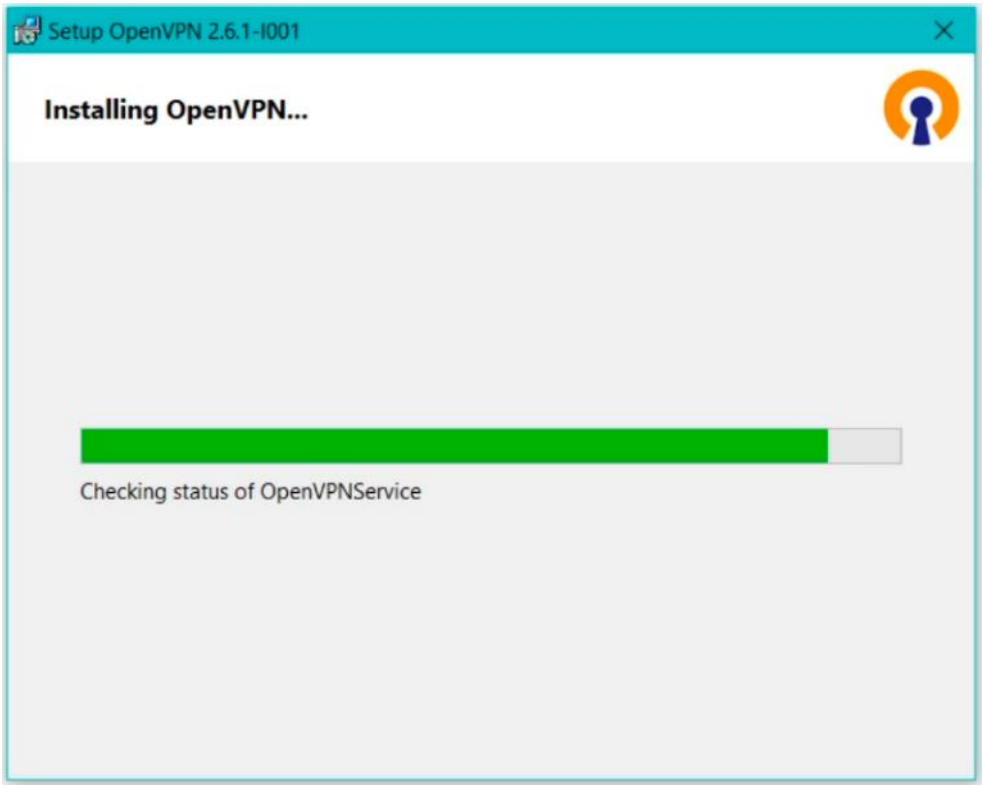




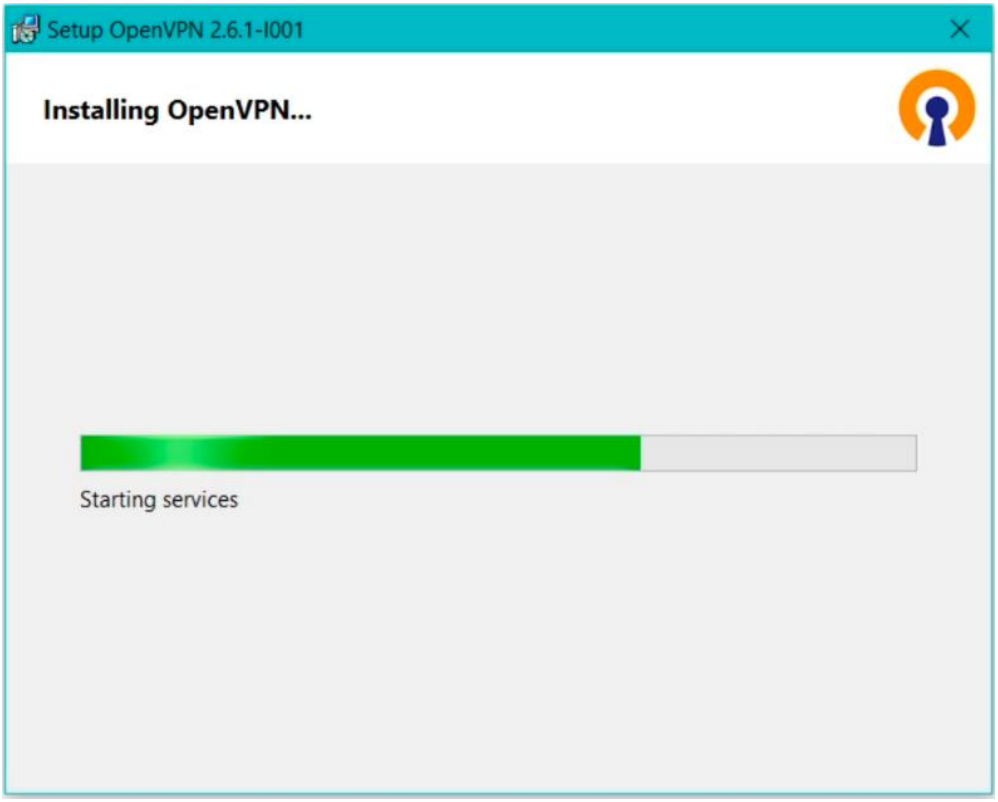
Para comenzar la instalación, se pulsará sobre el botón superior Install Now.

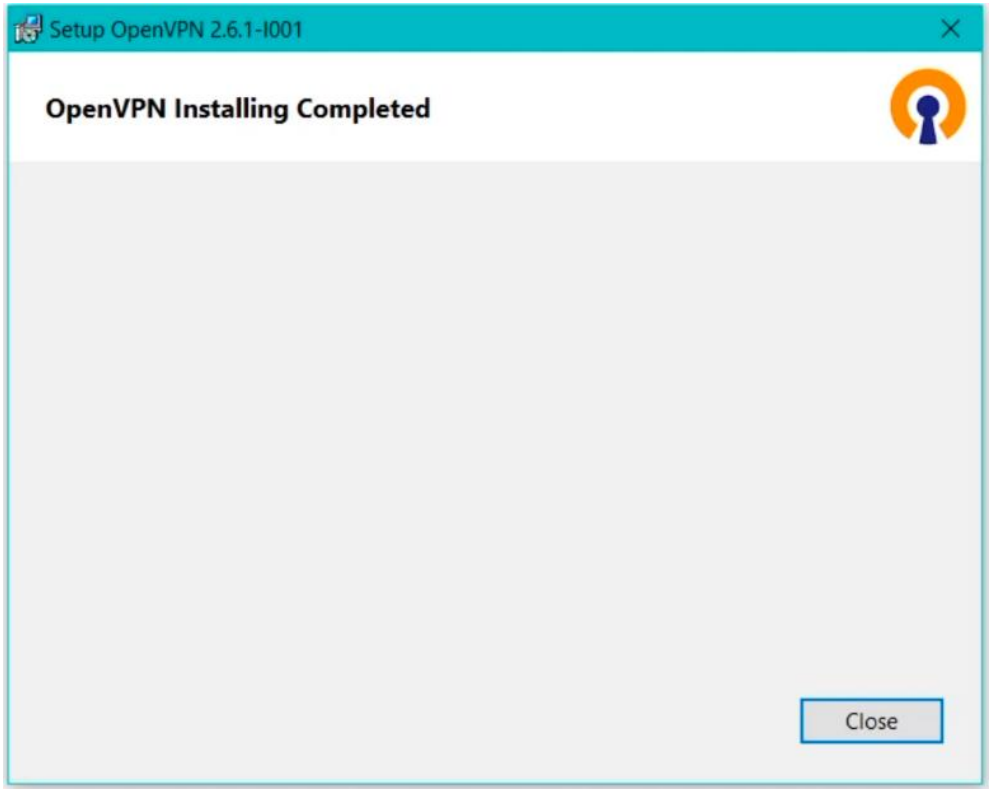
En caso de aparecer la ventana Control de cuentas de usuario, se pulsará Sí.





Comenzando el proceso de instalación.

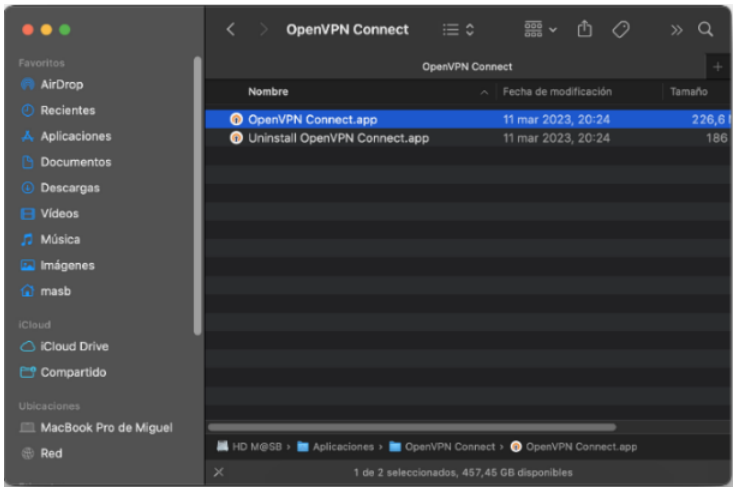


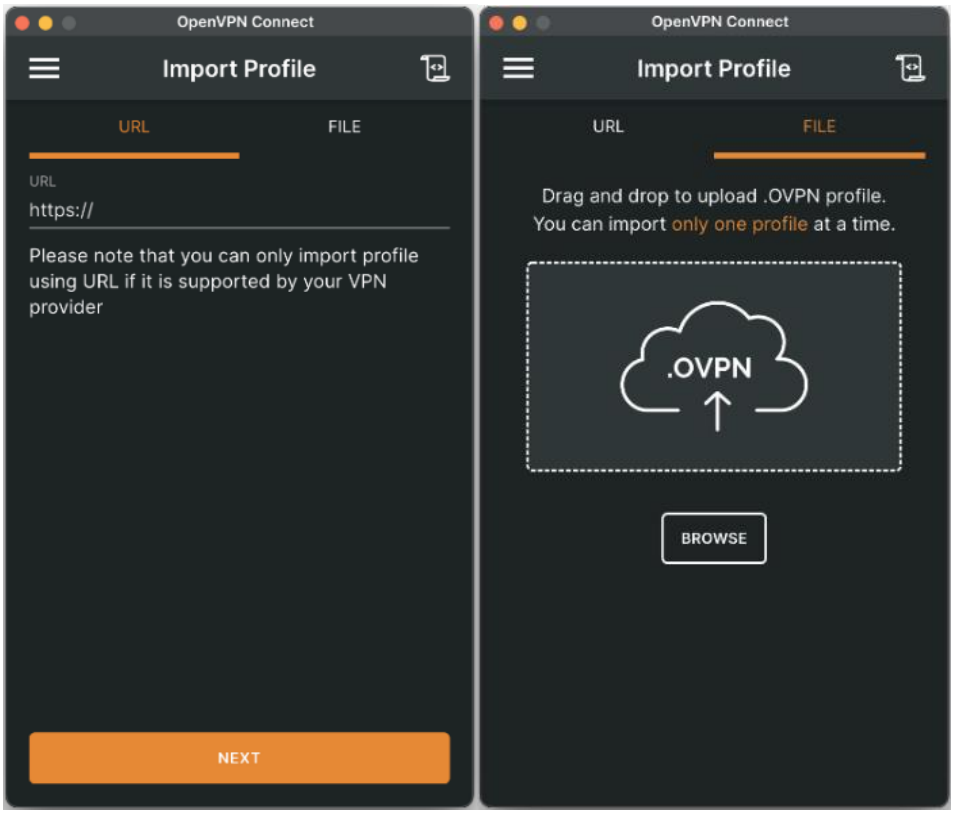


Finalizada la instalación, se tendrá que pulsar sobre Close.

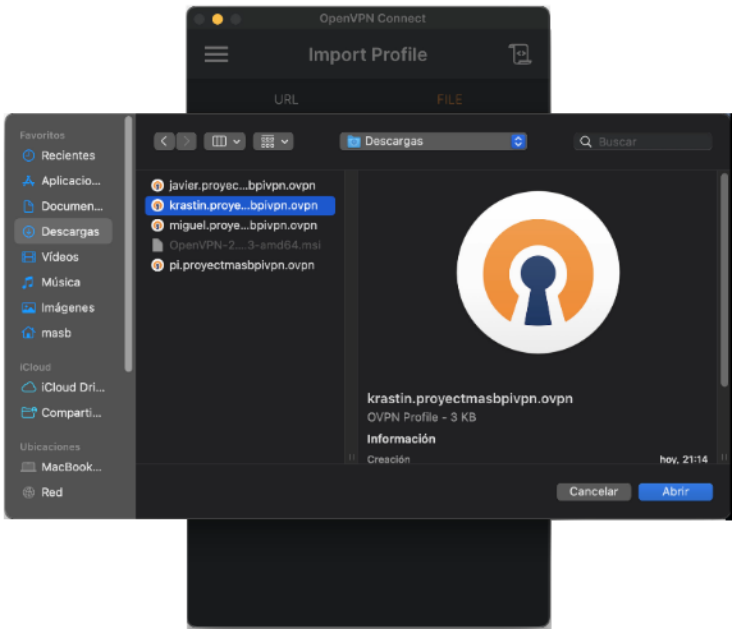
Importación ficheros OVPN configuración conexión aplicación OpenVPN.

Importación en S.O. macOS.

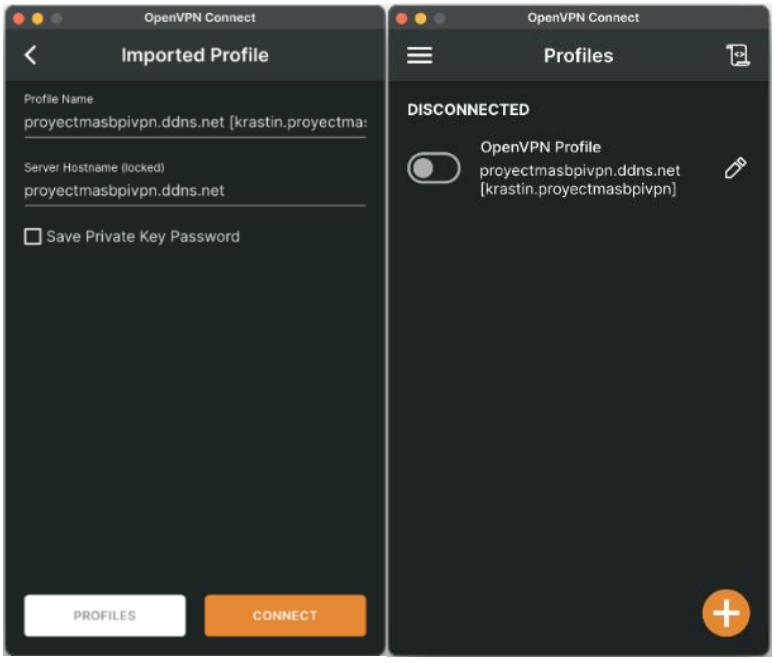




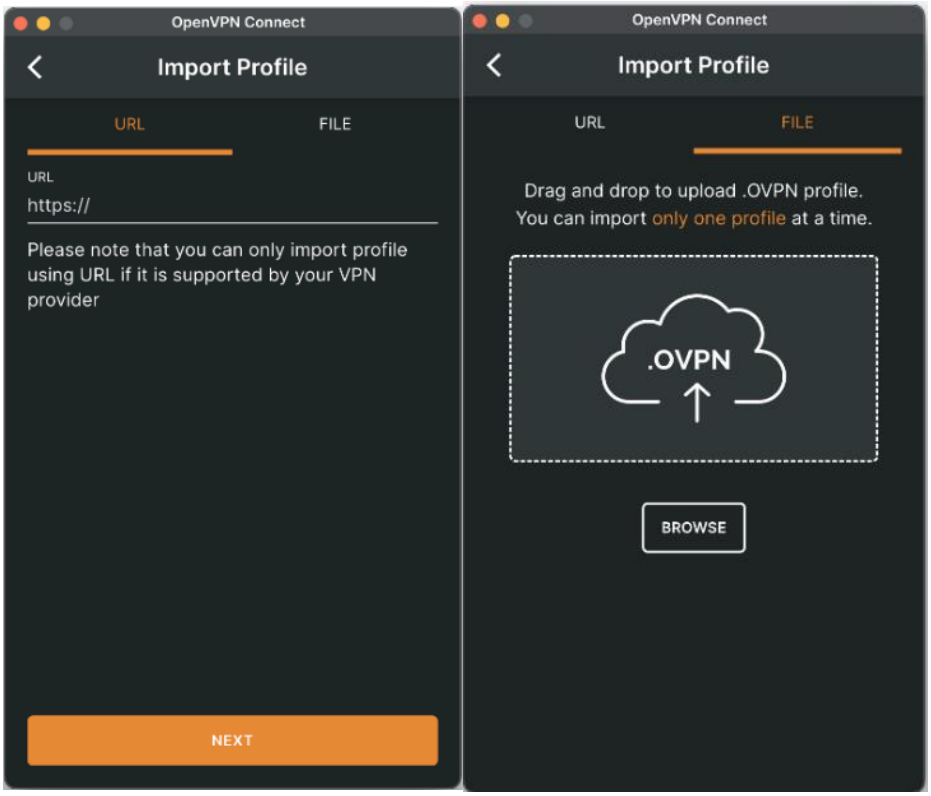
Teniendo instalada la aplicación OpenVPN (OpenVPN Connect.app), para abrirla, habrá que dirigirse a la carpeta Aplicaciones \ OpenVPN Connect, haciendo doble clic con el botón izquierdo del ratón sobre la aplicación OpenVPN Connect.app, la aplicación OpenVPN Connect tiene el aspecto que se muestra en la ventana de la captura superior izquierda, se pulsará sobre las letras superiores parte derecha FILE, para importar los ficheros de configuración necesarios.



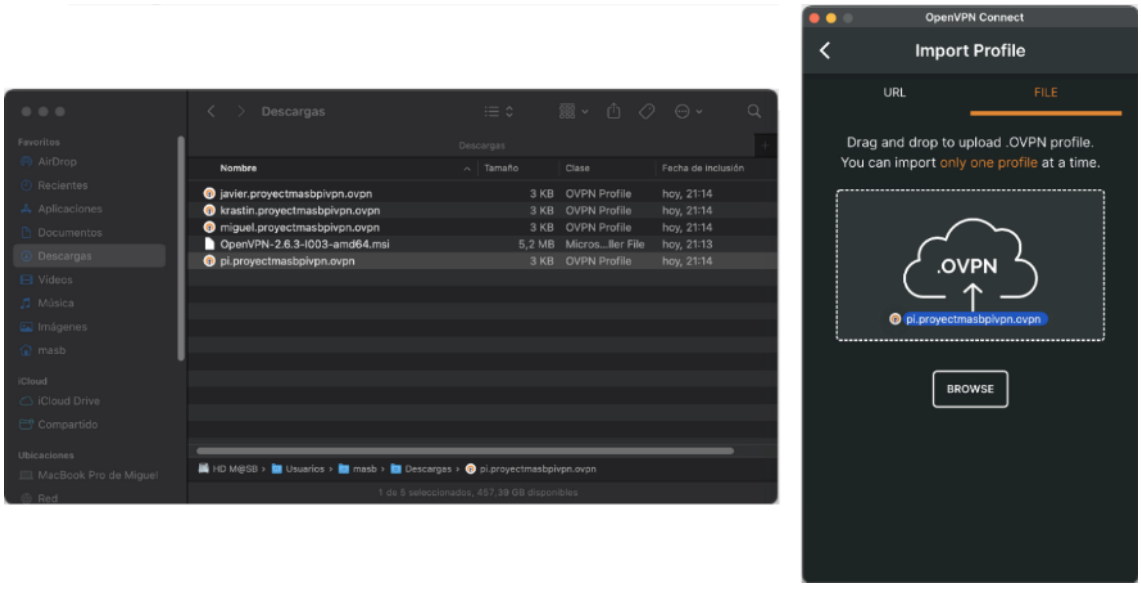
Apareciendo un asistente donde habrá que dirigirse a la ubicación donde se encuentran los ficheros de configuración, en la ubicación, en este caso se trata de la carpeta Descargas, se selecciona un fichero de configuración y se pulsará sobre el botón Abrir.



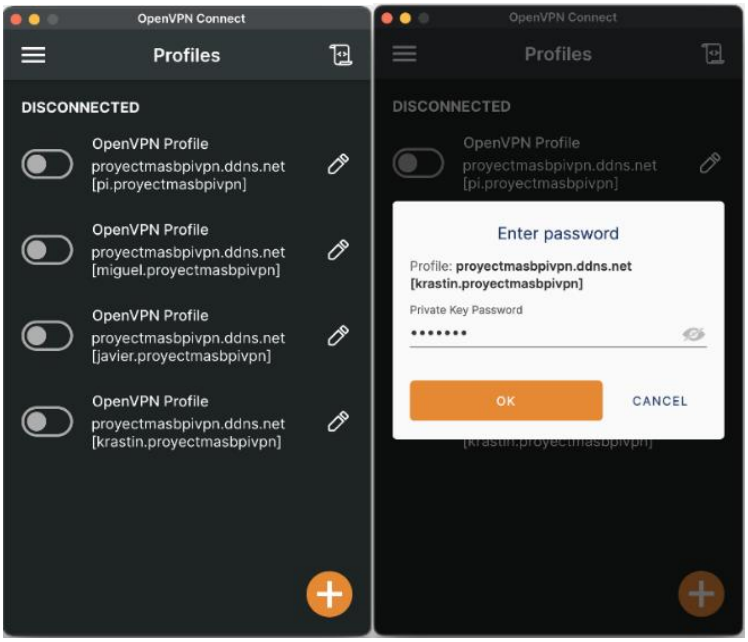
Se podría dejar añadida la contraseña del perfil de configuración marcando la opción Save Private Key Password, para este proyecto no se facilita la contraseña, pulsando en las letras inferiores de la izquierda PROFILES, ventana de la captura superior izquierda, apareciendo la ventana de la captura superior derecha, donde habrá que pulsar sobre el botón inferior derecho para poder añadir otro perfil de configuración.



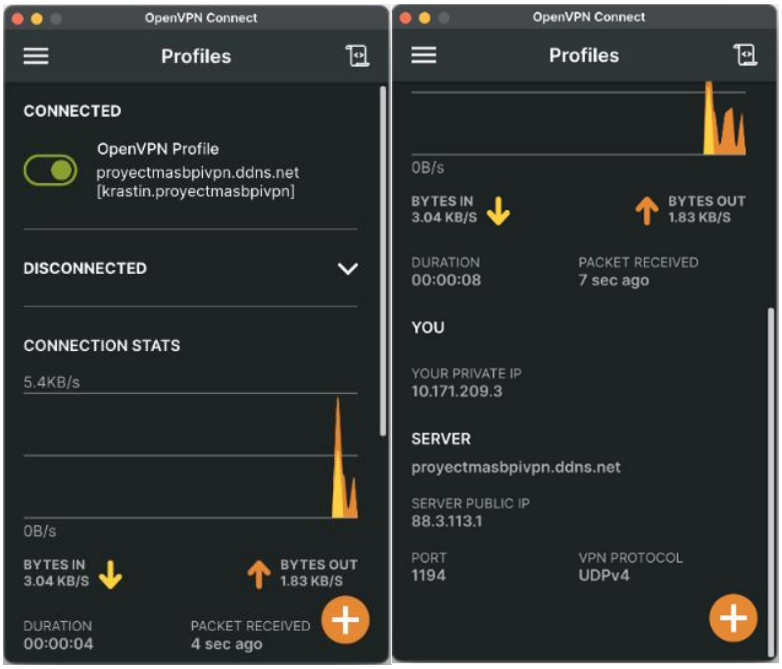
Nuevamente se pulsará sobre las letras superiores FILE, ventana de la captura superior izquierda.



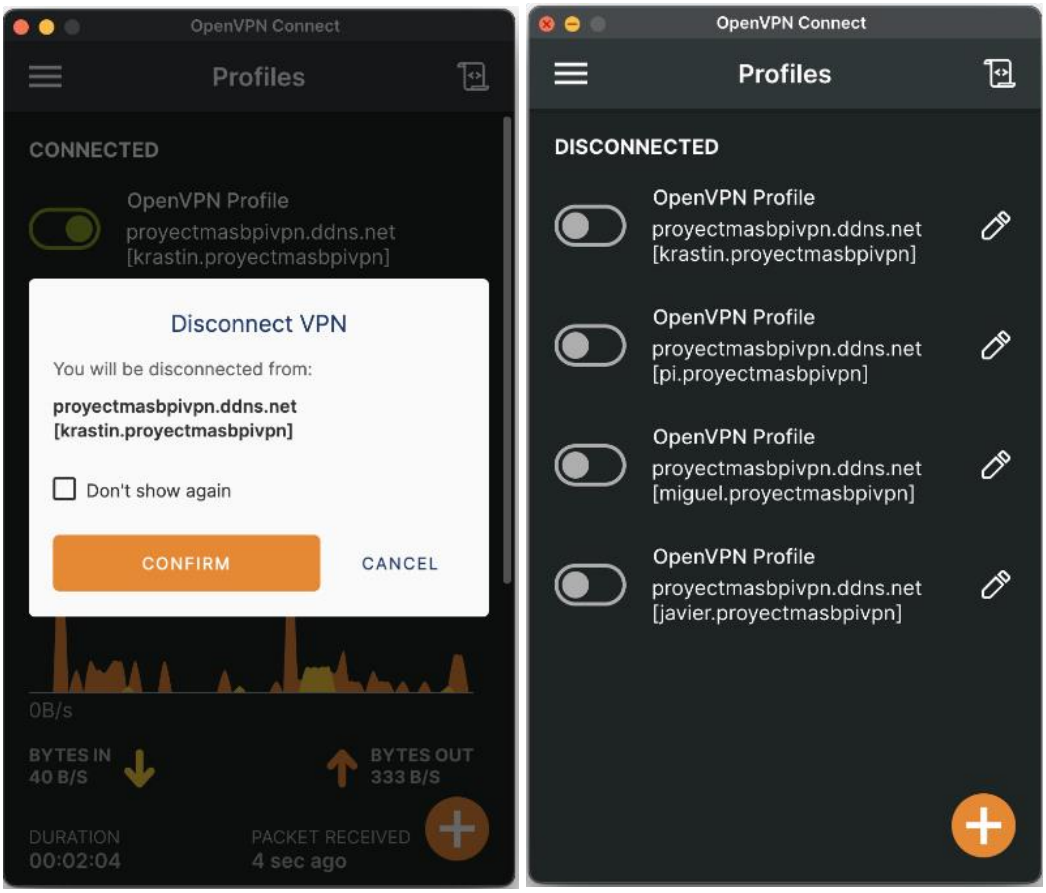
En este otro ejemplo, teniendo la aplicación OpenVPN Connect abierta y en la ventana de importación de ficheros ovpn dentro de la pestaña FILE, se arrastrará uno de los ficheros de configuración desde la ventana de Descargas a la ventana de la aplicación OpenVPN Connect, como se puede observar en la ventana de la captura superior.



Con los ficheros de configuración de los usuarios necesarios importados en la aplicación, se podrá pulsar sobre uno, en el deslizador , para realizar la conexión con ese usuario en concreto, al no haber configurado la conexión al importarse el fichero con la contraseña, en esta ocasión, al establecer la conexión, se solicitará la contraseña.

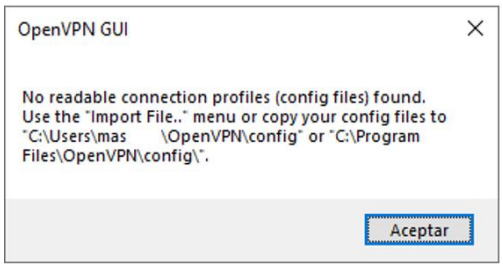


Como se puede apreciar en las ventanas de las capturas superiores, el deslizador cambia de color, pasando en ese momento a ser de color verde , la conexión se establece correctamente, mostrándose en la ventana información respecto a la conexión.

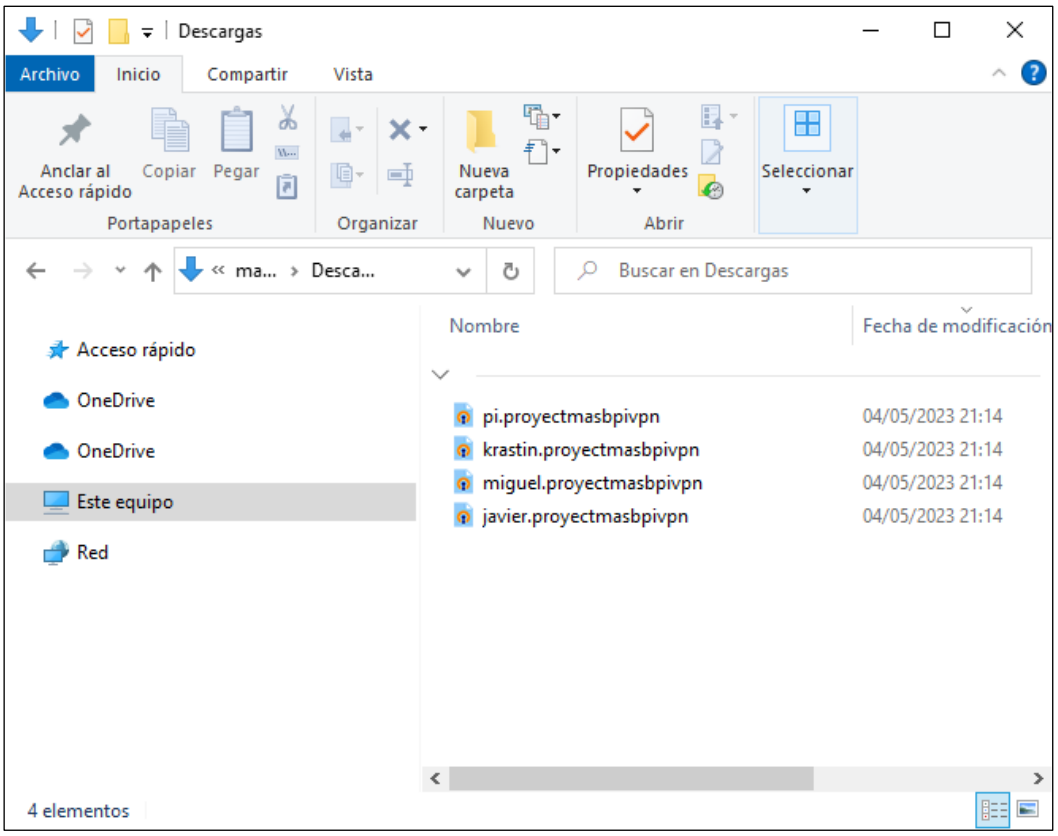


Para finalizar la conexión, se pulsará nuevamente sobre el deslizador , mostrándose una ventana emergente, en la que se tendrá que pulsar sobre CONFIRM para confirmar la finalización de la conexión, ventana captura superior izquierda, quedándose la aplicación a la espera por si se necesita una nueva conexión, pudiéndose cerrar la aplicación.

Importación en S.O. Windows.



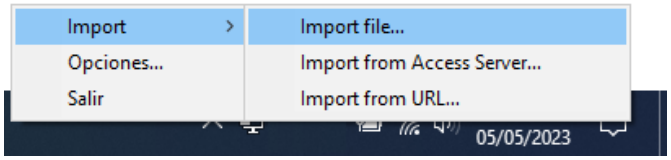
Dentro del S.O. Windows, teniendo la aplicación OpenVPN instalada y en el caso de que al abrirla aparezca la ventana de la captura superior, se pulsará en Aceptar.



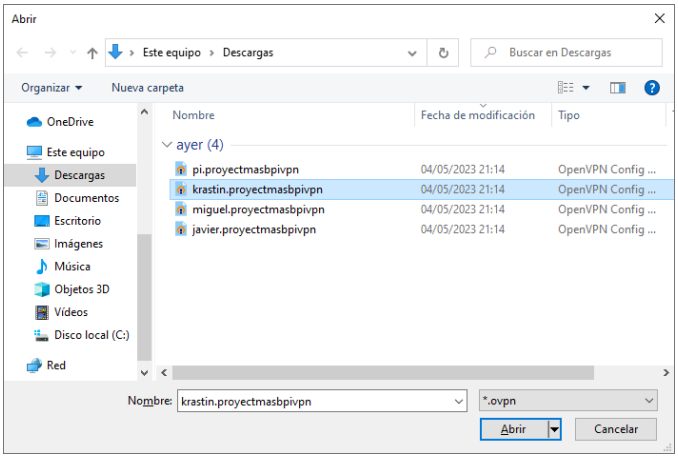
Por otro lado, teniendo ya los ficheros de configuración de la conexión VPN en este ejemplo en la carpeta Descargas, se procederá a la importación del fichero o ficheros necesarios.



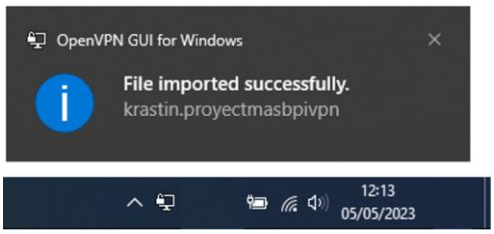
Para comenzar con el proceso de importación, se pulsará con el botón derecho del ratón sobre el icono de la aplicación, ubicado en el área de notificaciones de la barra de tareas, en la parte inferior derecha, en la imagen de la captura superior corresponde al icono que se encuentra dentro del rectángulo azul, en caso de no aparecer, puede ser necesario pulsar en el icono situado a la izquierda con forma de flecha apuntando hacia arriba.



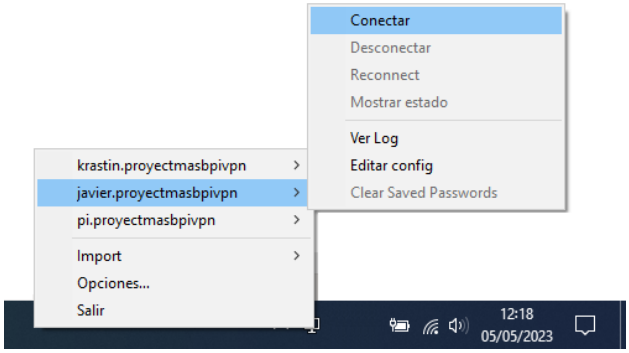
En el menú que se muestra, se pulsará sobre Import y posteriormente sobre Import file…



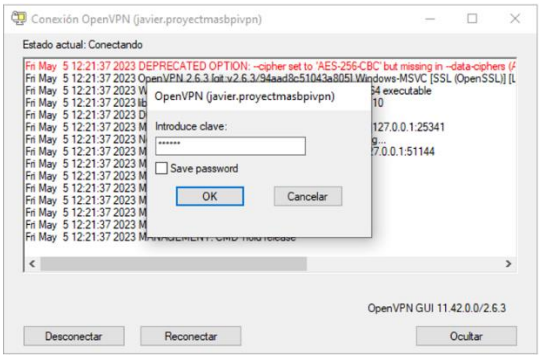
Se abrirá un asistente, en el que habrá que ir a la ubicación donde se encuentran los ficheros de configuración, en este caso en la carpeta Descargas, se seleccionará el fichero y se pulsará sobre el botón inferior derecho Abrir.



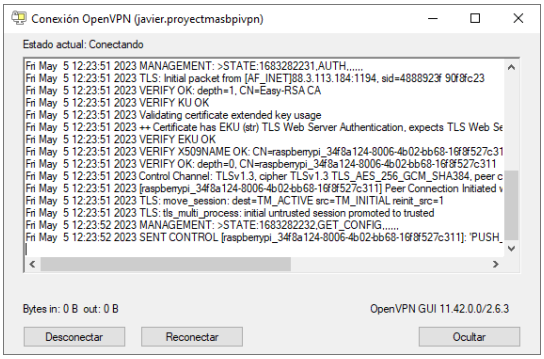
Nuevamente en el área de notificaciones de la barra de tareas, en la parte inferior derecha, puede aparecer una notificación informando que el fichero ha sido importado correctamente.



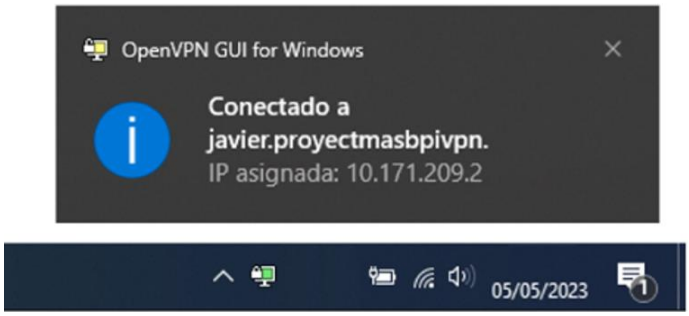
Tras la importación del/los ficheros de conexión necesarios, para realizar la conexión al servidor VPN/WOL, se pulsará sobre el icono de la aplicación ubicado en el área de notificaciones de la barra de tareas , en este momento se seleccionará el fichero correspondiente al usuario con el que se necesite conectarse vía VPN, posteriormente, se tendrá que pulsar sobre Conectar.



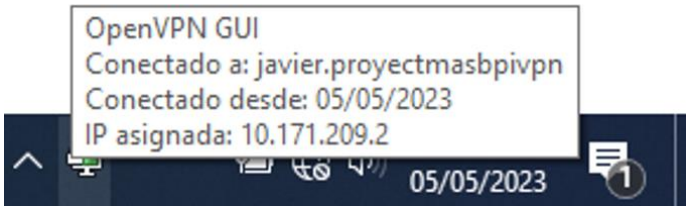
Al no haber facilitado la contraseña anteriormente, cuando se procedió a la importación de los ficheros de configuración para la conexión, a la hora de proceder a establecer la conexión vía VPN, se tendrá que facilitar la contraseña para llevar a cabo la conexión, pudiendo guardarla si se marca la opción Save password, cosa que para este proyecto no se hace, y se pulsa sobre OK, una vez facilitada la contraseña de conexión, esta se establece correctamente.



Al establecerse la conexión correctamente, la ventana de la captura superior se cerrará automáticamente.

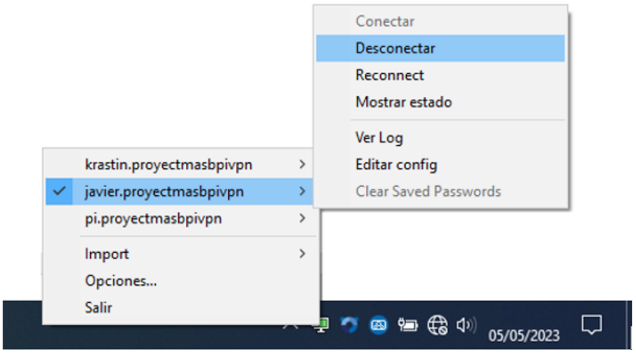


Establecida la conexión, puede aparecer un globo o ventana informativa en el área de notificaciones de la barra de tareas, en la parte inferior derecha, informando que se encuentra “Conectado a javier.proyectmasbpivpn., IP asignada: 10.171.209.2”.

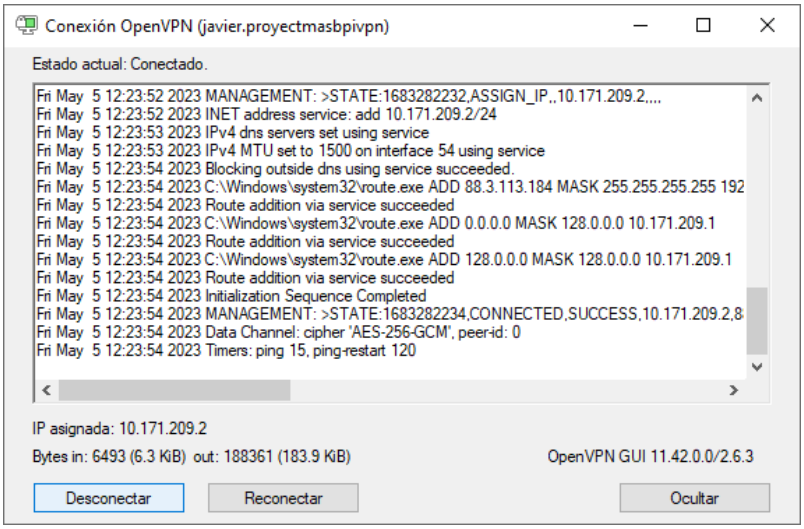


En el caso de pasar el ratón por el icono de la aplicación y encontrarse conectado, se mostrará la ventana de la captura superior, informando de los datos de la conexión.

Según se va procediendo los pasos de la conexión, el icono situado en el área de notificaciones de la barra de tareas cambiará de color, estando sin conexión, el icono se encuentra de esta forma , al pulsar sobre Conectar, cambiará y pasará a estar de color amarillo y al establecerse la conexión con éxito, pasará a tener color verde .



Por último, tras realizar las tareas administrativas necesarias, para cerrar la conexión VPN, se pulsará con el botón derecho del ratón sobre el icono de la aplicación ubicado en el área de notificaciones de la barra de tareas , en el menú que se muestra, se pulsará sobre la conexión activa y posteriormente se pulsará sobre Desconectar, en las opciones de la conexión activa, como se puede observar en la ventana de la captura superior.



Otra opción algo más rápida, es hacer doble clic con el botón izquierdo del ratón sobre el icono de la aplicación en el área de notificaciones de la barra de tareas  , apareciendo la ventana de la captura superior, donde se podrá pulsar sobre Desconectar, para finalizar la conexión establecida con el servidor VPN/WOL.

Al igual que en el proceso de conexión, en el de desconexión, el color del icono de la aplicación ubicado en la barra de tareas cambiara al ir realizando las acciones, al encontrarse conectado tendrá este aspecto  , al estar desconectado pasara a este otro  .

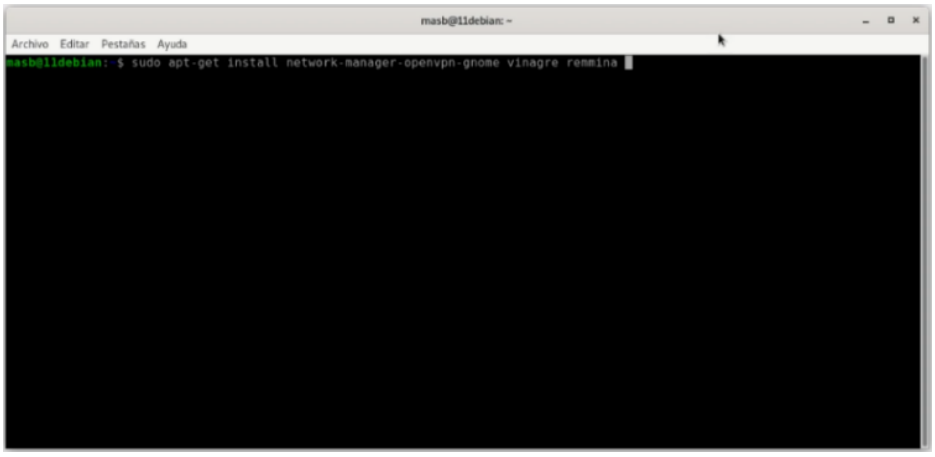
Importación en S.O. Linux.

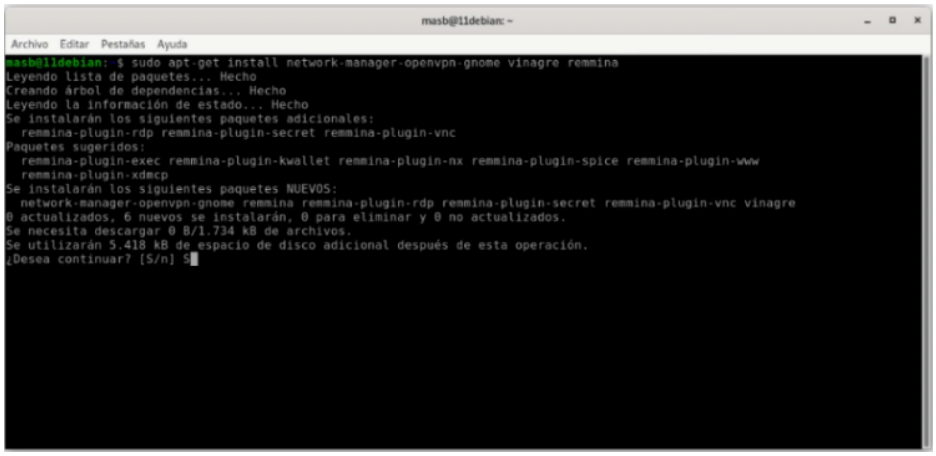
Dependiendo de la distribución de Linux que se utilice, puede ser necesario la instalación de la aplicación network-manager-openvpn-gnome

En caso de ser necesario esta acción, será tan sencillo como acceder a una ventana de terminal y ejecutar el comando.

sudo apt-get install network-manager-openvpn-gnome

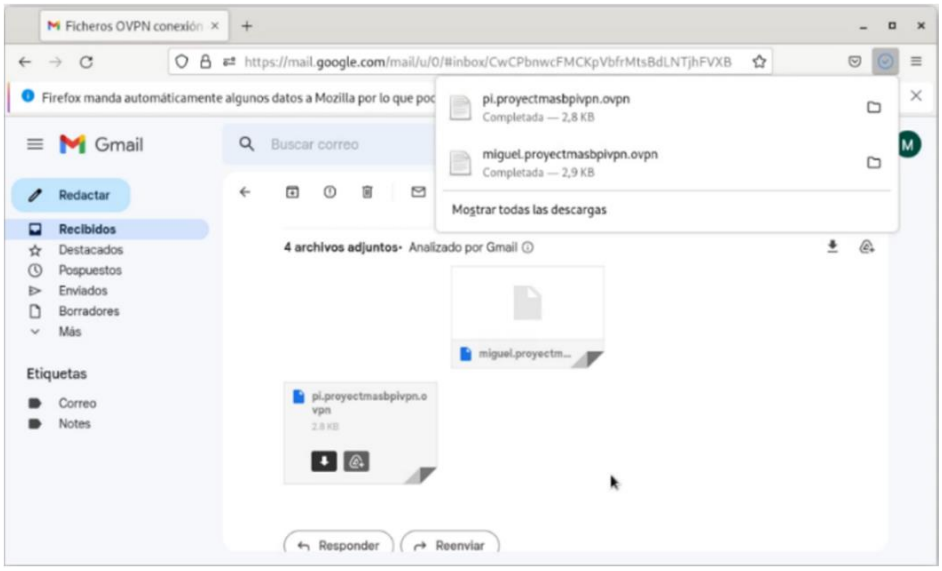
En este ejemplo, la instalación de las aplicaciones vinagre y remmina no son necesarias.





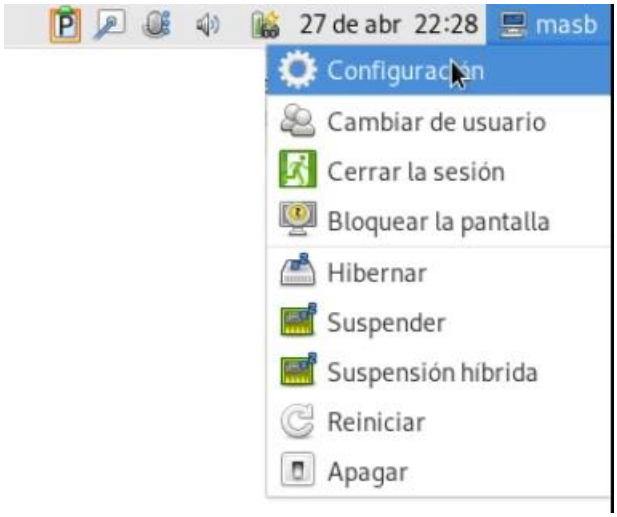
En caso de solicitar la contraseña de un usuario con permisos de instalación se facilitará la contraseña, puede que dependiendo de las aplicaciones instaladas sea necesario instalar las dependencias de la aplicación a instalar, en ese caso se escribirá la letra “S” y se pulsará INTRO.

Terminada la instalación se podrán utilizar los ficheros de configuración creados en el servidor VPN/WOL.

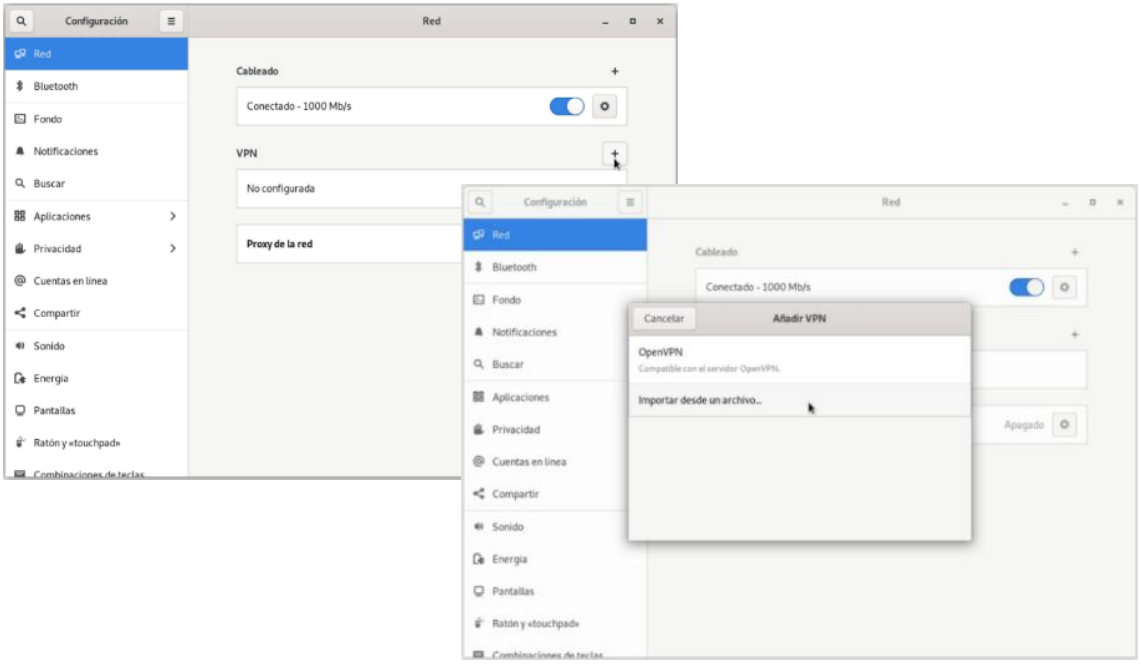


Las opciones que se describen a continuación, pueden diferir por el tipo de escritorio elegido para trabajar dentro de la sesión del usuario.

Para la importación de los ficheros de configuración OVPN de los usuarios creados en el servidor, una vez descargados los ficheros necesarios y en este caso en el S.O. Linux Debian.



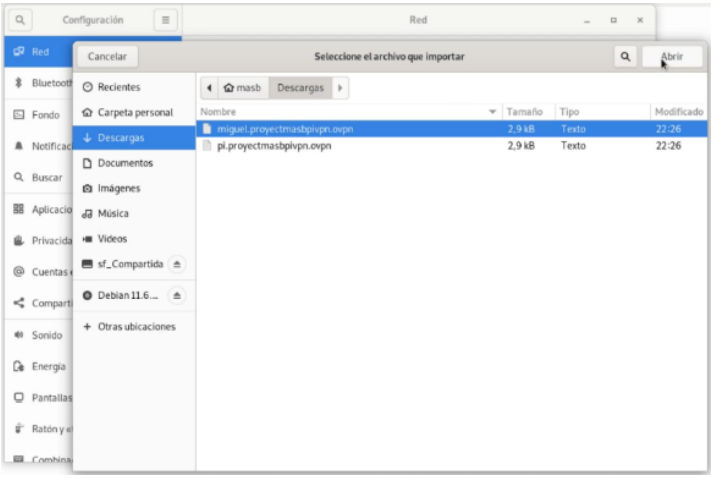
Habrá que acceder a las opciones de configuración del sistema, en este ejemplo en la parte superior derecha, sobre el nombre de usuario que ha iniciado sesión, habrá que pulsar con el botón izquierdo del ratón y se pulsará sobre Configuración en el menú que aparece.



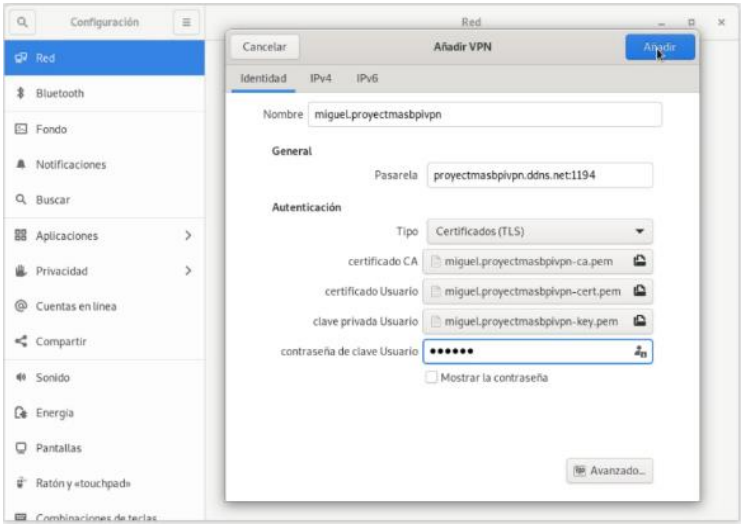


Dentro de Configuración, en el panel lateral izquierdo, se pulsará sobre Red y en el panel lateral derecho, se pulsará en el símbolo “+”, situado en el apartado derecho de la opción VPN, captura superior izquierda.

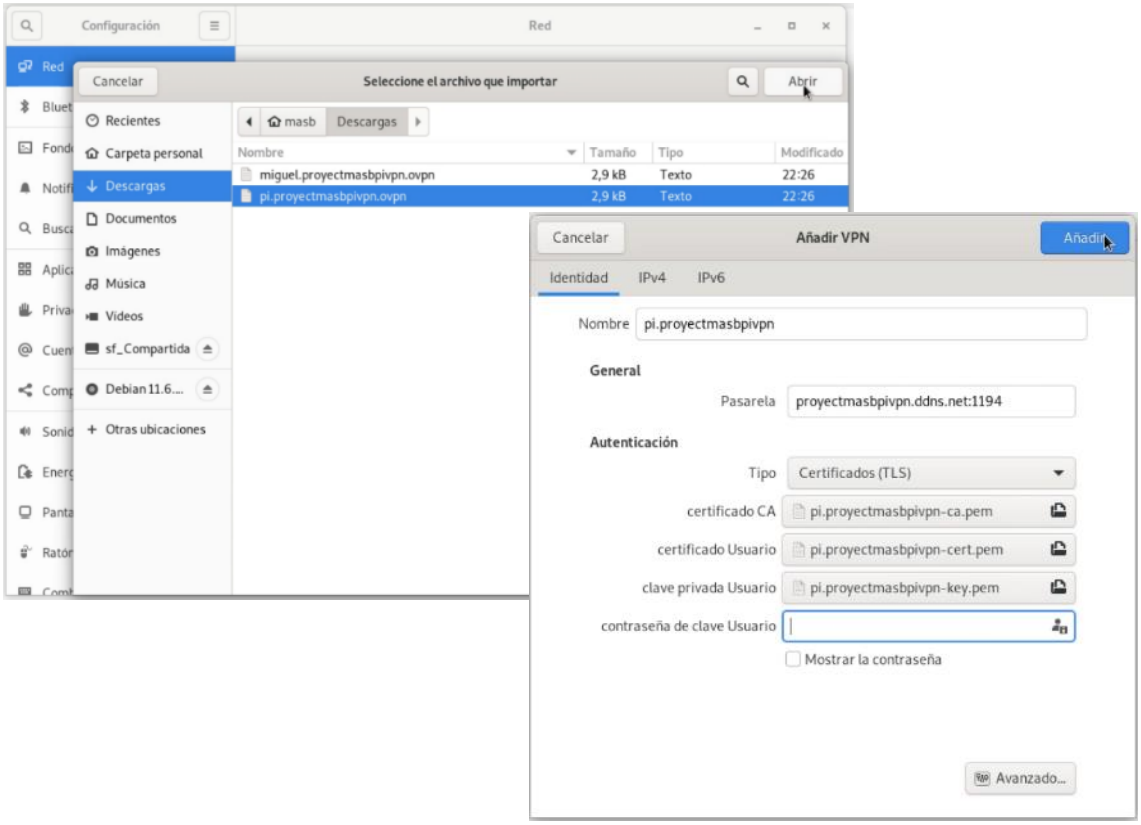
Posteriormente, en el cuadro de dialogo que se muestra, se pulsará sobre Importar desde un archivo…, captura superior derecha.



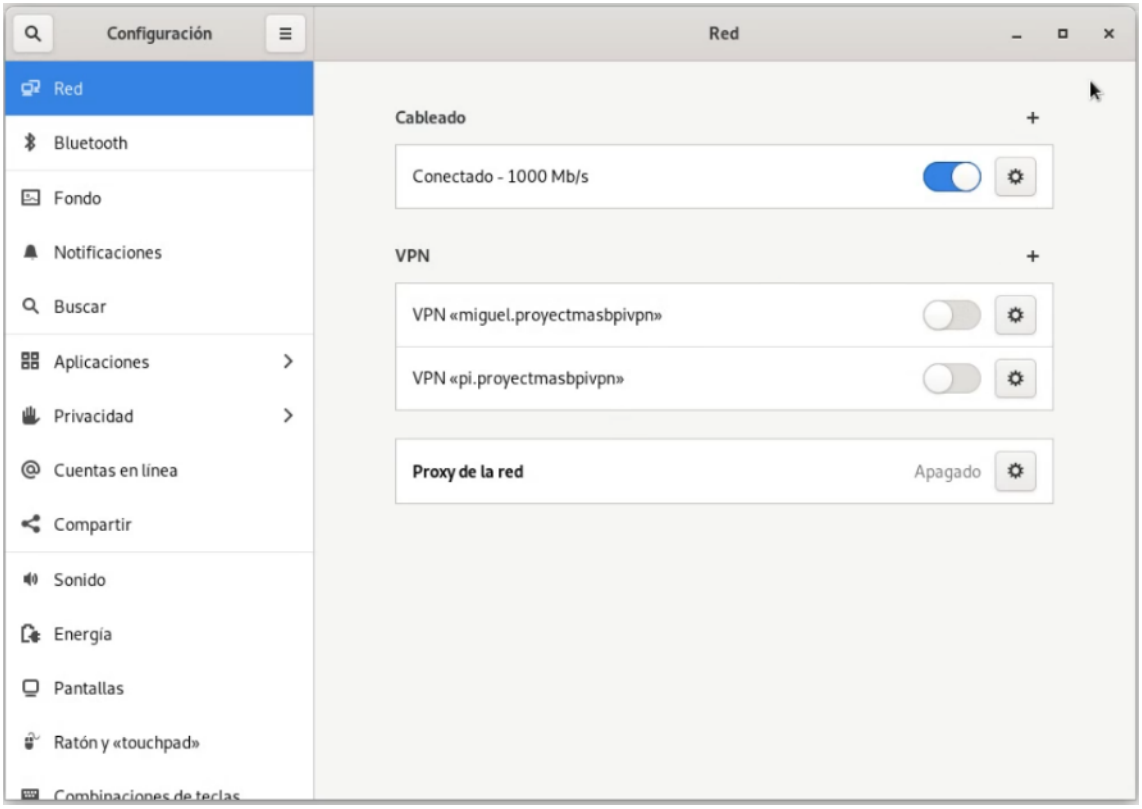
En la ventana del asistente que se abre, habrá que dirigirse a la carpeta donde se descargaron los ficheros de configuración, en este caso, en la carpeta Descargas, se seleccionará un fichero y se pulsará el botón superior derecho Abrir.



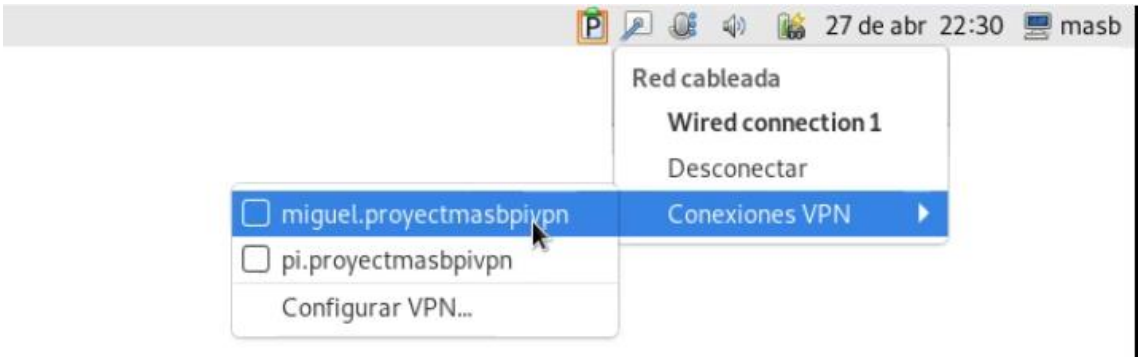
Como se puede observar en la ventana de la captura superior, se podrá facilitar la contraseña del usuario para realizar la conexión automáticamente sin que se solicite, se facilite o no, se pulsará el botón superior derecho Añadir.



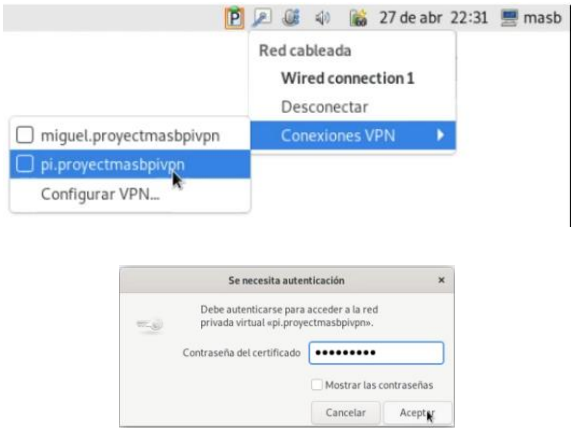
Ejemplo de importación de la configuración de un fichero de configuración sin añadir la contraseña, en este caso, al proceder a realizar la conexión, se solicitará la contraseña.



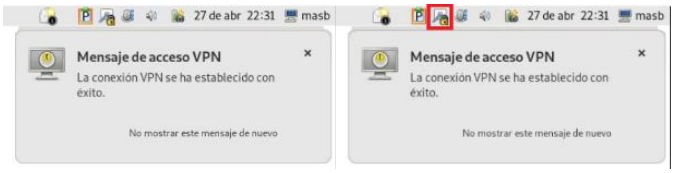
Como se puede observar en la captura superior, ventana Configuración \ Red, panel derecho VPN, ya aparecen las dos conexiones, una por cada usuario importado, en este ejemplo no se realiza la conexión desde la ventana Configuración.



Para realizar la conexión, se pulsará con el botón izquierdo del ratón sobre el icono  , situado en la parte superior derecha de la barra superior, en el menú que se muestra, se pulsará sobre Conexiones VPN y posteriormente, se seleccionará y se pulsará sobre el perfil de conexión que se disponga.

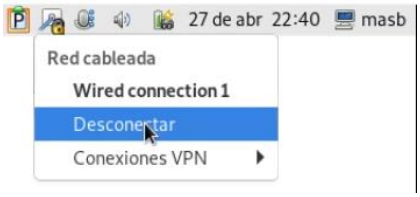


Si se selecciona un perfil de conexión donde no se facilitó la contraseña, a la hora de proceder a establecer la conexión se solicitará, teniendo que escribir la contraseña y tras escribirla, se pulsará en Aceptar.



Establecida la conexión, el icono de la barra de tareas cambiará, icono sin establecerse la conexión , icono al establecerse la conexión , como puede apreciarse, apareciendo un cuadro de dialogo indicando que la conexión VPN se ha establecido con éxito.

Una vez finalizadas las acciones administrativas como administrador, o el trabajo como usuario, se podrá desconectar del servidor VPN/WOL.



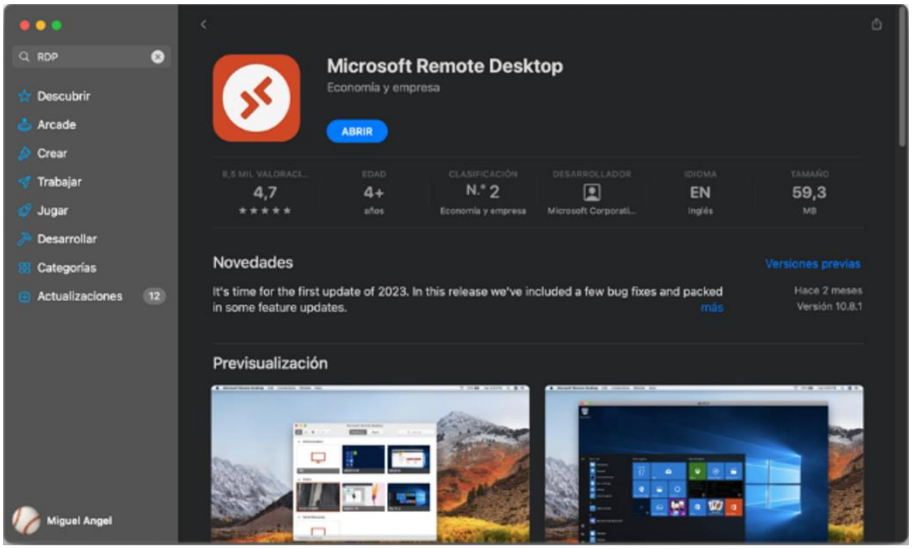
Para realizar la desconexión, se pulsará con el botón izquierdo del ratón sobre el icono , situado en la parte superior derecha de la barra superior, en el menú que se muestra, se pulsará sobre Desconectar.



El icono de la barra de tareas , cambiará al terminar la conexión , cómo puede apreciarse en la ventana de la captura superior.

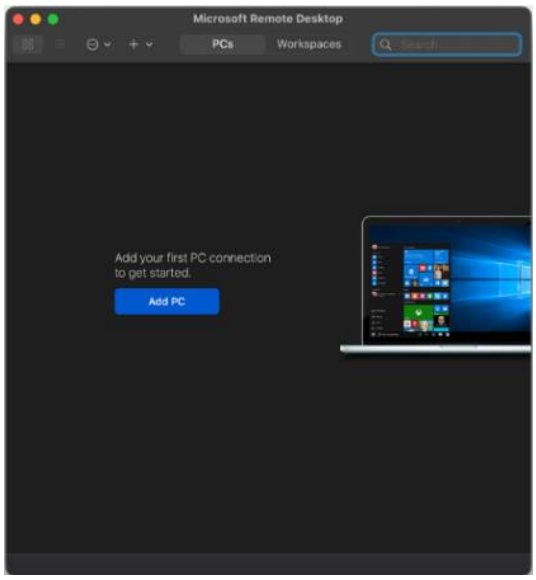
Descarga instalación configuración y conexión Microsoft Remote Desktop y remmina.

Descarga e instalación Microsoft Remote Desktop Apple macOS.



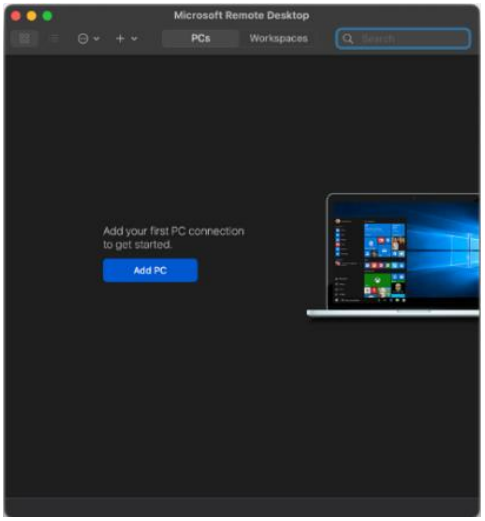
Para instalar la aplicación, habrá que ir a la Apple Store, en el buscador, en la imagen superior, parte superior izquierda, se escribirá RDP, al pulsar INTRO o pulsar sobre la lupa comenzará la búsqueda, como se puede observar en la ventana de la captura superior.

Localizada la aplicación, se pulsará sobre el botón Instalar u Obtener, al instalarse la aplicación, se podrá pulsar sobre el botón Abrir.

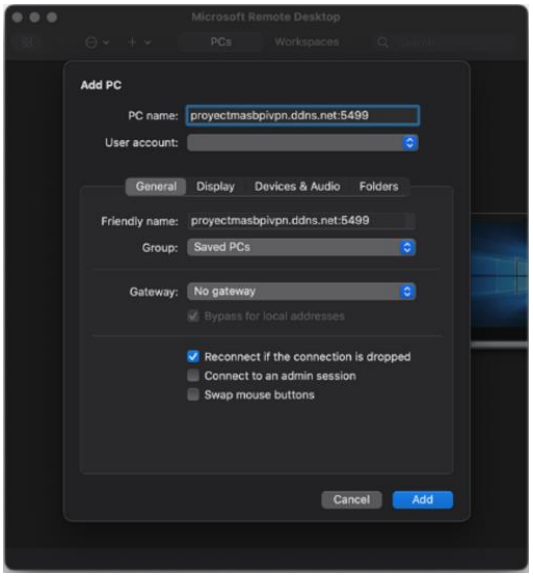


Con la aplicación Microsoft Remote Desktop instalada, se abrirá para poder agregar los escritorios remotos.

Configuración aplicación Microsoft Remote Desktop en Apple macOS.

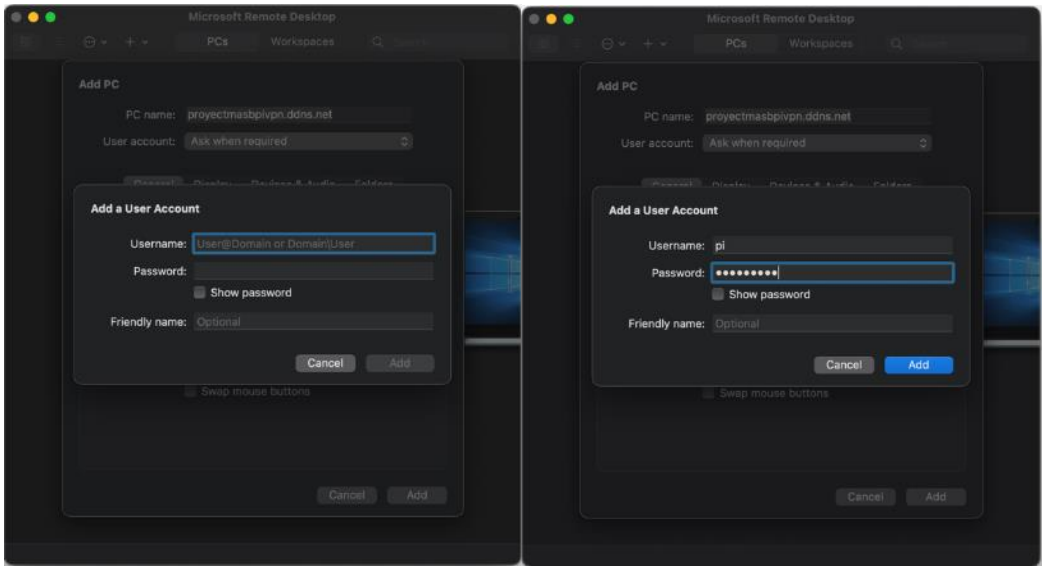


Una vez instalada la aplicación Microsoft Remote Desktop, se abrirá para realizar la configuración de las conexiones.
En este ejemplo, se crea la conexión al equipo servidor VPN/WOL, correspondiente a la Raspberry Pi, la creación de la conexión de cualquier otro equipo es similar a la explicación que se describe aquí.
Para agregar un equipo, en este caso como ejemplo, se añadirá como equipo la Raspberry Pi, se pulsará sobre el botón azul Add PC.



En la nueva ventana que aparece, se tendrán que rellenar los siguientes campos.

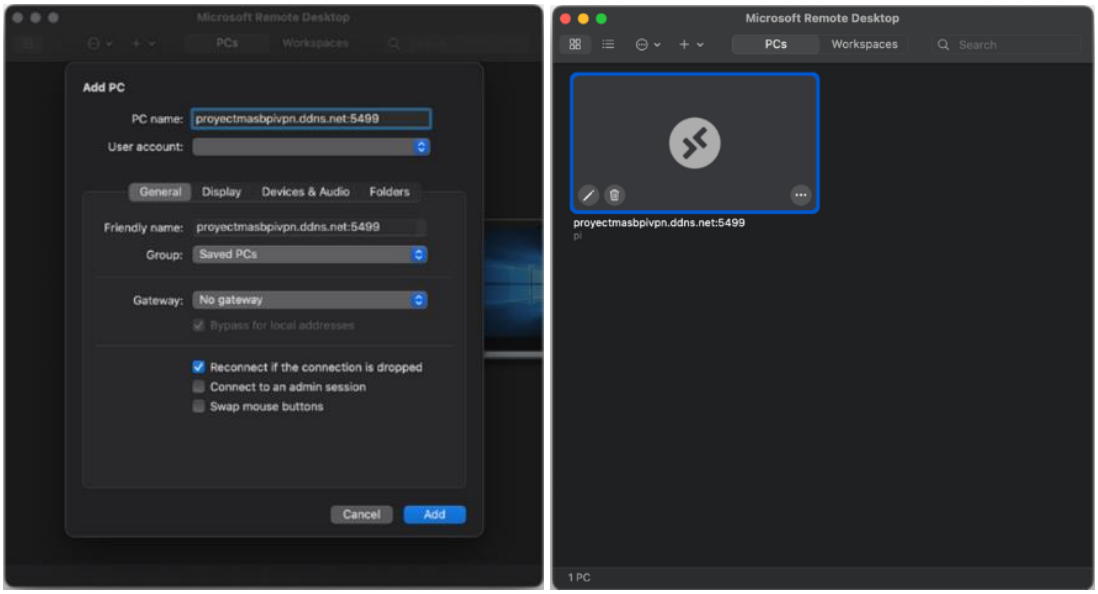
- Nombre de PC, se coloca el nombre de dominio o host creado anteriormente junto con el puerto abierto en el router para esta conexión. proyectmasbpivpn.ddns.net:5499
- User account se pulsará sobre Add User Account…, en caso de querer añadir el usuario y su contraseña, en este caso no se agrega, con lo que se solicitará cada vez que se quiera establecer la conexión con el servidor VPN/WOL.
- Friendly name, es opcional, nombre descriptivo, en este caso se coloca el nombre de dominio o host creado anteriormente junto con el puerto abierto en el router para esta conexión, proyectmasbpivpn.ddns.net:5499



En el caso de haber seleccionado User Account, para añadir usuario y contraseña, se mostrará la ventana de la captura superior, Add a User Account , donde se tendrá que introducir el usuario y la contraseña para la conexión que se está creando.

- Username, el nombre de usuario que corresponda, en este caso pi.
- Password, se proporcionará la contraseña del usuario indicado en el apartado Username.

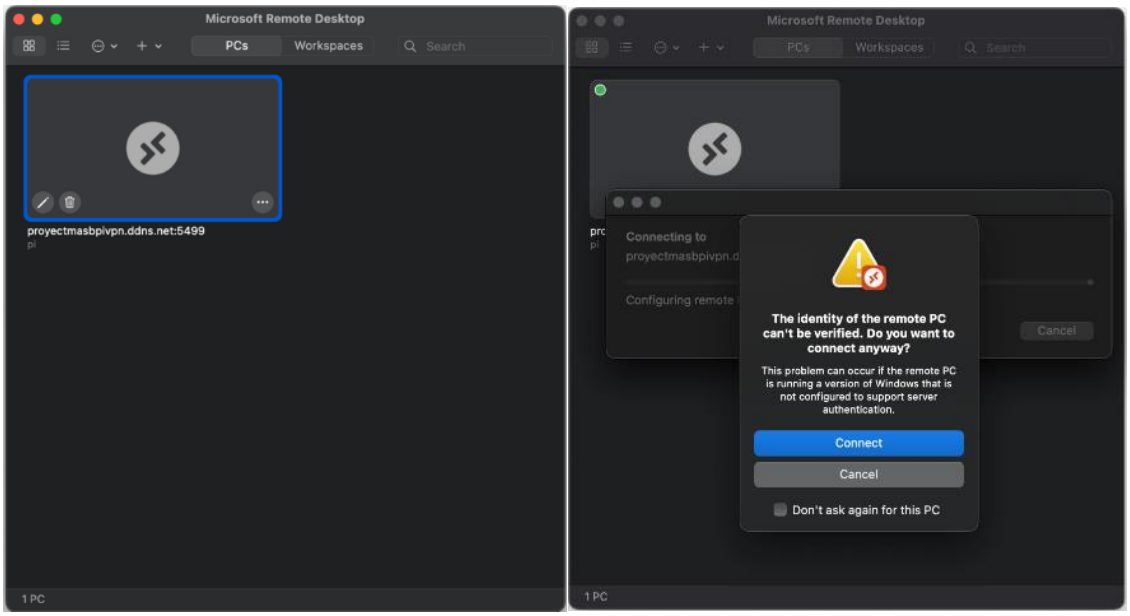
Facilitados los datos se pulsará sobre Add.



Añadidos todos los datos se pulsará Add.

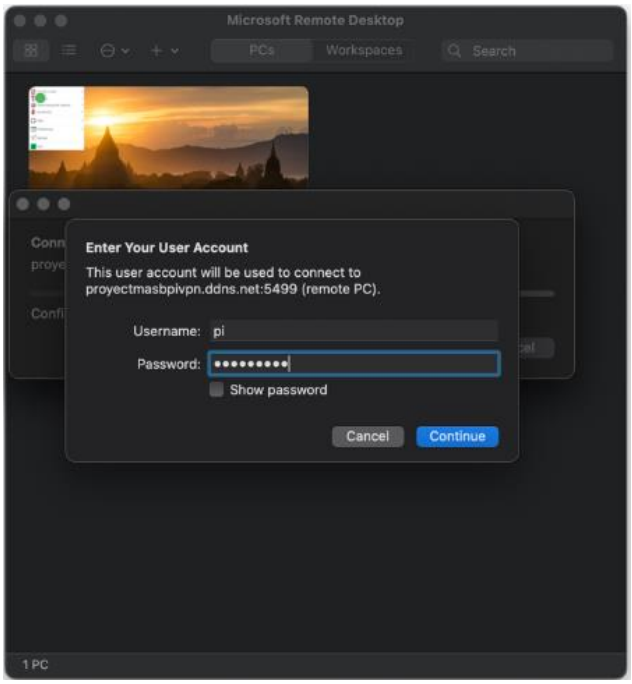
Creándose la conexión y apareciendo una miniatura a esta conexión dentro de la aplicación, como se puede apreciar en la ventana de la captura superior derecha.

Conexión RDP Microsoft Remote Desktop.

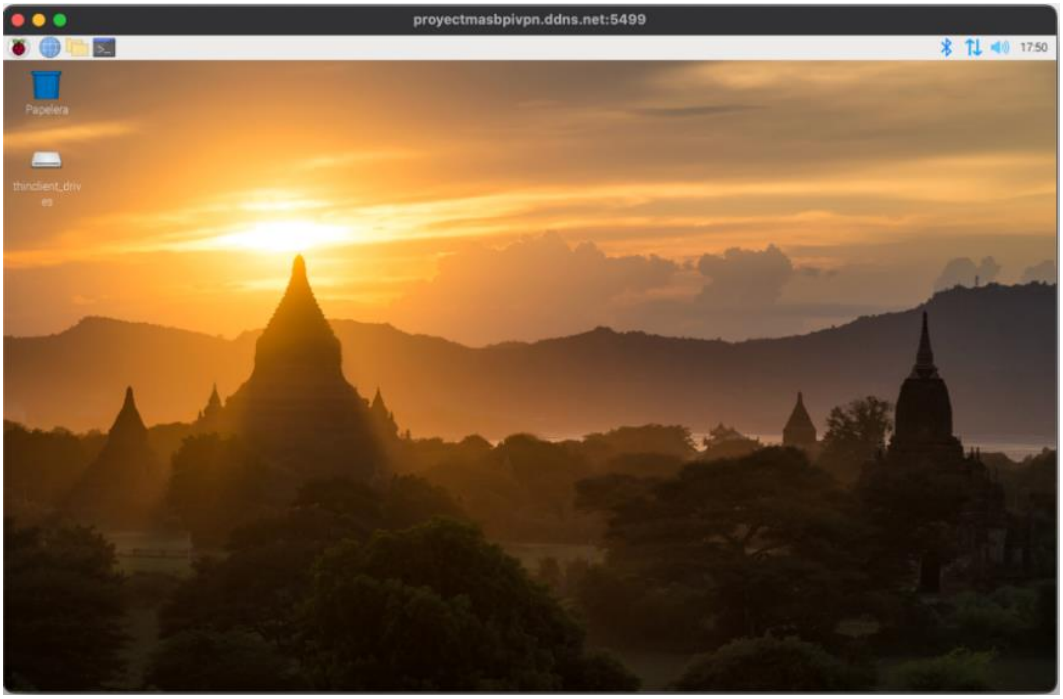


Para realizar la conexión, teniendo abierta la aplicación Microsoft Remote Desktop, se podrá pulsar con el botón derecho del ratón sobre la miniatura de la conexión creada, y en el menú que se muestra, se pulsará sobre Connect, o en su defecto, hacer doble clic con el botón izquierdo del ratón sobre la miniatura de la conexión creada.

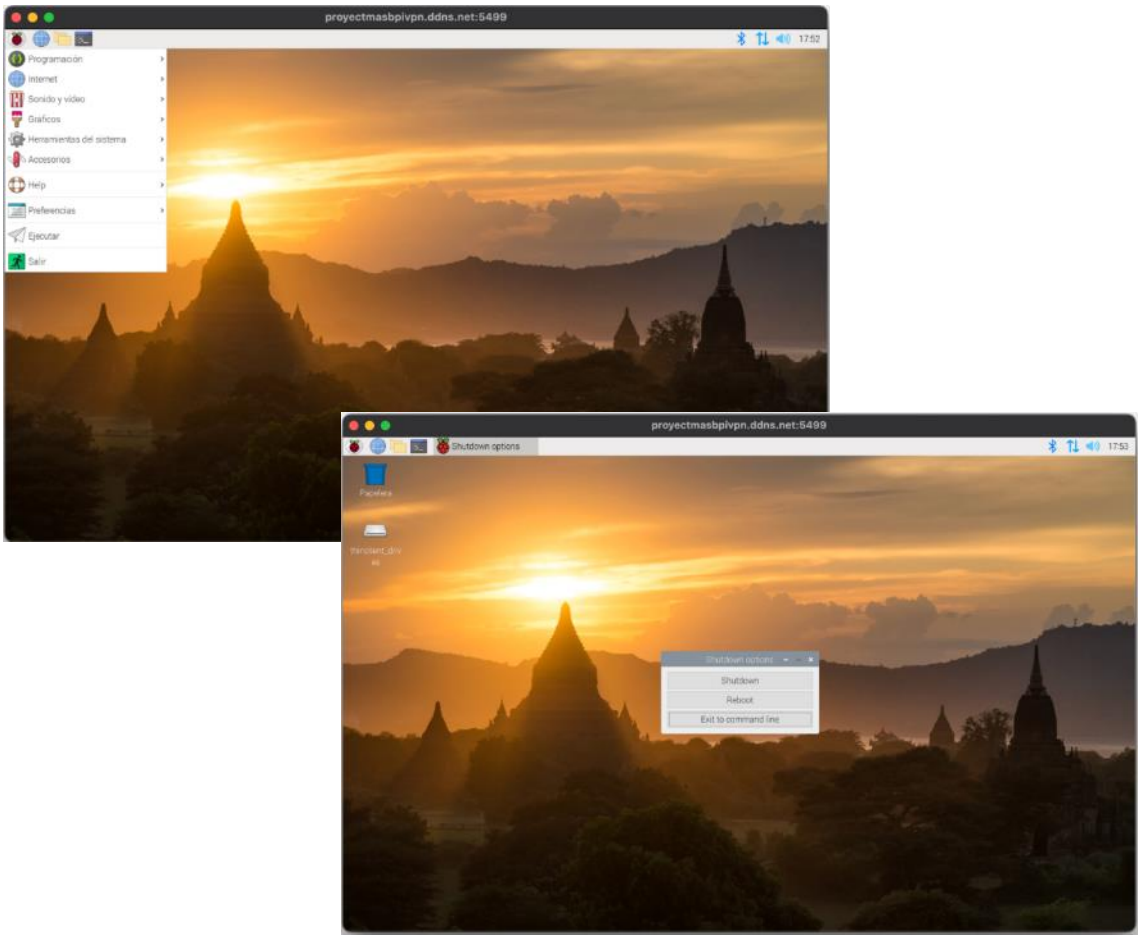
En la ventana que aparece, indicando que no se ha verificado la identidad del equipo se pulsara sobre Connect.

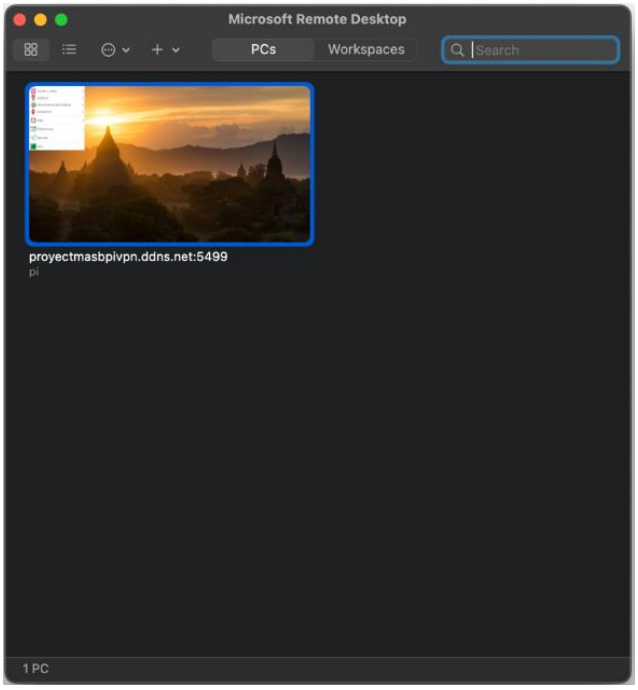


Acto seguido, se tendrá que facilitar el usuario y la contraseña para autenticarse y establecer la conexión, en caso de que estos datos se facilitasen a la hora de la creación de la conexión, estos datos no se solicitaran realizando la conexión automáticamente.

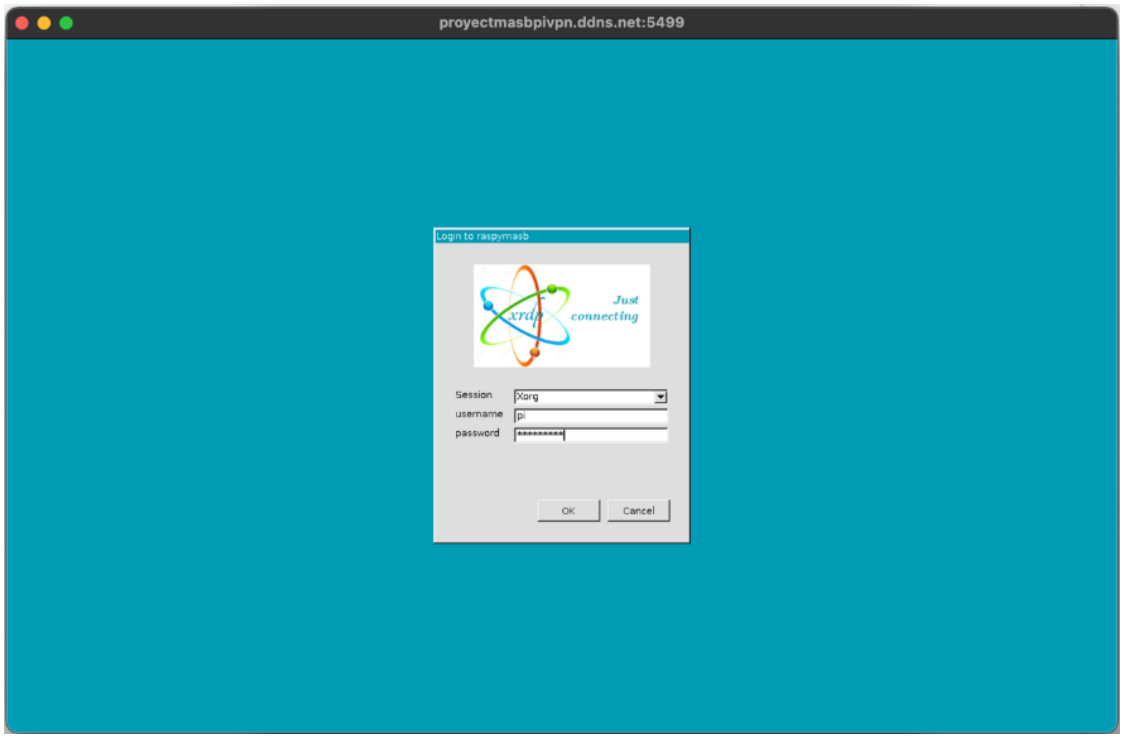


Como se puede observar, aparece el escritorio de la Raspberry Pi, servidor VPN/WOL.



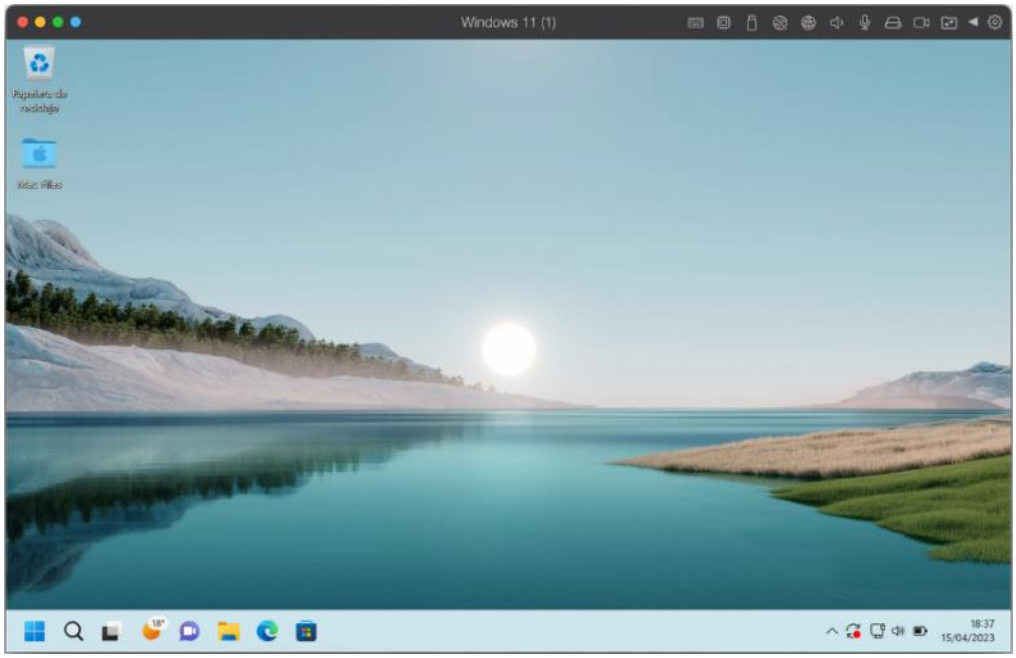


Finalizada la conexión, en el programa donde se realizó la configuración, se mostrará una miniatura de la conexión.

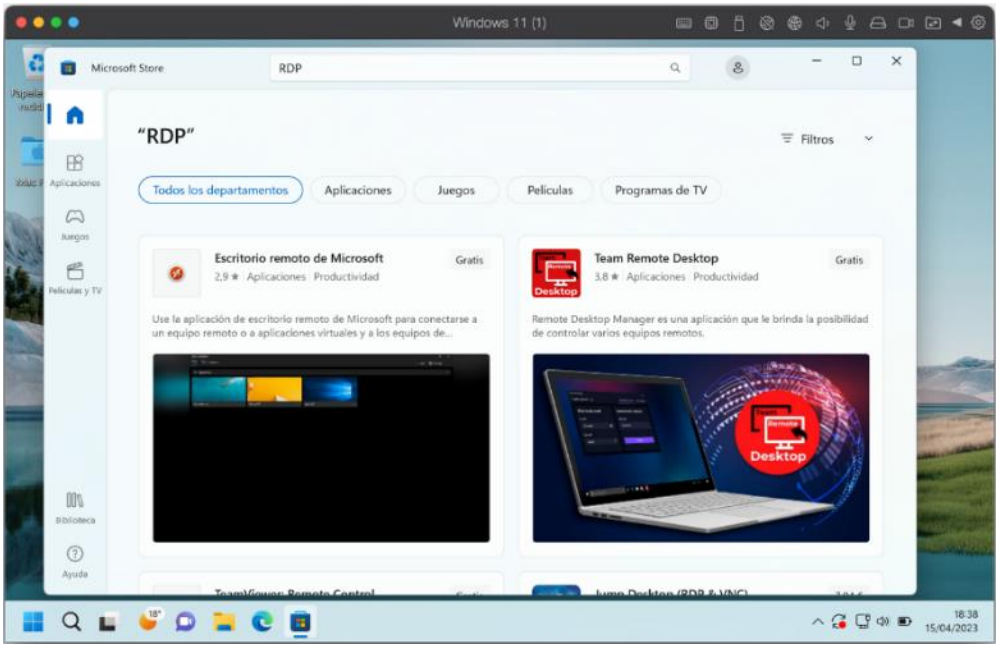


En el caso de que al escribir las credenciales (usuario y contraseña), estas se facilitasen erróneamente, al intentar establecer la conexión, se mostrará una ventana donde se tendrá la posibilidad de realizar nuevamente la autenticación, introduciendo correctamente el usuario y la contraseña.

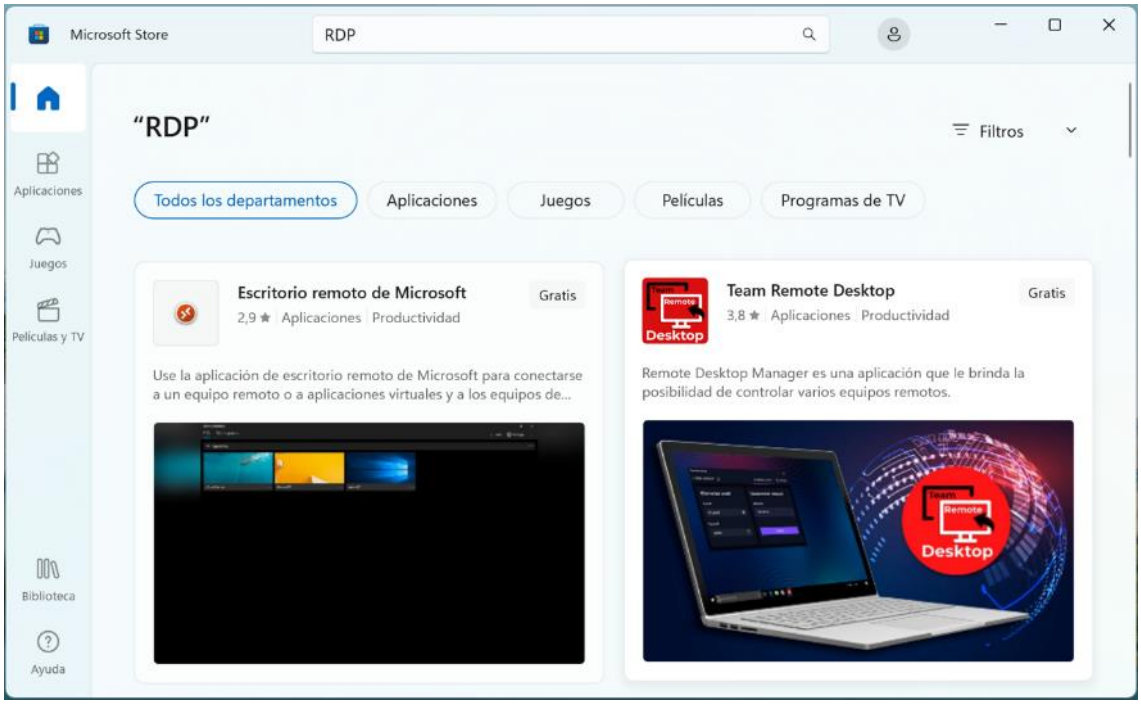
Descarga e instalación en S.O. Windows.



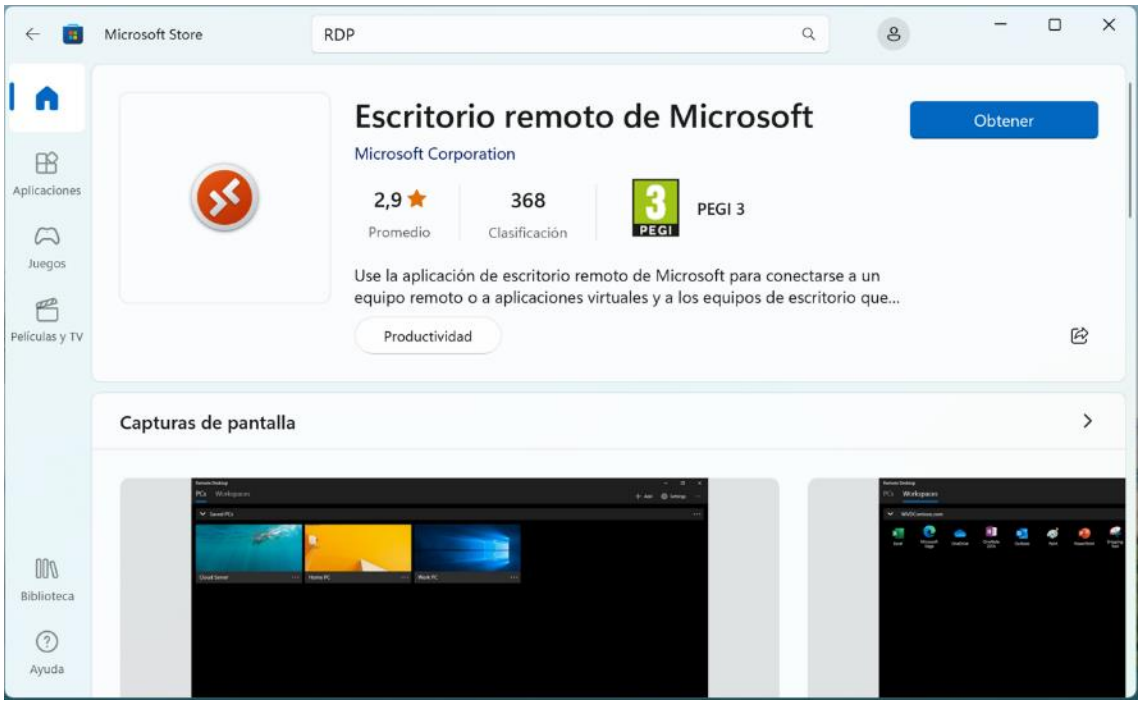
Se ha realizado este proceso de instalación en equipos reales físicos, y como se puede apreciar en la ventana de la captura superior, en este caso se realizará en una máquina virtual con S.O. Windows, dentro de un equipo con S.O. macOS.



Dentro de la máquina virtual con S.O. Windows, habrá que acceder a la Microsoft Store (Tienda de Microsoft), en la parte superior, en la zona de búsqueda, se escribirá RDP y se pulsará INTRO.



Tras pulsar INTRO, se mostrarán los resultados, se seleccionará y se pulsará sobre Escritorio remoto de Microsoft.

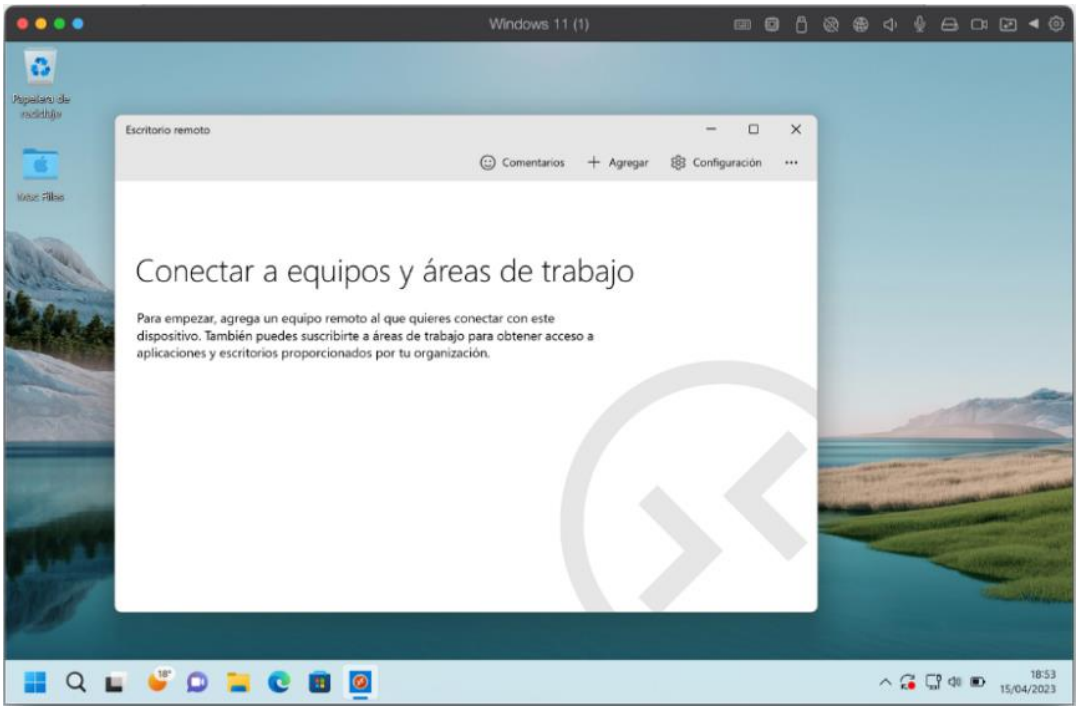


Mostrándose información de la aplicación, se pulsará sobre el botón superior derecho Obtener.



Instalada la aplicación, se podrá pulsar sobre el botón superior derecho Abrir, para abrir la aplicación.

Configuración aplicación Microsoft Remote Desktop en Windows.



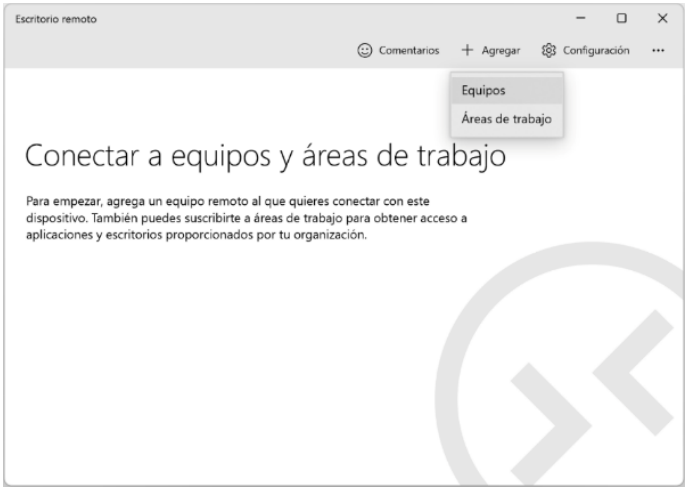
Una vez instalada la aplicación Microsoft Remote Desktop, se abrirá para realizar la configuración de la conexión.

En este ejemplo, se crea la conexión al equipo servidor VPN/WOL, correspondiente a la Raspberry Pi, la creación de cualquier otro equipo, es similar al ejemplo que se describe aquí.

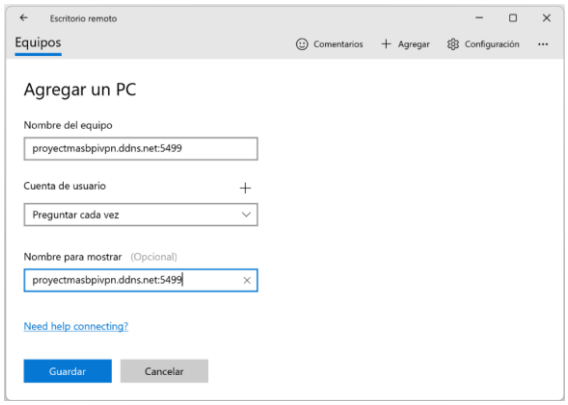


Para agregar un equipo, en este caso como ejemplo se añadirá como equipo la Raspberry Pi, se pulsará sobre Agregar en la parte superior derecha, 

.



En las opciones que se muestran, se pulsará sobre Equipos.



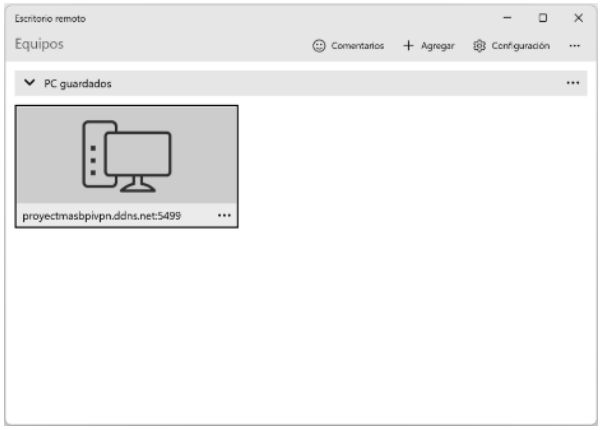
En la nueva ventana que aparece, habrá que rellenar ciertos datos como se indica a continuación.

- Nombre del equipo, se coloca el nombre de dominio o host creado anteriormente junto con el puerto abierto en el router para esta conexión proyectmasbpivpn.ddns.net:5499
- Cuenta de usuario, se pulsará sobre el símbolo “+” +, en caso de querer añadir usuario y su contraseña, en este caso no se agrega, con lo que se solicitará cada vez que se quiera establecer la conexión.
- Nombre para mostrar, es opcional, nombre descriptivo, como ejemplo se pone proyectmasbpivpn.ddns.net:5499

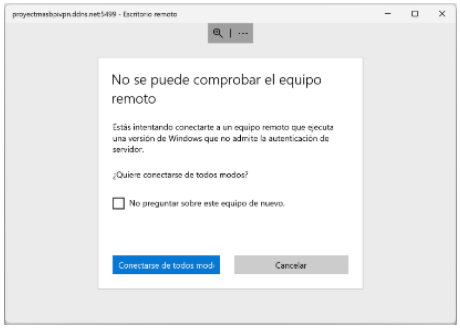
En el caso de añadir en el apartado Cuenta de usuario, un usuario y su contraseña, aparecerá una ventana donde habrá que indicar los datos requeridos (usuario y contraseña), para la conexión que se está creando, posteriormente se pulsará sobre Guardar, para guardar las credenciales de autenticación para esa conexión.

Facilitados los datos, se pulsará sobre Guardar.

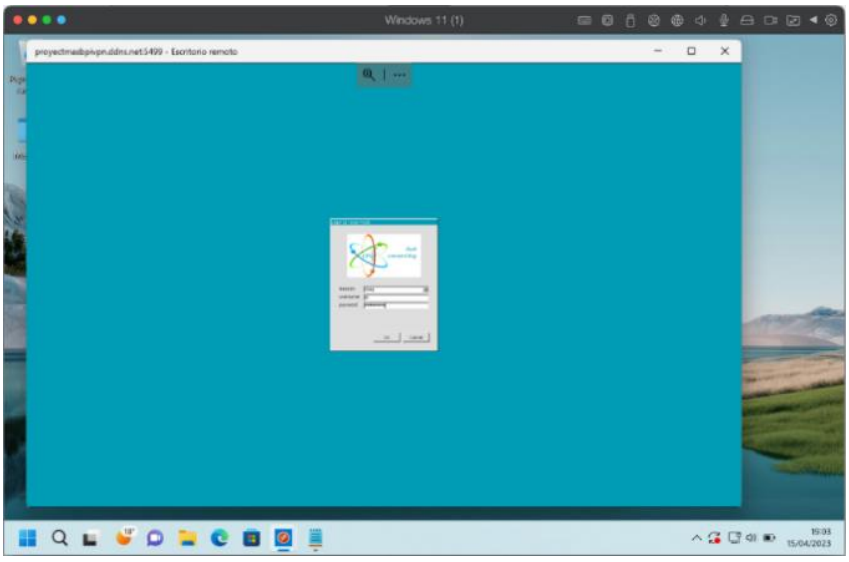
Conexión RDP Microsoft Remote Desktop.



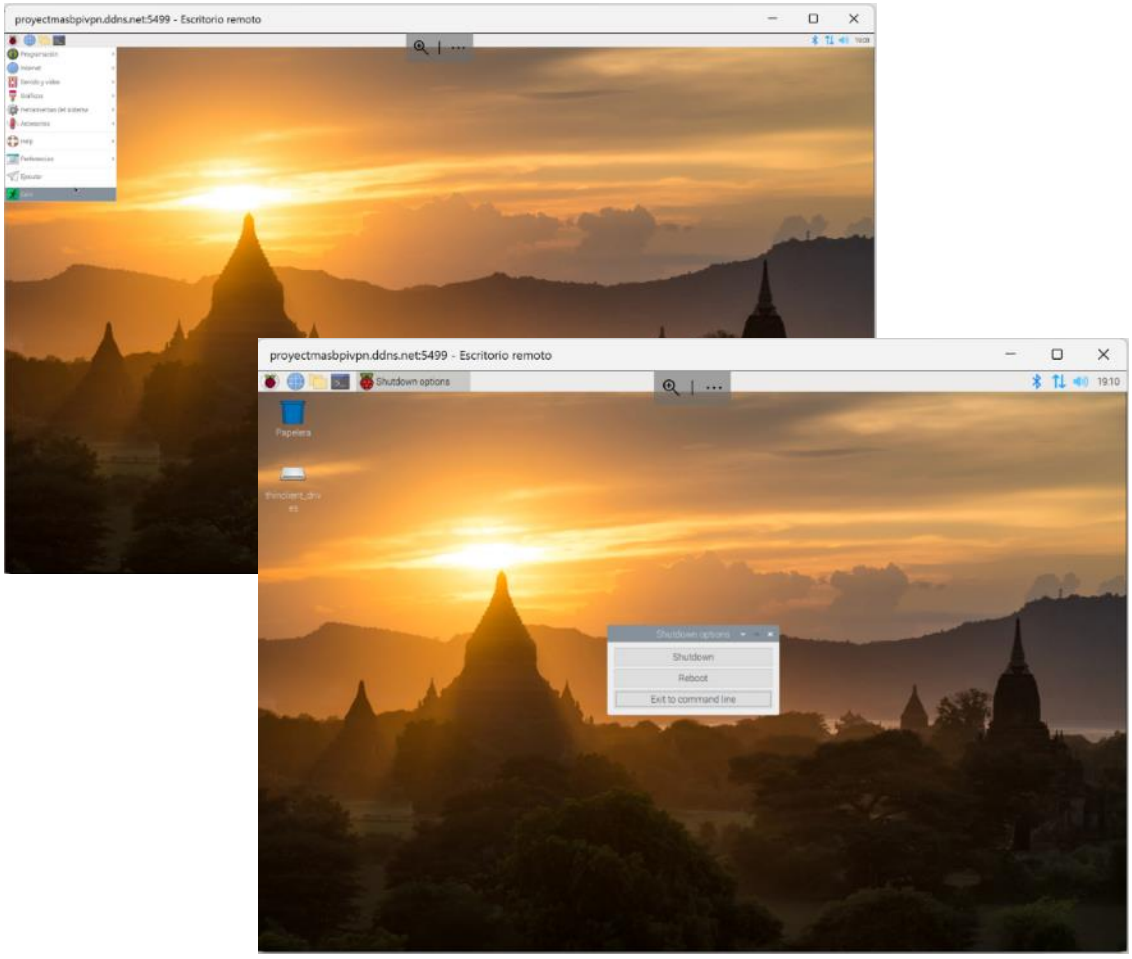
Con la aplicación Escritorio remoto abierta y la configuración de la conexión creada, se podrá hacer doble clic con el botón izquierdo del ratón sobre la miniatura de la conexión, para comenzar el establecimiento de la conexión con el servidor VPN/WOL.



En la ventana donde se indica que no se puede comprobar el equipo remoto, se pulsará sobre Conectarse de todos modos.

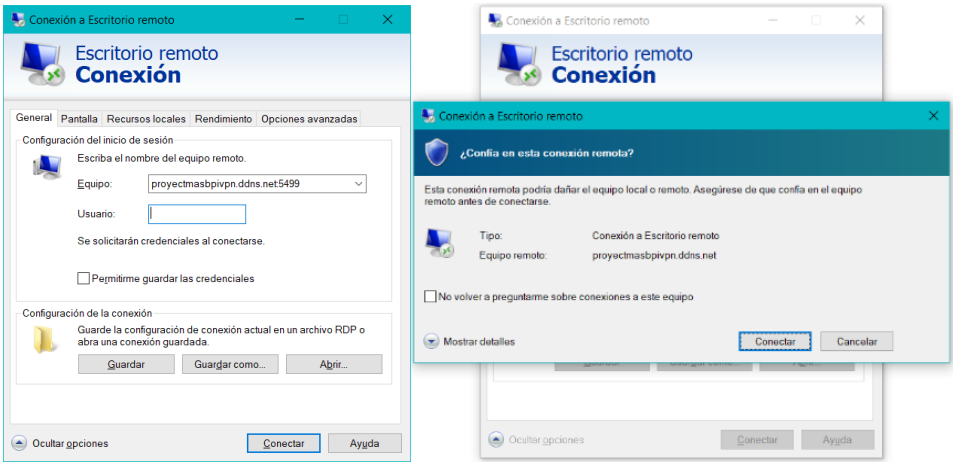


Al establecerse la conexión, y no haber facilitado las credenciales en la configuración, se muestra una ventana para realizar la autenticación, teniendo que proporcionar el usuario y la contraseña y se pulsará OK.



Proporcionadas las credenciales usuario y contraseña, se pulsará sobre Ok, accediendo al escritorio remoto del servidor VPN/WOL, donde se podrá realizar las tareas necesarias, y posteriormente al finalizar estas tareas, finalizar la sesión de escritorio remoto y salir a la línea de comandos, perdiéndose la conexión.

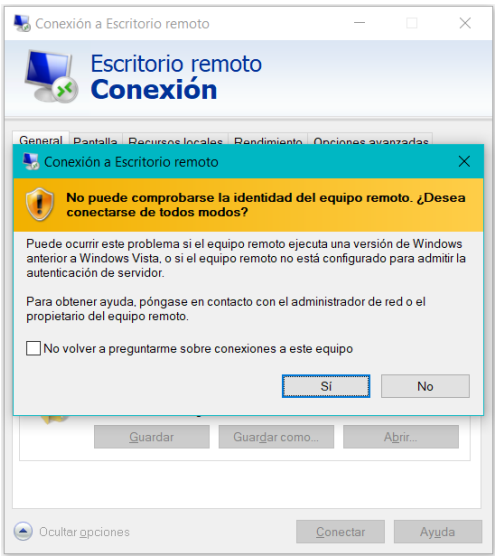
Conexión RDP Escritorio remoto S.O. Windows.



Esta aplicación se encuentra por defecto en equipos con S.O. Windows, totalmente gratuita.

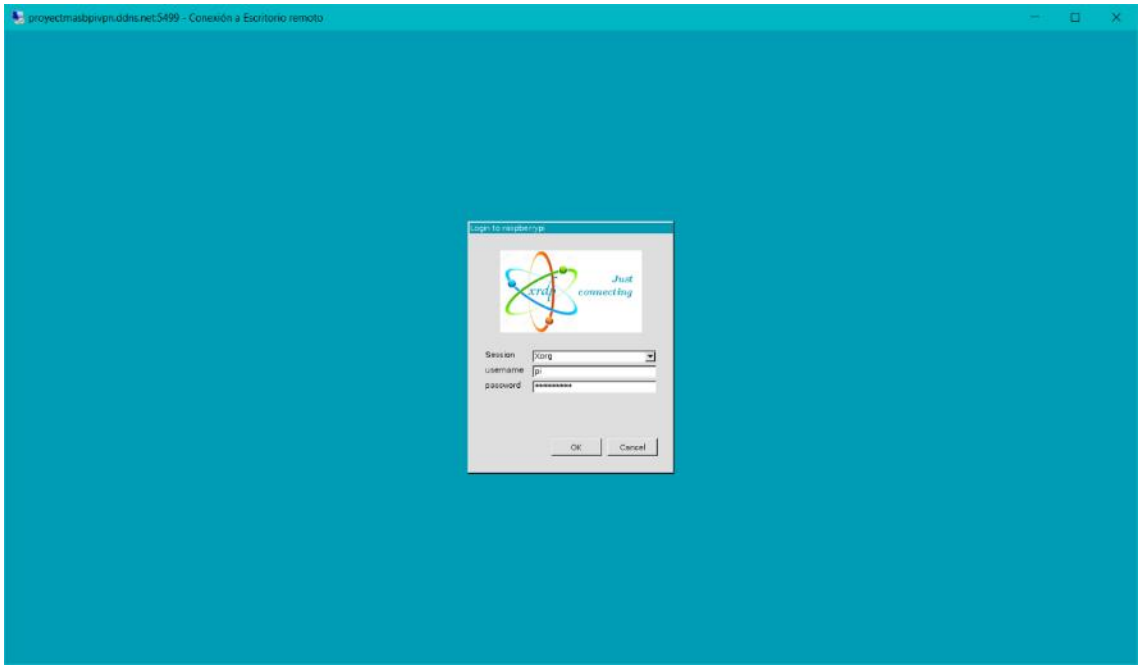
Esta opción de conexión, se encuentra por defecto en los S.O. Windows, se podrá acceder a ella buscándola en el cuadro de búsqueda de la barra de tareas en la parte inferior izquierda, donde se escribirá “Escritorio”, sin las comillas, apareciendo como resultado de la búsqueda, Conexión a Escritorio Remoto, se pulsará con el botón izquierdo del ratón para abrir la aplicación.

Con la aplicación abierta, en el apartado Equipo, se escribirá el nombre de dominio o host creado y el puerto abierto para esta conexión separado por “:”, siendo en este caso proyectmasbpivpn.ddns.net:5499, se podrá indicar el usuario en el apartado Usuario, con los datos introducidos se pulsará en el botón inferior Conectar, ventana de la captura superior izquierda.



En la nueva ventana que se muestra se seleccionara y se pulsara sobre Conectar, ventana de la captura superior derecha.

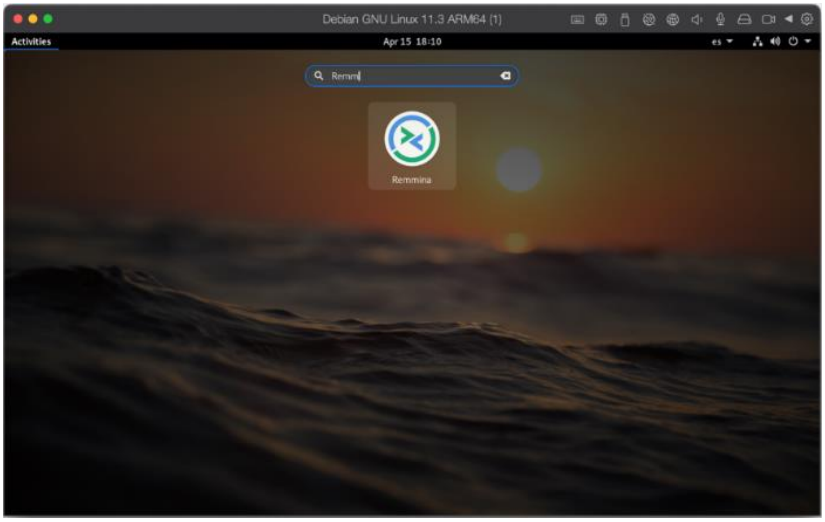
Para establecer la conexión se pulsará sobre Sí en la nueva ventana que se muestra.



Al no haber proporcionado la contraseña, se tendrá que facilitar en la ventana de la captura superior, para realizar la autenticación y establecerse la conexión.

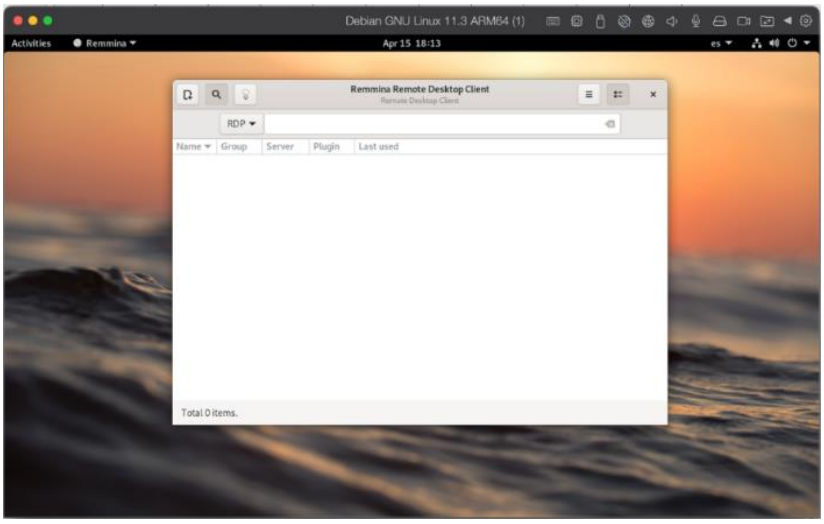
Configuración conexión RDP remmina S.O. Linux.

Al haber instalado vinagre y remmina, no es necesario la instalación de ningún otro software en una distribución Linux cliente, en este ejemplo, se realizan las pruebas en una máquina virtual con Linux Debian Desktop, ejecutándose dentro de un equipo con S.O. macOS.

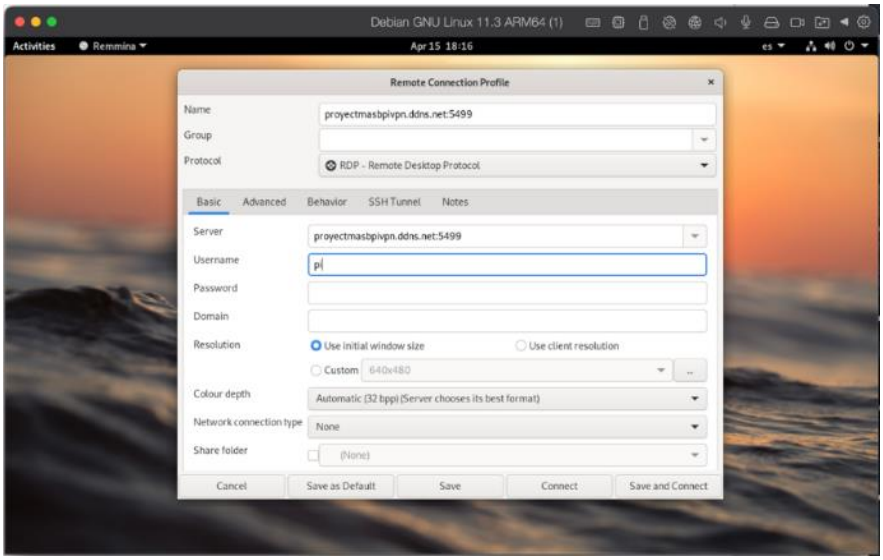


Se buscará la aplicación Remmina para abrirla, puesto que su instalación ya se explicó, aunque se explicó como instalarse en el equipo servidor, esta instalación es válida para un equipo cliente con S.O. Linux Desktop, donde únicamente, dentro de un terminal habrá que ejecutar el comando de instalación. (en distribuciones derivadas de Debian).

sudo apt-get install vinagre remmina



Dentro de la aplicación, para agregar una configuración de conexión, se pulsará sobre el icono superior izquierdo  .



En la nueva ventana que se muestra, habrá que rellenar ciertos datos como se indica a continuación.

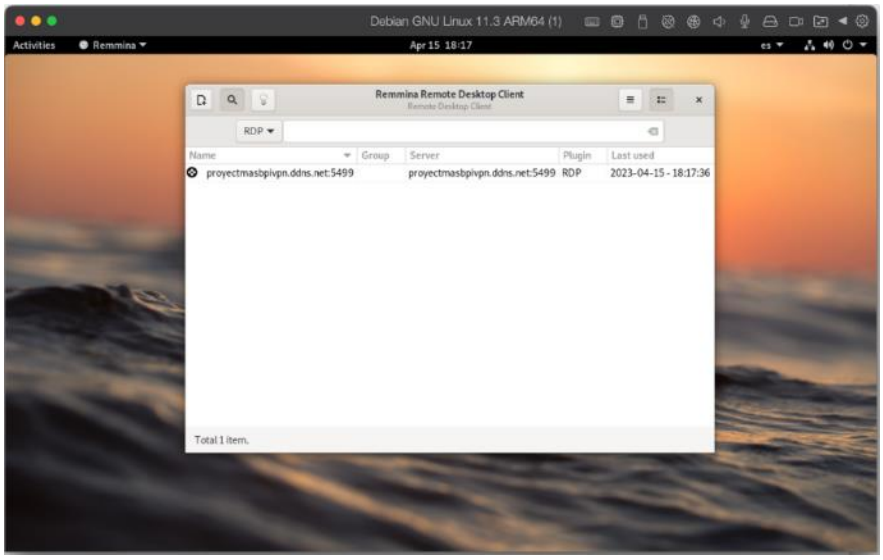
- Name, se coloca el nombre de dominio o host creado anteriormente junto con el puerto abierto en el router para esta conexión separado por ":". proyectmasbpivpn.ddns.net:5499
- Protocol, se dejará la opción por defecto RDP – Remote Desktop Protocol.
- Server, se indicará el nombre de dominio o host creado, junto con el puerto abierto en el router para esta conexión, separado por ":". proyectmasbpivpn.ddns.net:5499
- Username, en este apartado se podrá indicar el usuario con el que se pretende establecer la conexión al escritorio remoto, en este ejemplo se coloca el usuario "pi".
- Password, se podrá facilitar la contraseña del usuario indicado en el apartado Username, para realizar la conexión al escritorio remoto automáticamente sin solicitar usuario ni contraseña.

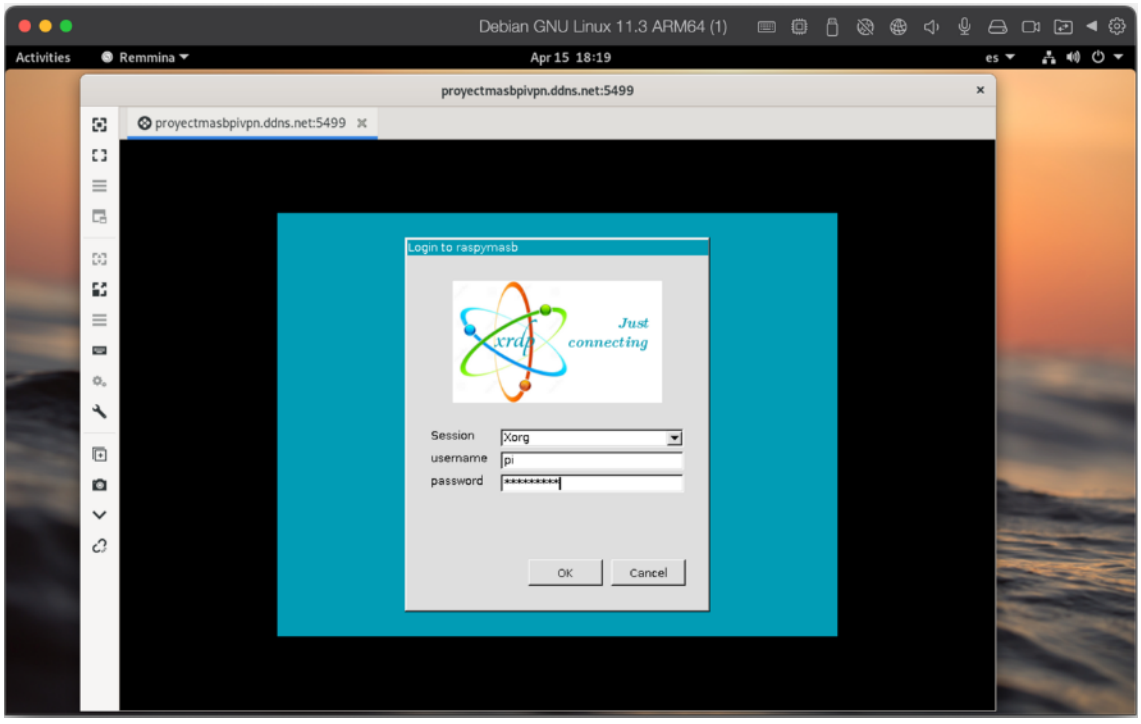
En el apartado Resolution, al seleccionar la opción Custom, se podrá indicar la resolución con la que se mostrará el escritorio remoto configurado.

Facilitados los datos, se pulsará sobre Save.

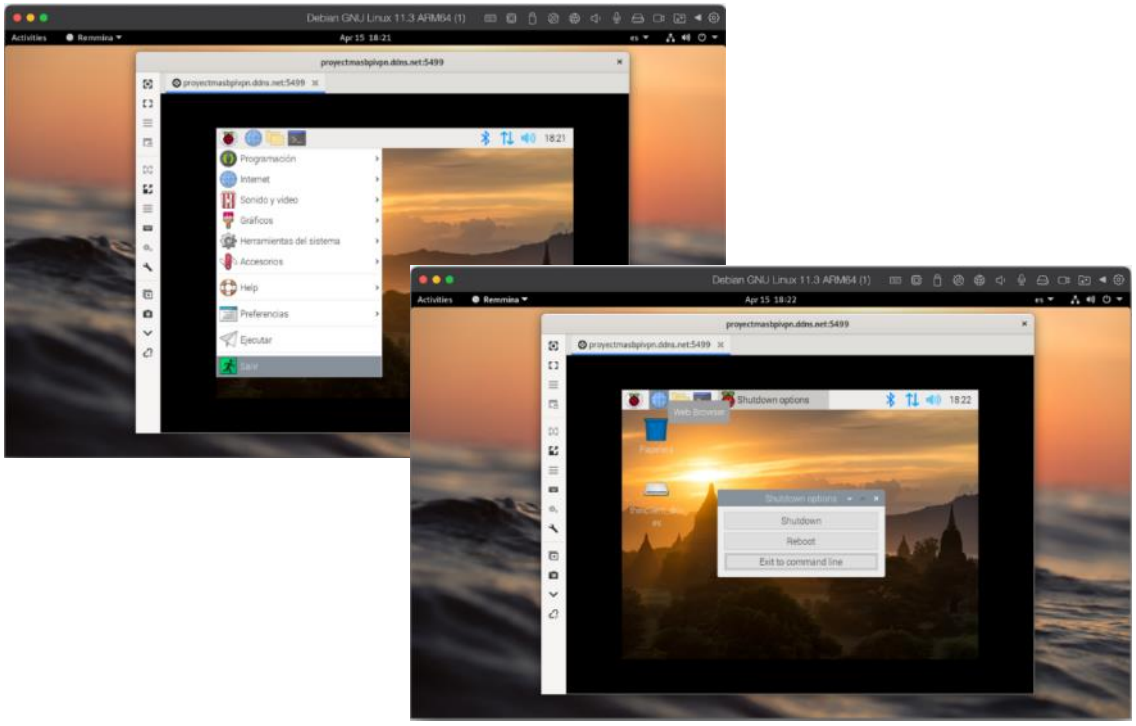
Conexión RDP remmina S.O. Linux.

Con la configuración a la conexión guardada, se podrá hacer doble clic con el botón izquierdo del ratón para abrir y establecer la conexión, en este caso al servidor VPN/WOL.

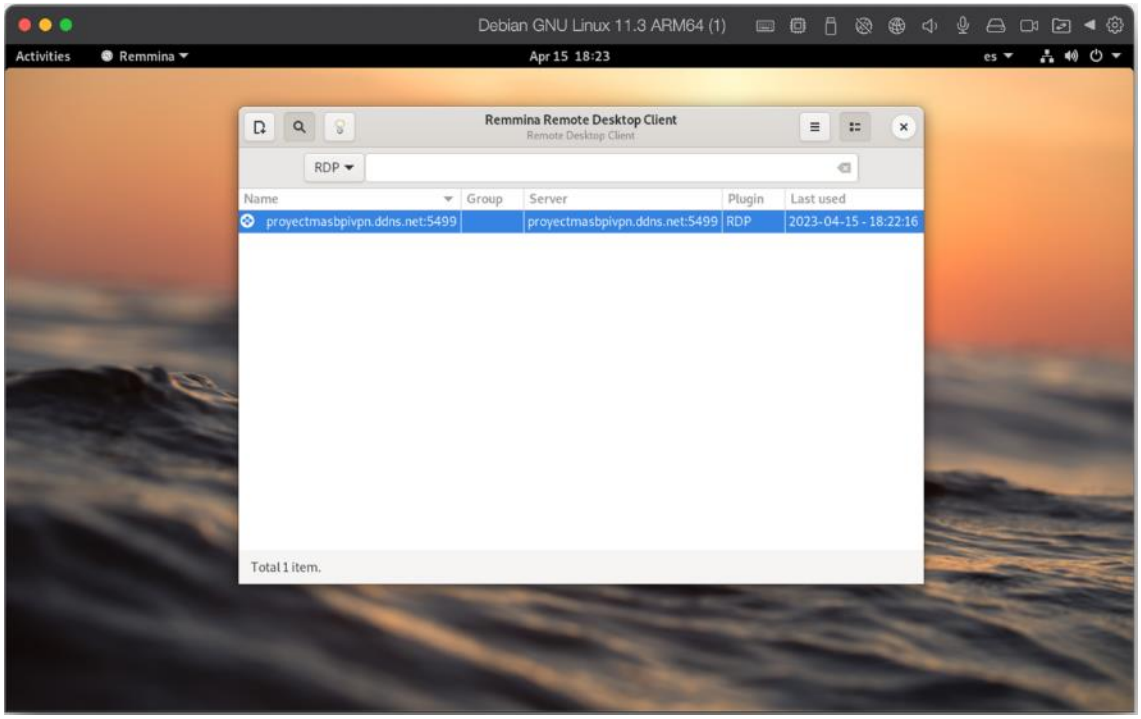




Al no haber facilitado la contraseña, se nos solicita en la ventana de la captura superior, al facilitarse la contraseña, se finaliza la autenticación y se establece la conexión tras pulsar sobre el botón OK.



Como se puede observar en las ventanas de las capturas superiores, se podrá realizar las tareas administrativas necesarias y posteriormente se podrá desconectar del servidor VPN/WOL, que en este ejemplo correspondiente a la Raspberry Pi.

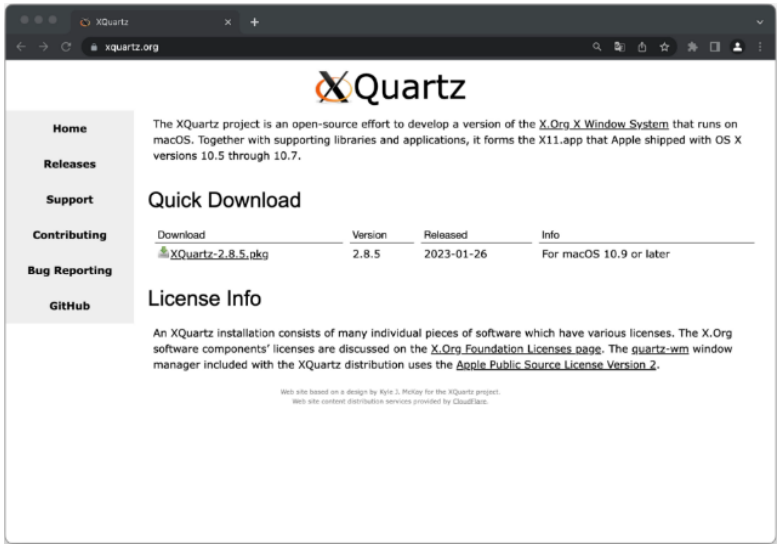


Instalación y configuración aplicación XQuartz en S.O. macOS.

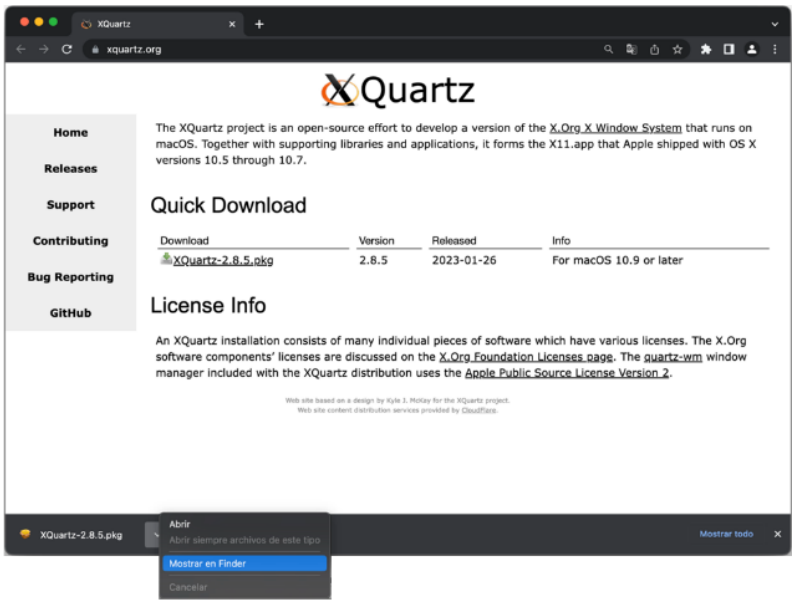
Se ha comprobado que teniendo la aplicación instalada XQuartz y aun sin estar iniciada ni configurada, a la hora de realizar la conexión SSH con la opción -X, opción que habilita la redirección de las X, la aplicación XQuartz se inicia y muestra la aplicación grafica del servidor VPN/WOL en el escritorio del equipo con S.O. macOS.

Habrá que dirigirse a la WEB oficial de la aplicación.

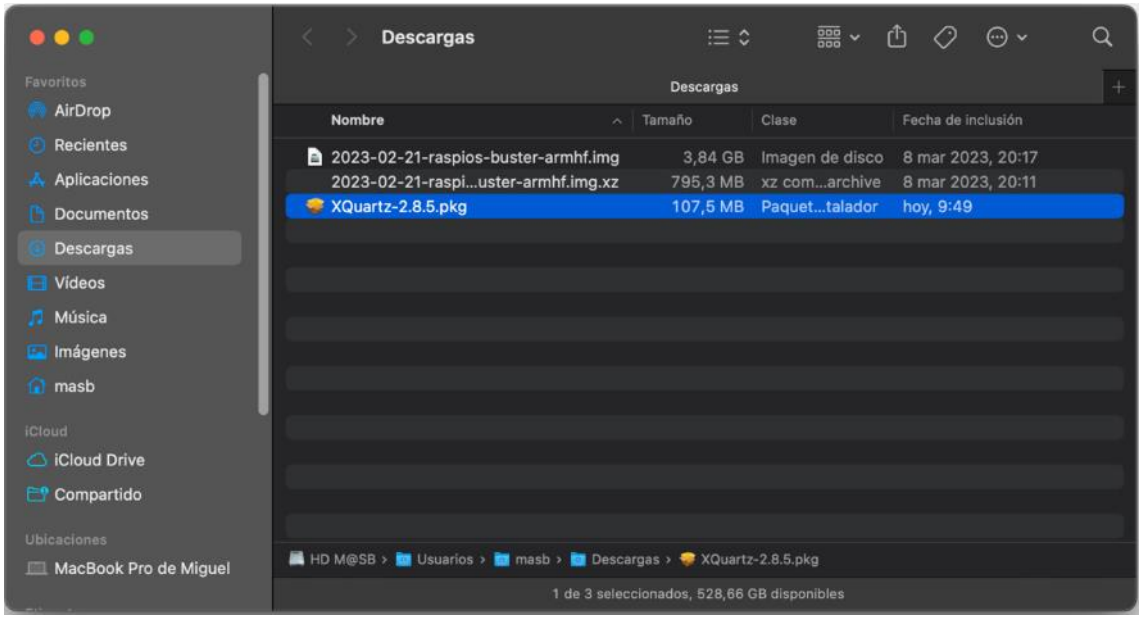
URL. https://www.xquartz.org/



Estando dentro de la WEB, se pulsará sobre el link de descarga del fichero XQuartz-2.8.5.pkg



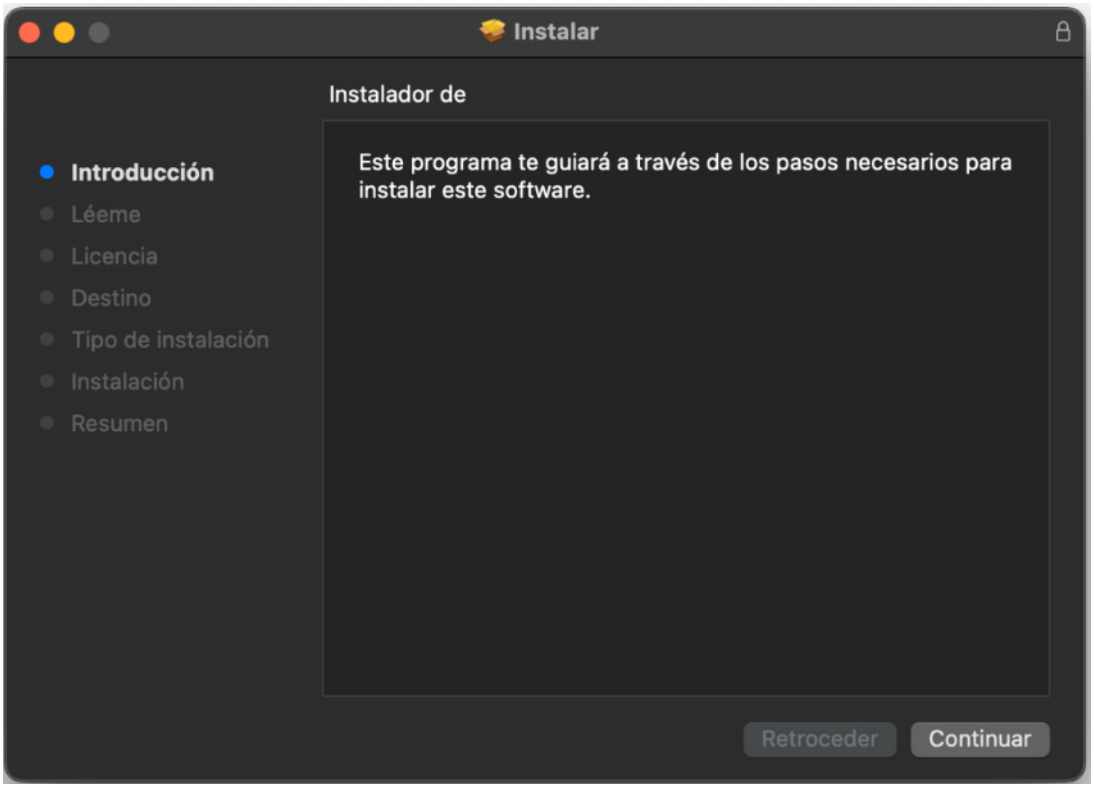
Una vez descargado el fichero, se pulsa sobre la flecha que apunta hacia abajo en la ventana de aviso de la descarga en el navegador, en el menú que aparece, se pulsará sobre Mostrar en Finder.



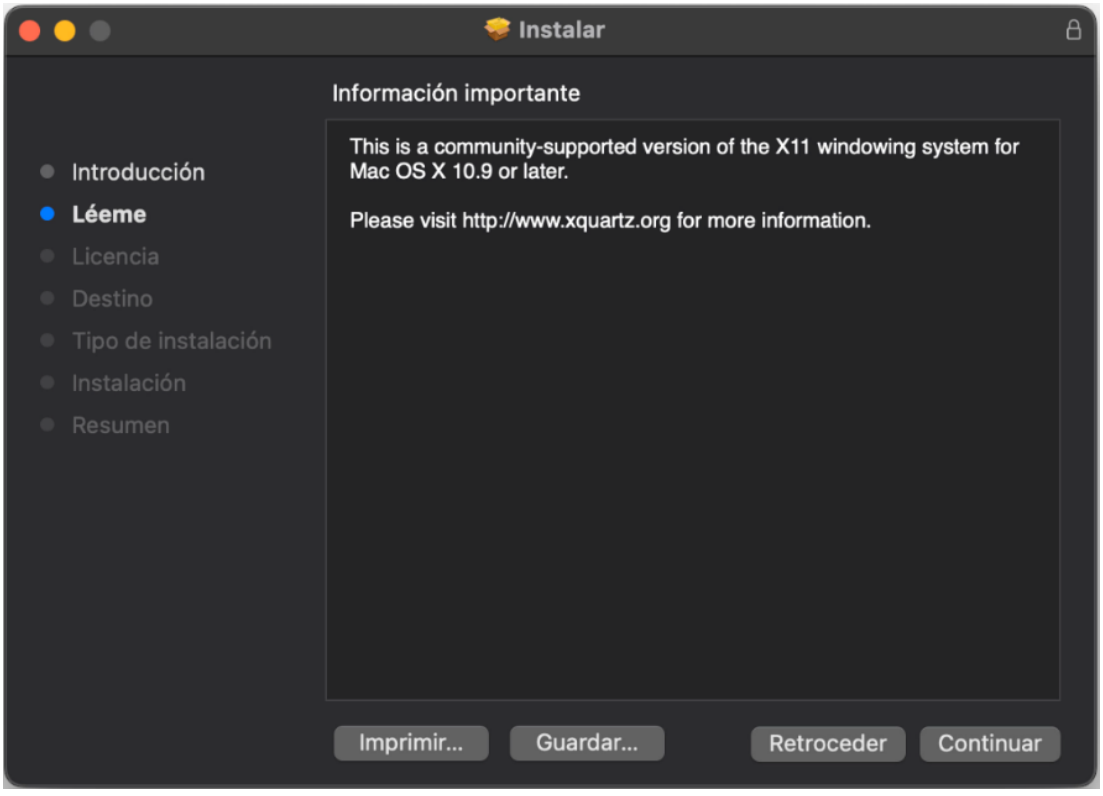
Una vez dentro del Finder, en la carpeta donde se descargó el fichero, siendo la carpeta Descargas, se hará doble clic con el botón izquierdo del ratón sobre el fichero descargado XQuartz-2.8.5.pkg



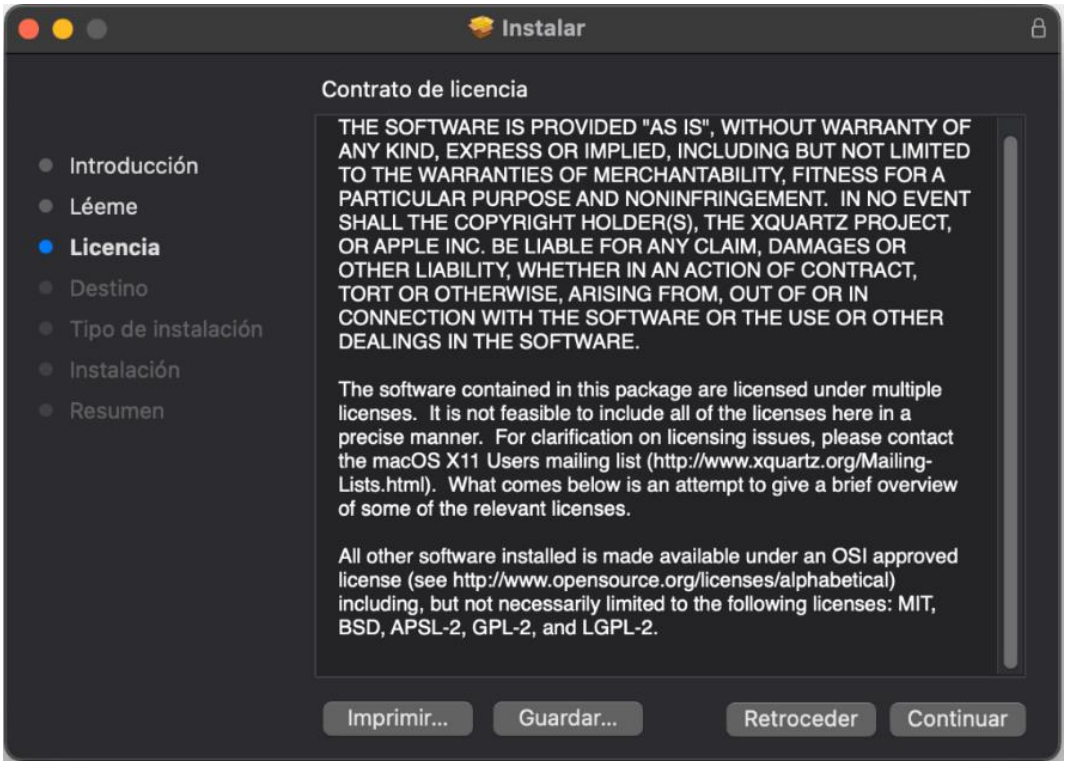
En el cuadro de dialogo que aparece, se pulsará sobre Permitir.



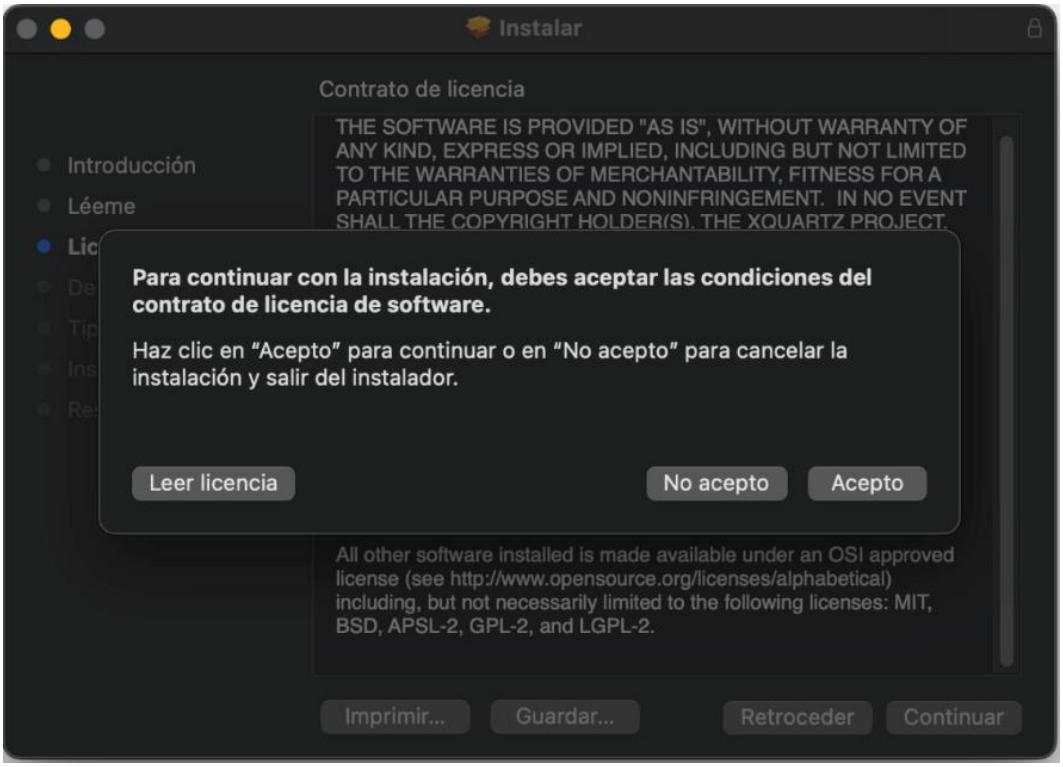
En la siguiente ventana, se tendrá que pulsar en Continuar.



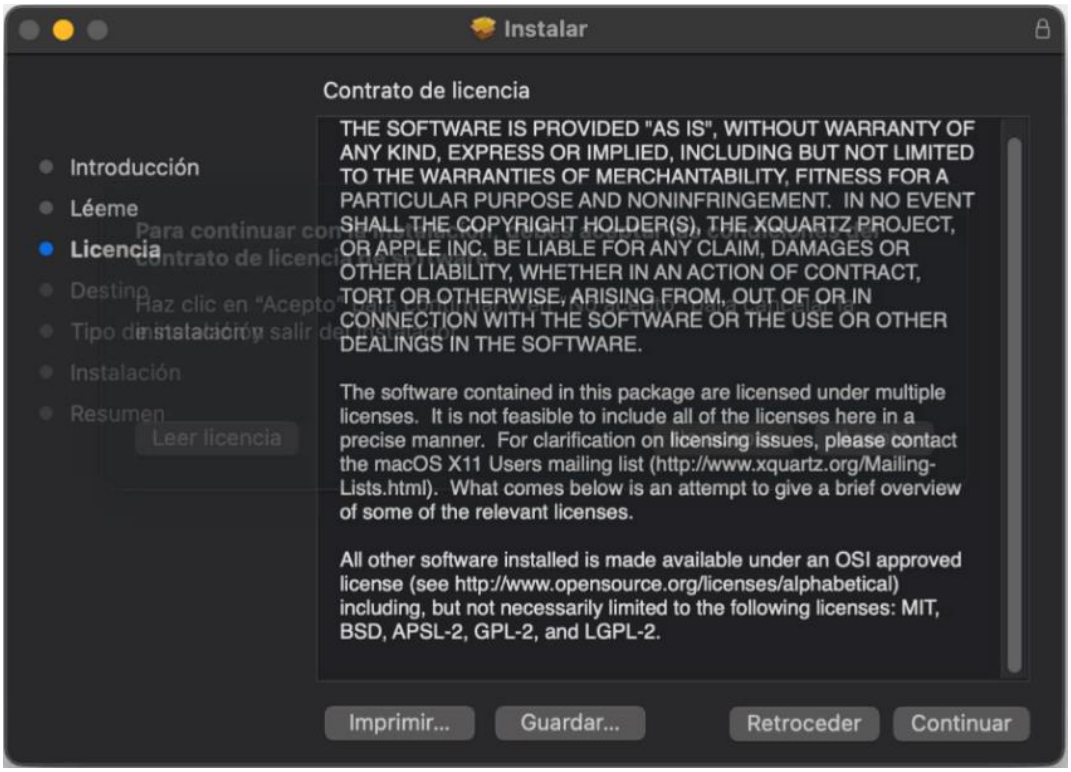
Se pulsará sobre Continuar.



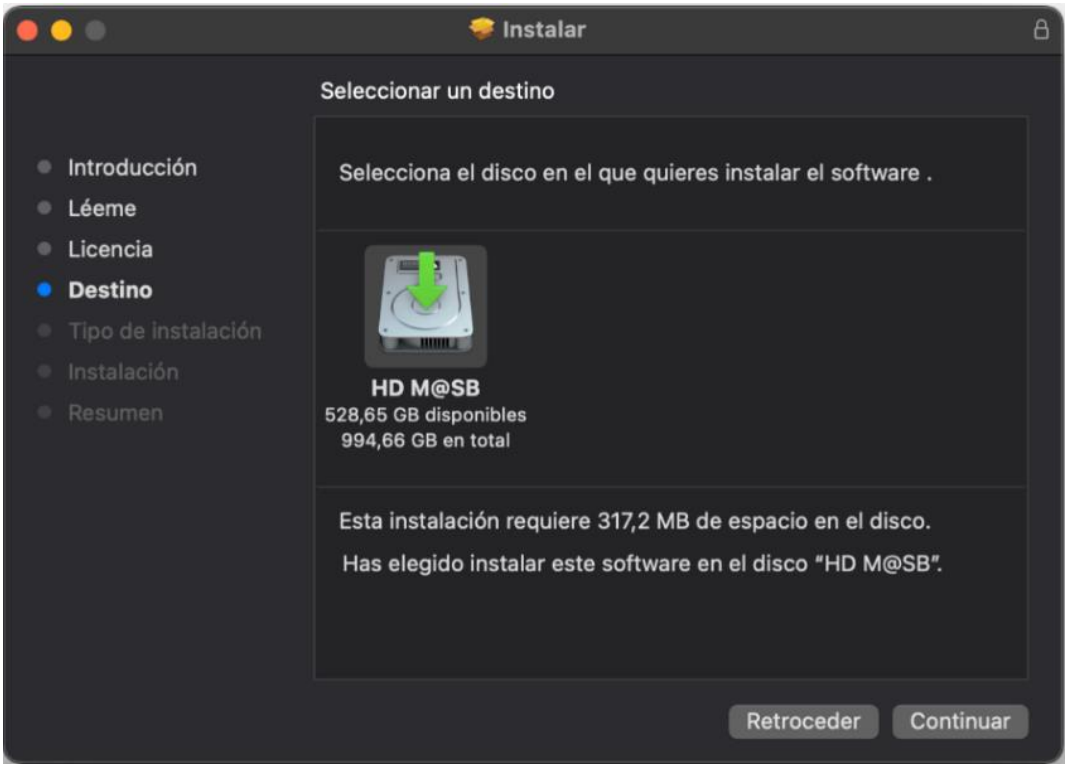
Nuevamente, se pulsará sobre Continuar.



En el cuadro de dialogo que se muestra, habrá que pulsar sobre Acepto, para continuar con la instalación.



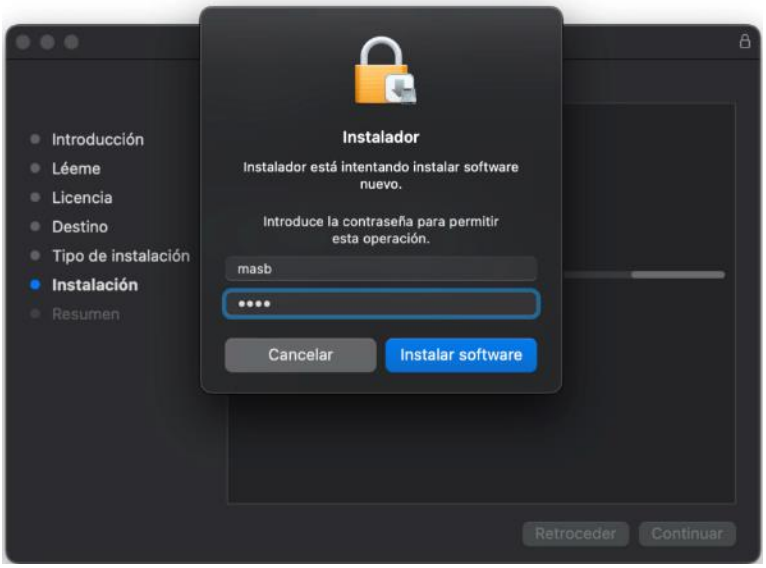
Acto seguido, se pulsará en Continuar.



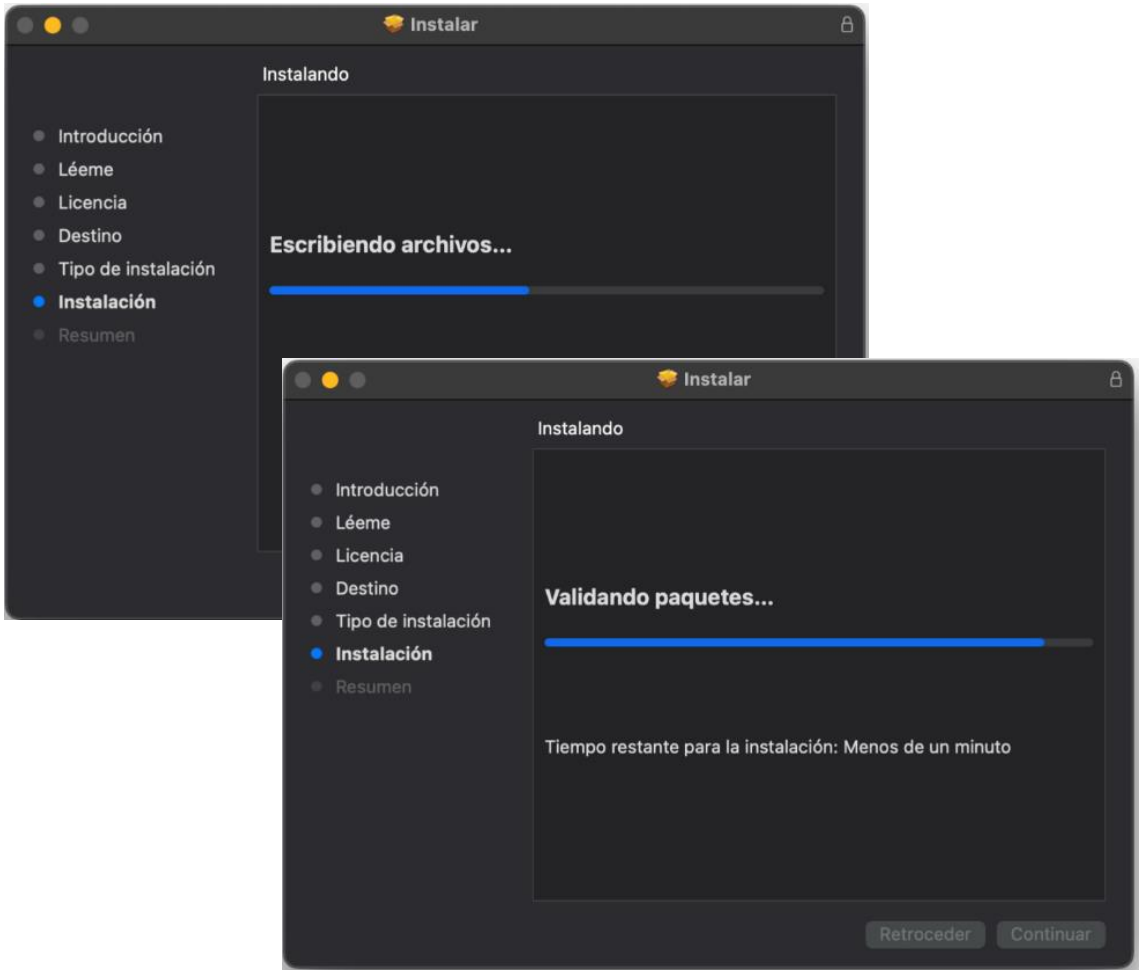
Al encontrarse seleccionado por defecto el disco donde se instalará la aplicación, se pulsará en Continuar.



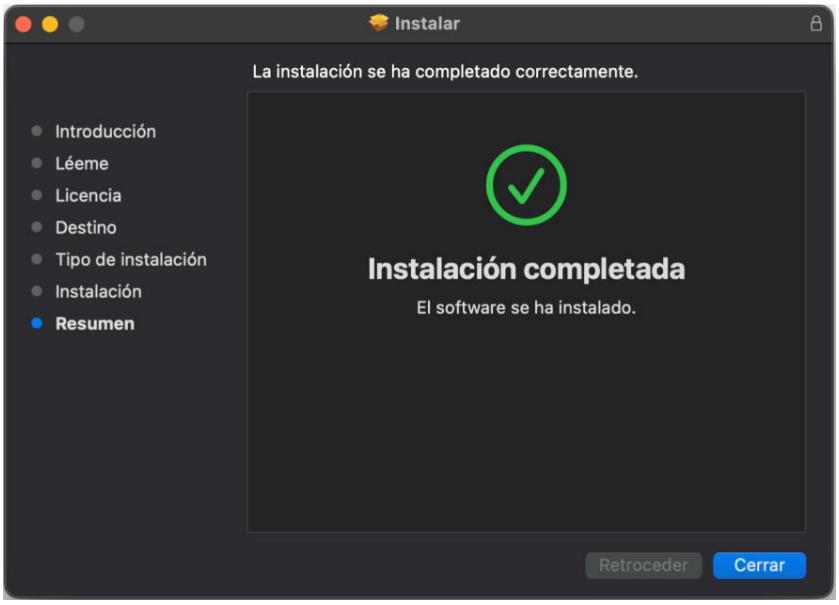
En la ventana de la captura superior, se pulsará en Instalar.



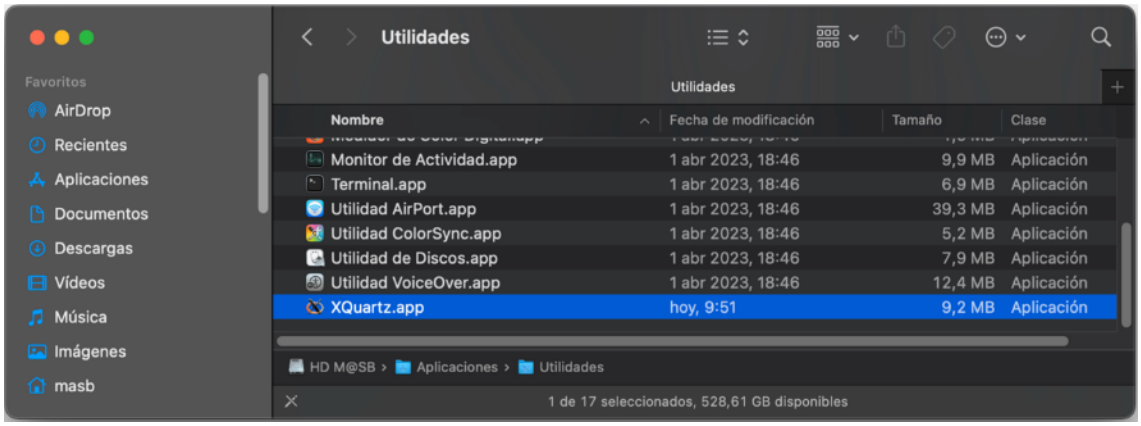
Dependiendo como se tenga configurado el S.O., puede que aparezca una ventana solicitando credenciales para poder realizar la instalación, teniendo que autenticarse, habrá que introducir un usuario y su contraseña, el cual, disponga de permisos para poder instalar aplicaciones, tras proporcionar las credenciales se pulsará sobre Instalar software.



Comenzando el proceso de instalación.



Terminada la instalación, se pulsará sobre Cerrar.



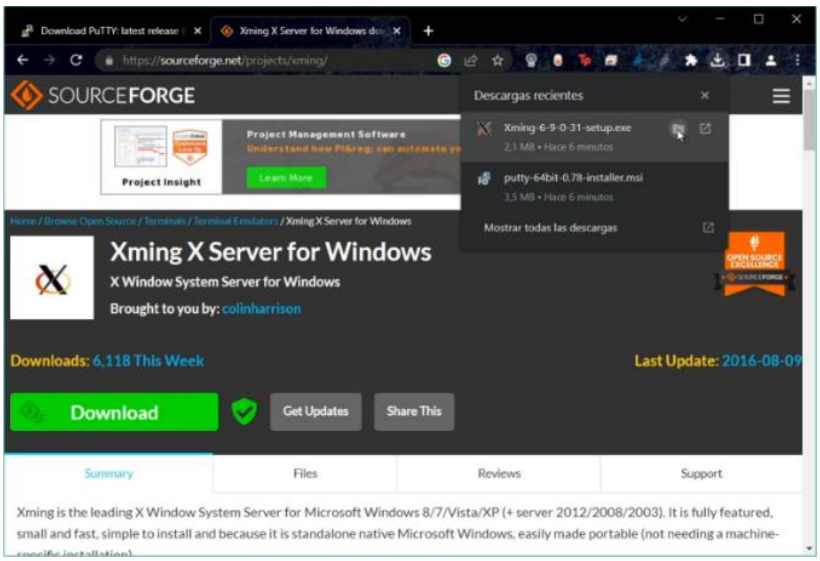
Como se puede observar en la ventana de la captura superior, se habrá instalado la aplicación XQuartz.app en la ubicación / Aplicaciones / Utilidades.

Por las pruebas realizadas, no es necesario tener la aplicación iniciada ni configurarla para que funcione la redirección X a través de SSH, al ejecutar una aplicación X en el terminal remoto estando conectado vía SSH, la aplicación XQuartz en todo momento se inicia y se ejecuta la aplicación gráfica remota en el escritorio del equipo con S.O. macOS.

Descarga e instalación aplicación Xming en S.O. Windows.

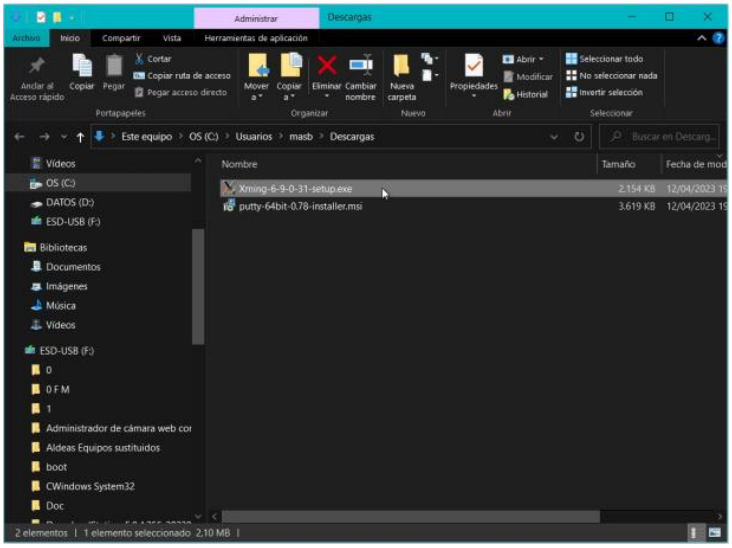
Descarga en S.O. Windows.

Xming, implementación portátil del sistema de ventanas X para sistemas operativos Microsoft.



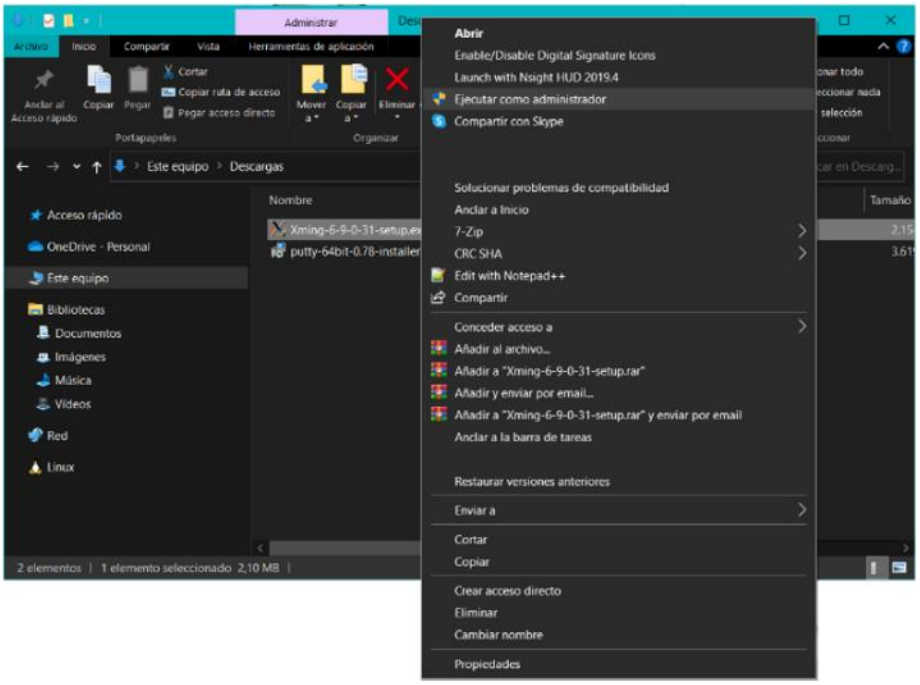
Para descargar Xming, se podrá acceder a la WEB.
URL. https://sourceforge.net/projects/xming/

Dentro de la WEB indicada, se pulsará el botón Download.



Dependiendo como se encuentre configurado el S.O., puede que la descarga se realice en otra carpeta, en este caso, la descarga se realiza en la carpeta Descargas, fichero Xming-6-9-0-31-setup.exe

Instalación en S.O. Windows.



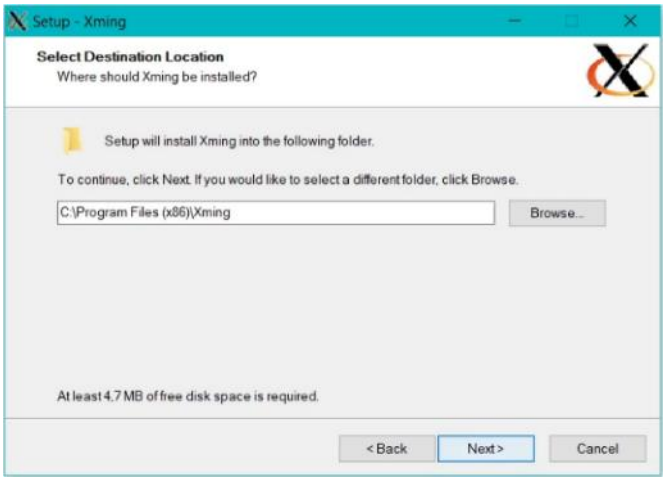
Terminada la descarga y con el fichero en cuestión en la carpeta Descargas, se pulsará con el botón derecho del ratón sobre el fichero Xming-6-9-0-31-setup.exe, en el menú que aparece, se pulsará sobre Ejecutar como administrador.

Si se muestra la ventana Control de cuentas de usuario, se pulsará Sí.

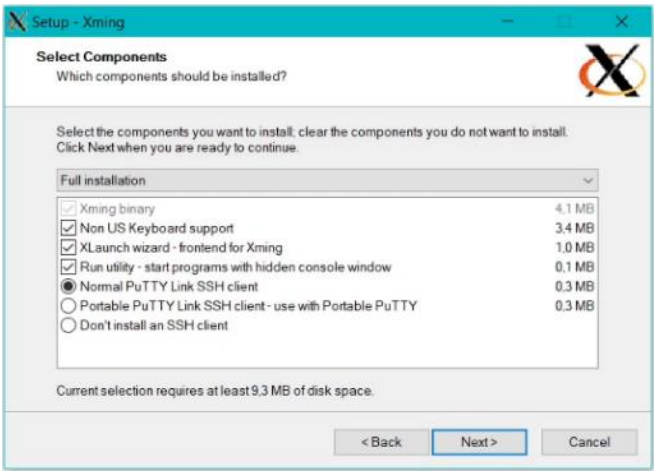
En el caso de aparecer la ventana Advertencia de seguridad de Abrir archivo, se pulsará sobre Ejecutar.



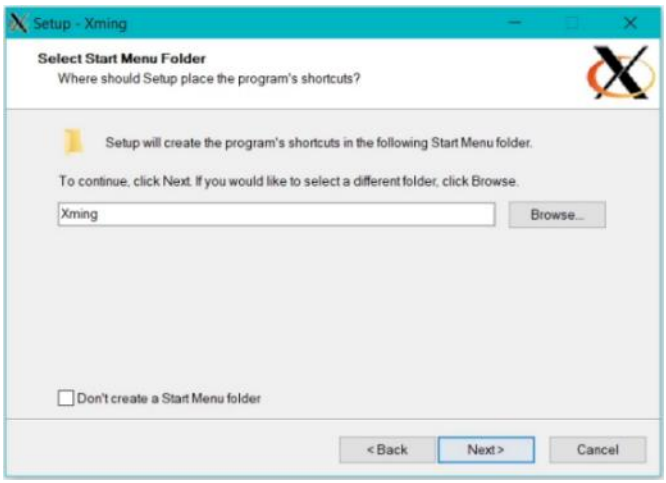
Habrá que pulsar Next para comenzar la instalación.



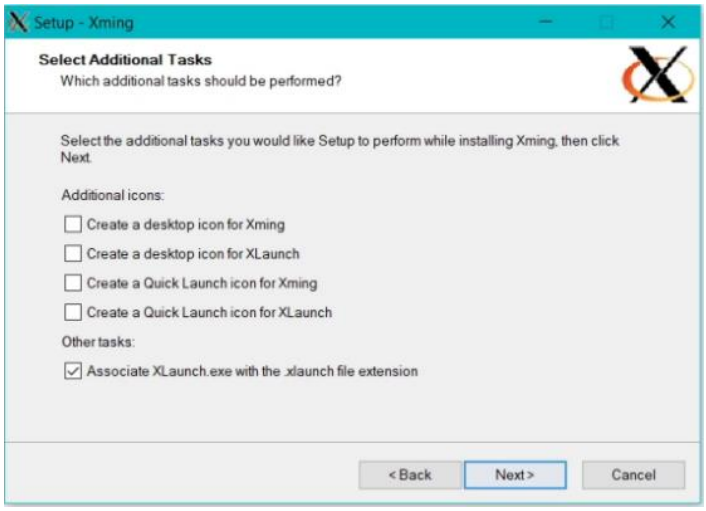
Se podrá dejar el directorio de instalación por defecto, (C:\Program Files (x86)\Xming) y se pulsará Next.



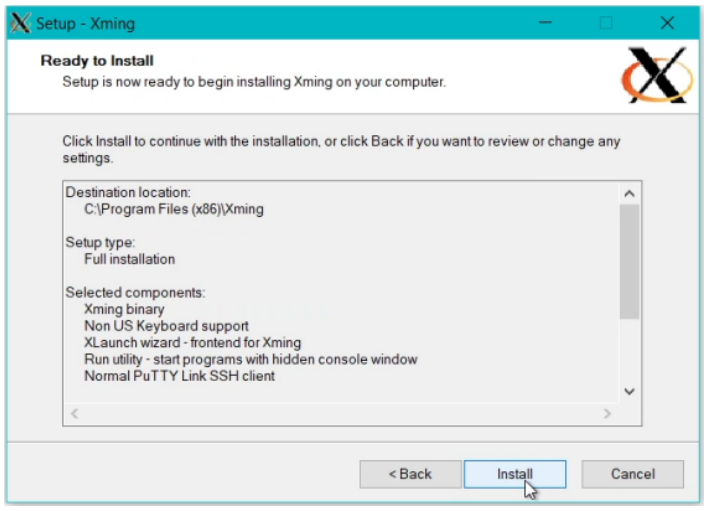
No se realiza ninguna modificación en las opciones de instalación, pulsando en Next.



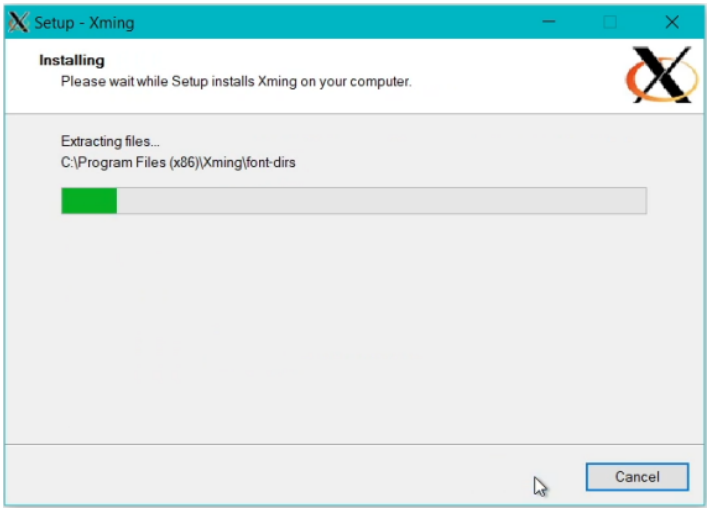
Se pulsará Next.

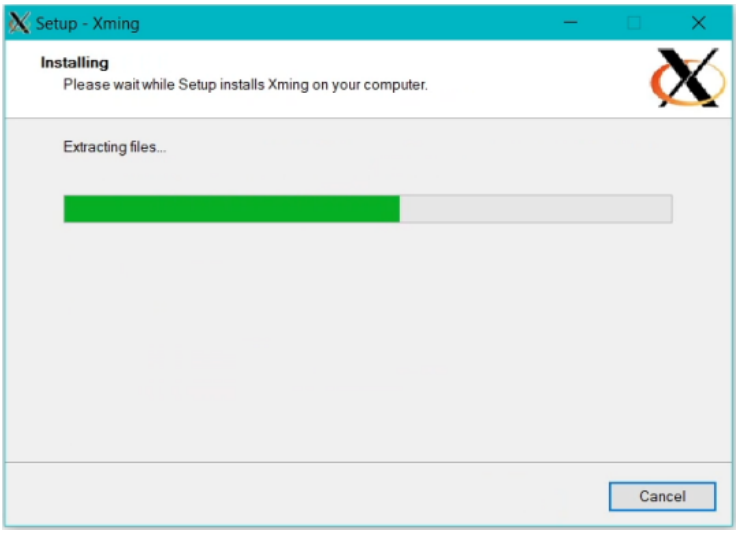


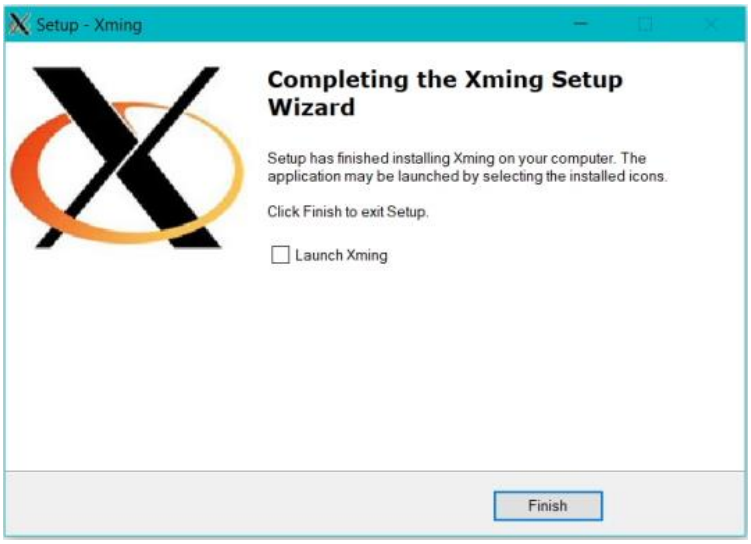
Se dejan las opciones por defecto y se pulsa sobre Next.



Habrá que pulsar Install para comenzar la instalación.

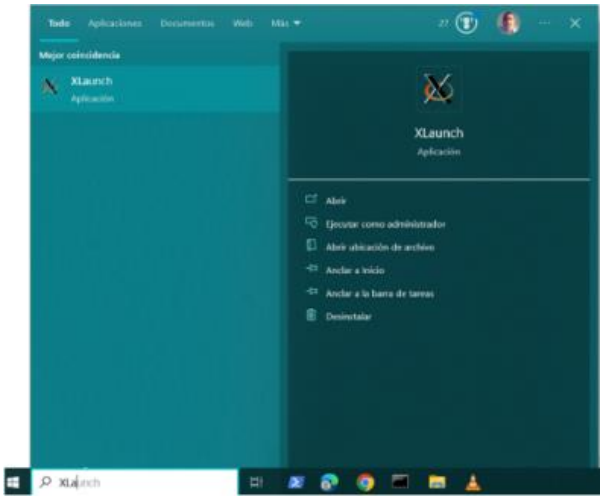




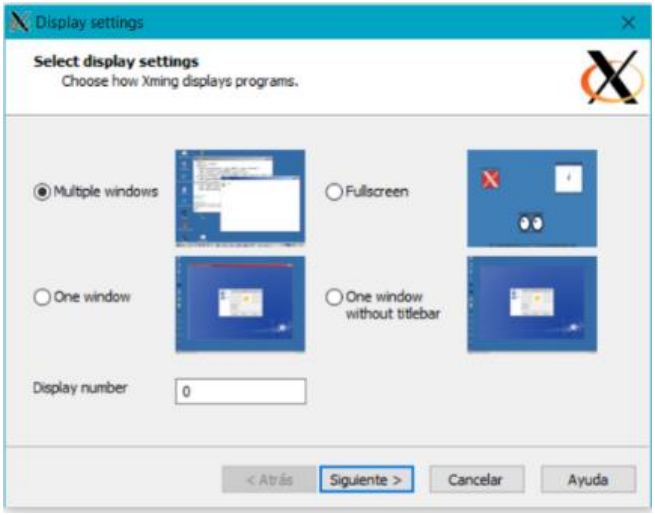


Terminada la instalación, se pulsará Finish.

Configuración aplicación Xming en S.O. Windows.

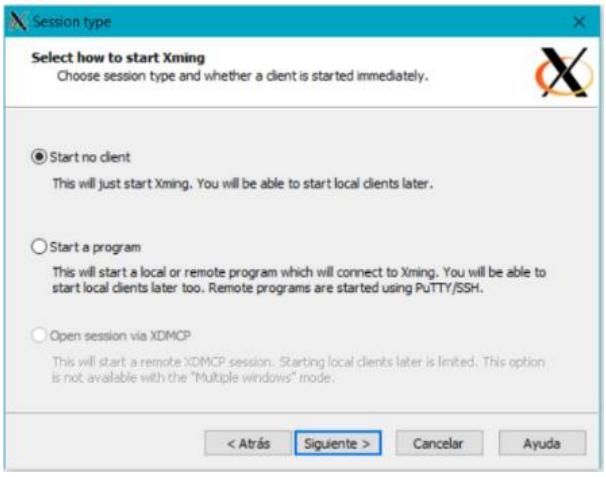


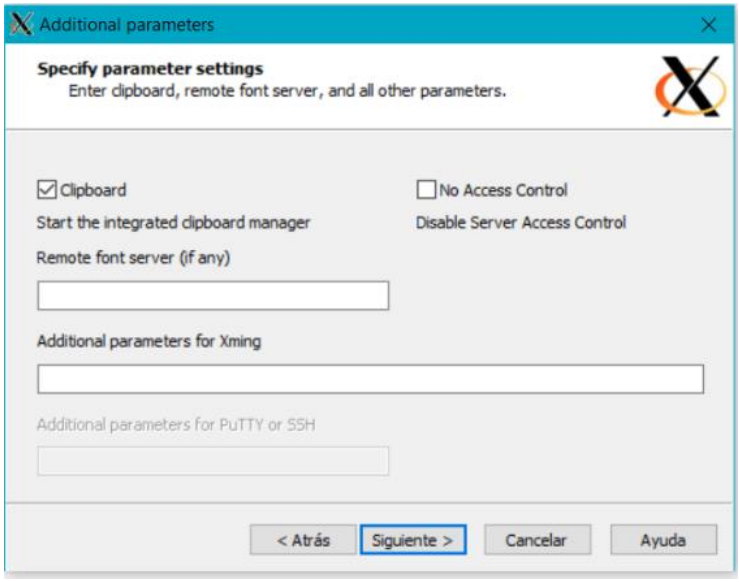
Para realizar la configuración de la aplicación Xming, se localizará la aplicación XLaunch, escribiendo en el cuadro de búsqueda inferior izquierdo XLaunch.



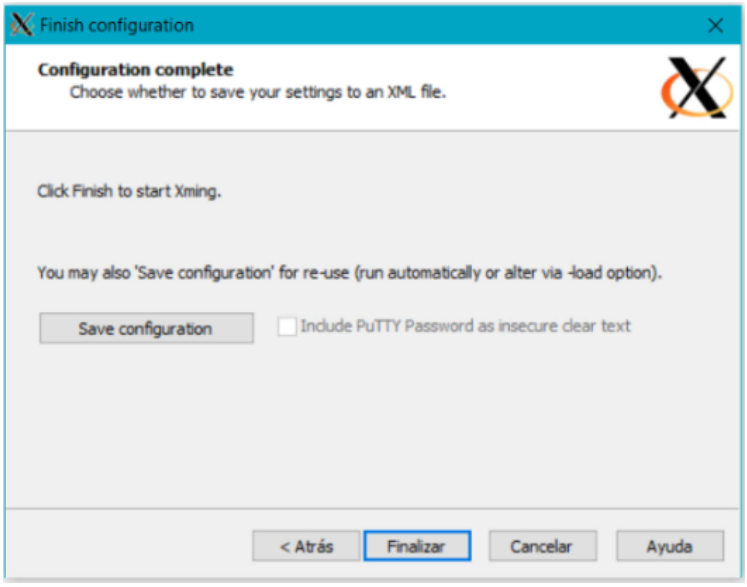
Al hacer clic con el botón izquierdo del ratón sobre XLaunch para abrir la aplicación, aparece el asistente de configuración, en las pruebas realizadas, se dejan las opciones por defecto y se pulsa Siguiente.

Se pulsará Siguiente, sin realizar ninguna modificación para continuar.



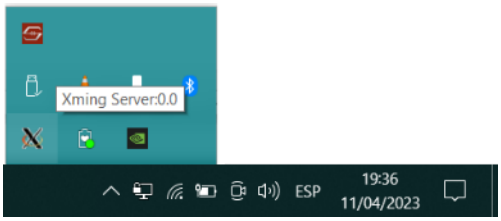


En la nueva ventana que aparece del asistente, no se hará ninguna modificación y se pulsará Siguiente para continuar.



Finalizada la configuración, se pulsa sobre Finalizar.

En el área de notificaciones de la barra de tareas, parte inferior derecha, queda la aplicación en ejecución, si tras algún reinicio o cierre de sesión no se ejecuta, al intentar traer la aplicación grafica en la conexión remota mediante SSH, aparecerá un mensaje de error, teniendo nuevamente que lanzar la aplicación XLaunch.

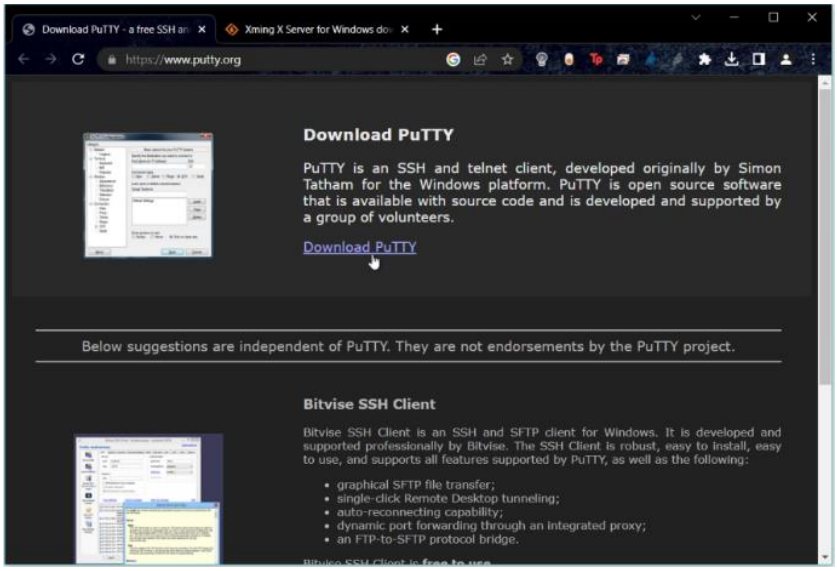


Descarga e Instalación PuTTY en S.O. Windows.

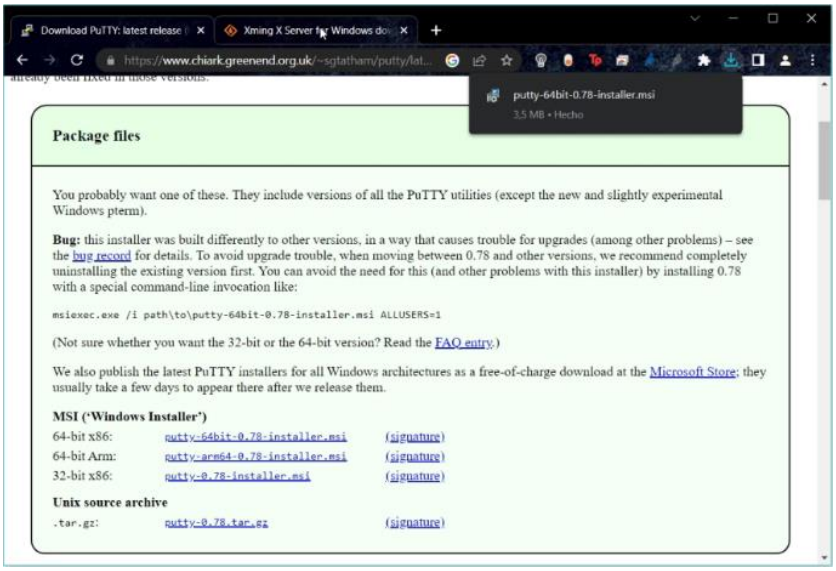
Descarga en S.O. Windows.

Se accederá a la WEB oficial de PuTTY.

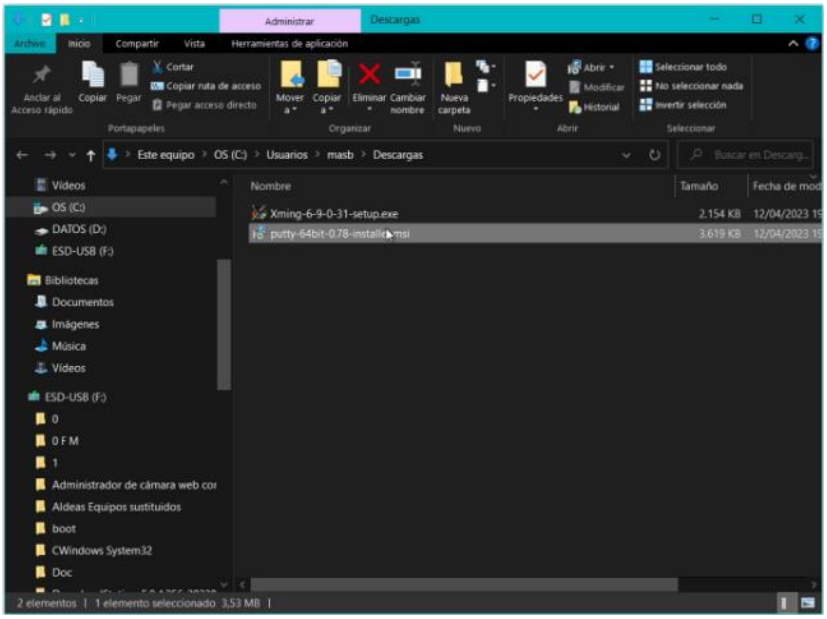
URL. https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html



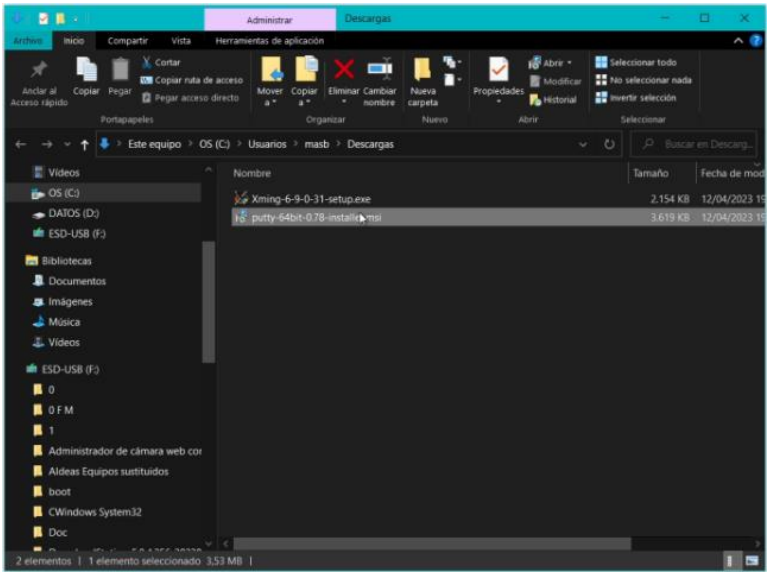
Dentro de la mencionada WEB, se pulsará sobre Download PuTTY (Download PuTTY).



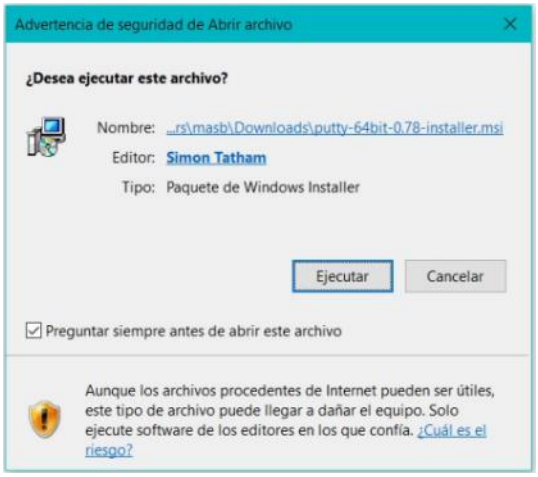
En la nueva ventana que se abre, se deslizará la barra lateral derecha para localizar el fichero putty-64bit-0.78-installer.msi, si se dispone de un cliente con arquitectura de 32 bits, se descargará el fichero putty-0.78-installer.msi, una vez localizado, se pulsará sobre él para descargarlo.


Administrar
Descargas
Archivo
Inicio
Compartir
Vista
Herramientas de aplicación
Anclar al Acceso rápido
Copiar
Pegar
Cortar
Copiar ruta de acceso
Pegar acceso directo
Portapapeles
Mover a
Copiar a
Eliminar
Cambiar nombre
Organizar
Nueva carpeta
Nuevo
Propiedades
Abrir
Modificar
Historial
Abrir
Seleccionar todo
No seleccionar nada
Invertir selección
Seleccionar
Este equipo
OS (C:)
Usuarios
masb
Descargas
Buscar en Descarg...
Videos
OS (C:)
DATOS (D:)
ESD-USB (F:)
Bibliotecas
Documentos
Imágenes
Música
Videos
ESD-USB (F:)
0
0 F M
1
Administrador de cámara web cor
Aldeas Equipos sustituidos
boot
CWindows System32
Doc
Nombre
Tamaño
Fecha de mod
Xming-6-9-0-31-setup.exe
2.154 KB
12/04/2023 19
putty-64bit-0.78-installe.msi
3.619 KB
12/04/2023 19
2 elementos | 1 elemento seleccionado 3,53 MB |

Instalación en S.O. Windows.

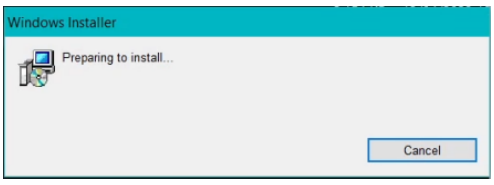


Posteriormente, dentro de la ubicación donde se realizan las descargas, en este caso en la carpeta Descargas, se hará doble clic con el botón izquierdo del ratón sobre el fichero descargado putty-64bit-0.78-installer.msi.

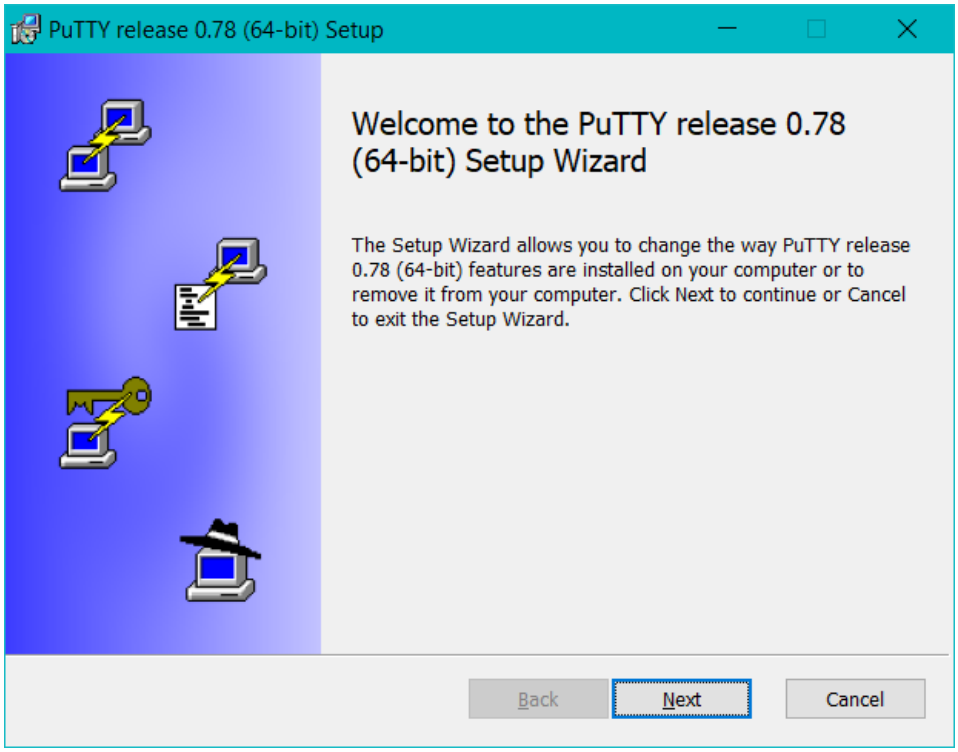


En la ventana Advertencia de seguridad de Abrir archivo, se pulsará sobre Ejecutar.

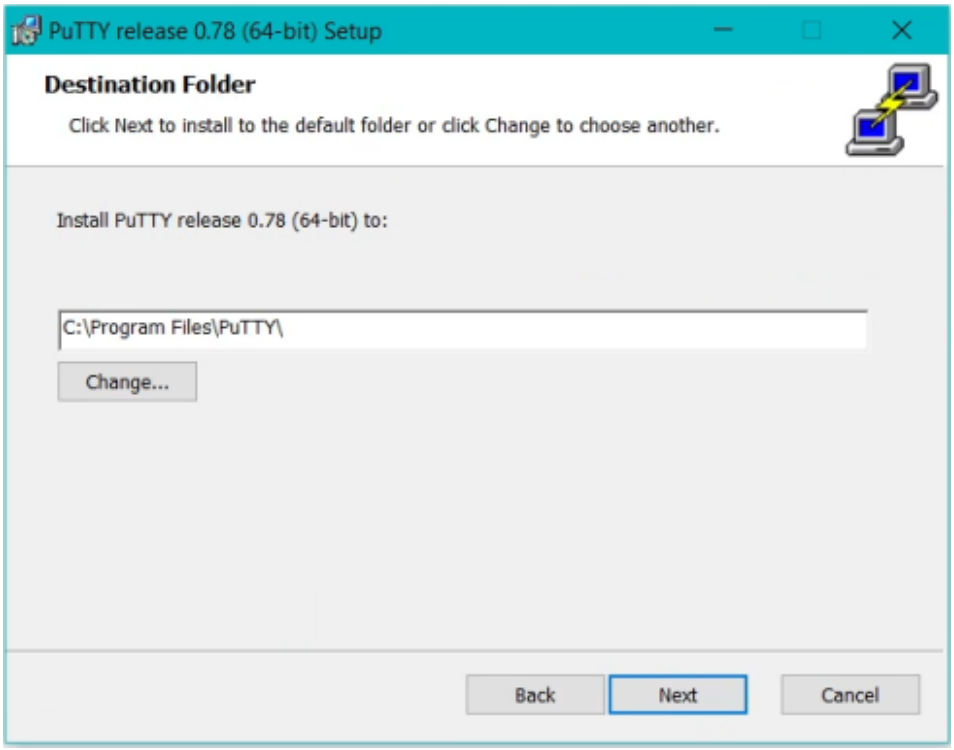
En caso de aparecer la ventana Control de cuentas de usuario, se pulsará sobre Sí.



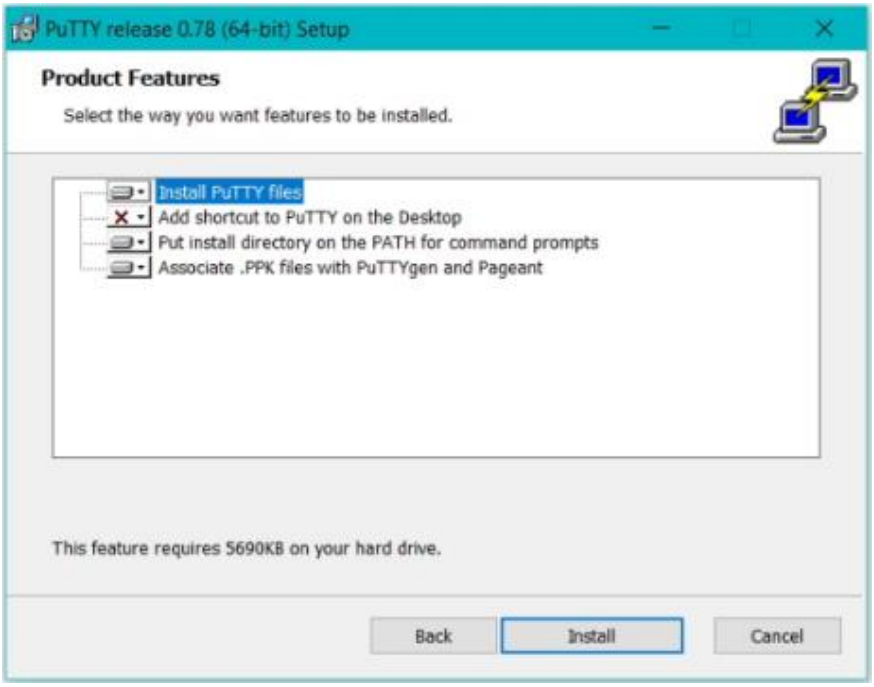
Comenzando la preparación de la instalación.



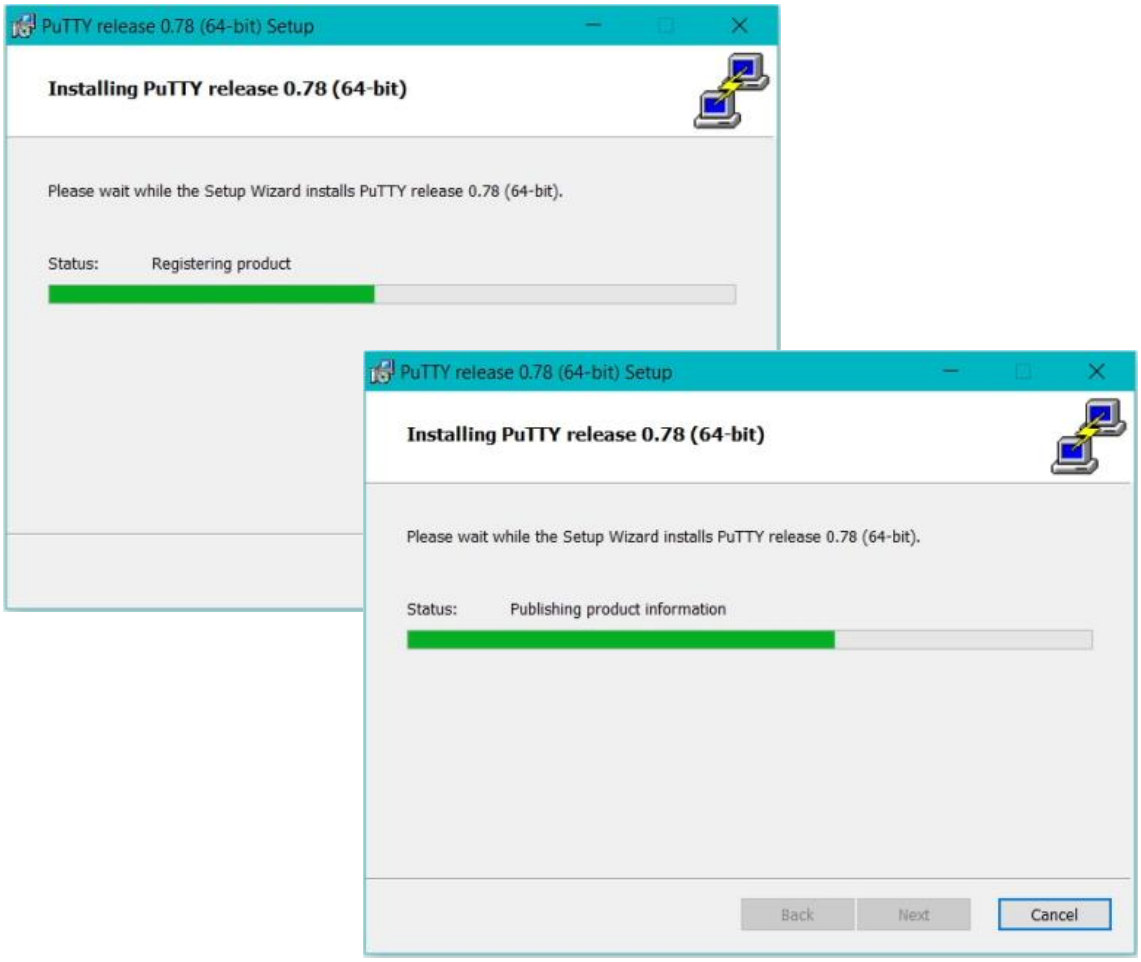
En la ventana de bienvenida, se pulsará Next, para comenzar la instalación.

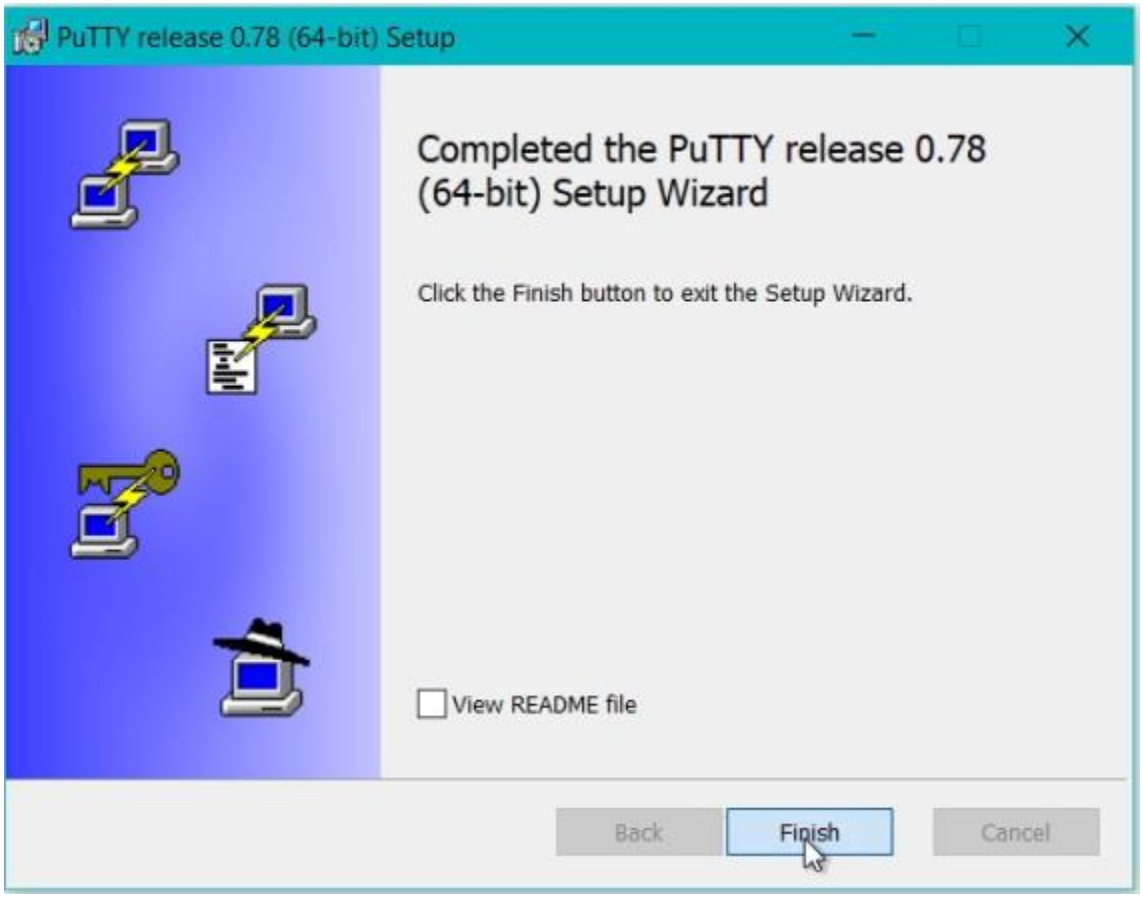


Para este proyecto, se deja el directorio de instalación por defecto (C:\Program Files\PuTTY\), y se pulsa Next.



Habrá que pulsar Install para comenzar la instalación.





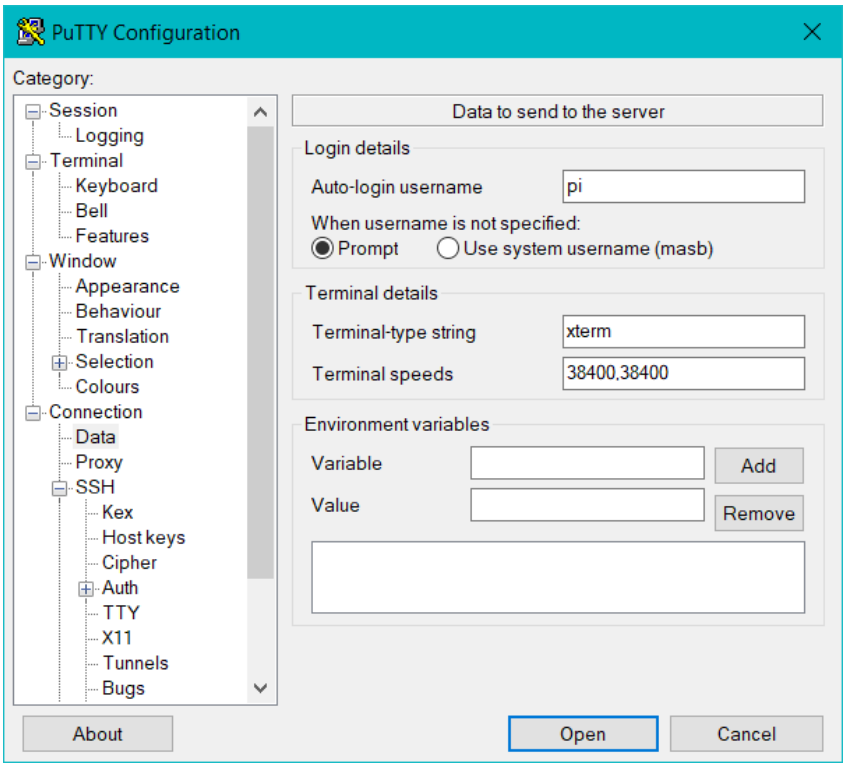
En el caso de encontrarse seleccionada la opción View README file, se desmarcará.

Terminada la instalación, se pulsará Finish.

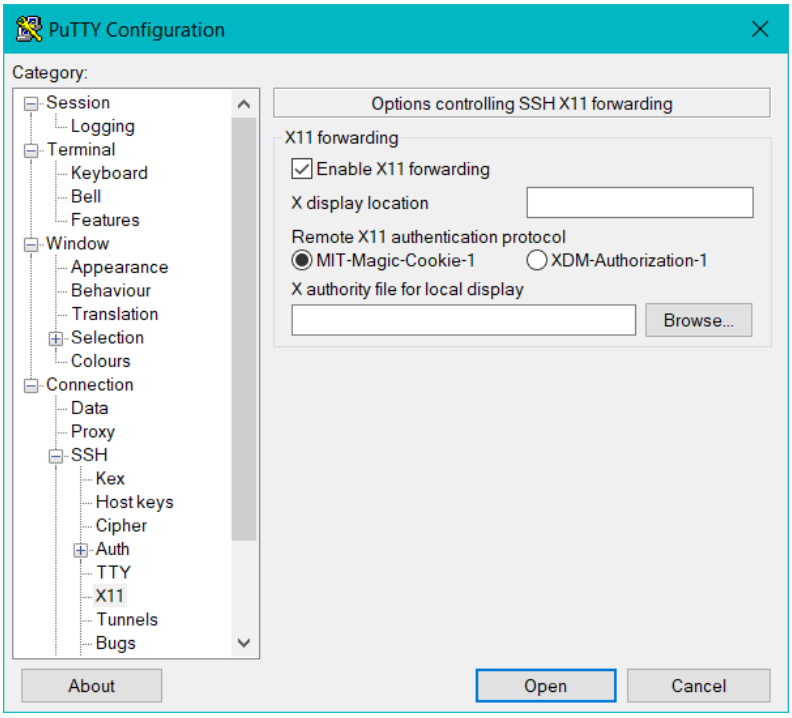
Configuración creación conexión en S.O. Windows aplicación PuTTY.

Una vez instalada y abierta la aplicación PuTTY, para este proyecto se ha realizado una configuración que da mucho juego, puesto que en conjunto con la aplicación Xming, permite de una forma rápida tras guardar la configuración, realizar conexiones por terminal sin tener que estar escribiendo cada vez que se requiera establecer la conexión, el comando dentro de una ventana de Símbolo de sistema en Windows.

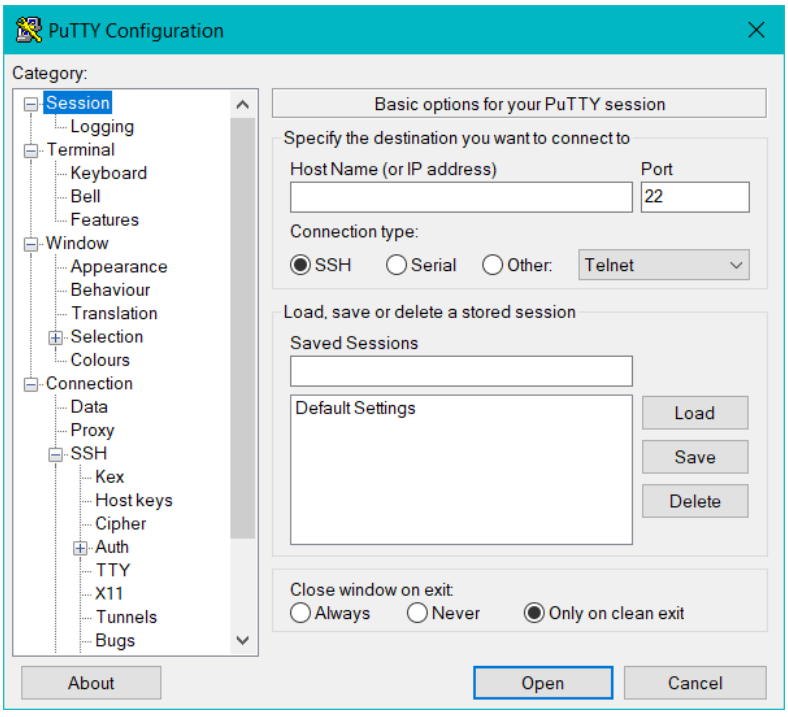
Es necesario tener la aplicación Xming instalada e iniciada, ejecutando la aplicación XLaunch, para que al ejecutar la configuración guardada en PuTTY con la redirección X, la aplicación remota del servidor VPN/WOL, se muestre en el equipo con S.O. Windows.



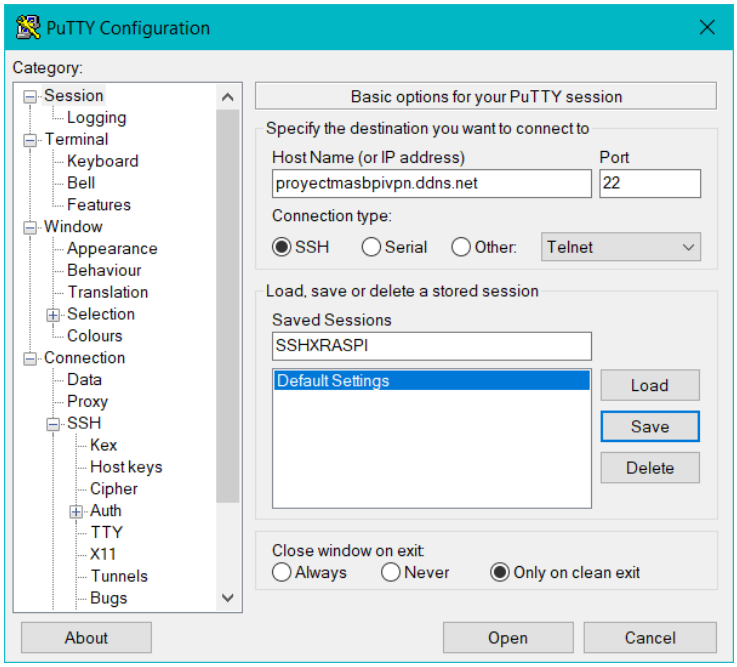
Se indica en este proyecto, como guardar la configuración y realizar una configuración de conexión SSH con la redirección X habilitada, facilitando así al usuario la conexión en la aplicación PuTTY, dentro de la aplicación PuTTY, en el Panel lateral izquierdo, apartado inferior Connection \ Data, habrá que dirigirse en este momento al panel lateral derecho apartado superior Login datails \ Auto-login username, donde se podrá poner el usuario de acceso a la Raspberry Pi, en este ejemplo es el usuario por defecto pi.



Nuevamente, en el panel lateral izquierdo, opción inferior Connection \ SSH \ X11, posteriormente en el panel lateral derecho, apartado X11 forwardind, se marcará el checkbox Enable X11 forwarding, como se puede observar en la ventana de la captura superior.



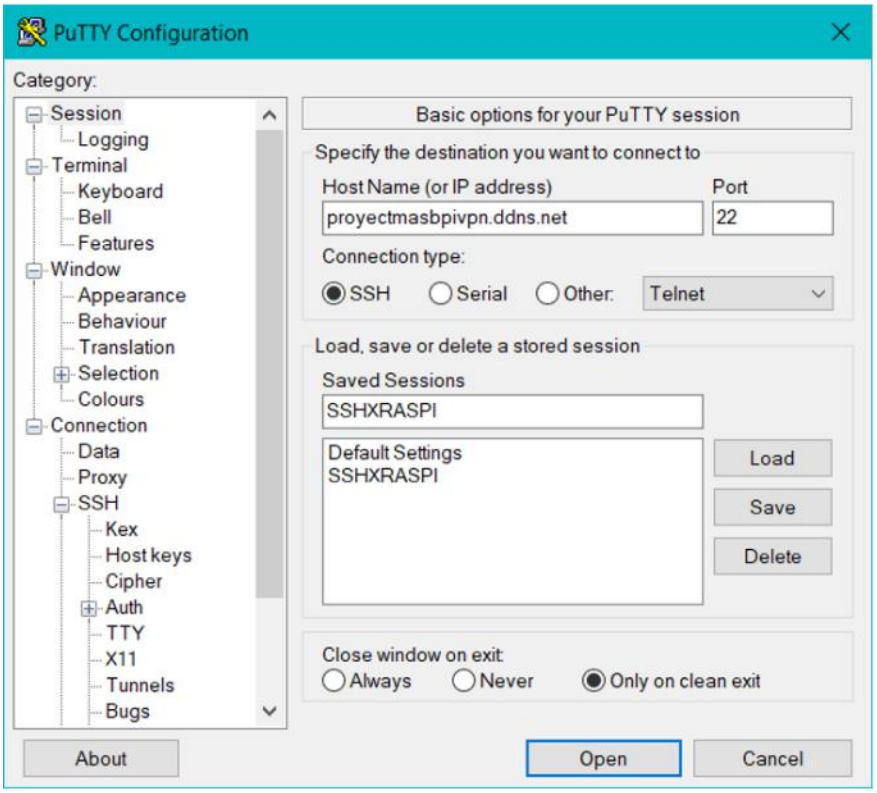
Acto seguido, se pulsará en Session, en el panel lateral izquierdo, opción ubicada en la parte superior.



Para finalizar esta configuración, estando en la opción superior Session del panel izquierdo, en el panel derecho, se escribirán los datos necesarios para poder establecer la conexión.

- Apartado Host Name (or IP address), en este caso, se trata del nombre del dominio o host creado en el proveedor de servicios DDNS. proyectmasbpivpn.ddns.net
- Apartado Port, en caso de no haberlo modificado, se dejará el que se muestra, puerto 22, puerto por defecto para conexiones SSH, en caso de haber modificado las opciones de acceso por SSH, se colocará el puerto que corresponda, teniendo que estar habilitado el puerto en el router y habilitado el tráfico en el cortafuegos del servidor VPN/WOL, el puerto que se utilice para la conexión SSH.

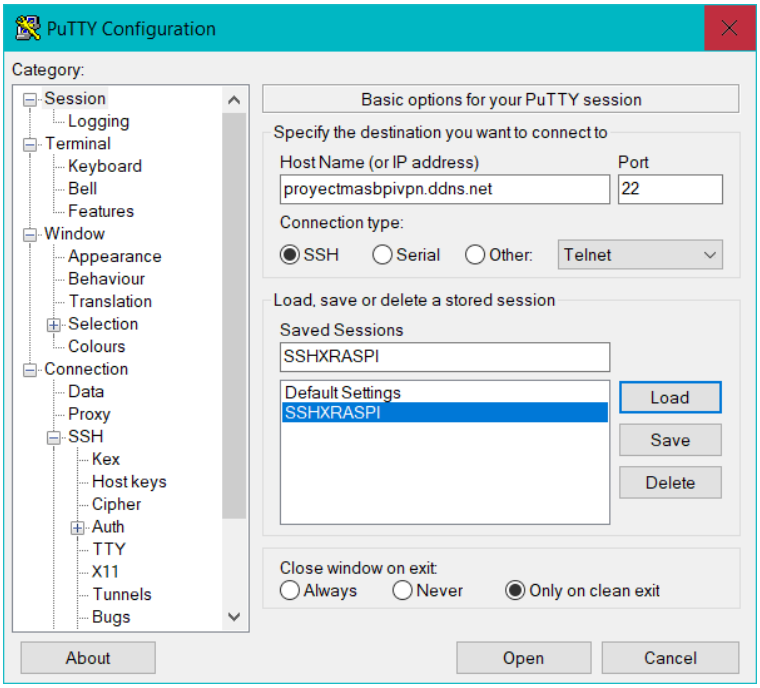
En el apartado Saved Sessions, se escribirá un nombre descriptivo para dejar todas las opciones guardadas dentro de ese nombre de configuración, en este caso se pone como nombre, SSHXRASPI y se pulsa sobre el botón Save.



Como se aprecia en la ventana de la captura superior, la configuración se guarda en el apartado Saved Sessions, hasta aquí, se ha terminado de configurar la conexión en la aplicación PuTTY.

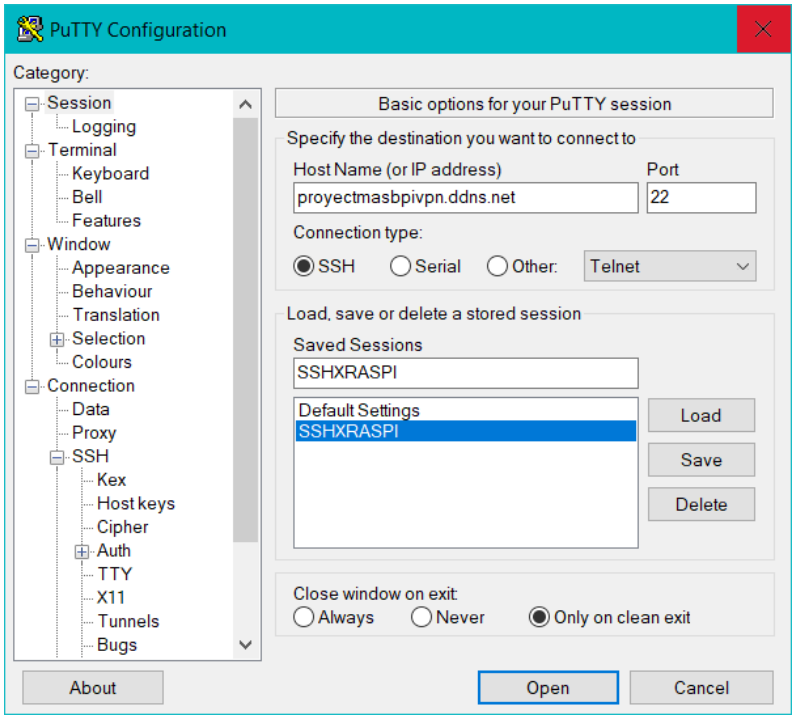
Uso de la conexión remota con PuTTY S.O Windows.

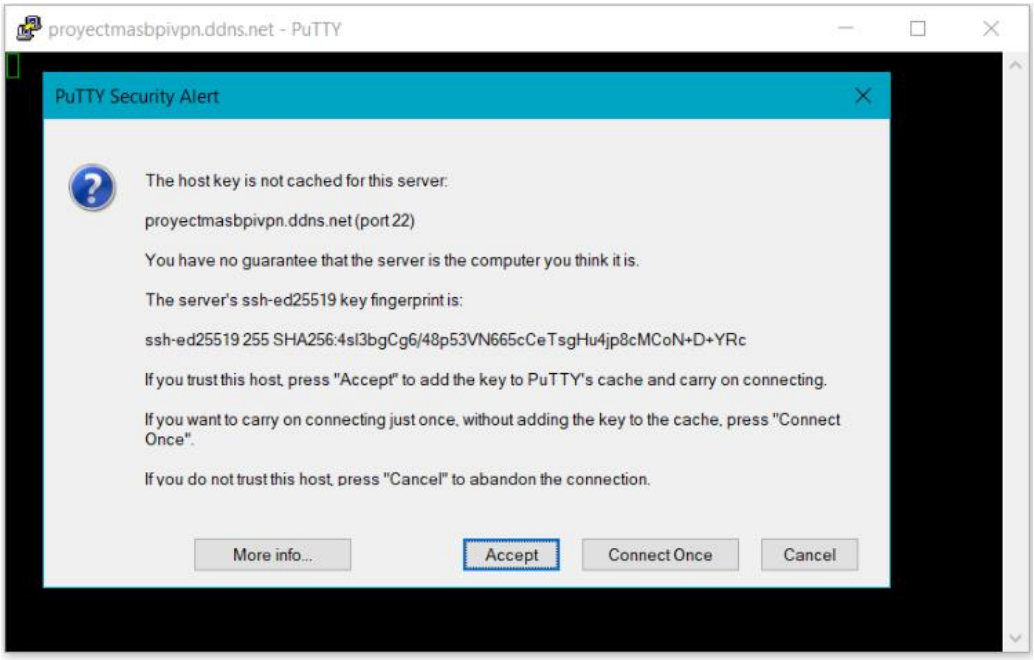
Conexión a través de Terminal.



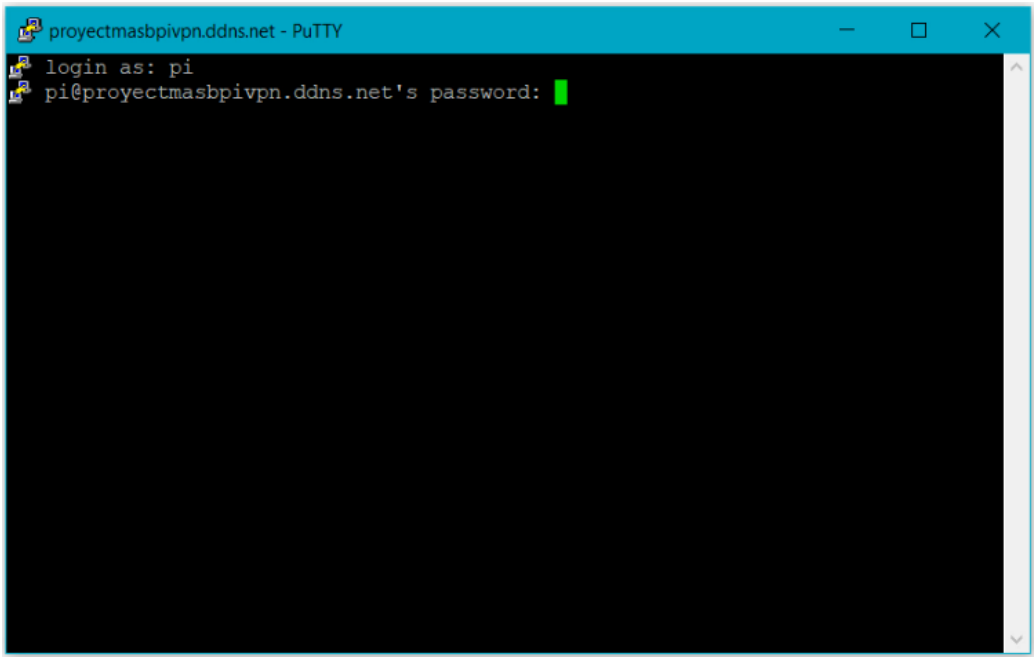
Una vez abierta y dentro de la aplicación PuTTY, se seleccionará la sesión guardada en el apartado Saved Sessions, en este ejemplo, se trata de la configuración con nombre SSHXRASPI, pulsando posteriormente el botón Load, captura superior.

Tras pulsar el botón Load, se cargará automáticamente la configuración de la conexión guardada, pudiendo pulsarse en el botón inferior Open, para establecer la conexión, imagen captura derecha.

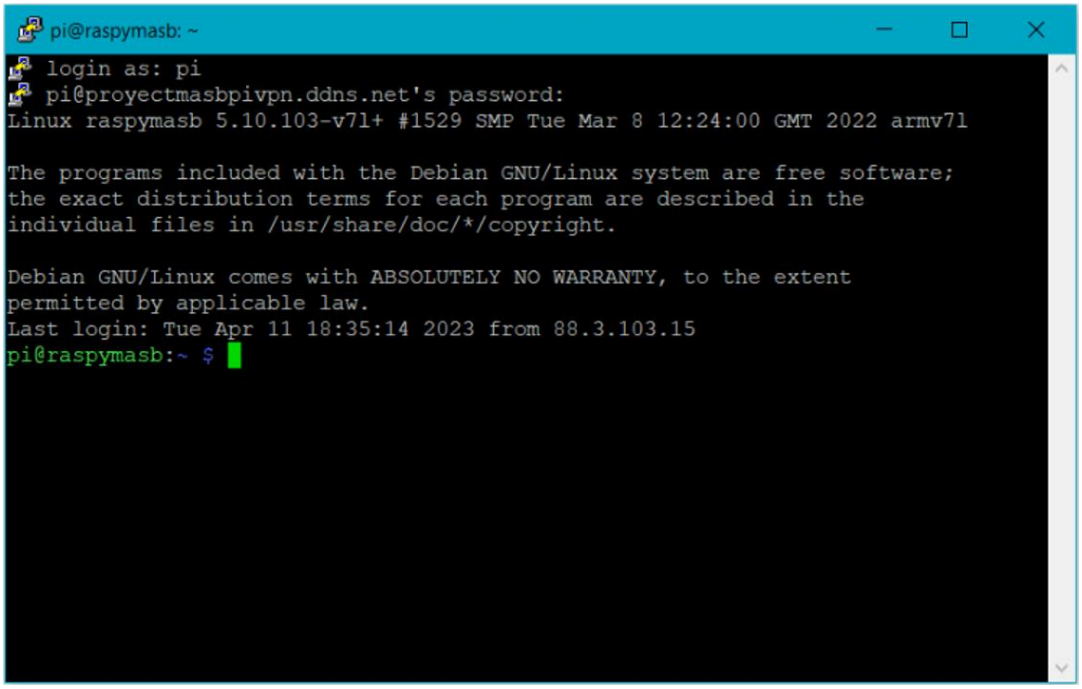




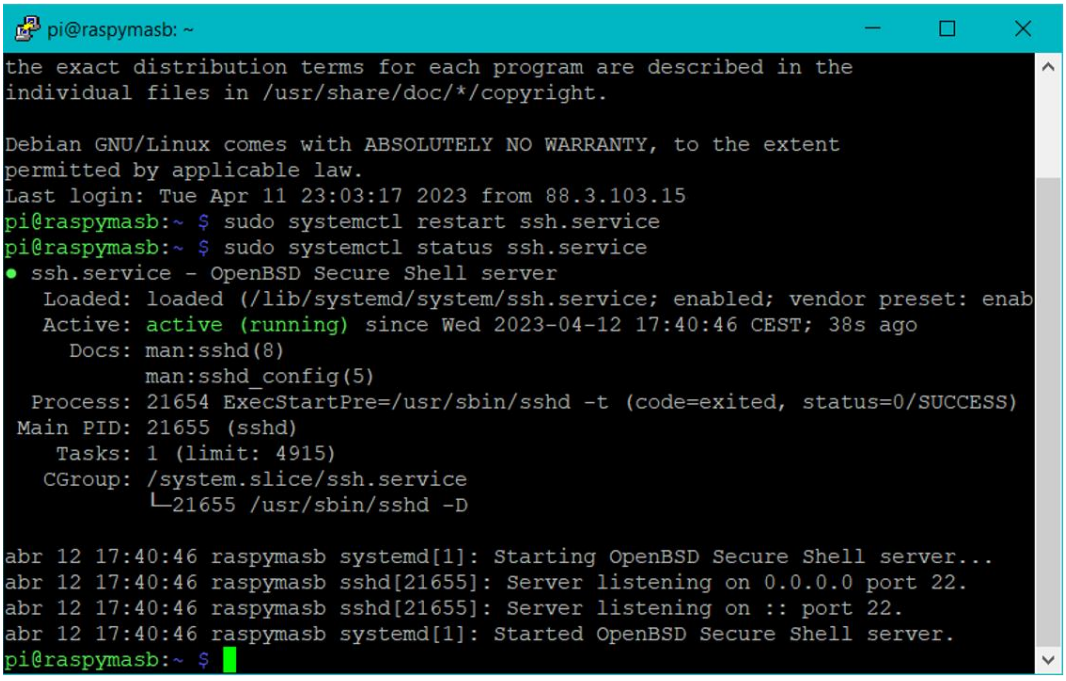
Si como en la captura de la ventana superior, es la primera vez que se establece la conexión con el servidor VPN/WOL, o el cliente, se mostrará la ventana que aparece, teniendo que pulsar sobre Accept.



Como puede apreciarse en la ventana de la captura superior, al ya haber facilitado el usuario cuando se realizó la configuración y se guardó, al establecer la conexión solo habrá que facilitar la contraseña del usuario en cuestión, para este proyecto y por la configuración previa que se llevó a cabo, se trata del usuario pi, posteriormente se pulsará INTRO.

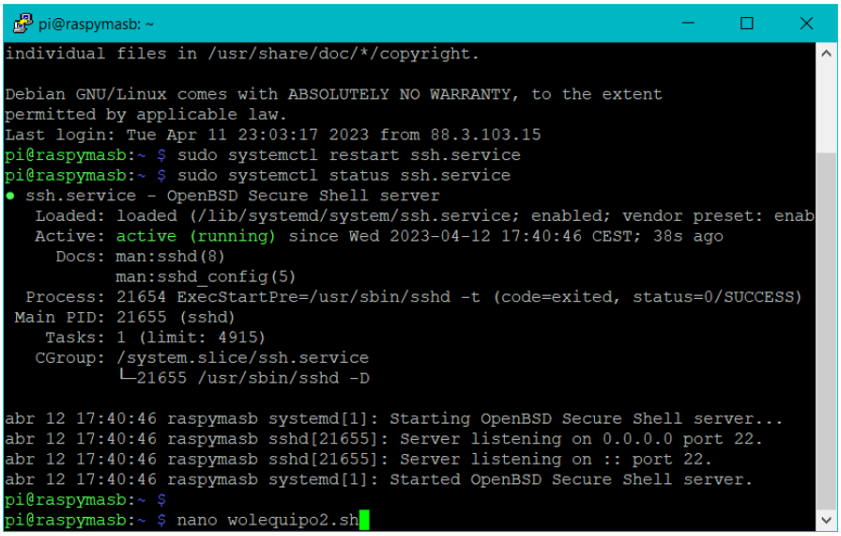


Una vez facilitada la contraseña y habiendo pulsado INTRO, se estará remotamente conectado en un terminal vía SSH a la Raspberry Pi.



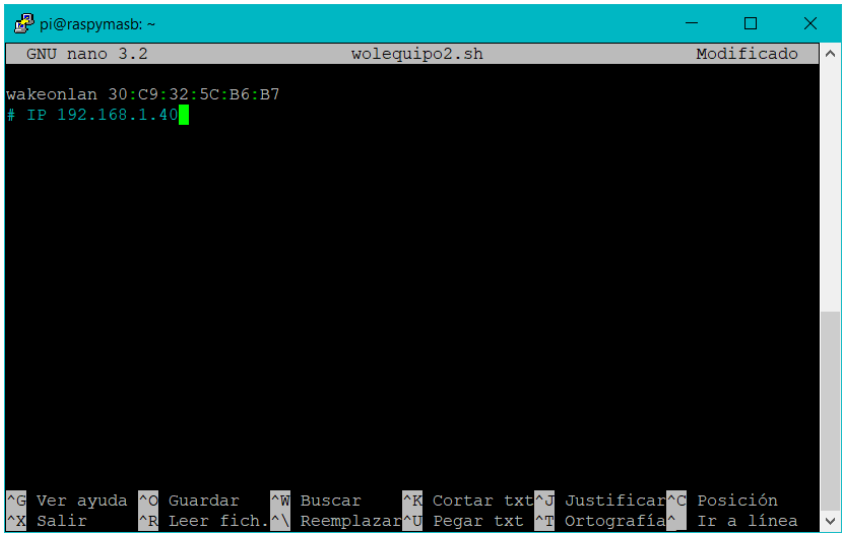
Dentro del terminal, se podrá realizar ciertas acciones de administración como parar, iniciar, reiniciar y consultar como se encuentran servicios, etc. Ejemplos.

sudo systemctl restart ssh.service (reiniciar servicio SSH).
sudo systemctl status ssh.service (comprobar el estado del servicio SSH).



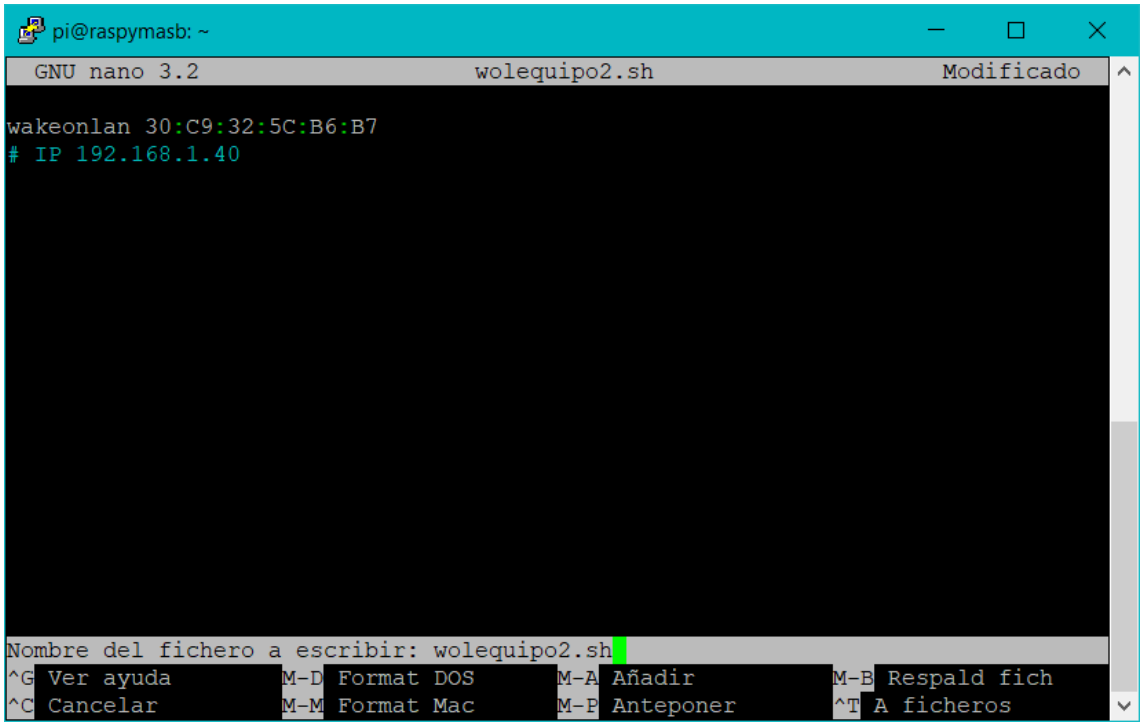
Remotamente, también como administrador y en referencia a la administración de Wake On LAN (WOL), se podrá crear los ficheros para su posterior ejecución e iniciar los equipos remotamente por comando, también se explica cómo realizar este proceso remotamente a través de la aplicación grafica gwakeonlan.

En este ejemplo, se crea el fichero para el equipo2, llamado wolequipo2.sh

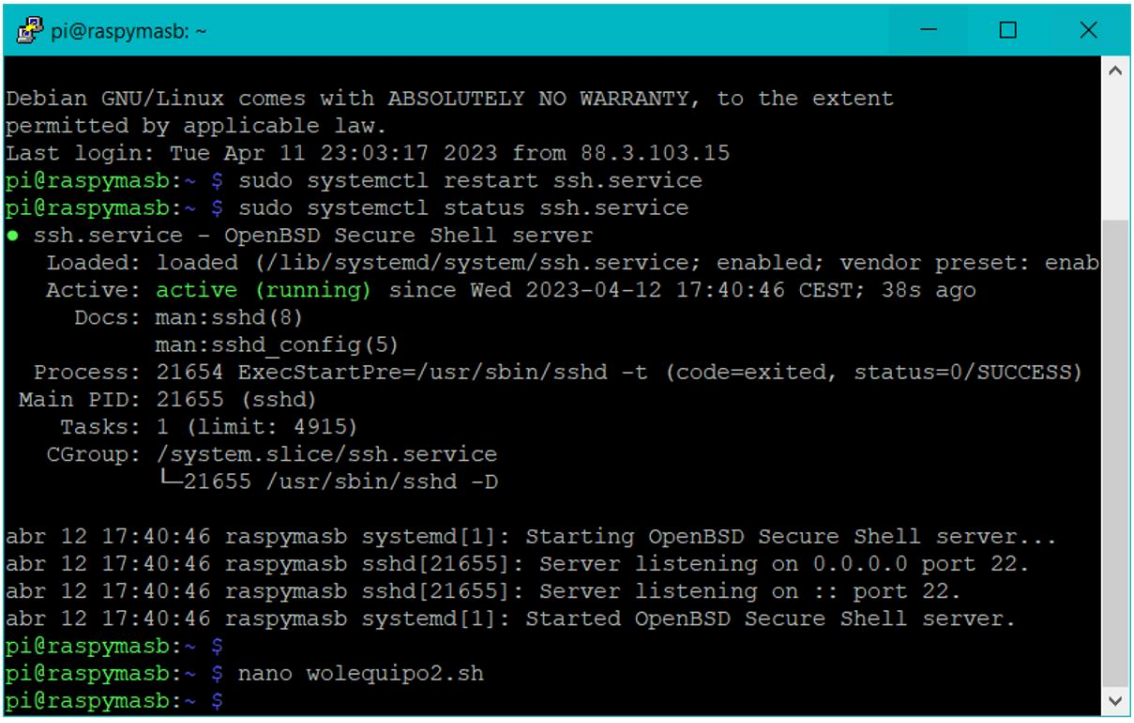


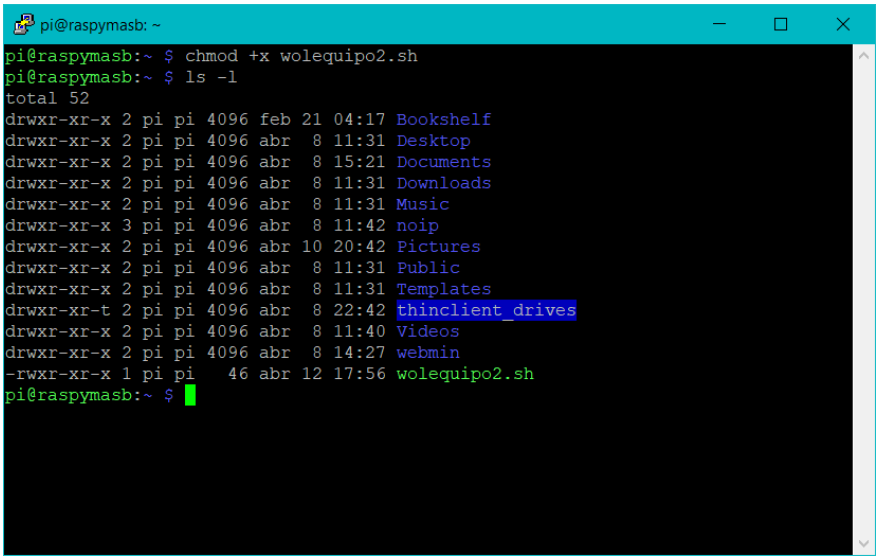
Dentro del fichero se escribe.
Comando wakeonlan “espacio” MAC (Dirección MAC de la tarjeta de red).
En el caso de colocar almohadilla ““#””, lo que se escriba a la derecha de la almohadilla, es un comentario, no se tiene en cuenta.
Como puede observar en la imagen de la captura superior, este fichero solo tiene las siguientes líneas.

wakeonlan 30:C9:32:5C:B6:B7
IP 192.168.1.40



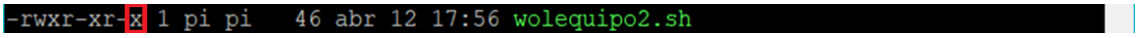
Con los datos añadidos correctamente, se pulsará la combinación de teclas CTRL (Control) y sin soltarla la tecla “O” para guardar el contenido, posteriormente CTRL (Control) y sin soltarla la tecla “X” para salir del editor nano.



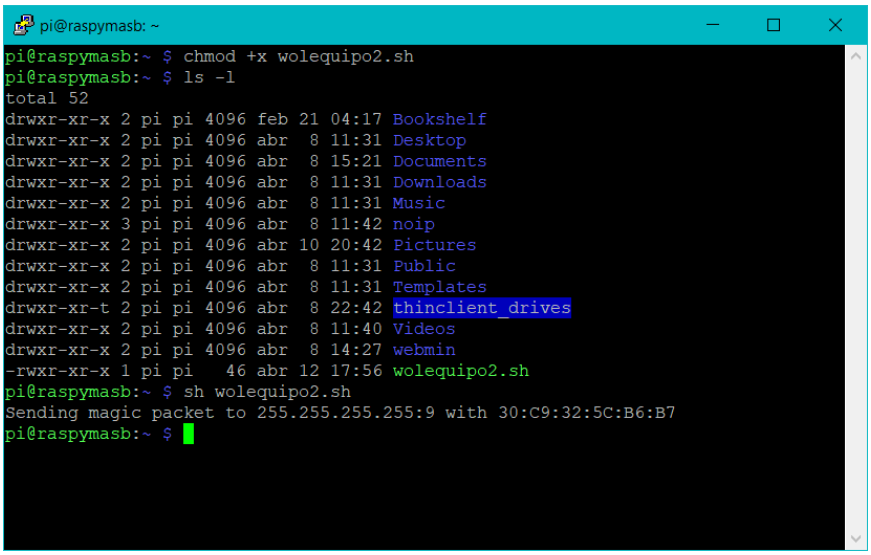


Se podrá limpiar el terminal con el comando. clear
Acto seguido, para dar permisos de ejecución al fichero wolequipo2.sh, se ejecuta el comando.
chmod +x wolequipo2.sh

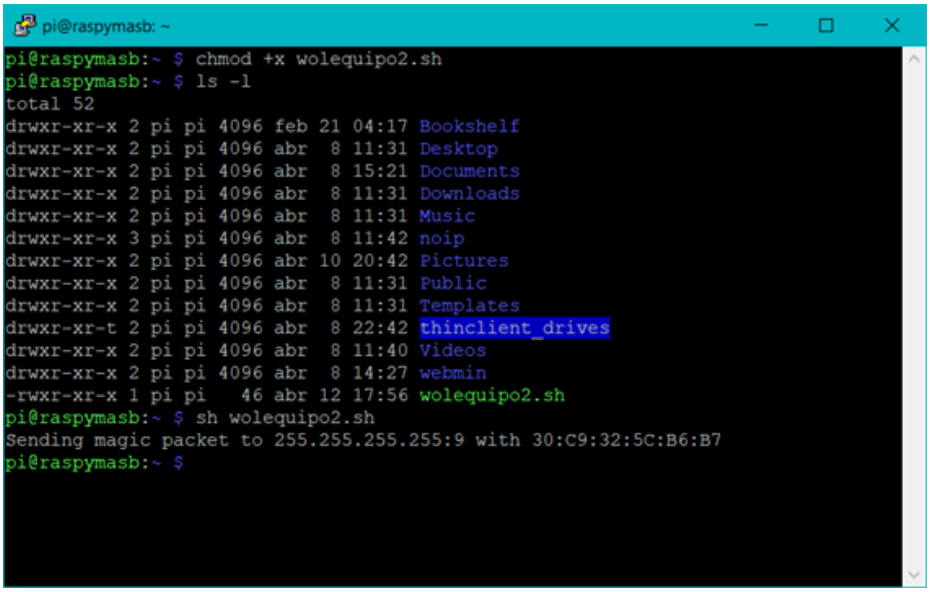
Para finalizar, con el comando. ls –l (si todo ha salido bien, tendría que salir el fichero en caso de estar configurado el color en el terminal, de color verde).



O como se observa, aparecer una “X” en la posición del cuadro rojo, en la ventana de la captura superior, tras ejecutar el comando. ls -l .

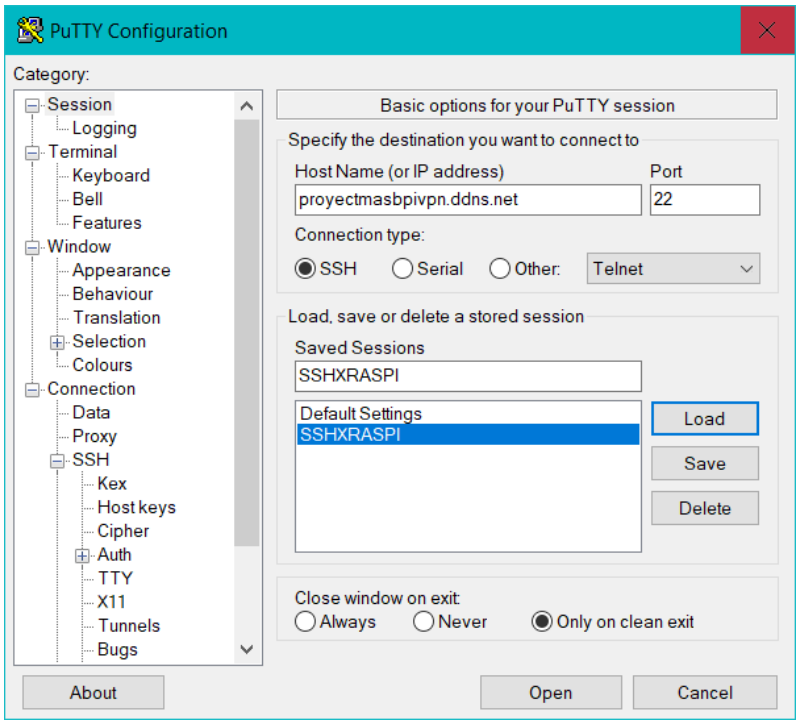


Terminada la creación, para ejecutar el fichero, simplemente se ejecutará el comando.
sh wolequipo2.sh



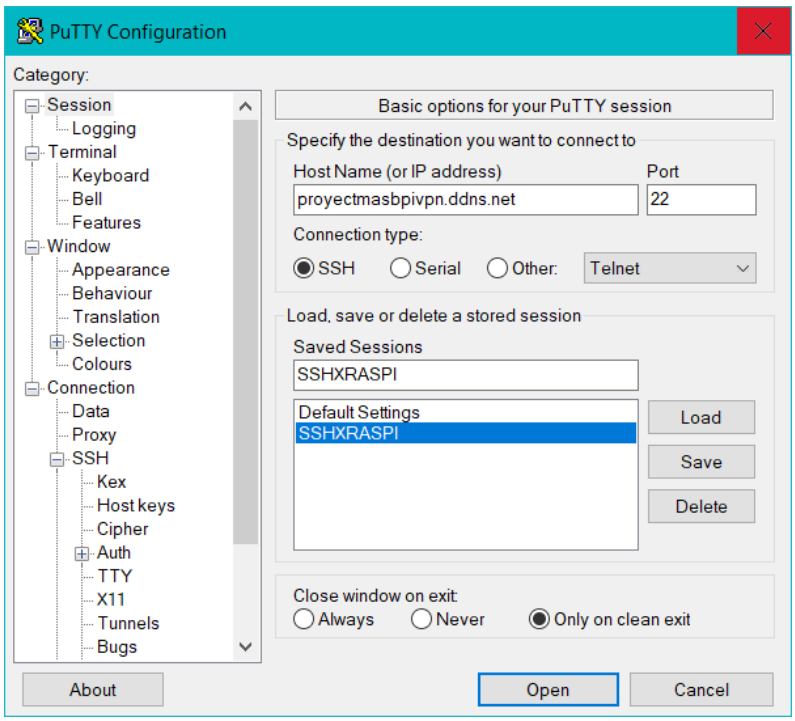
Al ejecutar el comando. sh wolequipo2.sh, se puede apreciar en la ventana de la captura superior, como se envía el “paquete mágico” a la dirección MAC indicada, con lo que el equipo en cuestión, si se encuentra correctamente configurado, arrancará y comenzará a cargarse el S.O.

Conexión grafica redirección X.

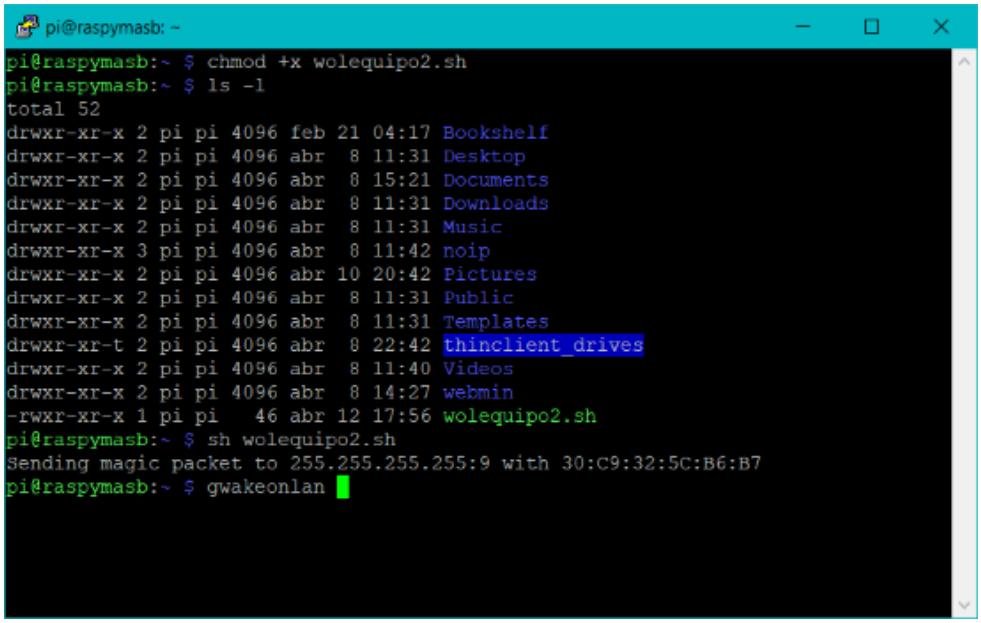


Una vez abierta y dentro de la aplicación PuTTY, se selecciona la sesión guardada, en el apartado Saved Sessions SSHXRASPI, ventana de la captura superior y se pulsará el botón Load.

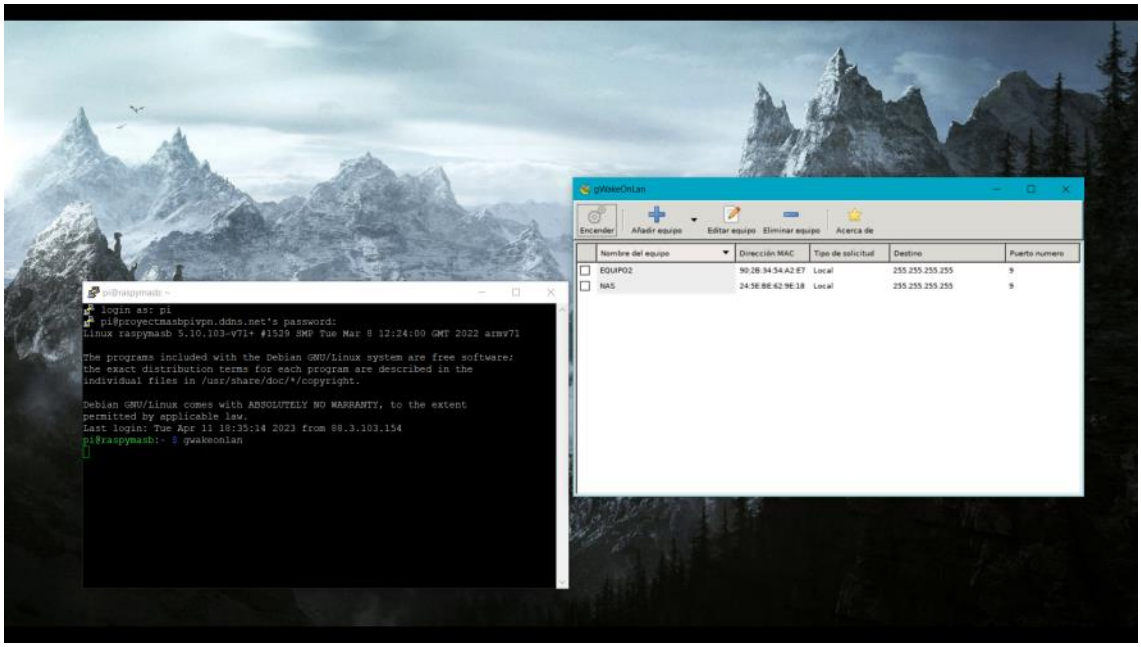
Posteriormente, tras pulsar el botón Load, se cargará automáticamente la configuración guardada de la conexión, teniendo que pulsar sobre el botón inferior Open, para establecer la conexión, imagen captura derecha.



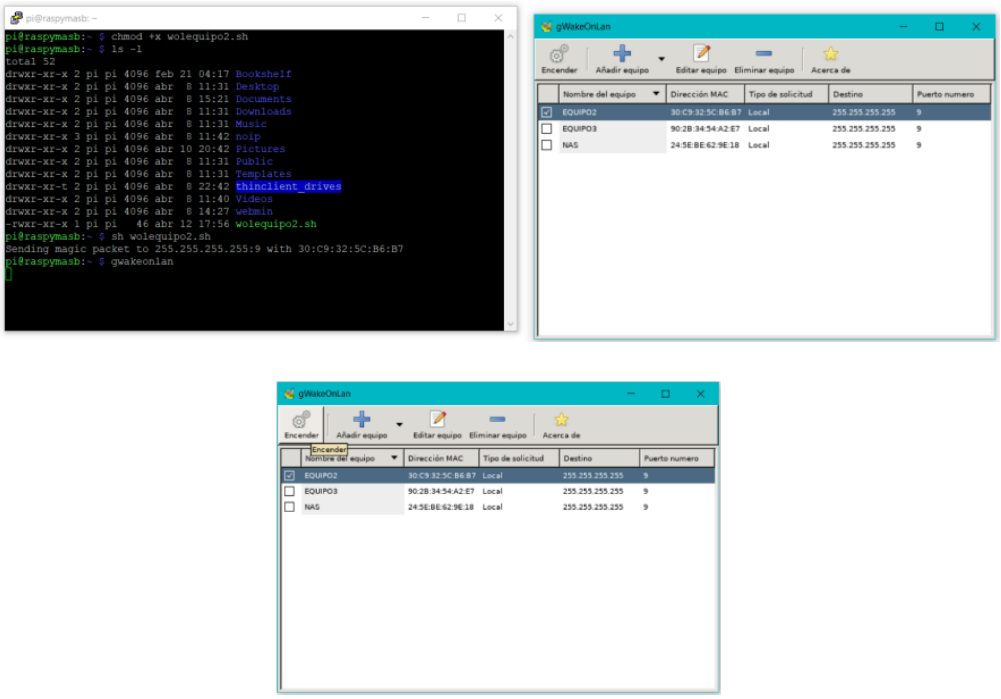
En este otro caso, y es por lo que se ha creado y guardado la configuración previa en PuTTY con la redirección X activa, es hacer uso de la redirección X, en el S.O. Windows se tendrá que tener instalada e iniciada la aplicación Xming ejecutando XLaunch, mientras que en el equipo servidor, se habrá habilitado X11Forwarding.



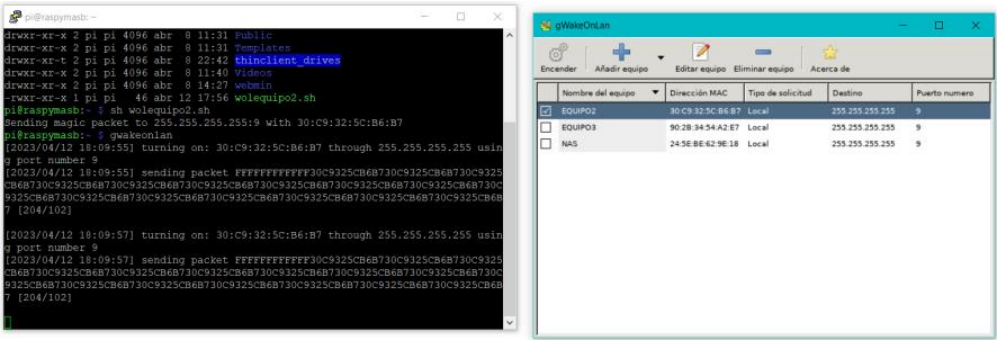
Nuevamente, dentro del terminal y establecida la conexión remota al servidor VPN/WOL vía SSH, se ejecutará el comando gwakeonlan



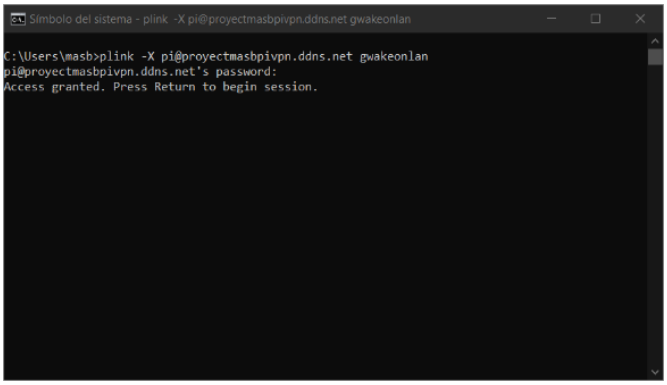
Pasado un poco de tiempo, se mostrará la ventana de la aplicación grafica instalada en el servidor Linux VPN/WOL, la aplicación gwakeonlan esta vez se muestra en el escritorio del equipo con S.O. Windows.



En la que se podrá seleccionar el/los equipos a encender y pulsar el botón superior izquierdo Encender.


pi@raspymasb: ~
drwxr-xr-x 2 pi pi 4096 abr 8 11:31 Public
drwxr-xr-x 2 pi pi 4096 abr 8 11:31 Templates
drwxr-xr-t 2 pi pi 4096 abr 8 22:42 thinclient_drives
drwxr-xr-x 2 pi pi 4096 abr 8 11:40 Videos
drwxr-xr-x 2 pi pi 4096 abr 8 14:27 webmin
-rwxr-xr-x 1 pi pi 46 abr 12 17:56 wolequipo2.sh
pi@raspymasb:~ $ sh wolequipo2.sh
Sending magic packet to 255.255.255.255:9 with 30:C9:32:5C:B6:B7
pi@raspymasb:~ $ gwakeonlan
[2023/04/12 18:09:55] turning on: 30:C9:32:5C:B6:B7 through 255.255.255.255 using port number 9
[2023/04/12 18:09:55] sending packet FFFFFFFFFFFF30C9325CB6B730C9325CB6B730C9325CB6B730

Conexión grafica uso comando plink.



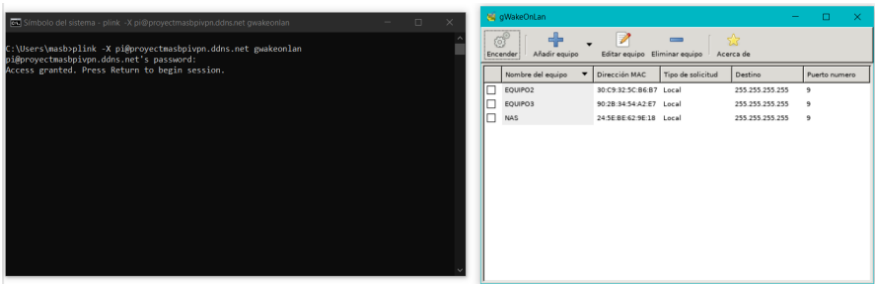
Esta aplicación se instala, al instalarse la aplicación PuTTY.

Otra opción para iniciar remotamente la aplicación gráfica y temiendo en el S.O. Windows iniciada la aplicación Xming, es simplemente ejecutar dentro de un Símbolo del Sistema “CMD” el comando.

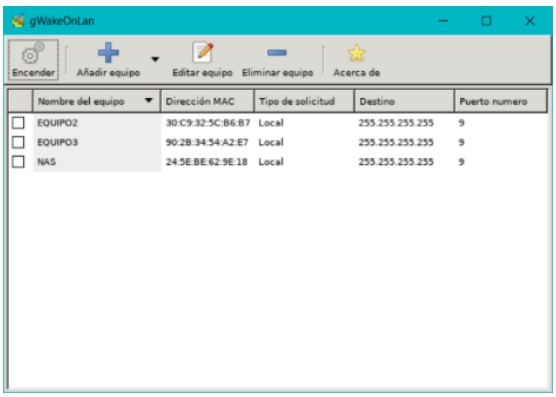
plink -X pi@proyectmasbpivpn.ddns.net gwakeonlan

Tras pulsar INTRO, se facilitará la contraseña del usuario, en este ejemplo pi, y se pulsará INTRO en el mensaje que aparece indicando.

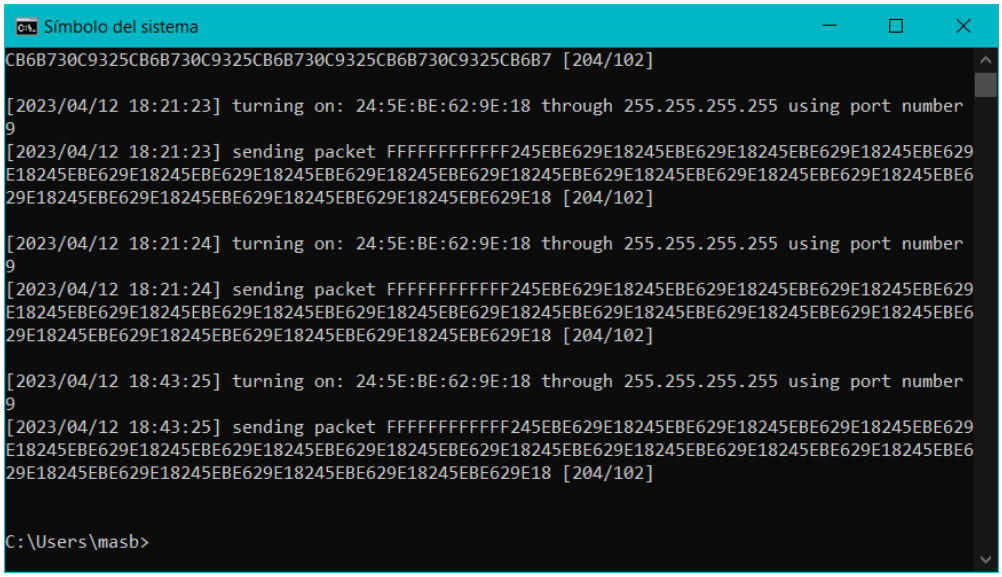
“”Access granted. Press Return to begin session.””
“”Acceso permitido. Presione Retorno para comenzar la sesión.””



Nuevamente, pasado un tiempo, se mostrará la ventana de la aplicación grafica instalada en el servidor Linux VPN/WOL, mostrándose en el escritorio del equipo con S.O. Windows.



En la ventana de la aplicación grafica gwakeonlan, se podrá seleccionar el/los equipos a encender y pulsar el botón superior izquierdo Encender.



En la ventana de la captura superior, se puede observar cómo se envía a través del terminal, las acciones que se están seleccionando en la aplicación gráfica gwakeonlan.

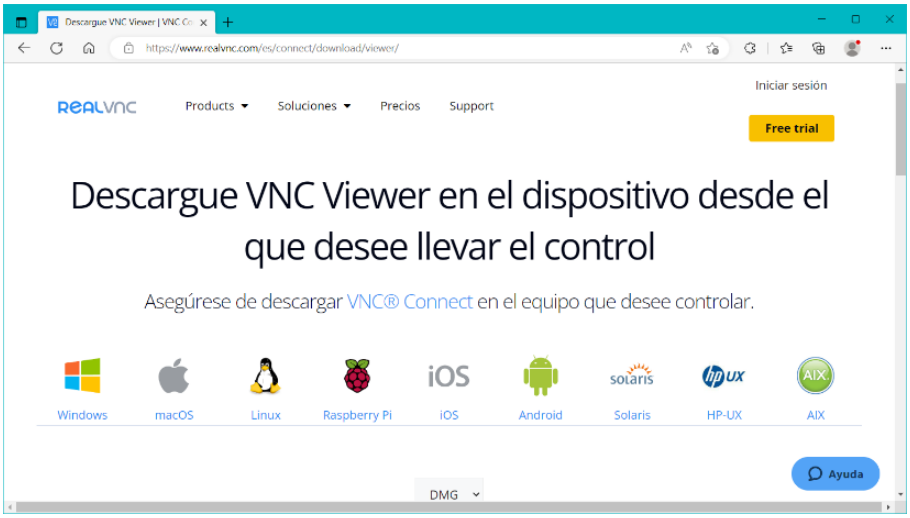
Tras cerrar la aplicación gwakeonlan, por ejemplo, presionando sobre la “X” superior derecha, esta se cerrará y se permanecerá dentro de la ventana del Símbolo del Sistema (CMD), pudiendo cerrarla.

Descarga instalación y configuración aplicación RealVNC.

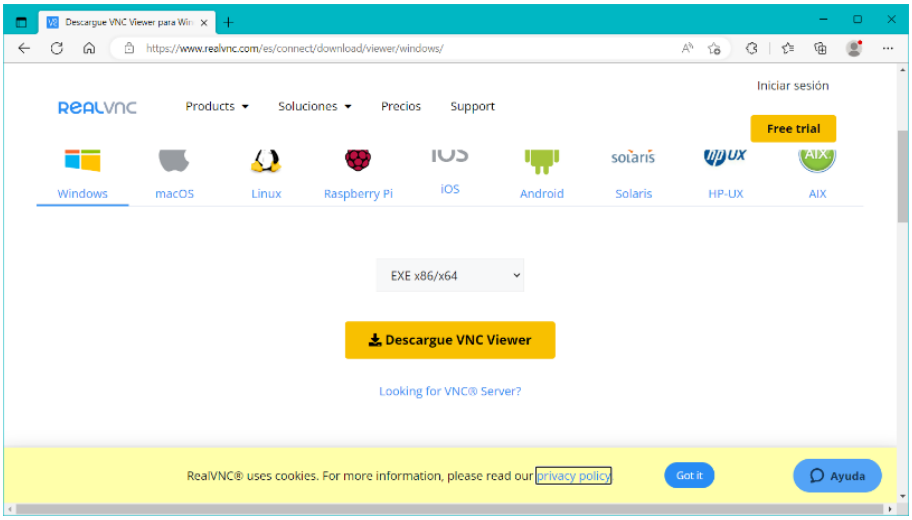
Descarga en S.O. Windows.

El puerto de conexión por defecto para la aplicación RealVNC es el TCP 5900, el cual, habrá que abrirlo en el router y habilitar el tráfico TCP puerto 5900 en el cortafuegos del servidor VPN/WOL.

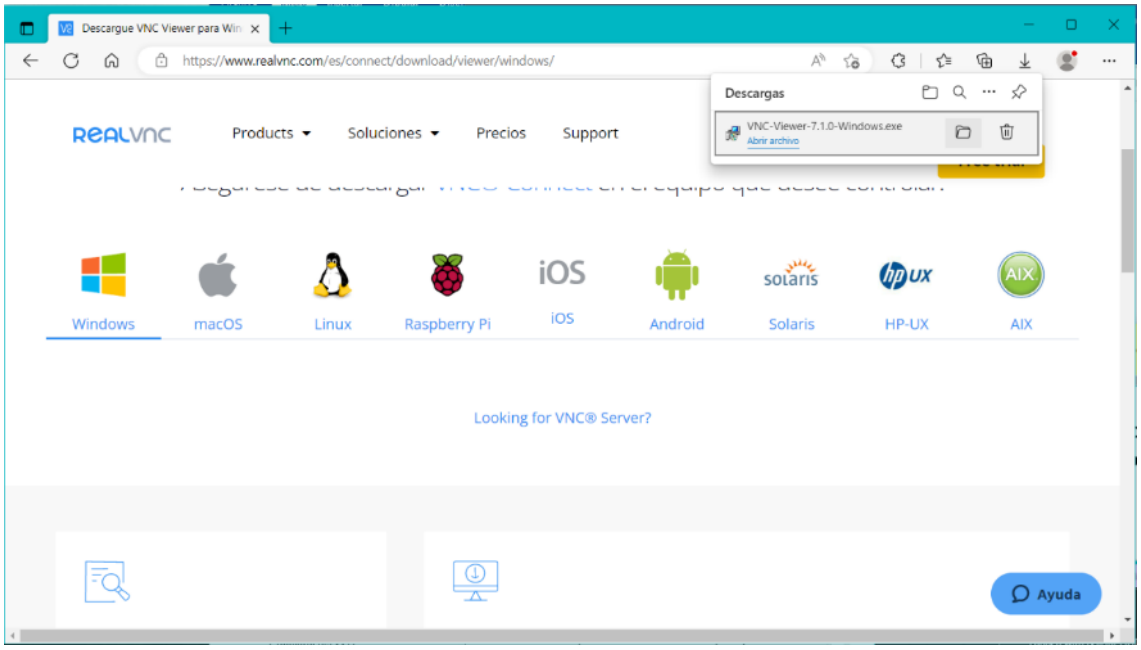
WEB oficial de la aplicación.
URL. https://www.realvnc.com/es/connect/download/viewer/



En la WEB oficial, se pulsará en este caso, sobre el icono correspondiente al S.O. Windows.

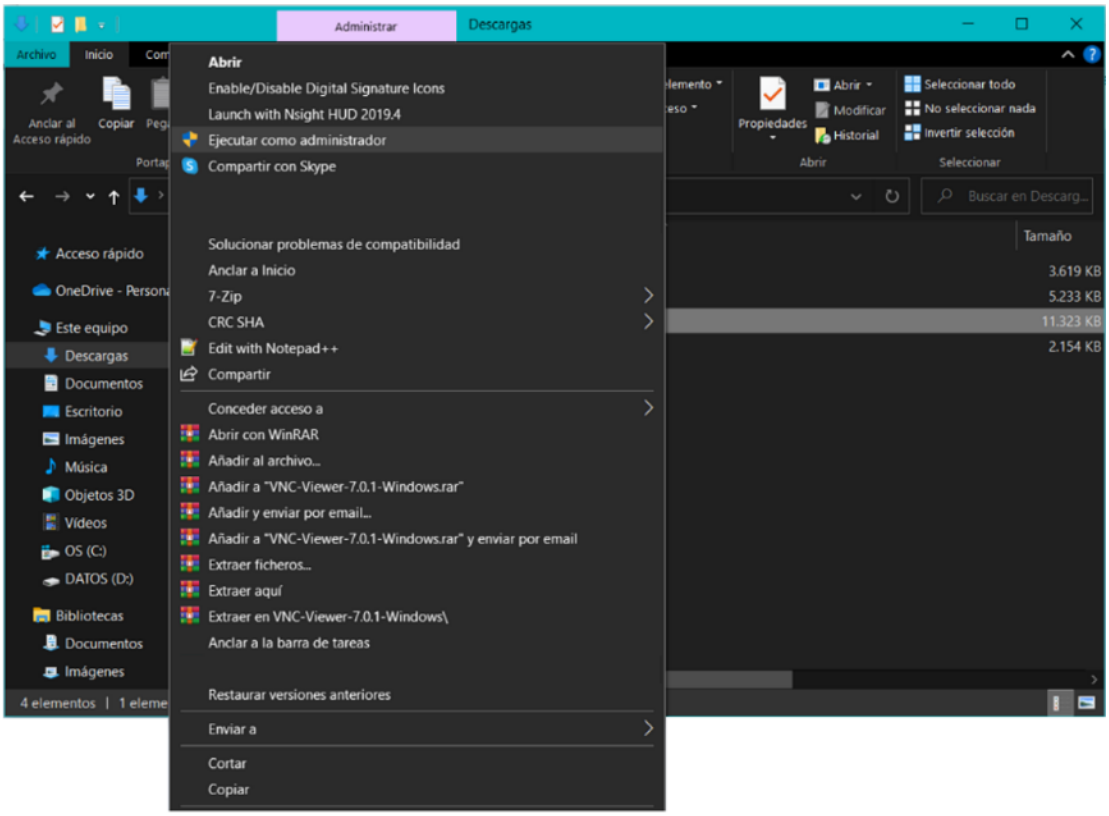


Al seleccionar el S.O. Windows, se deslizará la barra lateral derecha hasta localizar el link de descarga, pulsando con el botón izquierdo del ratón sobre el botón Descargue VNC Viewer.

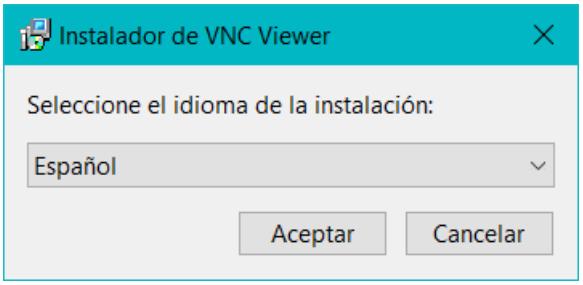


El fichero se descargará a la ubicación que se tenga configurado por defecto la descarga del navegador utilizado.

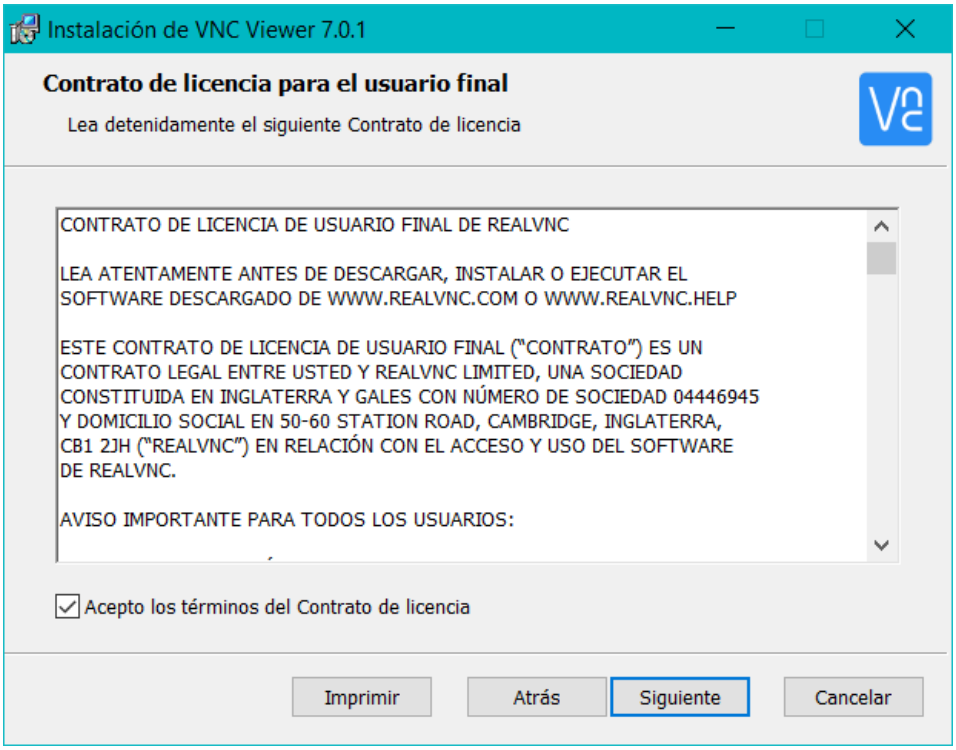
Instalación en S.O. Windows.



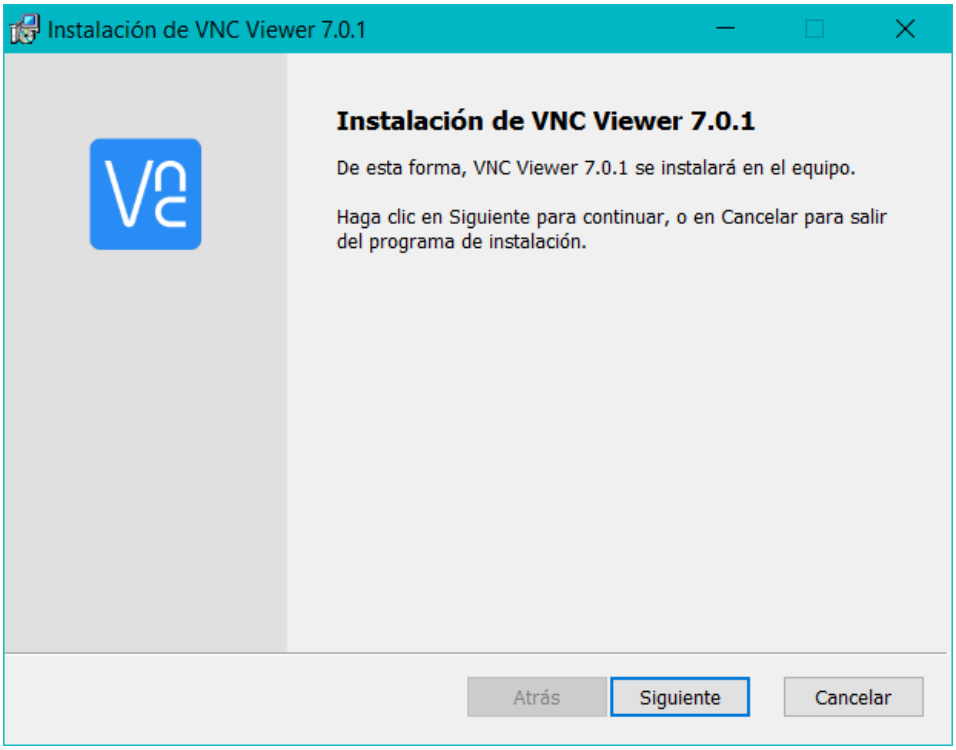
Sobre el ejecutable descargado, en este caso VNC-Viewer-7.1.0-Windows.exe, se pulsará con el botón derecho del ratón, en el menú que aparece se pulsará sobre Ejecutar como administrador.



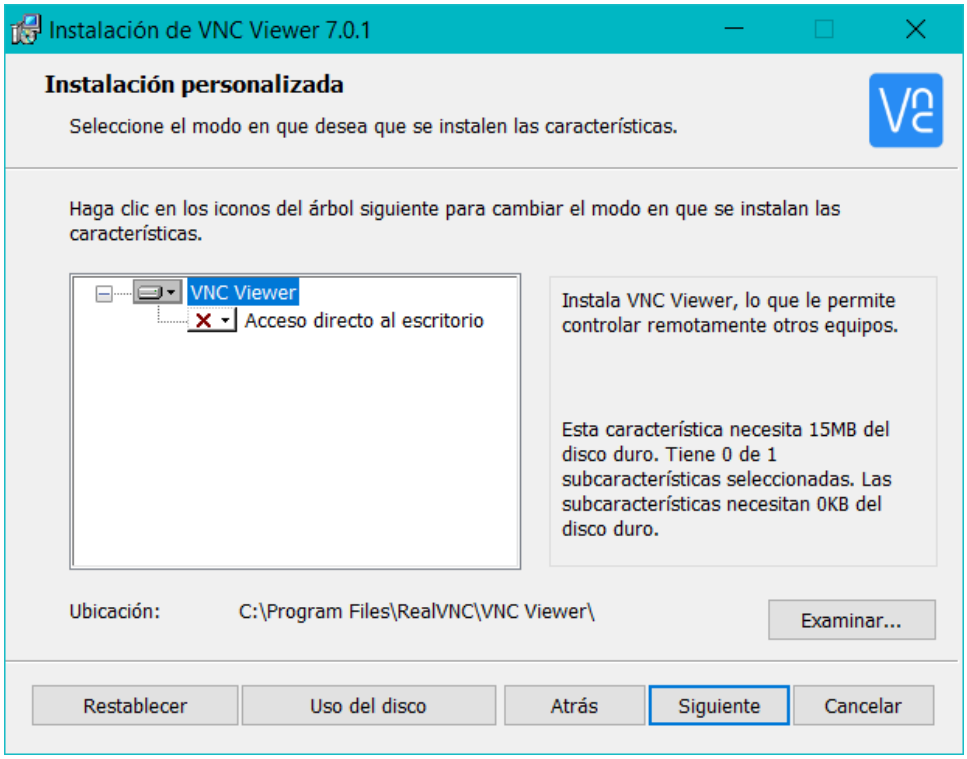
Se seleccionará el idioma que proceda, en este caso Español y se pulsará Aceptar.



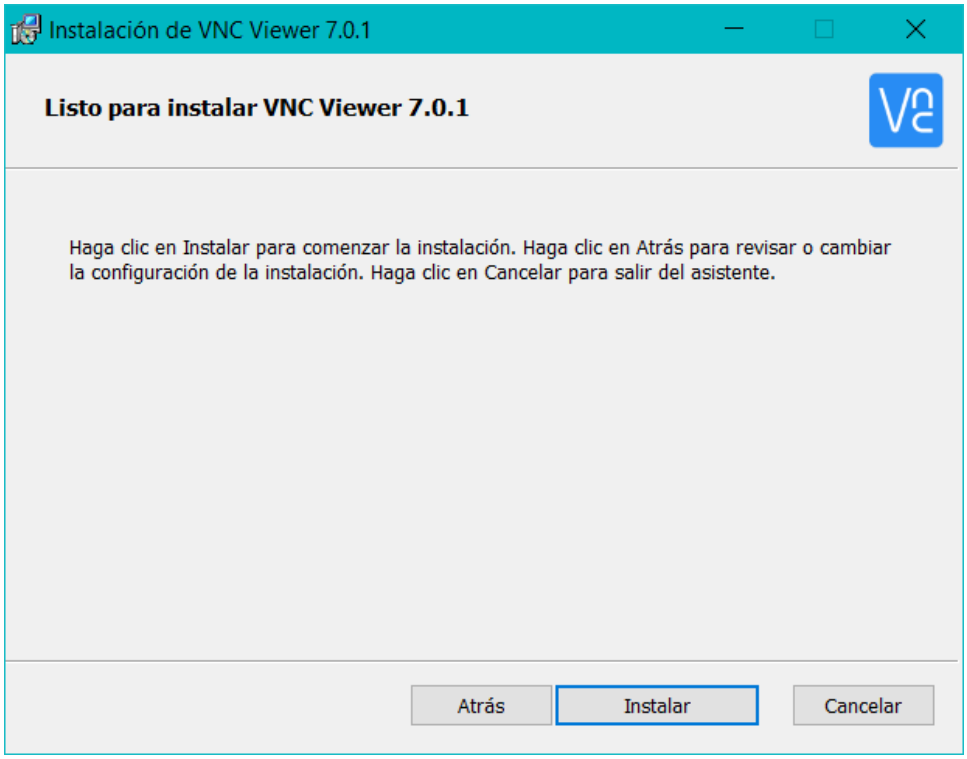
Habrá que seleccionar la opción Acepto los términos del contrato de licencia y se pulsará Siguiente.



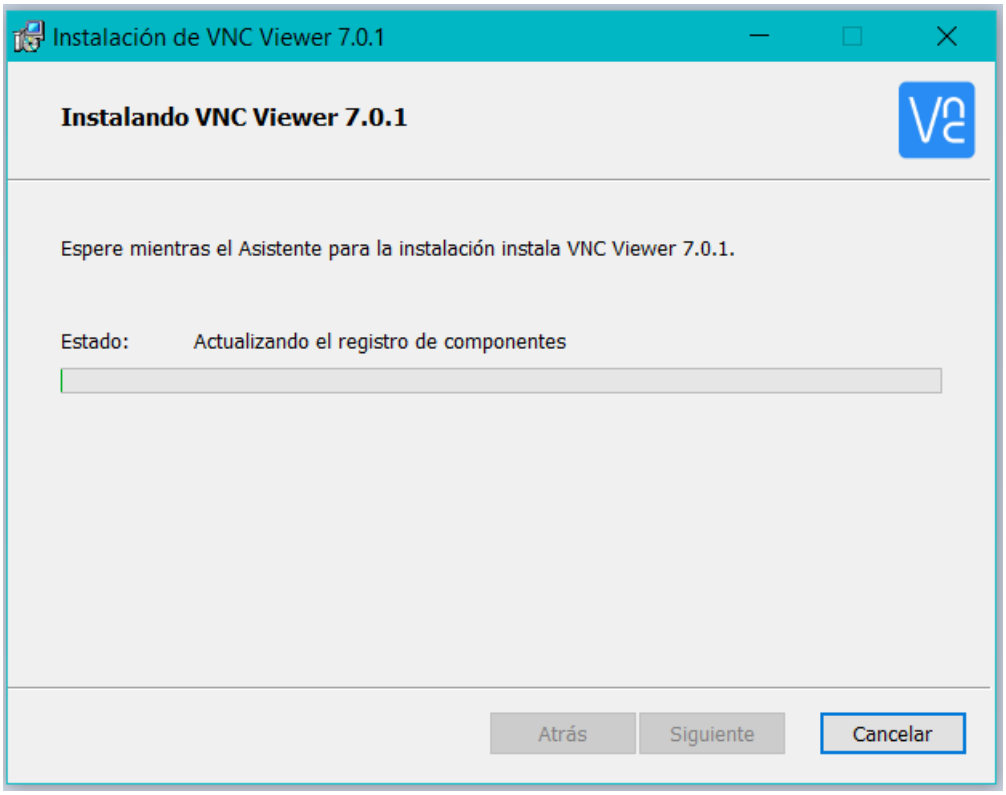
Se pulsará Siguiente.



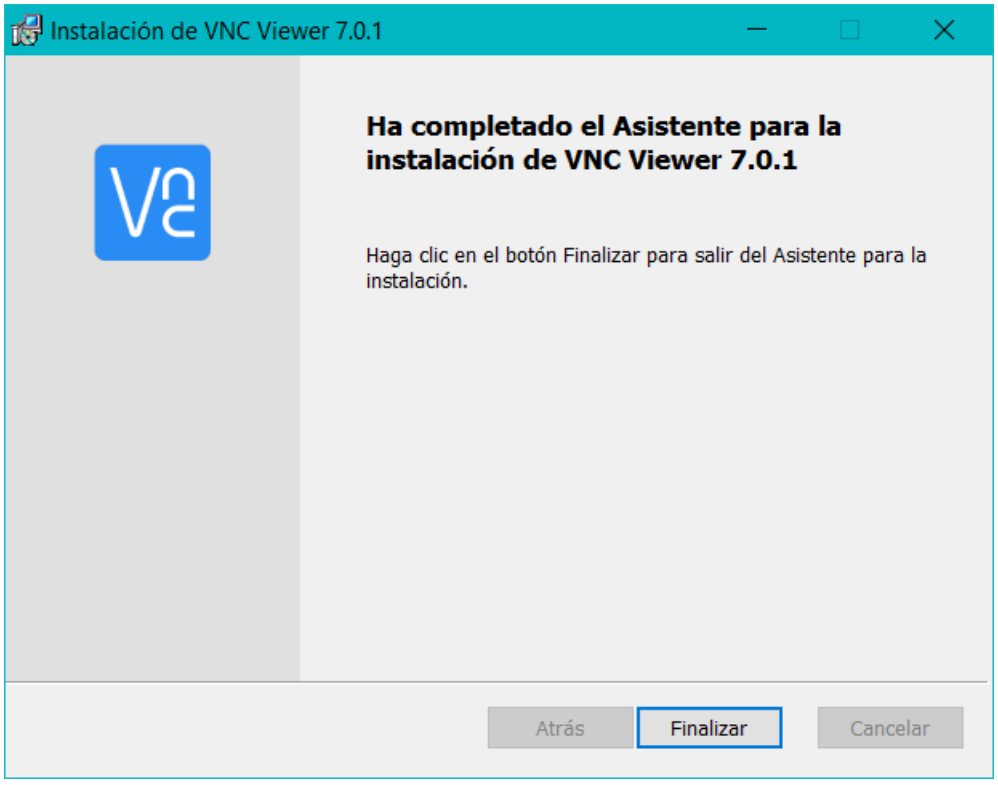
Para este proyecto, se dejan tanto las opciones de instalación como el directorio de instalación por defecto y se pulsa Siguiente.



Para comenzar la instalación, se pulsará Instalar.

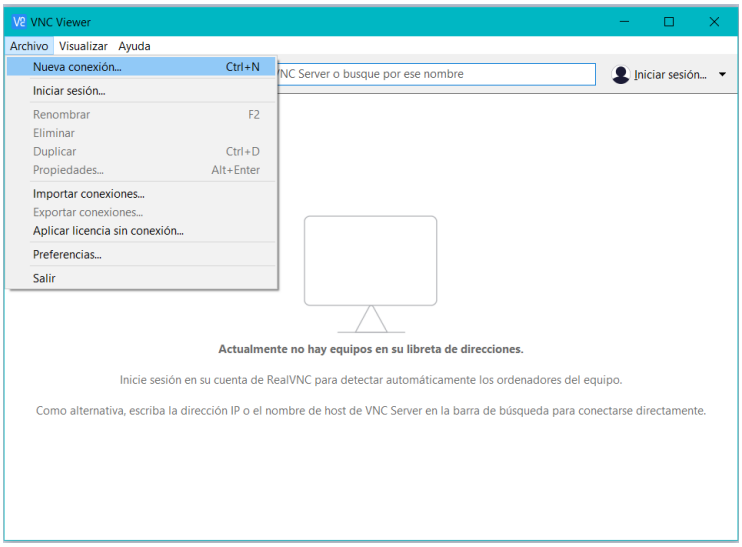


Comenzando el proceso de instalación de la aplicación.

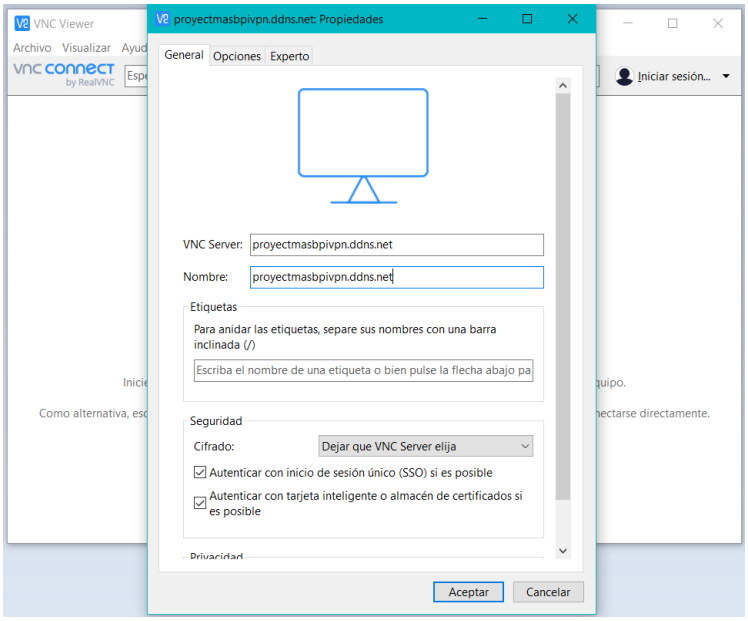


Realizada la instalación, se pulsará Finalizar.

Configuración creación conexión S.O. Windows.



Con la aplicación abierta, se pulsará sobre Archivo \ Nueva conexión.

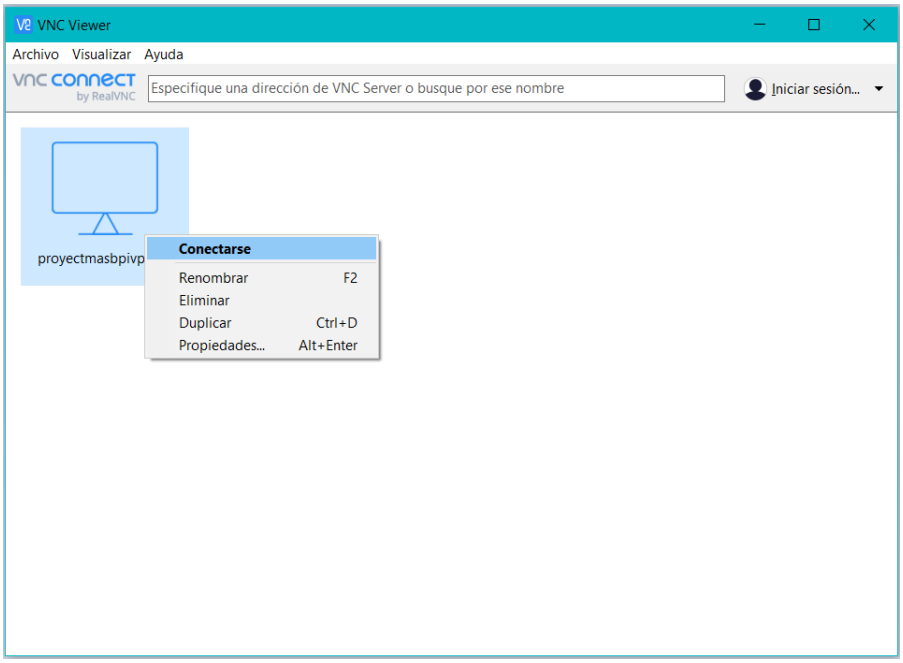


En la ventana que aparece, habrá que introducir los datos necesarios para la creación de la conexión.

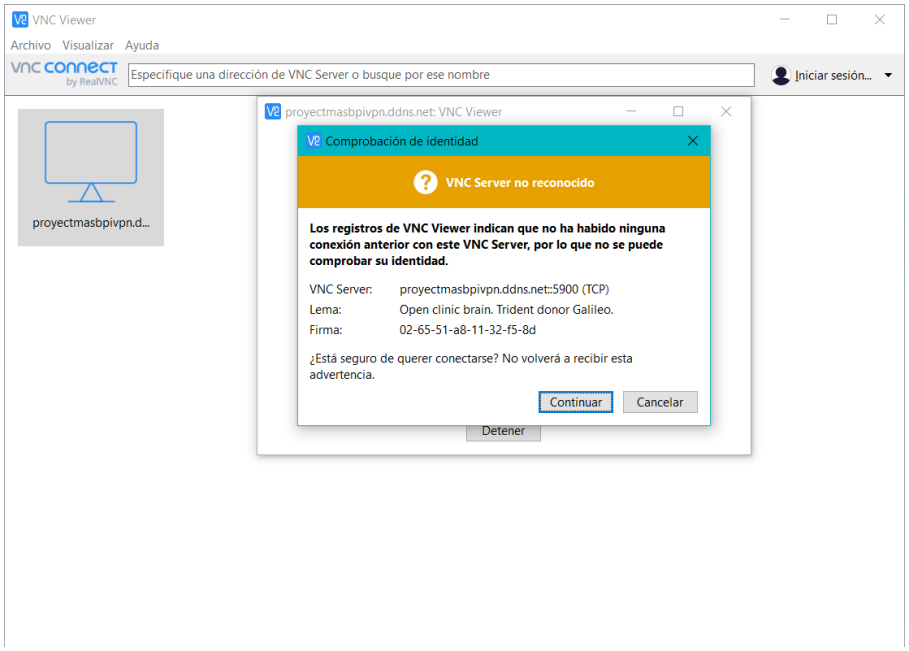
- VNC Server, en este ejemplo, se colocará el nombre de dominio o host creado en el proveedor de servicios DDNS, proyectmasbpivpn.ddns.net
- Nombre, en este ejemplo, se colocará el nombre de dominio o host creado en el proveedor de servicios DDNS, proyectmasbpivpn.ddns.net

Pudiendo pulsar en Aceptar tras rellenar los campos indicados.

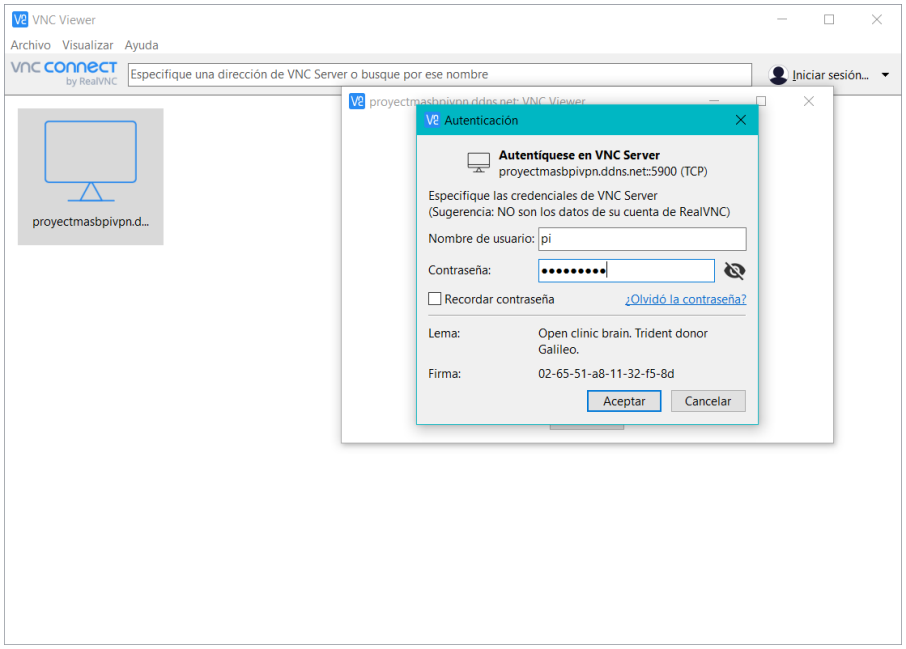
Conexión S.O. Windows.



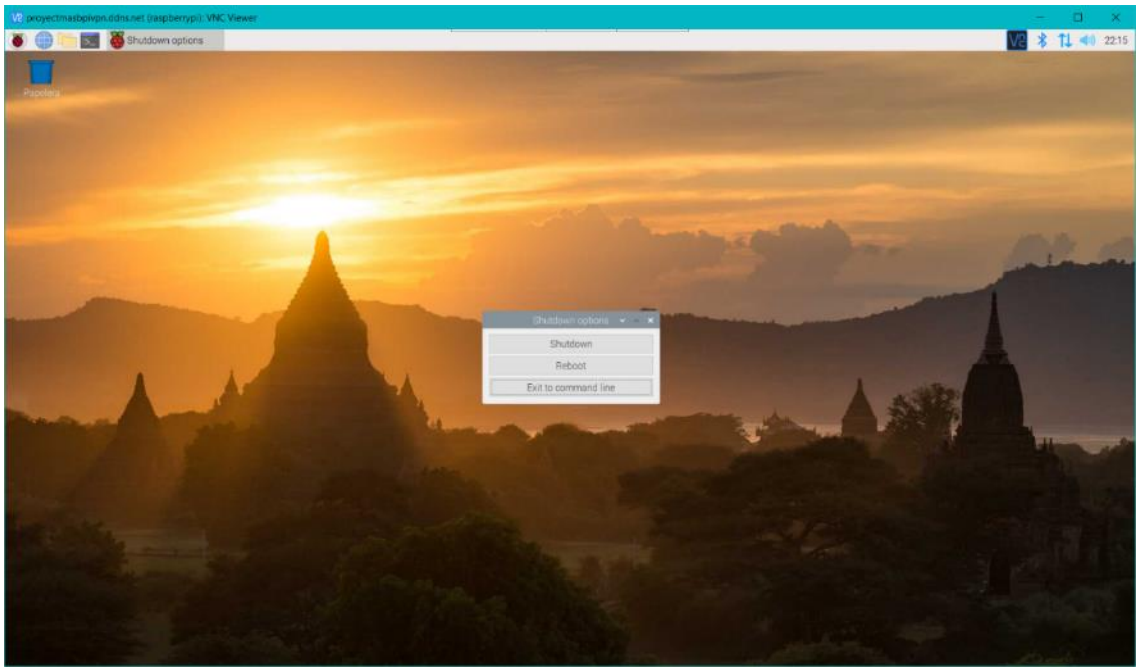
Dentro de la aplicación VNC Viewer y con la conexión creada, se podrá pulsar con el botón derecho del ratón sobre la miniatura creada a la conexión, en el menú que aparece se pulsará sobre Conectarse.

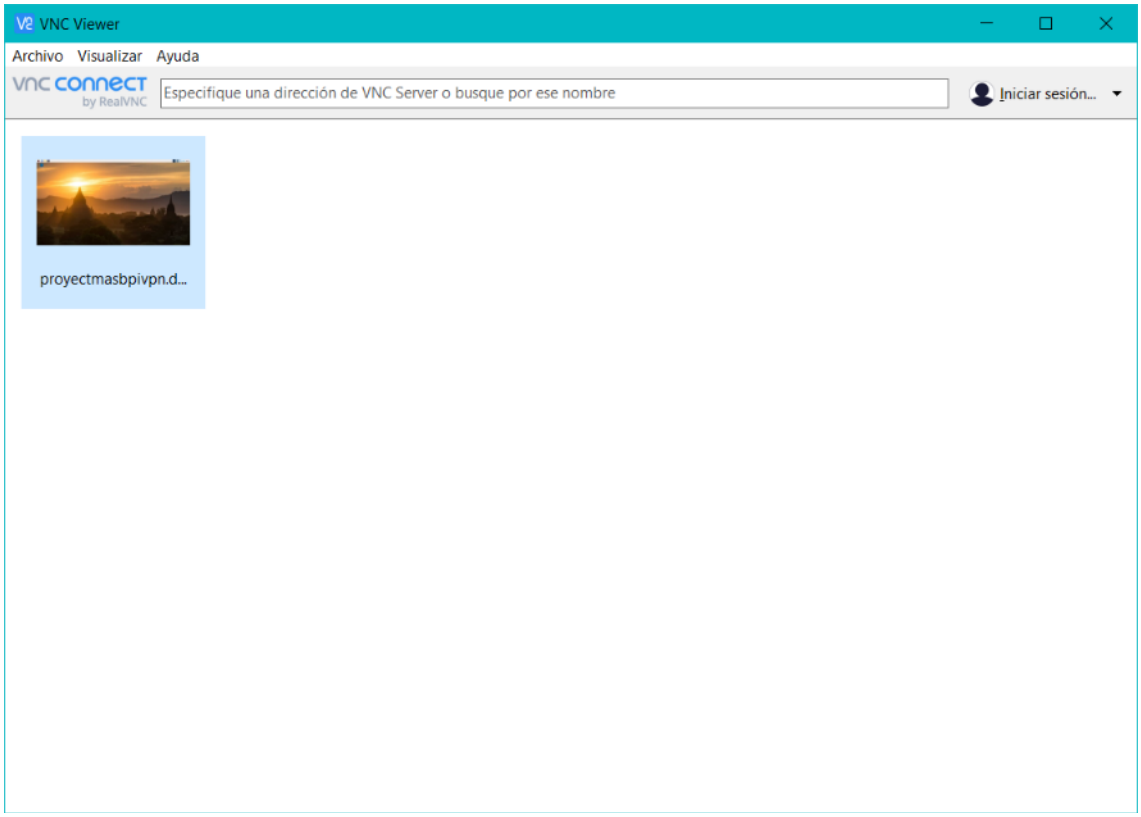


En la ventana donde se informa que el server no es reconocido, se pulsará en Continuar.



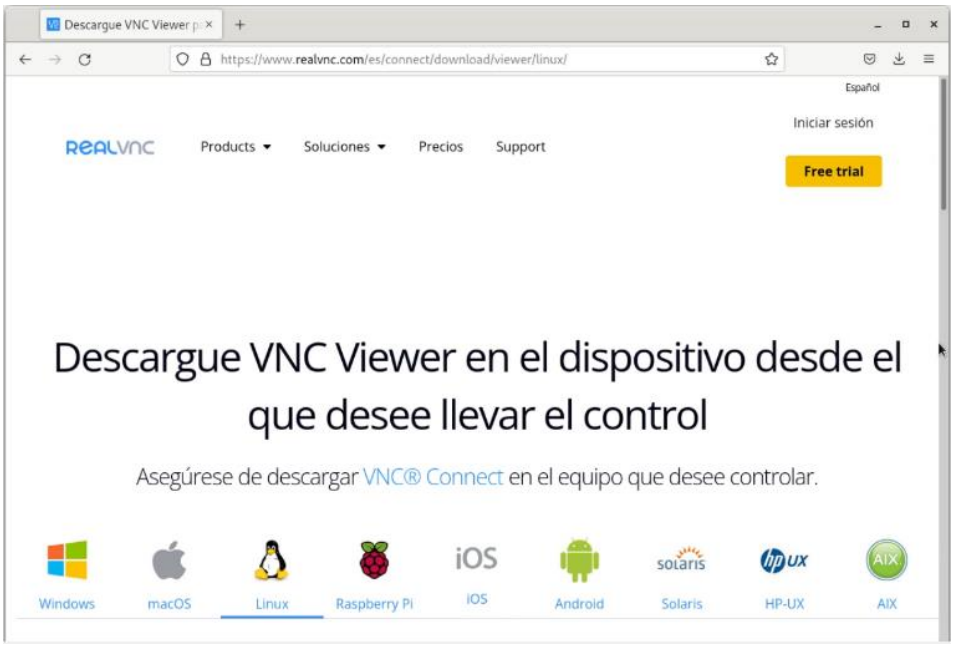
Se solicitarán y se facilitarán las credenciales para la autenticación, llevándose a cabo la conexión al pulsar sobre Aceptar.





Finalmente, como se puede apreciar en la venta de la captura superior, tras cerrar la conexión, aparece una miniatura de la conexión realizada como icono de la conexión creada y establecida, pudiendo este icono cambiar de aspecto.

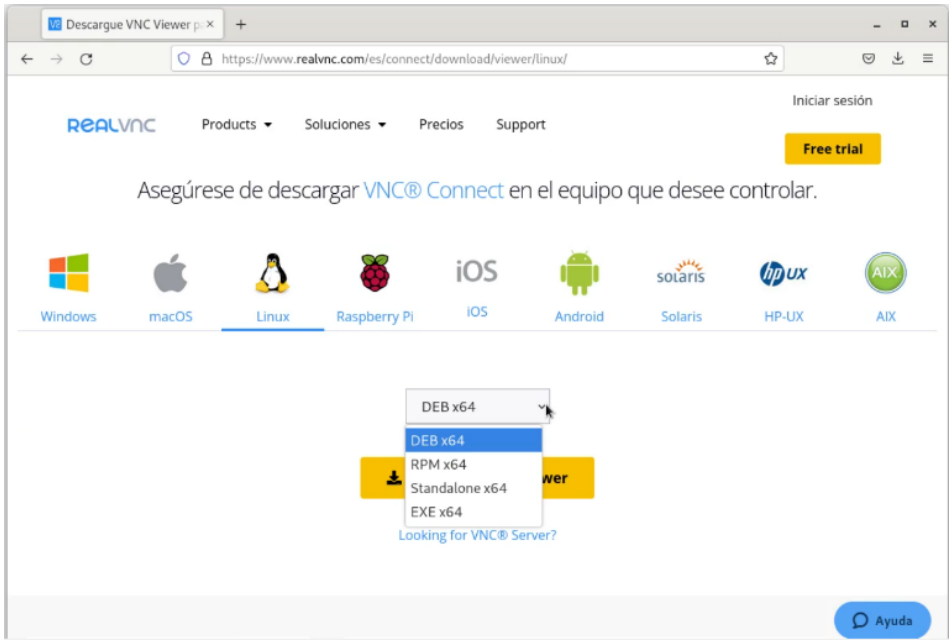
Descarga en S.O. Linux.



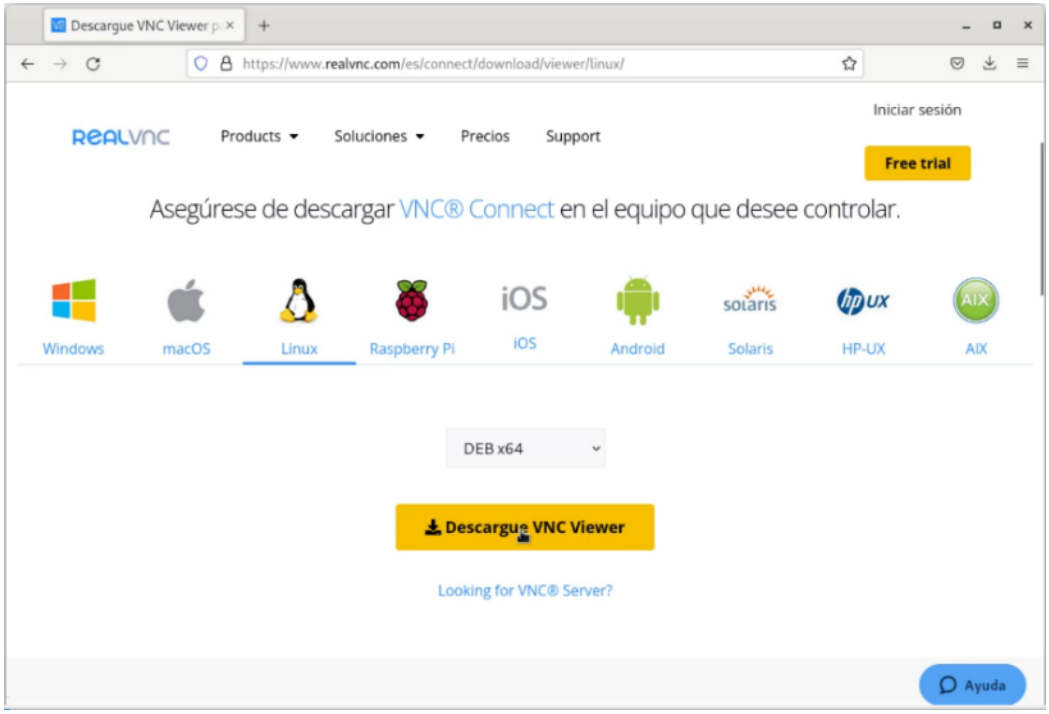
Para realizar la descarga de la aplicación, dentro de la WEB oficial.

URL. https://www.realvnc.com/es/connect/download/viewer/

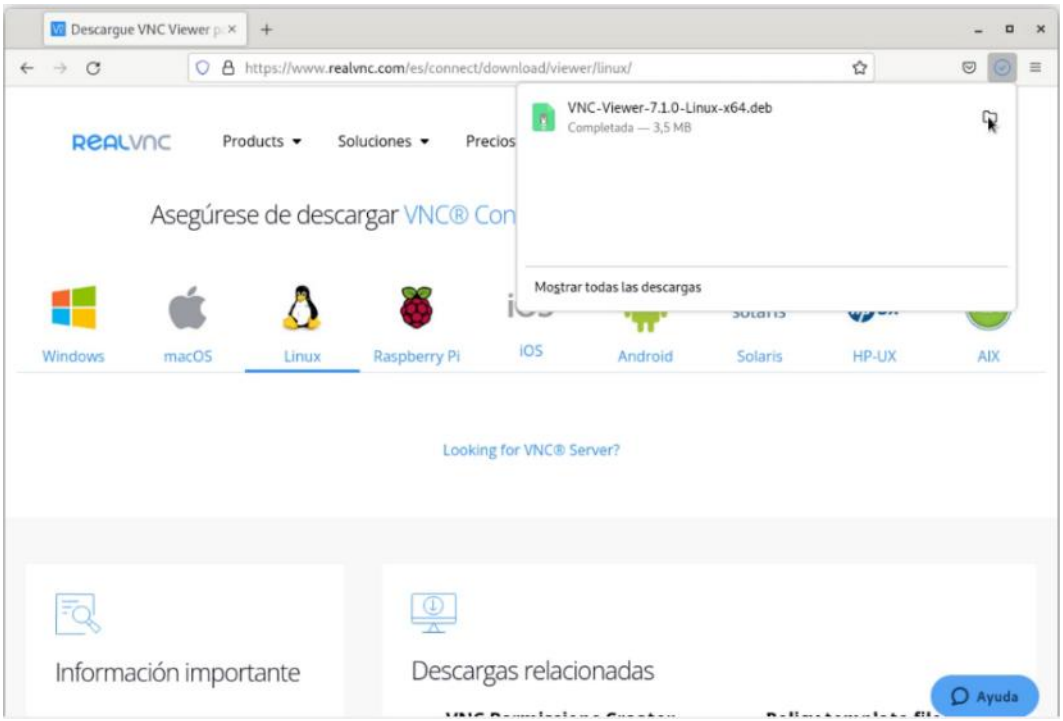
Se pulsará sobre el icono, en este caso del S.O. Linux.



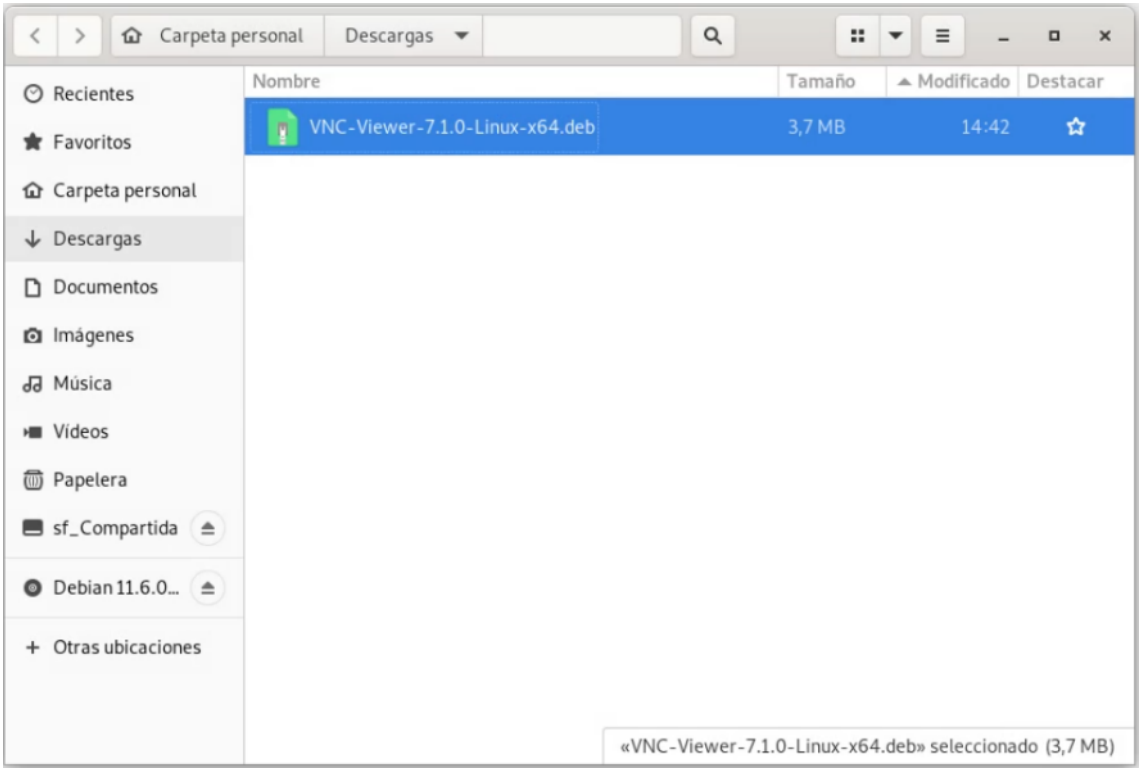
Al ser esta distribución Linux Debian, se necesita descargar un fichero DEB y al ser arquitectura de 64 Bits, se descargará el fichero DEBx64.



Al seleccionar la descarga correcta, se pulsará sobre el botón Descargar VNC Viewer.

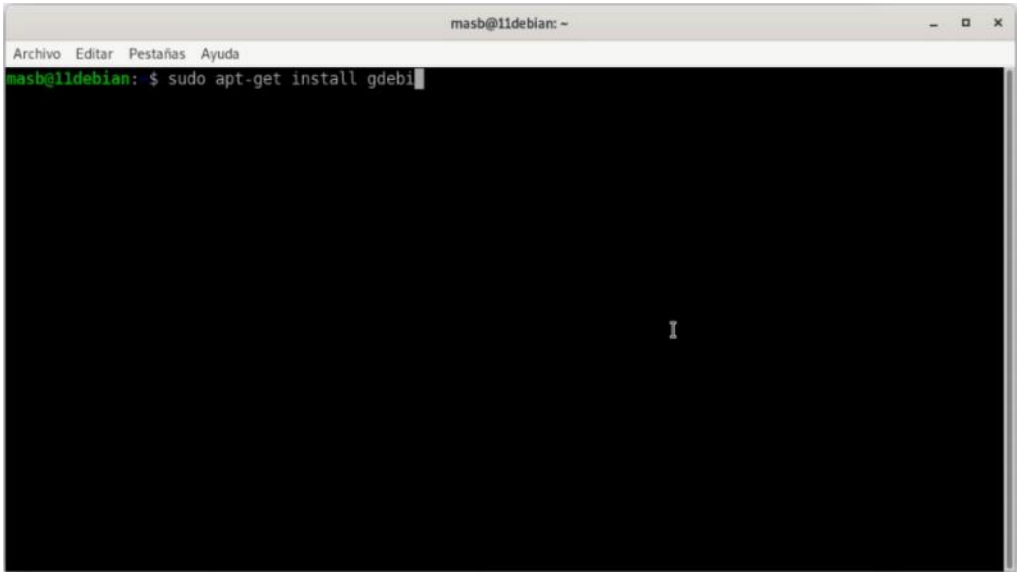


Finalizada la descarga, el fichero en este caso VNC-Viewer-7.1.0-Linux-x64.deb, se habrá descargado en el directorio por defecto donde se realizan las descargas.



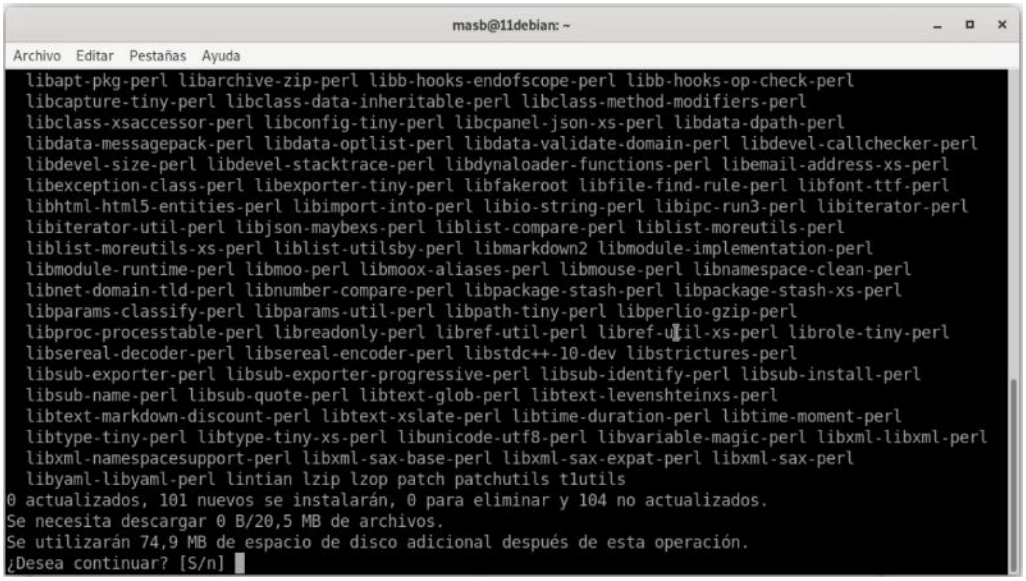
Directorio por defecto de descarga, con el fichero descargado VNC-Viewer-7.1.0-Linux-x64.deb.

Instalación en S.O. Linux.

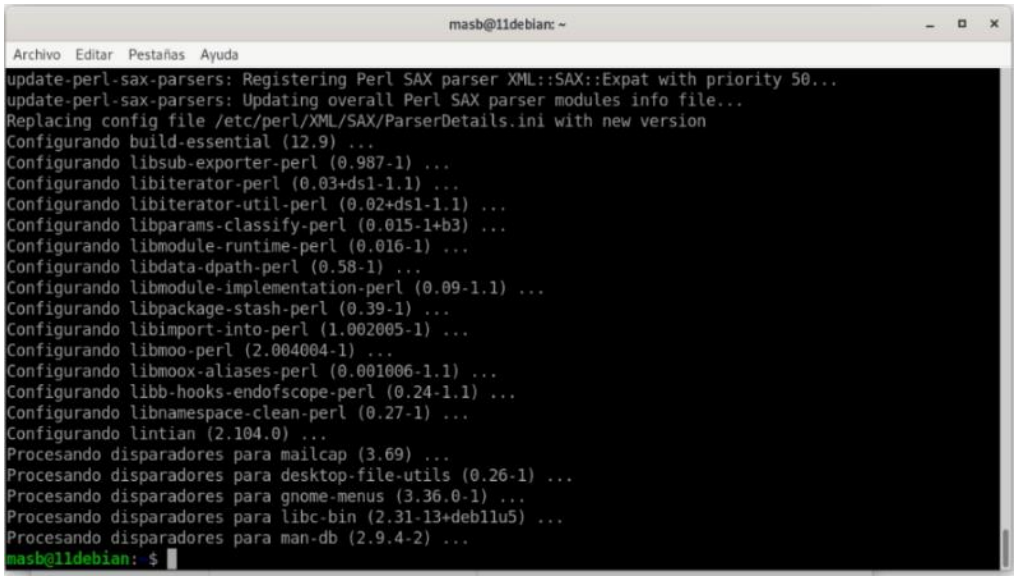


Para realizar la instalación con la aplicación gdebi, en el cliente Linux, en este caso Debian, ha sido necesaria la instalación de la aplicación, por lo que dentro de un terminal se ejecuta el comando sudo apt-get install gdebi

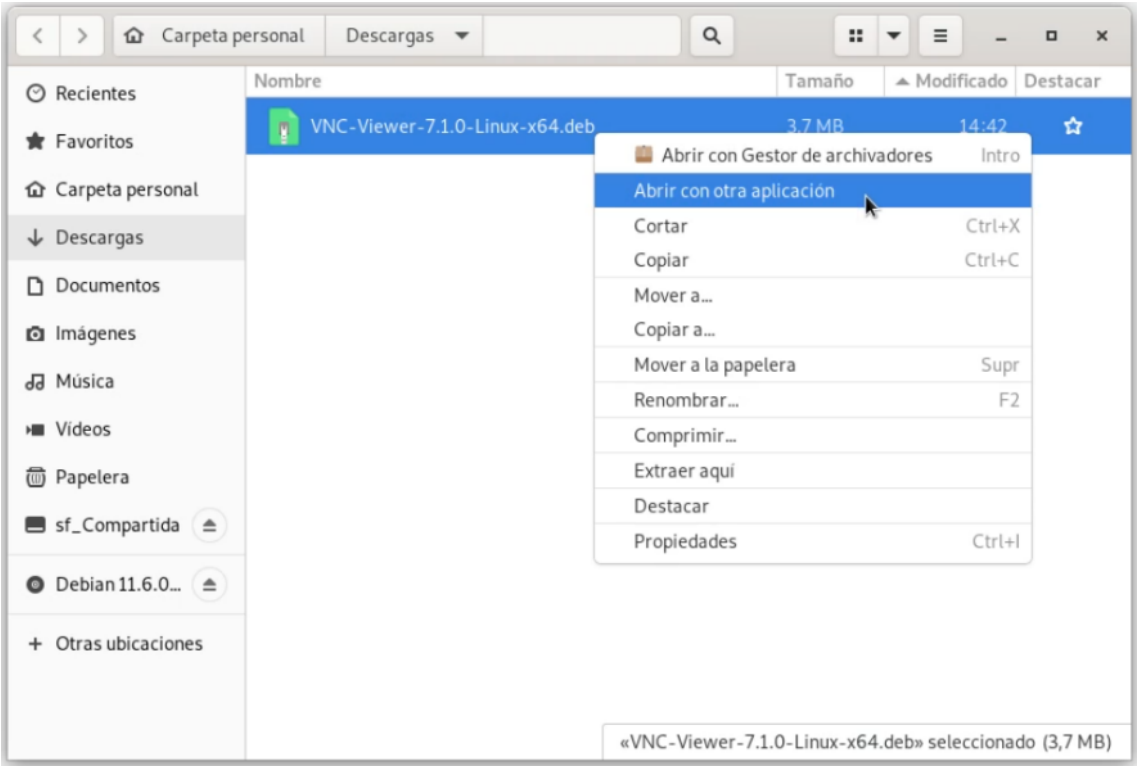
En caso de solicitarnos la contraseña de un usuario con permisos de instalación se facilitará y se pulsará INTRO.



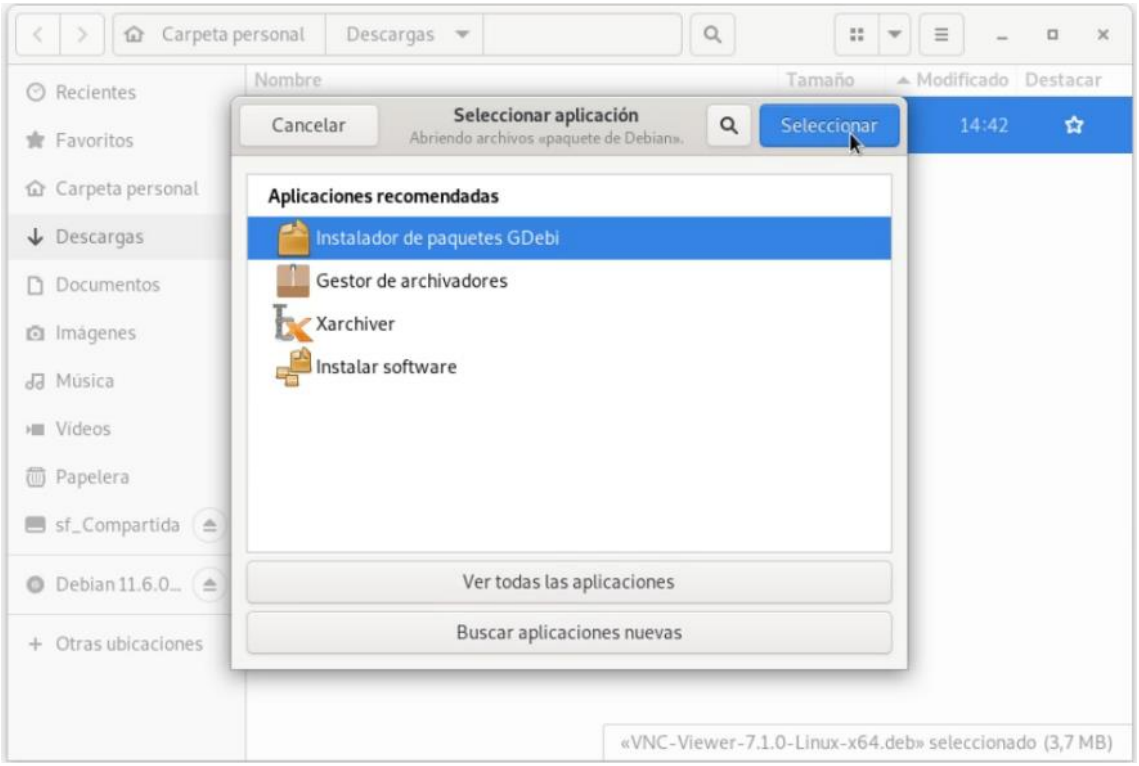
Como se puede apreciar en la ventana de la captura superior, existen dependencias a instalar además del propio software, por lo que se pulsara la tecla “S” y se pulsara INTRO.



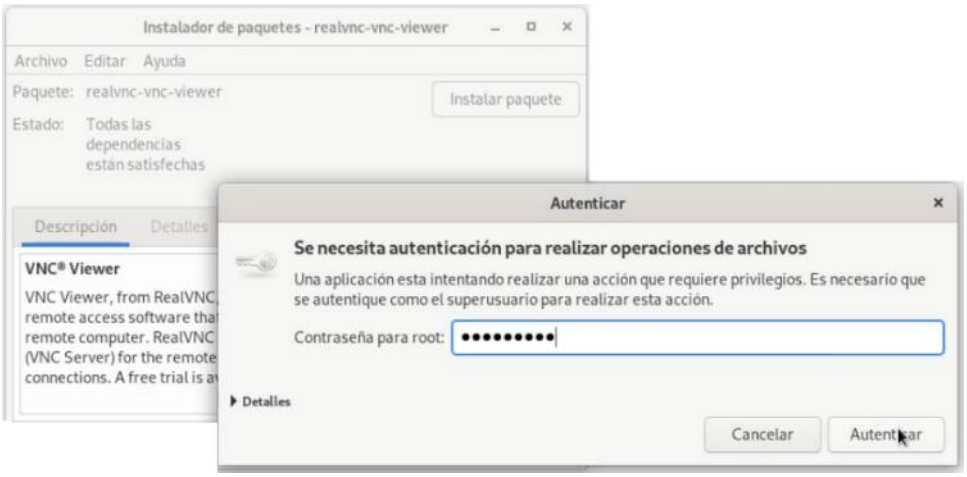
Finalizada la instalación, ya se dispondrá de la aplicación gdebi instalada en el S.O. cliente



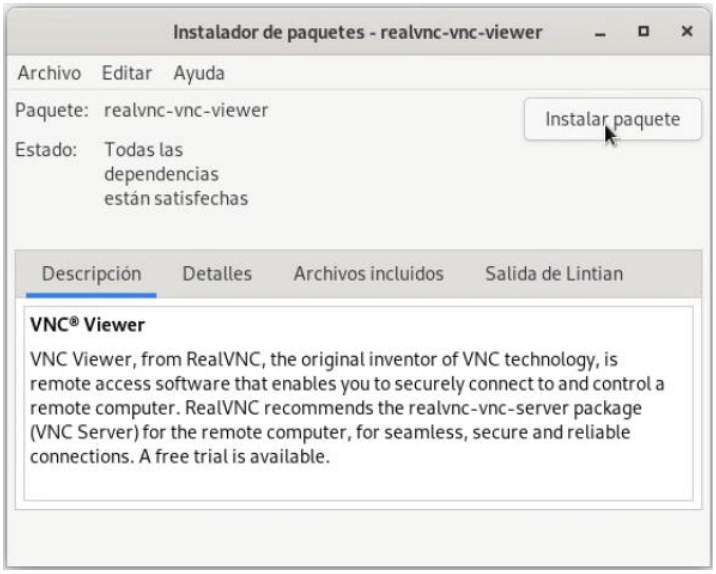
En el directorio de descarga, se pulsará con el botón derecho del ratón sobre el fichero descargado VNC-Viewer-7.1.0-Linux-x64.deb, en el menú que se muestra a continuación, se pulsará sobre Abrir con otra aplicación.



En el cuadro de dialogo que se abre, se seleccionará la opción Instalador de paquetes Gdebi y se pulsará sobre el botón superior derecho Seleccionar.



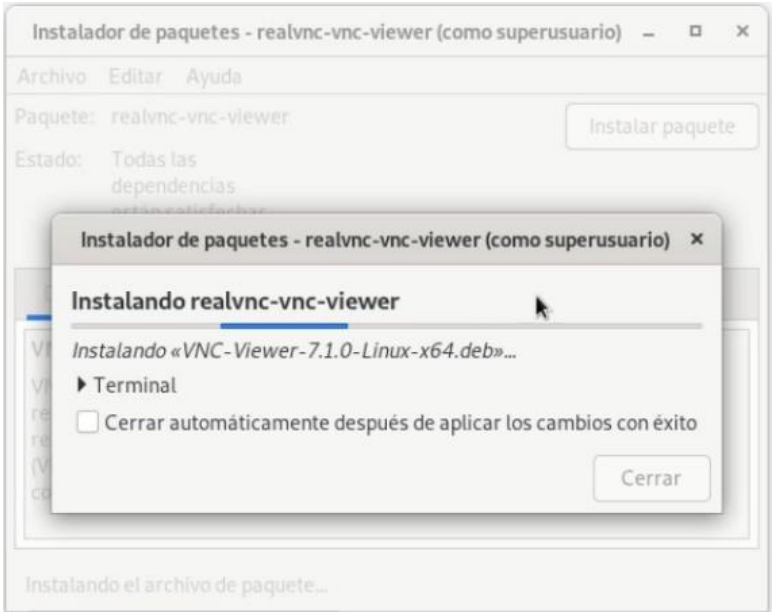
Se facilitará la contraseña del usuario para poder realizar la instalación.

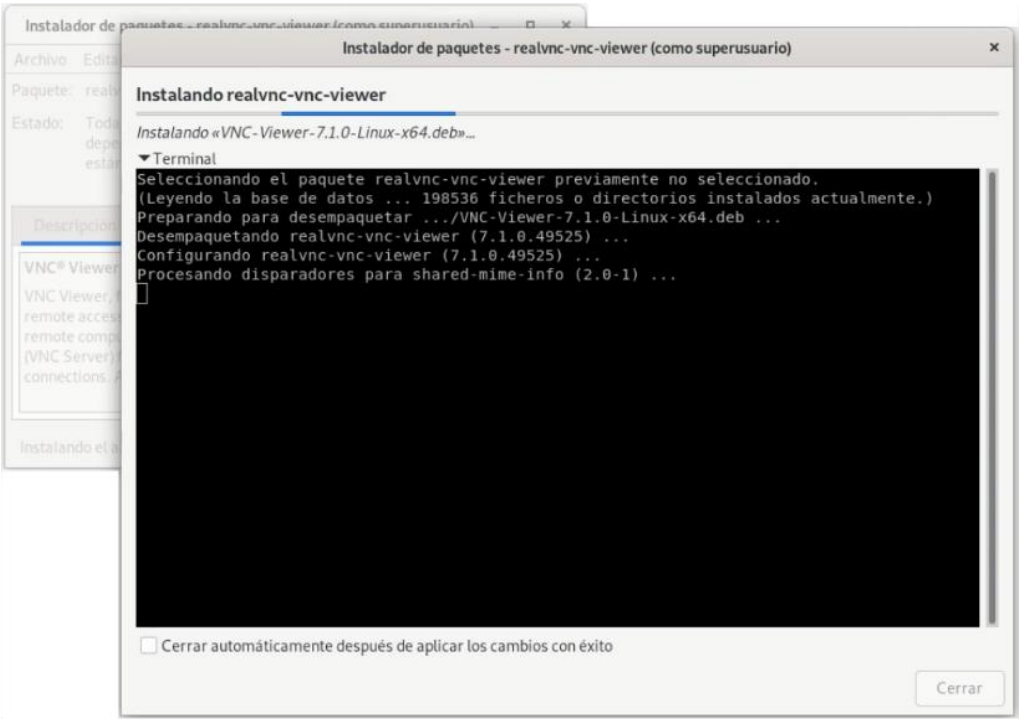


En la aplicación gdebi, y en el caso de tras finalizar la comprobación de la existencia de dependencias incumplidas sin mostrarse ningún error, se pulsará sobre el botón superior derecho Instalar paquete.

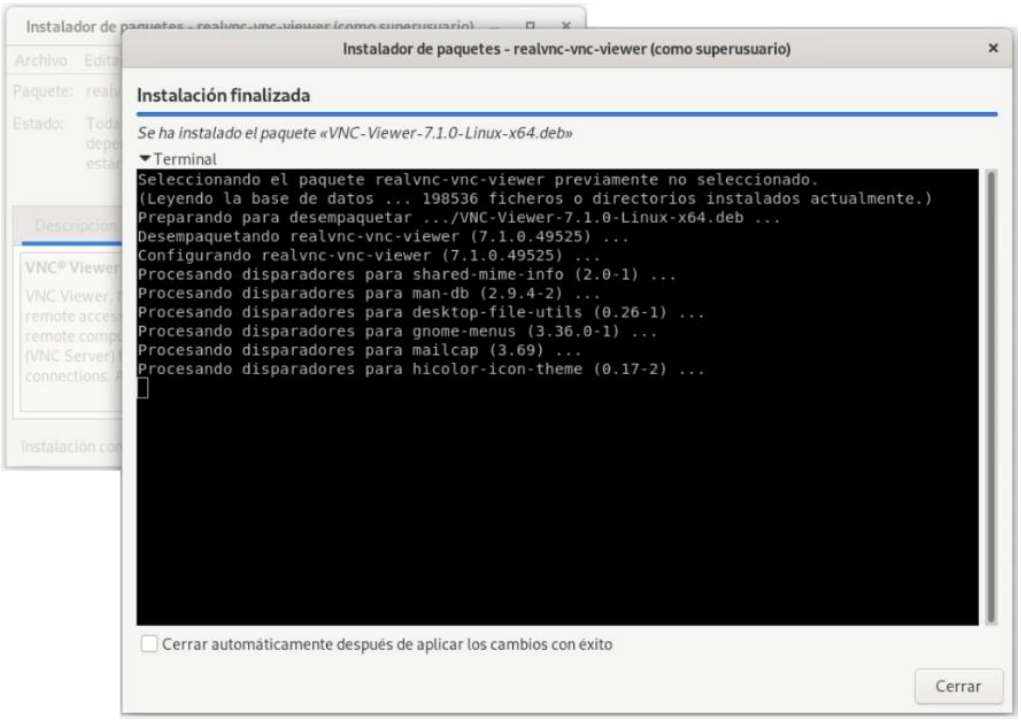


Puede que nuevamente se solicite la contraseña de un usuario con permisos de instalación, se facilitará la contraseña del usuario para poder realizar la instalación.

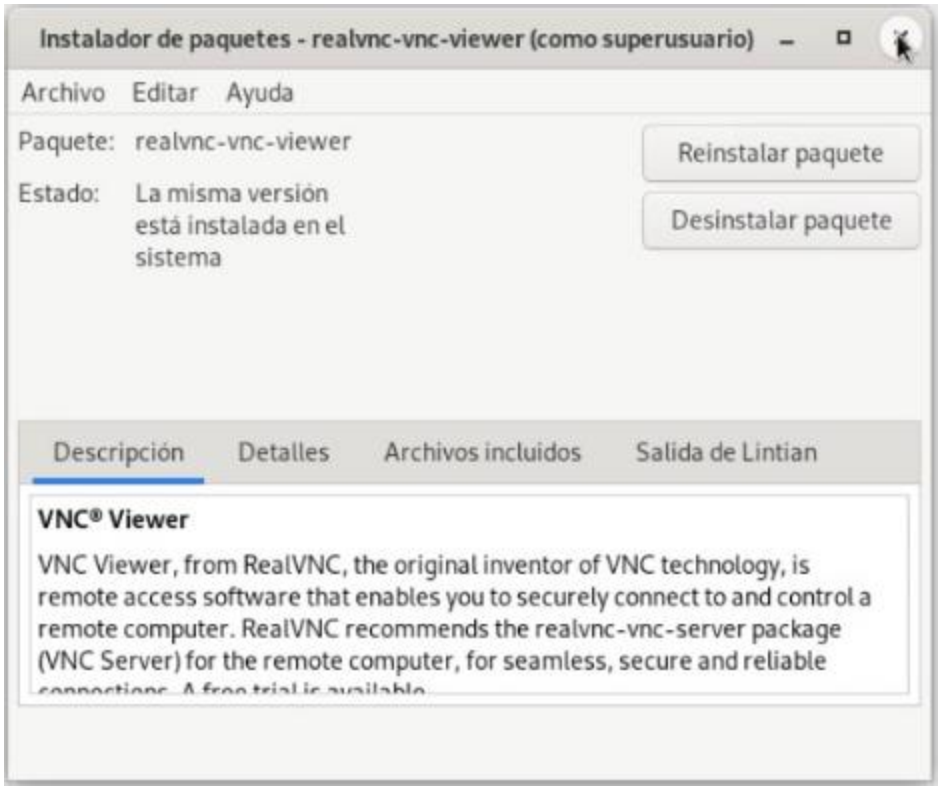




El proceso de instalación comenzará, pudiendo ver dicho proceso al pulsar en la flecha que apunta hacia abajo, delante de terminal, ▾Terminal.



Finalizada la instalación, se podrá cerrar la ventana del terminal pulsando sobre el botón inferior derecho Cerrar.

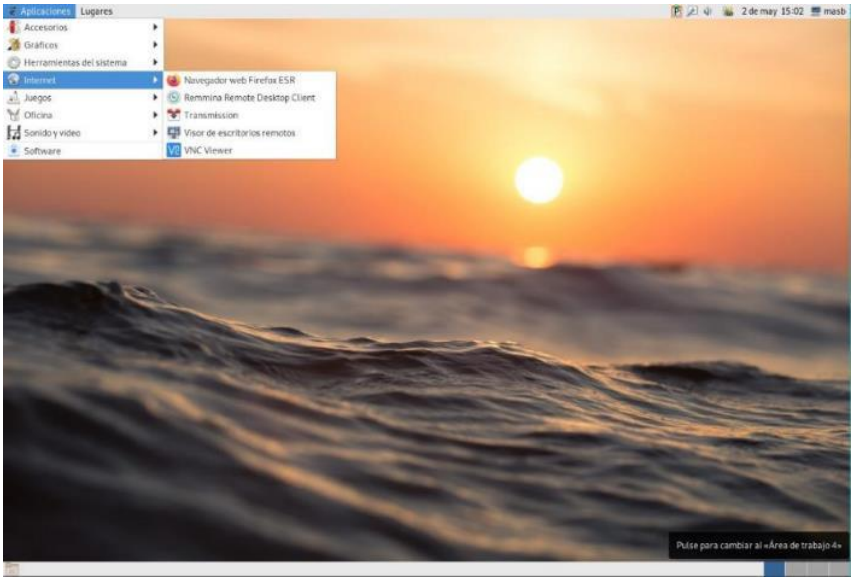


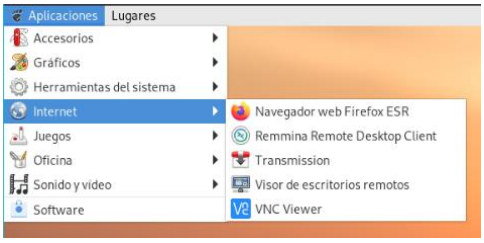
Pudiendo cerrar también la aplicación gdebi, pulsando sobre el icono superior derecho con forma de “X”, como se puede observar en la ventana de la captura superior.

Puede ser necesario reiniciar el equipo cliente para que se muestre el icono de acceso directo a la aplicación tras la instalación.

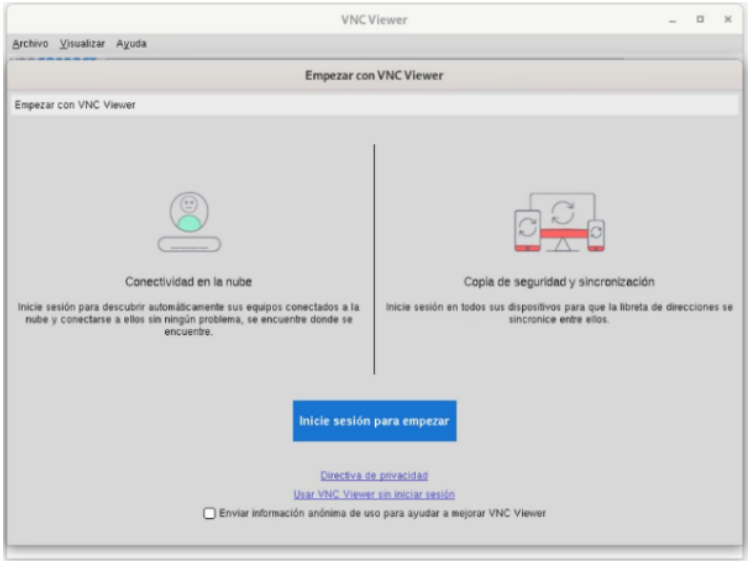
Configuración creación conexión S.O. Linux.

Puede ser necesario reiniciar el equipo cliente para que se muestre el icono de acceso directo a la aplicación tras la instalación.





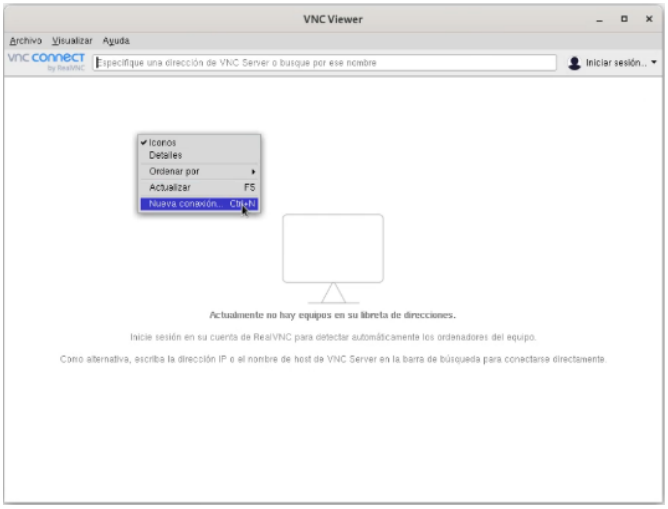
Una vez la aplicación se encuentra instalada, se abrirá pulsando en este ejemplo, en el menú superior Aplicaciones \ Internet \ VNC Viewer.



Se desmarcará la opción.

Enviar información anónima de uso para ayudar a mejorar VNC Viewer y se pulsará sobre las letras,
Usar VNC Viewer sin iniciar sesión.





Se podrá pulsar con el botón derecho del ratón dentro de la aplicación, en el menú que aparece se pulsará sobre Nueva conexión.

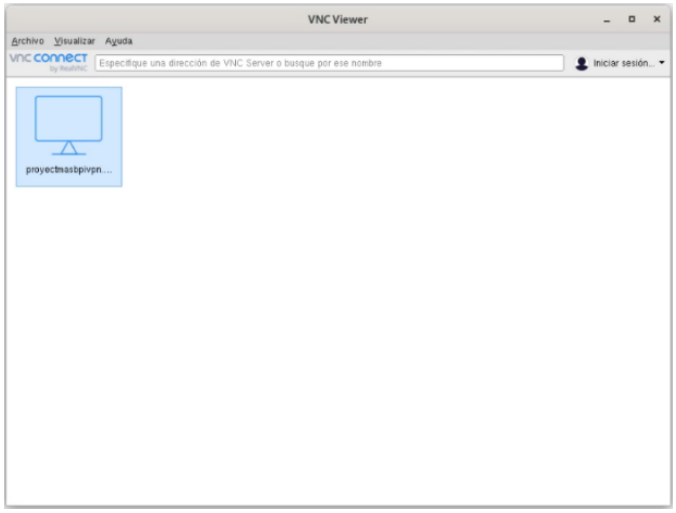


En la ventana de creación de la conexión, se facilitarán los datos indicados.

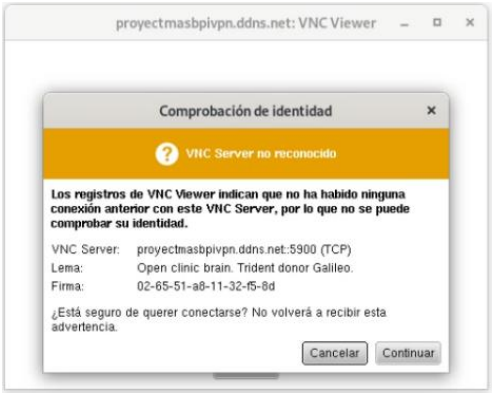
- VNC Server, en este caso, se utiliza el nombre de dominio o host creado en el proveedor de servicios DDNS, proyectmasbpivpn.ddns.net
- Nombre, en este caso, se utiliza el nombre de dominio o host creado en el proveedor de servicios DDNS, proyectmasbpivpn.ddns.net

Con los datos indicados rellenados, se pulsará sobre el botón inferior derecho Aceptar.

Conexión S.O. Linux.

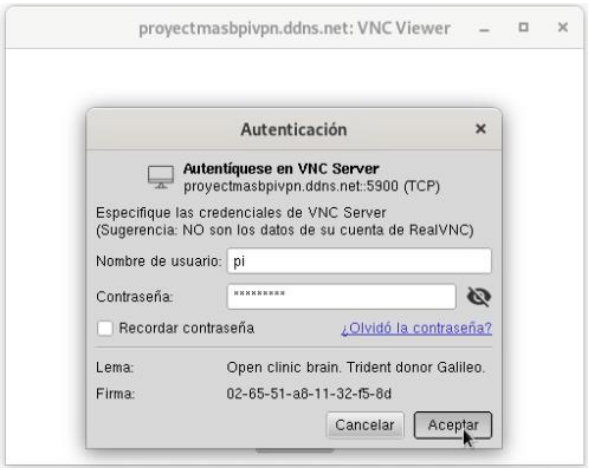


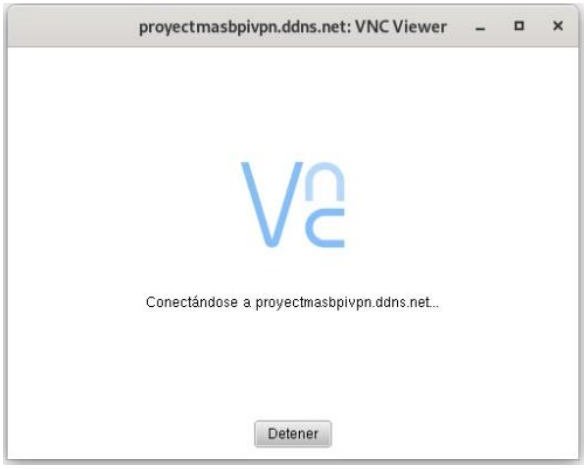
Dentro de la aplicación VNC Viewer, se podrá hacer doble clic con el botón izquierdo del ratón sobre la miniatura a la conexión creada, para comenzar el establecimiento de la conexión al equipo remoto, en este ejemplo se trata del servidor VPN/WOL.

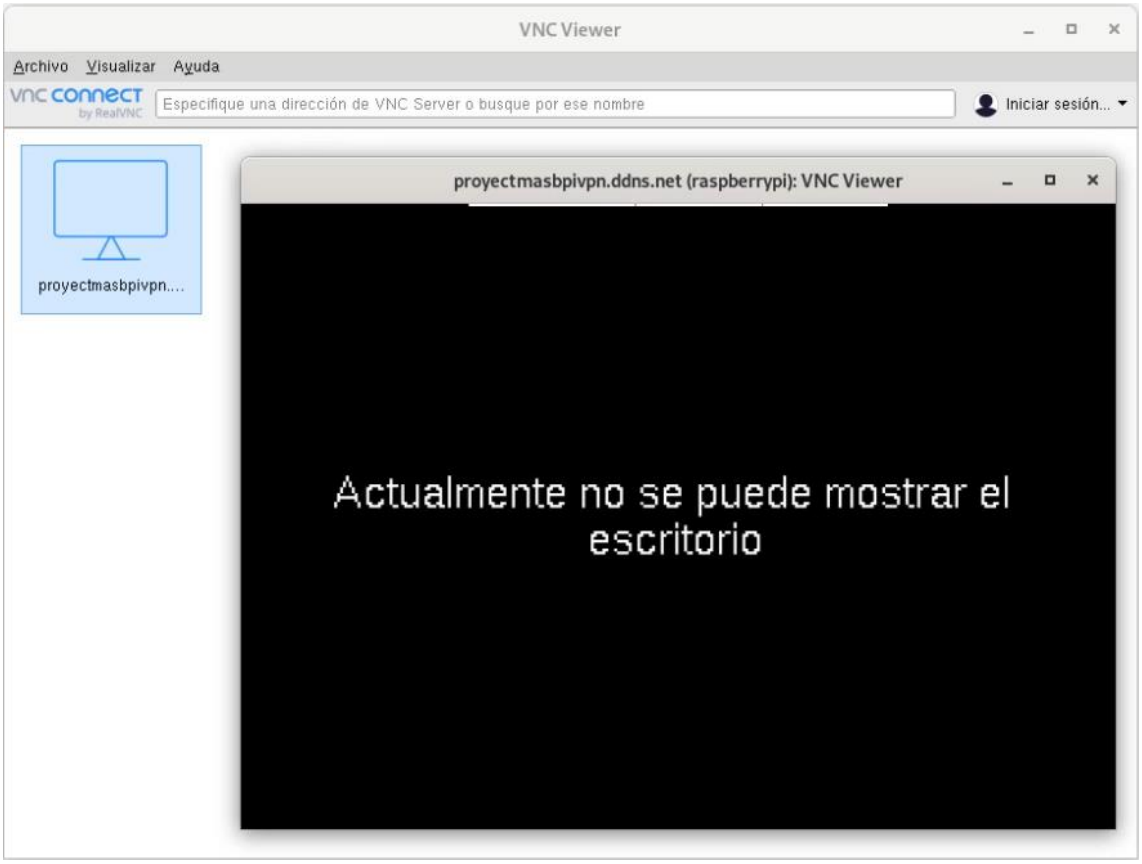


En la ventana Comprobación de identidad, se pulsará en el botón Continuar.

Se tendrá que facilitar las credenciales de un usuario valido, usuario y su contraseña, para poder establecer la conexión al escritorio remoto, posteriormente se pulsará Aceptar, en el caso de querer guardar estas credenciales, se marcará la opción Recordar contraseña.







Tras facilitar las credenciales correctas, se comienza a establecer la conexión con el escritorio remoto, en este ejemplo corresponde con el servidor VPN/WOL, como se puede observar en la ventana de la captura superior, en este caso, no se muestra el escritorio, al no encontrarse este activo en el servidor VPN/WOL, puesto que se configuró la Raspberry Pi para que arrancara en modo terminal y sin inicio de sesión automático.

Descarga en S.O. macOS.

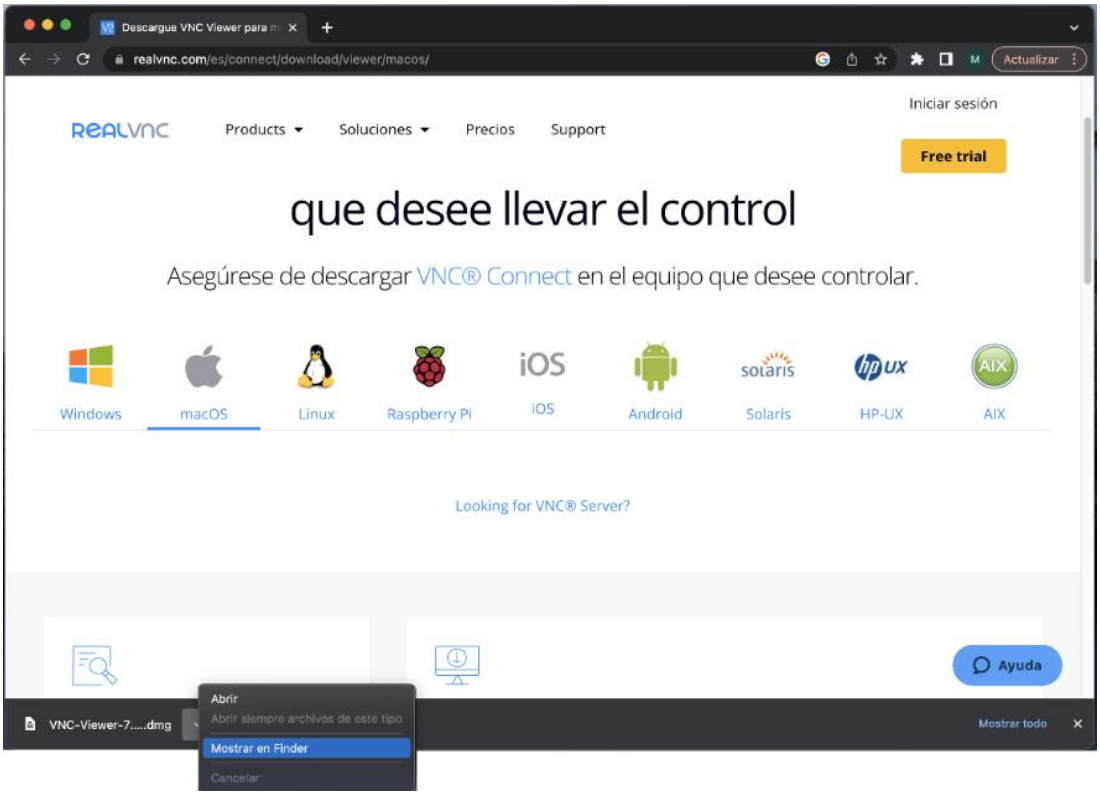


Dentro de la WEB oficial.

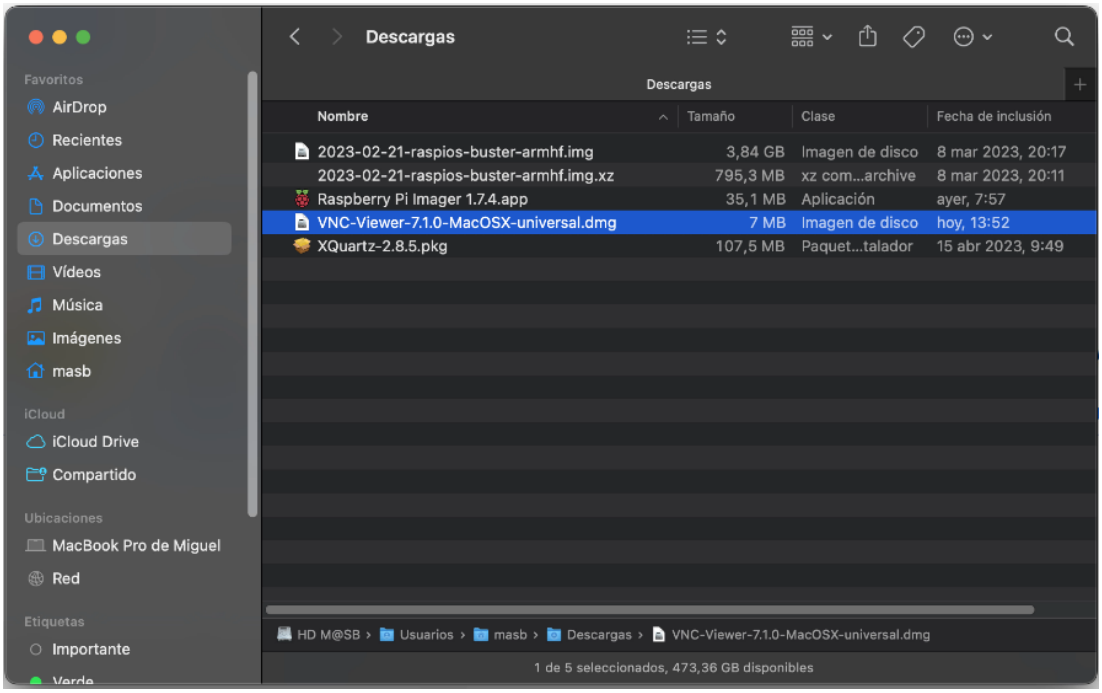
URL. https://www.realvnc.com/es/connect/download/viewer/



En este último ejemplo, se pulsará sobre el icono del S.O. macOS y posteriormente sobre el botón Descargue VNC Viewer.

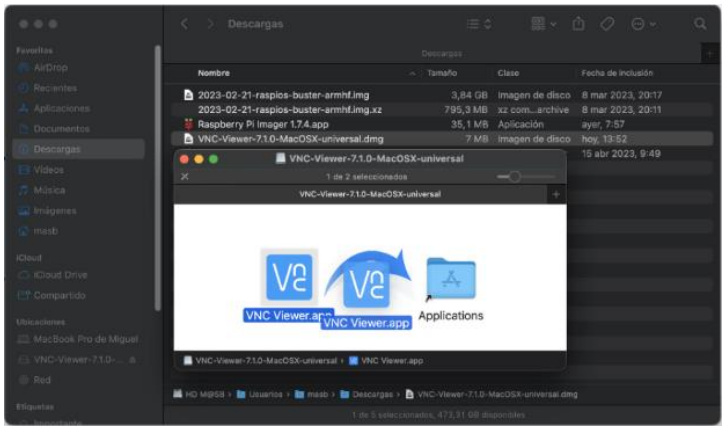


Descargado el fichero, dentro del navegador se pulsa en la flecha apuntando hacia abajo en la notificación de descarga del fichero, en el menú que se muestra se pulsará sobre Mostrar en Finder.

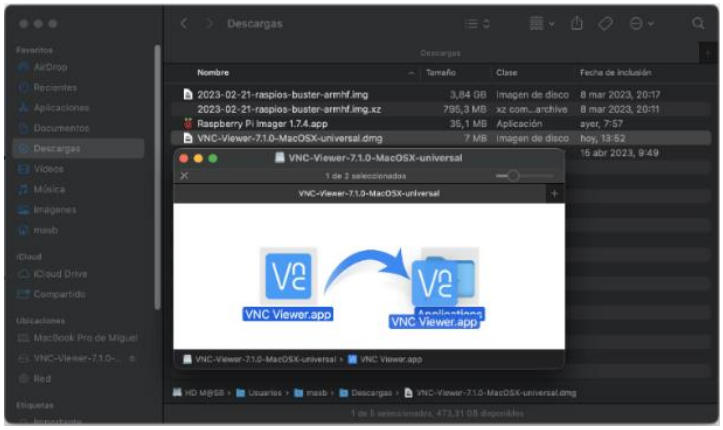


Fichero descargado VNC-Viewer-7.1.0-MacOSX-universal.dmg, ubicado en Descargas.

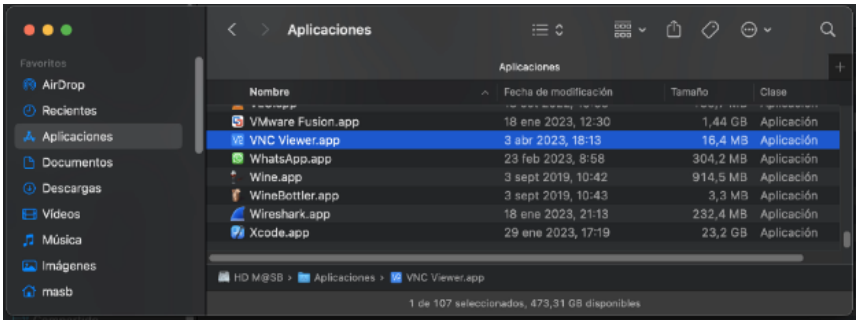
Instalación en S.O. macOS.



En el Finder, dentro de la carpeta Descargas, se hará doble clic con el botón izquierdo del ratón sobre el fichero descargado VNC-Viewer-7.1.0-MacOSX-universal.dmg, abriéndose el fichero imagen de la aplicación.

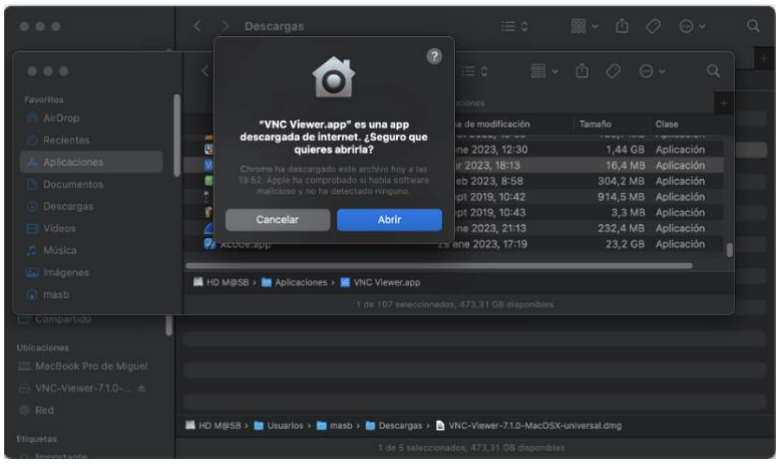


Con la imagen de disco abierta, se seleccionará con el botón izquierdo del ratón la aplicación VNC Viewer.app (izquierda), y sin soltar el botón izquierdo, se arrastrará la aplicación hacia el icono de la carpeta Applications (derecha), una vez se encuentre encima, se soltará el botón y la aplicación se copiará en la carpeta Aplicaciones.

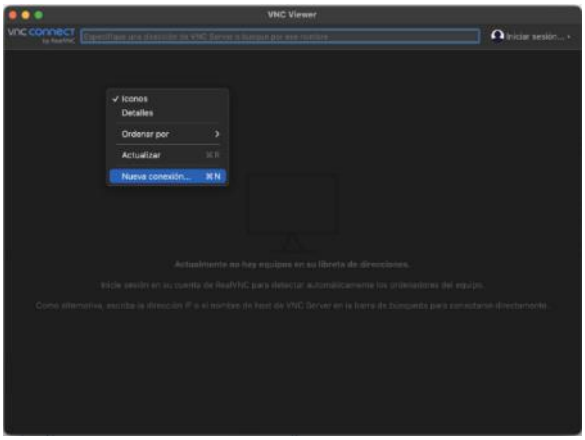


Aplicación VNC Viewer.app copiada en la carpeta Aplicaciones.

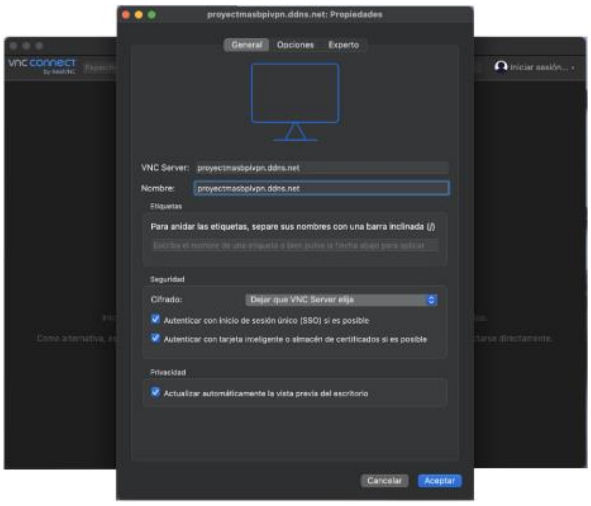
Configuración creación conexión S.O. macOS.



Con la aplicación dentro de Aplicaciones, al hacer doble clic con el botón izquierdo del ratón, en caso de aparecer la ventana que se muestra en la captura de la ventana superior, se pulsará sobre Abrir.



Dentro de la aplicación, se pulsará con el botón derecho del ratón en el área interna de la aplicación, en el menú que aparece, se pulsará sobre Nueva conexión…



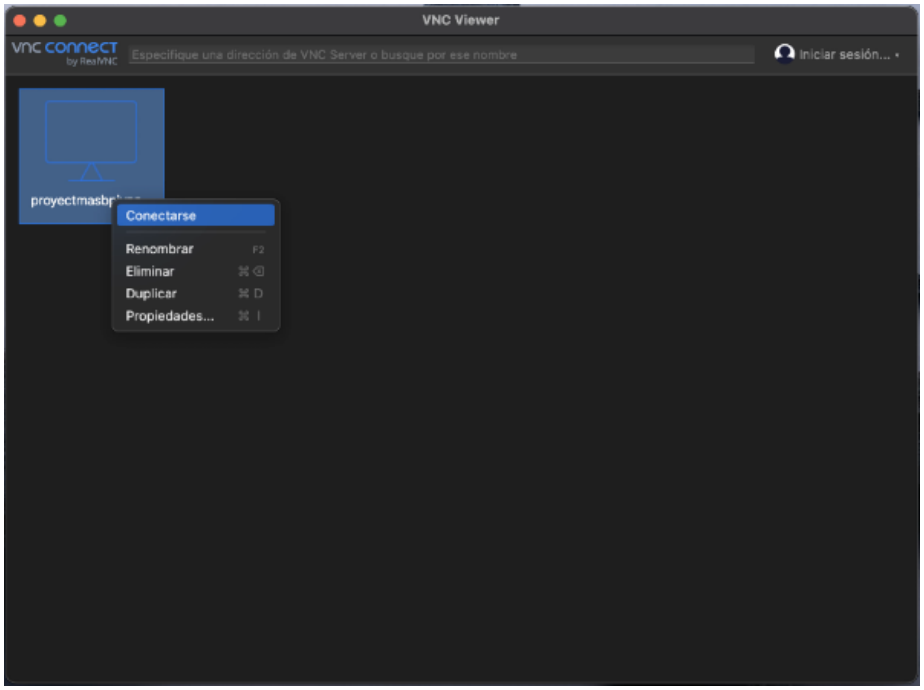


En la ventana de creación de conexión, se facilitarán los datos indicados.

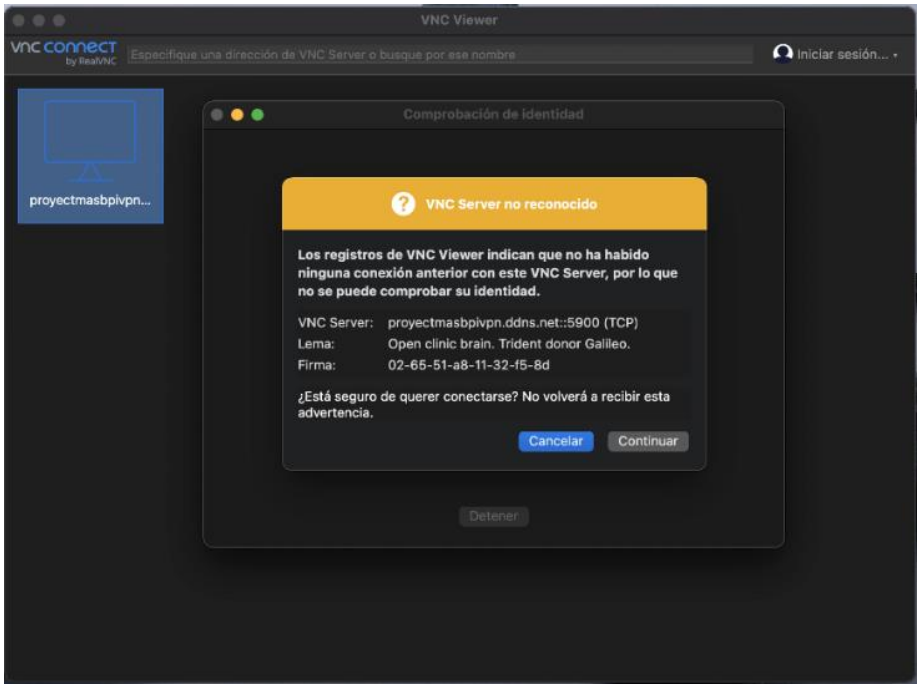
- VNC Server, en este ejemplo, se utiliza el nombre de dominio o host creado en el proveedor de servicios DDNS, proyectmasbpivpn.ddns.net
- Nombre, en este ejemplo, se utiliza el nombre de dominio o host creado en el proveedor de servicios DDNS, proyectmasbpivpn.ddns.net

Con los datos indicados rellenados, se podrá pulsar Aceptar, habiendo finalizado la configuración de la conexión.

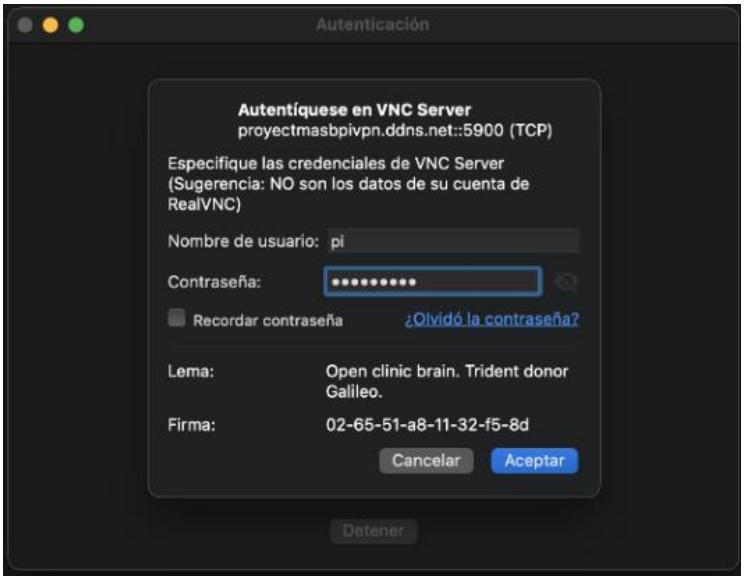
Conexión S.O. macOS.



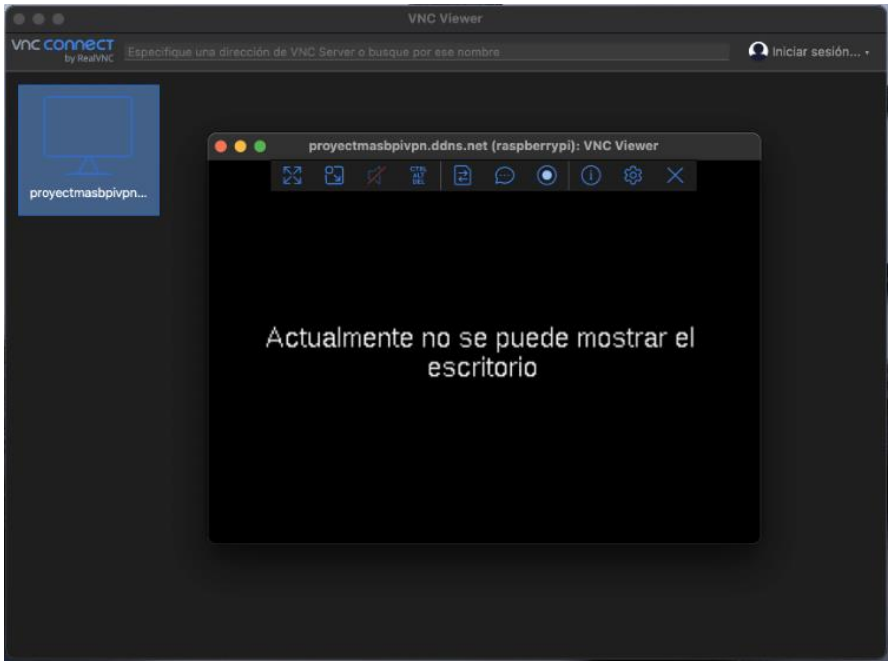
Con la aplicación Vnc Viewer abierta y con la conexión configurada, para establecer la conexión, se podrá pulsar con el botón derecho del ratón sobre la miniatura creada a la conexión, en el menú que aparece, se pulsará sobre Conectarse, o se puede hacer doble clic con el botón izquierdo del ratón sobre la miniatura creada a la conexión.



En la ventana VNC Server no reconocido, se pulsará sobre Continuar.

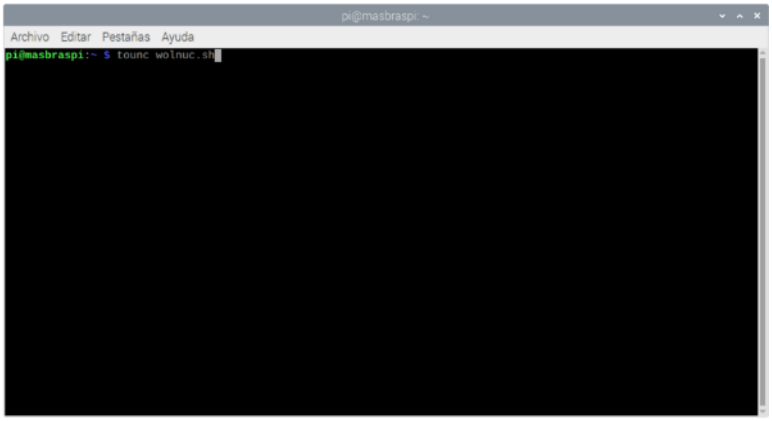


Se tendrá que facilitar las credenciales de un usuario valido para poder establecerse la conexión, proporcionado el usuario y la contraseña válidos, se pulsará Aceptar, en el caso de querer guardar estas credenciales, se marcará la opción Recordar contraseña.

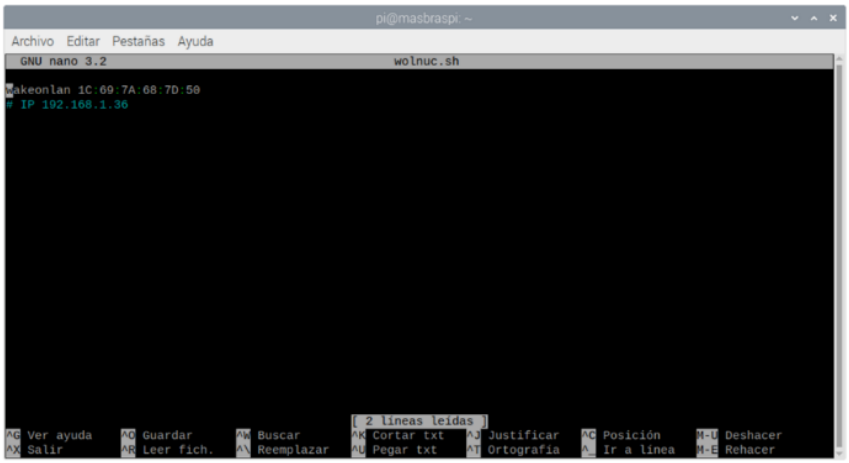


Tras facilitar las credenciales correctas, se comienza a establecer la conexión con el escritorio remoto, en este ejemplo corresponde con le servidor VPN/WOL, como se puede observar en la ventana de la captura superior, en este caso, no se muestra el escritorio, al no encontrarse este activo en el servidor VPN/WOL, puesto que se configuró la Raspberry Pi para que arrancara en modo terminal y sin inicio de sesión automático.

Configuración creación fichero arranque equipos wakeonlan local.



Como primer paso, se podrá crear el correspondiente fichero con el comando.
touch wolnuc.sh (y se pulsará INTRO).



Creado el fichero, se accederá al fichero para su modificación ejecutando el comando.

nano wolnuc.sh (y se pulsará INTRO).

Dentro de este fichero se escribirá.

Comando wakeonlan “espacio” MAC (Dirección MAC de la tarjeta de red).
En caso de colocar ““#”” almohadilla, lo que se escriba a la derecha de la almohadilla, se tomará como un comentario, no se tiene en cuenta.

#! /bin/sh (esta línea, en las pruebas no se ha colocado y la ejecución del fichero funciono correctamente, por lo que no se indica que sea necesaria).

Como puede observar en la imagen de la captura superior, este fichero solo tiene las siguientes líneas.

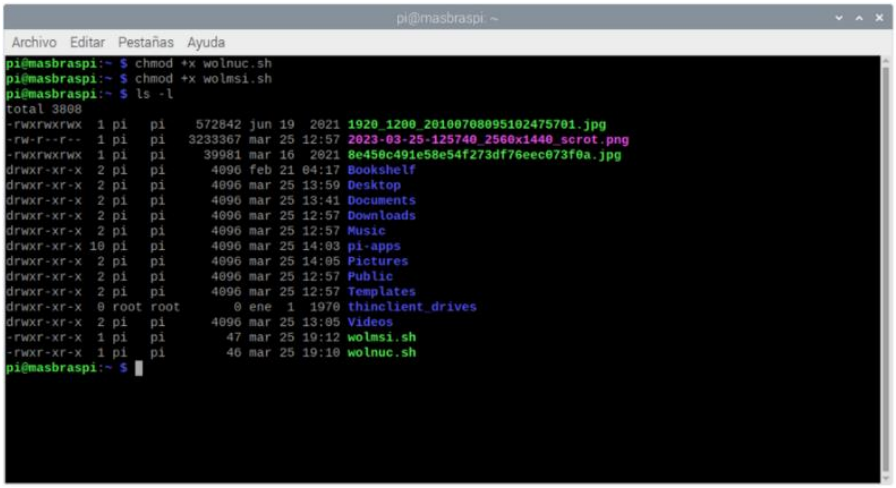
wakeonlan 7A:69: 1C:68:7D:50
IP 192.168.1.36

En este fichero, en caso de necesitar encender/arrancar varios equipos a la vez, se podrá colocar una línea por cada equipo a arrancar.

Como por ejemplo.

wakeonlan 70:90: 1C:88:5D:56
wakeonlan 7A:68: 1C:08:70:55
wakeonlan 7B:59: 1C:00:75:50
wakeonlan 03:9C:23:5C:6B:4B

Con los datos añadidos correctamente en el fichero, se pulsará la combinación de teclas CTRL (Control) y sin soltarla la tecla “O” para guardar el contenido, posteriormente CTRL (Control) y sin soltarla la tecla “X” para salir del editor nano.



Tras finalizar la creación del fichero y estando fuera del fichero, se tendrá que dar permisos de ejecución al/los ficheros creados con el comando.

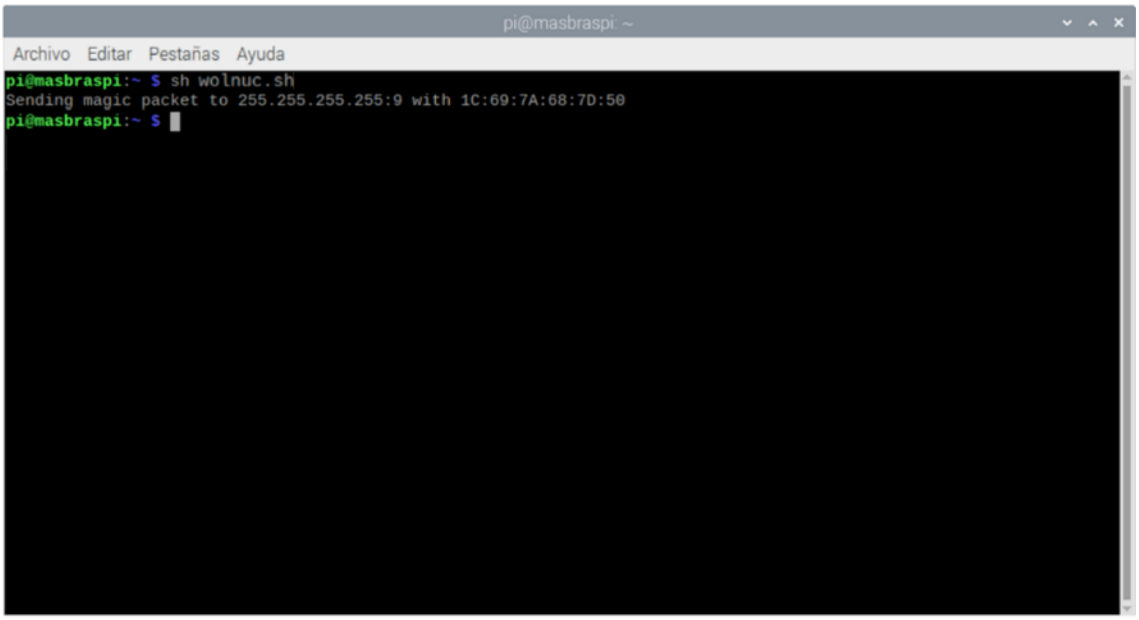
chmod +x wolnuc.sh
chmod +x wolmsi.sh

Para comprobar si los ficheros creados wolnuc.sh y wolmsi.sh tienen permiso de ejecución, con la ejecución del comando.

ls –l (si todo ha salido bien, tendría que salir el fichero en caso de estar configurado el color en el terminal, de color verde).



Si no se muestra de color verde, otra opción tras ejecutar el comando. ls -l, como se observa en la imagen superior, aparecerá una “X” en la posición del rectángulo rojo una por cada fichero creado y dado los permisos correspondientes.

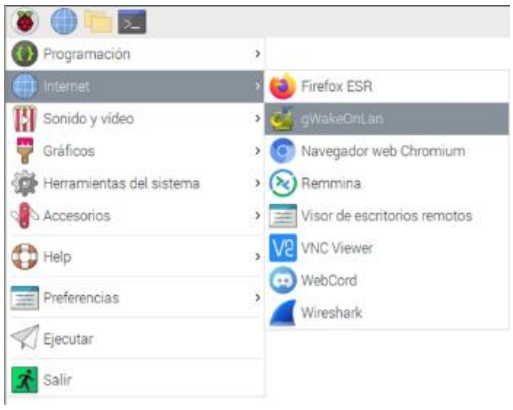


Con las acciones realizadas, para ejecutar el fichero, únicamente se tendrá que ejecutar el comando.

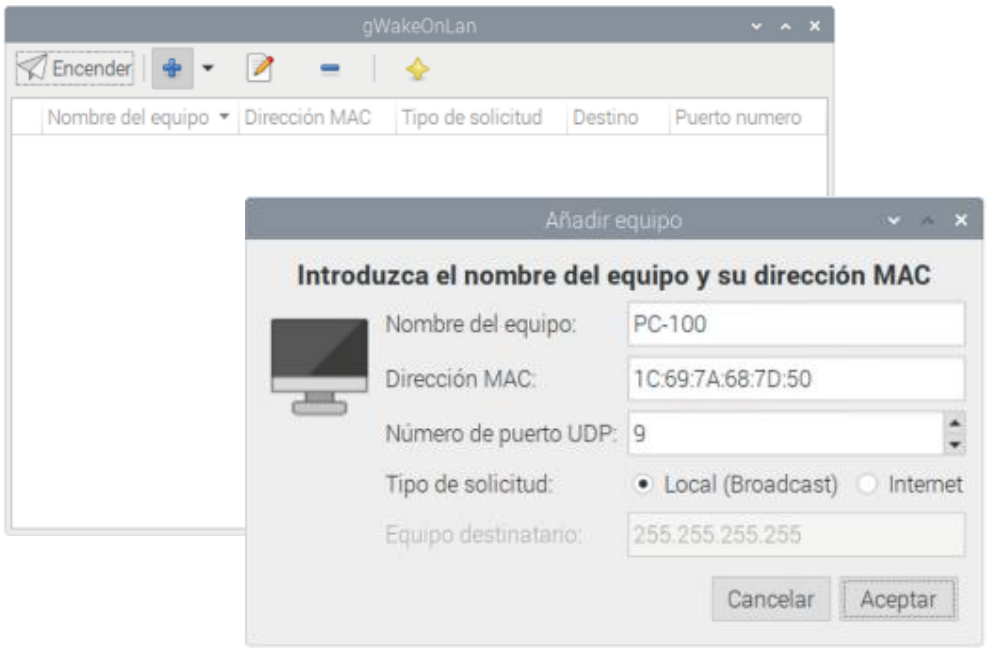
sh wolnuc.sh

Como se puede apreciar en la ventana de la captura superior, tras la ejecución del comando sh wolnuc.sh, se envía el “paquete mágico”.

Configuración creación fichero arranque Gwakeonlan Linux local.



Dentro del escritorio, en la sesión del usuario, en este caso el usuario pi, se pulsará sobre , ubicado en la barra superior izquierda, posteriormente se pulsará en Internet \ gWakeOnLan.

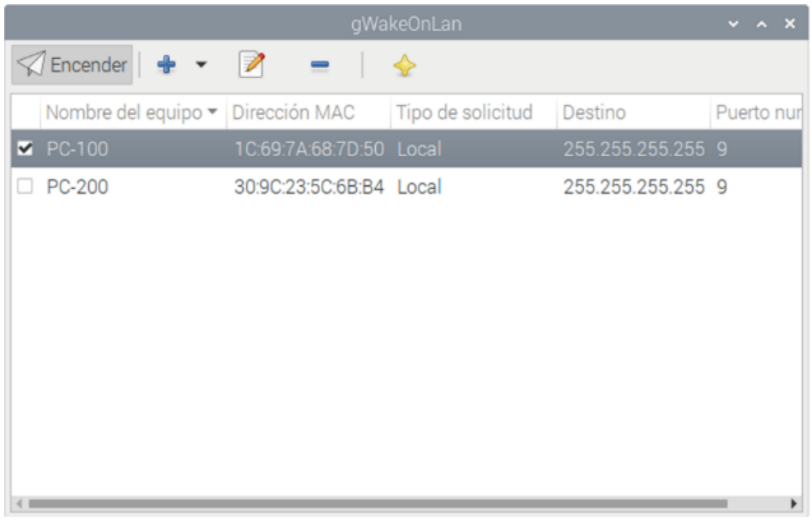


Dentro de la aplicación gráfica gWakeOnLan, se pulsará sobre el icono .

En la nueva ventana que aparece, se tendrá que colocar los datos necesarios.

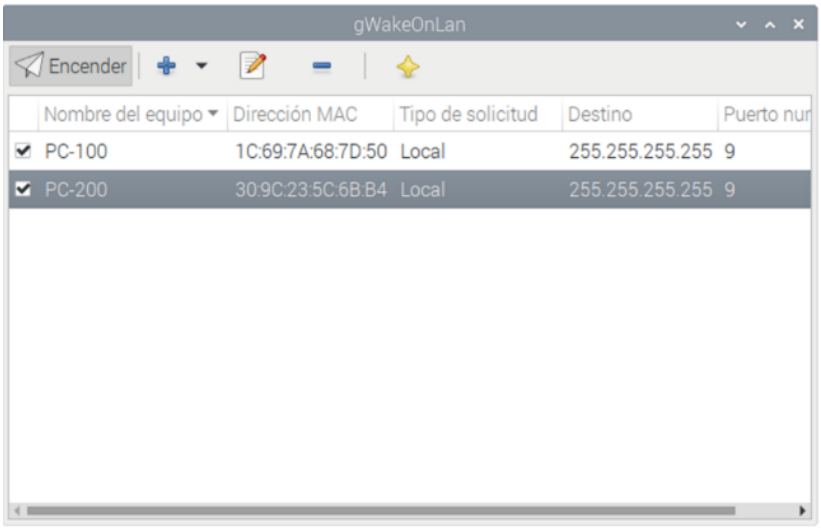
- Nombre del equipo: Nombre del equipo, en este ejemplo PC-100.
- Dirección MAC: Dirección MAC de la tarjeta de red del equipo que se está configurando, en este ejemplo 1C:69:7A:68:7D:50
- Número de puerto UDP: En este ejemplo no se modifica.
- Tipo de solicitud: En este ejemplo no se modifica.

Con los campos rellenados como se necesiten se pulsará sobre Aceptar.



Con la configuración creada, para encender un equipo, se seleccionará el que se desee encender y se pulsará sobre el botón superior Encender.

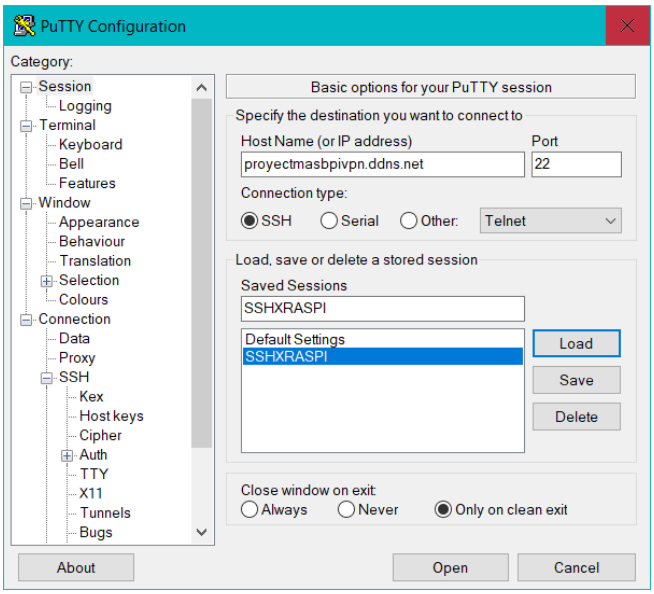
(Puede que sea necesario pulsar más de una vez sobre el botón Encender).



Si como en la ventana de la captura superior, se tiene más de un equipo configurado y se necesita encender más de un equipo a la vez, se seleccionarán los equipos a encender y posteriormente se pulsará sobre el botón Encender.

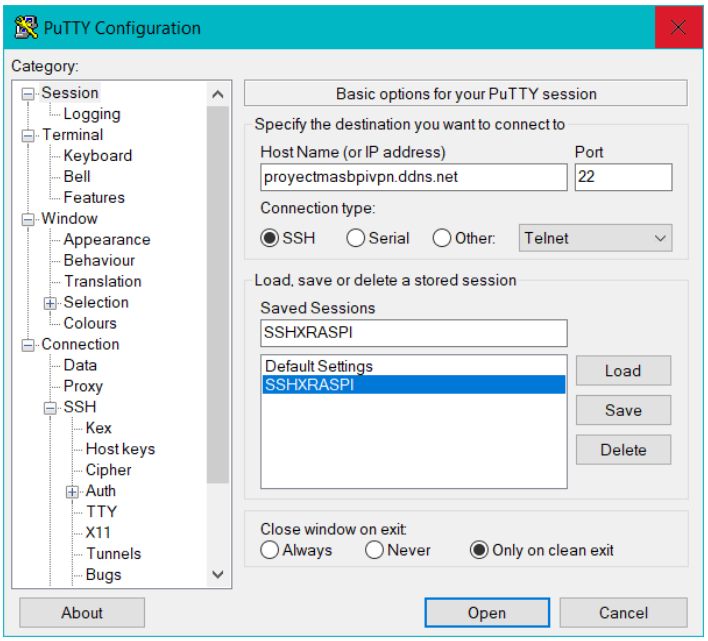
(Puede que sea necesario pulsar más de una vez sobre el botón Encender).

Creación fichero arranque equipos en terminal remoto.



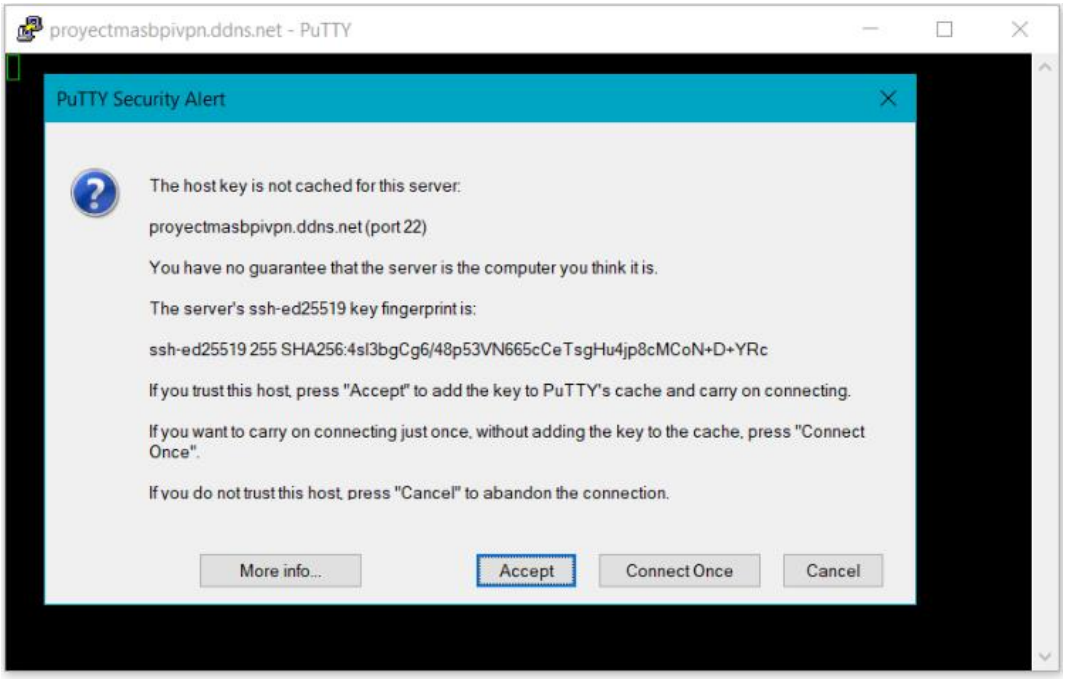
Para este ejemplo, se utiliza la misma explicación anterior en la que se explica la conexión vía SSH, puesto que realmente es lo mismo. Una vez abierta y dentro de la aplicación PuTTY, se selecciona la sesión guardada en el apartado Saved Sessions SSHXRASPI, ventana de la captura superior y se pulsará el botón Load.

Posteriormente, tras pulsar el botón Load, se carga automáticamente la configuración guardada de la conexión, se pulsará sobre el botón inferior Open, para establecer la conexión, imagen captura derecha.

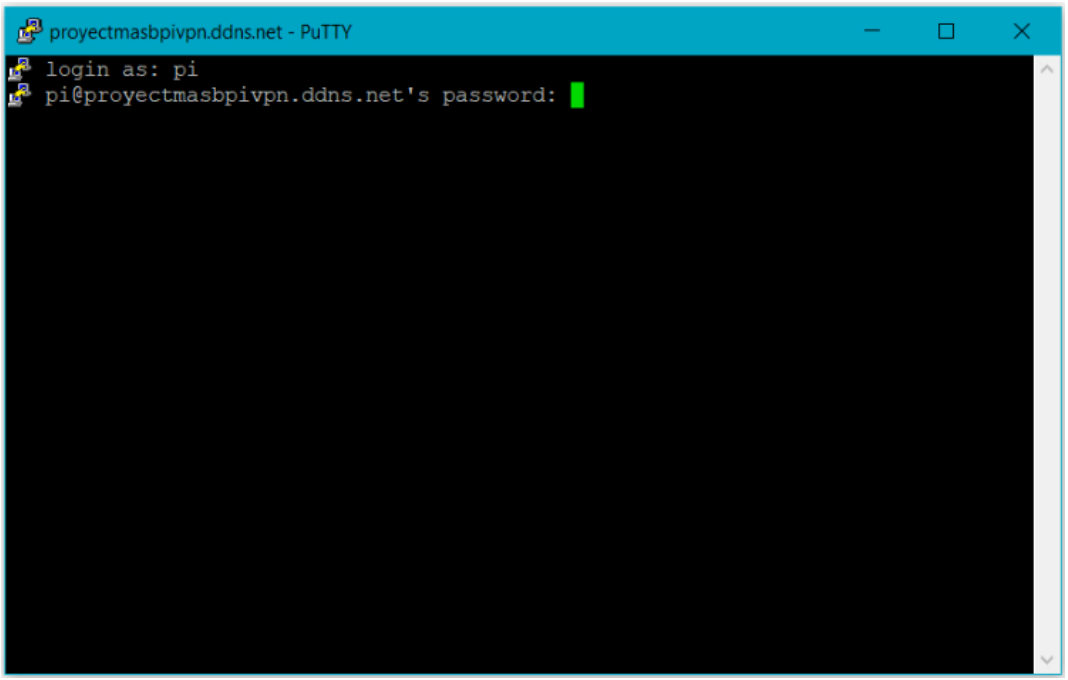


Si el establecimiento de la conexión se realiza en un terminal Linux o macOS, o en un Símbolo del sistema (CMD) Windows, se ejecutará el comando.

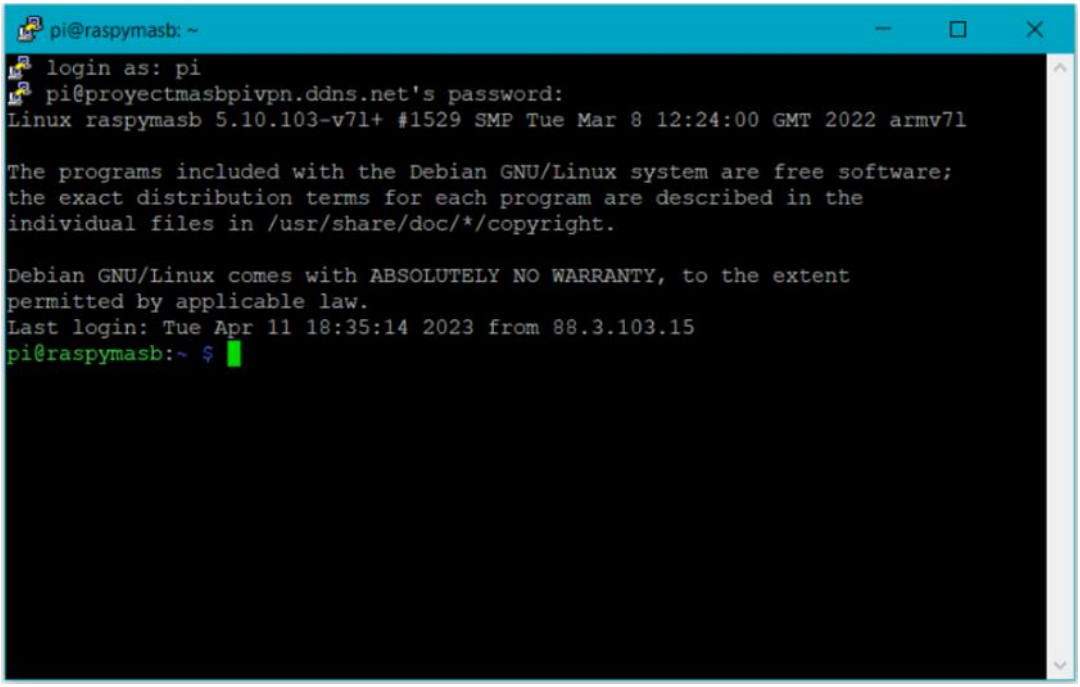
ssh -X pi@proyectmasbpivpn.ddns.net -p 22



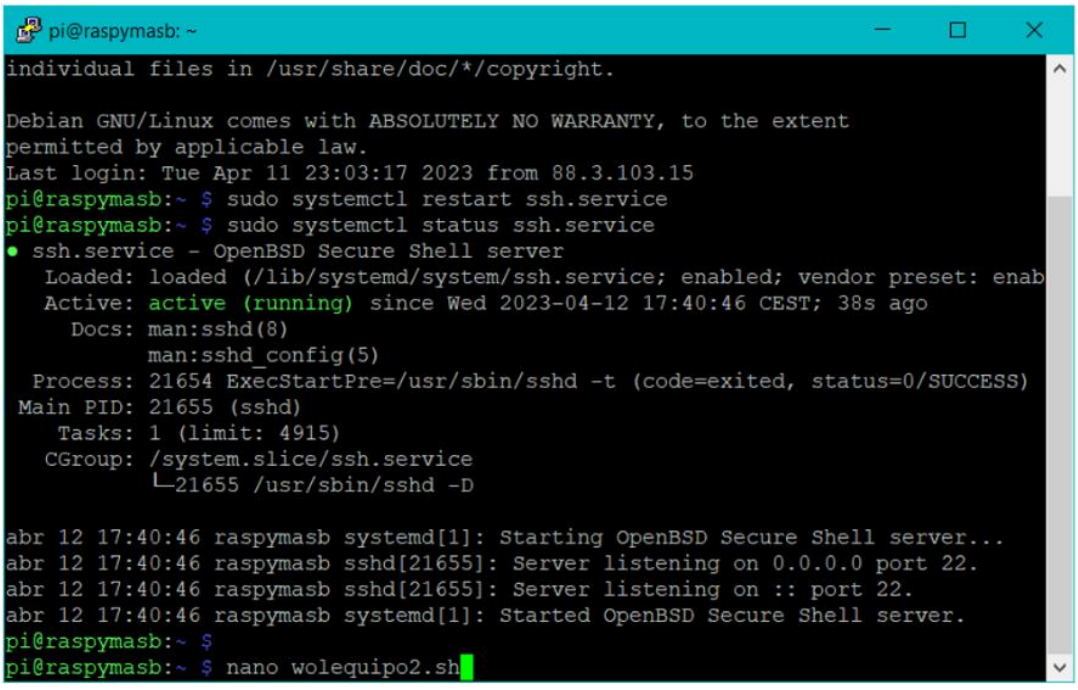
Si como en la captura de la ventana superior, es la primera vez que se establece la conexión con el servidor VPN/WOL, o el cliente, se mostrará la ventana que aparece, teniendo que pulsar sobre Accept.



Como se puede apreciar en la nueva ventana que aparece, al ya haber facilitado el usuario cuando se realizó la configuración y se guardó, al establecer la conexión solo habrá que facilitar la contraseña del usuario en cuestión, para este proyecto el usuario es pi, tras facilitar la contraseña, se pulsará INTRO.

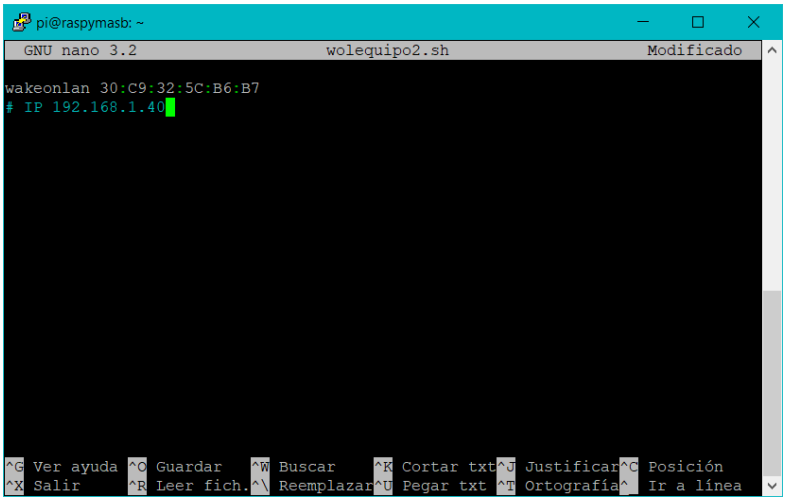


Una vez facilitada la contraseña y habiendo pulsado INTRO, se estará remotamente conectado en un terminal vía SSH a la Raspberry Pi.



Dentro de este terminal, para crear el fichero que se utilizará para iniciar al/los equipos que se tengan que arrancar para posteriormente poderse conectarse a los equipos, se utilizará el siguiente comando para la creación del fichero.

nano wolequipo2.sh



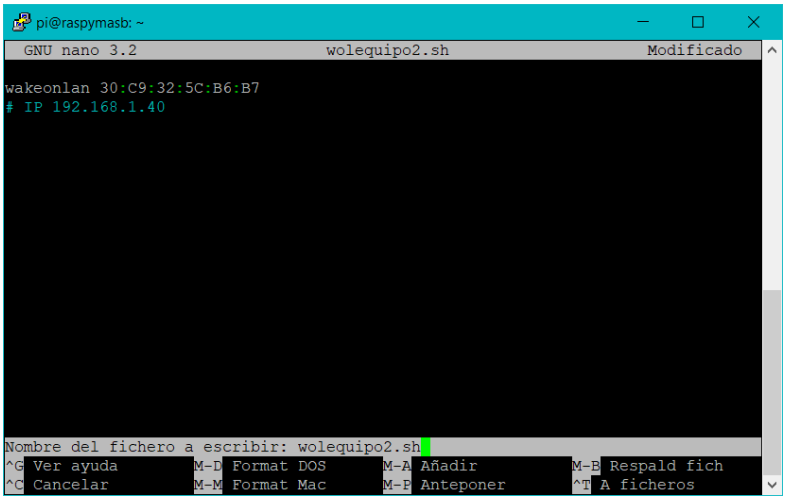
Dentro de este fichero se escribirá.

Comando wakeonlan “espacio” MAC (Dirección MAC de la tarjeta de red).
En el caso de colocar ““#”” almohadilla, lo que se escriba a la derecha de la almohadilla, se tomara como un comentario, no teniéndose en cuenta.

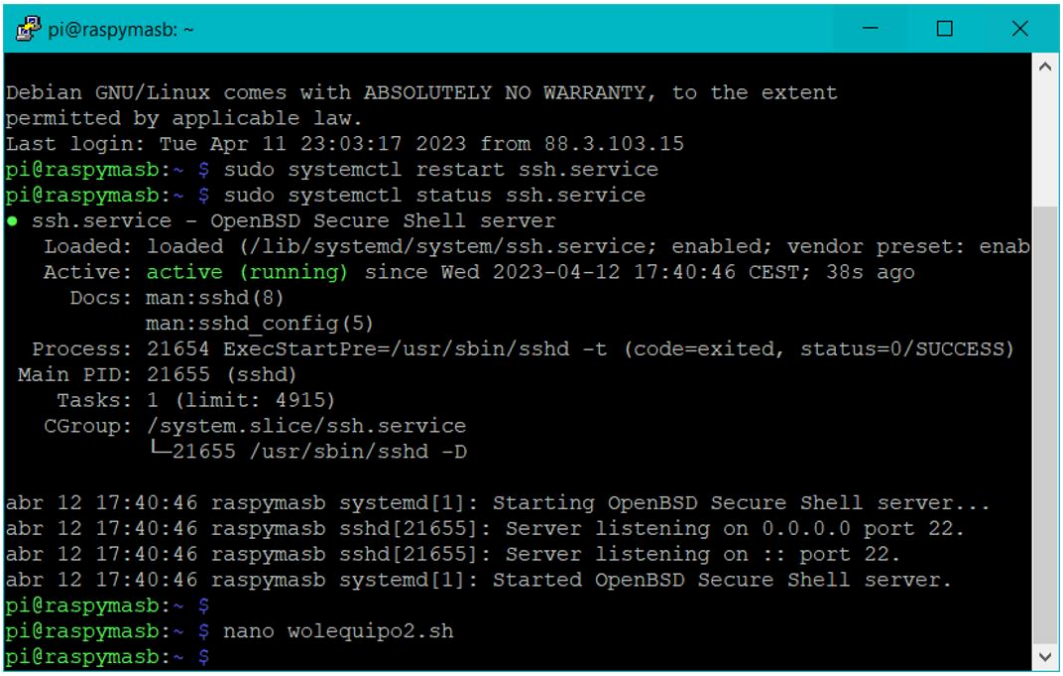
#! /bin/sh (esta línea, en las pruebas no se ha colocado y la ejecución del fichero funciono correctamente, por lo que no se indica que sea necesaria).

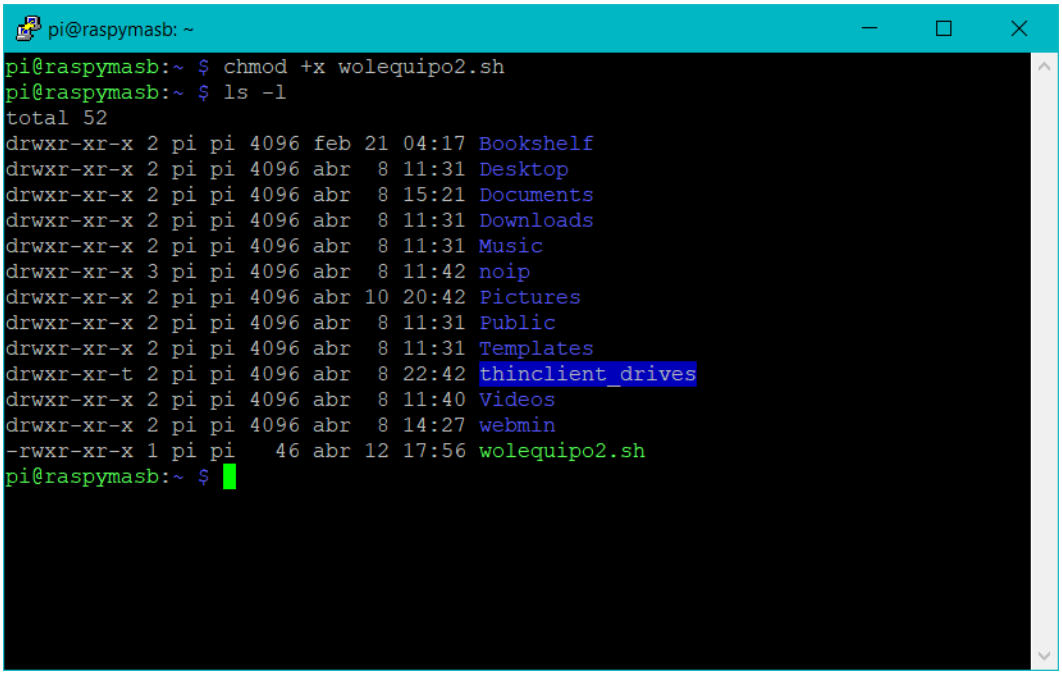
Como puede observar en la imagen de la captura superior, este fichero solo tiene las siguientes líneas.

wakeonlan 30:C9:32:5C:B6:B7
IP 192.168.1.40



Con los datos añadidos correctamente, se pulsará la combinación de teclas CTRL (Control) y sin soltarla la tecla “O” para guardar el contenido, posteriormente CTRL (Control) y sin soltarla la tecla “X” para salir del editor nano.



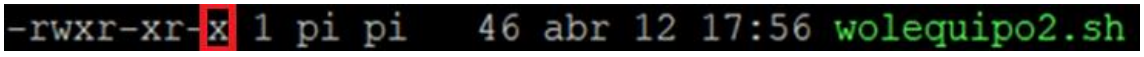


Se podrá limpiar el terminal con el comando.
clear

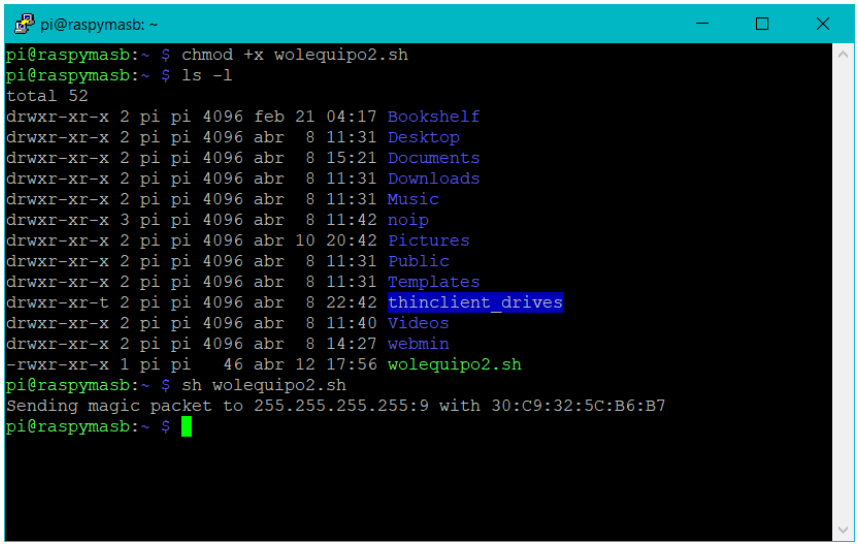
Acto seguido, para dar permisos de ejecución al fichero wolequipo2.sh, se ejecuta el comando

chmod +x wolequipo2.sh

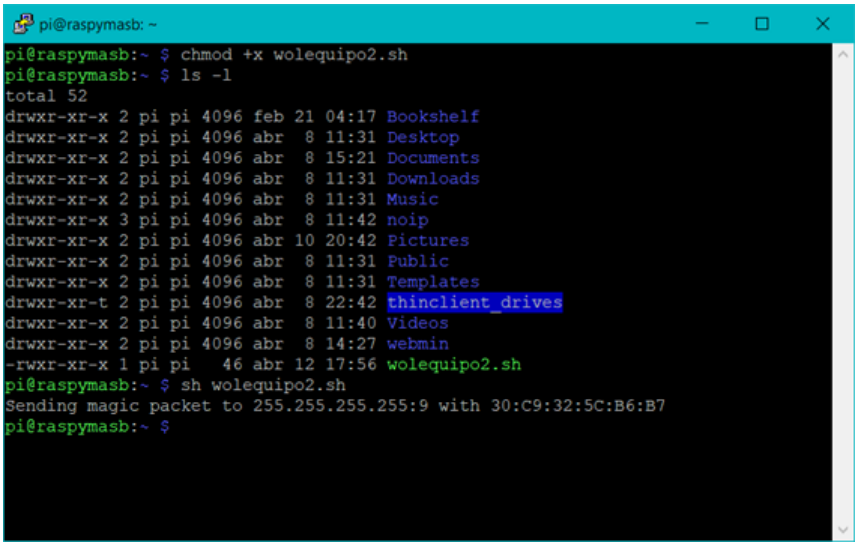
Para comprobar si el fichero wolequipo2.sh tiene el permiso de ejecución, con el comando.
ls –l (si todo ha salido bien, tendría que aparecer el nombre del fichero en caso de estar configurado el color en el terminal, de color verde).



Si no se muestra de color verde el nombre del fichero al ejecutar el comando ls -l, como se observa en la imagen superior, aparecerá una “X” en la posición del rectángulo rojo.

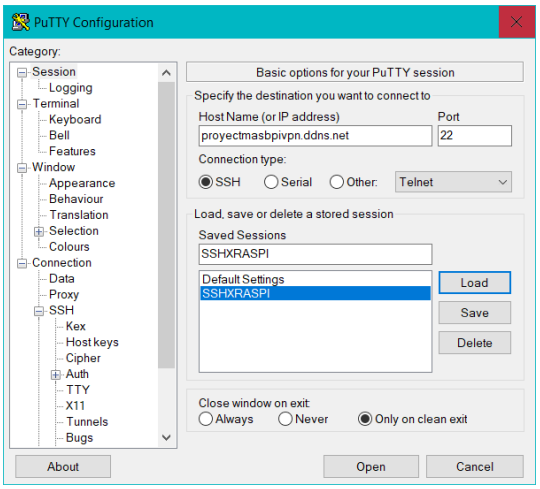


Terminada la creación del fichero, para proceder a su ejecución, tan solo habrá que ejecutar el comando.
sh wolequipo2.sh



Para terminar con este ejemplo, tras ejecutar el comando sh wolequipo2.sh, se puede apreciar en la ventana de la captura superior, como se envía el “paquete mágico” a la dirección MAC indicada, con lo que el equipo en cuestión, si se encuentra correctamente configurado arrancara y comenzara la carga del S.O.

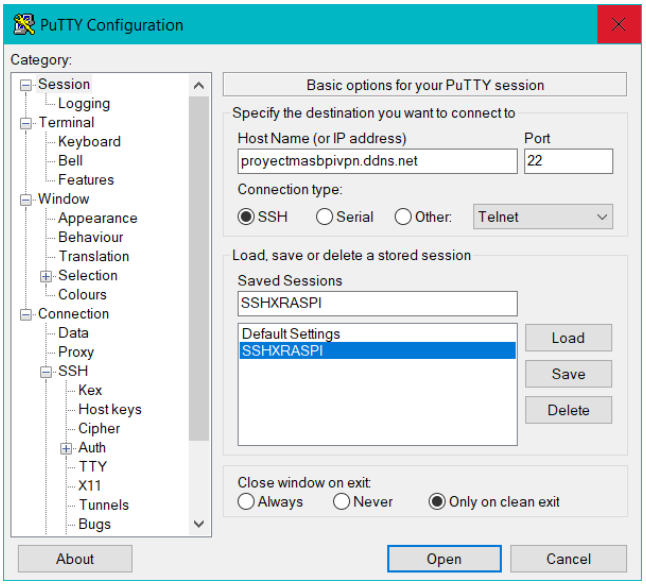
Creación fichero arranque equipos entorno gráfico Linux remoto.



Siempre para este tipo de conexión, en equipos con el S.O. Windows, es necesario tener instalada y en ejecución la aplicación Xming, ejecutando la aplicación XLaunch, para que la aplicación instalada en el servidor VPN/WOL, se pueda ejecutar en el escritorio del equipo con S.O. Windows, a través de la conexión SSH.

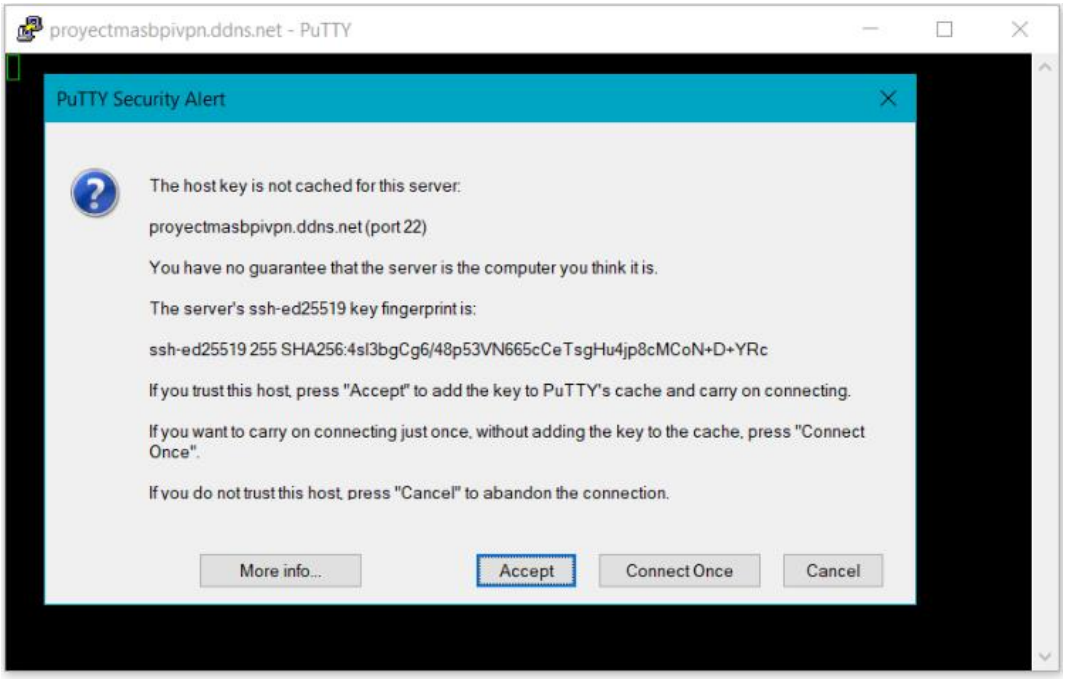
Para este ejemplo, se utiliza la misma explicación anterior, en la que se explica la conexión vía SSH, puesto que realmente es lo mismo. Una vez abierta y dentro de la aplicación PuTTY, se selecciona la sesión guardada en el apartado Saved Sessions SSHXRASPI, ventana de la captura superior y se pulsará el botón Load.

Posteriormente, tras pulsar el botón Load, se cargará automáticamente la configuración guardada de la conexión, se pulsará sobre el botón inferior Open, para establecer la conexión, imagen captura derecha.

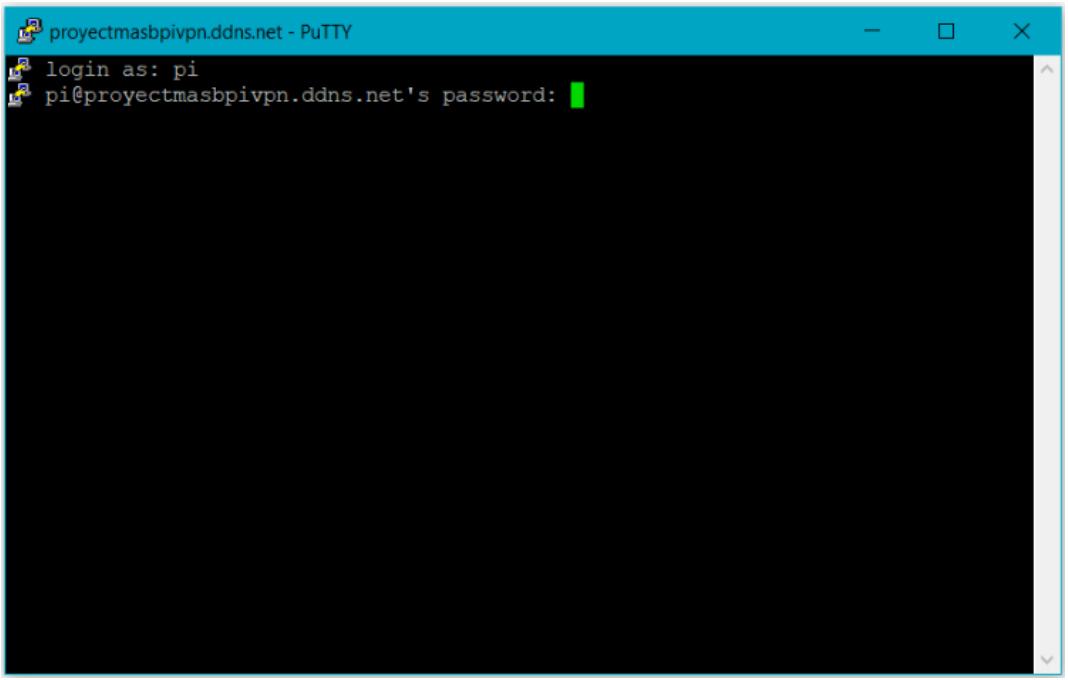


Si el establecimiento de la conexión se realiza en un terminal Linux o macOS, o en un Símbolo del sistema (CMD) Windows, se ejecutará el comando.

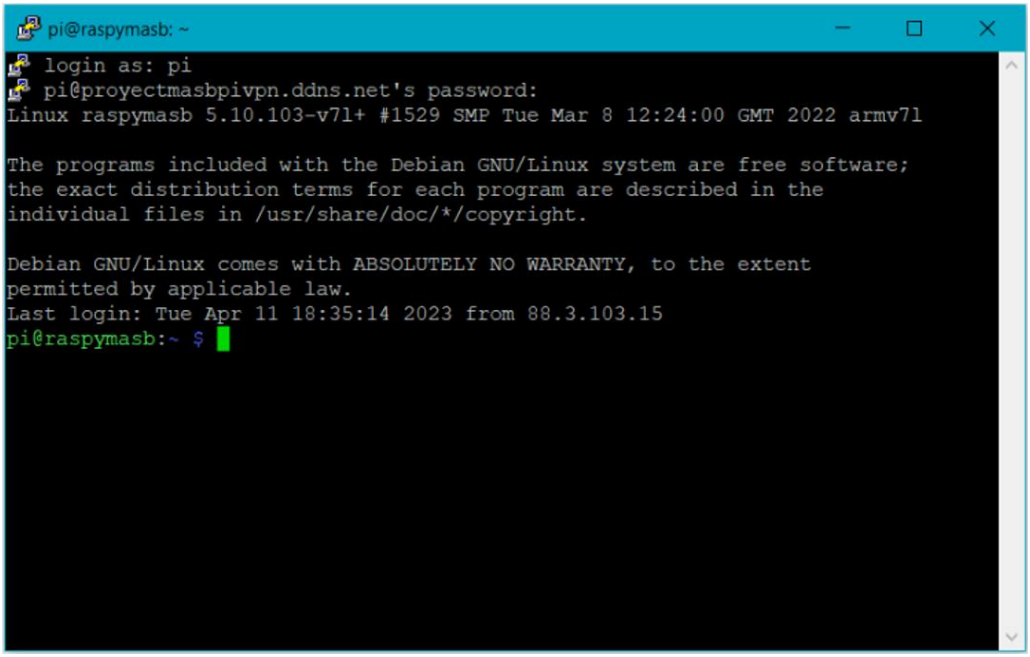
ssh -X pi@proyectmasbpivpn.ddns.net -p 22



Si como en la captura de la ventana superior, es la primera vez que se establece la conexión con el servidor VPN/WOL, o el cliente, se mostrará la ventana que aparece, teniendo que pulsar sobre Accept.

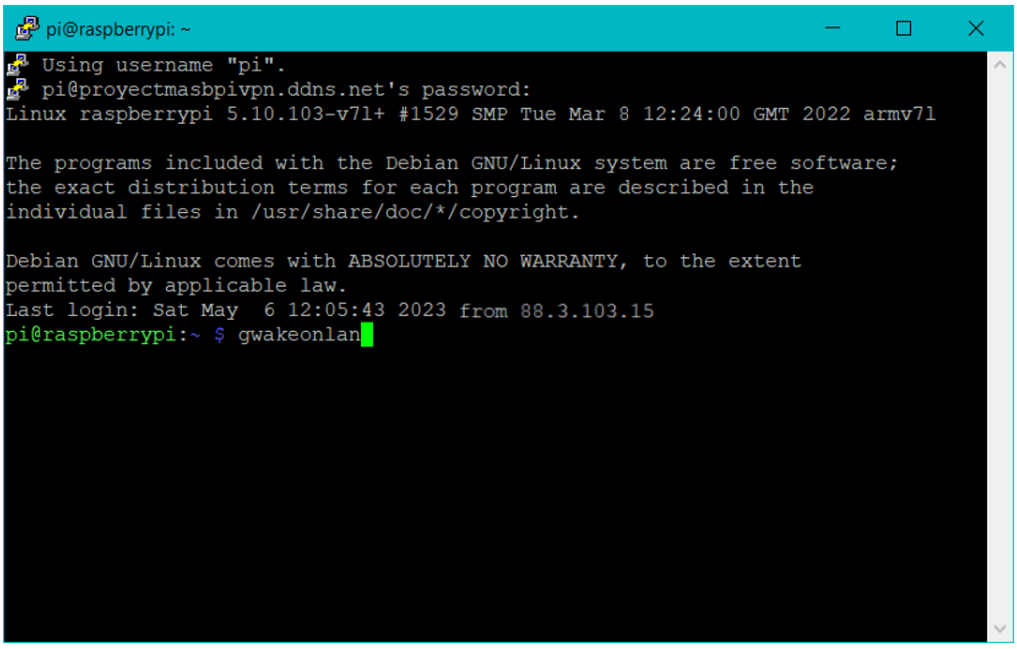


Como se puede apreciar en la ventana de la captura superior, al ya haber facilitado el usuario cuando se realizó la configuración y se guardó, al establecerse la conexión, solo habrá que facilitar la contraseña del usuario en cuestión, que en este ejemplo se trata del usuario pi, teniendo que pulsar INTRO, para establecer la conexión vía SSH.



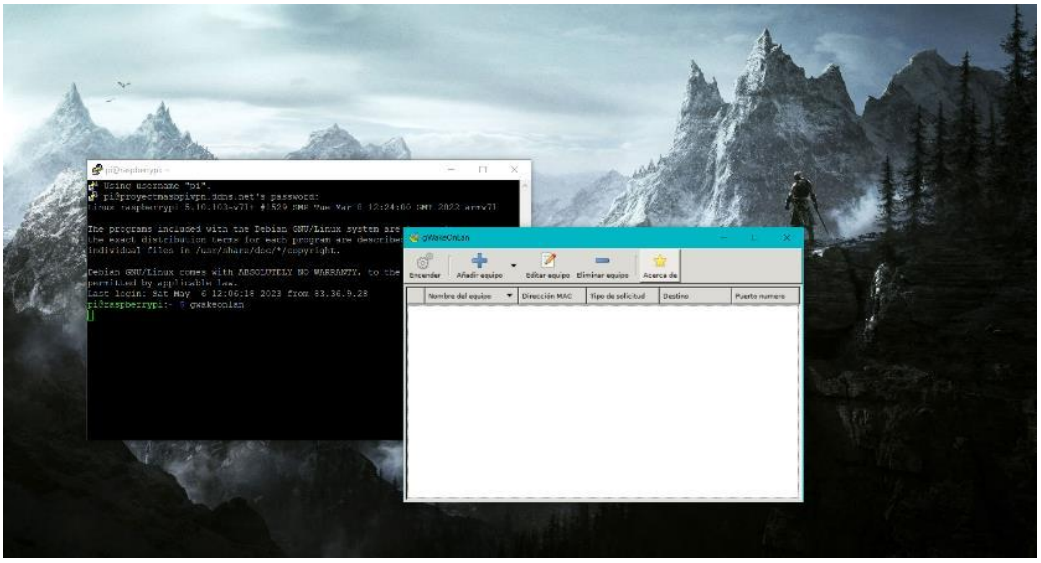
Una vez facilitada la contraseña y habiendo pulsado INTRO, se estará remotamente conectado en un terminal vía SSH a la Raspberry Pi.

Para que la redirección X funcione en equipos con el S.O. Windows, es necesario tener instalada y en ejecución la aplicación Xming, ejecutando la aplicación XLaunch.

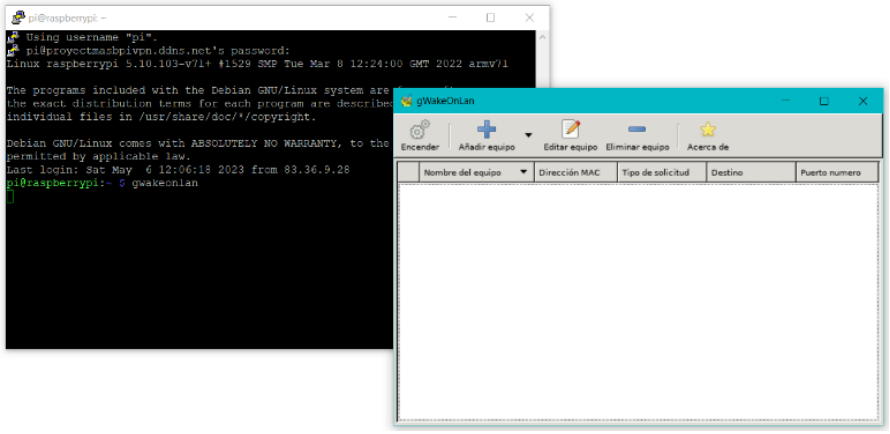


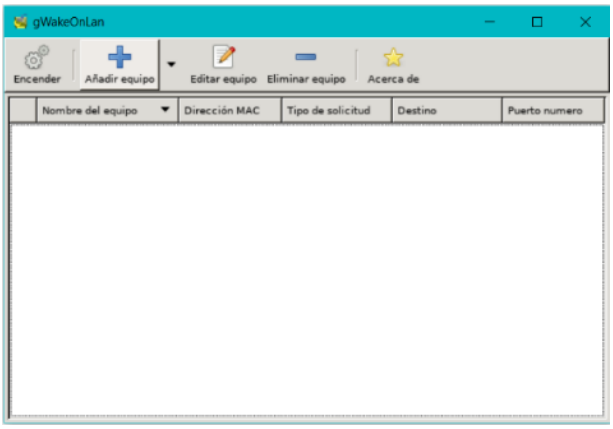
Al haber configurado la conexión en el programa PuTTY con la redirección X habilitada, dentro de este terminal se podrá ejecutar el comando.

gwakeonlan

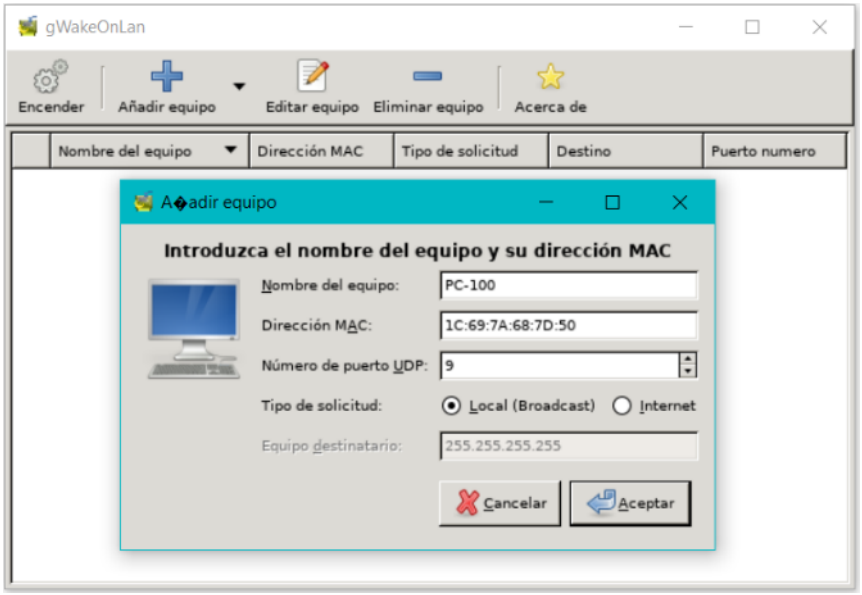


Pasado un momento, aparecerá la ventana de la aplicación gWakeOnLan instalada en el equipo servidor VPN/WOL, ejecutándose remotamente vía SSH, en el equipo cliente con S.O. Windows.





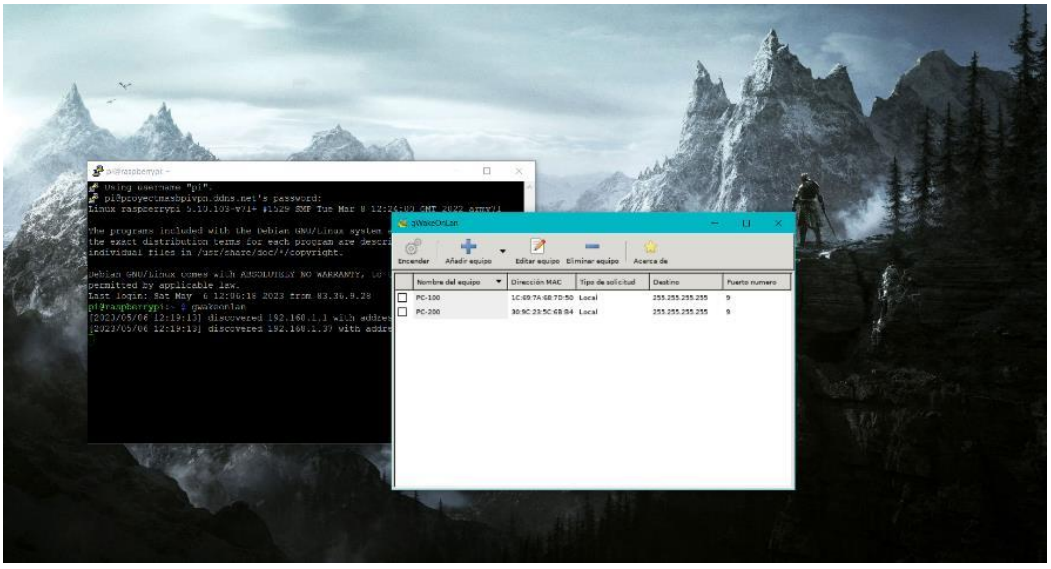
Con la aplicación gWakeOnLan abierta, para agregar la configuración de equipos, se pulsará sobre el botón superior, Añadir equipo  .

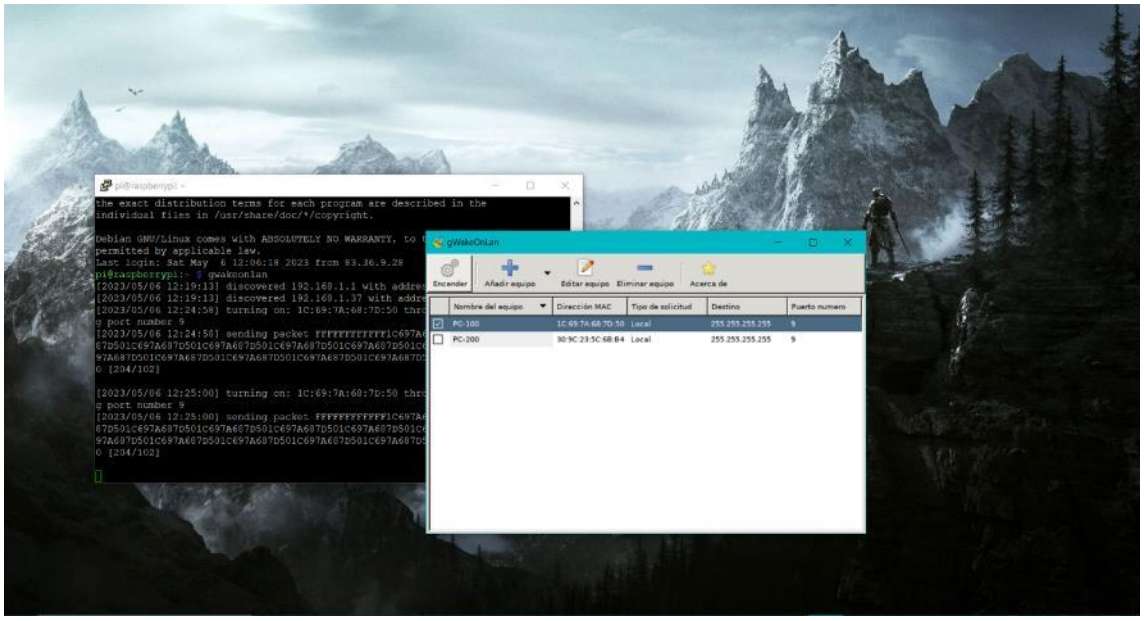


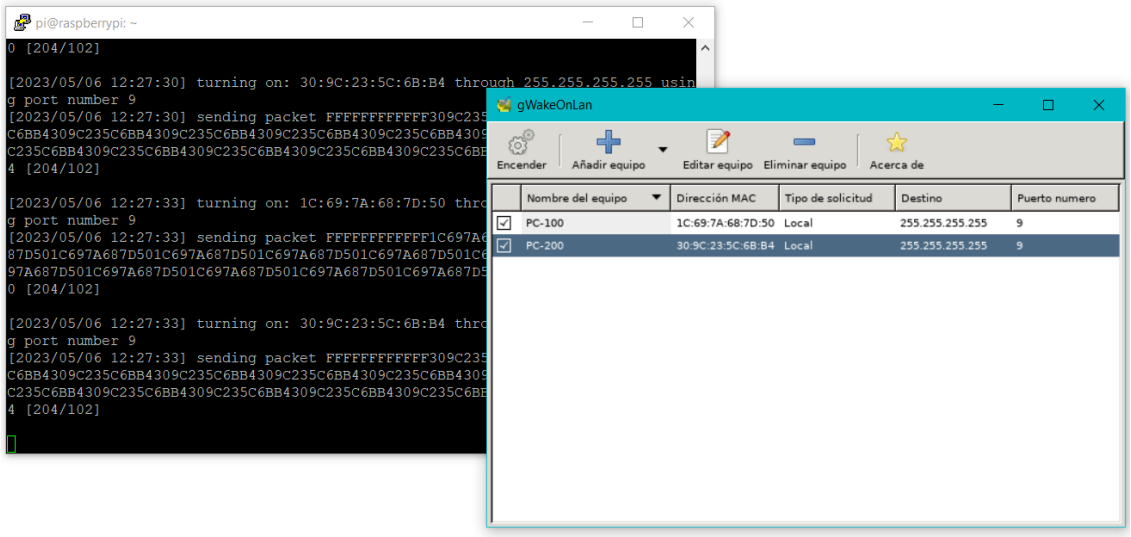
En la nueva ventana que aparece, se tendrá que colocar los datos necesarios.

- Nombre del equipo: Nombre del equipo, nombre descriptivo, en este ejemplo PC-100.
- Dirección MAC: Dirección MAC de la tarjeta de red del equipo que se está configurando, en este ejemplo 1C:69:7A:68:7D:50
- Número de puerto UDP: En este ejemplo no se modifica.
- Tipo de solicitud: En este ejemplo no se modifica.

Con los campos rellenados como se necesiten, se pulsará sobre Aceptar.

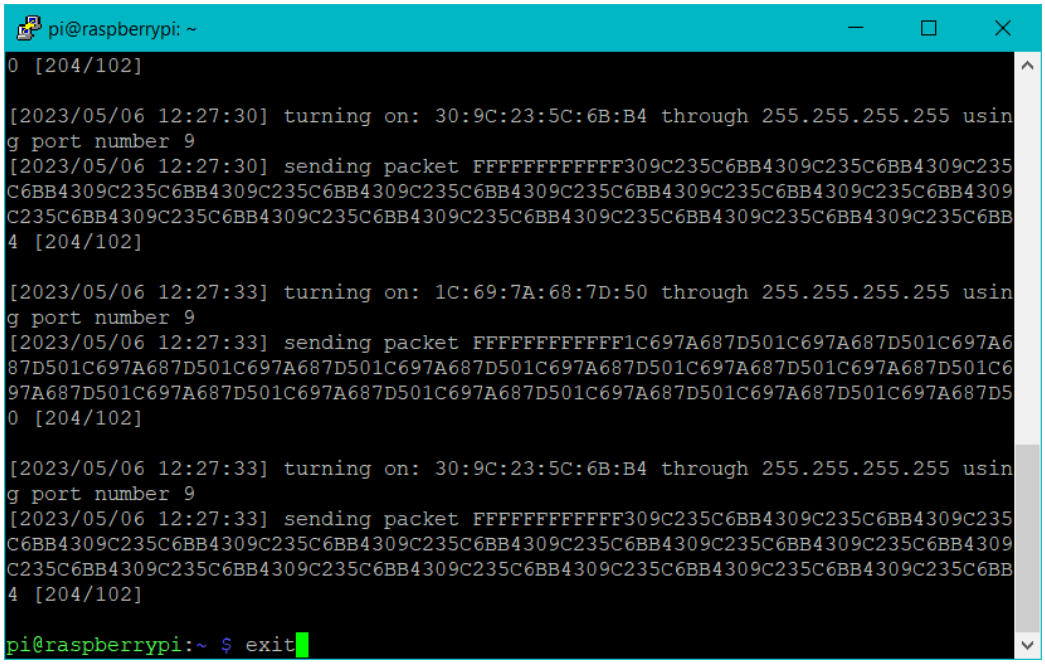






En caso de necesitar encender uno o más de un equipo a la vez, dentro de la aplicación gWakeOnLan abierta y con la configuración de los equipos necesarios a encender guardada, para iniciar los equipos, se seleccionarán y posteriormente se pulsará sobre el botón superior Encender, como se puede observar en la ventana de la captura superior, al pulsar sobre el botón superior Encender, en el terminal se envían los datos necesarios de las ordenes que se están ejecutando en la aplicación gWakeOnLan.

(Puede que sea necesario pulsar más de una vez sobre el botón Encender).



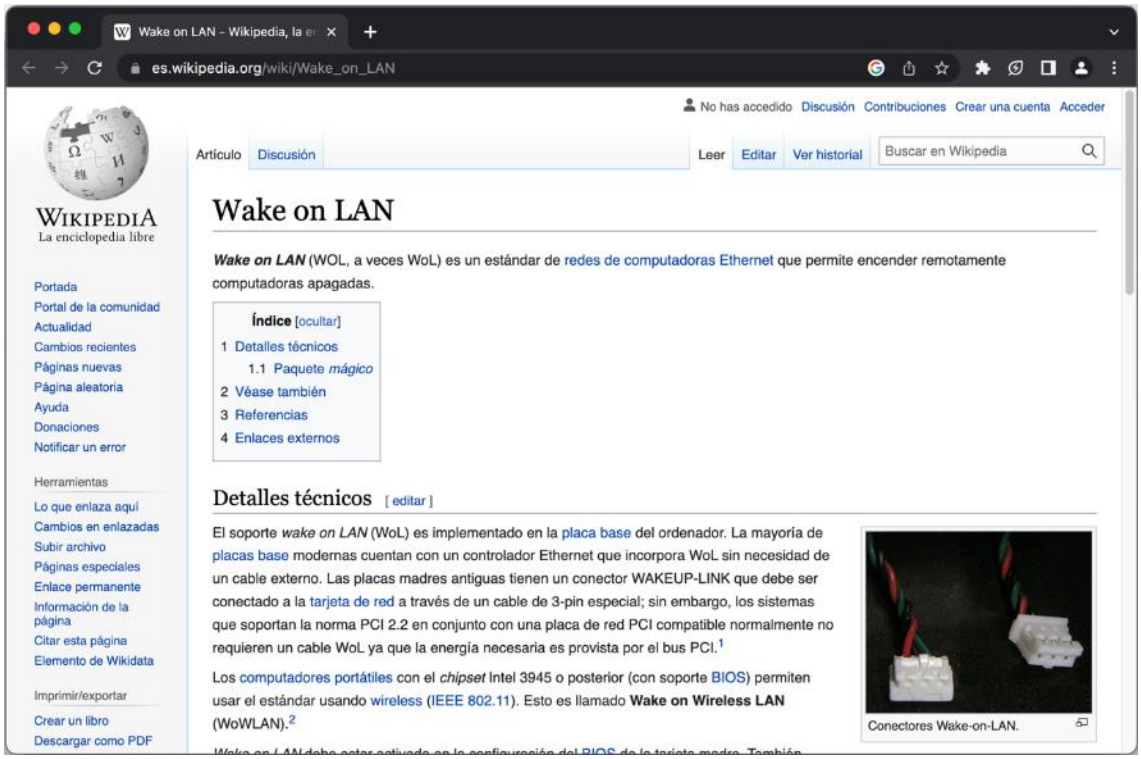
Para finalizar, se cerrará la aplicación gWakeOnLan y dentro del terminal, se escribirá exit y se pulsará INTRO para finalizar la conexión remota vía SSH.

Wake On LAN (WOL)

Ya se explicó anteriormente que es Wake On LAN (WOL), en este proyecto, se explica como habilitar esta característica en ciertos equipos, para equipos más antiguos, aunque también se menciona en esta documentación, se facilita un link de Wikipedia donde se disponen de detalles técnicos y demás, informando que en tarjetas de red antiguas, había que realizar la conexión de un cable desde la propia tarjeta de red a la placa base para poder hacer uso de esta característica y utilizar WOL, en la actualidad, prácticamente todos los equipos disponen de esta característica, teniendo que comprobar si se encuentra habilitada ya en la BIOS y encontrarse el S.O. configurando, en este proyecto, la configuración se lleva a cabo sobre equipos con S.O. Windows 10 y Windows 11, también se prueba en un equipo con S.O. Linux Ubuntu.

Puede que, realizadas las modificaciones, si no funciona puesto que, en caso de tener una BIOS más actualizada, se recomienda consultar la documentación del propio equipo o placa base, e incluso hacer una búsqueda en Internet, consultando como habilitar Wake On LAN en una placa base en concreto o en un equipo.

WEB WIKIPEDIA con documentación referente a Wake On LAN.
URL. https://es.wikipedia.org/wiki/Wake_on_LAN



Habilitar Wake On LAN en equipo MSI Gaming Trident 3.

MSI Wake On LAN.

BIOS.

Para habilitar WOL en el equipo MSI H110 Gaming Trident 3 (MS-B906), se deberá acceder a la BIOS, pulsando la tecla Supr, y sin soltar la tecla, encender el ordenador.



En la ventana principal de la BIOS, se pulsará o se seleccionará la opción. SETTINGS.



Dentro de Settings, se seleccionará Advanced.



Habrá que dirigirse ahora a la opción Power Management Setup.



Dentro de la opción Power Management Setup.



Habrá que deshabilitar la opción EuP 2013, dejando la opción en Disabled.



Nuevamente en Settings \ Advanced, se seleccionará el adaptador de red, en este caso Intel (R) Ethernet Connection (H) I219-V – 30:XXxxxxxxx.



Se accederá ahora a la opción NIC Configuration.

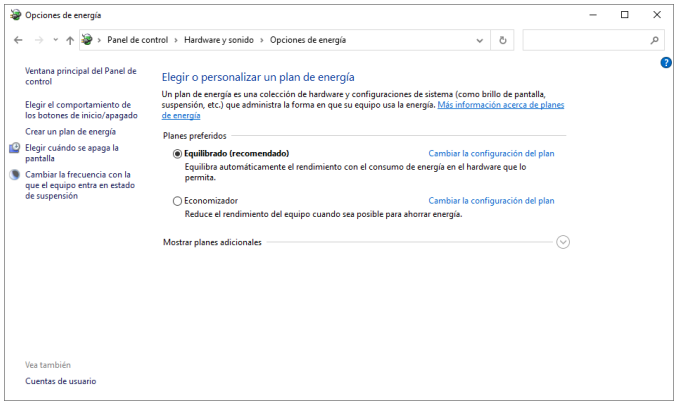


En este caso, la opción inferior Wake On LAN se encuentra deshabilitada, no pudiendo modificar su valor, aun así, con las opciones indicadas modificadas, el equipo despierta tras recibir el paquete mágico.



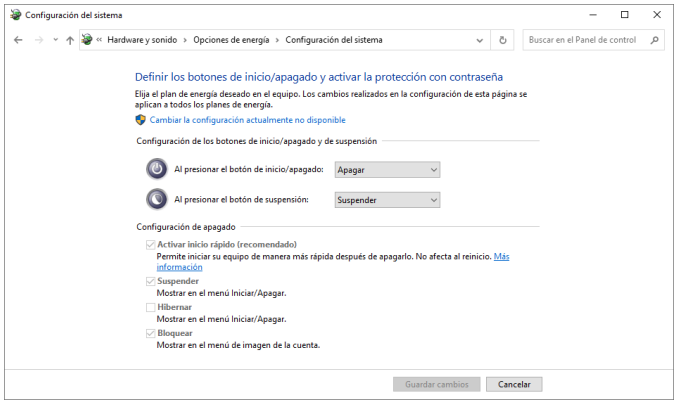
Tras realizar las modificaciones indicadas, para salir y guardar los cambios, se presionará sobre la tecla F10, en la ventana que se muestra, se seleccionará Yes y se pulsará INTRO.

S.O. Windows opciones de energía.

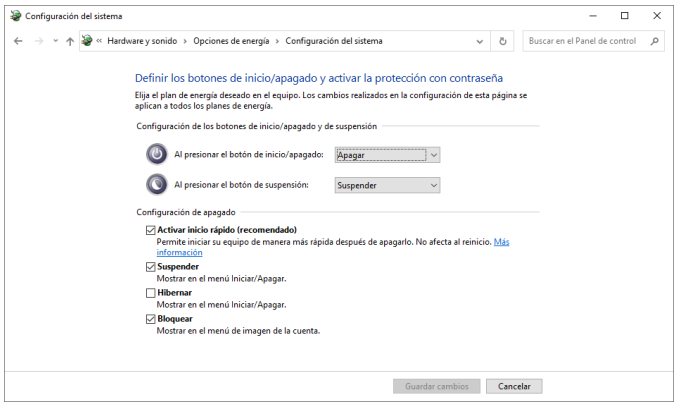


En un equipo cliente con S.O. Windows, dentro de la sesión de un usuario, habrá que acceder a Panel de control \ Hardware y sonido \ Opciones de energía

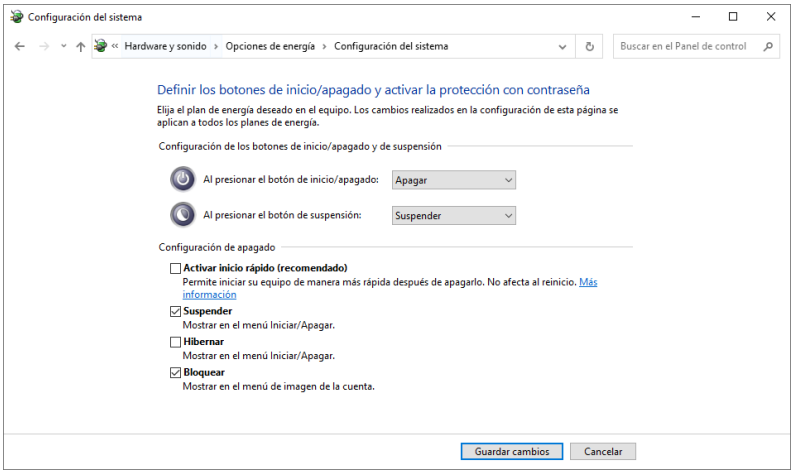
En el panel izquierdo, se pulsará sobre, Elegir el comportamiento de los botones de inicio/apagado.



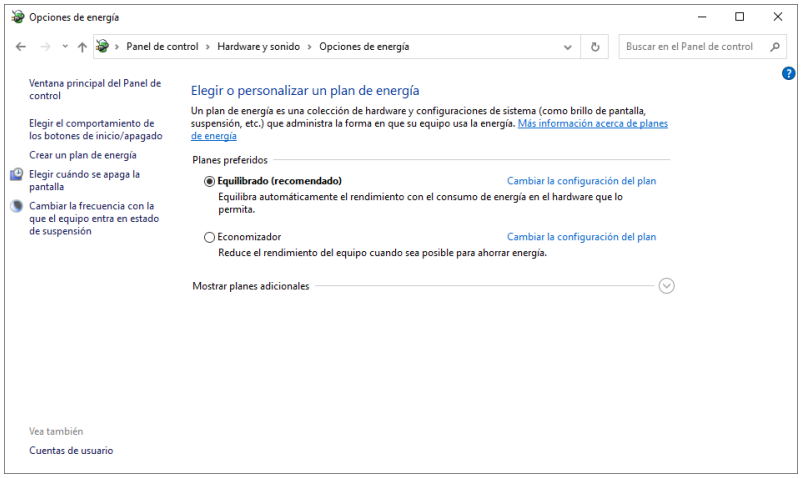
Habrá que pulsará ahora sobre Cambiar la configuración actualmente no disponible.



En el caso de que el checkbox de la opción Activar inicio rápido (recomendado), se encuentre marcado, se desmarcara.

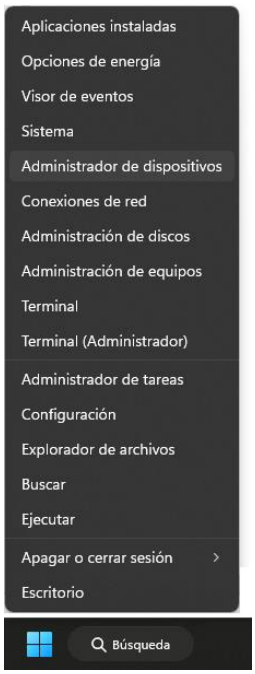


Realizadas las modificaciones, se pulsará sobre Guardar cambios en la parte inferior.

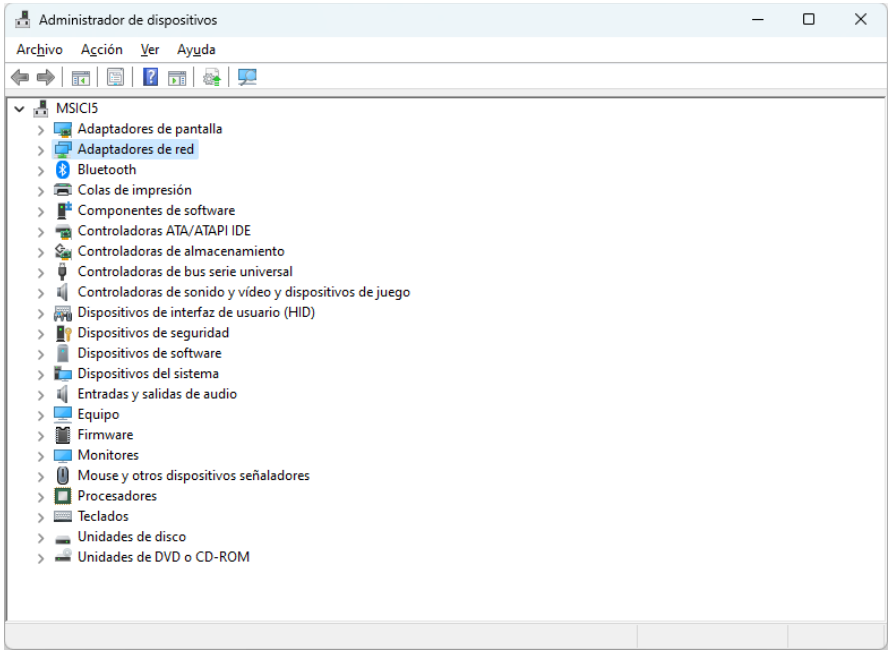


Para finalizar, se podrá cerrar la ventana de Panel de control.

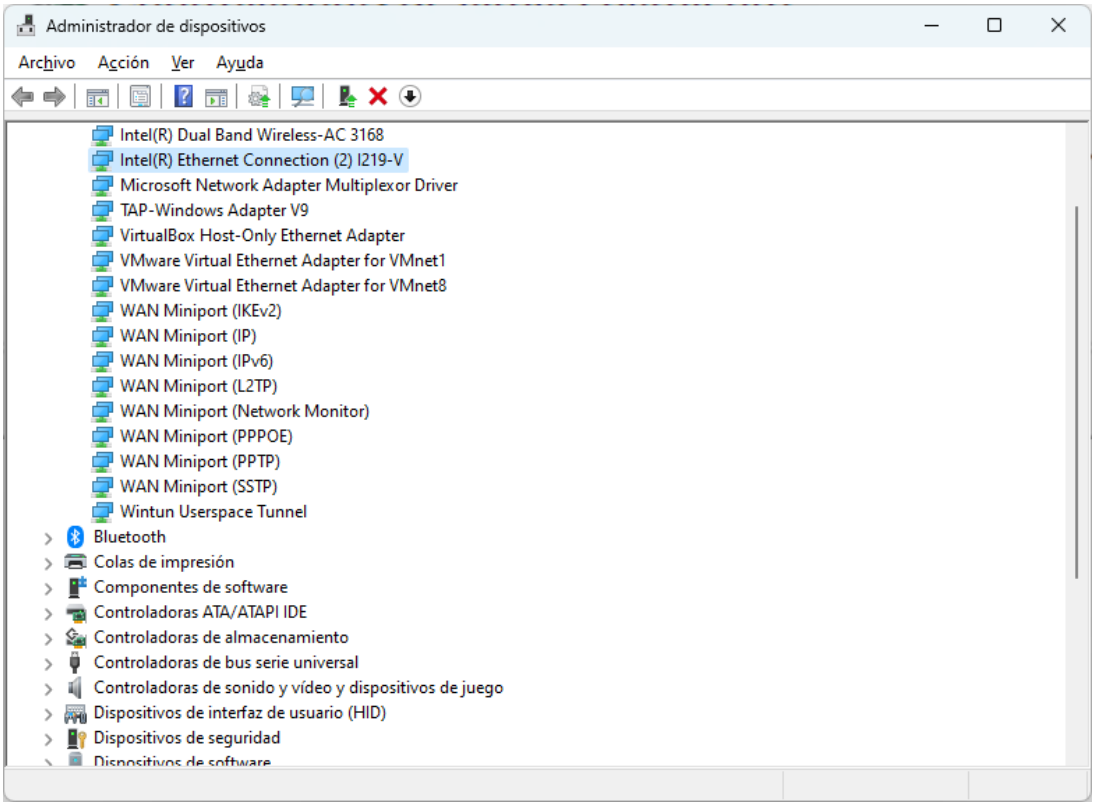
Configuración tarjeta de red S.O. Windows.



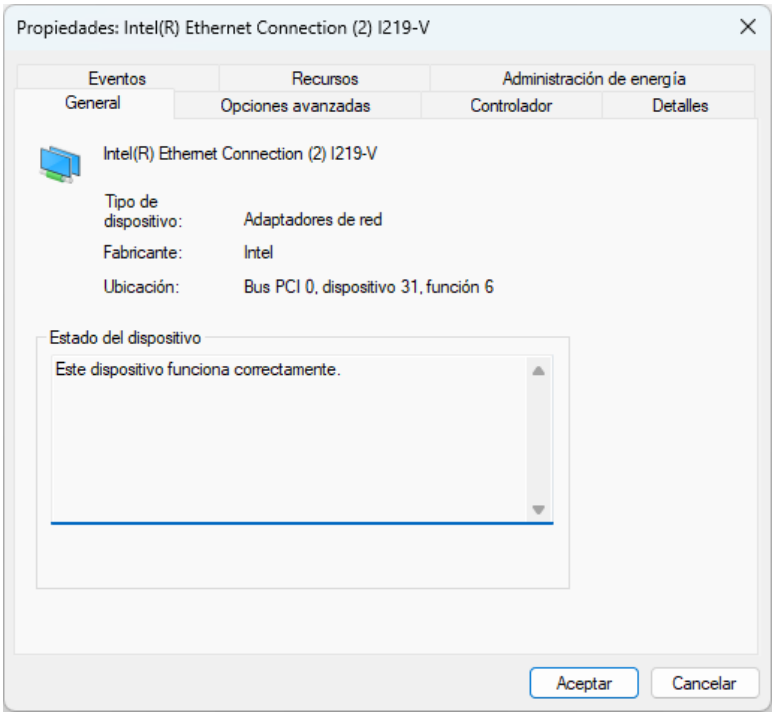
Se accederá al Administrador de dispositivos, haciendo clic con el botón derecho del ratón en la esquina inferior izquierda sobre el logotipo de Windows, apareciendo el menú que se observa en la ventana de la captura superior, teniendo que pulsar sobre Administrador de dispositivos.



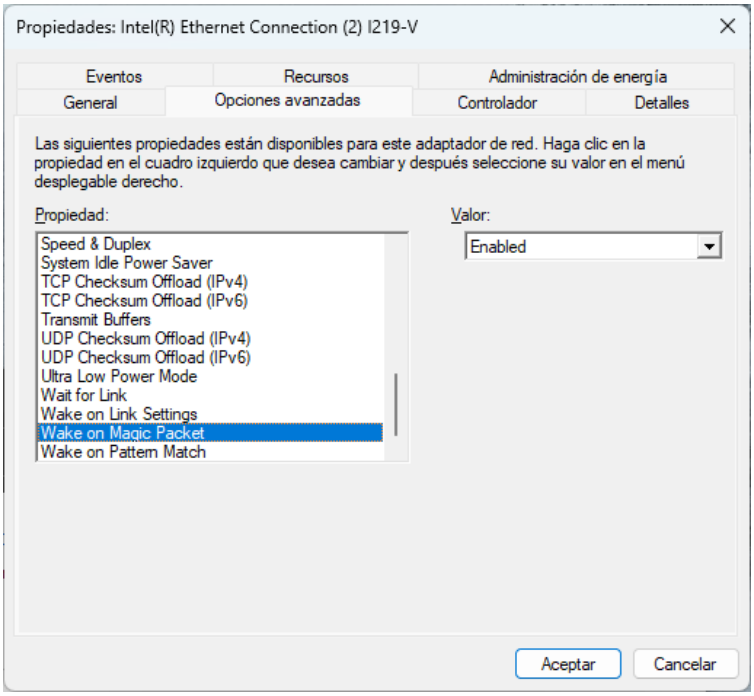
Dentro del Administrador de dispositivos, se accederá a los Adaptadores de red, desplegándolos.



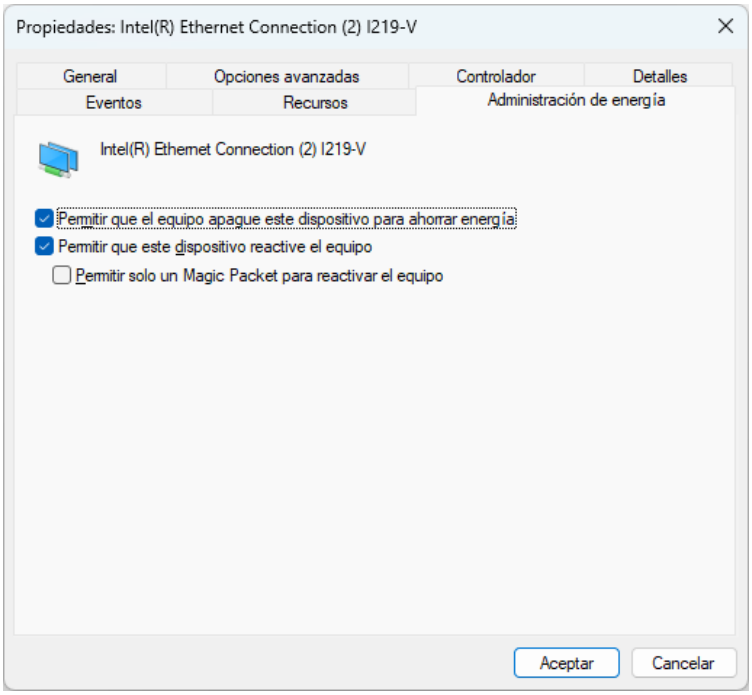
Se hará doble clic con el botón izquierdo del ratón sobre el adaptador ethernet, en este caso se trata del adaptador Ethernet Intel (R) Ethernet Connection (2) I219-V.



Mostrándose las opciones del adaptador ethernet en cuestión.



En la pestaña Opciones avanzadas, apartado izquierdo Propiedad, se localizará la propiedad Wake on Magic Packet (en otras ocasiones, puede aparecer como Activar en Magic Packet, WOL, Wake On LAN, o se tendrá que realizar una búsqueda para poder habilitar esta opción), localizada la mencionada opción y seleccionada, en el apartado superior derecho Valor, se seleccionará Enabled.



En la pestaña Administración de energía, se dejan las opciones seleccionadas por defecto.

Habilitar Wake On LAN en equipo Intel NUC.

NUC Wake On LAN.
NUC8BEB Intel.

BIOS.



En esta ocasión, para acceder a la BIOS, habrá que pulsar la tecla F9.

En la ventana de inicio de la BIOS, se pulsará sobre el botón izquierdo inferior o sobre el botón superior derecho Advanced.



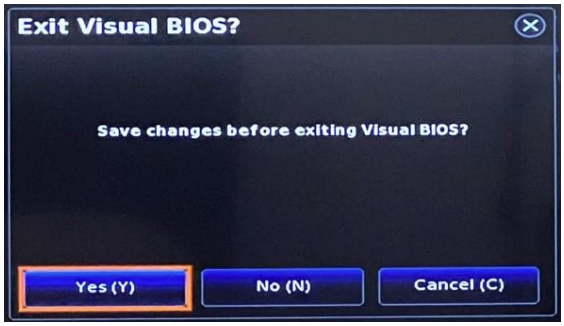
Estando dentro de la opción Advanced, se pulsará o se seleccionará la opción Power.



Dentro de la opción Power, habrá que deslizar la barra de deslizamiento lateral derecha para localizar la opción inferior, Wake on LAN from S4/S5.

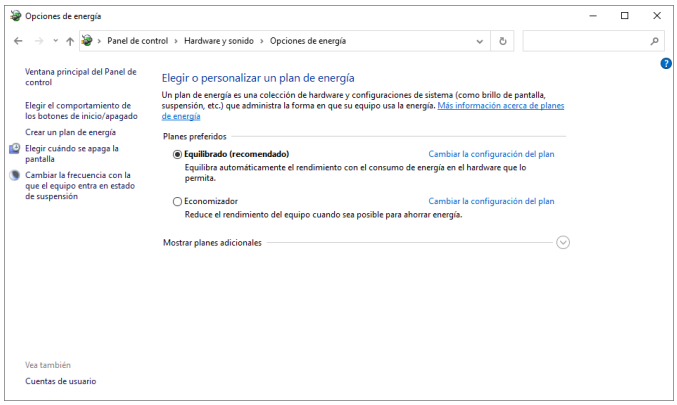


La opción Wake on LAN from S4/S5, se encuentra por defecto, como se muestra en la ventana de la captura superior, estando configurada de esta forma el funcionamiento es correcto, encendido remotamente el equipo, no realizándose ninguna modificación en la BIOS.



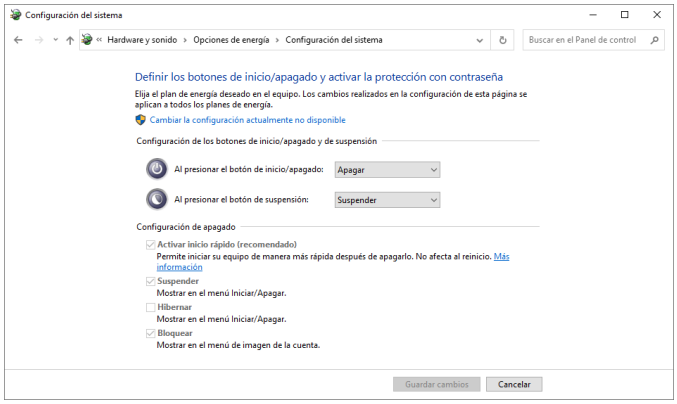
Se pulsará la tecla F10 para guardar los cambios y salir, el equipo se reiniciará, teniendo que configurar la parte del S.O. y el adaptador de red.

S.O. Windows opciones de energía.

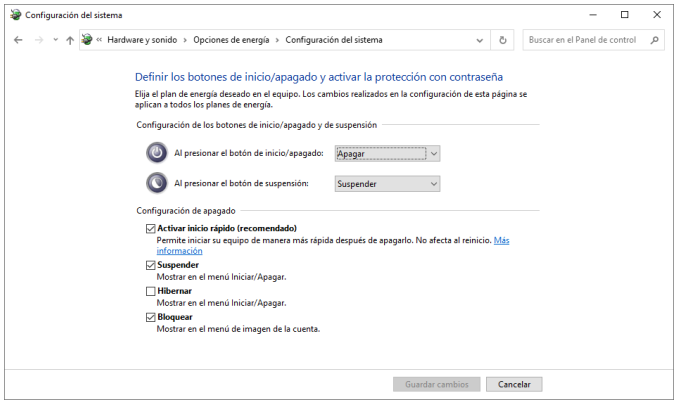


En un equipo cliente con S.O. Windows, dentro de la sesión de un usuario, habrá que acceder a Panel de control \ Hardware y sonido \ Opciones de energía

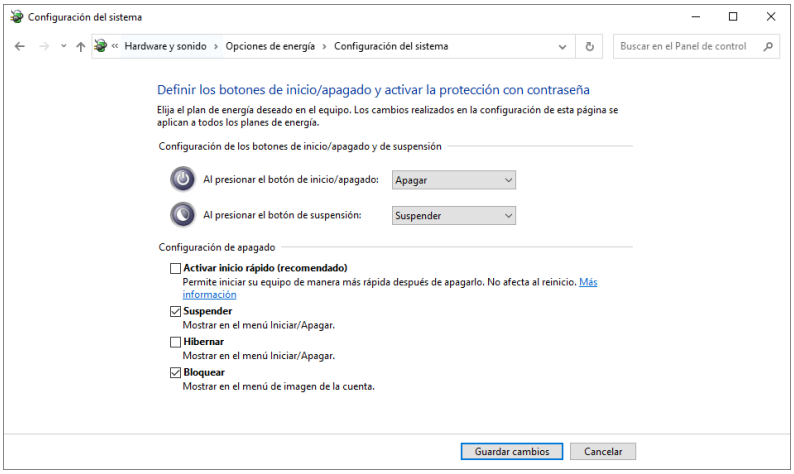
En el panel izquierdo, se pulsará sobre, Elegir el comportamiento de los botones de inicio/apagado.



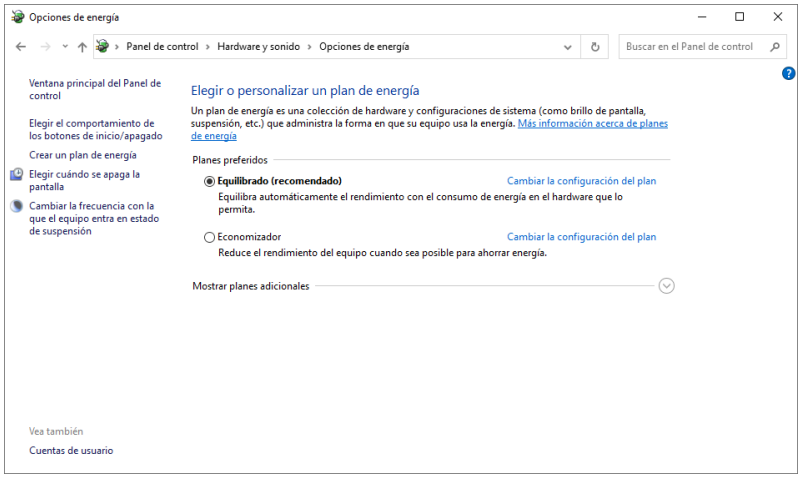
Habrá que pulsará ahora sobre Cambiar la configuración actualmente no disponible.



En el caso de que el checkbox de la opción Activar inicio rápido (recomendado), se encuentre marcado, se desmarcara.

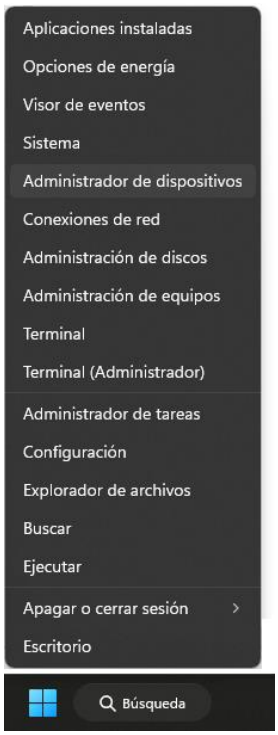


Realizadas las modificaciones, se pulsará sobre Guardar cambios en la parte inferior.

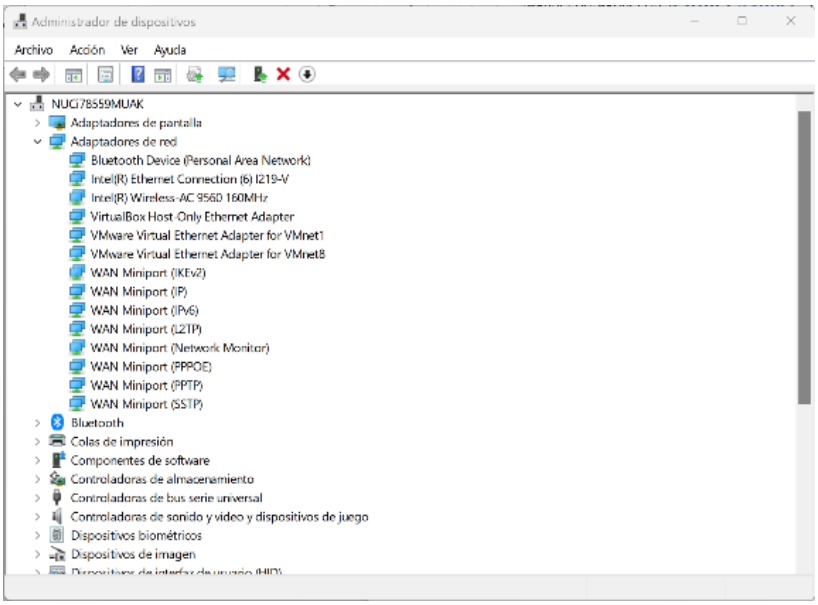


Para finalizar, se podrá cerrar la ventana de Panel de control.

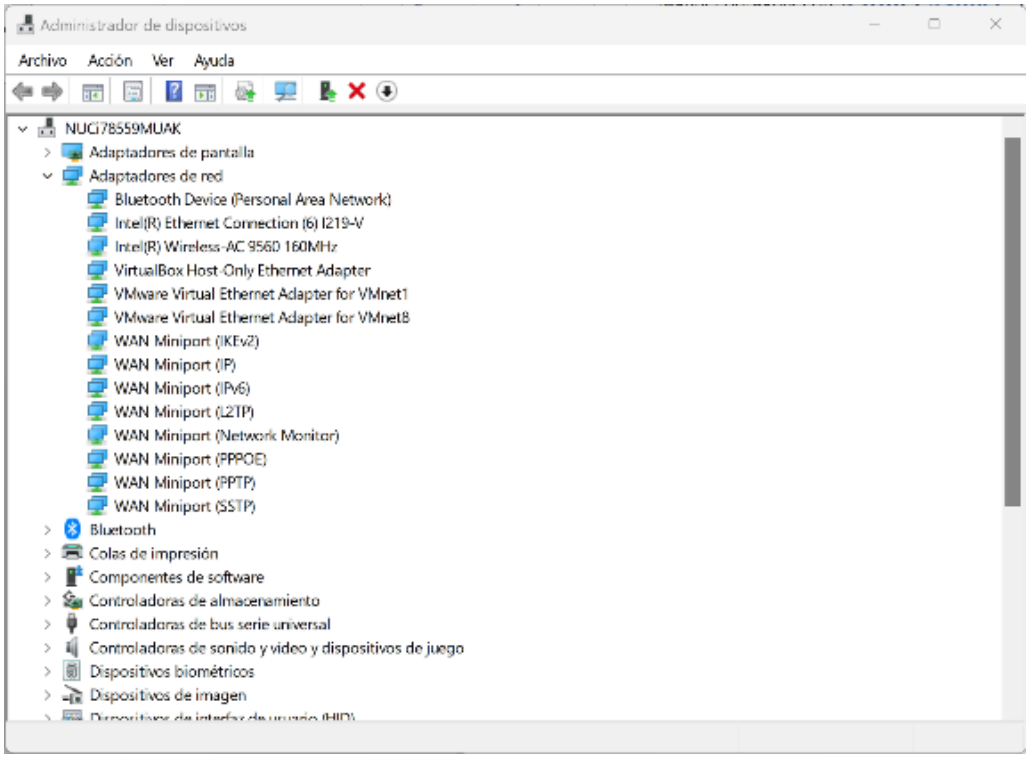
Configuración tarjeta de red S.O. Windows.



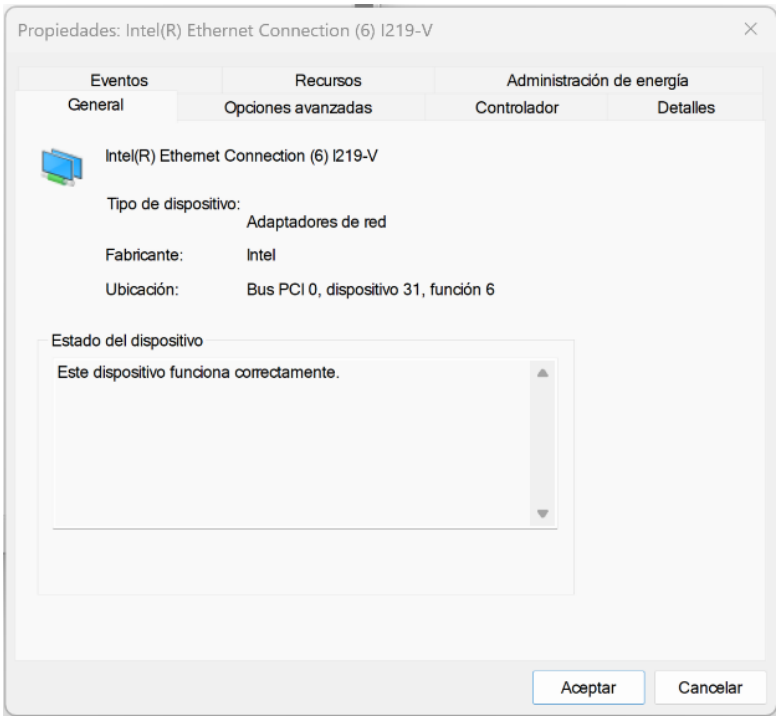
Se accederá al Administrador de dispositivos, haciendo clic con el botón derecho del ratón en la esquina inferior izquierda sobre el logotipo de Windows, apareciendo el menú que se observa en la ventana de la captura superior, teniendo que pulsar sobre Administrador de dispositivos.



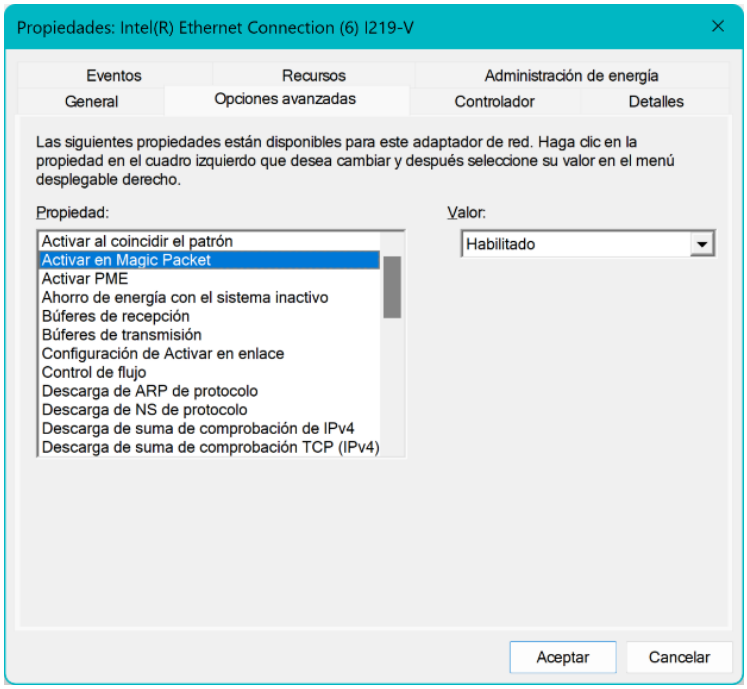
Dentro del Administrador de dispositivos, se accederá a los Adaptadores de red, desplegándolos.



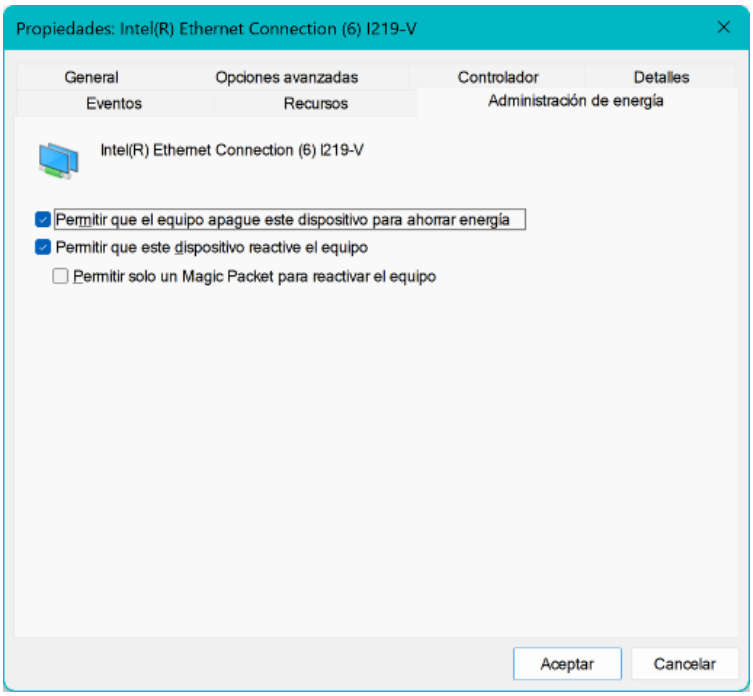
Se hará doble clic sobre el adaptador ethernet, en este caso se trata del adaptador Ethernet Intel (R) Ethernet Connection (6) I219-V.



Mostrándose las opciones del adaptador ethernet en cuestión.

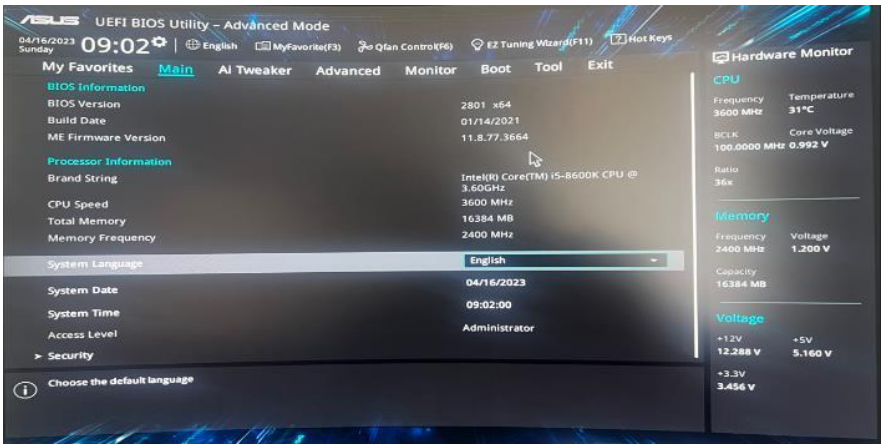


En la pestaña Opciones avanzadas, en el apartado izquierdo Propiedad, se localizará la propiedad Activar en Magic Packet (en otras ocasiones puede aparecer como Wake on Magic Packet, WOL, Wake On LAN, o se tendrá que realizar una búsqueda para poder habilitar esta opción), localizada la mencionada opción y seleccionada, en el apartado superior derecho Valor, se seleccionará Habilitado.

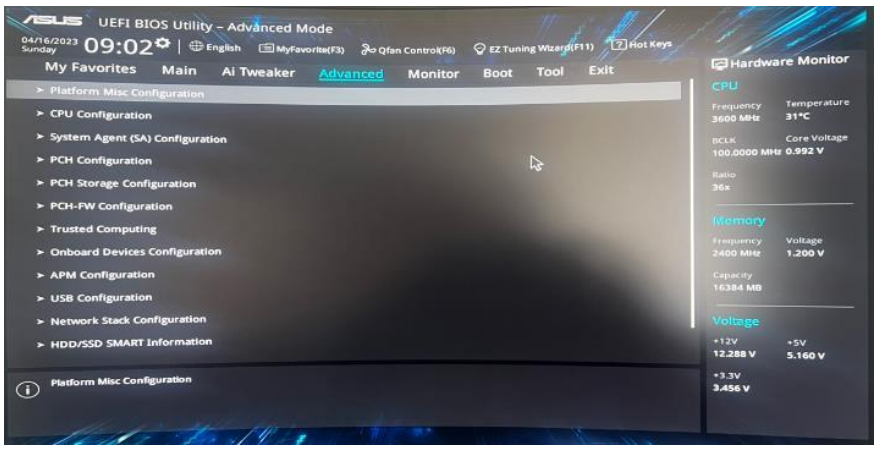


En la pestaña Administración de energía, se dejan las opciones seleccionadas por defecto.

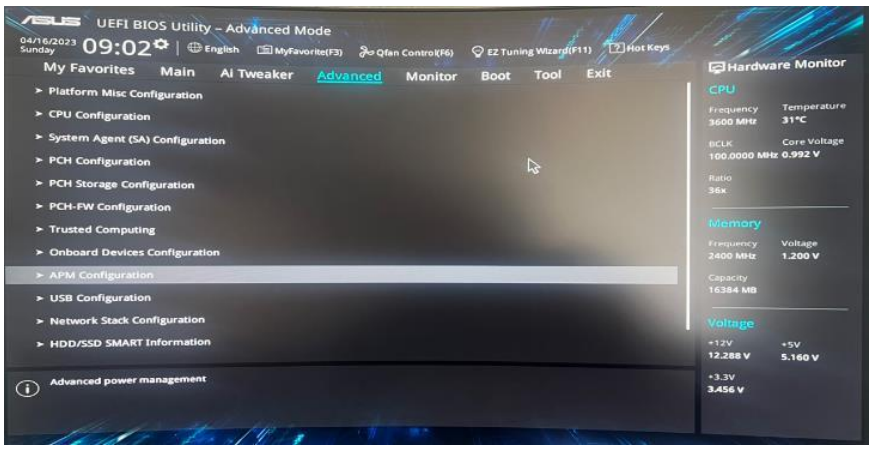
Habilitar Wake On LAN en placa base ASUS.



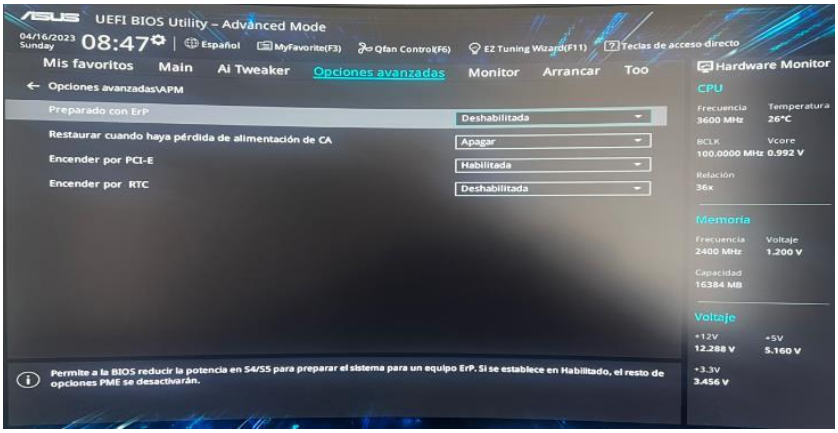
Se accederá a la BIOS, pulsando la tecla F2.



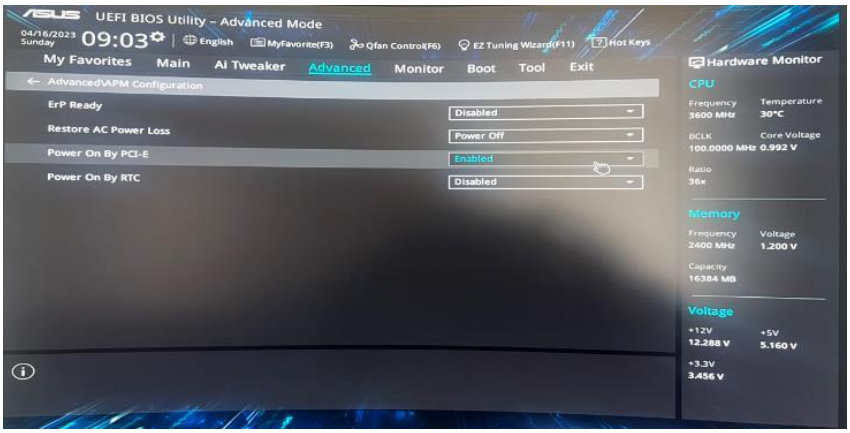
En el menú superior, se seleccionará el apartado Advanced.



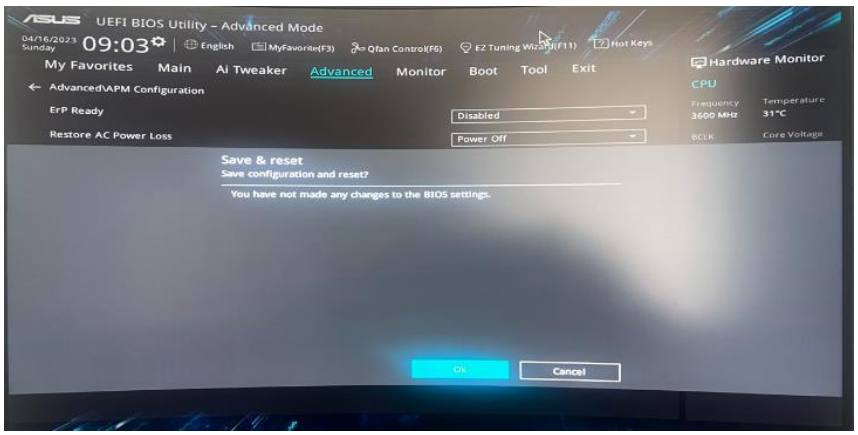
Teniendo que localizar dentro de Advanced, la opción inferior izquierda APM Configuration.



Dentro de La opción Advanced \ APM Configuration, la opción Preparado con ErP, se tendrá que dejar Deshabilitada.



Nuevamente, dentro del apartado Advanced \ APM Configuration, opción Power On By PCI-E habrá que dejarla en Enabled.



Realizadas las modificaciones, se pulsará la tecla F10, apareciendo una ventana preguntando si se quiere salvar la configuración y reiniciar, se seleccionará OK y se pulsará INTRO.

Habilitar Wake On LAN en placa Gigabyte.



Para acceder a la configuración de la BIOS, se pulsará la tecla Supr, luego, dentro de la BIOS habrá que pulsar la tecla F7 para cambiar el aspecto de la BIOS, posteriormente, se accederá a la opción del menú superior Power Management.

Dentro del apartado Power Management.

Habrá que localizar la opción intermedia ErP y habrá que dejarla como Disabled.



Nuevamente, dentro del apartado Power Management.

En la opción Wake on LAN, habrá que dejarla como Enabled.

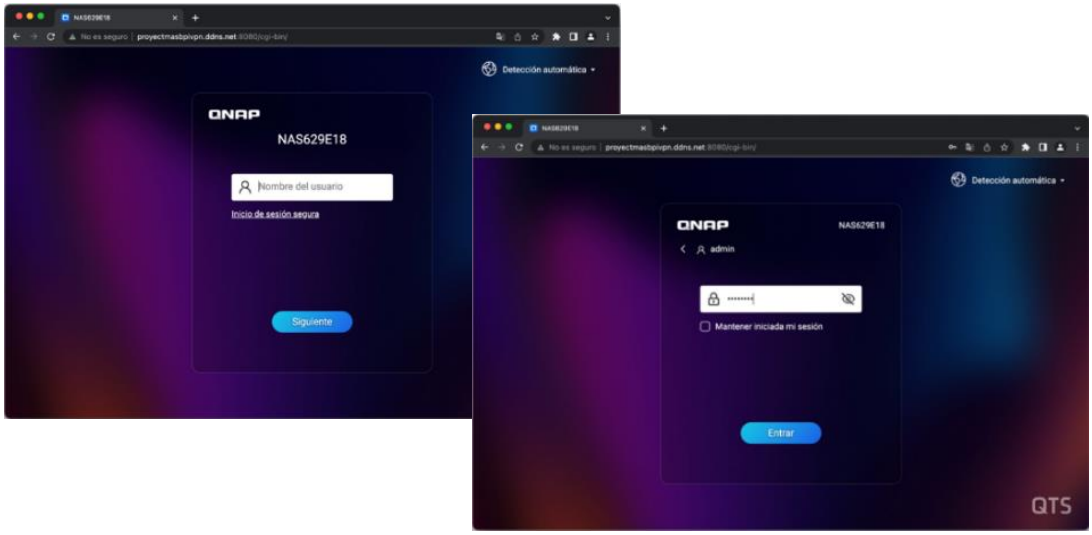
Realizadas las modificaciones descritas, se pasará al apartado del menú superior derecho Save & Exit, donde se seleccionará la opción de salir guardando los cambios y se aceptará, para el posterior reinicio del equipo.

Habilitar Wake On LAN en NAS QNAP.

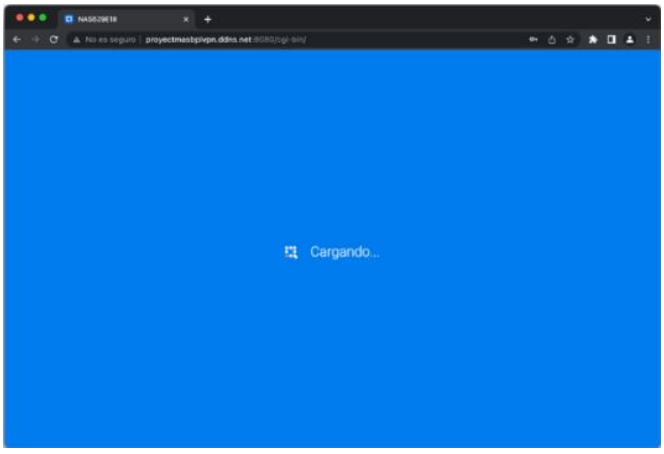
Esta es la manera de comprobar y habilitar si se encuentra habilitado Wake On LAN en un NAS QNAP modelo TS-431K.

Al tener habilitado y configurado un servicio DDNS, se podrá acceder al dispositivo NAS vía red local (interna) o externa, colocando como URL en el navegador la IP del dispositivo QNAP en la red LAN (interna), o bien, se podrá acceder a él colocando como URL el nombre de dominio o host creado en el proveedor de servicios DDNS, colocando a continuación como puerto “8080”, separado por “:”, este puerto (8080), habrá que abrirlo en el router como también se tendrá que habilitar el tráfico en el cortafuegos de Linux, o el puerto que se decida y se configure.

URL
http://proyectmasbpivpn.ddns.net:8080/

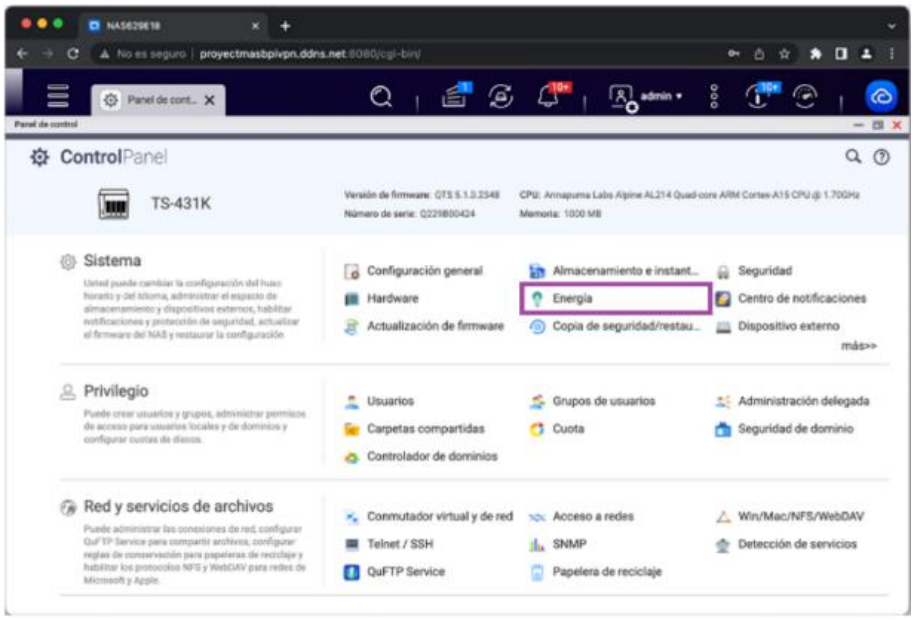


Al colocar la url indicada y pulsar INTRO, habrá que facilitar un usuario y su contraseña con permisos de acceso.

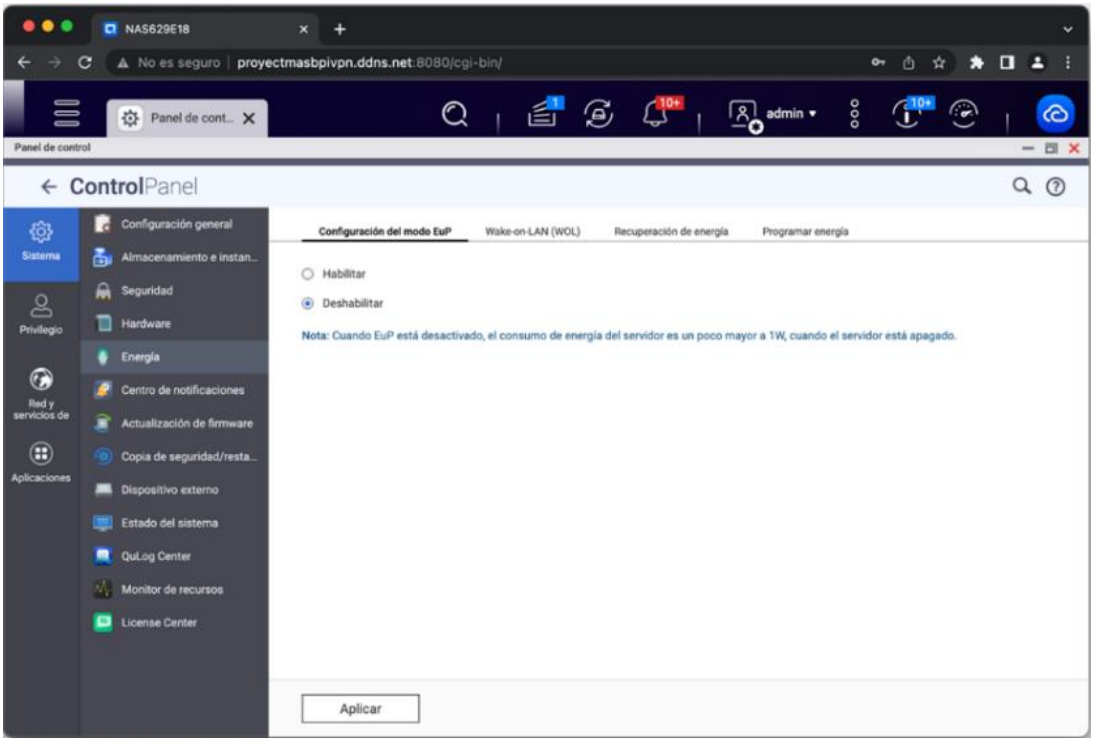




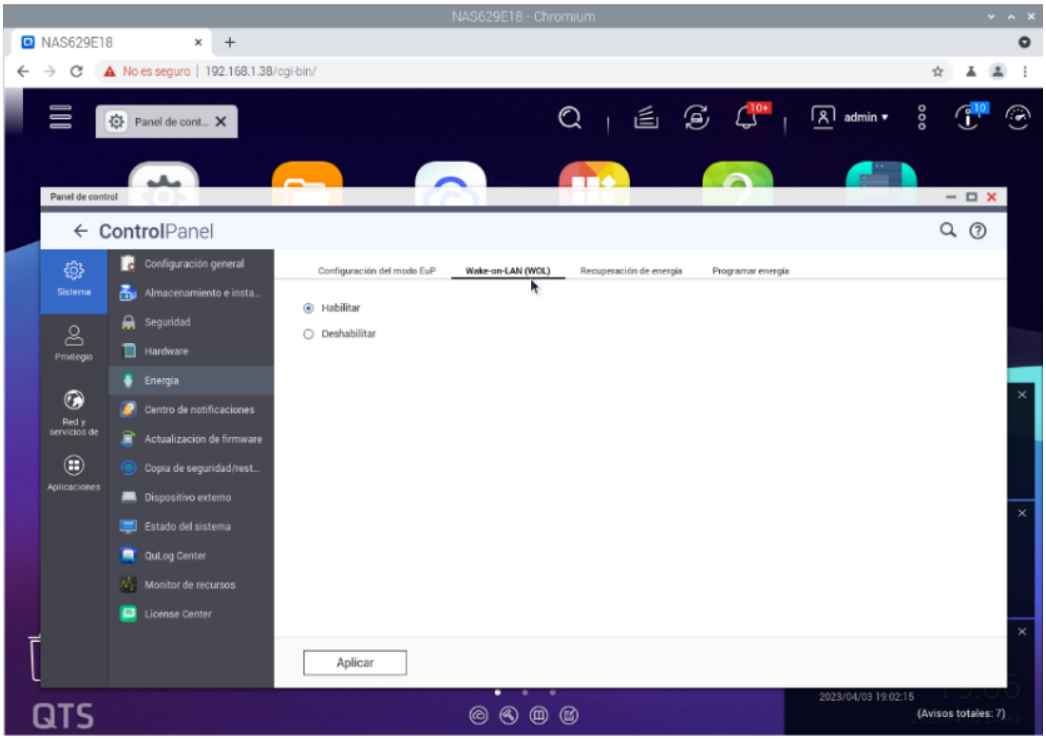
En la ventana principal del dispositivo NAS, se pulsará sobre el icono superior, Panel de control.



Dentro de Panel de control, en el apartado superior izquierdo Sistema, habrá que buscar posteriormente en el panel superior derecho la opción Energía, pulsando sobre Energía.



Dentro de la opción Energía, como se aprecia en la ventana de la captura superior.



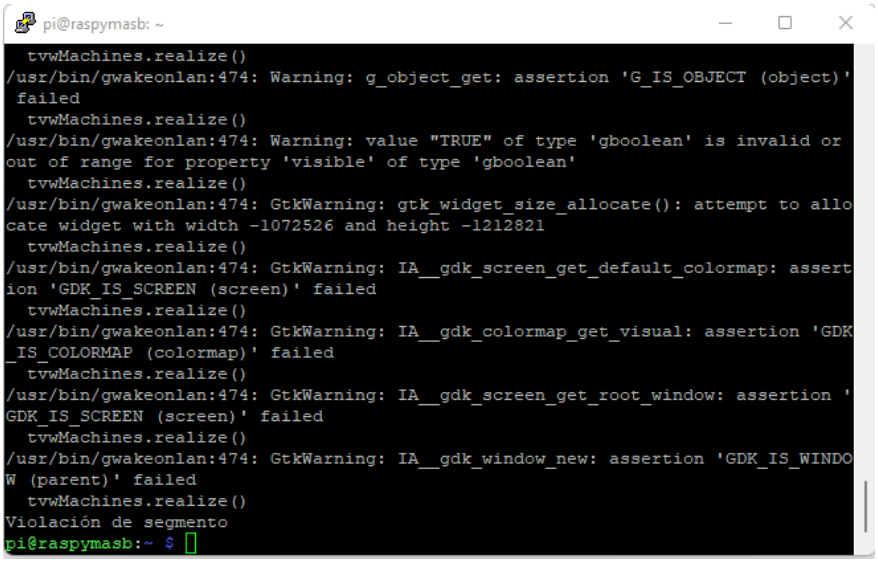
Se pulsará en la pestaña superior Wake-on-LAN (WOL), en el apartado inferior, en caso de encontrarse seleccionada la opción Deshabilitar, se seleccionará Habilitar y para finalizar, se pulsará sobre Aplicar, pudiendo cerrar la página.

Problemas, errores.

Ejecución PuTTY.

Redirección X SSH.

Al ejecutar PuTTY para establecer la conexión SSH, incluso al utilizar un terminal en macOS o la aplicación Símbolo del sistema en Windows, ejecutando la conexión vía SSH con el comando incluyendo la opción -X y con la redirección X activa, si no se tiene instalada e iniciada la aplicación Xming (XLaunch) aparecerán errores sin mostrarse la aplicación gráfica, en macOS se tendrá que tener instalada la aplicación XQuartz.

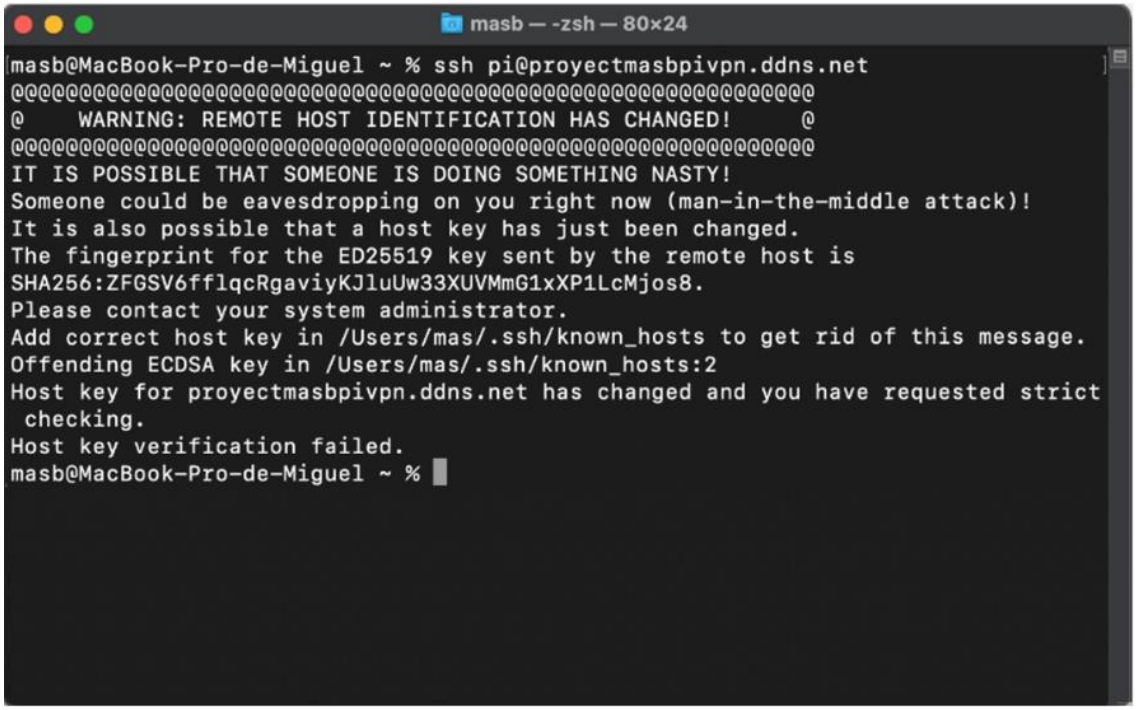


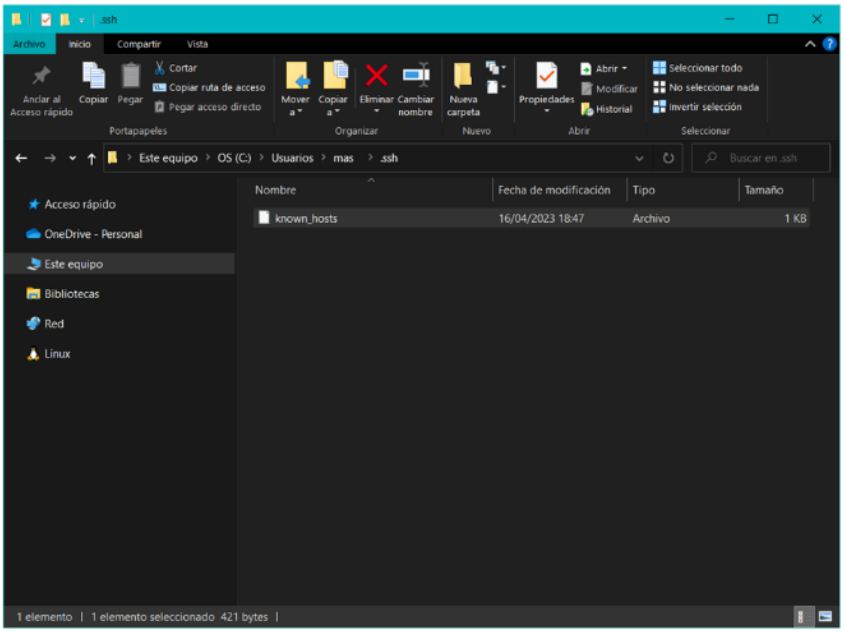
Por ejemplo, captura superior, mostrando el error dentro de la aplicación PuTTY al ejecutar gwakeonlan sin tener abierta la aplicación Xming en el S.O. Windows.

Se tendrá que instalar si no se encuentra instalada la aplicación Xming, o en caso de tenerla instalada, se tendrá que iniciar ejecutando la aplicación XLaunch.

Error al acceder a través de SSH.

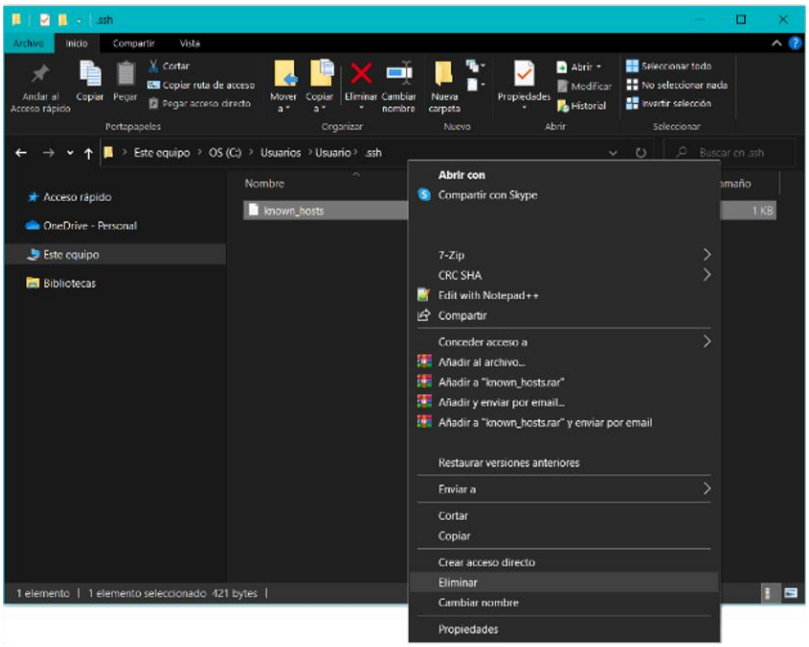
Problema por cambio de identificación del Host remoto.


masb — -zsh — 80×24
masb@MacBook-Pro-de-Miguel ~ % ssh pi@proyectmasbpivpn.ddns.net
@@@



Para solucionarlo, en equipos con S.O. Windows, macOS o Linux, dentro de la sesión del usuario, se accederá a la carpeta oculta .ssh ubicada dentro del directorio del usuario.

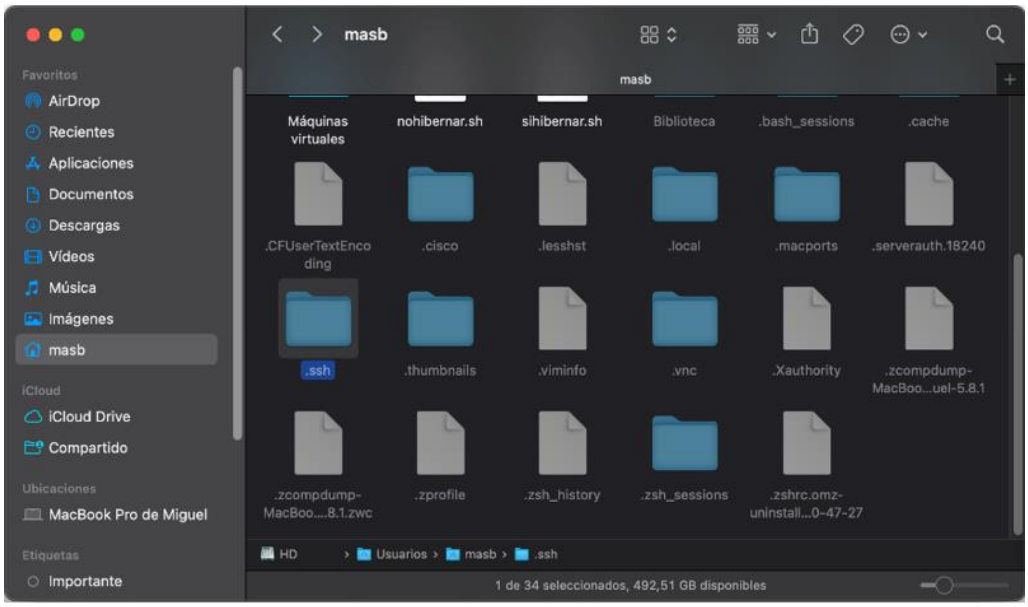
Windows.



Se accederá al directorio C:\Users\USUARIO\.ssh

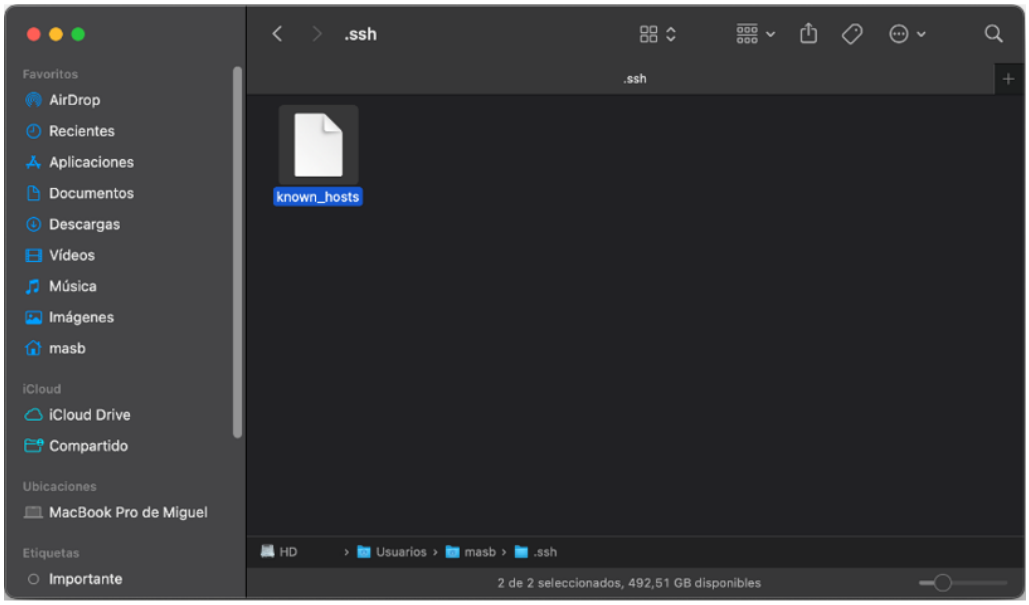
Donde se tendrá que eliminar el fichero Known_host

macOS.



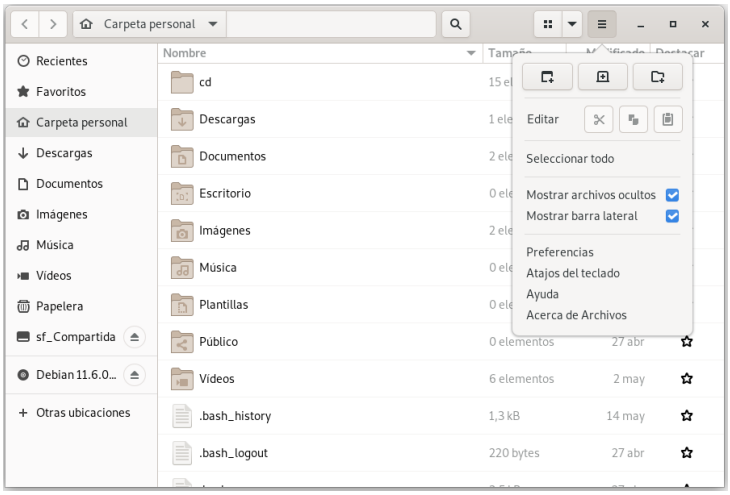
Dentro de la carpeta de la ubicación del usuario en cuestión, /Usuarios/masb, se localizará la carpeta oculta .ssh

Para mostrar los ficheros y carpetas ocultas en macOS, se pulsarán las teclas Shyft+Command+”.” (punto).



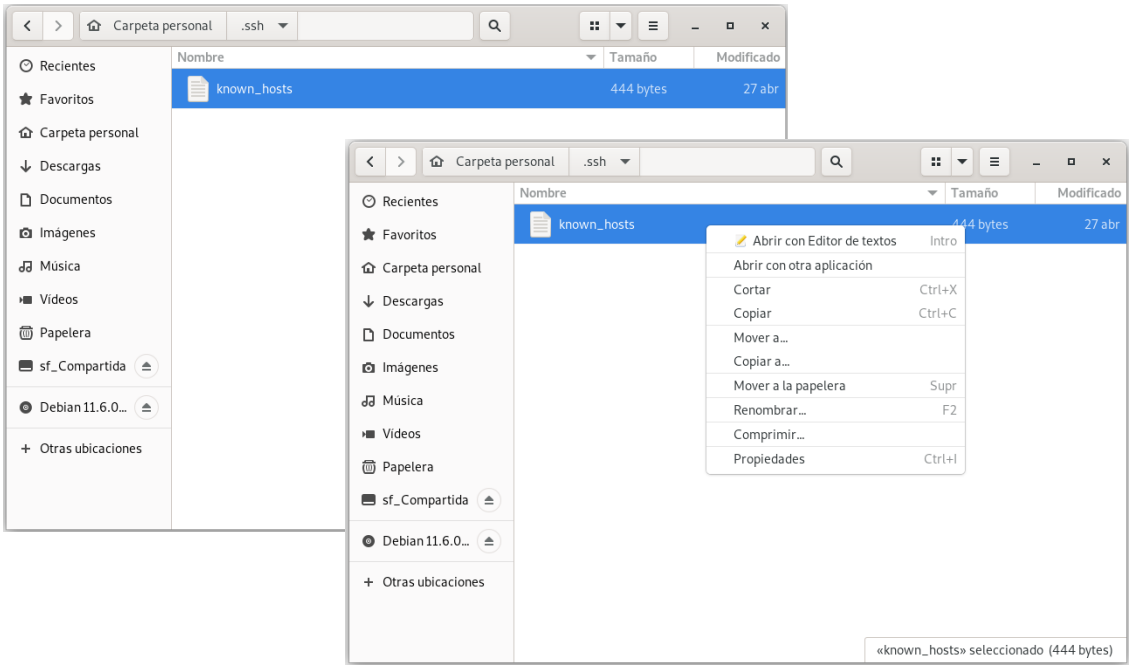
Dentro de la carpeta .ssh, se eliminarán los ficheros existentes, pudiendo utilizar nuevamente la combinación de teclas indicadas para dejar de visualizar los ficheros y carpetas ocultas, tras cerrar Finder, se podrá conectar nuevamente por SSH sin que aparezca de nuevo el problema.

Linux.



Dependiendo de la distribución de Linux como del tipo de escritorio que se esté utilizando, estas opciones pueden diferir.

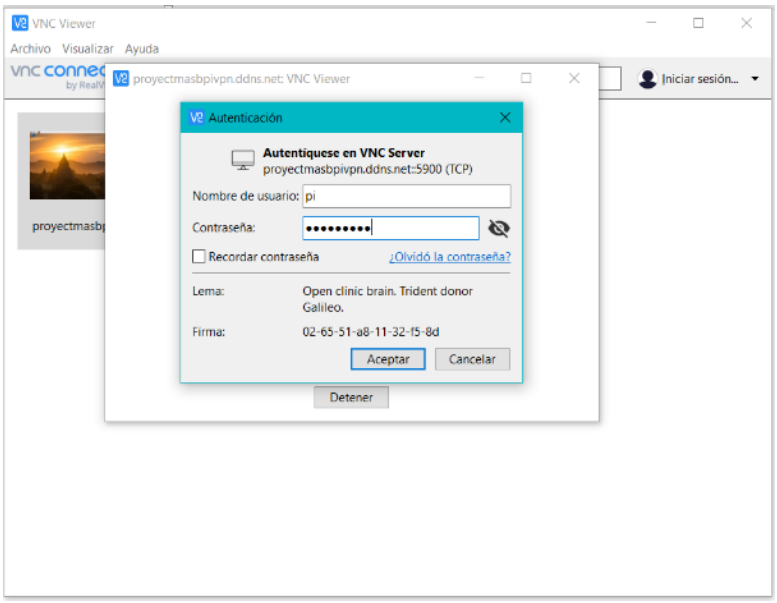
Dentro de la sesión del usuario, se habilitará la visualización de los ficheros y carpetas ocultos, como se observa en la ventana de la captura superior.

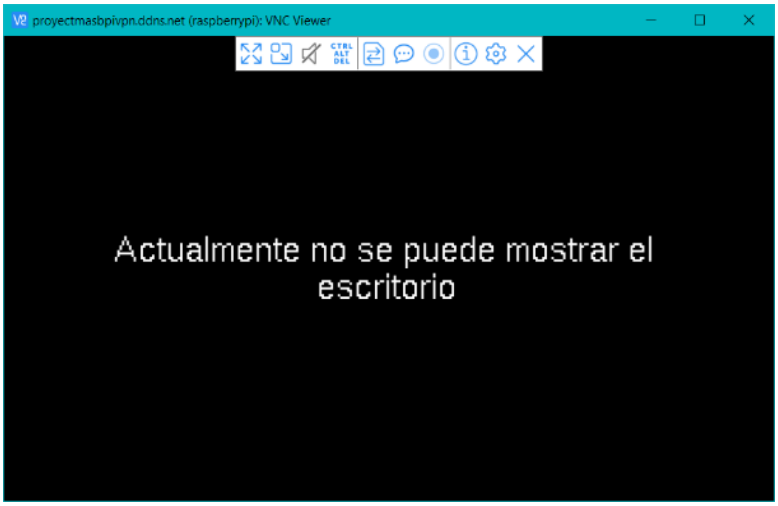


Una vez dentro de la carpeta oculta .ssh, ubicada dentro del directorio del usuario, se eliminarán los ficheros existentes, como se puede apreciar en la ventana de la captura superior, se selecciona con el botón derecho del ratón, en el menú que aparece se seleccionará Mover a la papelera, pudiendo cerrar en ese momento el explorador de archivos y comenzar nuevamente a establecer la conexión vía SSH sin que aparezca el problema.

Problema con RealVNC.

Realmente este problema, no se si se podrá interpretar como un problema o error, o puede ser que esta aplicación no se comporte como la aplicación Escritorio remoto de Microsoft, al intentar conectar con el servidor VPN/WOL, recordar que el servidor se encuentra configurado para que inicie en modo consola, en este proyecto siempre se indica que tras las acciones realizadas vía local o remota se salga del entorno gráfico dejando la sesión el servidor VPN/WOL, sin sesión iniciada y en modo consola.





Es por lo que no se si es un problema o la aplicación no lo permite, aunque al lanzar la aplicación desde un cliente, se solicita las credenciales de acceso, al proporcionarlas y pulsar el botón Aceptar, se muestra la ventana de la captura superior.

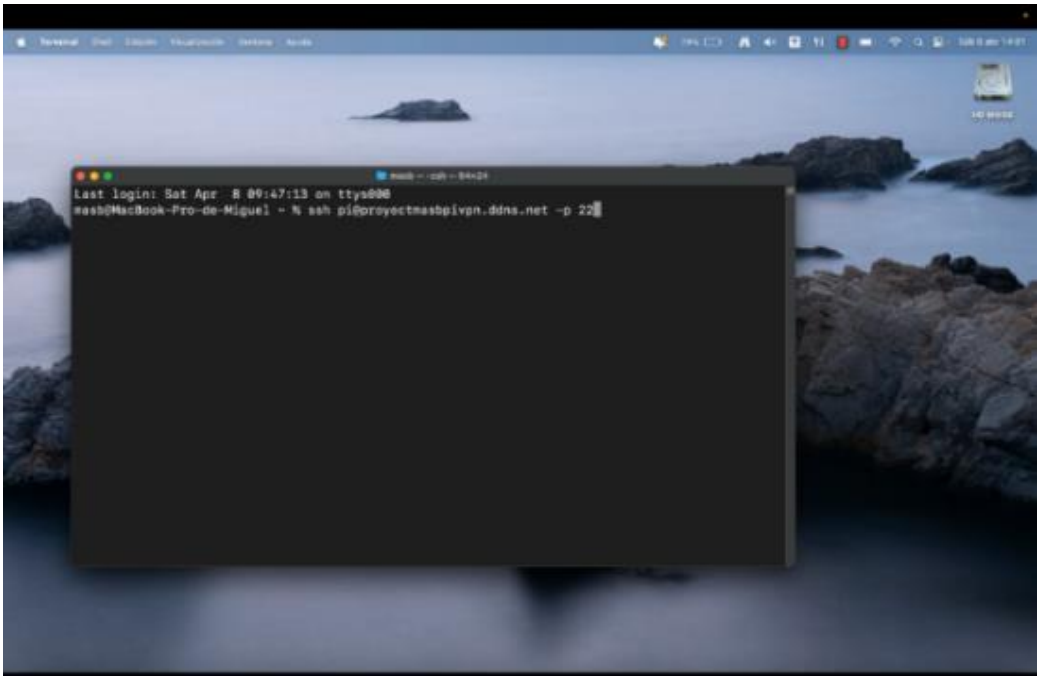
Si se deja el entorno gráfico activo, la conexión se produce sin mostrar el error.

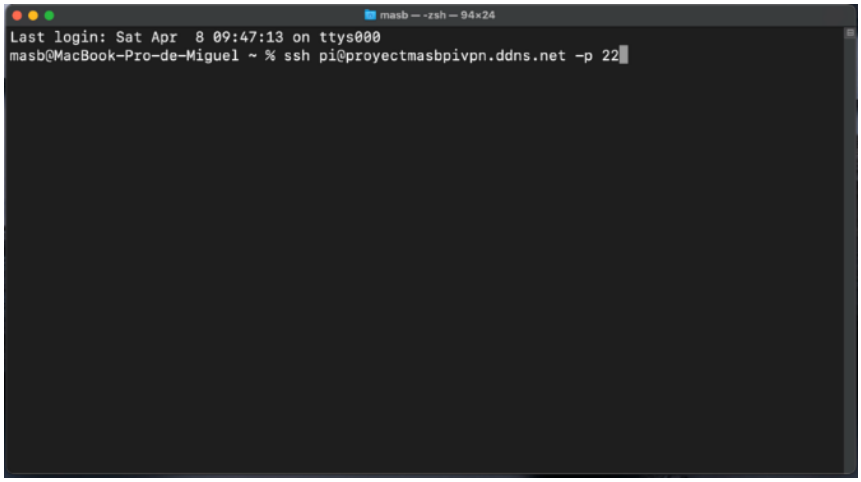
ANEXO

Conexión remota vía SSH.

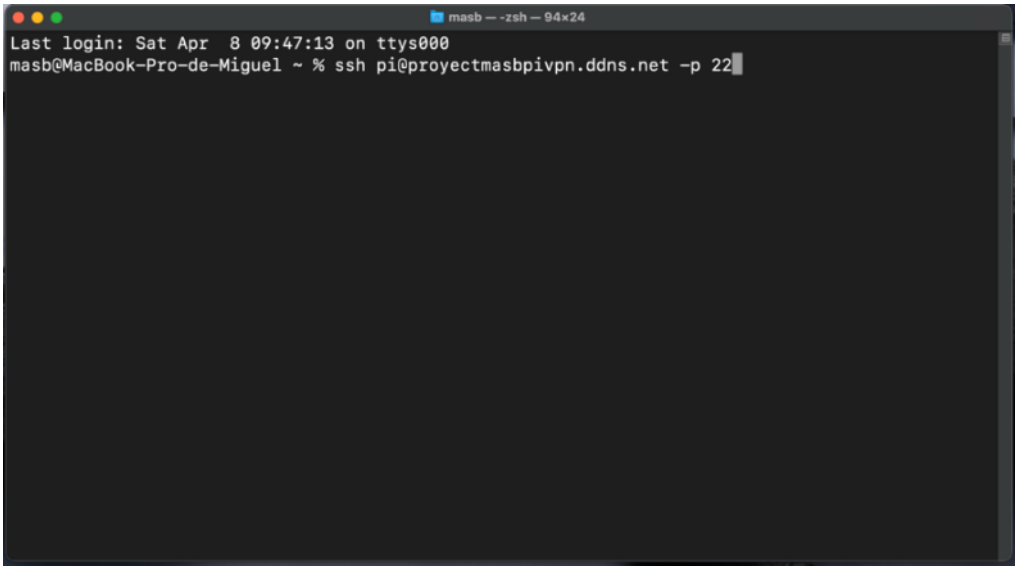
Conexión a través de terminal.

Para realizar esta explicación, solo se procederá en un S.O., puesto que lo único que varía sustancialmente es el hecho de que se realiza dentro de un terminal de Linux, Windows (Símbolo de sistema o CMD.) o un terminal en macOS.





En este ejemplo, se explica dentro del S.O. macOS, para lo que se accederá a un terminal.



Dentro del terminal, se establecerá una conexión vía SSH con el comando.

ssh “nombre de usuario”@”dirección IP, nombre de dominio o host” “opciones”

En el caso de no haber modificado el puerto por defecto para el acceso vía SSH, no es necesario indicar el puerto como se observa en la ventana de la captura superior, con la opción “-p 22”, puesto que el puerto por defecto del protocolo SSH es el 22.

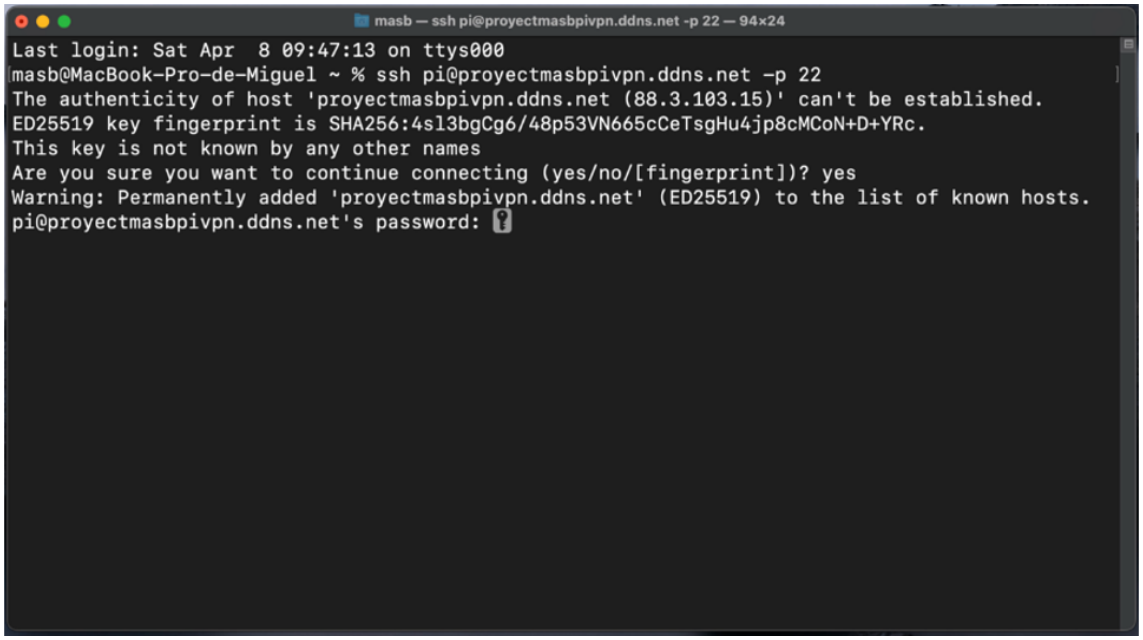
ssh pi@proyectmasbpivpn.ddns.net -p 22

Si se quiere hacer uso de la redirección “X” habrá que utilizar el comando.

ssh -X pi@proyectmasbpivpn.ddns.net -p 22

Para utilizar la redirección “X”, en Windows y en macOS se deberá tener instaladas las aplicaciones.

- Windows, Xming, e iniciada ejecutando la aplicación XLaunch.
- macOS, XQuartz, por las pruebas realizadas, no ha sido necesario tener en ejecución la aplicación XQuartz.
- Tener habilitado X11Forwarding en el servidor VPN/WOL (Raspberry Pi).



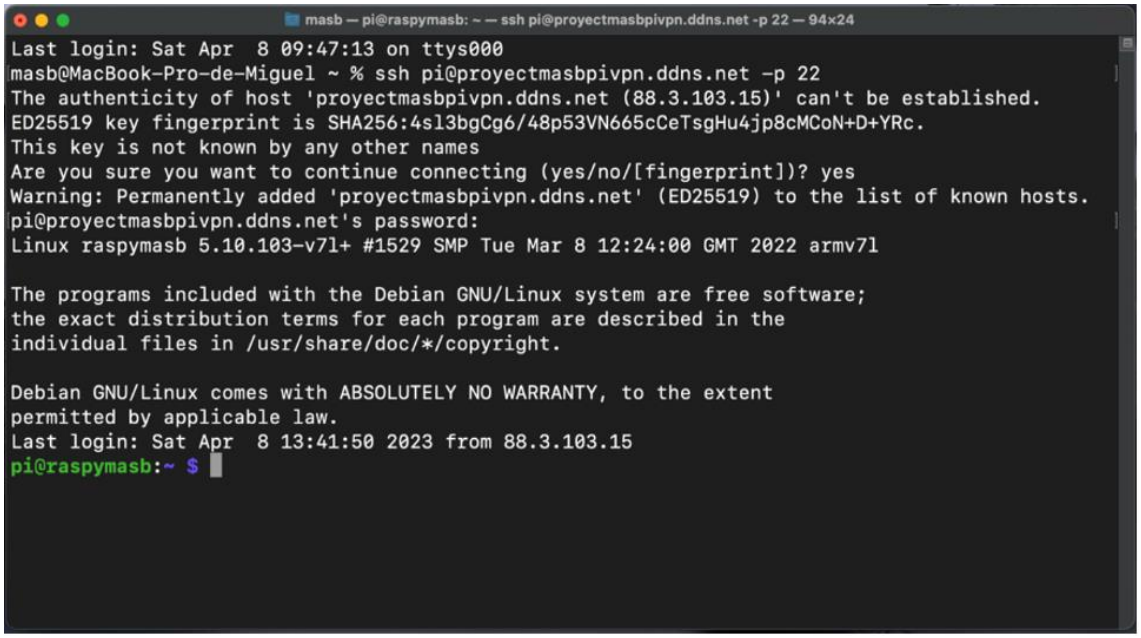
Si como en la ventana de la captura superior, es la primera vez que se establece la conexión, aparecerán los mensajes que se indican en la captura.

“The authenticity of host ‘proyectmasbpivpn.ddns.net (88.3.103.15)’ can´t be established.
ED25519 key fingerprint is `SHA256:4sl3bgCg6/48p53VN665cCeTsgHu4jp8cMCoN+D+YRc`
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?”

“No se puede establecer la autenticidad del host ‘proyectmasbpivpn.ddns.net (88.3.103.15)’.
La huella dactilar de la llave ED25519 es `SHA256:4sl3bgCg6/48p53VN665cCeTsgHu4jp8cMCoN+D+YRc`
Esta clave no es conocida por ningún otro nombre.
¿Está seguro de que desea continuar con la conexión (sí/no/[huella digital])?”

Se escribirá yes y se pulsará la tecla INTRO, pudiendo acceder vía SSH al dispositivo remoto.

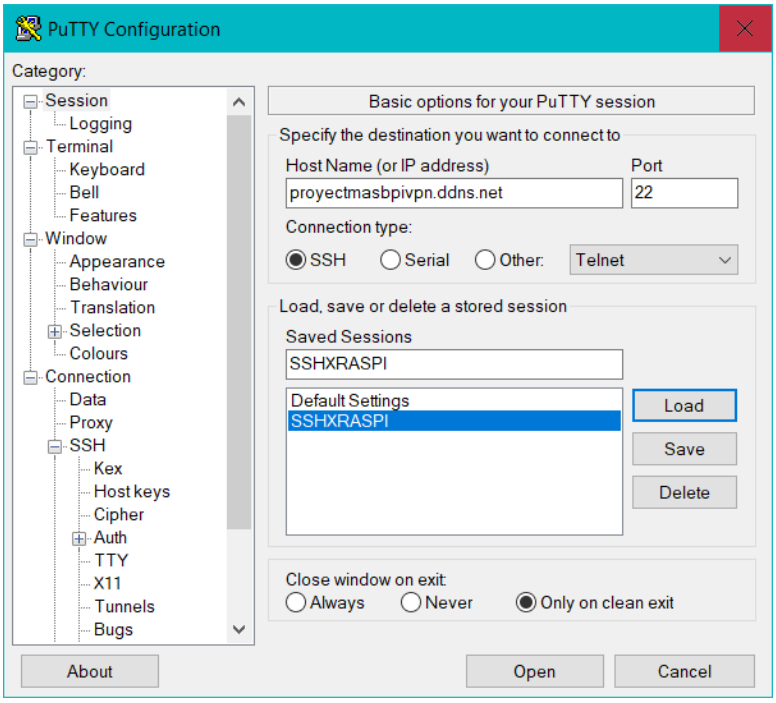
Se solicitará el password del usuario con el que se está intentando establecer la conexión, en este ejemplo se trata del usuario “pi”.



Una vez proporcionada la contraseña, se habrá establecido una sesión remota al dispositivo vía SSH.

En este caso, es como si nos encontrásemos sentados delante del monitor localmente y en el terminal de la Raspberry Pi.

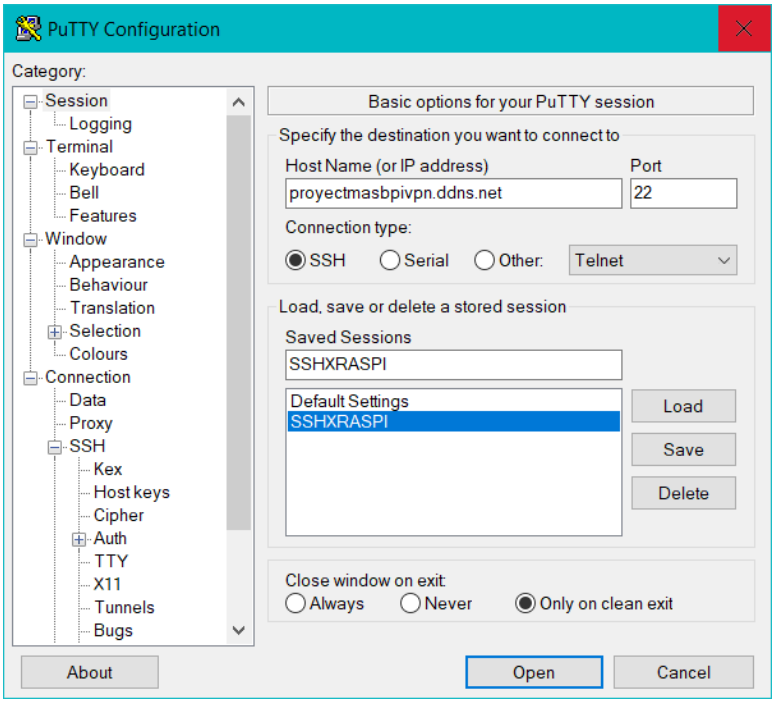
Conexión a través de la aplicación PuTTY S.O. Windows.

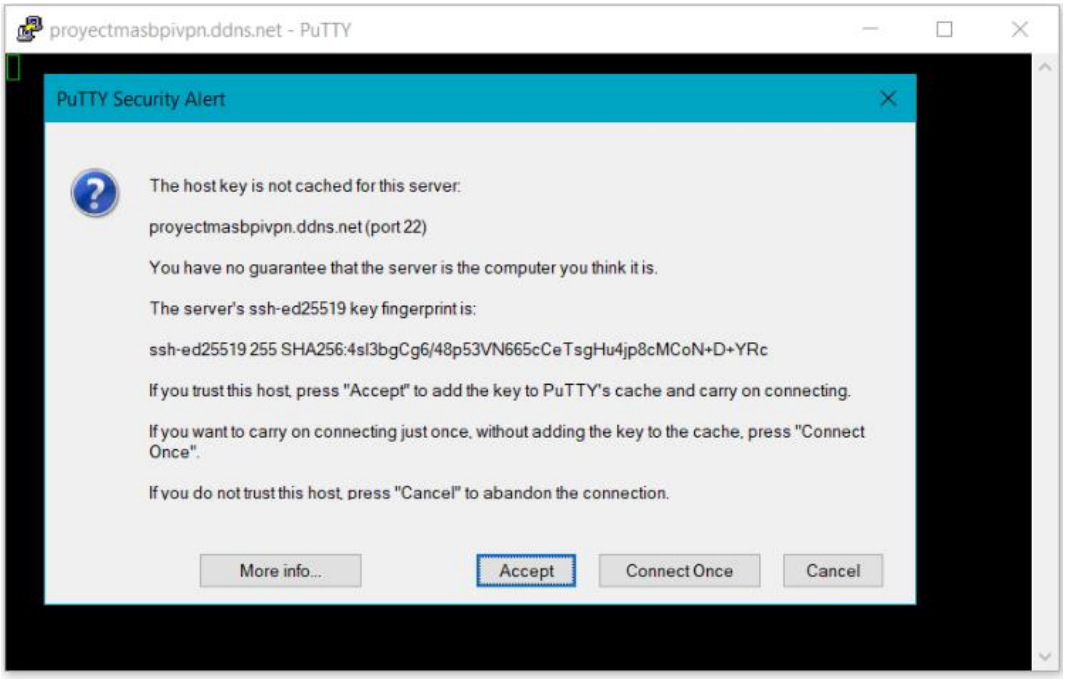


La configuración de la aplicación PuTTY, se explica en un apartado anterior.

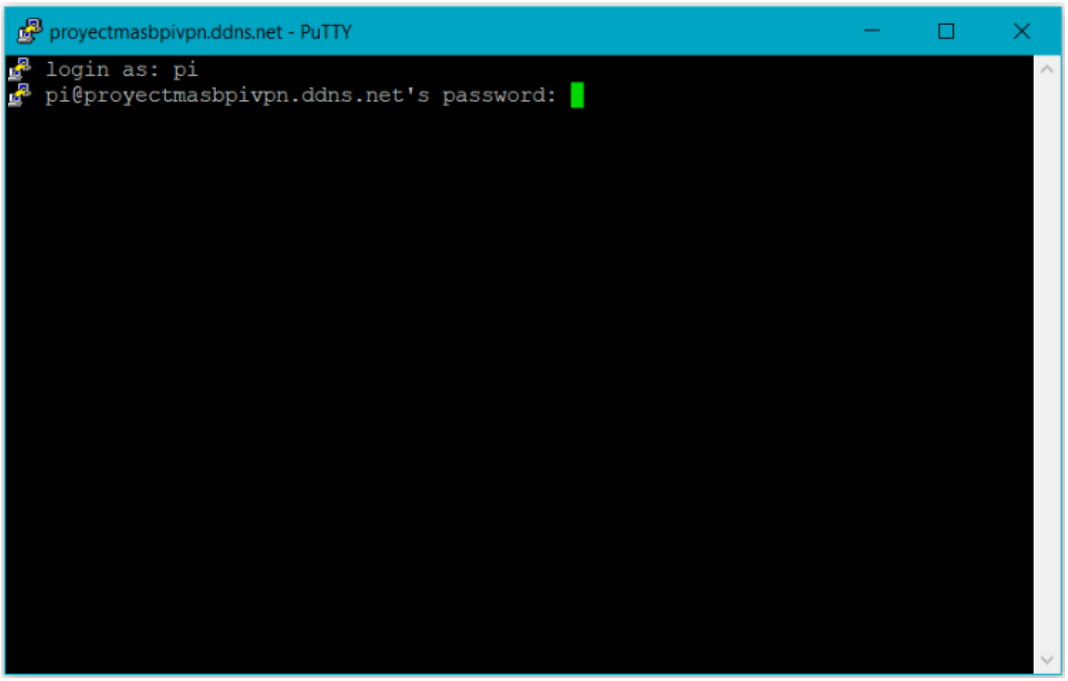
Una vez abierta y dentro de la aplicación PuTTY, se seleccionará la sesión guardada en el apartado Saved Sessions, en este ejemplo y como se explicó anteriormente, se trata de la sesión con el nombre SSHXRASPI, imagen captura superior y se pulsará el botón Load.

Posteriormente, tras pulsar el botón Load, se carga automáticamente la configuración guardada de la conexión, teniendo que pulsar sobre el botón inferior Open, para establecer la conexión, imagen captura derecha.

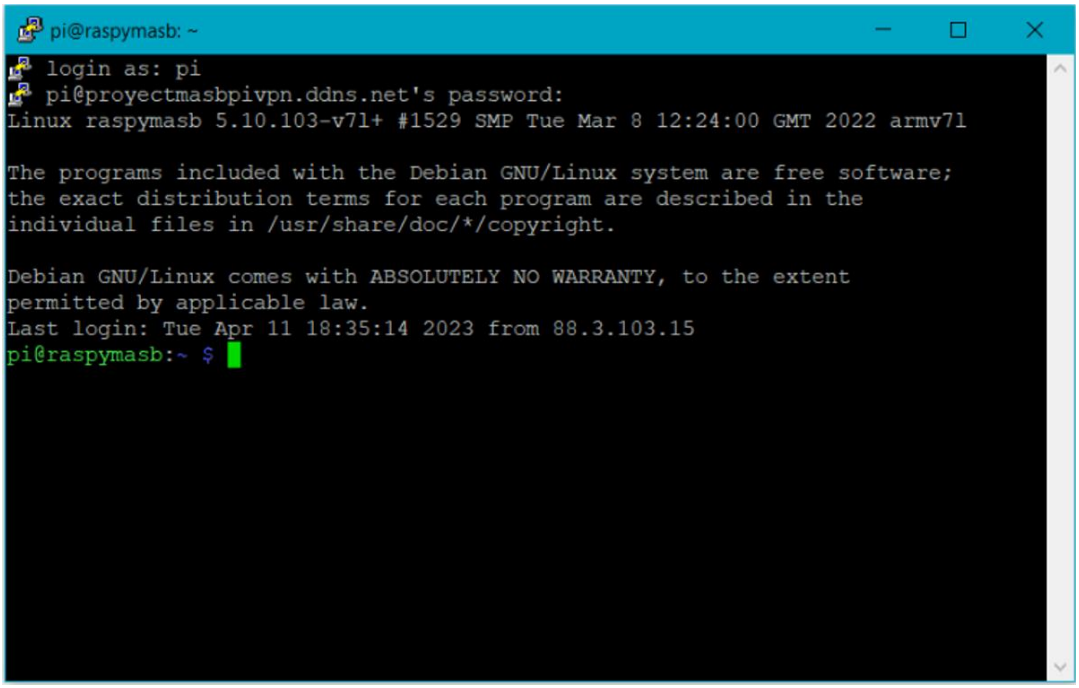




Si como en la captura de la ventana superior, es la primera vez que se establece la conexión con el servidor VPN/WOL, o el cliente, se mostrará la ventana que aparece, teniendo que pulsar sobre Accept.



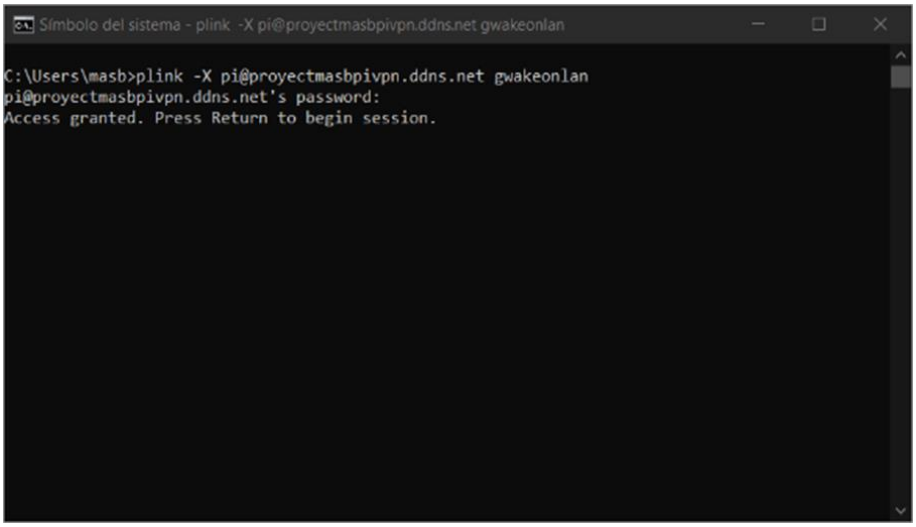
Como se puede apreciar en la ventana de la captura superior, al ya haber facilitado el usuario cuando se realizó la configuración y se guardó, al establecer la conexión solo habrá que facilitar la contraseña del usuario en cuestión y pulsar INTRO, para este proyecto el usuario utilizado es pi.



Una vez facilitada la contraseña y habiendo pulsado INTRO, se estará remotamente conectado en un terminal vía SSH a la Raspberry Pi.

Conexión usando el comando plink.

Esta aplicación, se instala al instalarse la aplicación PuTTY.



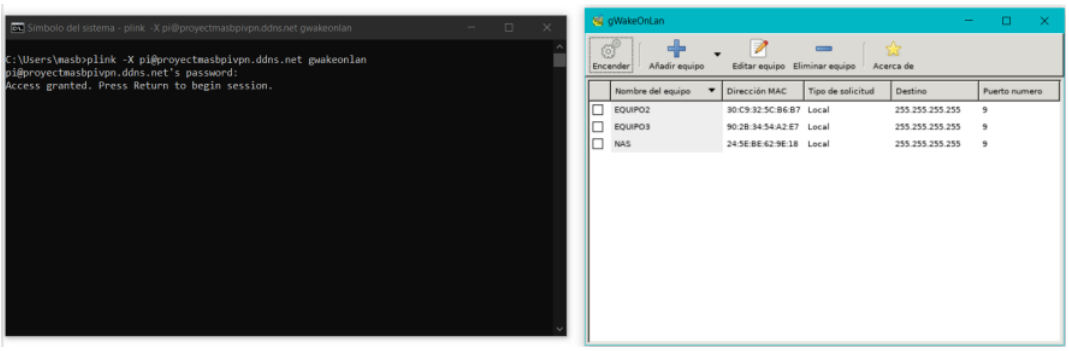
Otra opción para iniciar remotamente una aplicación gráfica y teniendo en el S.O. Windows iniciada la aplicación Xming, es simplemente, ejecutar dentro de un Símbolo del Sistema “CMD” el comando.

plink -X usuario@”dirección IP, nombre de dominio o host” nombre_aplicación

plink -X pi@proyectmasbpivpn.ddns.net gwakeonlan

Se tendrá que facilitar la contraseña del usuario, en este ejemplo, se trata del usuario pi, una vez facilitada la contraseña, se pulsará (Return) INTRO, en el mensaje que aparece indicando.

“”Access granted. Press Return to begin session.””
“”Acceso permitido. Presione Retorno para comenzar la sesión.””



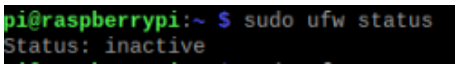
Tras pulsar INTRO, aparecerá pasado un momento, la aplicación instalada en el servidor VPN/WOL (Raspberry Pi), en el escritorio del equipo con S.O. Windows.

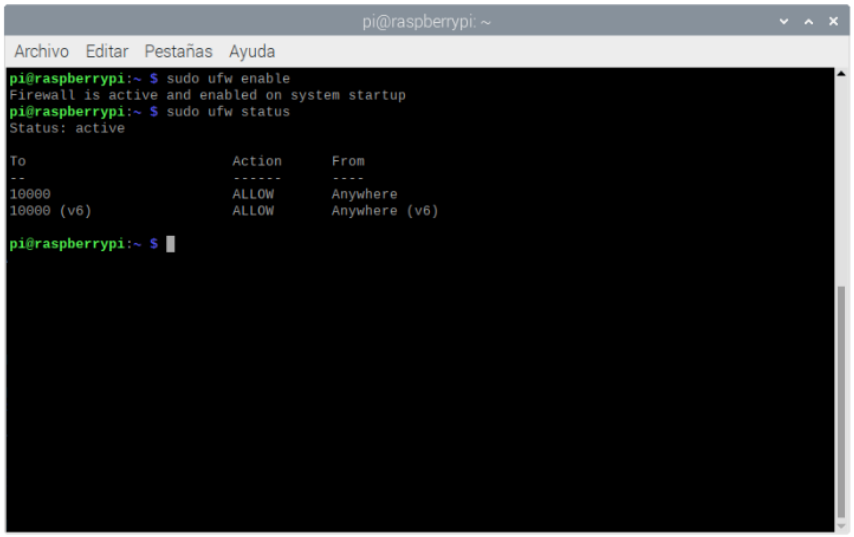
Configurar o habilitar tráfico en cortafuegos Linux ufw.

Para que ciertas características en este proyecto funcionen correctamente, es necesario como se explicó anteriormente, la apertura de ciertos puertos en el router, este es el facilitado por el proveedor de servicios de Internet (ISP), otra cosa importante es habilitar el tráfico dentro del servidor Linux VPN/WOL, al tratarse este de un S.O. Linux, Raspberry Pi OS, más concretamente una variante de Debian, en este proyecto se instala y se utiliza el cortafuegos ufw.

Estos ejemplos utilizados, son ejemplos con los números de puerto por defecto casi siempre, en caso de modificarlos, habrá que realizar las configuraciones necesarias para utilizarlos.

Para comprobar el estado del cortafuegos, si se encuentra activo o no, se podrá utilizar el comando.
sudo ufw status

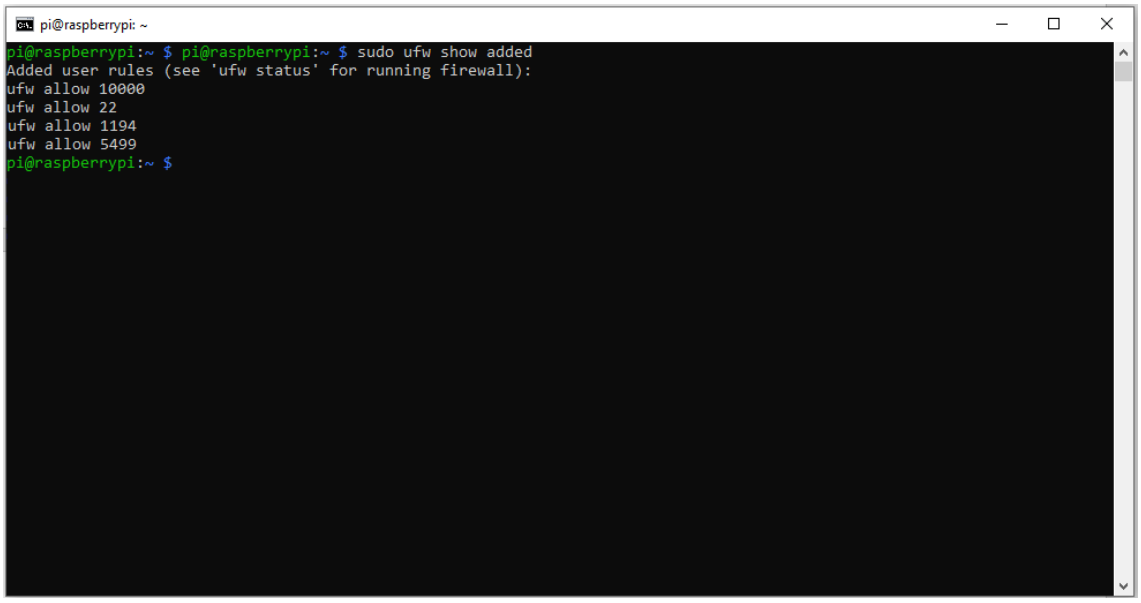




Si se encuentra inactivo, se ejecutará el comando.
sudo ufw enable

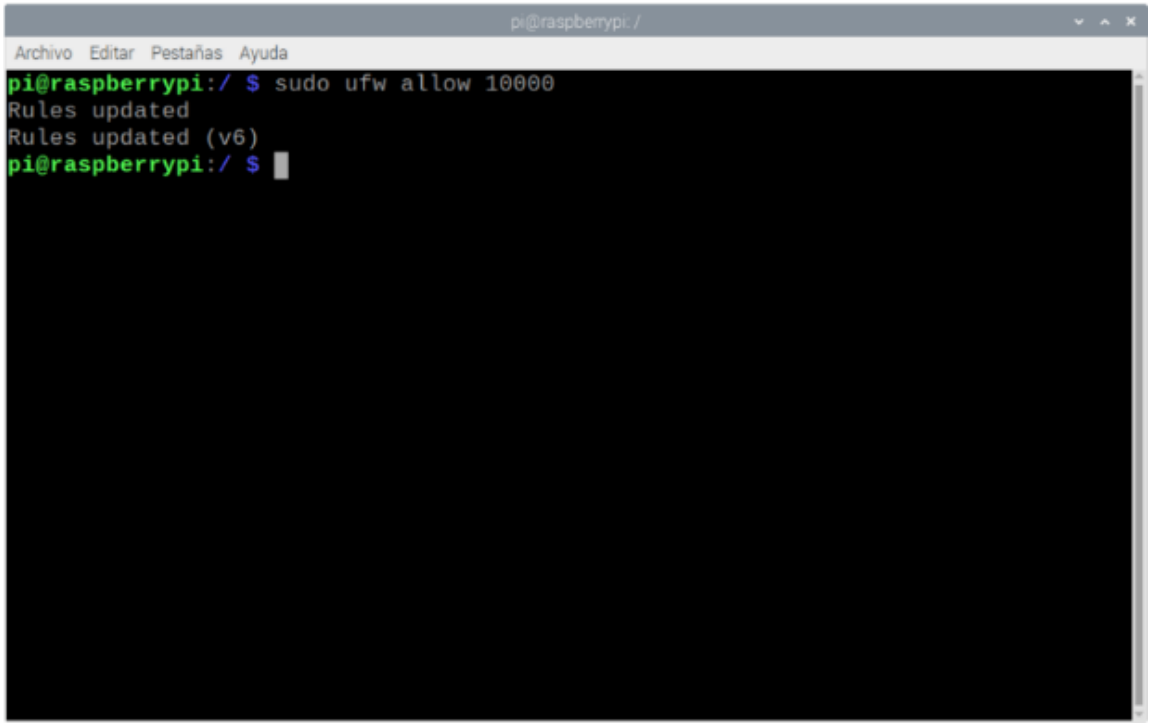
Con el comando sudo ufw status, sudo ufw status verbose o sudo systemctl status ufw, se muestra el estado del cortafuegos como las reglas, con la ejecución del último comando indicado (sudo systemctl status ufw), no se muestran las reglas, con este comando se puede comprobar el estado, iniciarlo, reiniciarlo o incluso detenerlo.

En el ejemplo de la ventana superior, solo se permitió “Action”, “allow” el tráfico al puerto “To”, puerto “10000”, desde cualquier red “From”, “Anywhere”, habitualmente WEBMIN utiliza el puerto 10000.



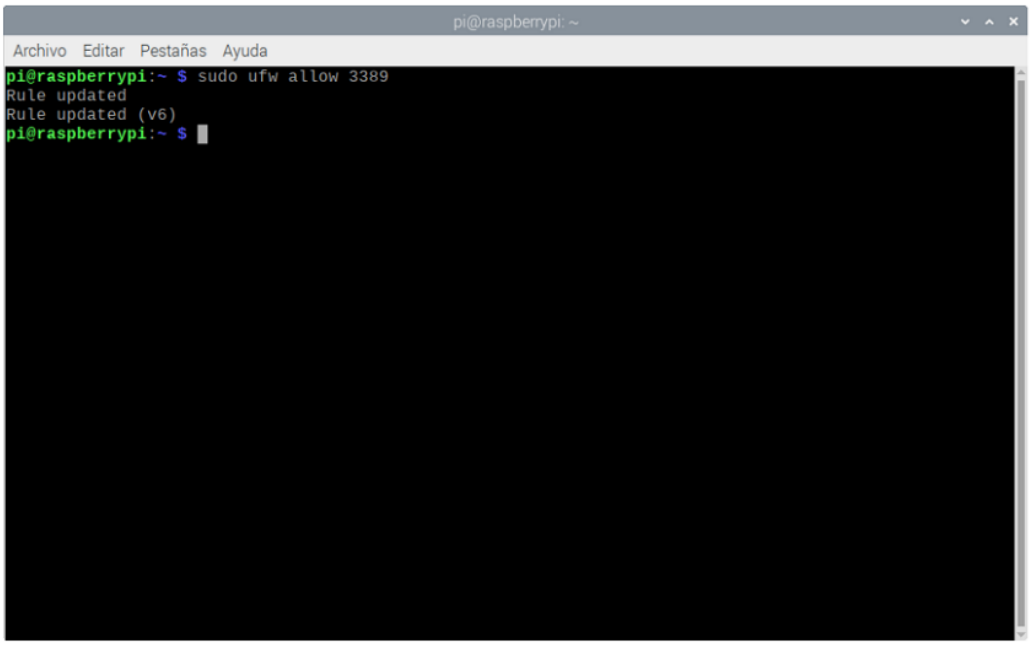
De usuario, comando sudo ufw show added

Ejemplo de uso básico, apertura tráfico para conexión WEBMIN.



Dentro del terminal, en el servidor VPN/WOL, remotamente o de forma local, se ejecutará el comando.

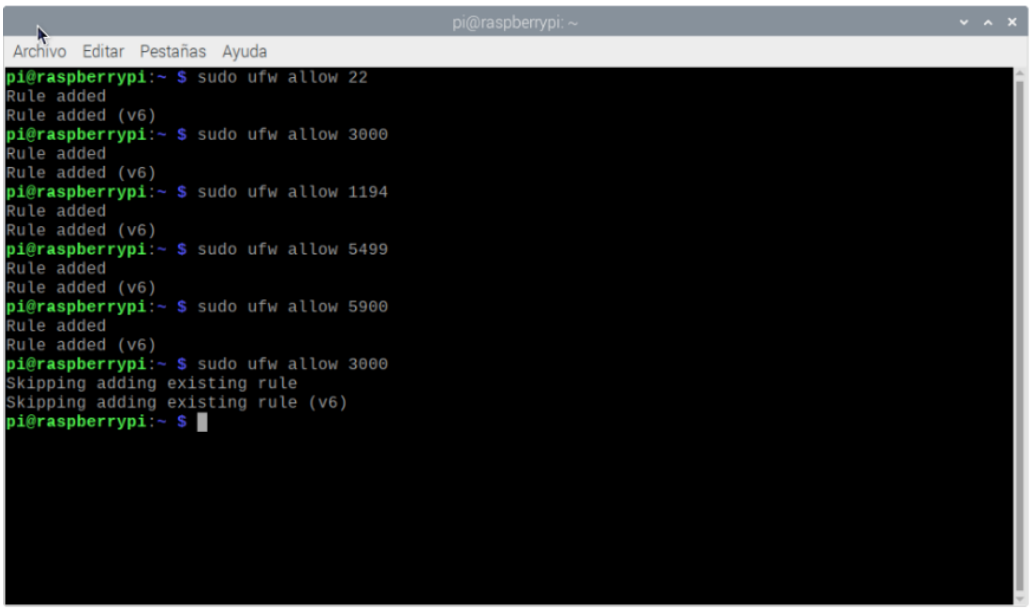
sudo ufw allow 10000



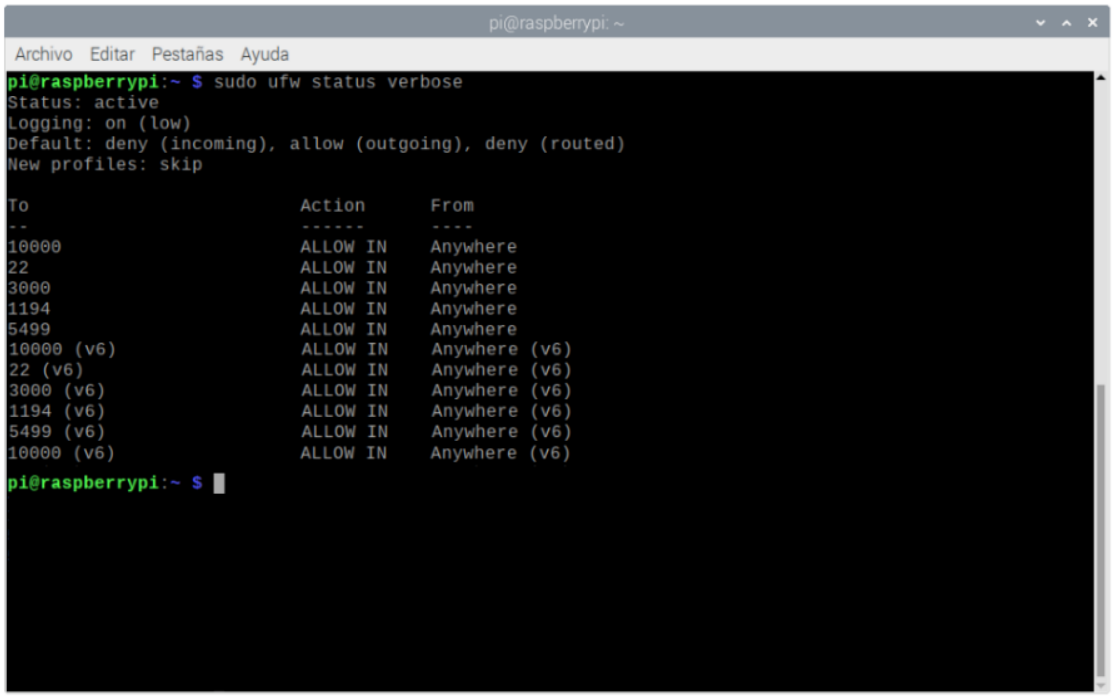
Ejemplo de uso básico, apertura tráfico para conexión RDP en el servidor VPN/WOL, comando.

sudo ufw allow 3389

En la captura de la imagen superior, se muestra el resultado de ejecutar el comando sudo ufw allow 3389, tras haberlo ejecutado previamente.



Como se puede observar en la ventana de la captura superior, se habilita el tráfico con el comando básico a los puertos 22, 3000, 1194, 5499, si se ejecuta el comando sobre una regla ya establecida, se informará como se puede apreciar en el último intento.

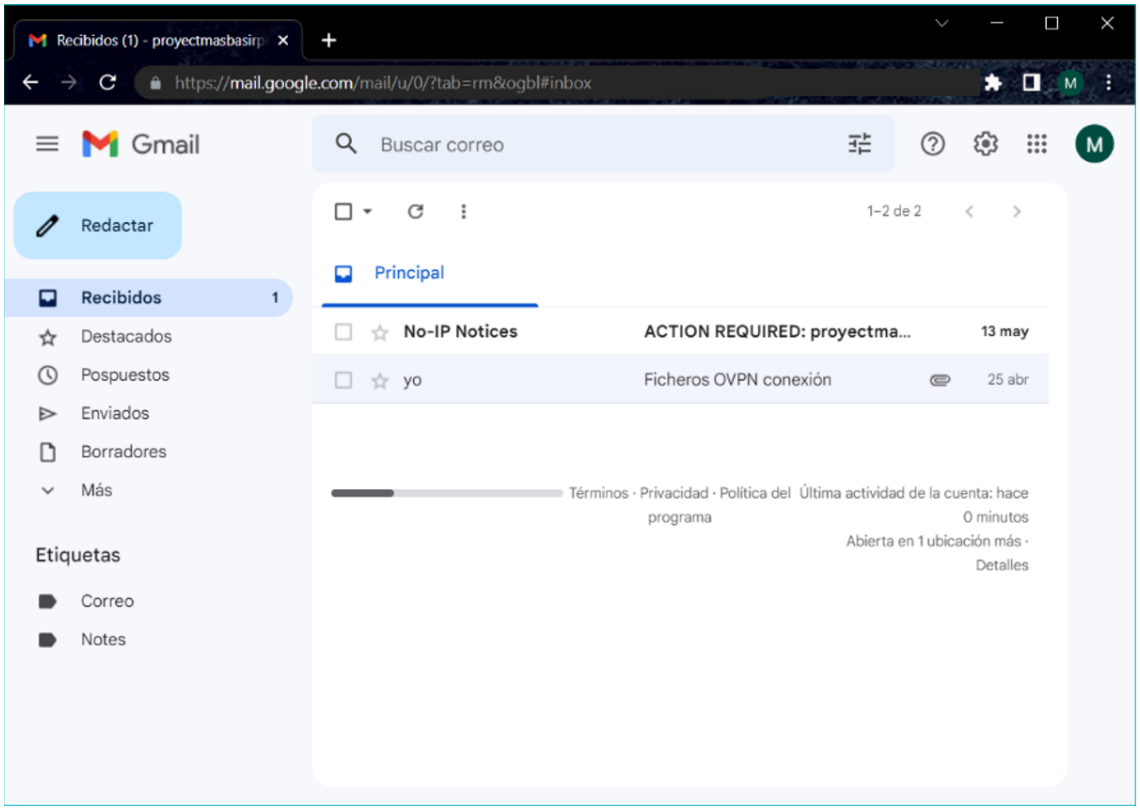


Habrá que habilitar el tráfico por tantos puertos/protocolos etc., como sea necesario, en este ejemplo, se muestra un ejemplo básico de cómo llevarlo a cabo.

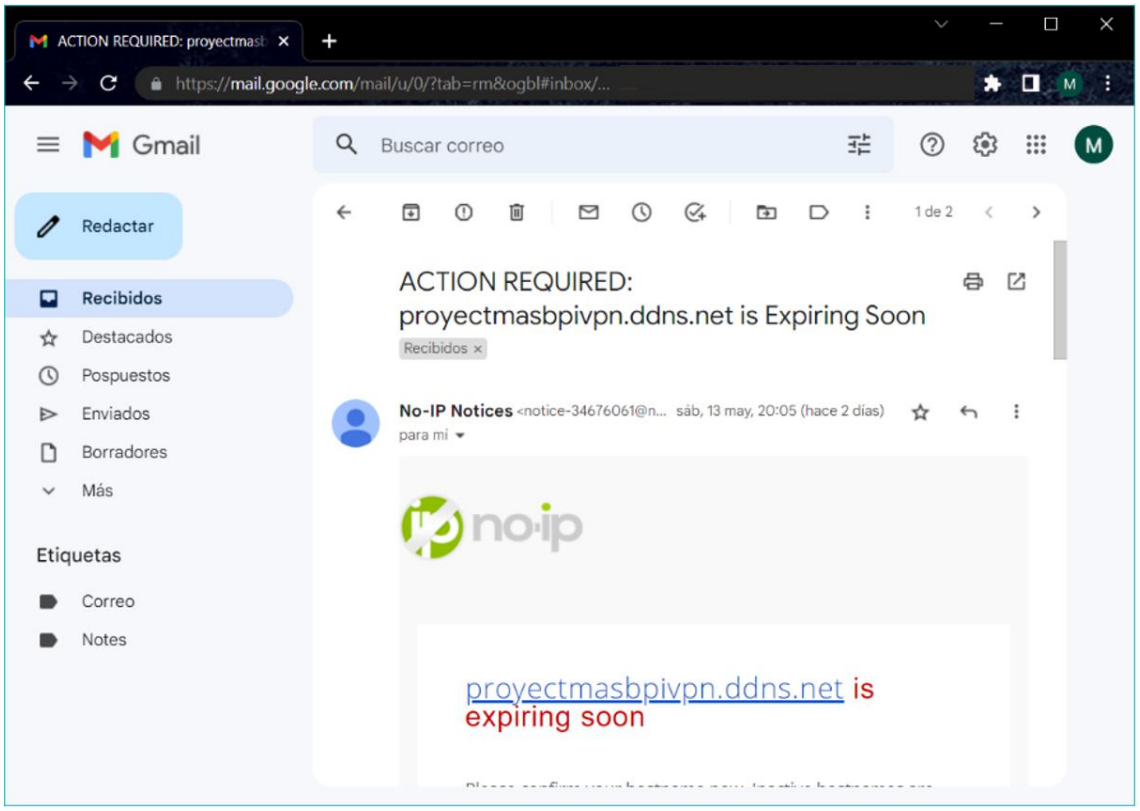
Estos ejemplos utilizados, son ejemplos con los números de puerto por defecto casi siempre, en caso de modificarlos, habrá que realizar las configuraciones necesarias para utilizarlos.

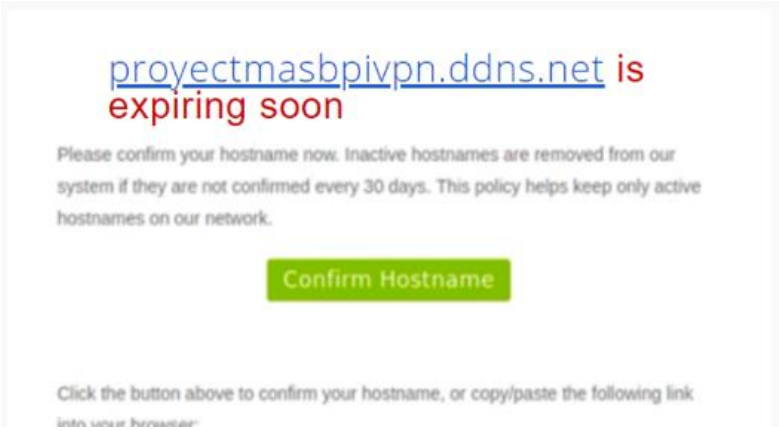
Actualización renovación nombre de domino o host proveedor servicios DDNS.

Como se mencionó anteriormente, la cuenta que se crea expresamente para este proyecto en el proveedor de servicios DDNS es gratuita, es por lo que cada “X” tiempo, cada 30 días, habrá que renovar o actualizar el nombre de dominio o host creado.

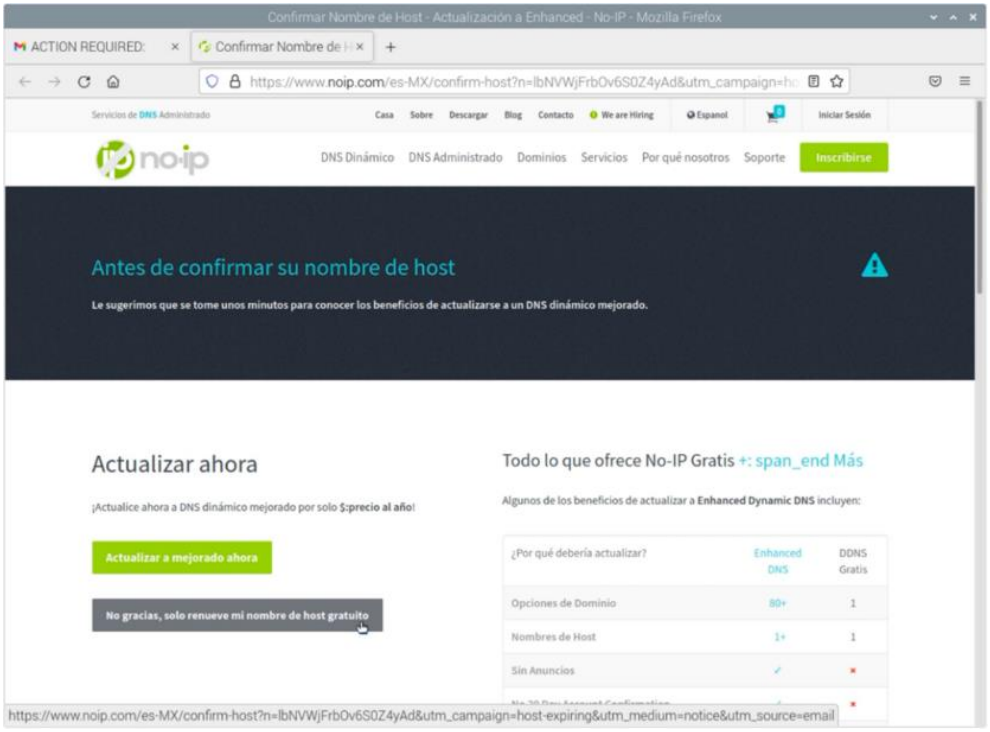


Habitualmente, se recibirá en la cuenta de correo utilizada para la creación del nombre de dominio o host, un correo enviado por el proveedor de servicios DDNS, indicando que se requiere una acción, en este ejemplo, el correo lo envió el proveedor No-IP.

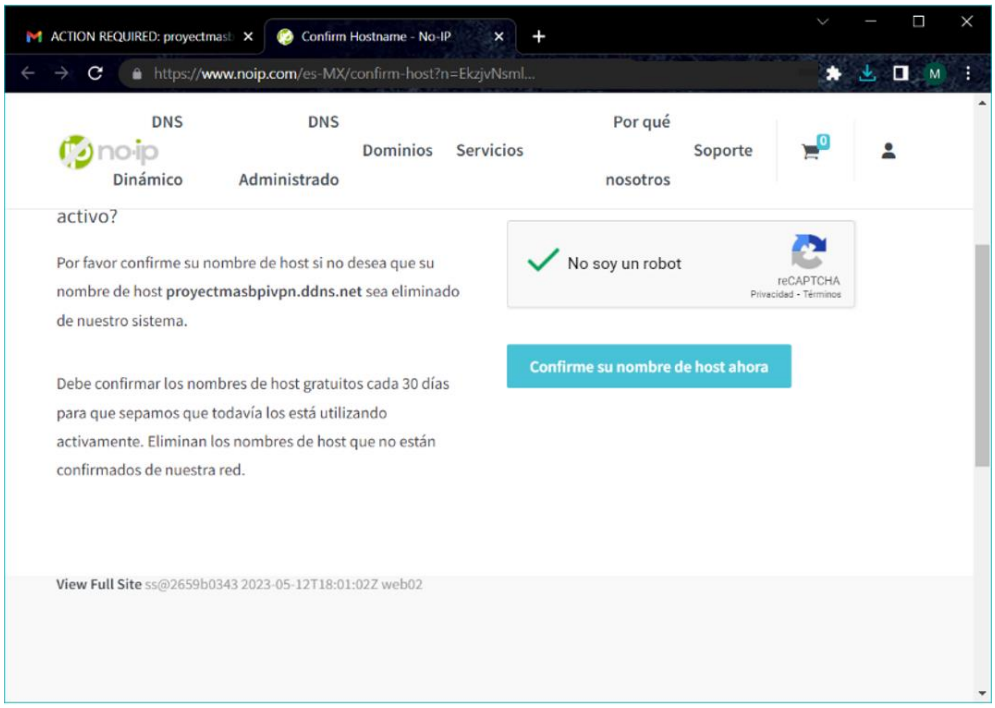




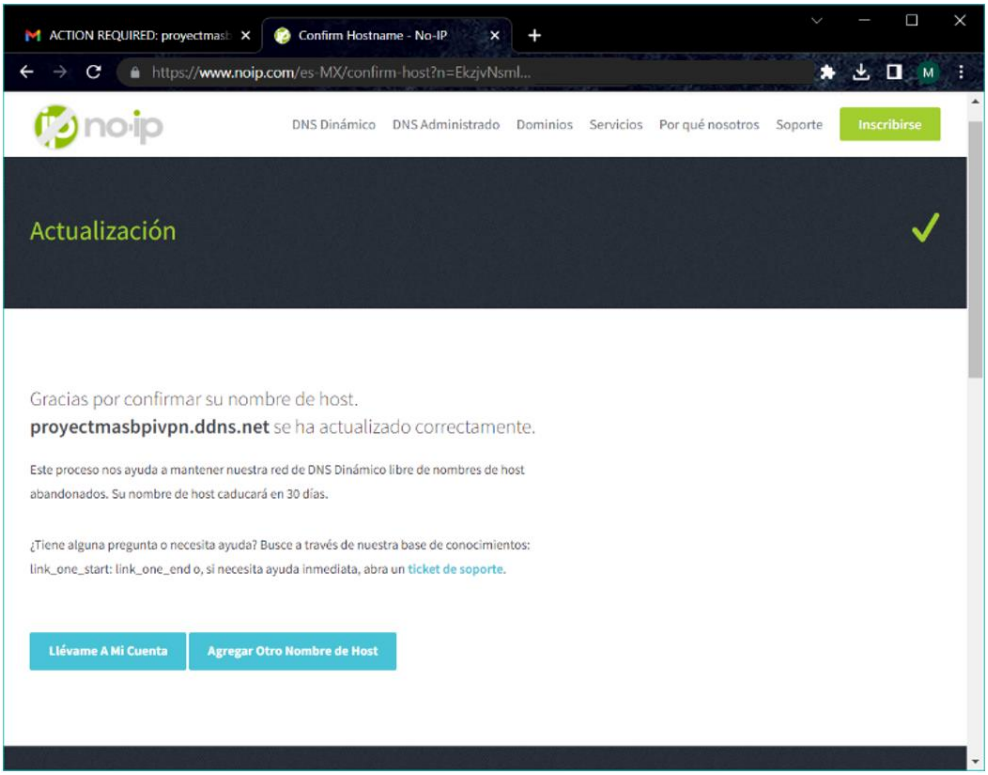
Al abrir el correo, se tendrá que localizar y pulsar sobre el botón inferior, Confirm Hostname.



En el caso de aparecer primero la ventana de la captura superior, se pulsará sobre el botón, “No gracias, solo renueve mi nombre de host gratuito”.



En la nueva ventana que aparece, como se aprecia, se seleccionará No soy un robot, en el apartado derecho Verificación CAPTCHA, acto seguido, se tendrá que pulsar sobre el botón azul, Confirme su nombre de host ahora.



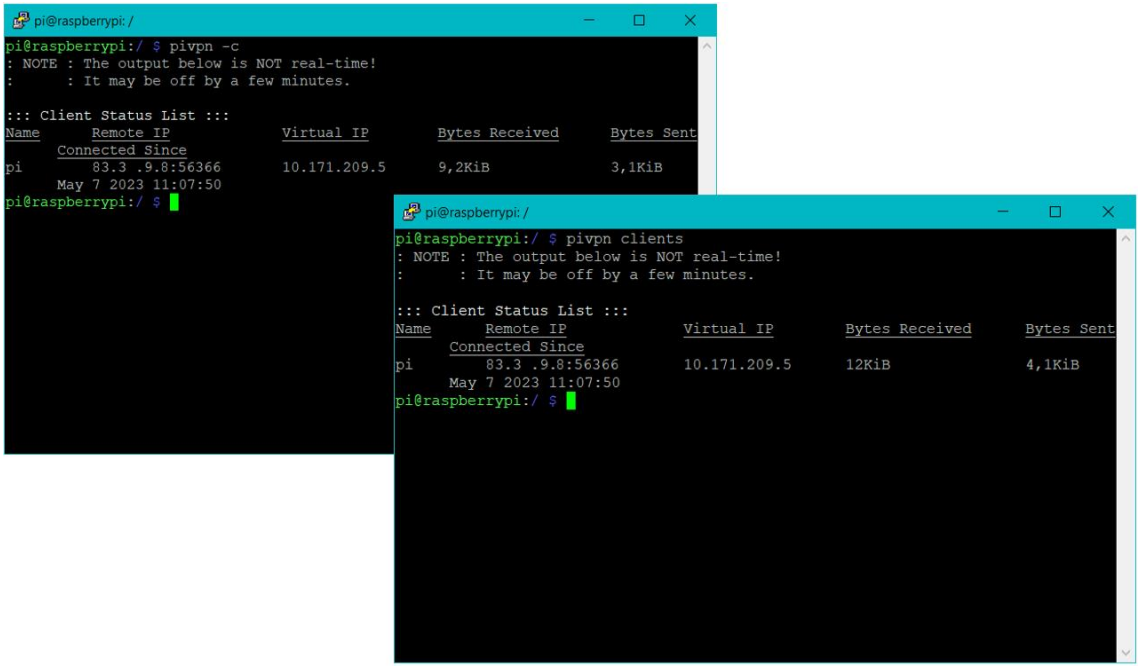
Como se puede observar en la ventana de la captura superior, la confirmación del nombre de dominio o host es satisfactoria, pudiendo cerrar la ventana y el correo.

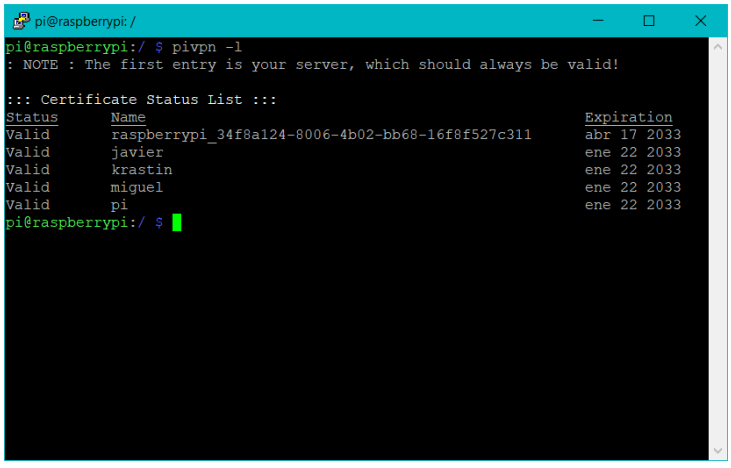
Comprobación usuarios conectados y su estado en servidor PiVPN.

Como administrador, si se tiene la necesidad de comprobar que clientes se encuentran conectados al servidor VPN/WOL, estas acciones se podrán realizar dentro de un terminal conectado al servidor, o incluso vía terminal conectado a través de SSH, como se indica a continuación, estando conectado remotamente como se puede apreciar en las capturas vía SSH, se podrá utilizar los comandos.

Comandos para comprobar los clientes conectados al servidor VPN/WOL.

pivpn clients
pivpn -c

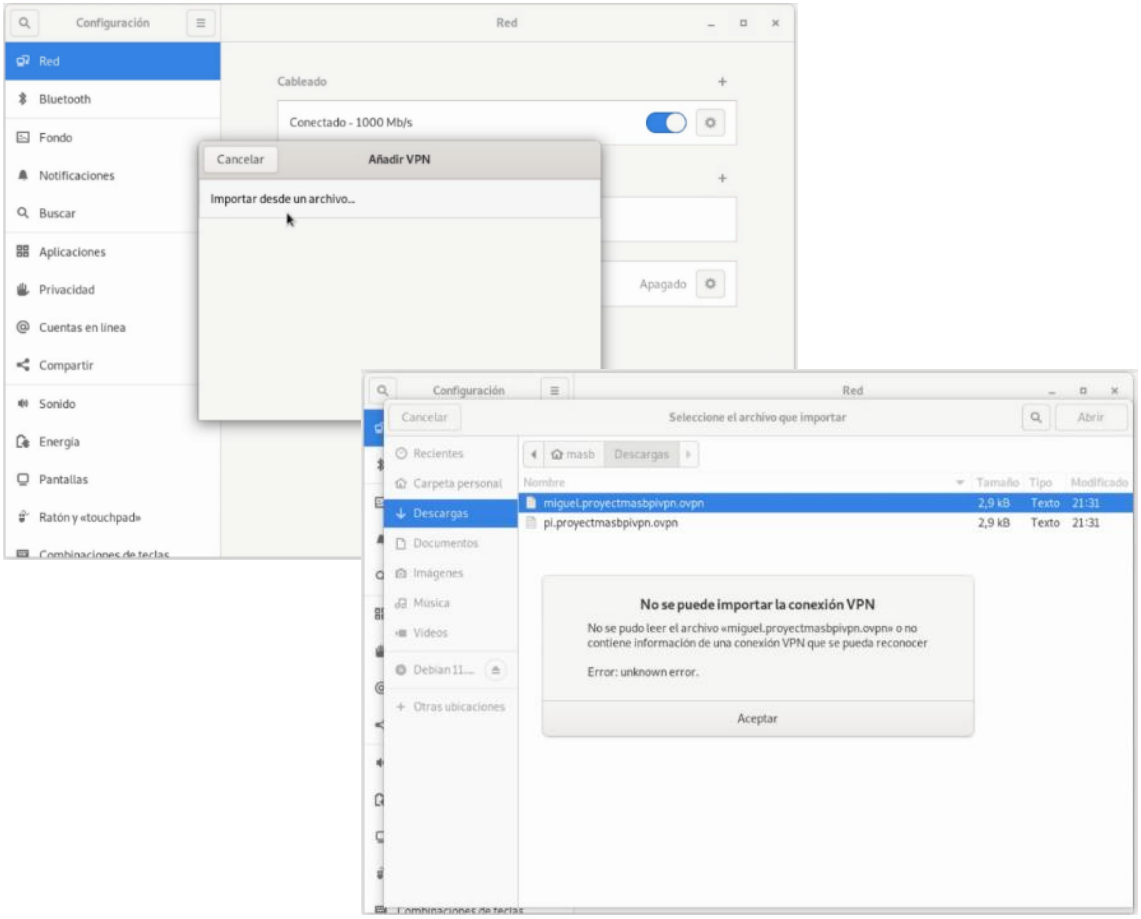




Mientras que si se quiere comprobar el estado de los clientes, se podrá ejecutar el comando.

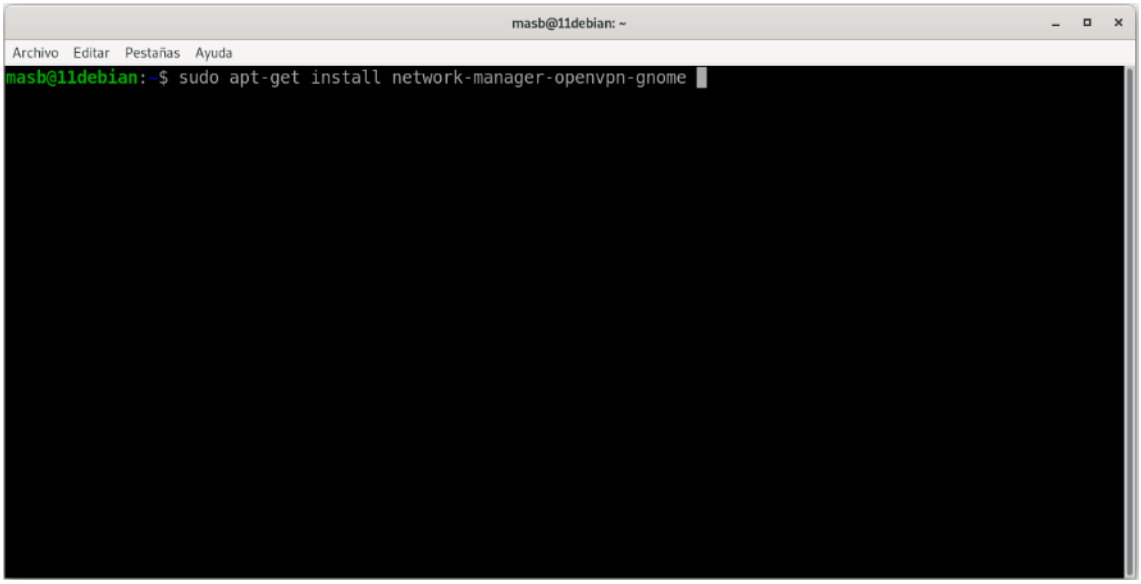
pivpn -l

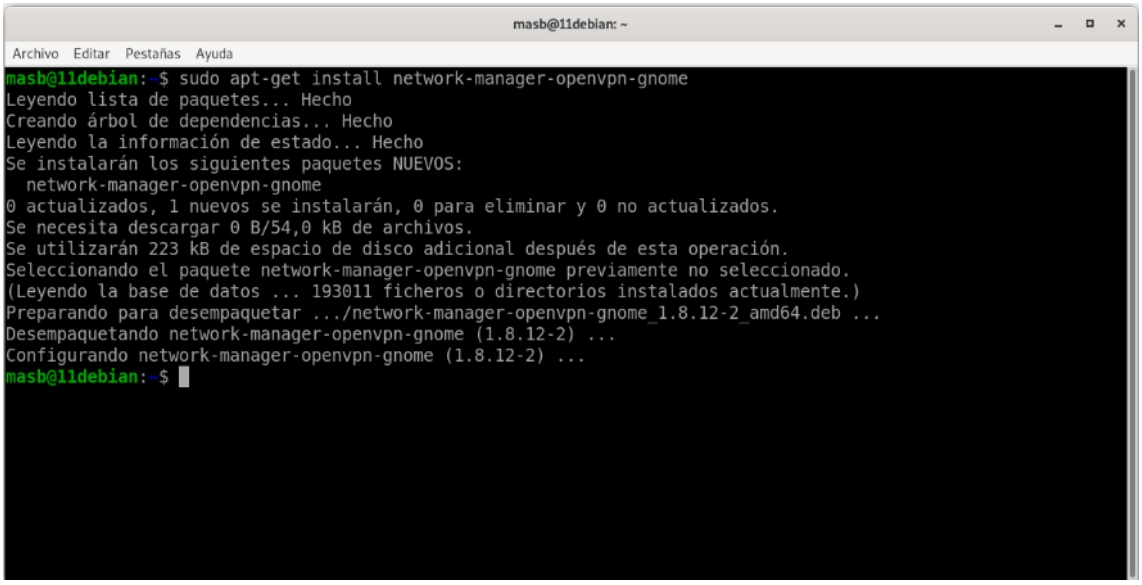
Posibilitar configuración fichero OpenVPN cliente Linux Debian.





Se ha detectado que al intentar importar la configuración creada en el servidor VPN/WOL, en un cliente con distribución Linux Debian, se muestra la ventana de la captura superior.





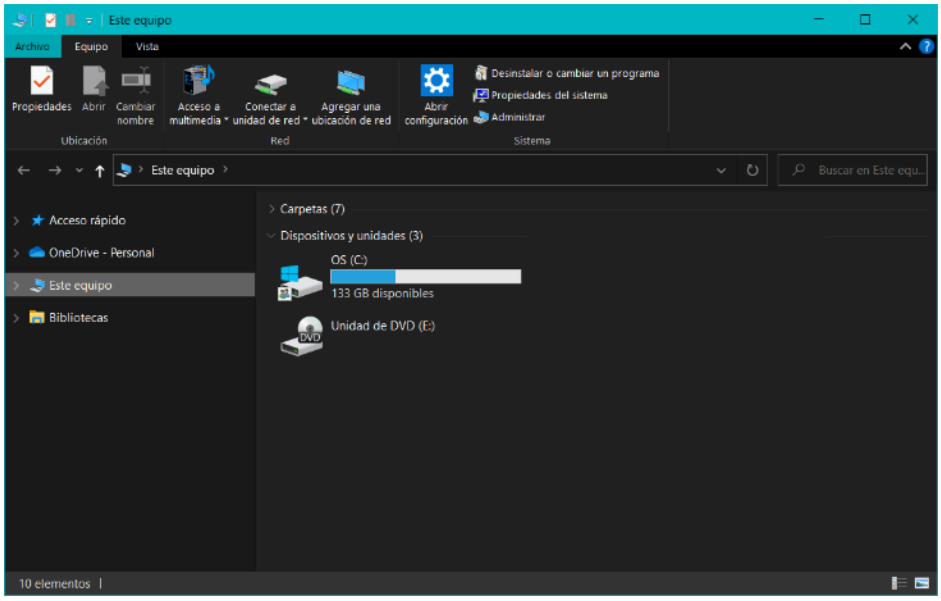
En el equipo con S.O. Linux Debian, para posibilitar el uso de los ficheros de configuración a la conexión VPN de un usuario, dentro de su sesión, se accederá a un terminal y se ejecutará el comando.

sudo apt-get install network-manager-openvpn-gnome

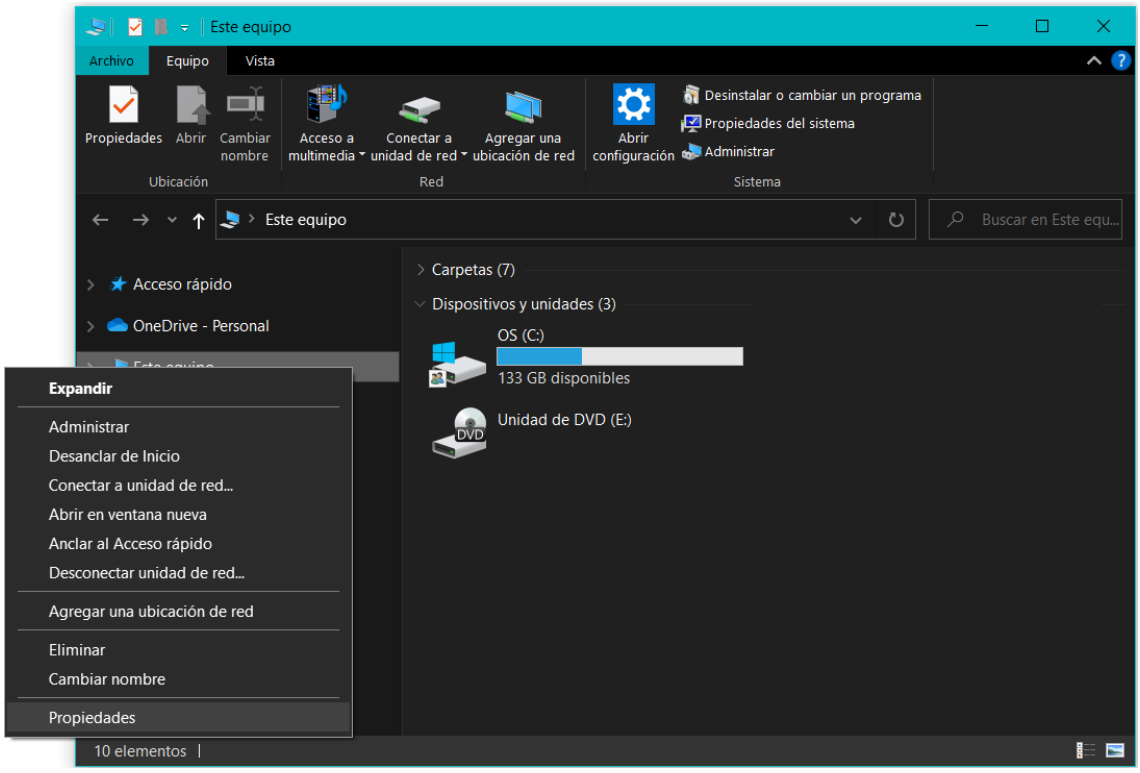
En el caso de existir dependencias al instalar la aplicación, se instalarán pulsando la tecla “S”, posteriormente se pulsará INTRO.

Terminada la instalación de la aplicación y de la instalación de las posibles dependencias, ya se podrá utilizar e importar la configuración del fichero ovpn, como se explicó anteriormente en el apartado correspondiente.

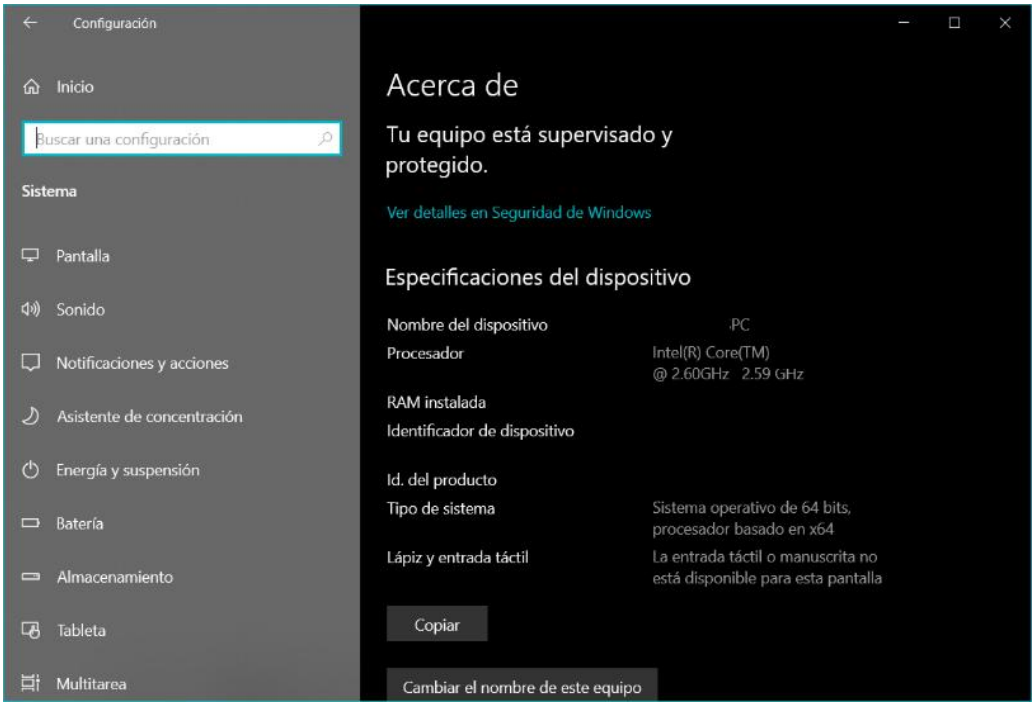
Habilitar conexión remota en cliente S.O. Windows.

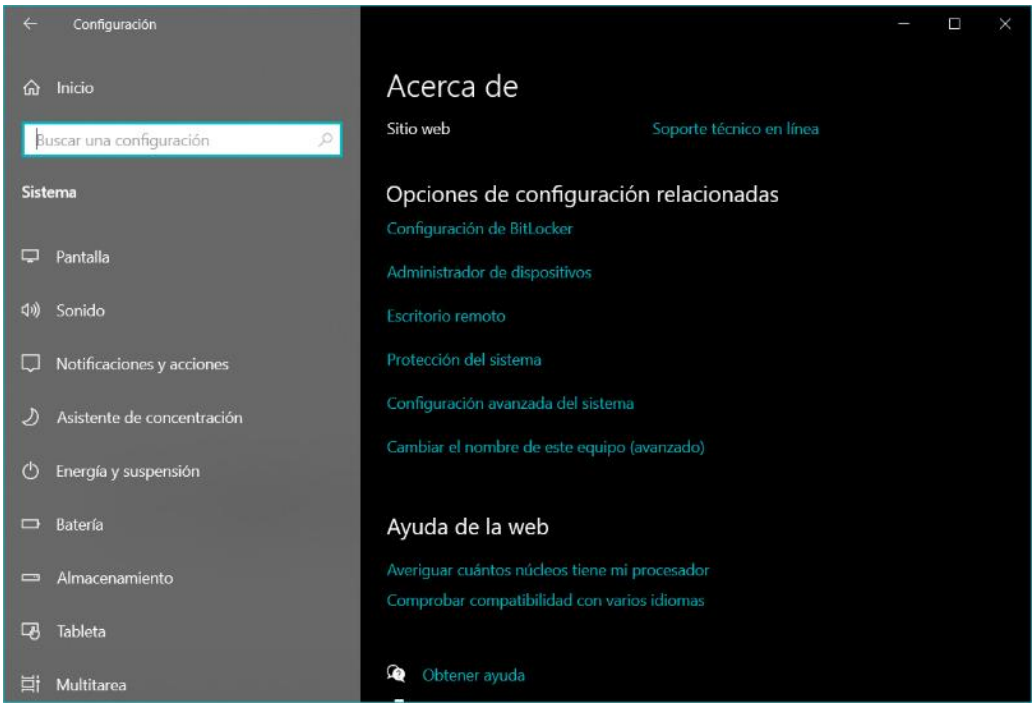


Dentro de la sesión de un usuario, se abrirá el explorador de archivos de Windows.



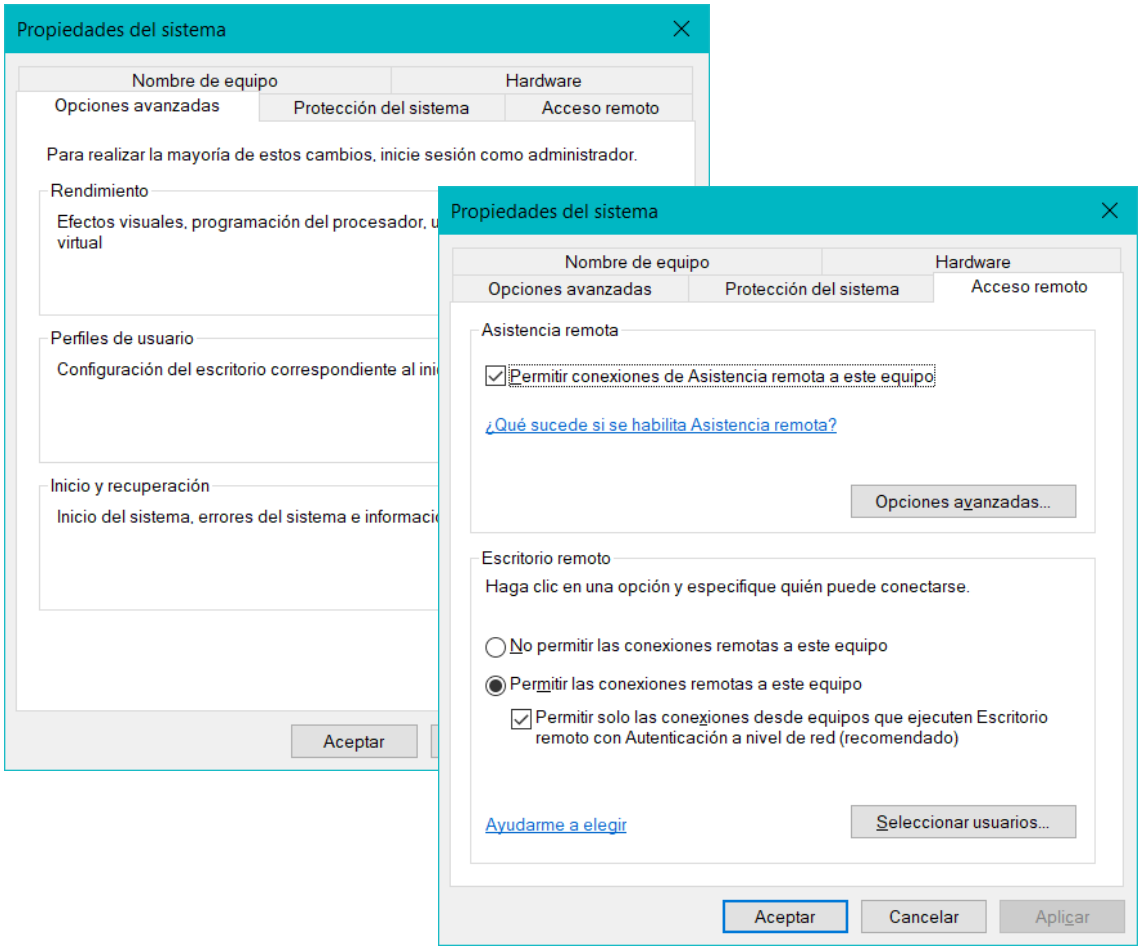
En el panel izquierdo, dentro de Este equipo, se pulsará con el botón derecho del ratón sobre Este equipo, en el menú que se muestra, se pulsará sobre Propiedades.



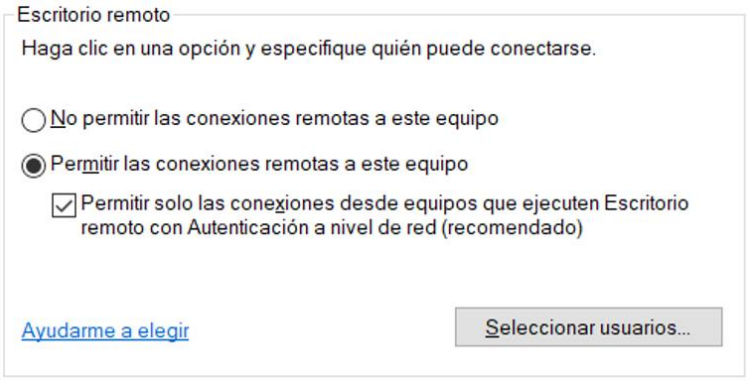


Configuración avanzada del sistema

Al abrirse la ventana Acerca de, dentro de Configuración, habrá que localizar el apartado Configuración avanzada del sistema, localizado el apartado, se pulsará sobre Configuración avanzada del sistema.

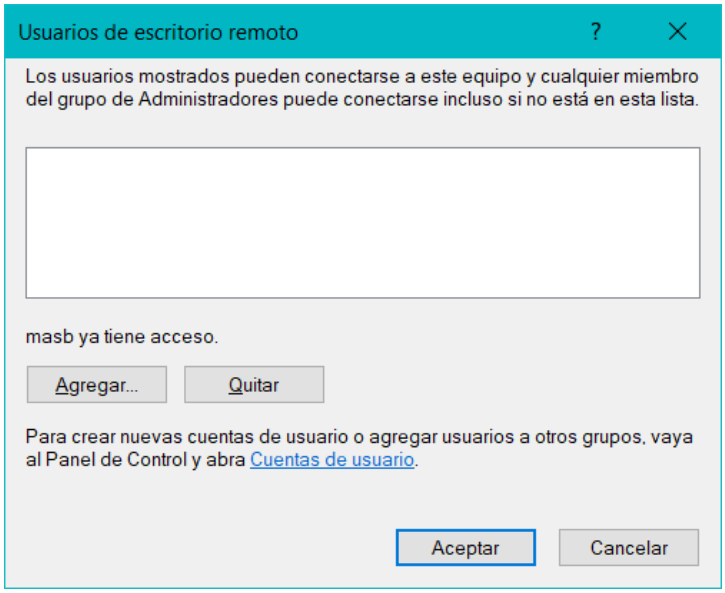


En la ventana Propiedades del sistema, se pulsará sobre la pestaña Acceso remoto.

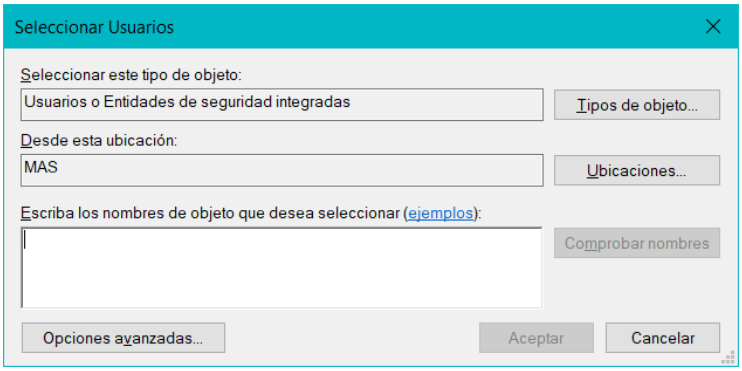


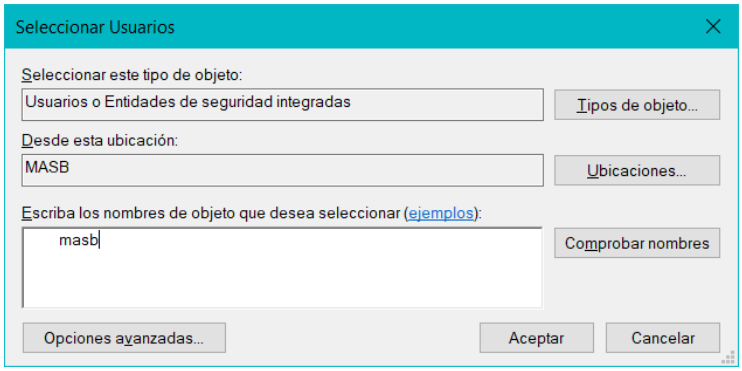
Una vez dentro de la pestaña Acceso remoto, en el apartado inferior Escritorio remoto, se marcará la opción Permitir las conexiones remotas a este equipo.

En el caso de querer permitir el acceso remoto a usuarios en concreto, en el apartado inferior Escritorio remoto, se pulsará el botón inferior Seleccionar usuarios.



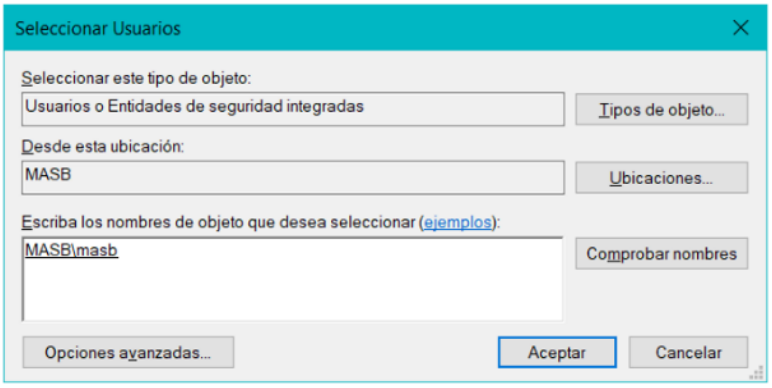
En esta nueva ventana que aparece, se pulsará sobre el botón Agregar…
Para este ejemplo, se utiliza el usuario masb, aunque el usuario masb ya tiene acceso.



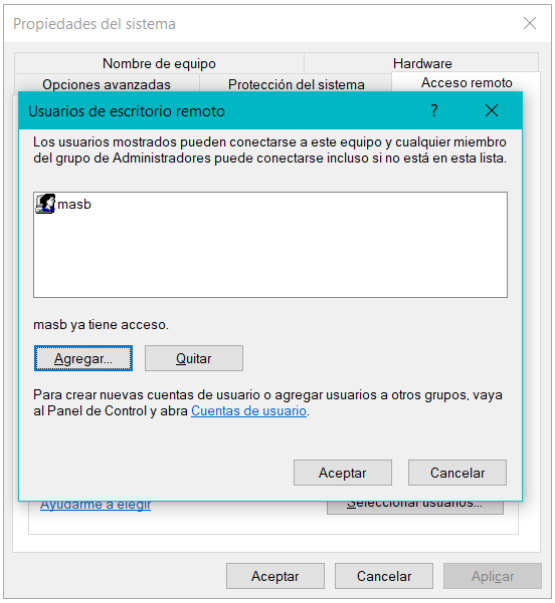


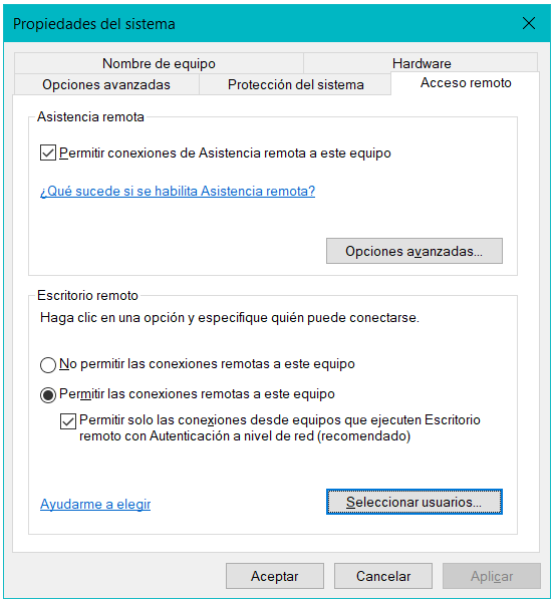
Al escribir un nombre de usuario valido, en el rectángulo inferior Escriba los nombres de objeto que desea seleccionar (ejemplos):.

En este ejemplo, el usuario es masb, (aunque como se ha podido apreciar, el usuario masb ya tiene acceso), al pulsar sobre el botón derecho Comprobar nombres.



Si el nombre es correcto, se valida como se puede observar en la ventana de la captura superior y se podrá pulsar en el botón Aceptar.





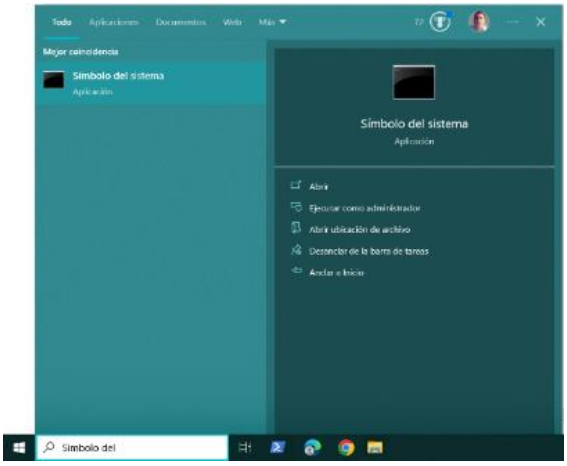
Tras la validación del usuario, se pulsará sobre el botón inferior Aceptar, captura de imagen superior izquierda.

Para finalizar, se pulsará sobre el botón Aceptar, captura de imagen superior derecha.

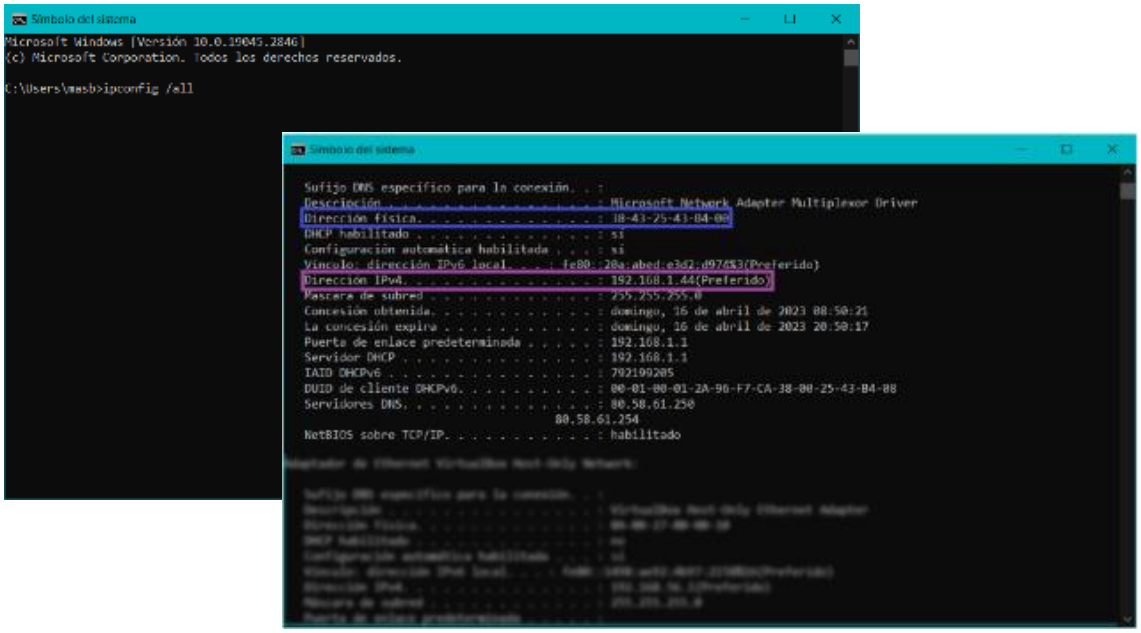
Averiguar dirección IP y dirección física MAC.

Para ciertas configuraciones que se utilizan en este proyecto, es necesario saber dónde y cómo poder adquirir los datos necesarios, como la dirección IP o la dirección física (MAC), de un adaptador de red.

S.O. Windows.



Este es uno de los métodos para poder tomar nota de los datos necesarios, como la dirección IP y la dirección física MAC del adaptador de red, en el S.O. Windows, dentro de la sesión de un usuario, habrá que acceder a un Símbolo del sistema (CMD).



Ya dentro del Símbolo del sistema, se ejecutará el comando. Ipconfig /all

De los resultados que se muestran, estos tienen que corresponder al adaptador de red que corresponda, se localizaran los datos Dirección física y Dirección IPv4, anotando los datos que aparecen a la derecha, en este caso, los datos a anotar son:
Dirección física 38-43-25-43-B4-00
Dirección IPv4 192.168.1.40(Preferido)

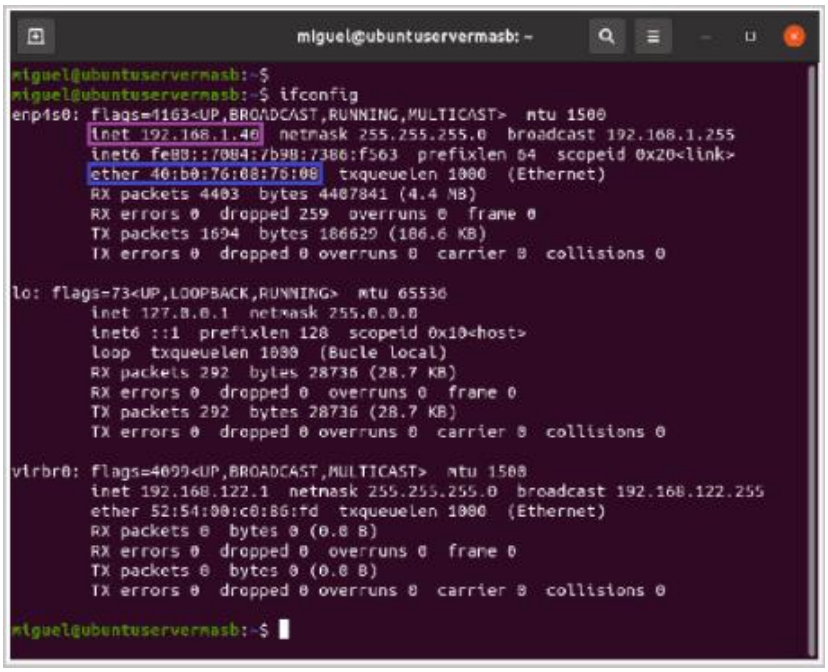
S.O. Linux.



Estas explicaciones que se indican aquí, puede que varíen dependiendo de la distribución de Linux que se utilice como también del escritorio que se ejecute.

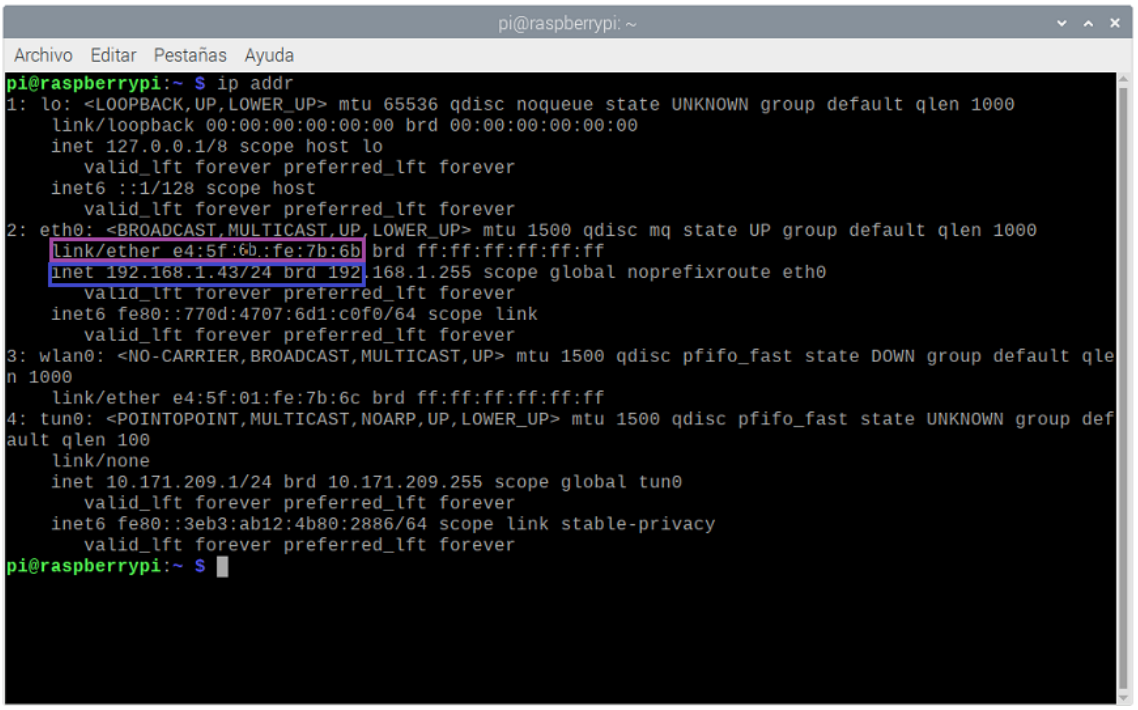
En un S.O. Linux como Ubuntu, en el menú de Aplicaciones \ Herramientas del sistema, se pulsará con el botón izquierdo del ratón sobre la aplicación Terminal.

Dentro del terminal, se escribirá el comando. ifconfig



Pudiendo anotar los datos que se indican en la captura de la imagen superior.

Dirección IP, Inet 192.168.1.40
Dirección física, ether 40:b0:76:08:76:08



Otro método en Linux, es acceder a un terminal, donde se podrá obtener los datos necesarios con el comando.

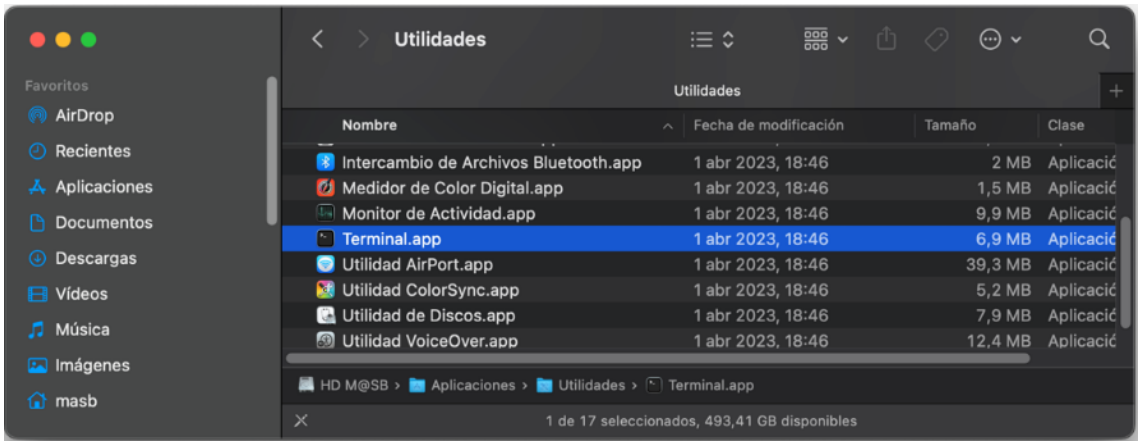
ip addr
ip addr show

Pudiendo anotar los datos que se indican en la captura de la imagen superior.

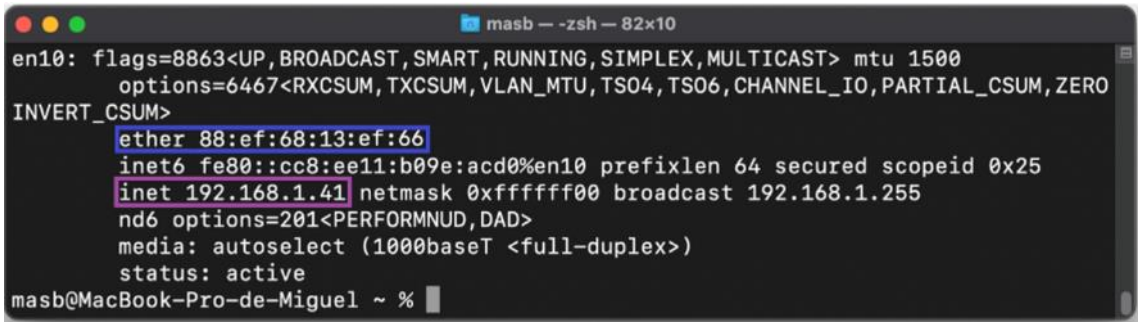
Dirección IP, Inet 192.168.1.43
Dirección física, link/ether e4:5f:6b:fe:7b:6b

S.O. Apple macOS.

Por último, en macOS.



Para abrir el terminal, se podrá acceder a Aplicaciones \ Utilidades, donde se localizará la aplicación Terminal.app, haciendo doble clic sobre ella con el botón izquierdo del ratón.



Dentro del terminal, se ejecutará el comando.

Ifconfig

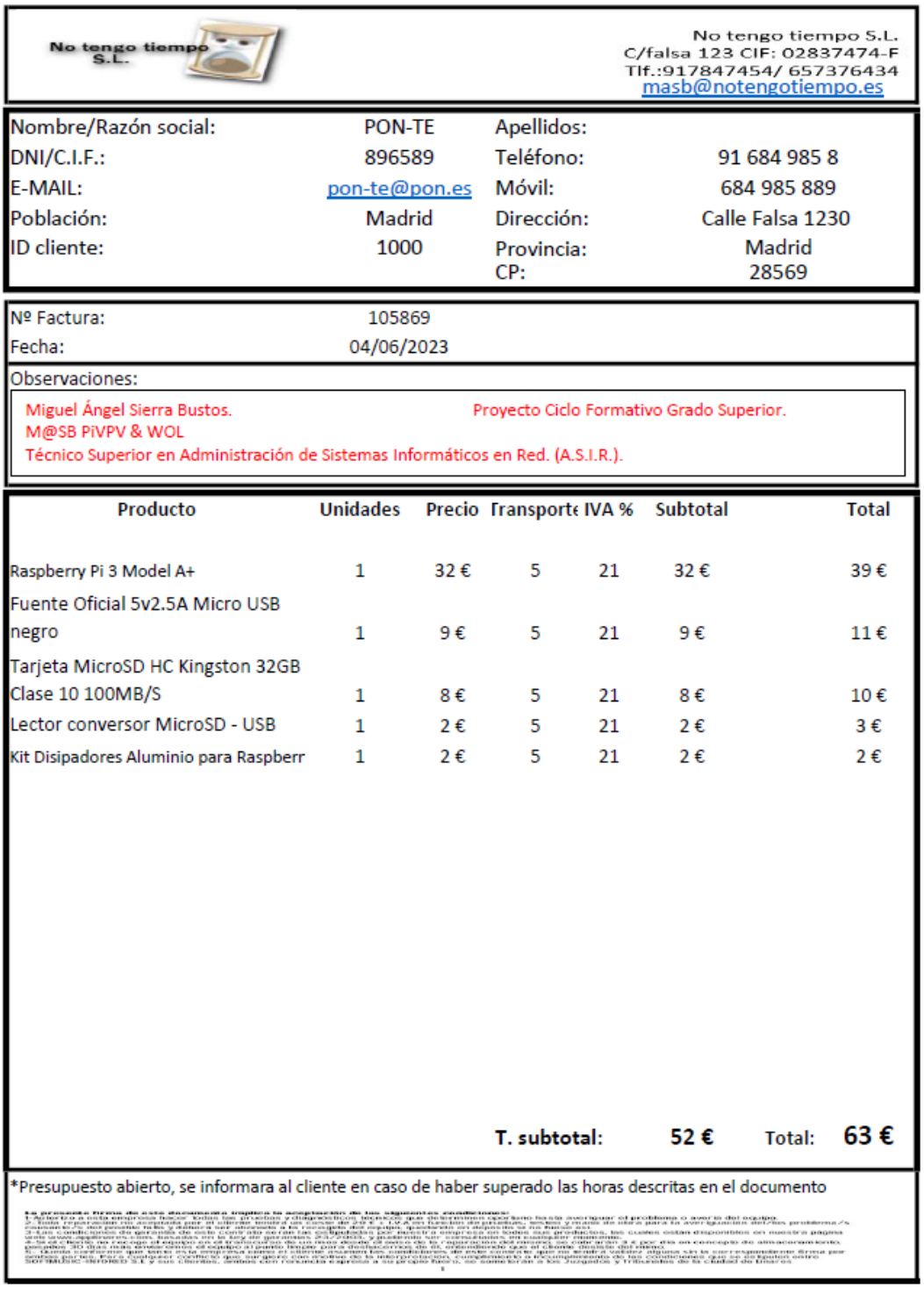
Los datos a anotar, son los que se muestran en la ventana de la captura superior, siendo estos.

Dirección IP, Inet 192.168.1.41
Dirección física, ether 88:ef:68:13:ef:66

Facturas de dispositivos.

Ejemplo de facturas para la compra del servidor, basado en una Raspberry Pi.

Para la realización de este ejemplo de facturas, se accede a la WEB, Raspberry Pi España, Distribuidor Autorizado, cuya URL es. https://www.raspipc.es/index.php



No tengo tiempo S.L.

No tengo tiempo S.L.
C/falsa 123 CIF: 02837474-F
Tlf.:917847454/ 657376434
masb@notengotiempo.es

Nombre/Razón social:	PON-TE	Apellidos:	
DNI/C.I.F.:	896589	Teléfono:	91 684 985 8
E-MAIL:	pon-te@pon.es	Móvil:	684 985 889
Población:	Madrid	Dirección:	Calle Falsa 1230
ID cliente:	1000	Provincia:	Madrid
		CP:	28569

Nº Factura:	105869
Fecha:	04/06/2023

Observaciones:

Miguel Ángel Sierra Bustos. Proyecto Ciclo Formativo Grado Superior.
M@SB PiVPV & WOL
Técnico Superior en Administración de Sistemas Informáticos en Red. (A.S.I.R.).

Producto	Unidades	Precio	Transporte	IVA %	Subtotal	Total
Raspberry Pi 3 Model A+	1	32 €	5	21	32 €	39 €
Fuente Oficial 5v2.5A Micro USB negro	1	9 €	5	21	9 €	11 €
Tarjeta MicroSD HC Kingston 32GB Clase 10 100MB/S	1	8 €	5	21	8 €	10 €
Lector conversor MicroSD - USB	1	2 €	5	21	2 €	3 €
Kit Disipadores Aluminio para Raspberr	1	2 €	5	21	2 €	2 €

T. subtotal: **52 €** Total: **63 €**

*Presupuesto abierto, se informara al cliente en caso de haber superado las horas descritas en el documento



No tengo tiempo S.L.
C/falsa 123 CIF: 02837474-F
Tlf.:917847454/ 657376434
masb@notengotiempo.es

Nombre/Razón social:	PON-TE	Apellidos:	
DNI/C.I.F.:	896589	Teléfono:	91 684 985 8
E-MAIL:	pon-te@pon.es	Móvil:	684 985 889
Población:	Madrid	Dirección:	Calle Falsa 1230
ID cliente:	1000	Provincia:	Madrid
		CP:	28569

Nº Factura:	105868
Fecha:	04/06/2023

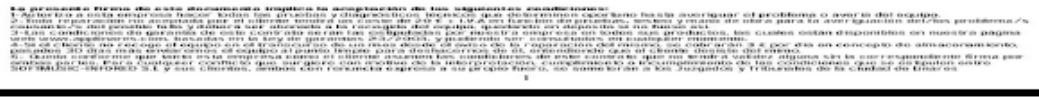
Observaciones:

Miguel Ángel Sierra Bustos. Proyecto Ciclo Formativo Grado Superior.
M@SB PiVPV & WOL
Técnico Superior en Administración de Sistemas Informáticos en Red. (A.S.I.R.).

Producto	Unidades	Precio	Transporte	IVA %	Subtotal	Total
Raspberry Pi 3 Model A+	1	32 €	5	21	32 €	39 €
Fuente Oficial 5v2.5A Micro USB negro	1	9 €	5	21	9 €	11 €
Tarjeta MicroSD HC Kingston 32GB Clase 10 100MB/S	1	8 €	5	21	8 €	10 €
Lector conversor MicroSD - USB	1	2 €	5	21	2 €	3 €
Kit Disipadores Aluminio para Raspberr	1	2 €	5	21	2 €	2 €
Caja Oficial Raspberry Pi 3 A+	1	4 €	5	21	4 €	4 €
Cable HDMI v1.4 M-M 1m	1	4 €	5	21	4 €	4 €

T. subtotal: **60 €** Total: **71 €**

*Presupuesto abierto, se informara al cliente en caso de haber superado las horas descritas en el documento





No tengo tiempo S.L.
C/falsa 123 CIF: 02837474-F
Tlf.:917847454/ 657376434
masb@notengotiempo.es

Nombre/Razón social:	PON-TE	Apellidos:	
DNI/C.I.F.:	896589	Teléfono:	91 684 985 8
E-MAIL:	pon-te@pon.es	Móvil:	684 985 889
Población:	Madrid	Dirección:	Calle Falsa 1230
ID cliente:	1000	Provincia:	Madrid
		CP:	28569

Nº Factura:	105871
Fecha:	04/06/2023

Observaciones:

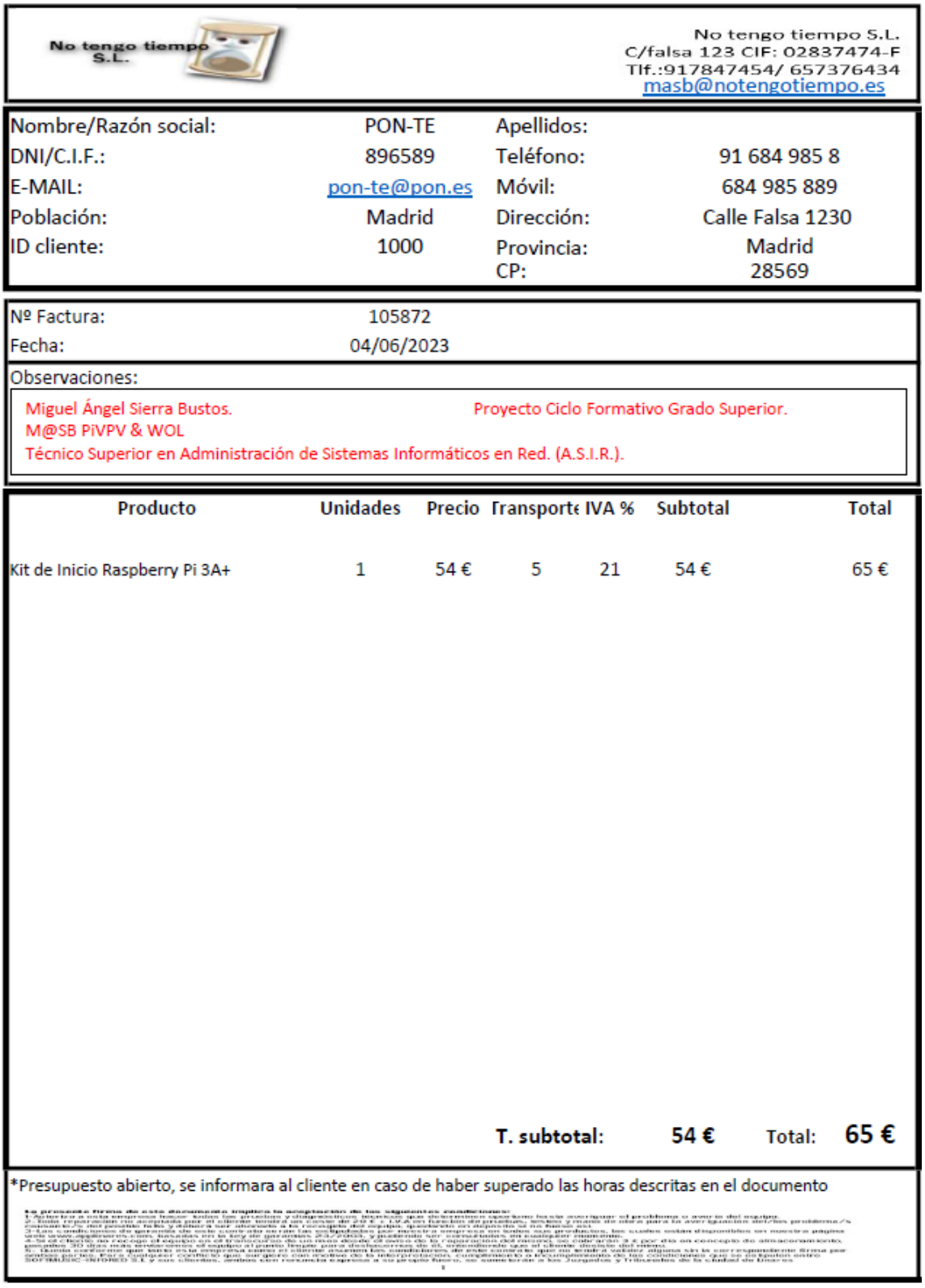
Miguel Ángel Sierra Bustos. Proyecto Ciclo Formativo Grado Superior.
M@SB PiVPV & WOL
Técnico Superior en Administración de Sistemas Informáticos en Red. (A.S.I.R.).

Producto	Unidades	Precio	Transporte	IVA %	Subtotal	Total
Raspberry Pi 3 Model B+	1	43 €	5	21	43 €	53 €
Fuente Oficial 5v2.5A Micro USB negro	1	9 €	5	21	9 €	11 €
Tarjeta MicroSD HC Kingston 32GB Clase 10 100MB/S	1	8 €	5	21	8 €	10 €
Lector conversor MicroSD - USB	1	2 €	5	21	2 €	3 €
Kit Disipadores Aluminio para Raspberr	1	2 €	5	21	2 €	2 €

T. subtotal: **64 €** Total: **77 €**

*Presupuesto abierto, se informara al cliente en caso de haber superado las horas descritas en el documento

Kit 1



No tengo tiempo S.L.

No tengo tiempo S.L.
C/falsa 123 CIF: 02837474-F
Tlf.:917847454/ 657376434
masb@notengotiempo.es

Nombre/Razón social:	PON-TE	Apellidos:	
DNI/C.I.F.:	896589	Teléfono:	91 684 985 8
E-MAIL:	pon-te@pon.es	Móvil:	684 985 889
Población:	Madrid	Dirección:	Calle Falsa 1230
ID cliente:	1000	Provincia:	Madrid
		CP:	28569

Nº Factura:	105872
Fecha:	04/06/2023

Observaciones:

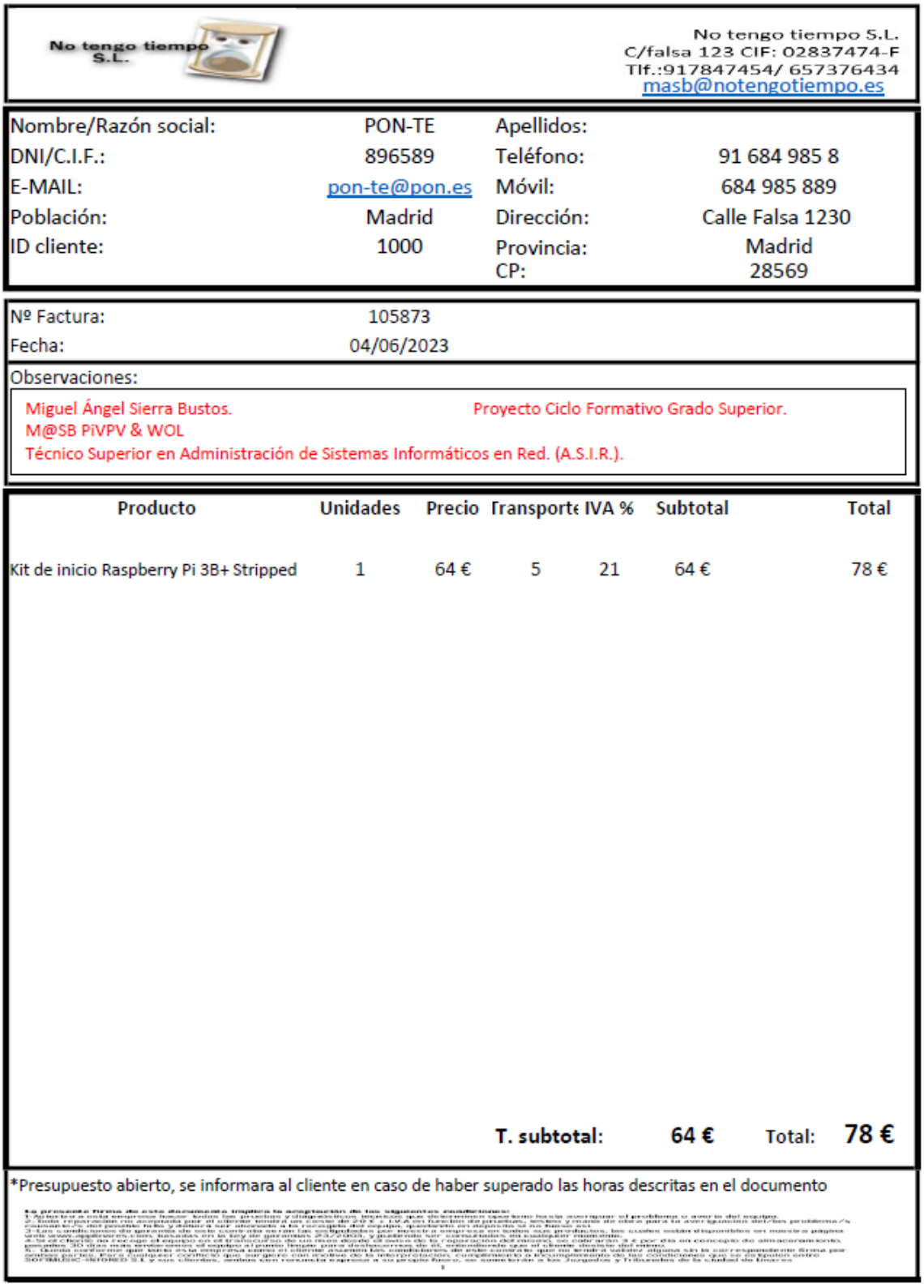
Miguel Ángel Sierra Bustos. Proyecto Ciclo Formativo Grado Superior.
M@SB PiVPV & WOL
Técnico Superior en Administración de Sistemas Informáticos en Red. (A.S.I.R.).

Producto	Unidades	Precio	Transporte	IVA %	Subtotal	Total
Kit de Inicio Raspberry Pi 3A+	1	54 €	5	21	54 €	65 €

T. subtotal: **54 €** Total: **65 €**

*Presupuesto abierto, se informara al cliente en caso de haber superado las horas descritas en el documento

Kit 2



No tengo tiempo S.L.

No tengo tiempo S.L.
C/falsa 123 CIF: 02837474-F
Tlf.:917847454/ 657376434
masb@notengotiempo.es

Nombre/Razón social:	PON-TE	Apellidos:	
DNI/C.I.F.:	896589	Teléfono:	91 684 985 8
E-MAIL:	pon-te@pon.es	Móvil:	684 985 889
Población:	Madrid	Dirección:	Calle Falsa 1230
ID cliente:	1000	Provincia:	Madrid
		CP:	28569

Nº Factura:	105873
Fecha:	04/06/2023

Observaciones:

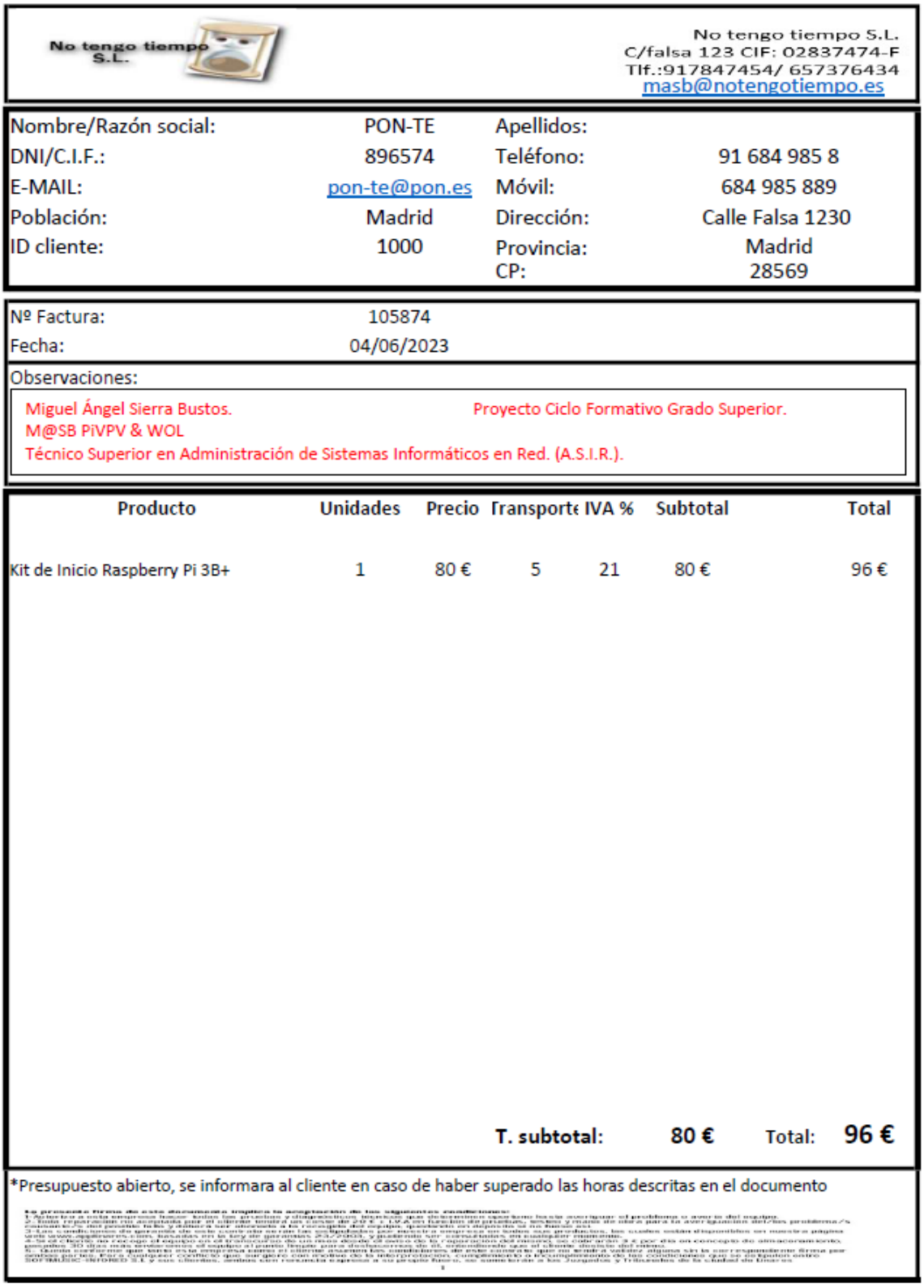
Miguel Ángel Sierra Bustos. Proyecto Ciclo Formativo Grado Superior.
M@SB PiVPV & WOL
Técnico Superior en Administración de Sistemas Informáticos en Red. (A.S.I.R.).

Producto	Unidades	Precio	Transporte	IVA %	Subtotal	Total
Kit de inicio Raspberry Pi 3B+ Stripped	1	64 €	5	21	64 €	78 €

T. subtotal: **64 €** Total: **78 €**

*Presupuesto abierto, se informara al cliente en caso de haber superado las horas descritas en el documento

Kit 3



No tengo tiempo S.L.

No tengo tiempo S.L.
C/falsa 123 CIF: 02837474-F
Tlf.:917847454/ 657376434
masb@notengotiempo.es

Nombre/Razón social:	PON-TE	Apellidos:	
DNI/C.I.F.:	896574	Teléfono:	91 684 985 8
E-MAIL:	pon-te@pon.es	Móvil:	684 985 889
Población:	Madrid	Dirección:	Calle Falsa 1230
ID cliente:	1000	Provincia:	Madrid
		CP:	28569

Nº Factura:	105874
Fecha:	04/06/2023

Observaciones:

Miguel Ángel Sierra Bustos. Proyecto Ciclo Formativo Grado Superior.
M@SB PiVPV & WOL
Técnico Superior en Administración de Sistemas Informáticos en Red. (A.S.I.R.).

Producto	Unidades	Precio	Transporte	IVA %	Subtotal	Total
Kit de Inicio Raspberry Pi 3B+	1	80 €	5	21	80 €	96 €

T. subtotal: **80 €** Total: **96 €**

*Presupuesto abierto, se informara al cliente en caso de haber superado las horas descritas en el documento

Fichero noip.sh

Ejemplo contenido fichero: /etc/init.d/noip.sh

```
#! /bin/bash
#
#
sudo /usr/local/bin/noip2
```

Fichero script instalación pivpn.

Dado la cantidad de información que contiene el script, no se anexa el contenido del fichero, en su defecto, se añade la URL donde se puede consultar el contenido íntegro del fichero install.sh

WEB oficial PiVPN.

https://www.pivpn.io/

Contenido del fichero install.sh

https://raw.githubusercontent.com/pivpn/pivpn/master/auto_install/install.sh

Fichero sshd_config en /etc/ssh.

Fichero sshd_config en /etc/ssh

/etc/ssh/sshd_config

```
#	$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile	.ssh/authorized_keys .ssh/authorized_keys2
```

```
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
```

```
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem	sftp	/usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#	X11Forwarding no
#	AllowTcpForwarding no
#	PermitTTY no
#	ForceCommand cvs server
```

Ficheros configuración servidor OpenVPN.

Puede ser necesario modificar la configuración del servidor PiVPN instalado en la Raspberry pi, para ello, con un usuario administrador se podrá modificar los ficheros de configuración del servidor que se indican a continuación.

Archivo.	Descripción.	Ubicación.
server.conf	Contiene parámetros de configuración del servidor.	/etc/openvpn
Default.txt	Se toma como referencia para generar el fichero de configuración de los clientes.	/etc/openvpn/easy-rsa/pki
xxxxx.ovpn	Archivo o archivos de configuración, creados en el servidor OpenVPN para cada cliente, cada fichero, corresponde a un usuario, es absolutamente necesario para establecer la conexión de los clientes al servidor OpenVPN.	~/ovpns y /etc/openvpn/easy-rsa/pki

Archivo.	Descripción.	Ubicación.
ca.key *raspberrypi_….key* *xxxxx1.key* *xxxxx2.key* . .	Ficheros en los cuales se almacena las claves privadas del servidor, la entidad certificadora y la de los clientes.	/etc/openvpn/easy-rsa/pki/private
server.crt *xxxxx1.crt* *xxxxx2.crt* . .	Certificados del servidor y de cada clientes.	/etc/openvpn/easy-rsa/pki/issued
xxx.pem *ta.key*	Donde se encuentran el certificado raíz de la entidad certificados. Archivos que contienen parámetros de Diffie Hellman y La clave para la autenticación TLS.	/etc/openvpn/easy-rsa/pki

El nombre de estos ficheros puede variar.

Desinstalación PiVPV.

URL. https://docs.pivpn.io/install/

Para realizar la desinstalación de PiVPN, se ejecutará el comando.

pivpn uninstall

Desinstalación No-IP, noip-duc.

Se describe a continuación el proceso de desinstalación de No-IP, aunque en la realización de este proyecto, no se ha realizado la desinstalación para su comprobación, se indica según la WEB.

URL. https://forums.raspberrypi.com/viewtopic.php?t=160038

Ejecución de los comandos

```
cd no-ip-2.1.9
make uninstall
make remove

rm /usr/local/bin/noip2
rm /usr/local/etc/no-ip2.conf

rm -rf noip-2.1.9-1


“”
sudo make uninstall
gcc -Wall -g -Dlinux -DPREFIX=\"/usr/local\" noip2.c -o noip2
noip2.c: In function ‘dynamic_update’:
noip2.c:1595:6: warning: variable ‘i’ set but not used [-Wunused-but-set-variable]
  int i, x, is_group, retval, response;
      ^
noip2.c: In function ‘domains’:
noip2.c:1826:13: warning: variable ‘x’ set but not used [-Wunused-but-set-variable]
        int x;
            ^
noip2.c: In function ‘hosts’:
noip2.c:1838:20: warning: variable ‘y’ set but not used [-Wunused-but-set-variable]
        int     x, y, z;
                    ^
rm /usr/local/bin/noip2
rm /usr/local/etc/no-ip2.conf


sudo make remove
make: *** No rule to make target 'remove'.  Schluss
”””
```

Desinstalación aplicaciones en servidor Raspberry Pi.

Para realizar la desinstalación de alguna aplicación en el servidor, se podrá utilizar el comando sudo apt-get purge (la opción purge, desinstalara la aplicación y se eliminaran los ficheros de configuración de la aplicación).

Como ejemplo se indica el comando para desinstalar la aplicación wireshark.

sudo apt-get purge wireshark

Wake On LAN en equipos con S.O. Linux.

Por la falta de tiempo y la envergadura ya de esta documentación, no se incluye información referente a cómo realizar este proceso, se facilita URL´s donde se indican los pasos a seguir para disponer de Wake On LAN por lo menos en Ubuntu.

Universidad de Valencia.

Wake On LAN.

https://www.uv.es/uvweb/servicio-informatica/es/red-comunicaciones/infraestructura-recursos/wake-on-lan-1285904035551.html

linuxadictos.com

Cómo activa Wake On LAN en Gnu/Linux

https://www.linuxadictos.com/como-activa-wake-on-lan-en-gnu-linux.html

En este punto, como puede comprobar, se termina toda la explicación de cómo llevar a cabo este proyecto, en el S.O. Linux para el uso de PiVPN en una Raspberry Pi, pudiendo utilizar como equipos clientes, equipos con S.O. Linux, Windows y Apple con S.O. macOS.

Sin más que añadir, se finalizan todas las explicaciones.

Bibliografía.

Raspberry Pi.

https://www.raspberrypi.com/
https://www.raspberrypi.org/help/
https://www.raspberrypi.com/software/

VPN.
Virtual Private Network, Red Privada Virtual.

https://es.wikipedia.org/wiki/OpenVPN
https://es.wikipedia.org/wiki/Red_privada_virtual

OpenVPN.

https://openvpn.net/
https://openvpn.net/faq/what-is-openvpn/
https://es.wikipedia.org/wiki/OpenVPN

PiVPN.

https://www.pivpn.io/
https://docs.pivpn.io/

DDNS.
Sistema Dinámico de Nombres de Dominio o DNS dinámico.

https://es.wikipedia.org/wiki/DNS_din%C3%A1mico
https://en.wikipedia.org/wiki/Dynamic_DNS

Wake On LAN.

https://es.wikipedia.org/wiki/Wake_on_LAN
https://www.uv.es/uvweb/servicio-informatica/es/red-comunicaciones/infraestructura-recursos/wake-on-lan-1285904035551.html
https://www.linuxadictos.com/como-activa-wake-on-lan-en-gnu-linux.html

WEBMIN.

https://webmin.com/
https://es.wikipedia.org/wiki/Webmin

RDP.
(Remote Desktop Protocol), Protocolo de Escritorio Remoto.

https://apps.microsoft.com/store/detail/escritorio-remoto-de-microsoft/9WZDNCRFJ3PS?hl=es-es&gl=es
https://es.wikipedia.org/wiki/Remote_Desktop_Protocol

SSH.
Secure Shell.

https://en.wikipedia.org/wiki/Secure_Shell

UFW.
Uncomplicated Firewall.

https://launchpad.net/ufw
https://es.wikipedia.org/wiki/Uncomplicated_Firewall
https://help.ubuntu.com/community/UFW

Xming.

http://www.straightrunning.com/XmingNotes/
https://es.wikipedia.org/wiki/Xming

Xquartz.

https://www.xquartz.org/
https://support.apple.com/es-es/HT201341
https://es.wikipedia.org/wiki/XQuartz