

CURSO ONLINE DE CIBERSEGURIDAD

Especialidad Introducción a la
Ciberseguridad Industrial

Taller 1

Unidad 4. Sistemas de control y
automatización industrial,
protocolos más utilizados y sus
vulnerabilidades



GOBIERNO
DE ESPAÑA
VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Contenidos

- | | | |
|---|--|----|
| 1 | CONSTRUCCIÓN DE UN ENTORNO
DE SIMULACIÓN DE DISPOSITIVOS OT | 4 |
| 2 | INSTALACIÓN Y CONFIGURACIÓN
DE UBUNTU | 6 |
| 3 | INSTALACIÓN Y CONFIGURACIÓN DE
MV UBUNTU DESKTOP | 29 |
| 4 | AJUSTES DE CONFIGURACIÓN | 55 |
| 5 | INSTALACIÓN DE HERRAMIENTAS DE
SIMULACIÓN DEL PROTOCOLO DE
COMUNICACIÓN MODBUS | 60 |

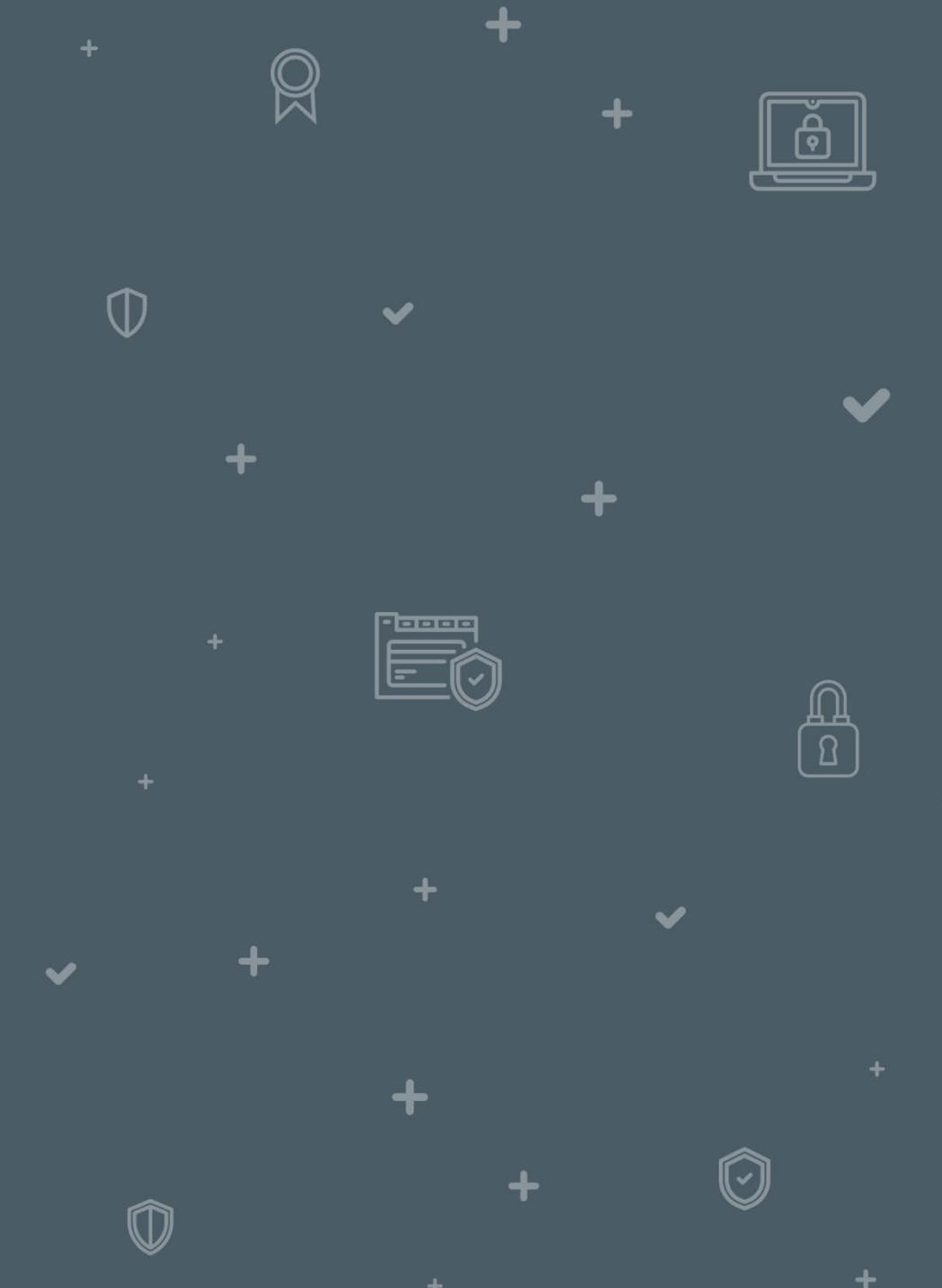
Contenidos

- 6** INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEO DE ACTIVOS: 114
NMAP Y PLCCAN
- 7** CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS 121
- 8** CREACIÓN DEL ESCLAVO Nº2 MODBUS Y LECTURA DE HOLDING REGISTERS 147
- 9** HERRAMIENTA PLCSCAN 162
- 10** AGRUPACIÓN DE MÁQUINAS 181

Duración total del taller: 2 horas

CONSTRUCCIÓN DE UN ENTORNO DE SIMULACIÓN DE DISPOSITIVOS OT

1



1 CONSTRUCCIÓN DE UN ENTORNO DE SIMULACIÓN DE DISPOSITIVOS OT

En este taller aprenderás a desplegar un entorno de simulación de dispositivos industriales OT, instalando simuladores del protocolo Modbus TCP y del protocolo s7comm que utilizan los dispositivos Siemens. Asimismo, también realizarás la instalación de herramientas de escaneo como Nmap y PLC Scan. Finalmente, configurarás esclavos de tipo Modbus TCP utilizando la aplicación ModbusPal y realizarás lecturas de estos esclavos desde la aplicación QModMaster.

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

2



2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

En este apartado realizarás la creación y configuración de la máquina virtual (a partir de ahora MV) Ubuntu 20.04 LTS en la que ejecutarás las diferentes prácticas de esta especialidad.



IMPORTANTE: Esta máquina virtual es la misma que la que utilizamos en la especialidad de «Administración de Sistemas de Ciberseguridad» en la unidad 5, por lo que si realizaste esta especialidad, puedes dirigirte directamente al apartado [«4. Ajustes de configuración»](#) para realizar los ajustes de configuración.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Lo primero que debes hacer es acceder a la página web de descargas de [Ubuntu](#).
- Haz clic en la entrada Ubuntu Desktop y descargamos la versión estable de Ubuntu (Desktop) que es la 20.04 LTS.
 - Ten en cuenta que, si has realizado la especialidad de Administración de Sistemas de Ciberseguridad, ya deberías tener instalada una máquina Ubuntu. Por ello, puedes saltar el proceso de instalación. No obstante, te recomendamos que revises la configuración para que sea la misma que en este taller.

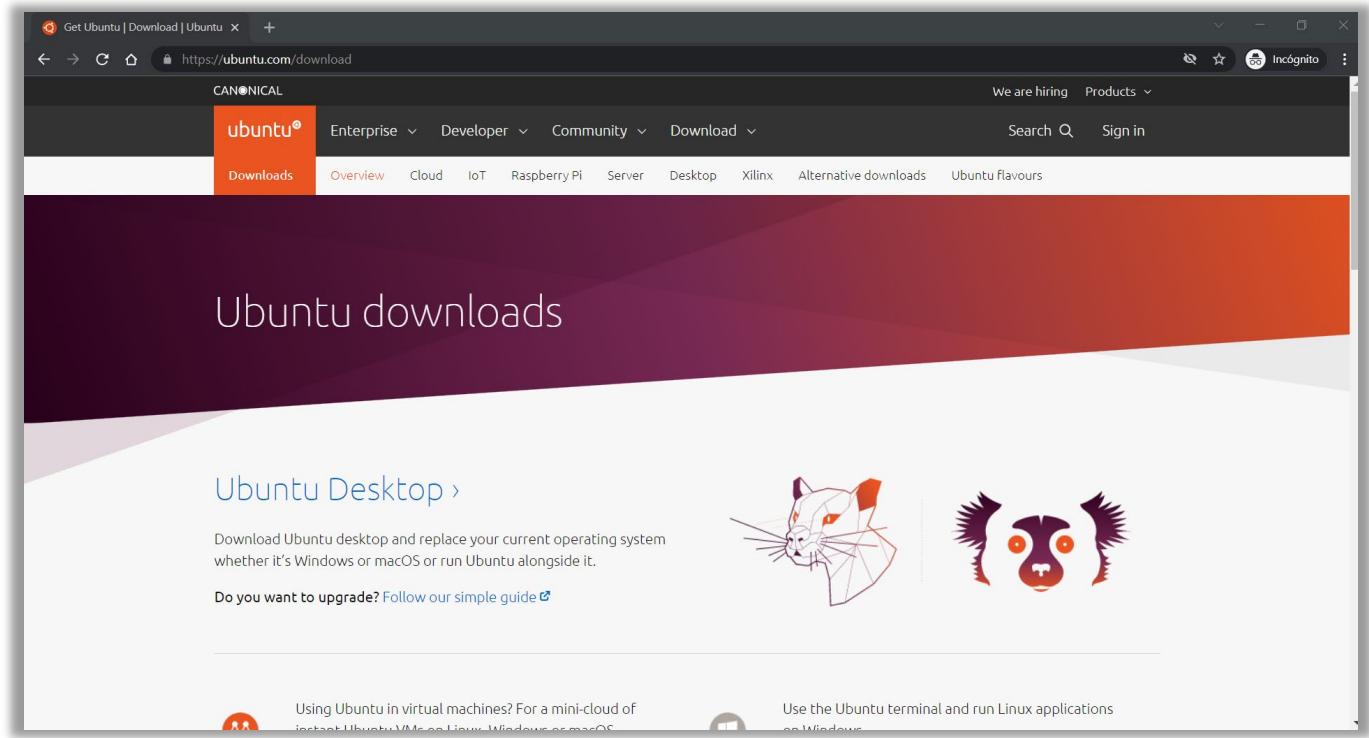


Ilustración 1: Acceso a la entrada Ubuntu Desktop.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

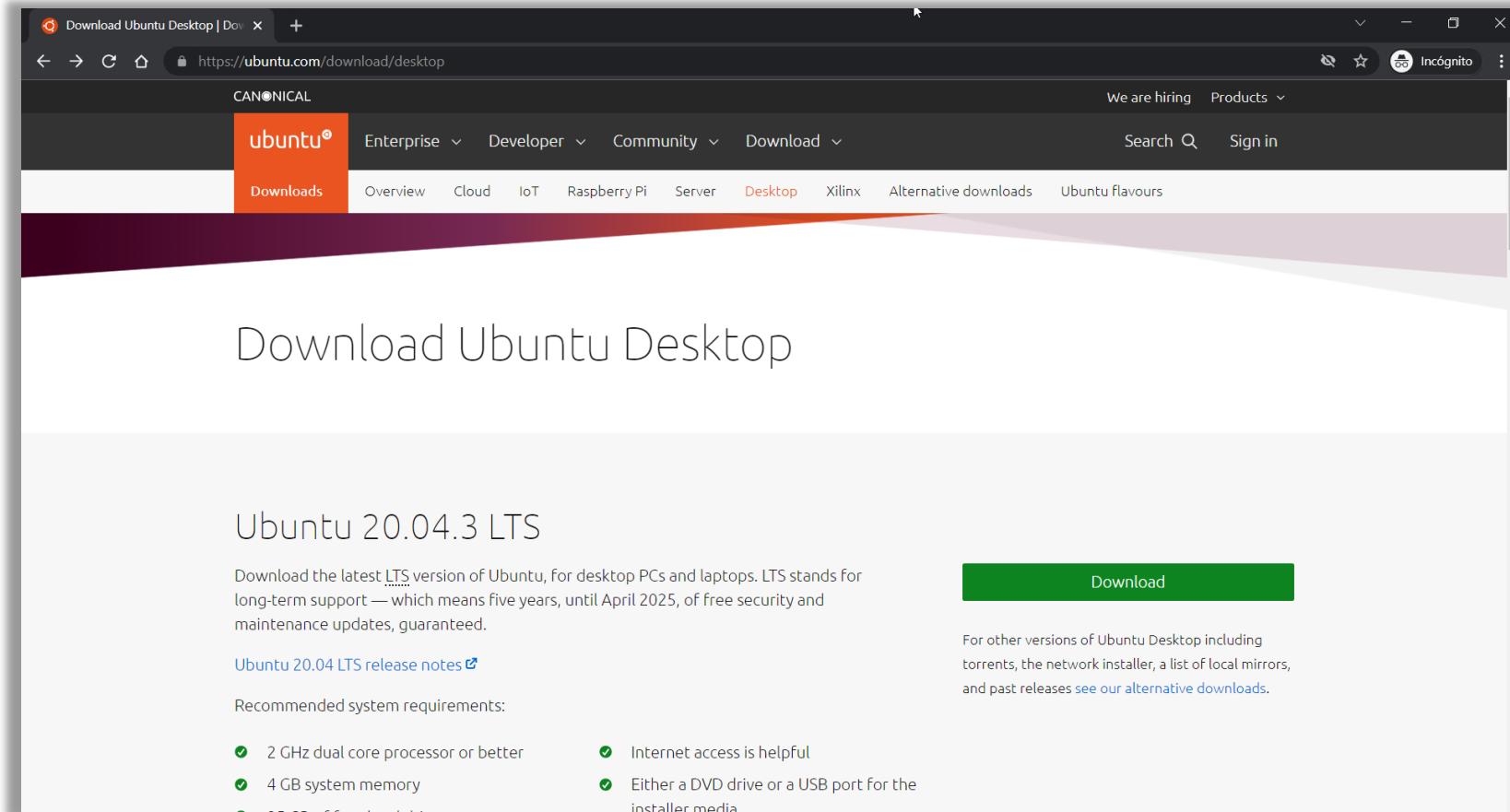


Ilustración 2: Página de descarga de la versión estable 20.04.3 LTS.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Después, en VirtualBox, que ya tendrás descargado, creas la MV (máquina virtual).

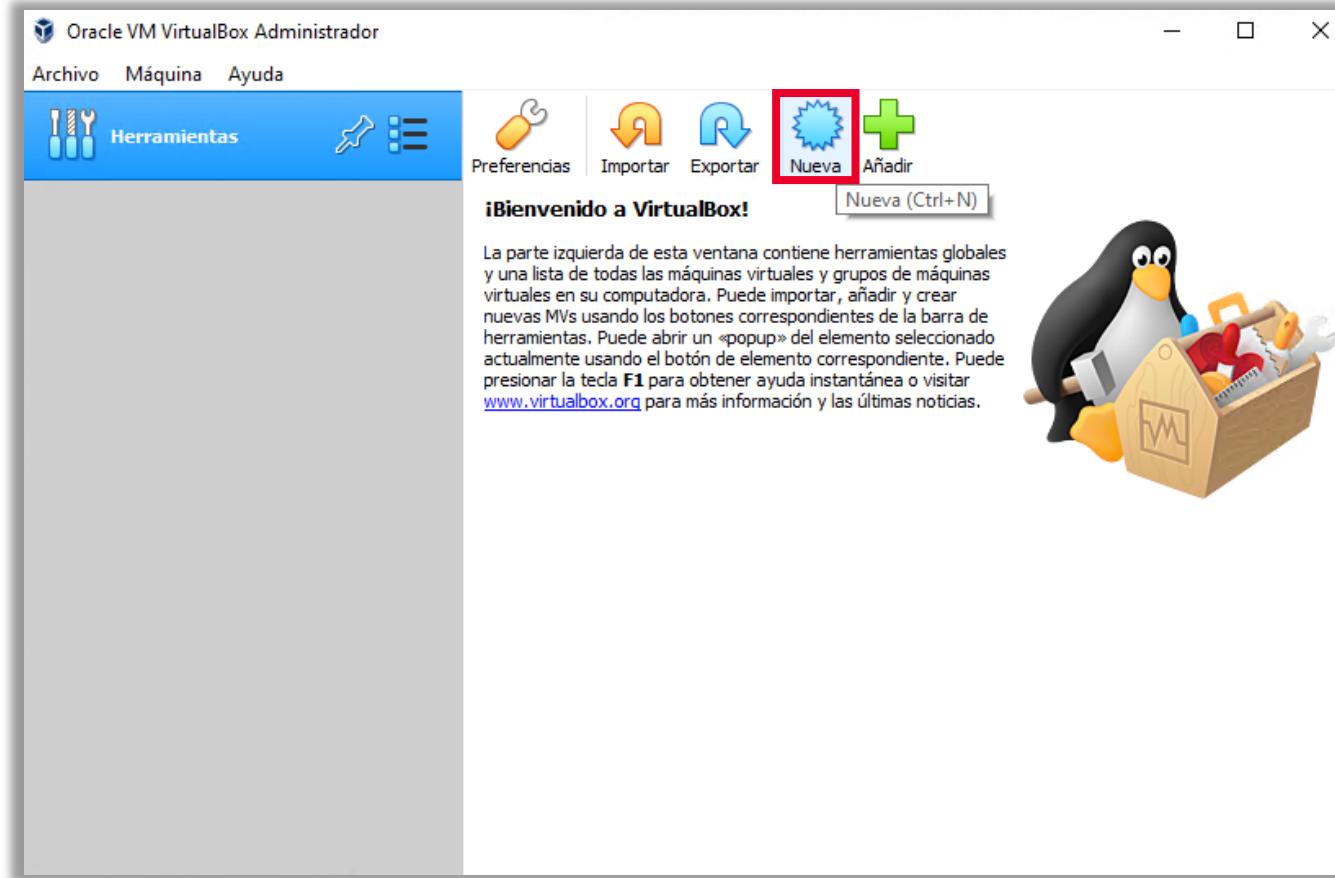


Ilustración 3: Creación de la máquina virtual en Virtual Box.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Pulsa en «nueva» y asignamos el nombre identificativo «Entorno Industrial_Ubuntu 20.04 LTS».

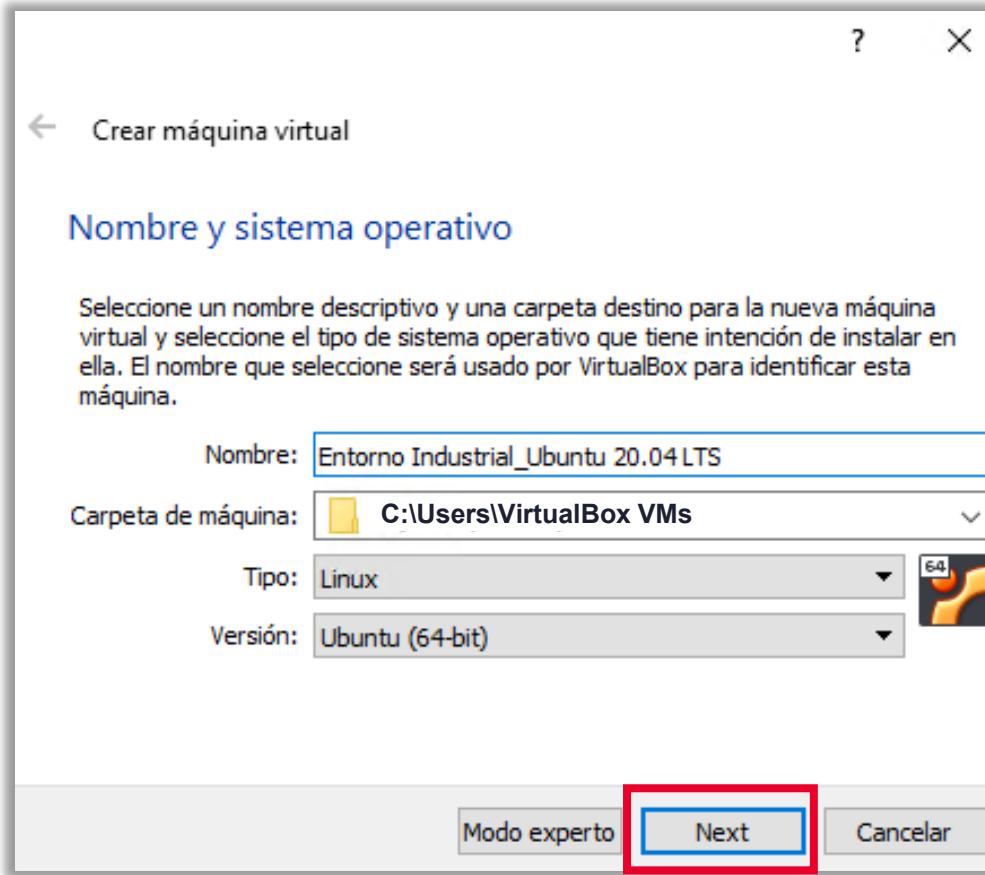


Ilustración 4: Asignación de nombre «Entorno Industrial_Ubuntu 20.04 LTS» en la nueva máquina virtual.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Selecciona el tipo de memoria a 4096 MB.

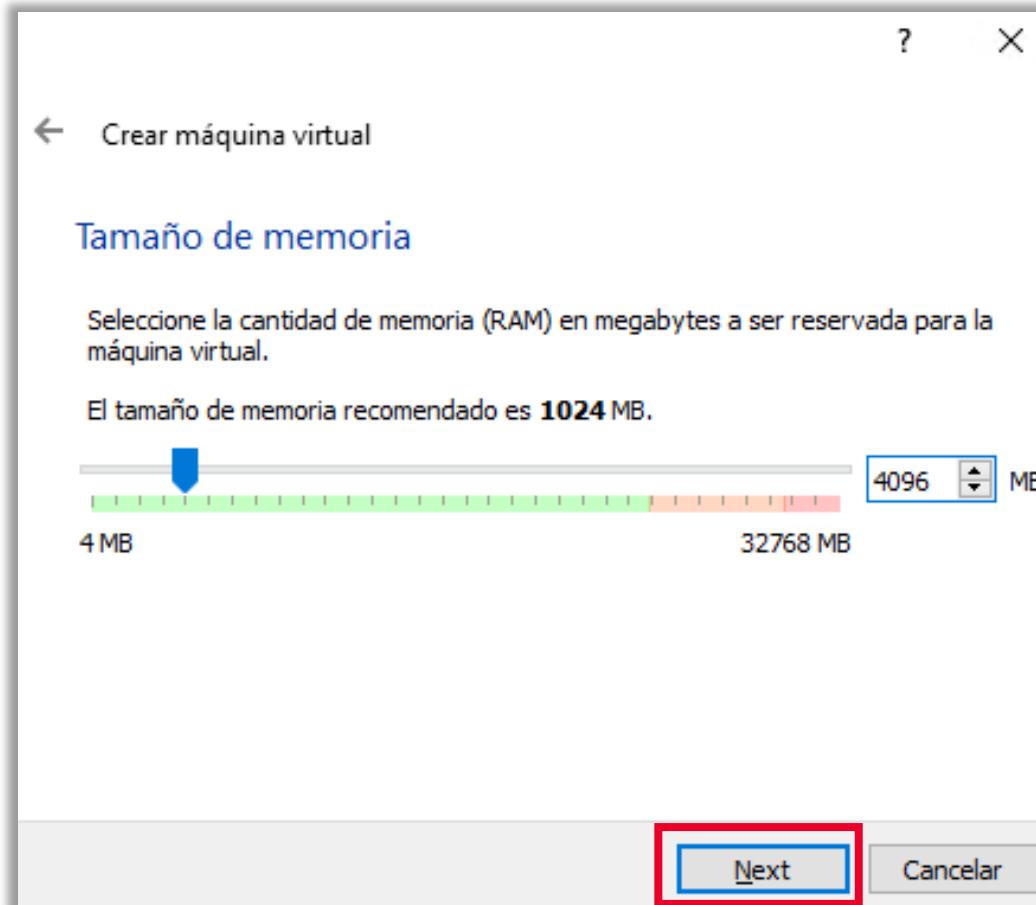


Ilustración 5: Aumento del tamaño de memoria a 4096MB.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Selecciona la opción de «Crear un disco virtual ahora».

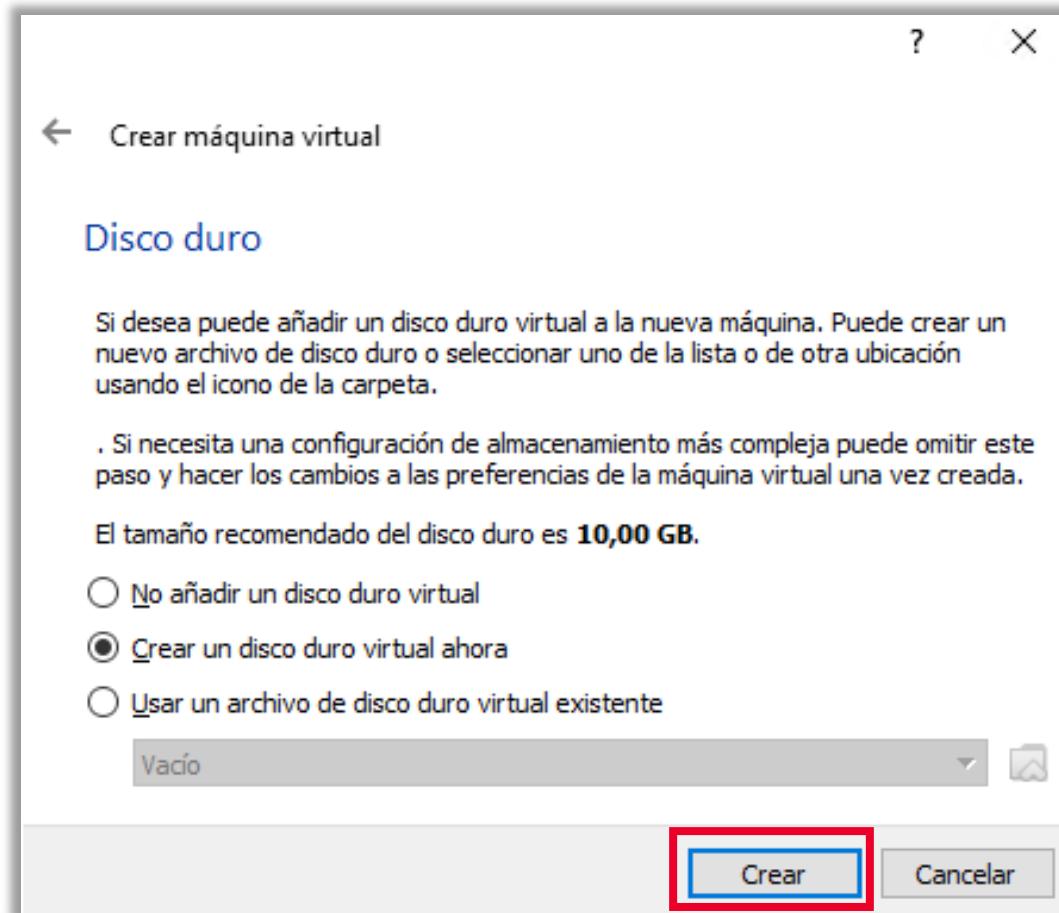


Ilustración 6: Creación del disco duro virtual.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Deja seleccionada la opción «VDI (Virtual Disk Image)».

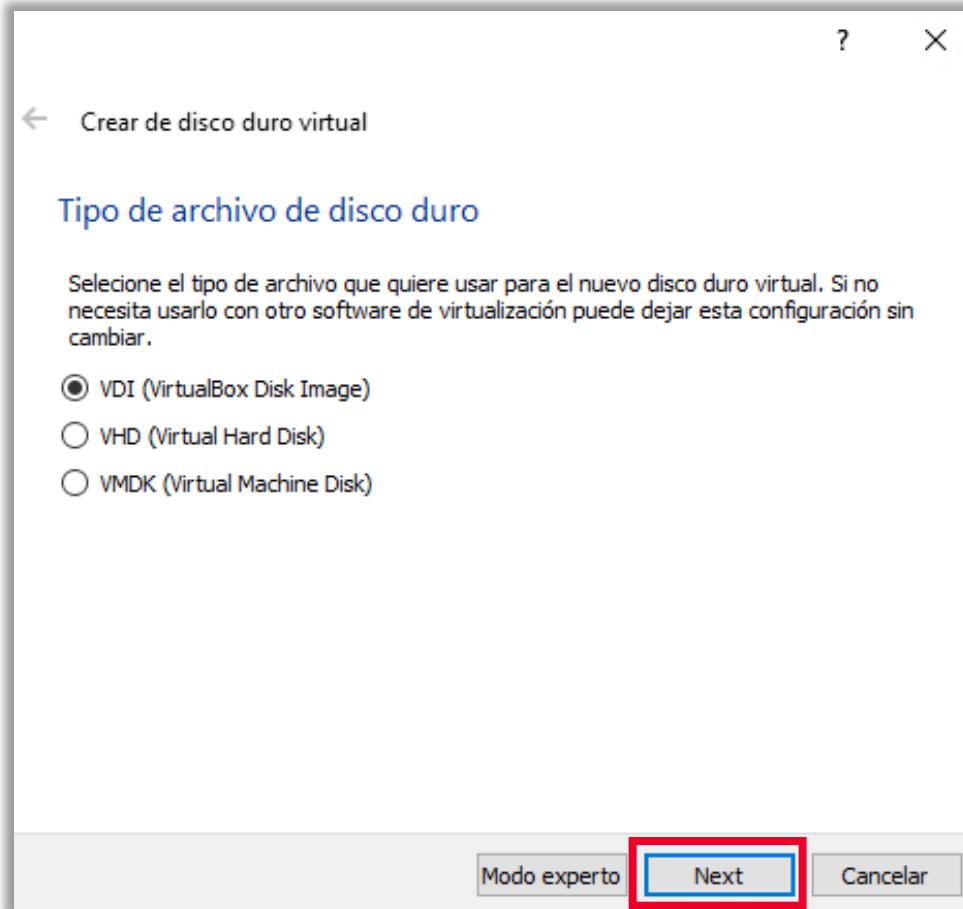


Ilustración 7: Selección del tipo de archivo de disco duro «VDI (Virtual Disk Image)».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Selecciona «Almacenamiento reservado dinámicamente».

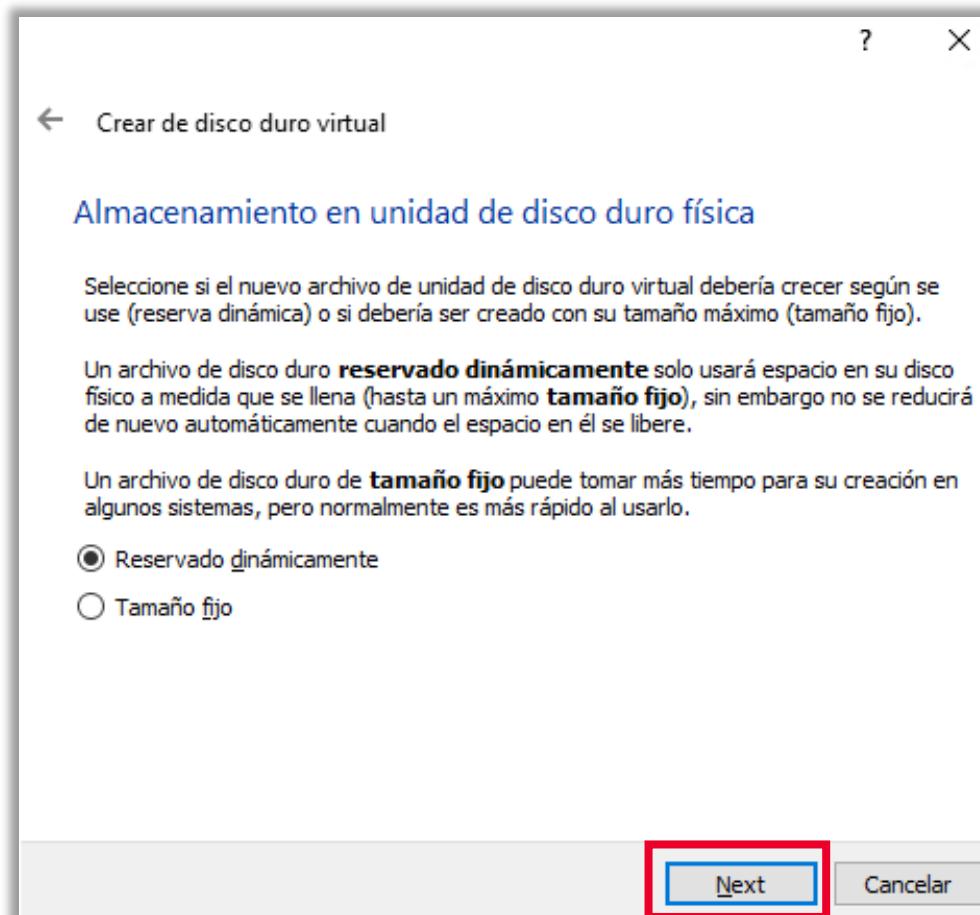


Ilustración 8: Selección del tipo de almacenamiento «Reservado dinámicamente».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Indica, como mínimo, 30,00 GB de tamaño.

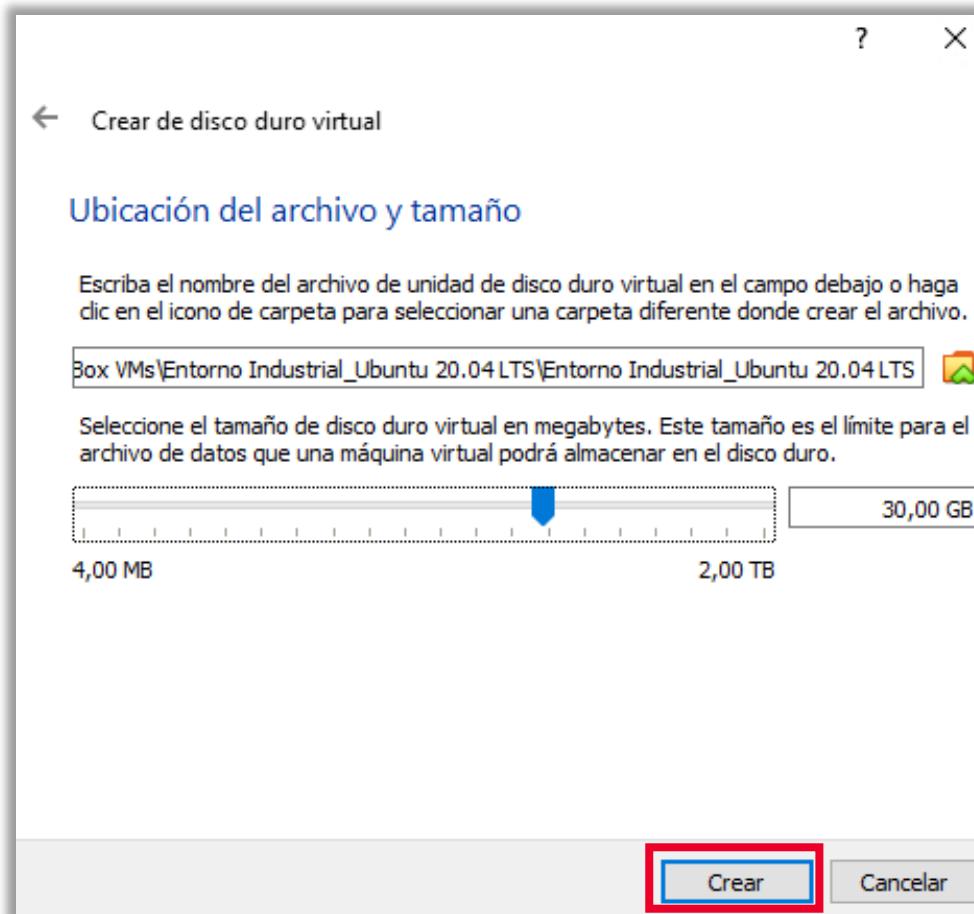


Ilustración 9: selección del tamaño
del disco duro virtual a 30 GB.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Pulsa en el botón «Crear» y ya tendrías lista tu máquina virtual.

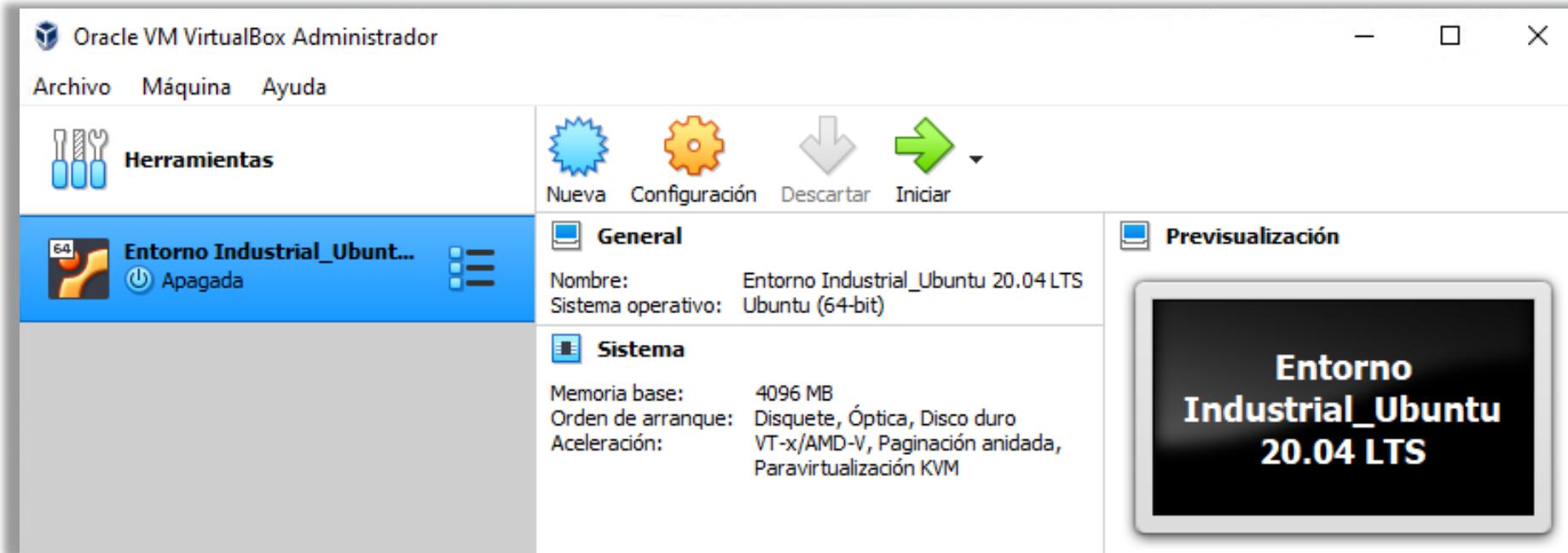


Ilustración 10: Confirmación de la creación de la máquina virtual al pulsar el botón «crear».

2 INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Manteniendo la máquina virtual seleccionada, pulsa en «Archivo → Preferencias», para configurar el tipo de red que vas a utilizar.

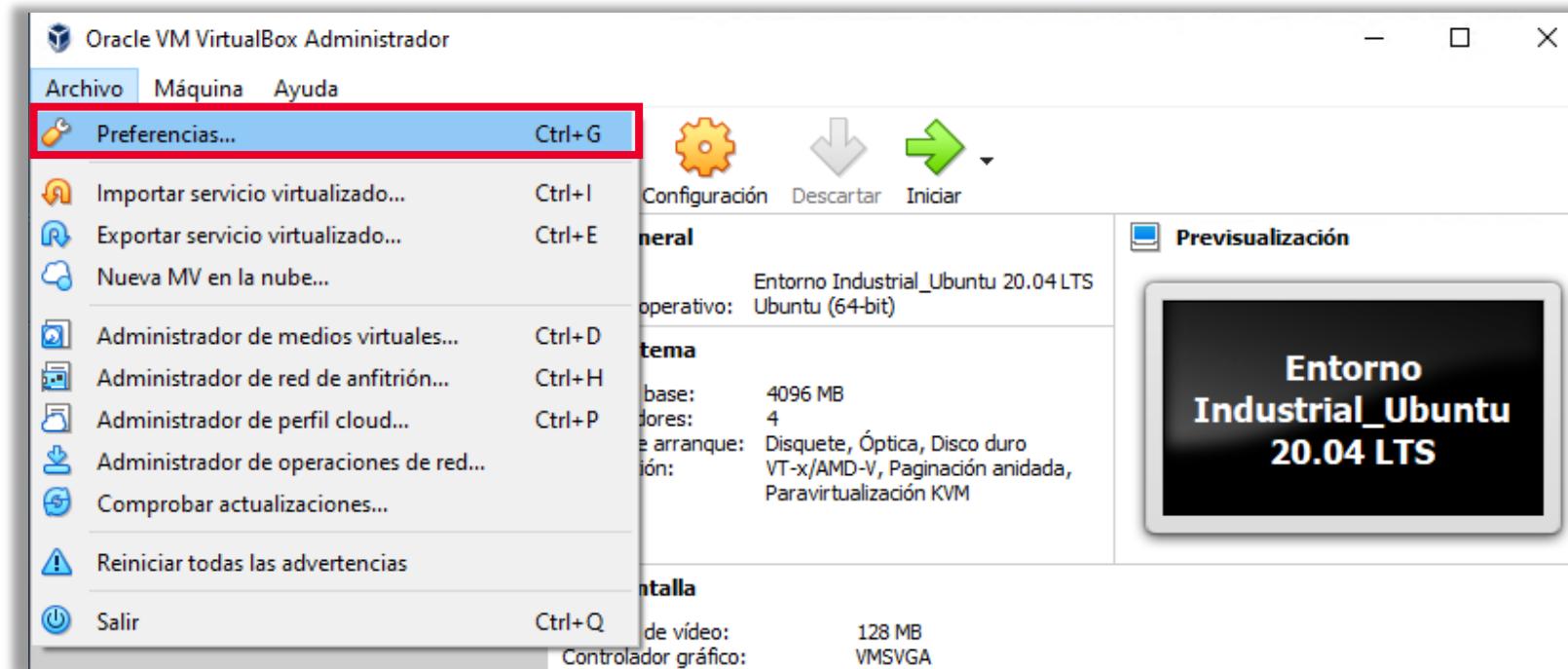


Ilustración 11: Configuración del tipo de red a través del submenú «preferencias» de la pestaña «archivo».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- En la ventana de Red, pulsa sobre el «+» para añadir una nueva red NAT.

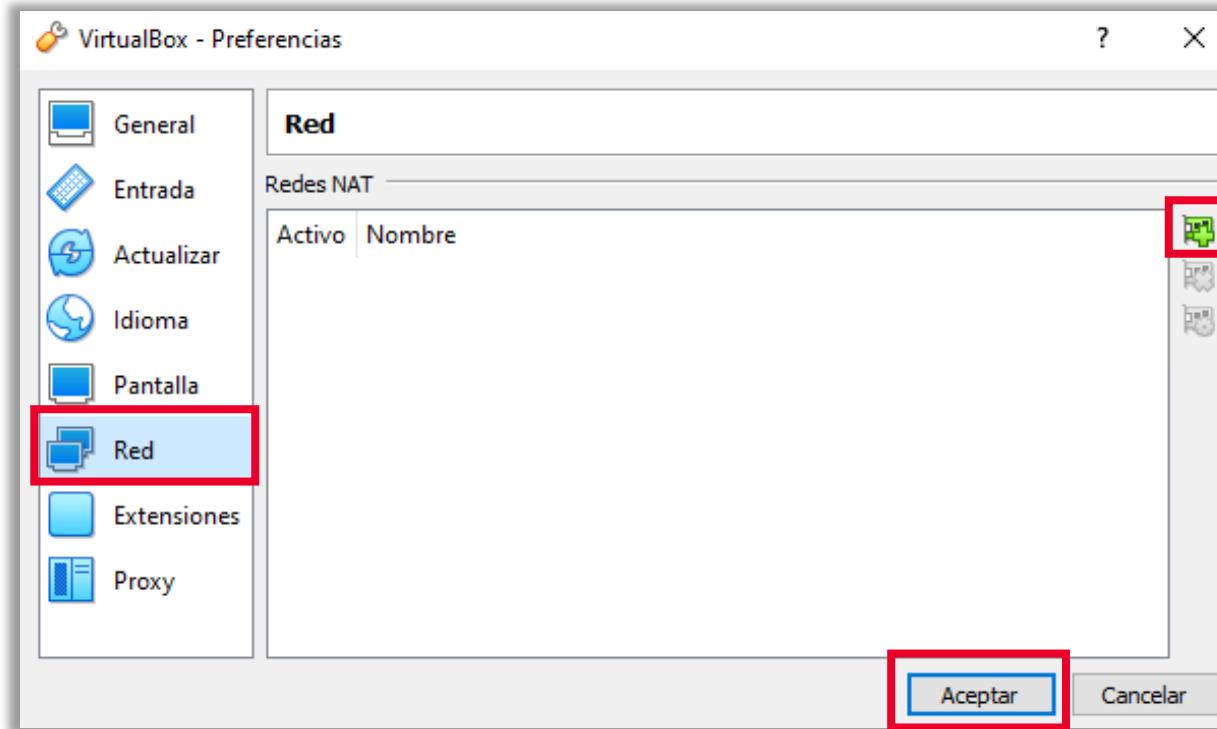


Ilustración 12: Creación de la nueva red NAT a través de la ventana «Red».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Pon el nombre que quieras, en nuestro caso hemos elegido RedNatVBox.
 - En Red CIDR deja el direccionamiento por defecto, en nuestro caso: 10.0.2.0/24. Este campo lo podrías cambiar, sin embargo, para la realización de las prácticas recomendamos que mantengas el valor por defecto, ya que lo utilizaremos posteriormente.
 - Deja seleccionado la opción de red Soporta DHCP y pulsa «Aceptar».

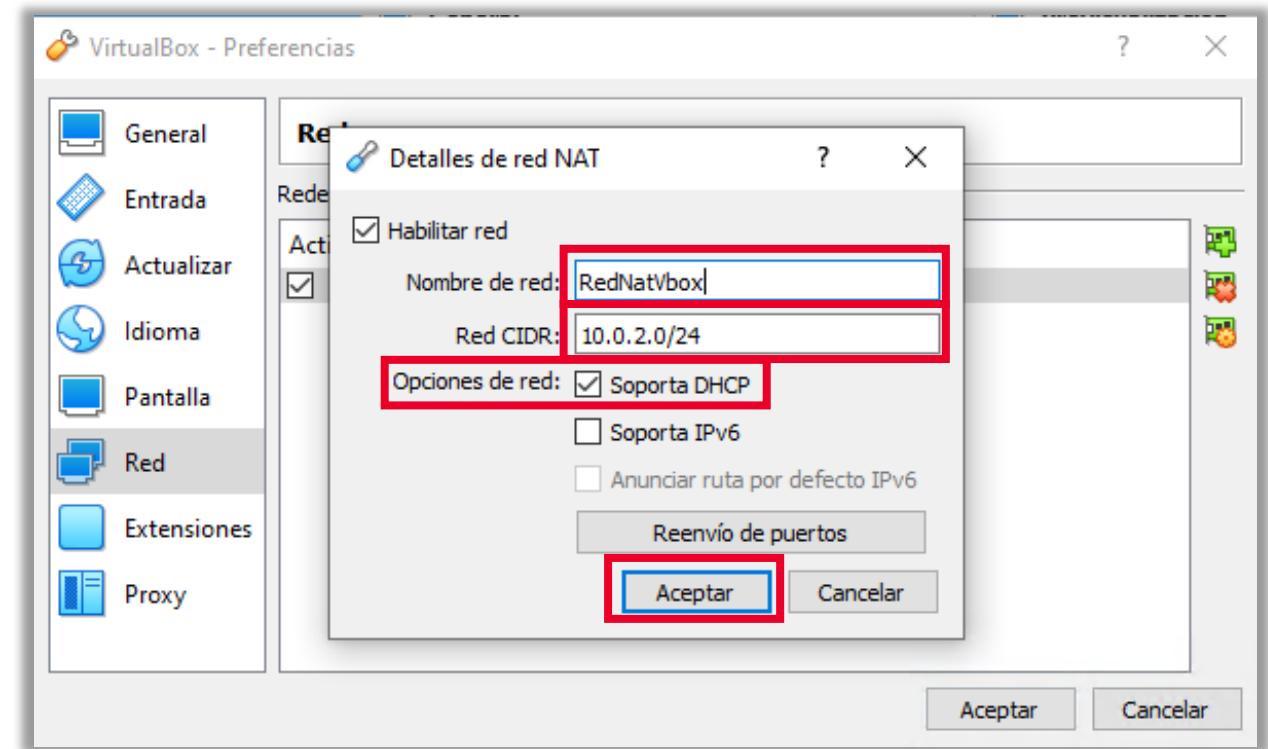


Ilustración 13: Introducción del nombre de la red, de red CIDR y de opciones de red.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- En la ventana «General», configura la MV estableciendo «compartir portapapeles» y «arrastrar y soltar» en «bidireccional» para facilitar la interacción con la MV.

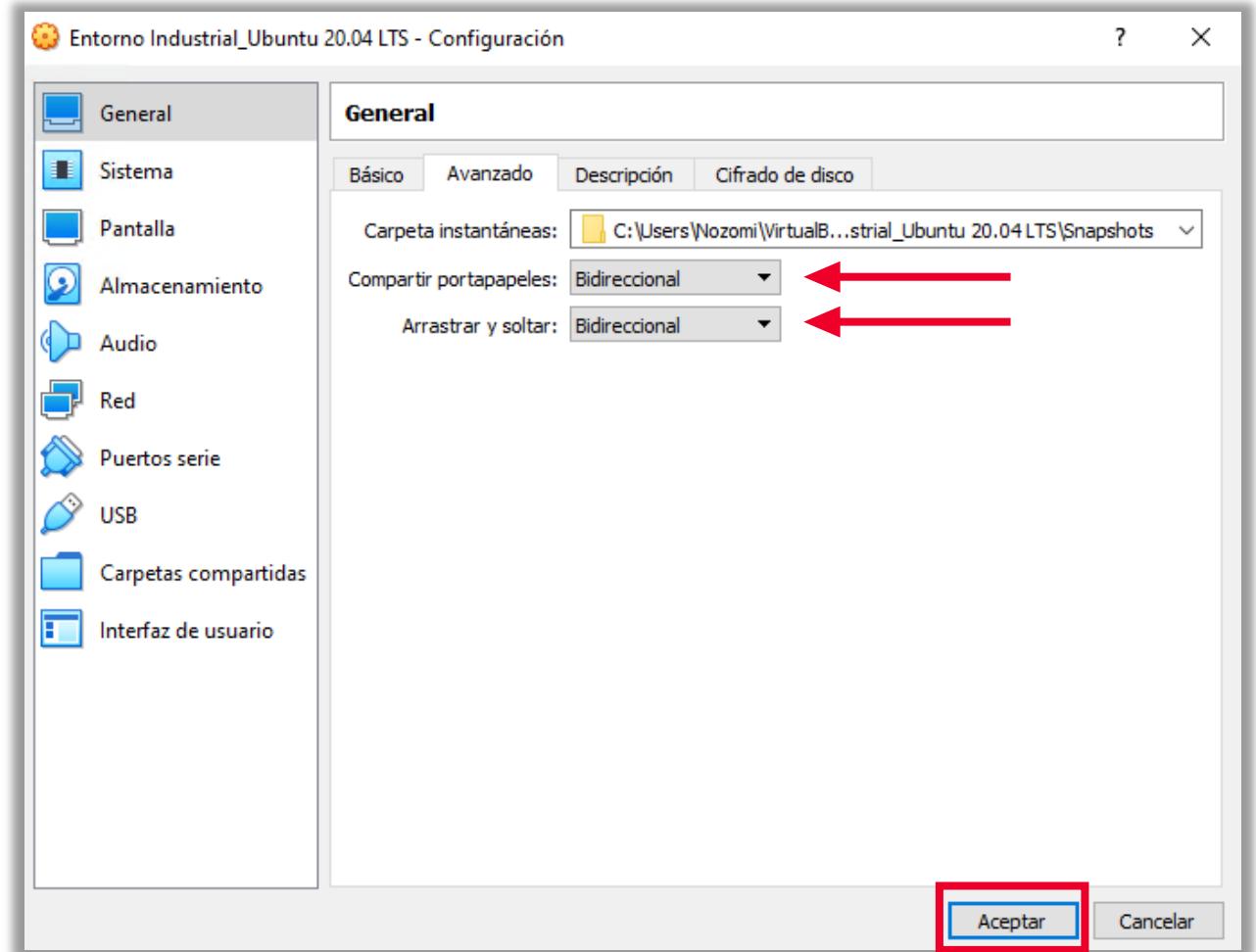


Ilustración 14: Configuración de la máquina virtual estableciendo «compartir portapapeles» y «arrastrar y soltar» en modo «bidireccional».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- En la ventana «Sistema», en la pestaña «Procesador», configura 4 CPU.

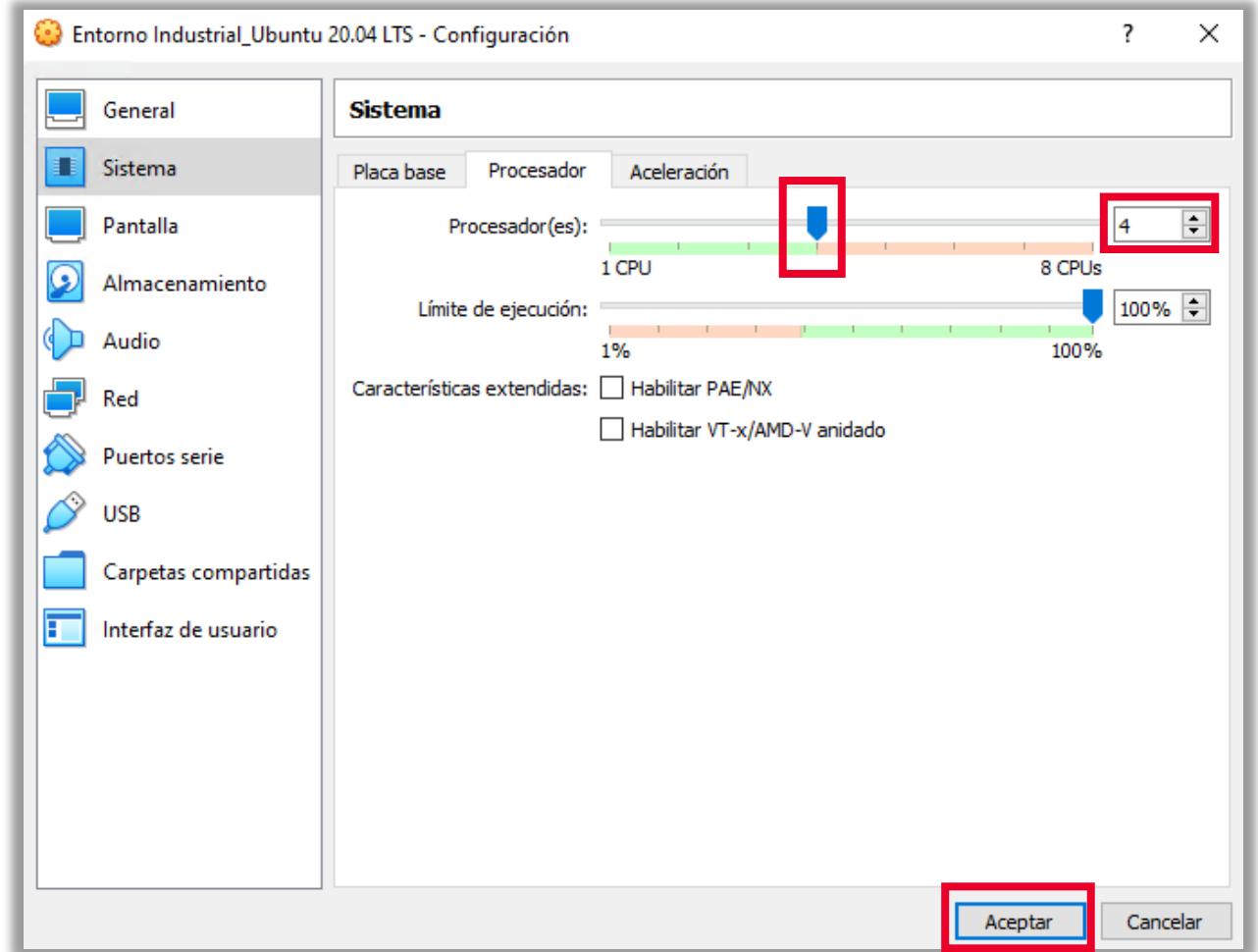


Ilustración 15: Configuración de cuatro CPU en la pestaña «Procesador» de la ventana «Sistema».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- En la ventana Pantalla, configura el valor de Memoria de Video en 128 Mb. Además, establece el controlador gráfico en «VboxSVGA» para que el instalador de Ubuntu te muestre toda la ventana y no te la recorte en el proceso de instalación. Este valor lo cambiarás cuando hayas terminado con la instalación de Ubuntu.

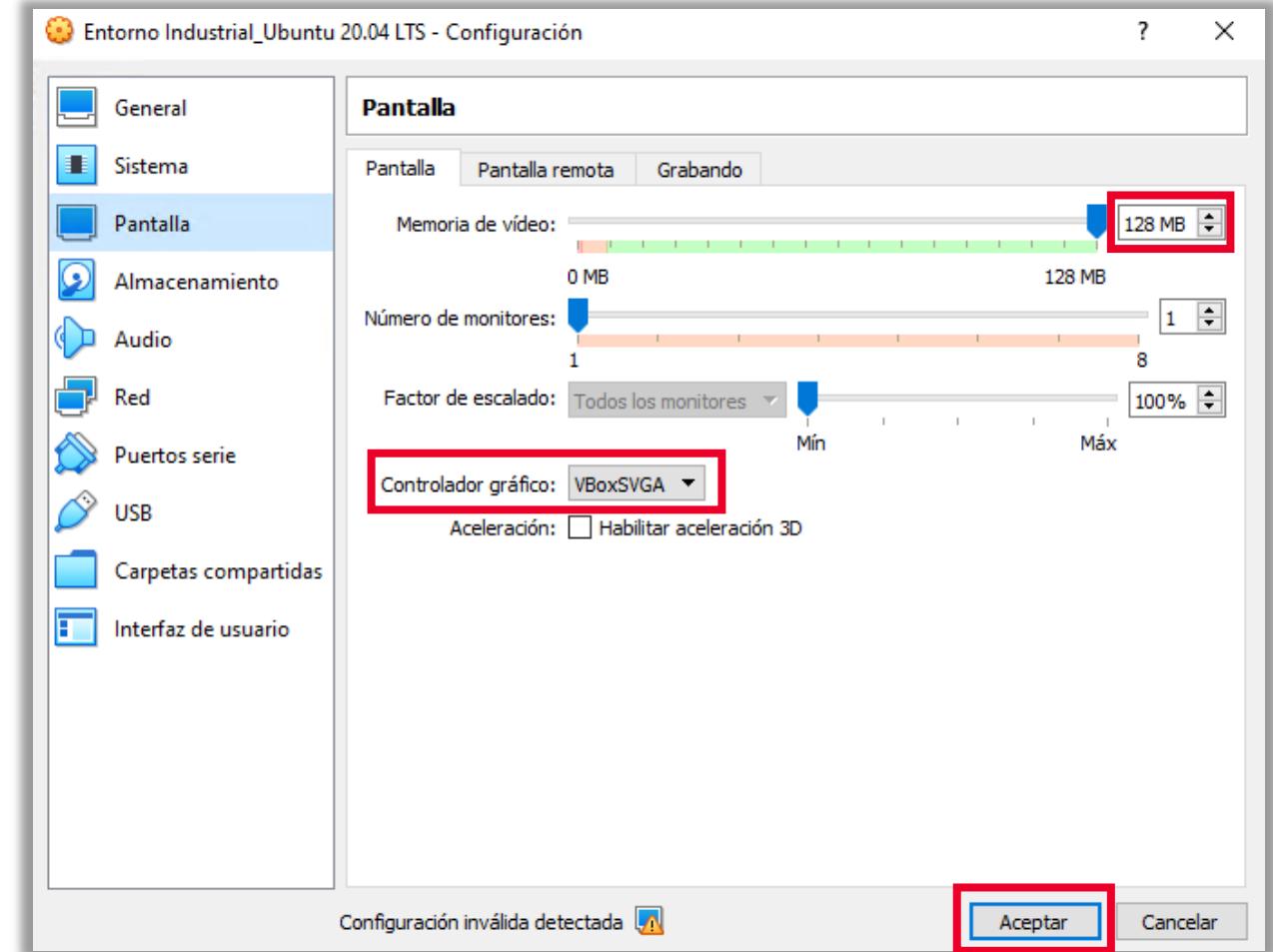


Ilustración 16: Configuración de la memoria de vídeo a 128 MB y establecimiento del controlador de vídeo.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- En la ventana «Almacenamiento», selecciona el disco «vacío» en «Controlador: IDE», y en «Unidad óptica» añade el archivo de instalación que has descargado al principio de Ubuntu 20.04 LTS.

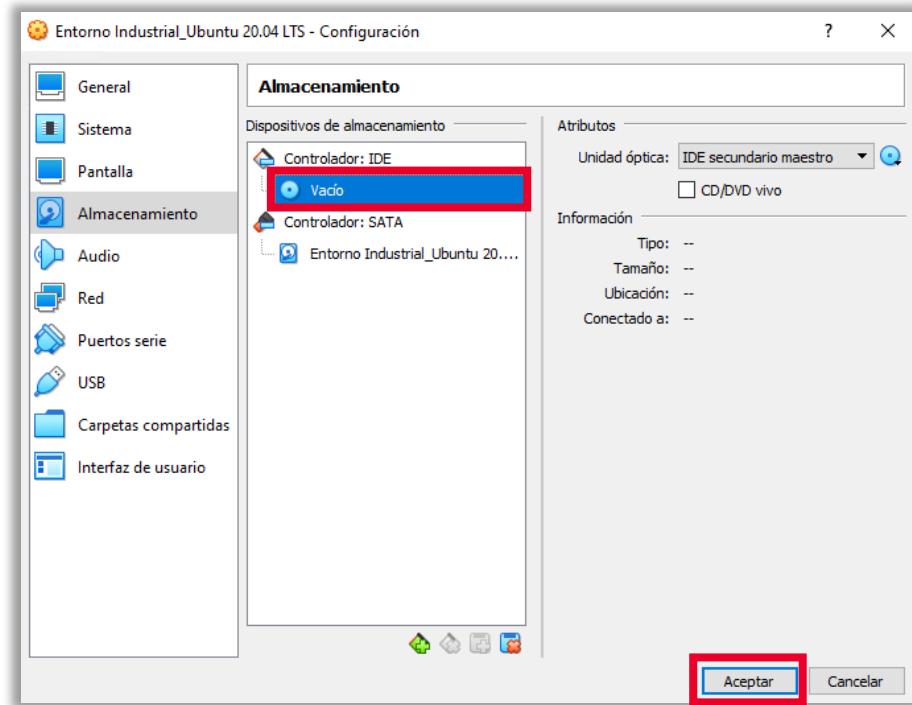


Ilustración 17: Ventana de configuración de la máquina.

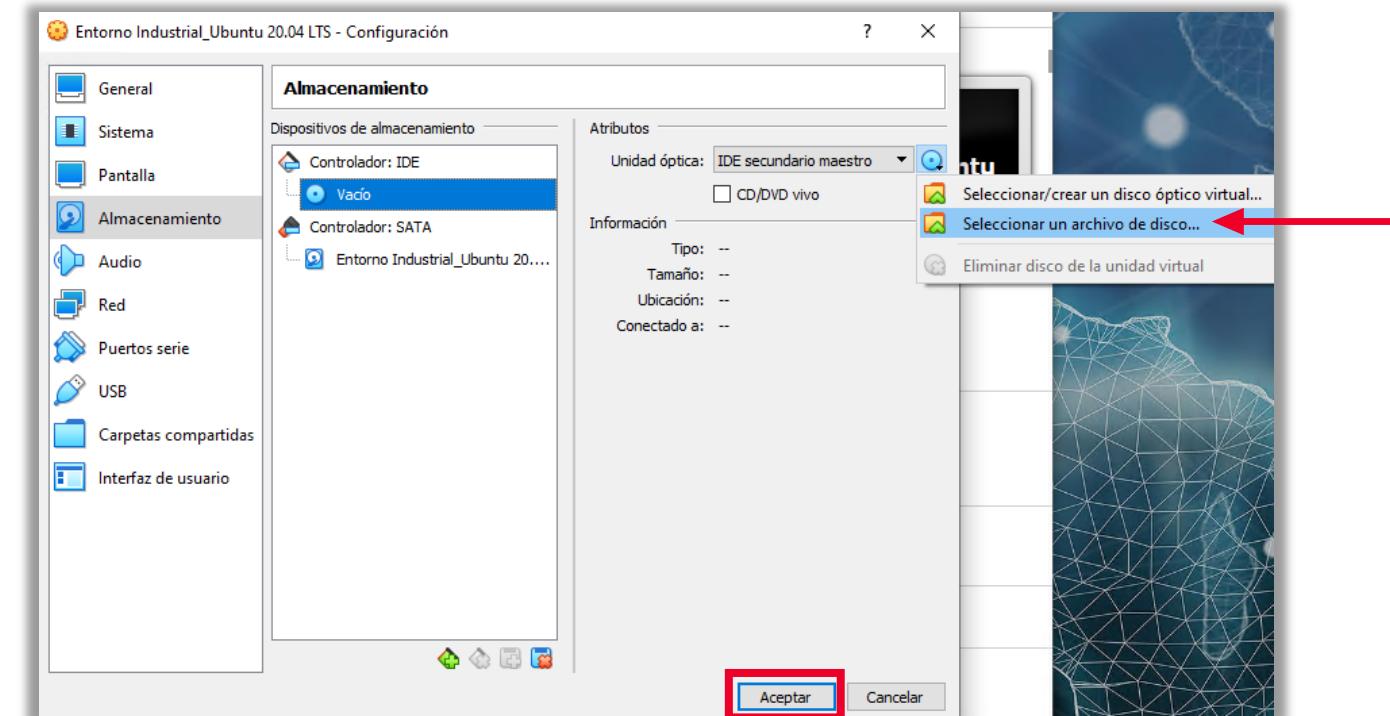


Ilustración 18: Selección del disco vacío en «Controlador: IDE».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

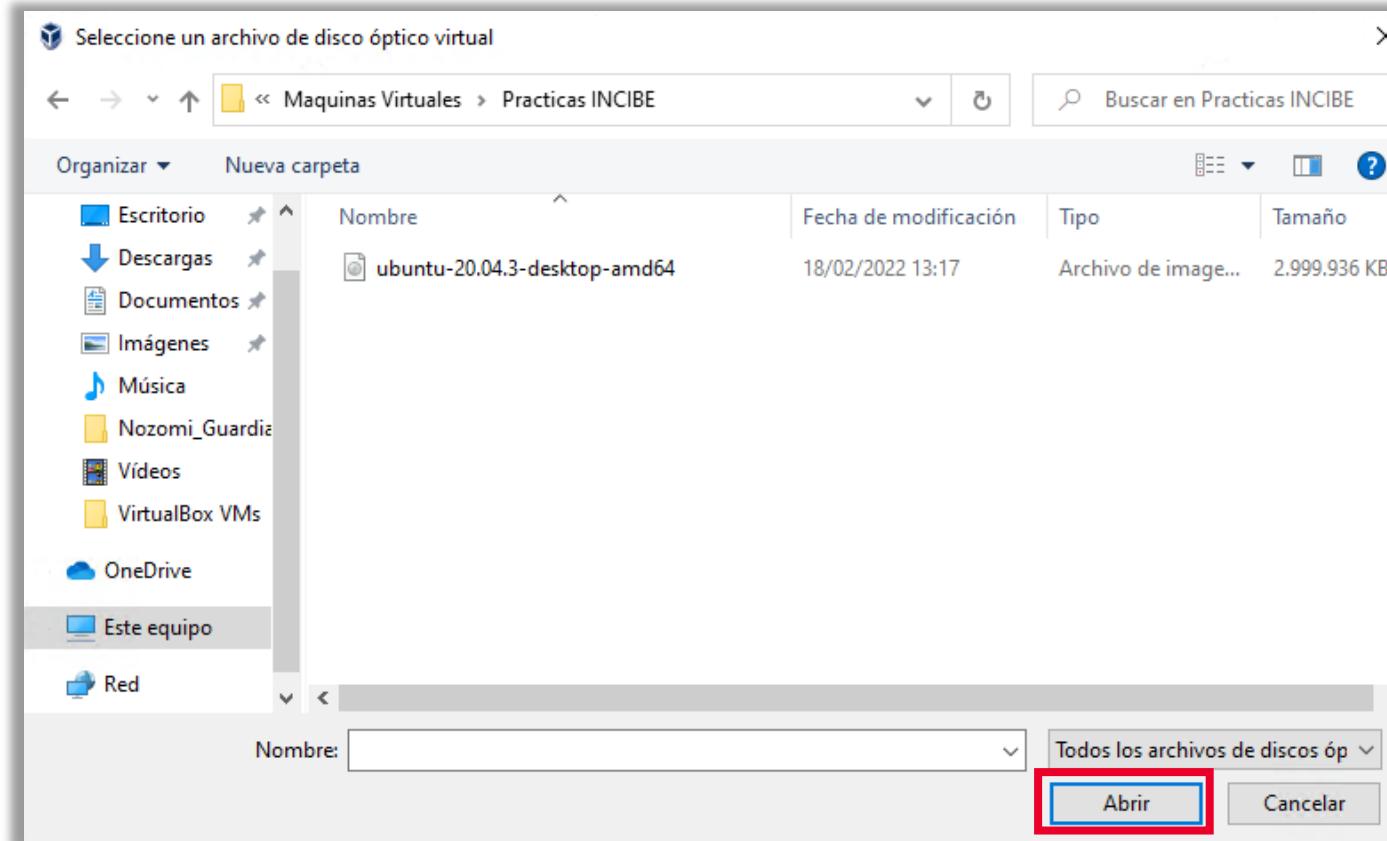


Ilustración 19: Introducción del archivo de instalación de Ubuntu 20.04.3 LTS.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Pulsa «Aceptar» para aplicar los cambios que has realizado.

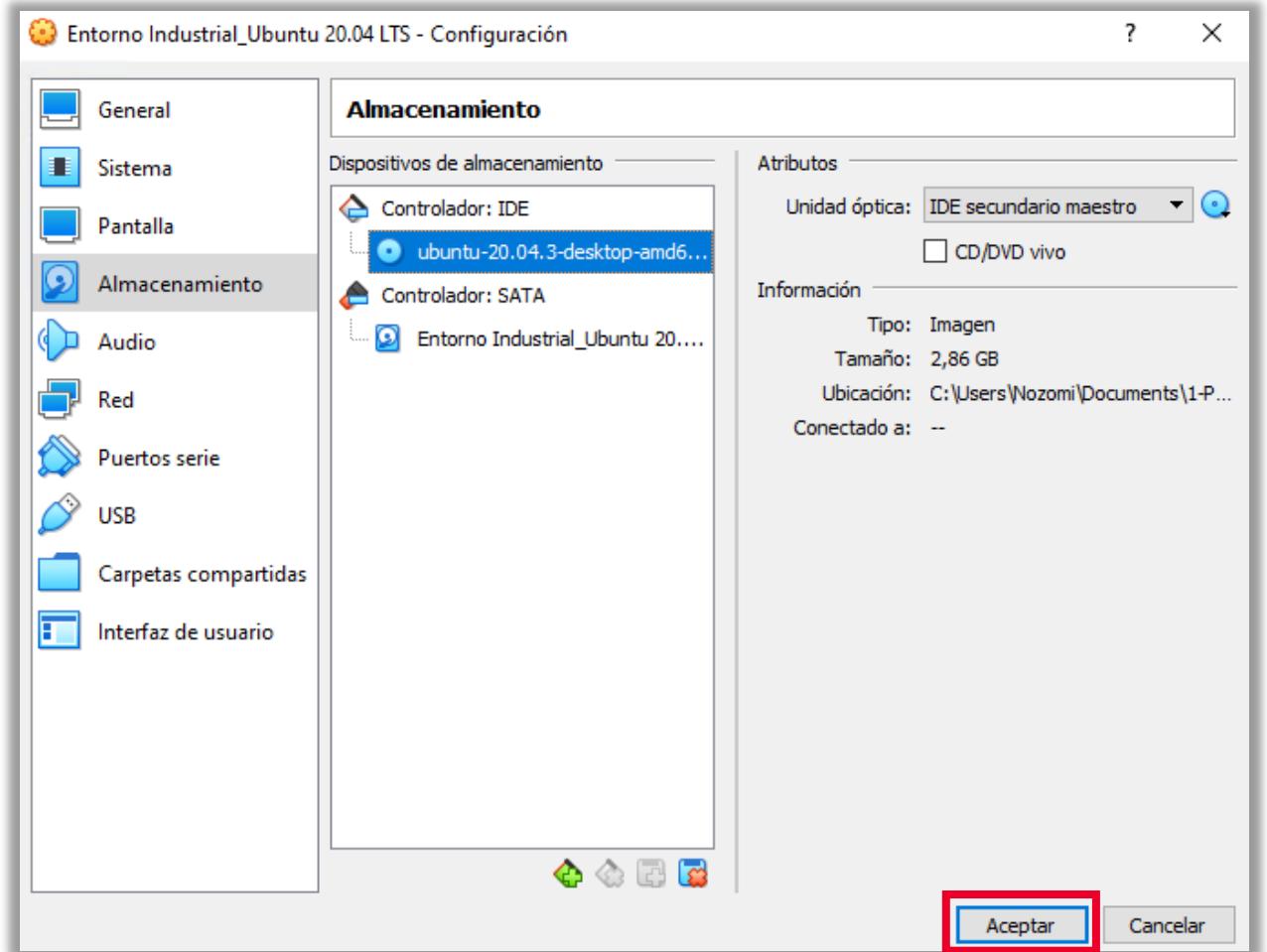


Ilustración 20: Ventana de aceptación de los cambios introducidos.

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Por último, cambia el adaptador de red a «Red NAT».

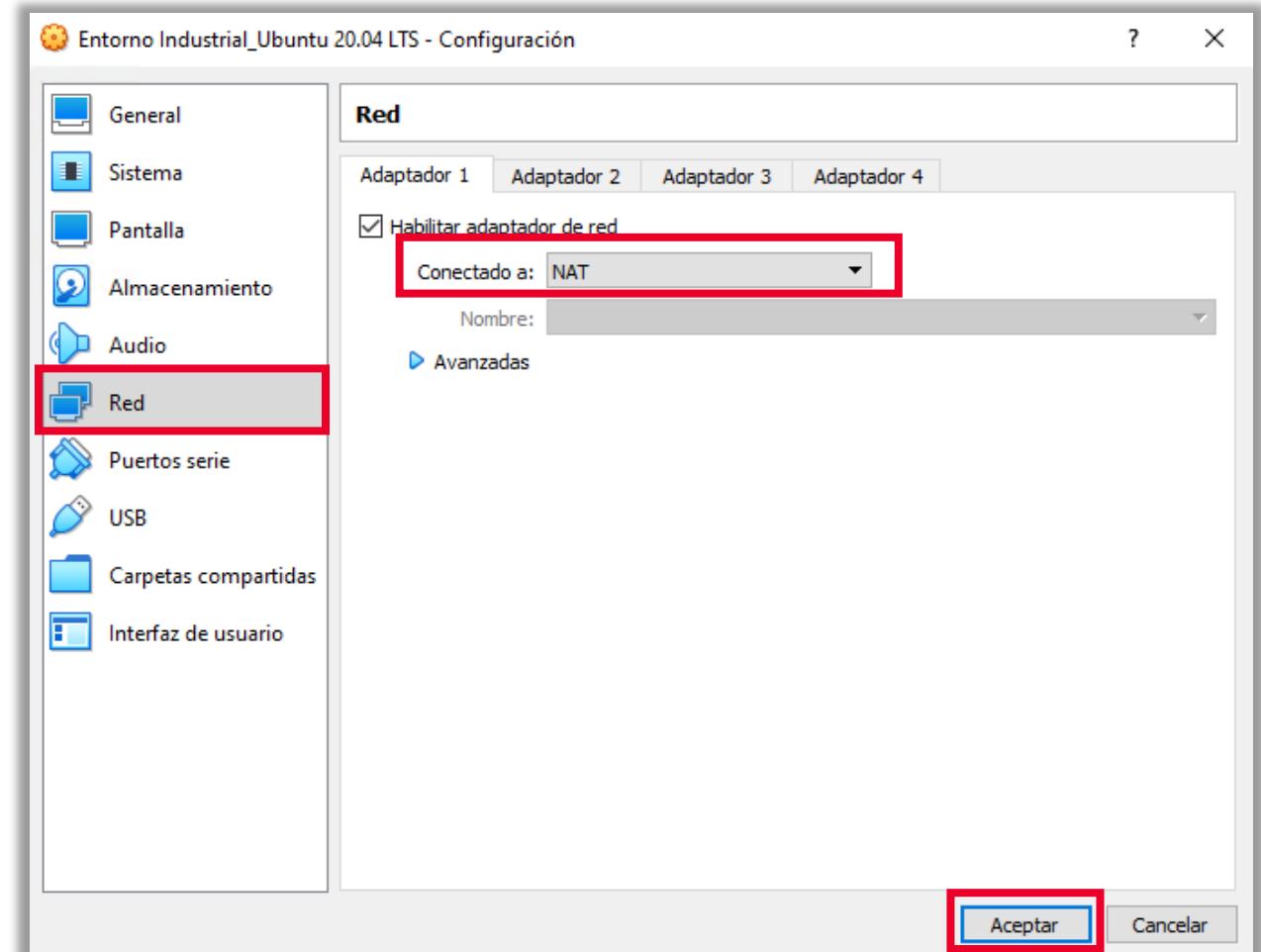


Ilustración 21: Ventana de «red».

2

INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU

- Para terminar de configurar, pulsa «Aceptar».

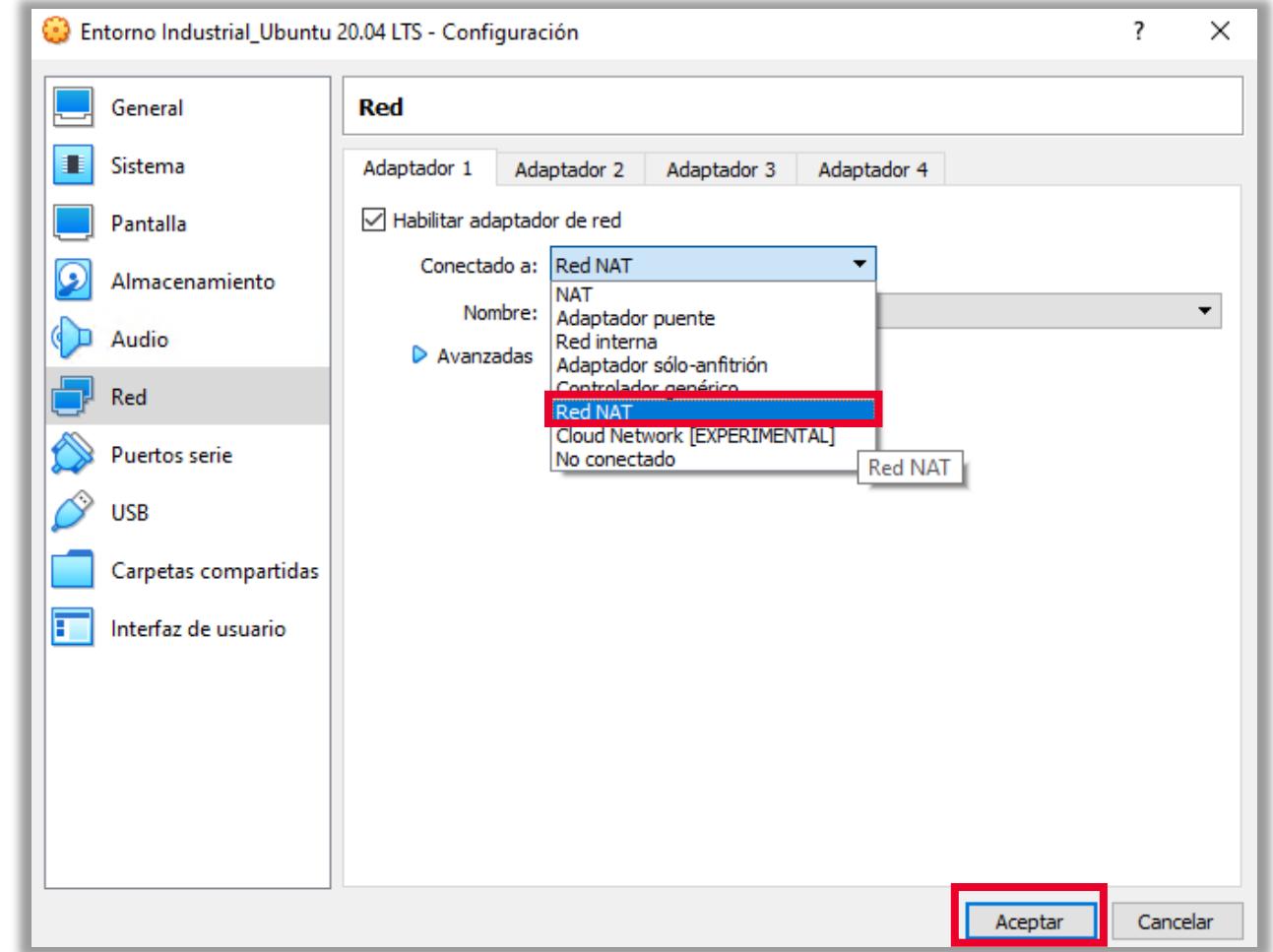
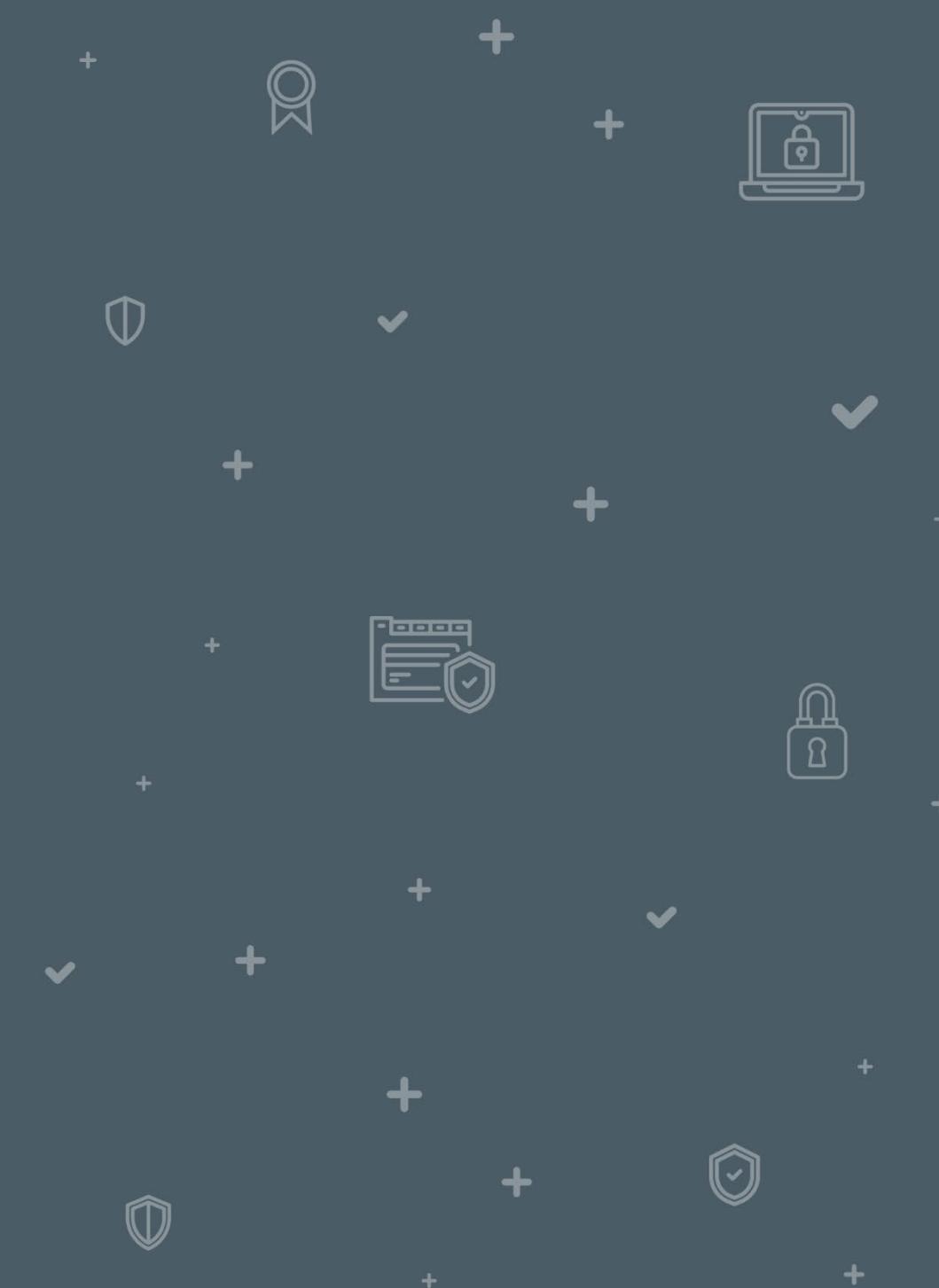


Ilustración 22: Cambio del adaptador 1 a «Red NAT».

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

3



3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Pulsa el botón «Iniciar» para arrancar la MV o haz doble clic sobre la MV para que comience el proceso de instalación de Ubuntu.

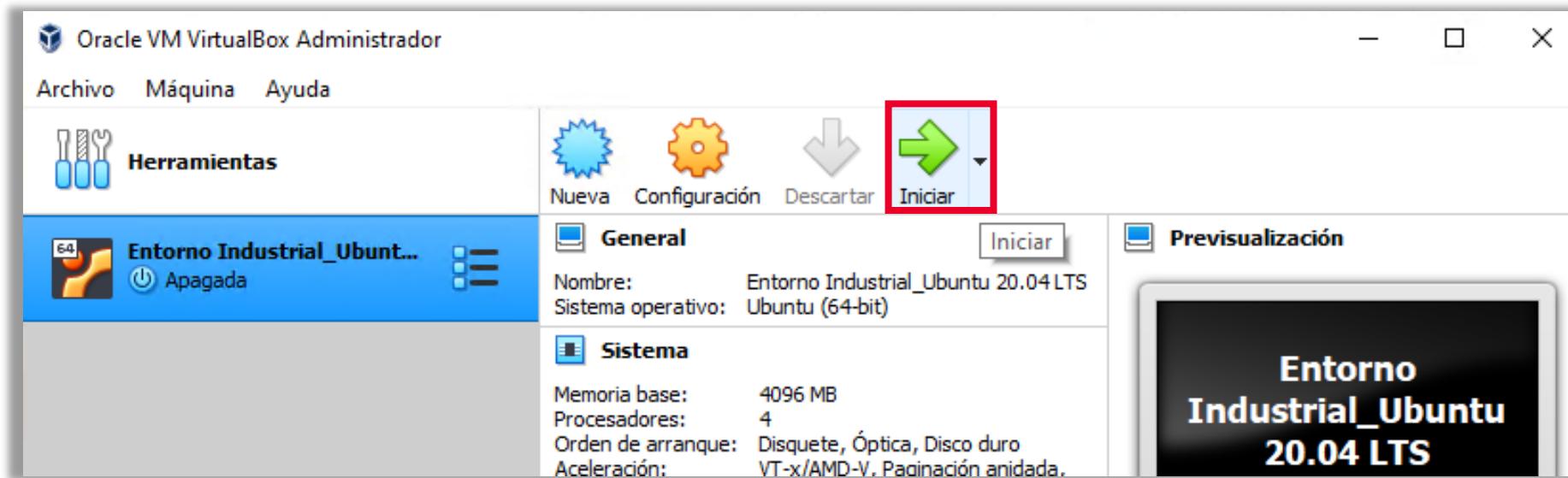


Ilustración 23: Ventana con botón iniciar para arrancar la máquina virtual.

3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- En caso necesario, modifica el tamaño de la ventana arrastrando los bordes para poder ver toda la ventana del instalador.
- Cuando la MV inicie, aparecerá esta pantalla.

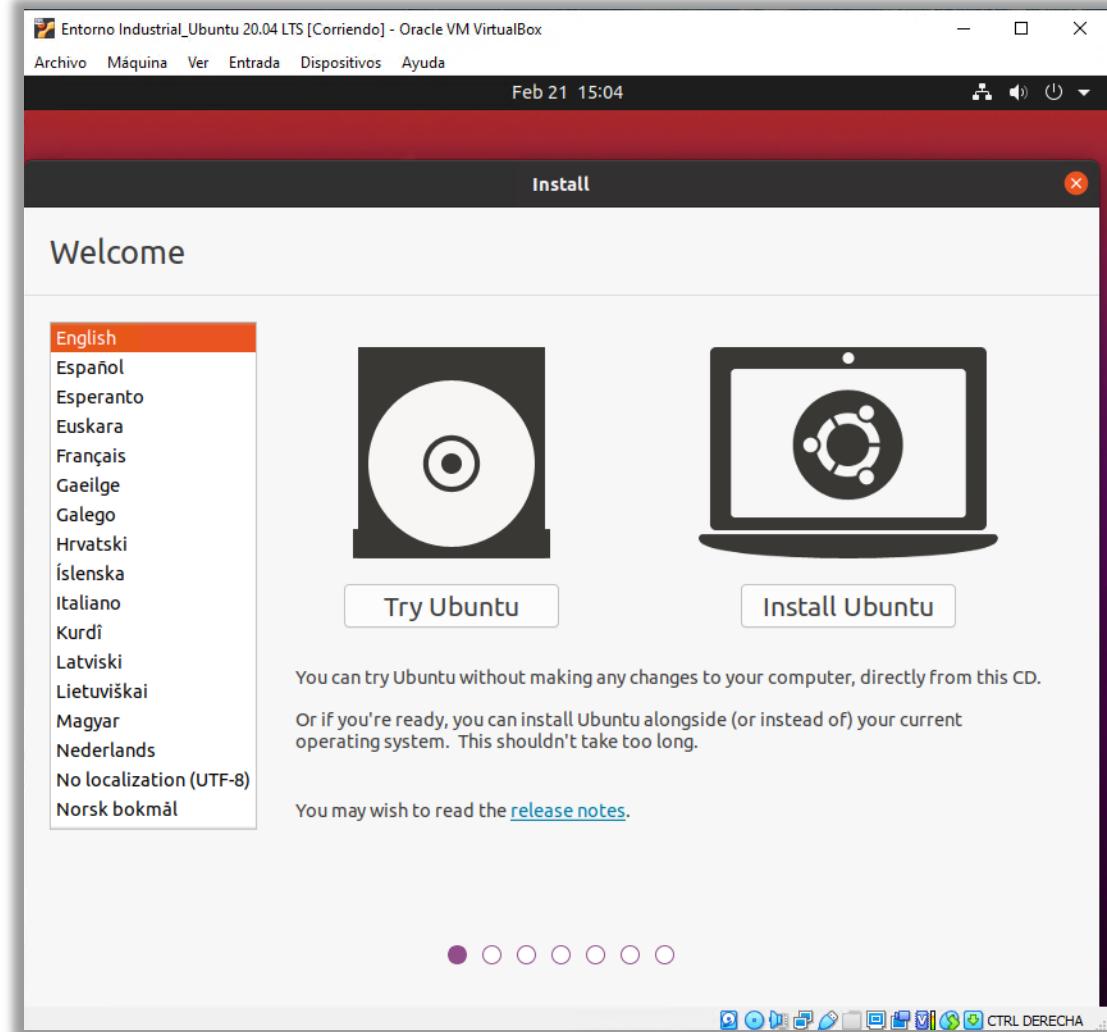


Ilustración 24: Ventana de inicio de la máquina virtual.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Selecciona el idioma «Español» y pulsa el botón «Instalar Ubuntu».



Ilustración 25: Selección de idioma «Español»
e instalación de «Ubuntu».

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

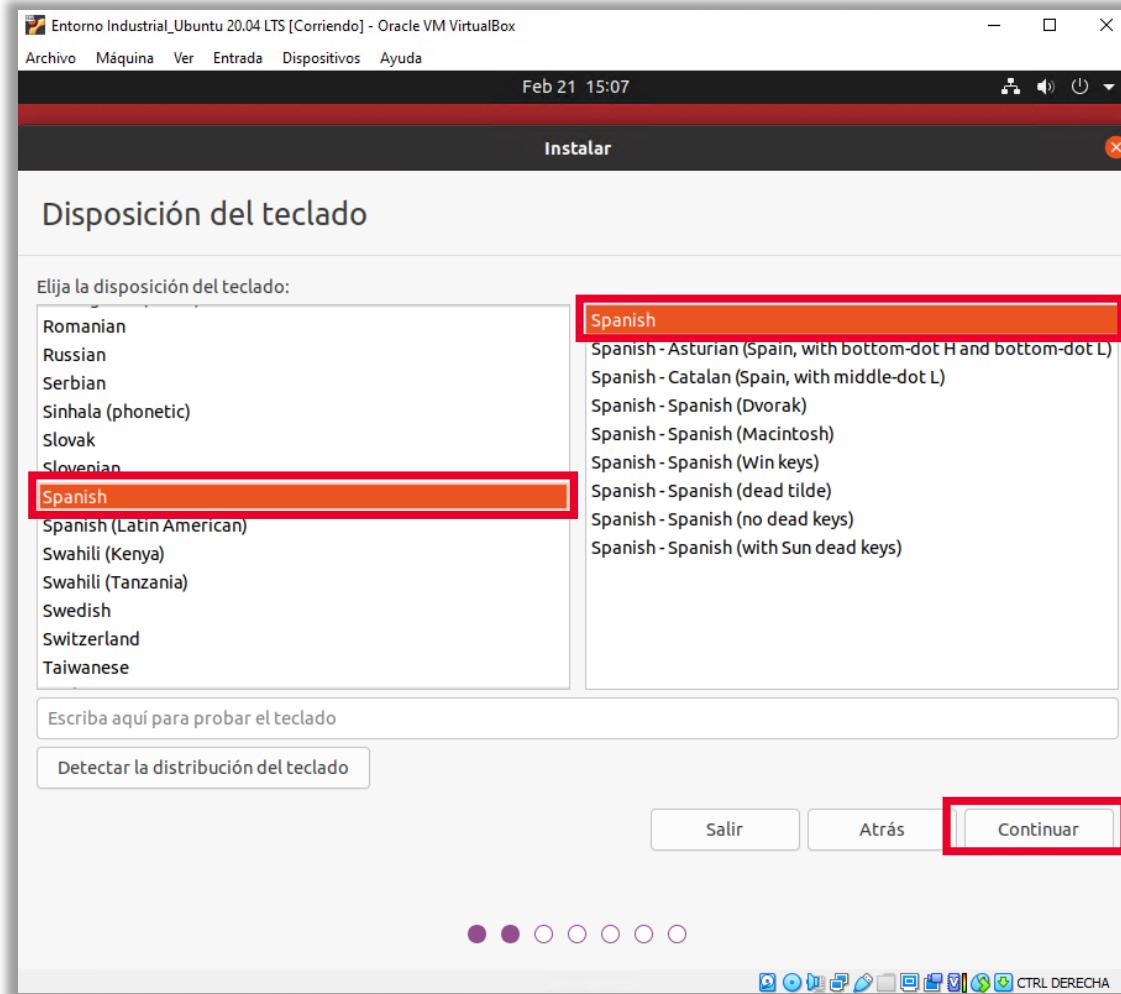


Ilustración 26: Ventana de selección del idioma del teclado.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Deja las opciones seleccionadas, como en la siguiente imagen.

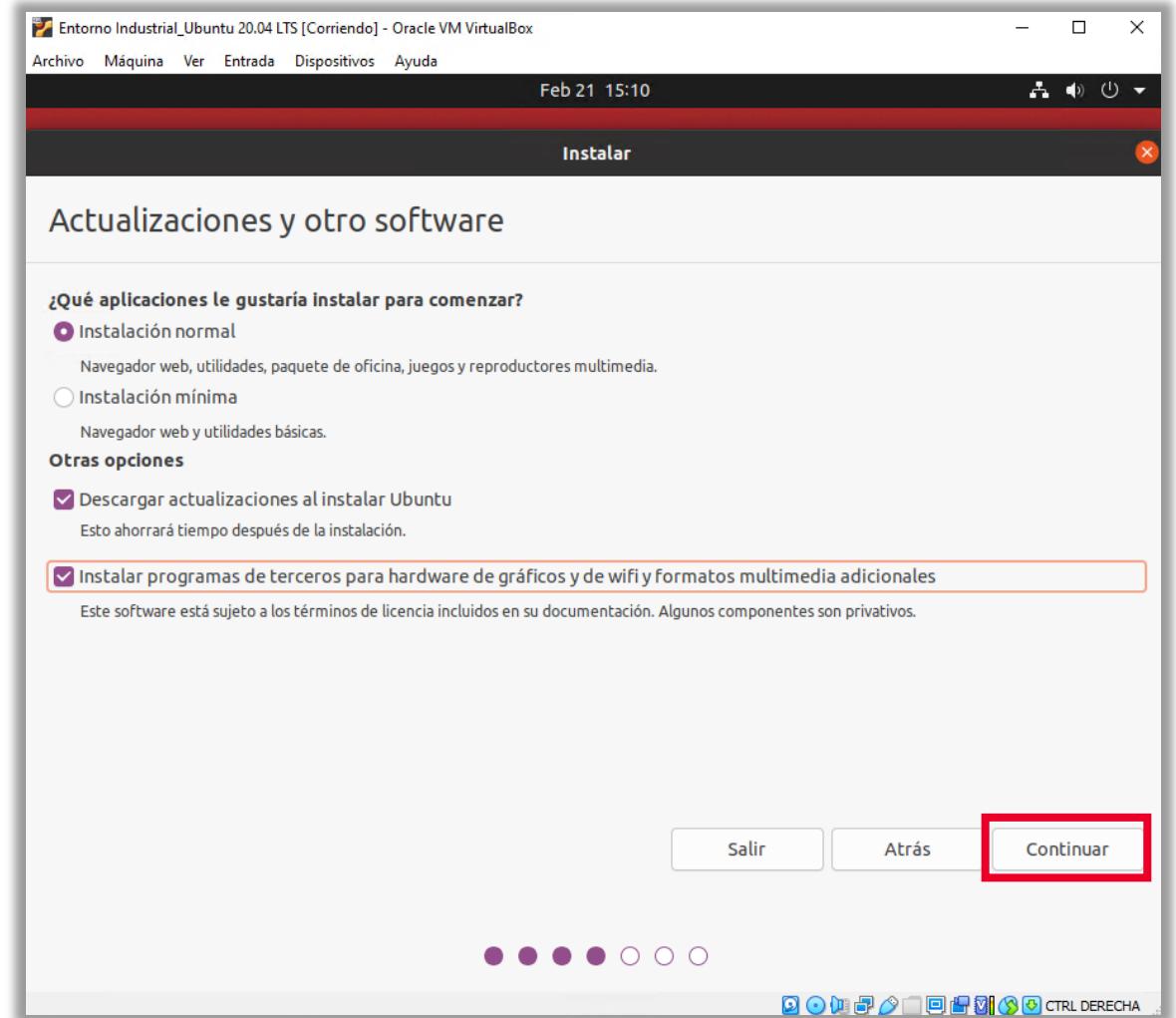


Ilustración 27: Selección de las aplicaciones a instalar.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Deja seleccionada por defecto la opción «Borrar disco e instalar Ubuntu». Te aparecerá un *pop up* que debes confirmar. Confirma los cambios que vas a realizar al disco «virtual» con el formateo de las particiones que aparecen en la imagen.

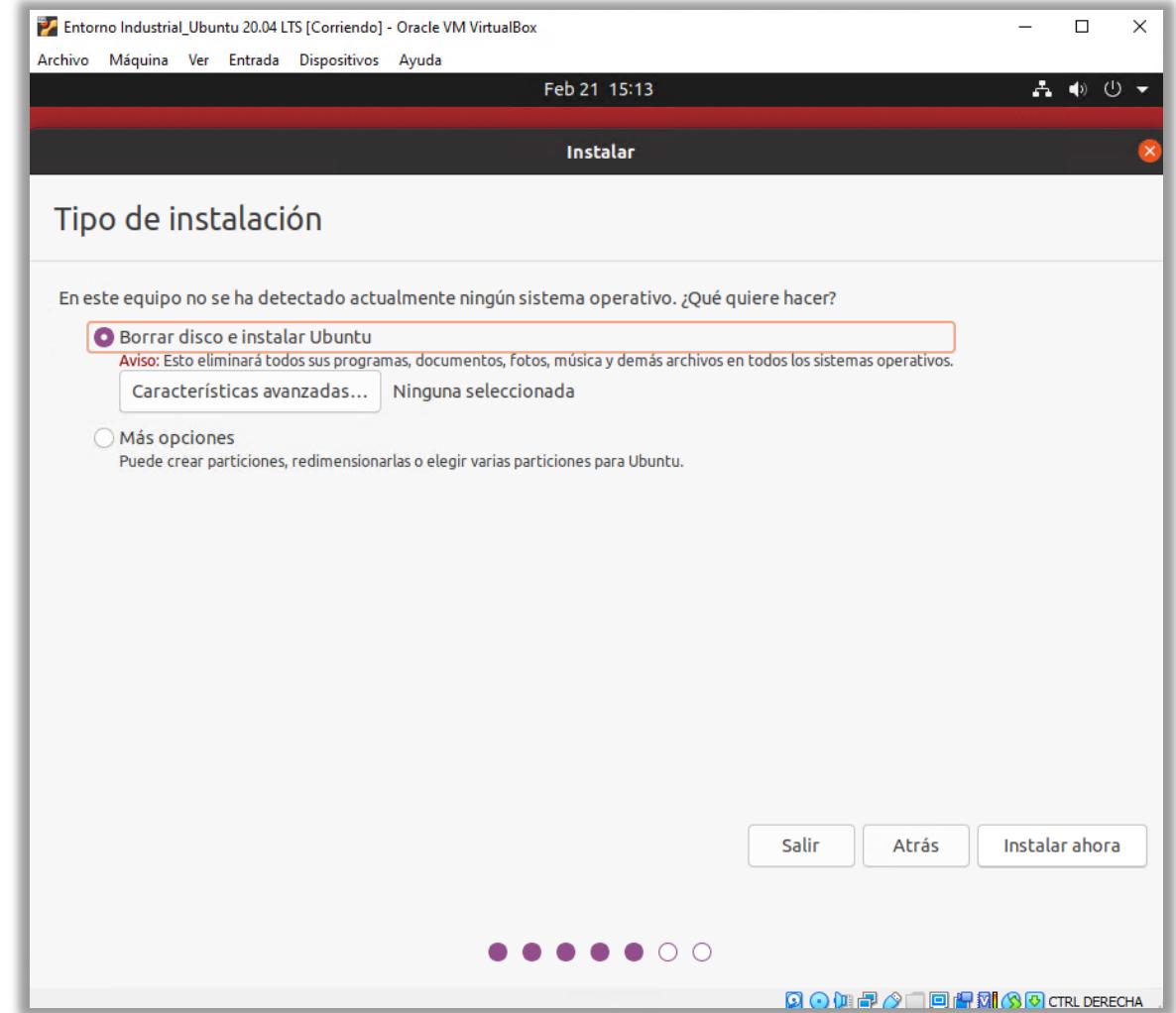


Ilustración 28: Selección de «Borrar disco e instalar Ubuntu» en la ventana de «Tipo de instalación».

3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

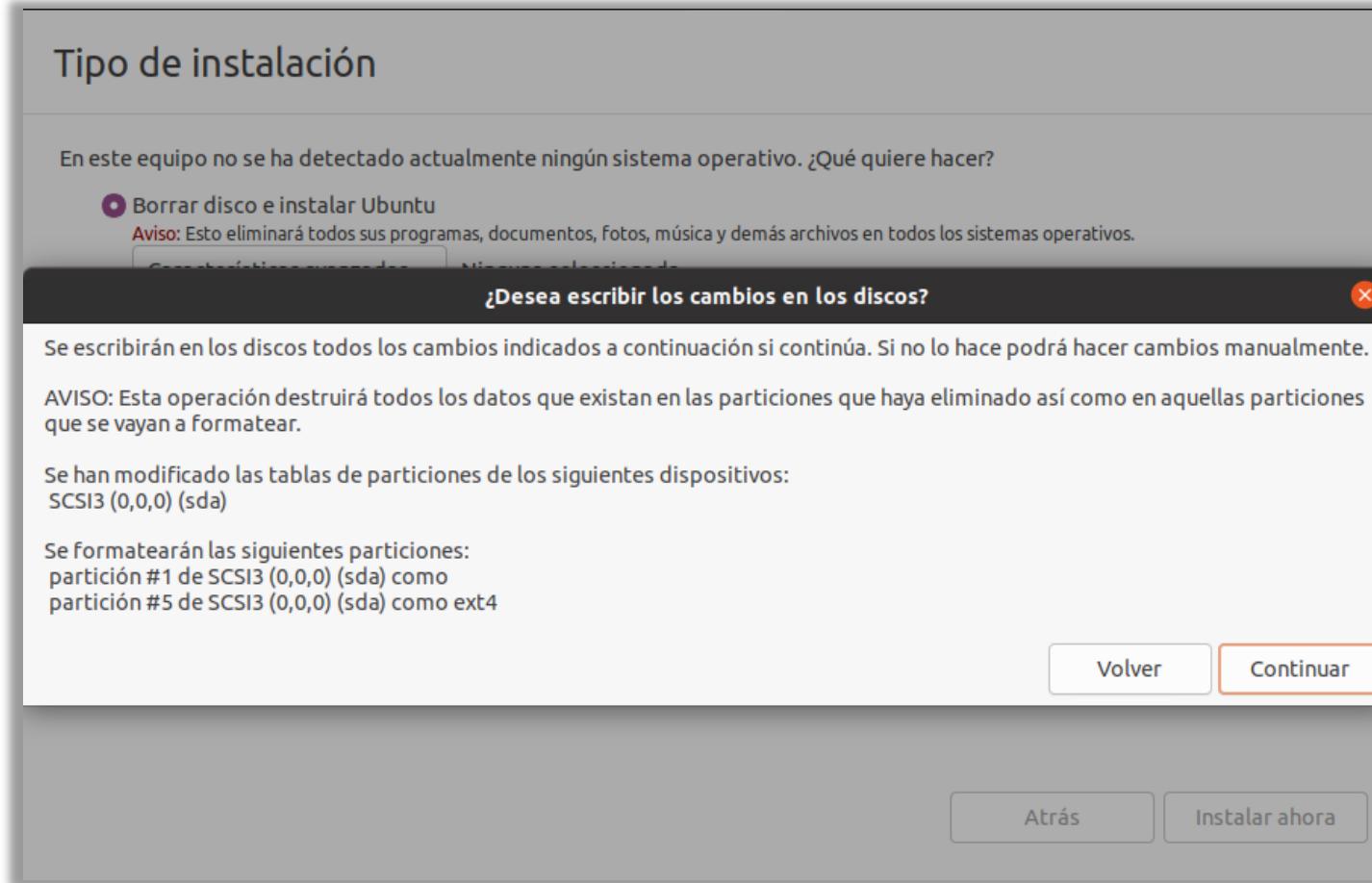


Ilustración 29: Ventana con aviso de los cambios que se van a producir.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Escribe «Madrid» en la caja de texto, para indicar tu localización (en caso de que no la haya detectado).

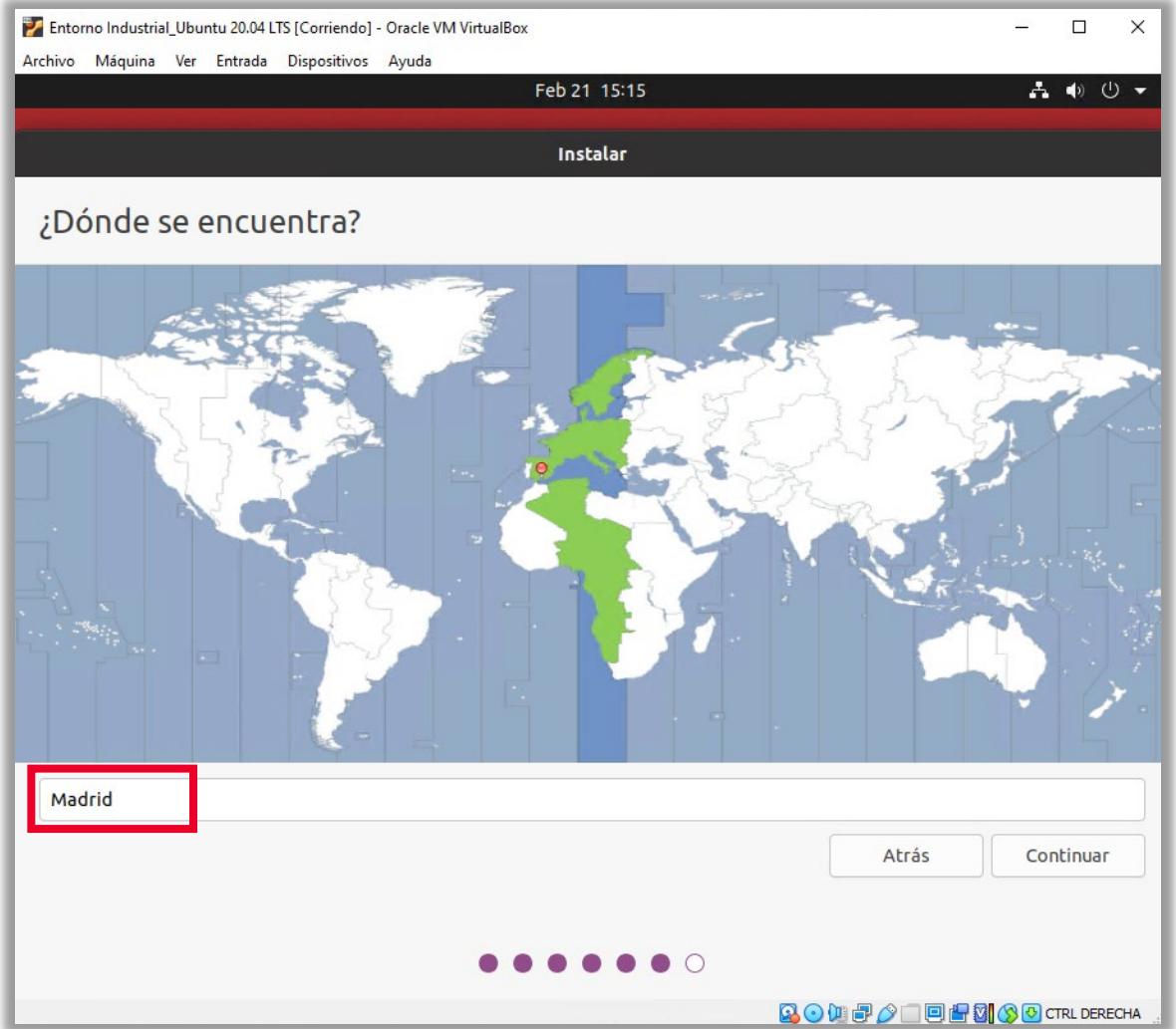


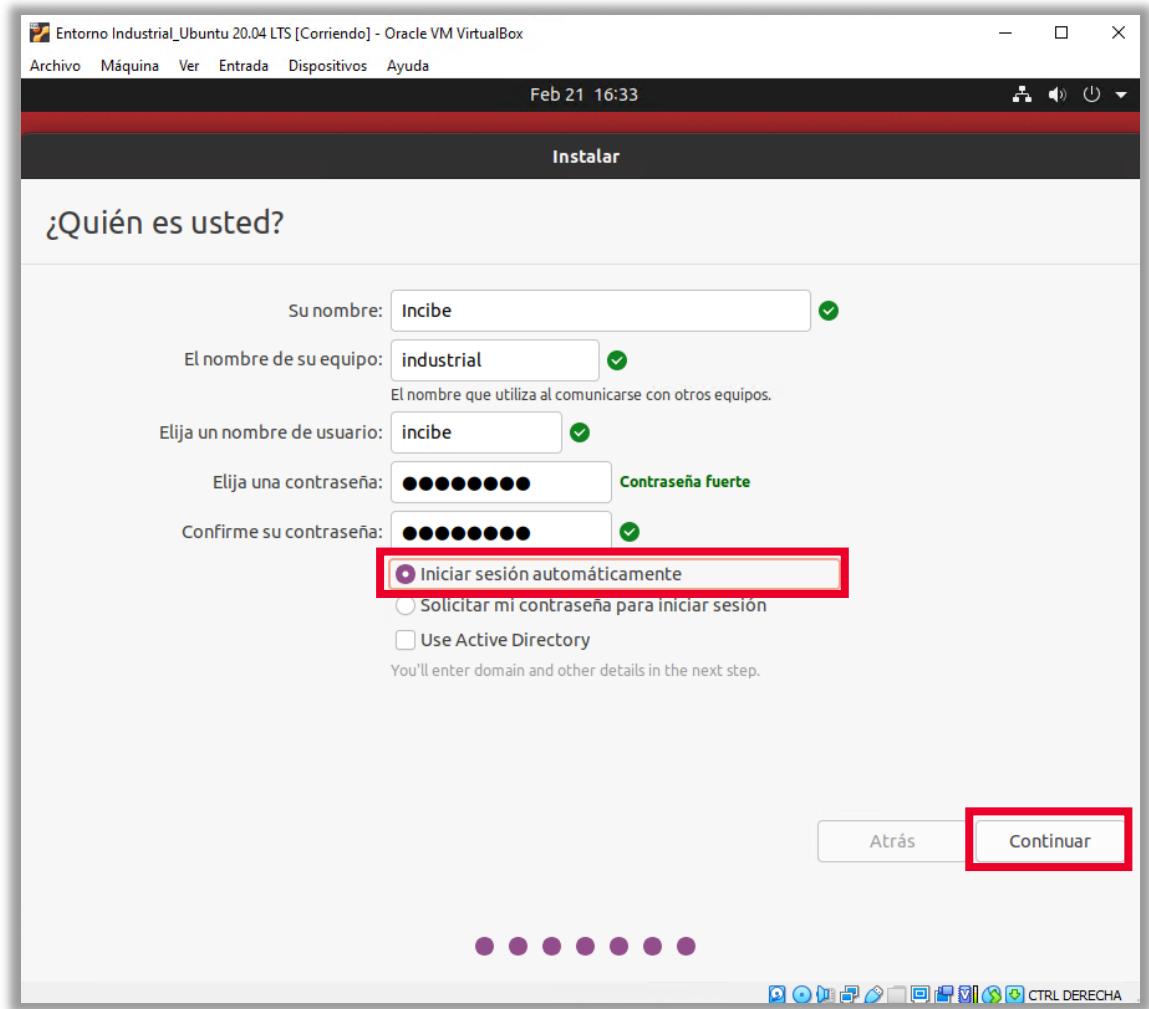
Ilustración 30: Ventana de selección de la ubicación «Madrid».

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Proporciona los datos de usuario, nombre del equipo y contraseña y marca «Iniciar sesión automáticamente». Debes acordarte de estas credenciales ya que serán las que debas introducir para acceder a la MV. Nosotros hemos utilizado los siguientes:
 - Su nombre: Incibe
 - El nombre de su equipo: industrial
 - Elija un nombre de usuario: Incibe

Ilustración 31: Ventana para introducir los datos personales y datos de acceso. Es importante no olvidarlos pues serán necesarios para acceder a la máquina virtual.



3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Después de esto comienza el proceso de descarga de paquetes de *software* e instalación de todo el sistema.

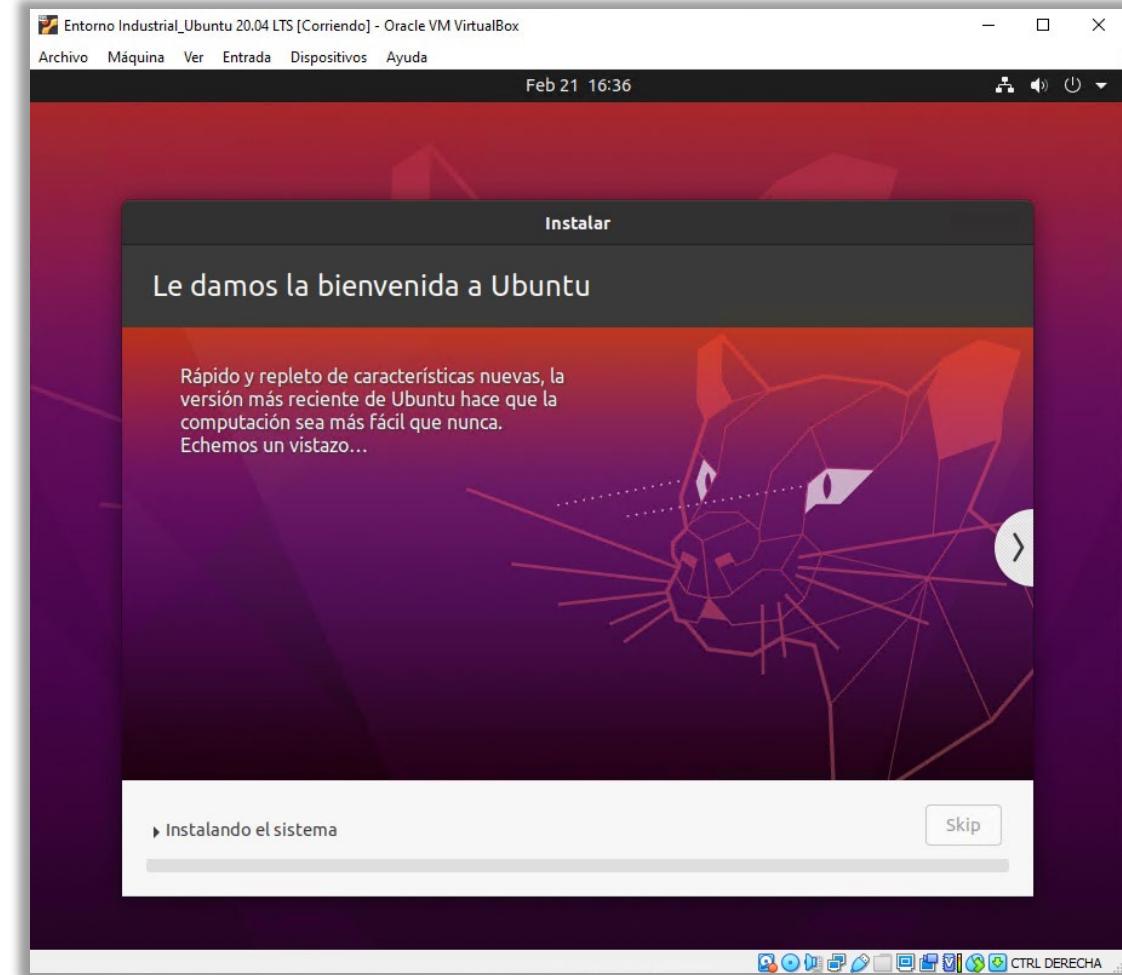


Ilustración 32: Ventana de inicio del proceso de instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Te pedirá reiniciar para completar la instalación de Ubuntu, así que pulsa sobre «Reiniciar ahora».

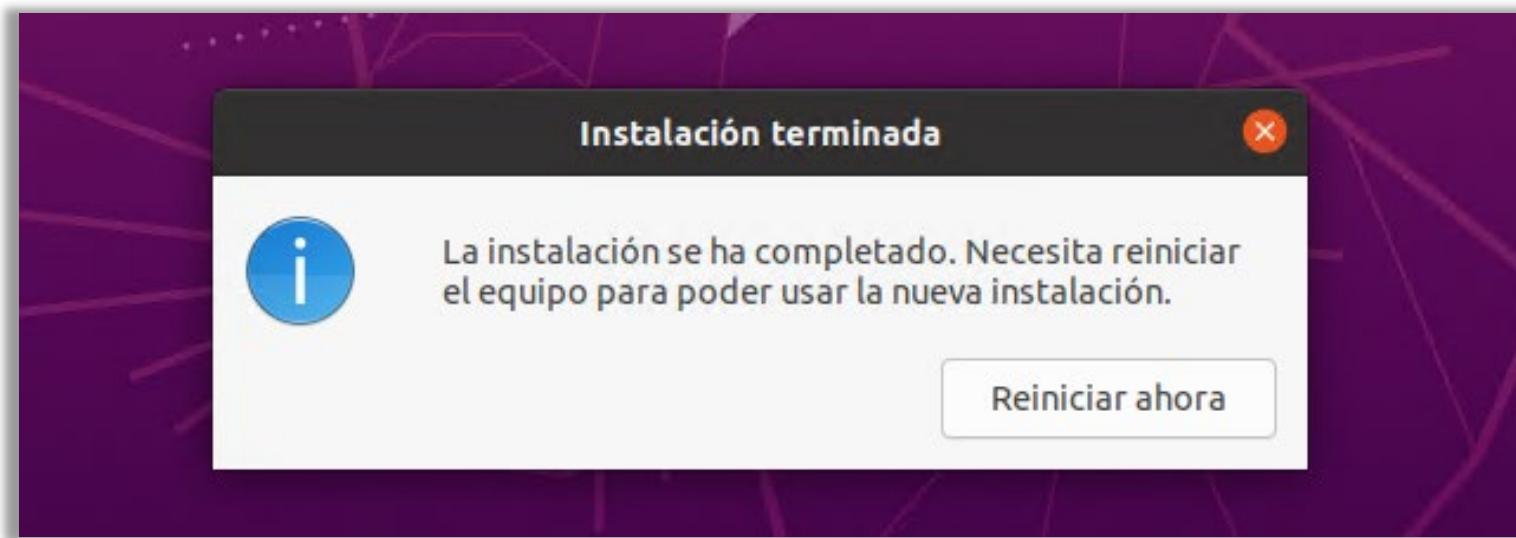


Ilustración 33: Aviso de que se ha completado la instalación y es necesario reiniciar el equipo.

3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Te pedirá en un mensaje en pantalla que elimines el disco de instalación de Ubuntu, así que pulsa «enter» para eliminarlo.

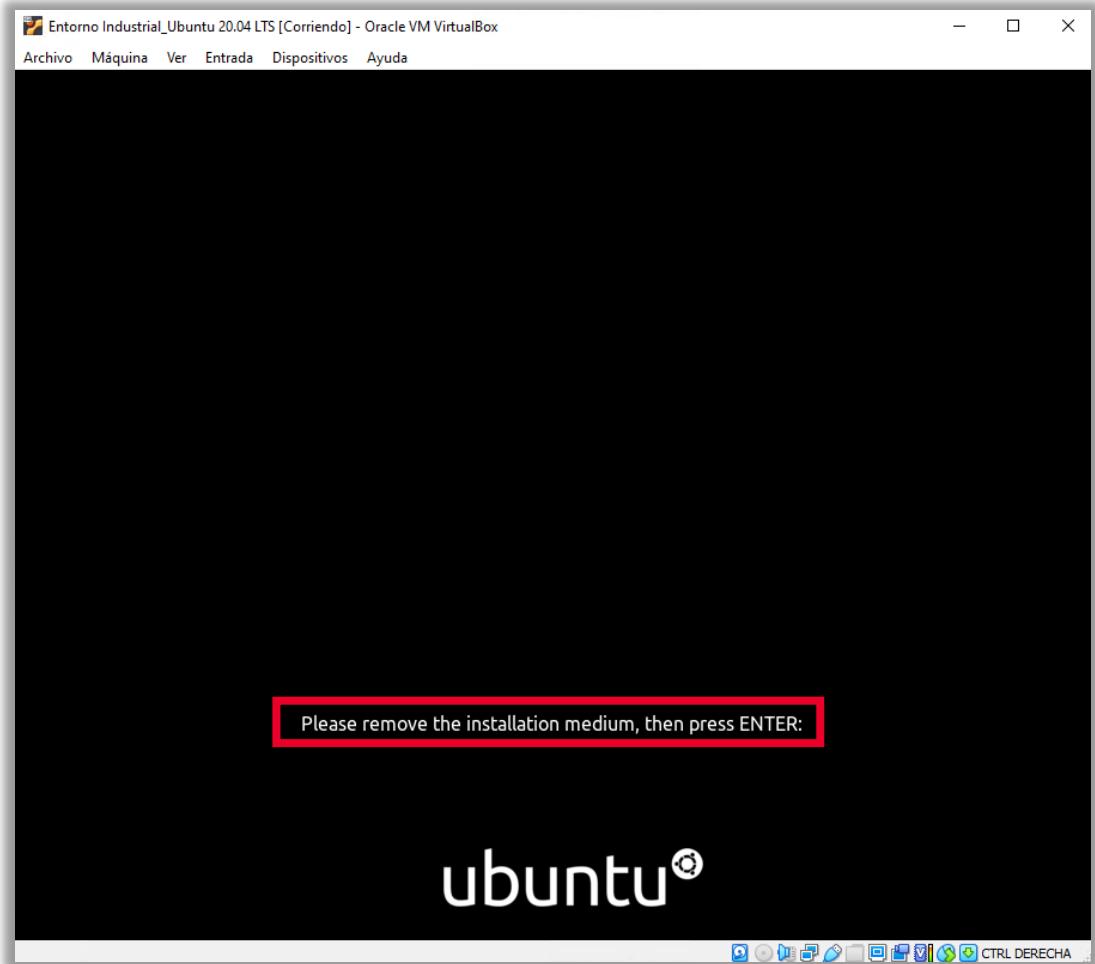


Ilustración 34: Mensaje de aviso de eliminación del disco de instalación de Ubuntu.
Pulsar «enter» para aceptar.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Comprueba en la ventana de VirtualBox, que en el apartado «Almacenamiento», la unidad óptica ya está vacía.

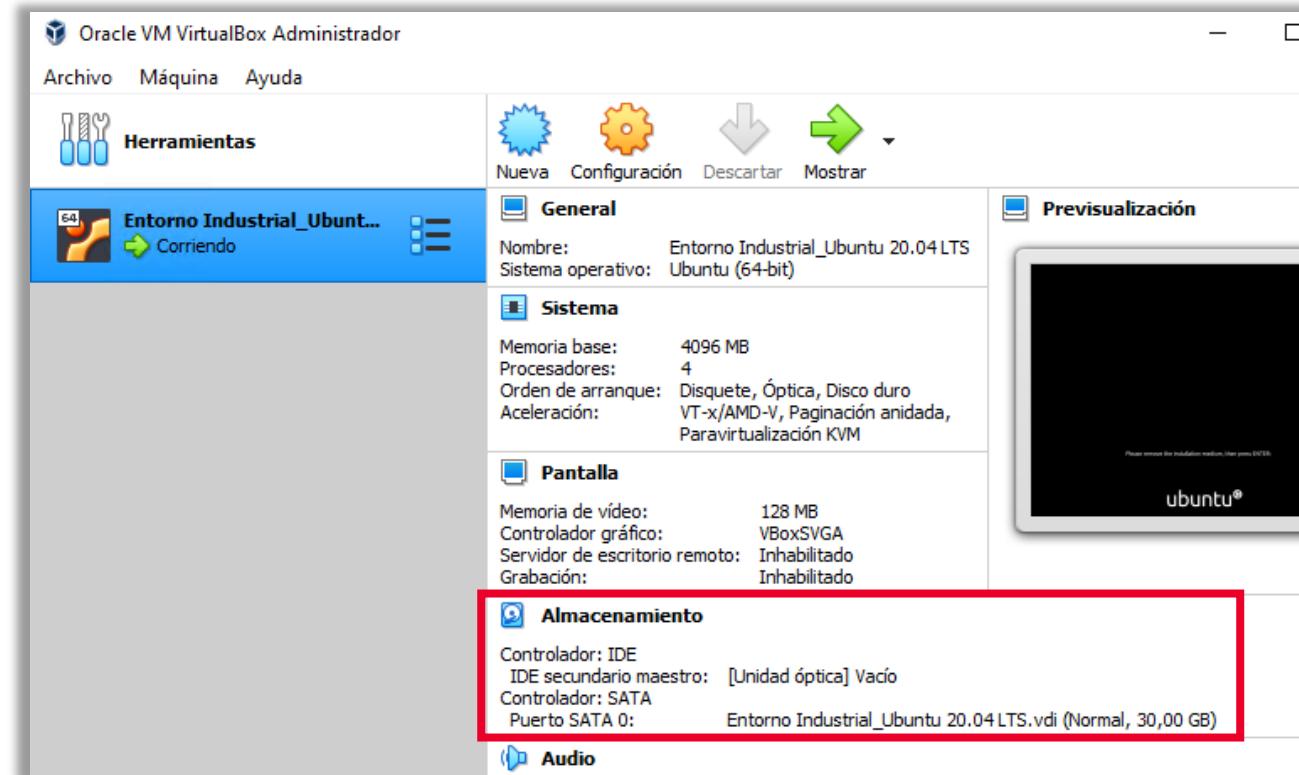


Ilustración 35: Ventana de Virtual Box en la que aparece que la unidad óptica está vacía.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Después de pulsar «enter», arranca de nuevo el sistema operativo recién instalado.

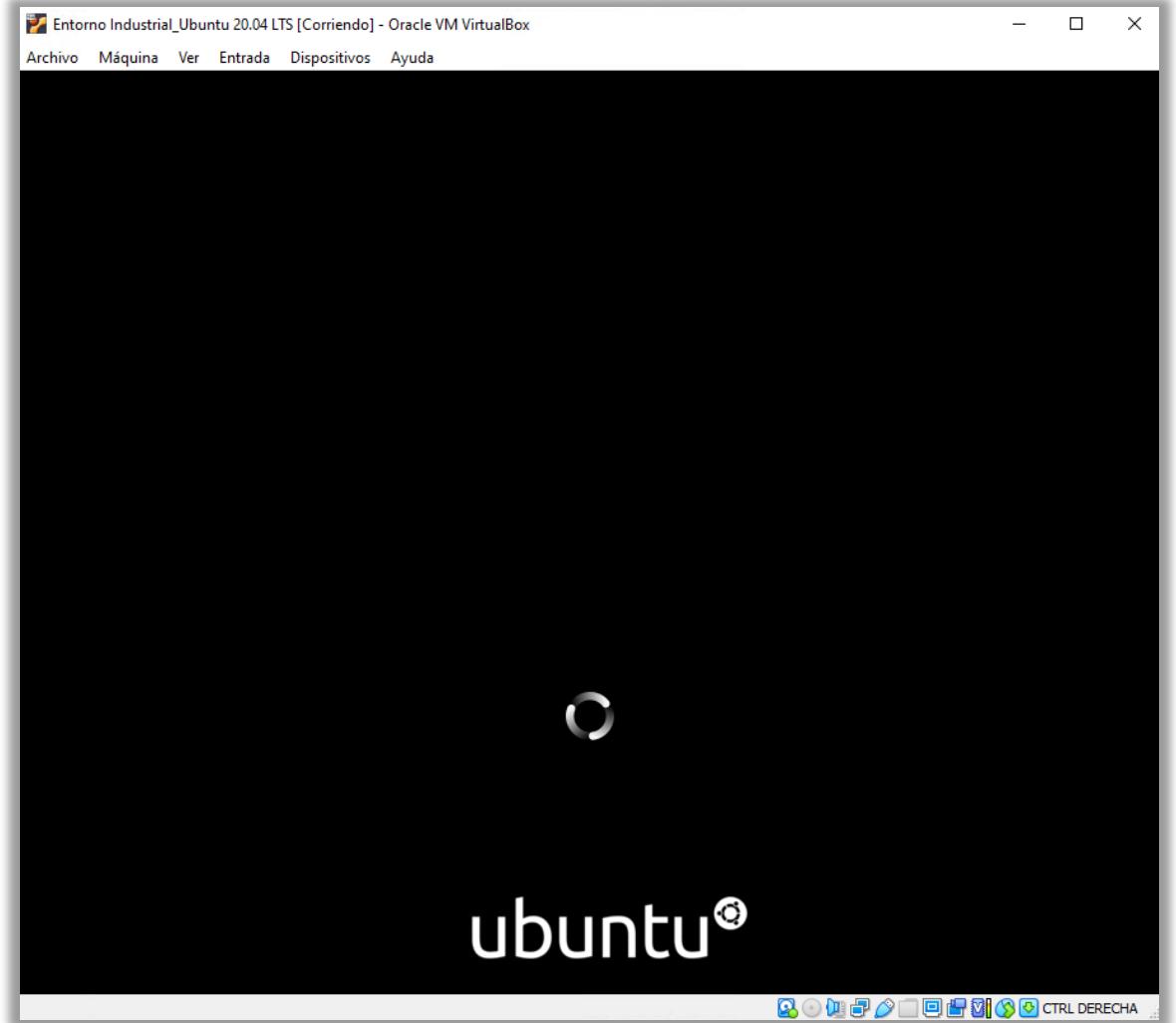


Ilustración 36: Al pulsar «enter» arranca el sistema operativo recién instalado.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Se mostrará la ventana de Ubuntu, y te pedirá configurar cuentas en línea. Haz clic en «Omitir».

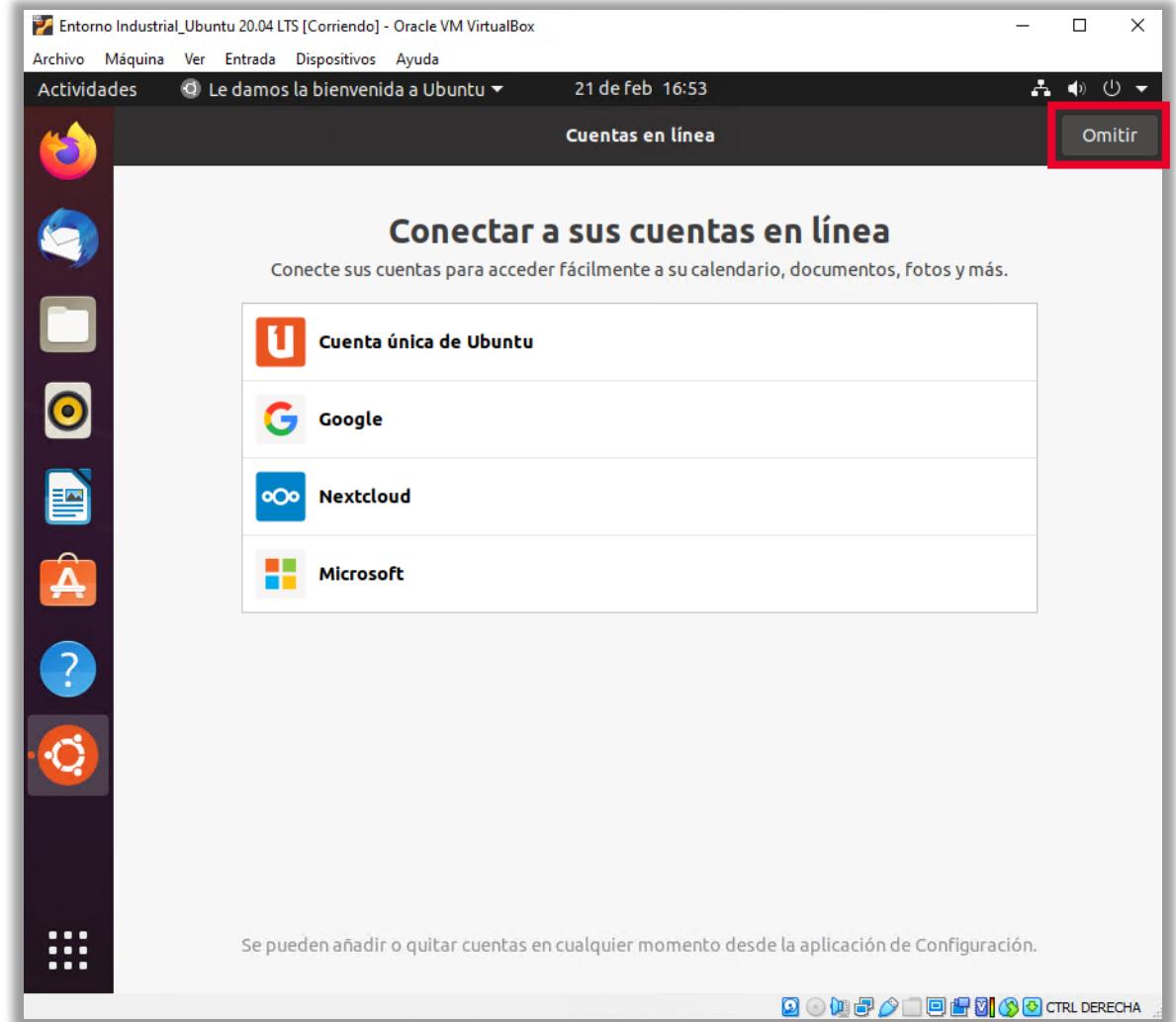


Ilustración 37: Ventana de Ubuntu para configurar cuentas en línea. Se pulsa en el botón «Omitir».

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Pulsa en siguiente, ya que no vas a utilizar Livepatch.



Ilustración 38: Ventana donde se pulsa siguiente al no querer utilizar «Livepatch».

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Selecciona la opción «No enviar información del sistema» y pulsa en el botón «Siguiente».

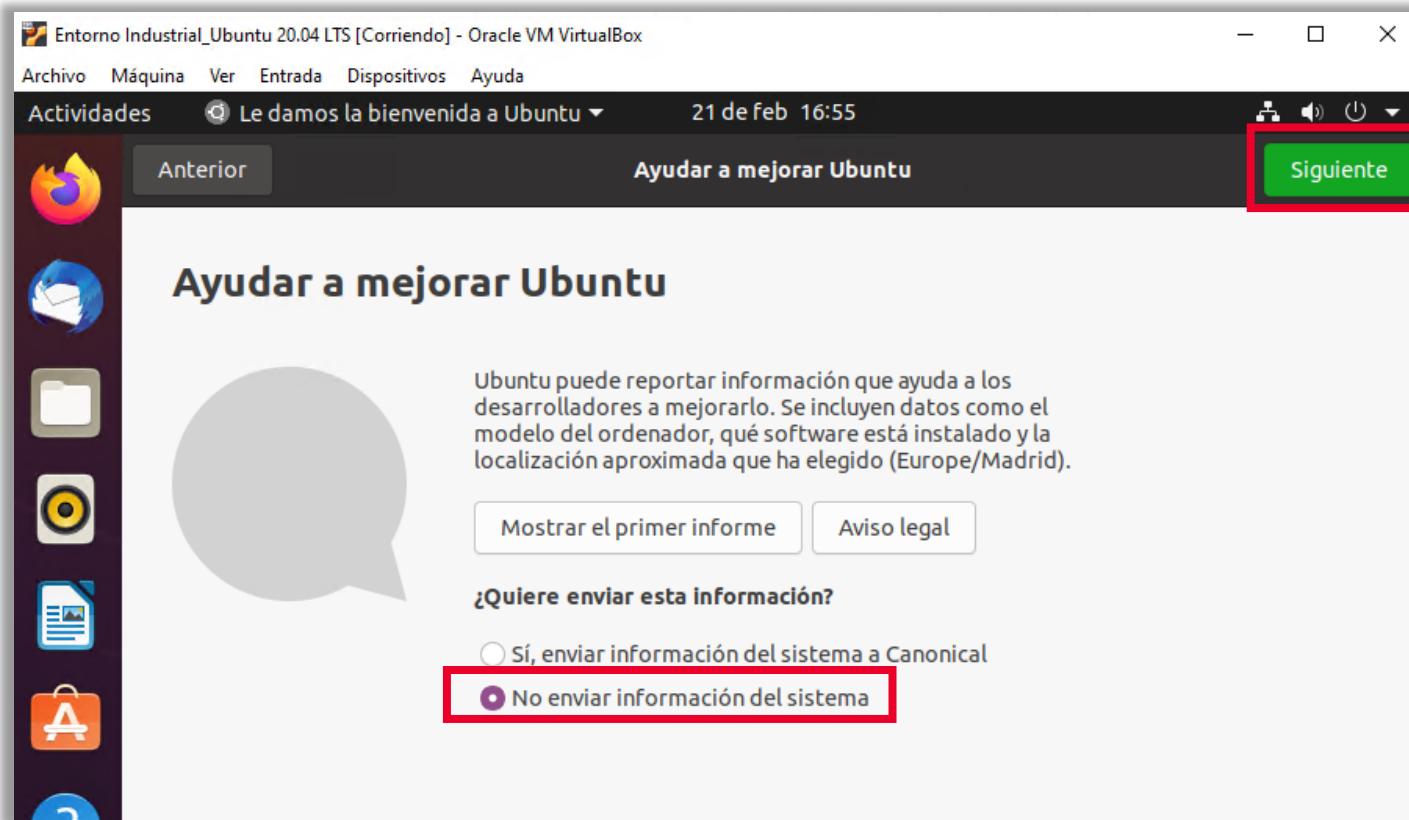


Ilustración 39: Ventana de selección de la opción «No enviar información del sistema» y se pulsa en el botón «Siguiente».

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Asegúrate de que el botón «Servicios de Ubicación» está desactivado y pulsa en el botón «Siguiente».



Ilustración 40: Desactivación de los servicios de ubicación.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Te pide actualizar el sistema. Pulsa el botón «Recordármelo más tarde».

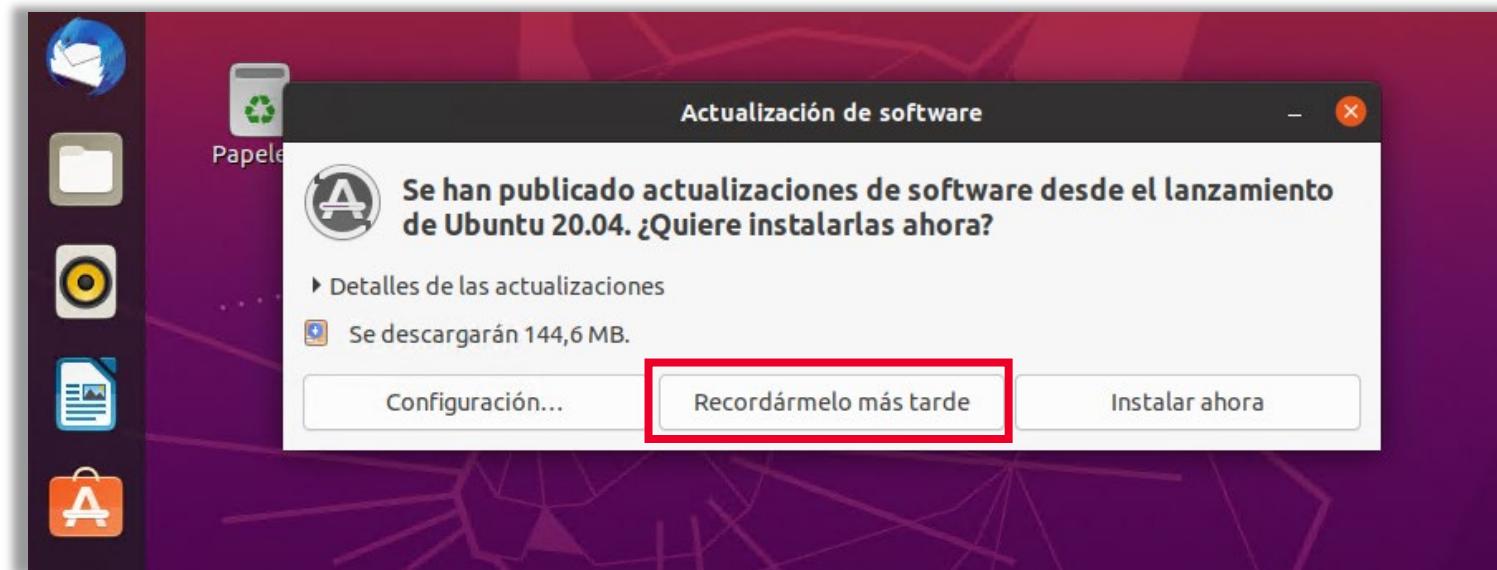


Ilustración 41: Aviso de actualización del sistema.
Se pulsa en el botón «Recordármelo más tarde».

3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Vas a tomar una instantánea del sistema operativo recién instalado, por si surgiera algún problema con la instalación de algunos paquetes de software.
 - En el menú «Máquina» selecciona «Tomar instantánea».

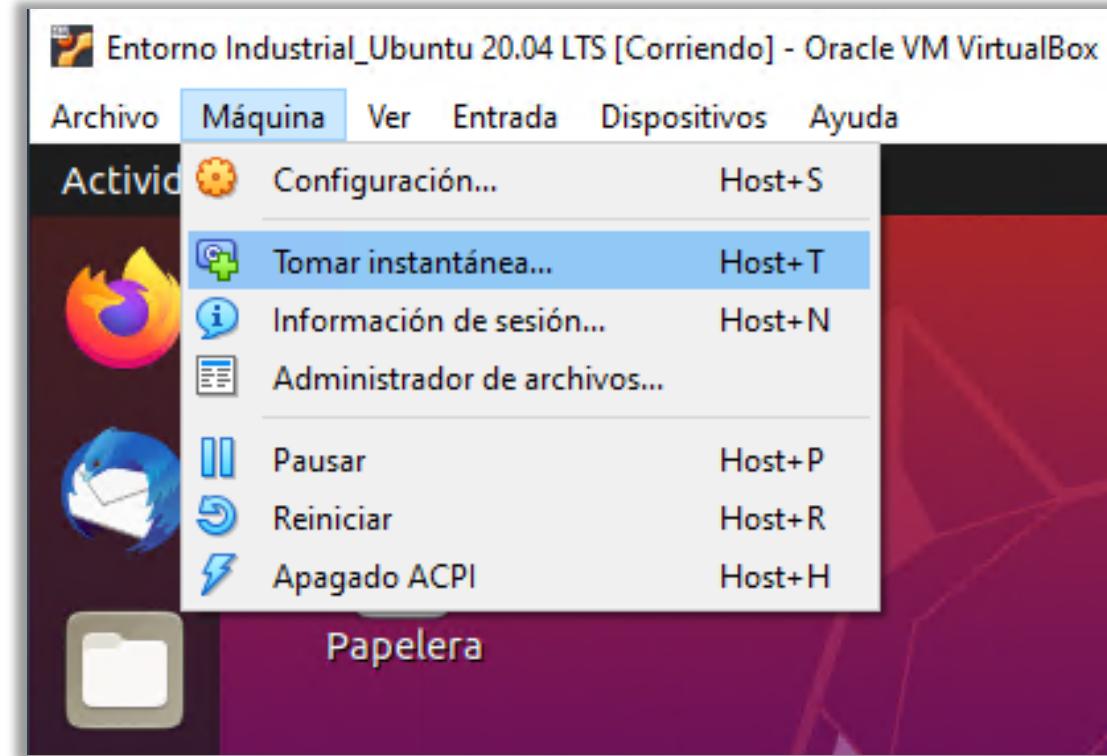


Ilustración 42: Recomendación de tomar una instantánea del sistema operativo en el submenú «Tomar instantánea» de la pestaña «Máquina» por si surgieran problemas más adelante.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Elige un nombre descriptivo y una descripción de la instantánea que estas tomando.

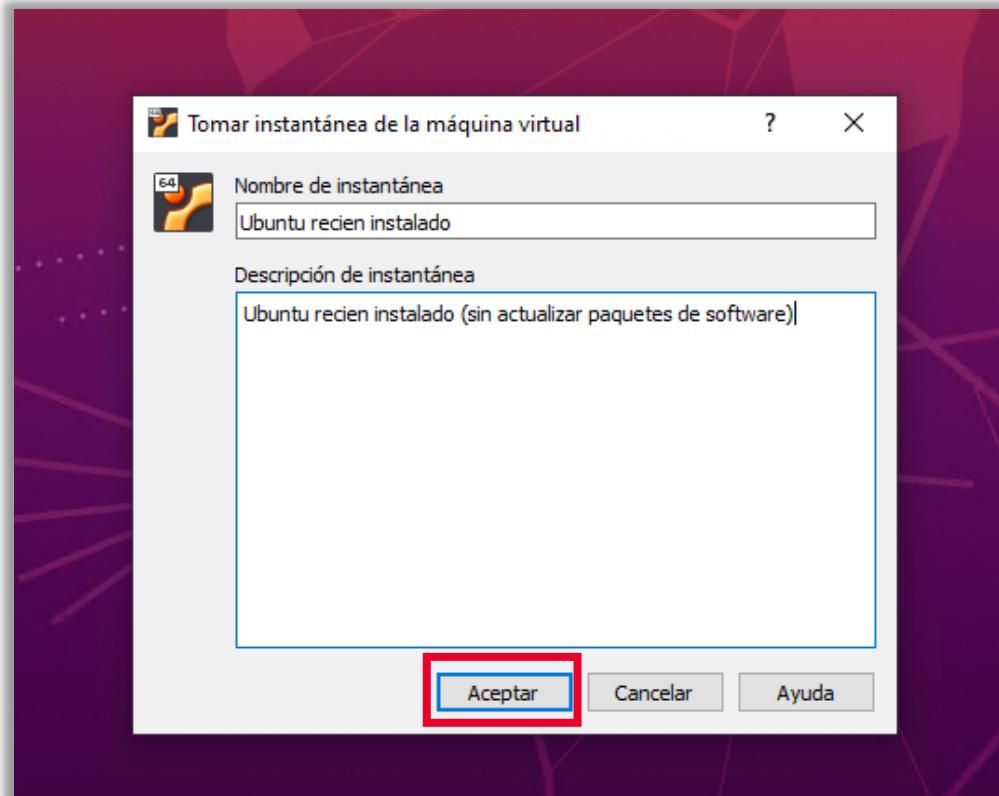


Ilustración 43: Ventana con opción de introducir nombre y descripción de la instantánea tomada.

3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Para actualizar los paquetes de *software* de Ubuntu, en la pestaña inferior selecciona «Todas» y haz clic en el ícono que aparece seleccionado en la imagen.

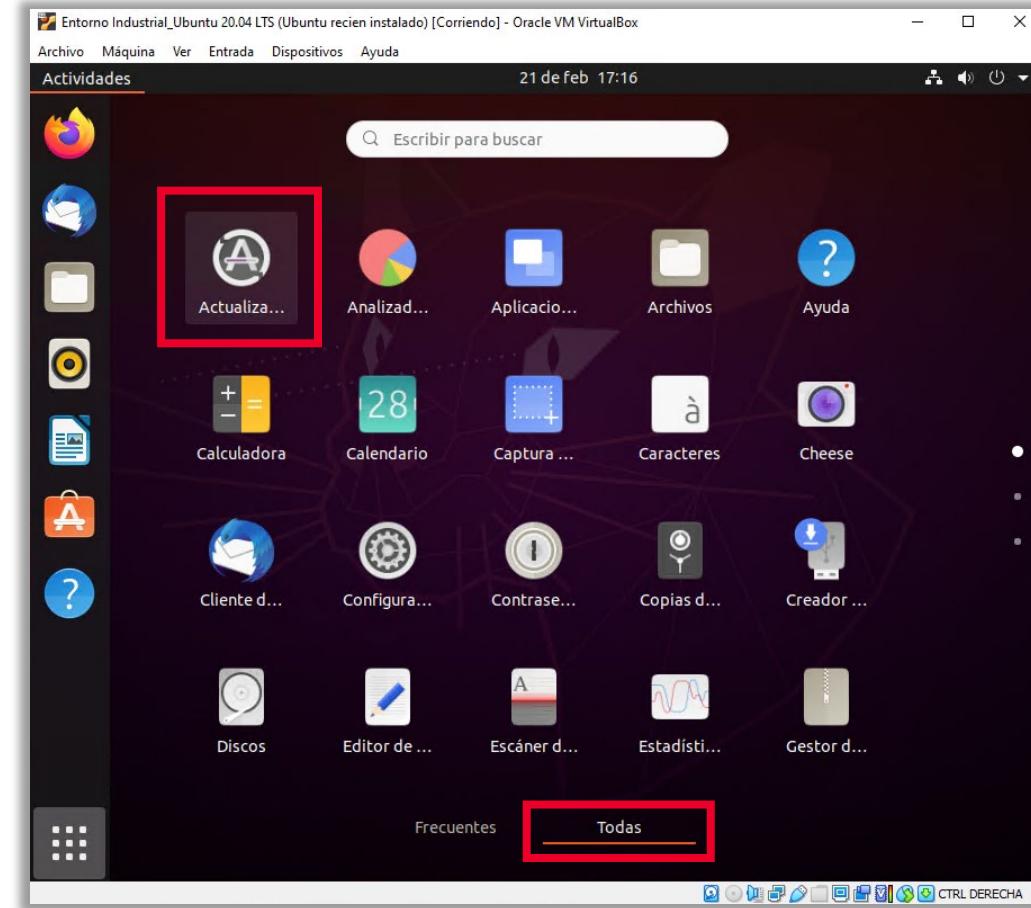


Ilustración 44: Ventana de actualización de paquetes de *software* de Ubuntu.

3 INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Pulsa «Instalar ahora» (tendrás que introducir la contraseña de usuario que estableciste en el proceso de instalación, ya que es necesaria para instalar cualquier tipo de paquetes de software en el sistema operativo).

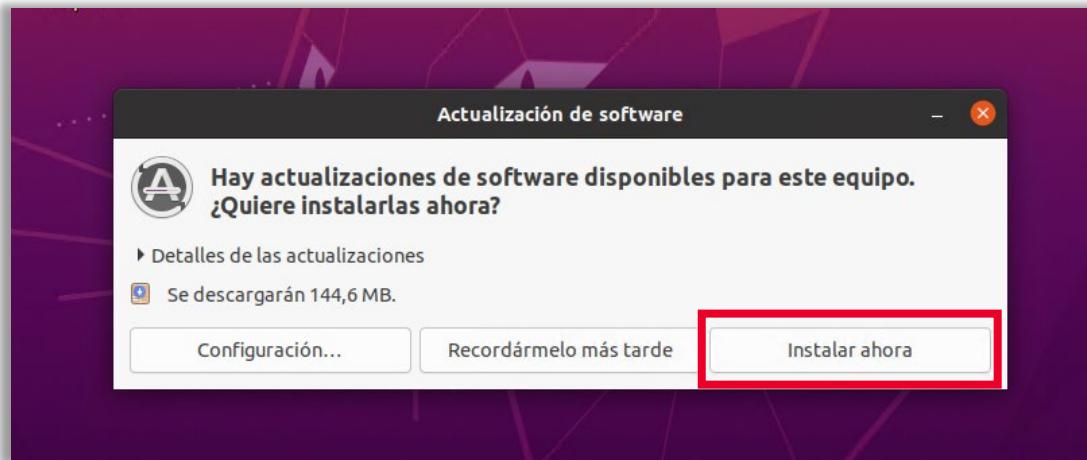


Ilustración 45: Ventana donde pregunta si se quieren instalar las actualizaciones ahora.

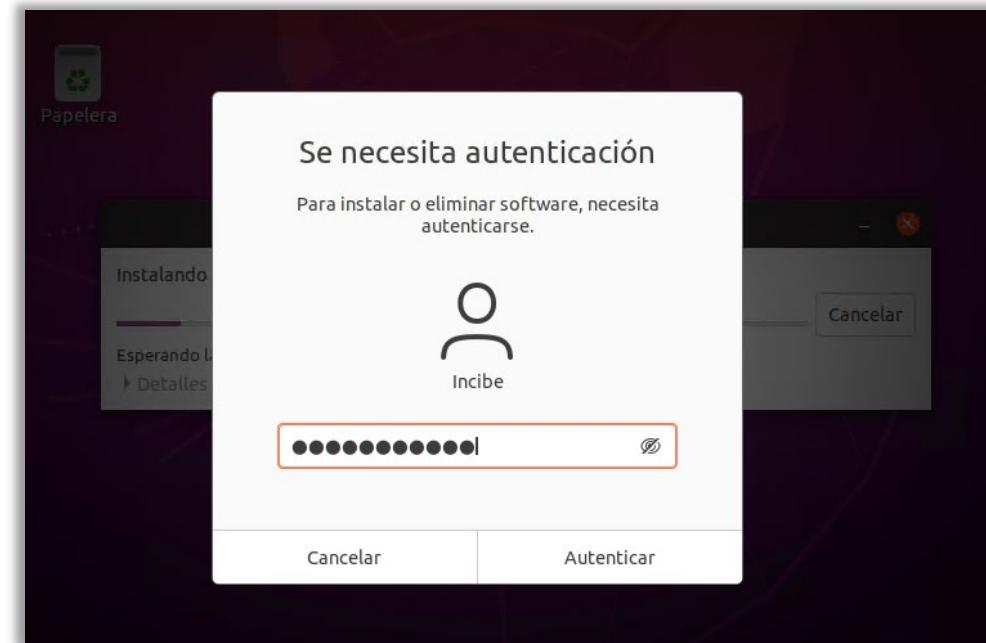


Ilustración 46: Ventana para introducir los datos de acceso (usuario y contraseña).

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- El proceso de instalación puede tardar un tiempo.

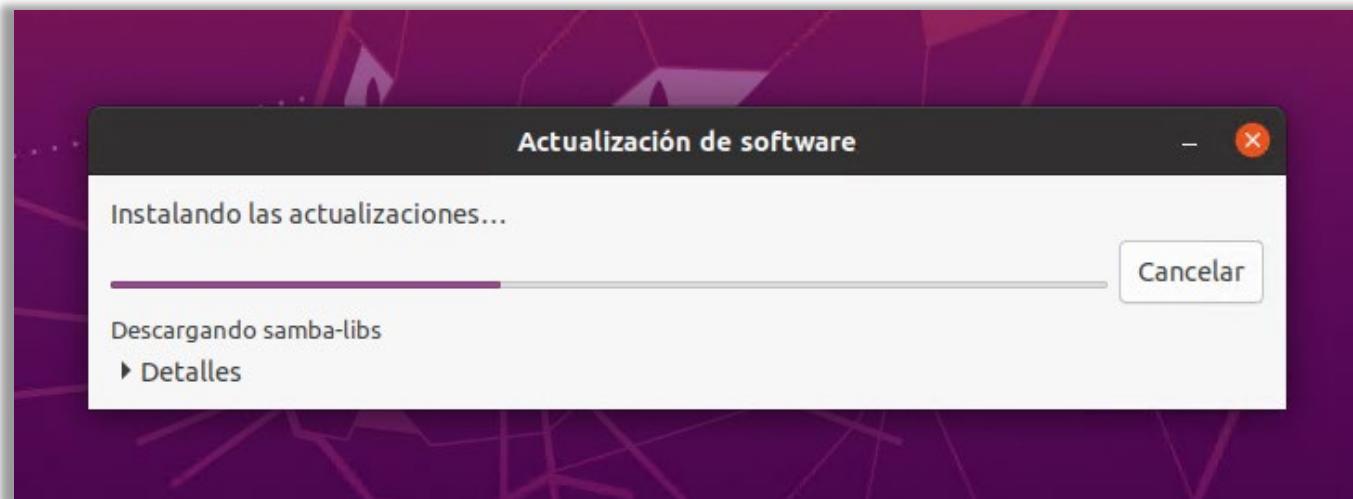


Ilustración 47: Ventana del progreso de la instalación.

3

INSTALACIÓN Y CONFIGURACIÓN DE MV UBUNTU DESKTOP

- Reinicia la máquina virtual.

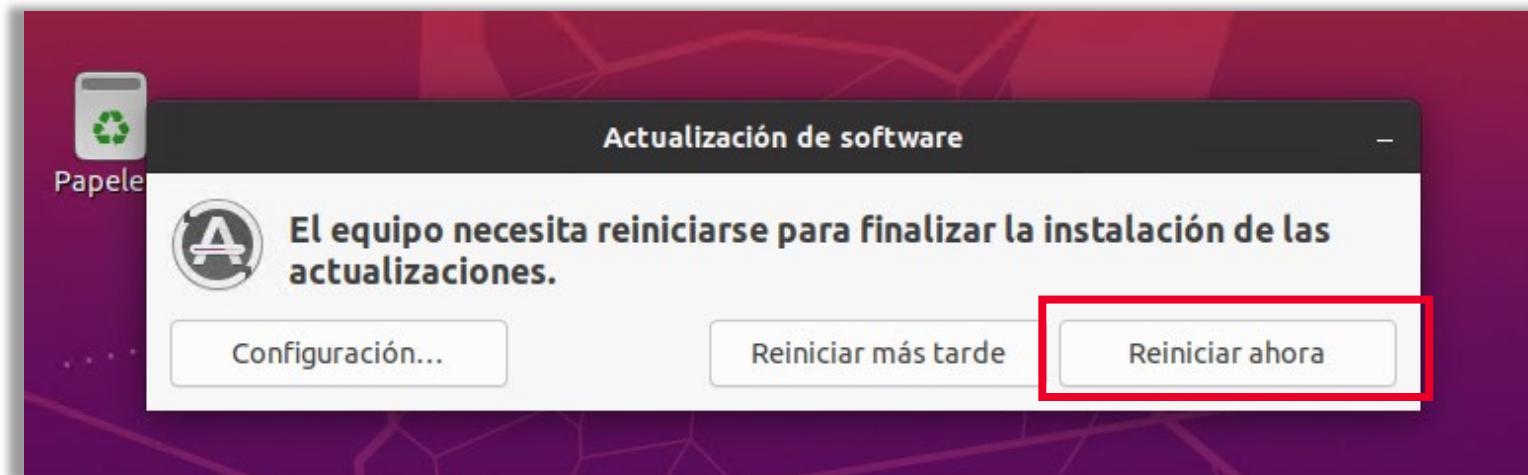
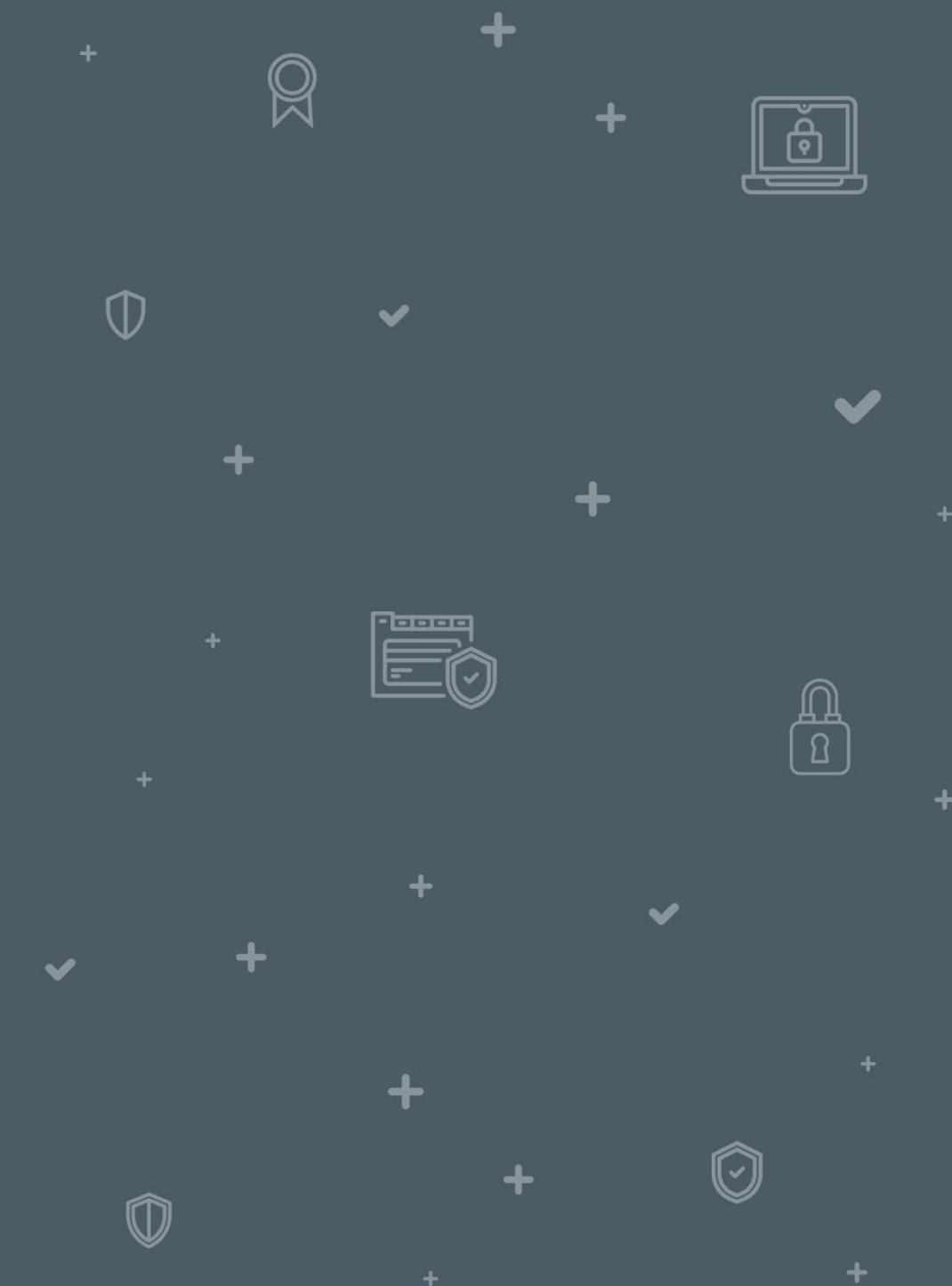


Ilustración 48: Aviso de reinicio de la máquina virtual.

AJUSTES DE CONFIGURACIÓN

4



4

AJUSTES DE CONFIGURACIÓN

- Desde Ubuntu, haz clic en la entrada «Actividades» que se encuentra en el menú superior izquierdo y escribe «Terminal». En el ícono que aparece haz un clic para abrir la aplicación.

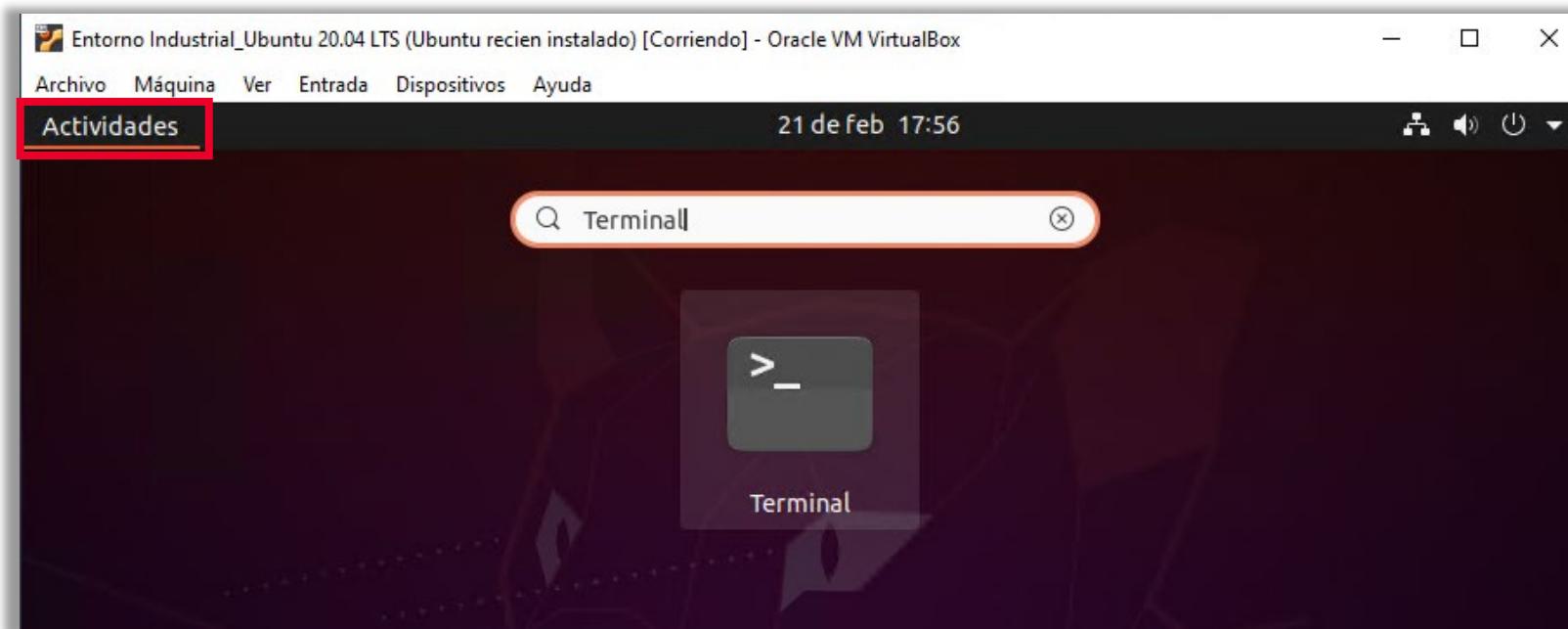
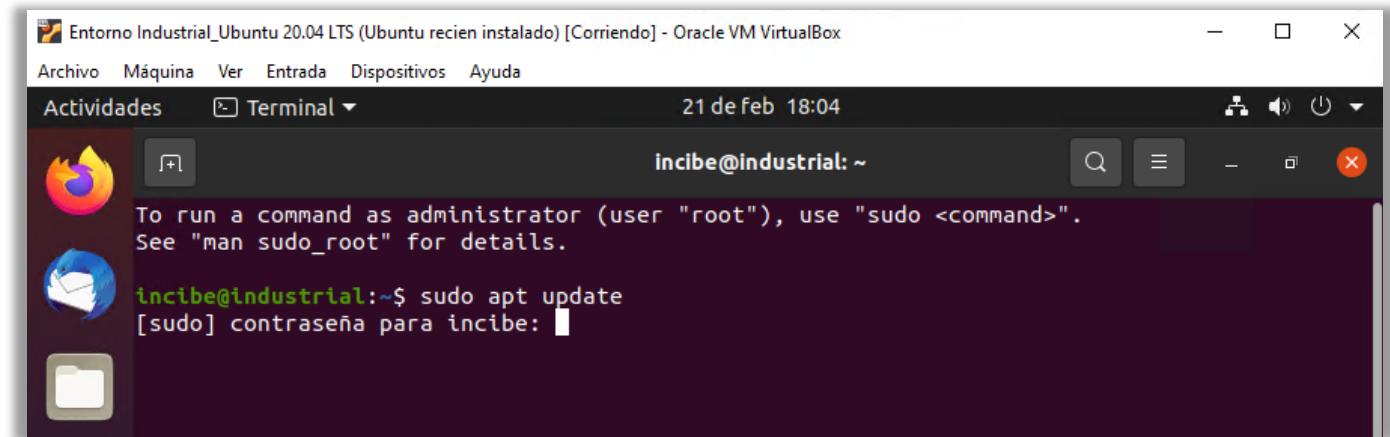


Ilustración 49: Acceso a «Terminal» para realizar los ajustes y configuraciones de la máquina virtual.

4 AJUSTES DE CONFIGURACIÓN

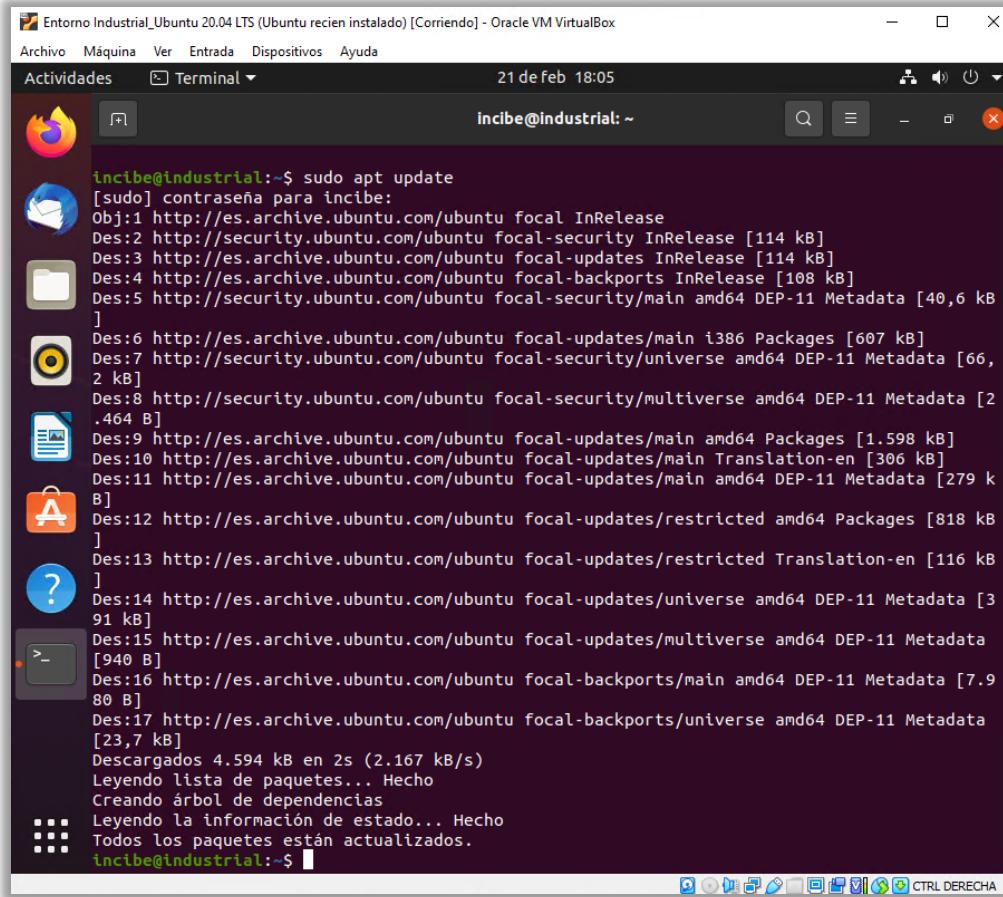
- Ejecuta los comandos que te permiten la actualización de los paquetes de *software* del repositorio:
 - **sudo apt update**
- Y la instalación de los paquetes de *software* que haya disponibles:
 - **sudo apt upgrade**
- Como utilizas el comando **sudo**, tendrás que escribir tu contraseña, ya que estos comandos se deben ejecutar con permisos de súper usuario.



The screenshot shows a terminal window titled "Entorno Industrial_Ubuntu 20.04 LTS (Ubuntu recien instalado) [Corriendo] - Oracle VM VirtualBox". The terminal window has a dark theme. At the top, there is a menu bar with options: Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda. Below the menu is a toolbar with icons for Actividades, Terminal, and a date and time indicator: 21 de feb 18:04. The main area of the terminal shows the command being run: "incibe@industrial:~\$ sudo apt update". A message from the system follows: "To run a command as administrator (user \"root\"), use \"sudo <command>\". See \"man sudo_root\" for details." Below this, it says "[sudo] contraseña para incibe: [REDACTED]" where the password field is redacted.

Ilustración 50: Ejecución del comando «**sudo apt update**» para la actualización del *software* del repositorio.

4 AJUSTES DE CONFIGURACIÓN



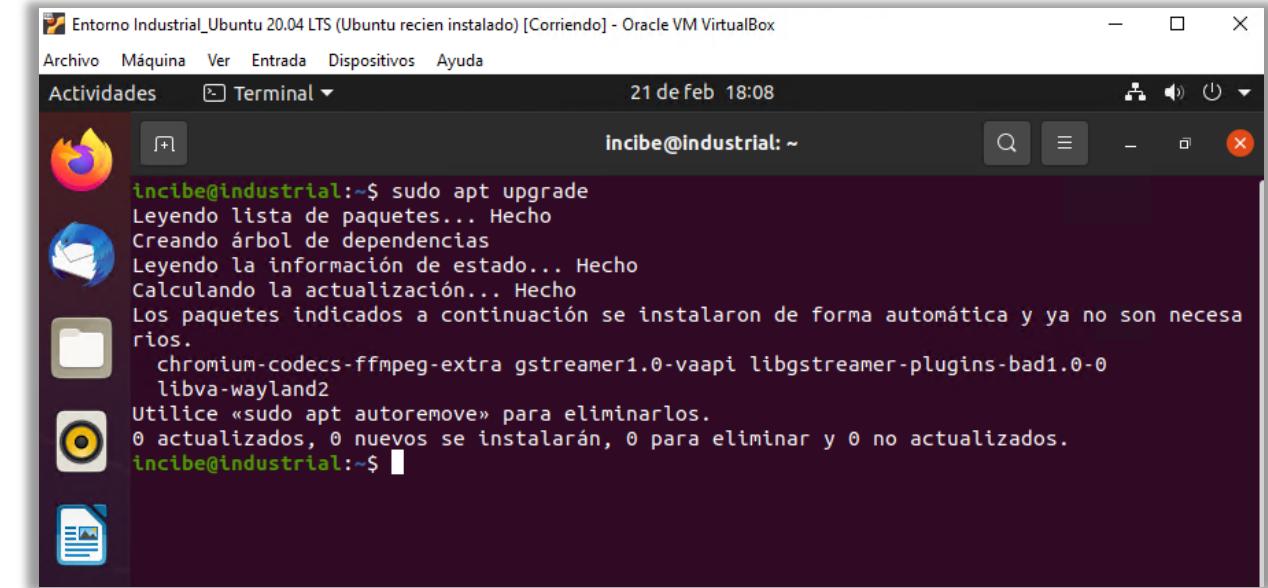
Entorno Industrial_Ubuntu 20.04 LTS (Ubuntu recien instalado) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 21 de feb 18:05 incibe@industrial: ~

```
incibe@industrial:~$ sudo apt update
[sudo] contraseña para incibe:
Obj:1 http://es.archive.ubuntu.com/ubuntu focal InRelease
Des:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Des:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [40,6 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [607 kB]
Des:7 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [66,2 kB]
Des:8 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2,464 kB]
Des:9 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,598 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [306 kB]
Des:11 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [279 kB]
Des:12 http://es.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [818 kB]
Des:13 http://es.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [116 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [3,91 kB]
Des:15 http://es.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [940 kB]
Des:16 http://es.archive.ubuntu.com/ubuntu focal-backports/main amd64 DEP-11 Metadata [7,980 kB]
Des:17 http://es.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [23,7 kB]
Descargados 4,594 kB en 2s (2,167 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Todos los paquetes están actualizados.
incibe@industrial:~$
```

Ilustración 51: Ventana con la relación de paquetes de actualización disponibles.



Entorno Industrial_Ubuntu 20.04 LTS (Ubuntu recien instalado) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 21 de feb 18:08 incibe@industrial: ~

```
incibe@industrial:~$ sudo apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0
libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
incibe@industrial:~$
```

Ilustración 52: Ejecución del comando «`sudo apt upgrade`» para la instalación de los paquetes de software disponibles.

4 AJUSTES DE CONFIGURACIÓN

- Una vez tienes los repositorios actualizados, instala el paquete *net-tools* para poder utilizar el comando **ifconfig** que va a devolver toda la información de la interfaz de red que estés utilizando, como la dirección IP.
 - **sudo apt install net-tools**

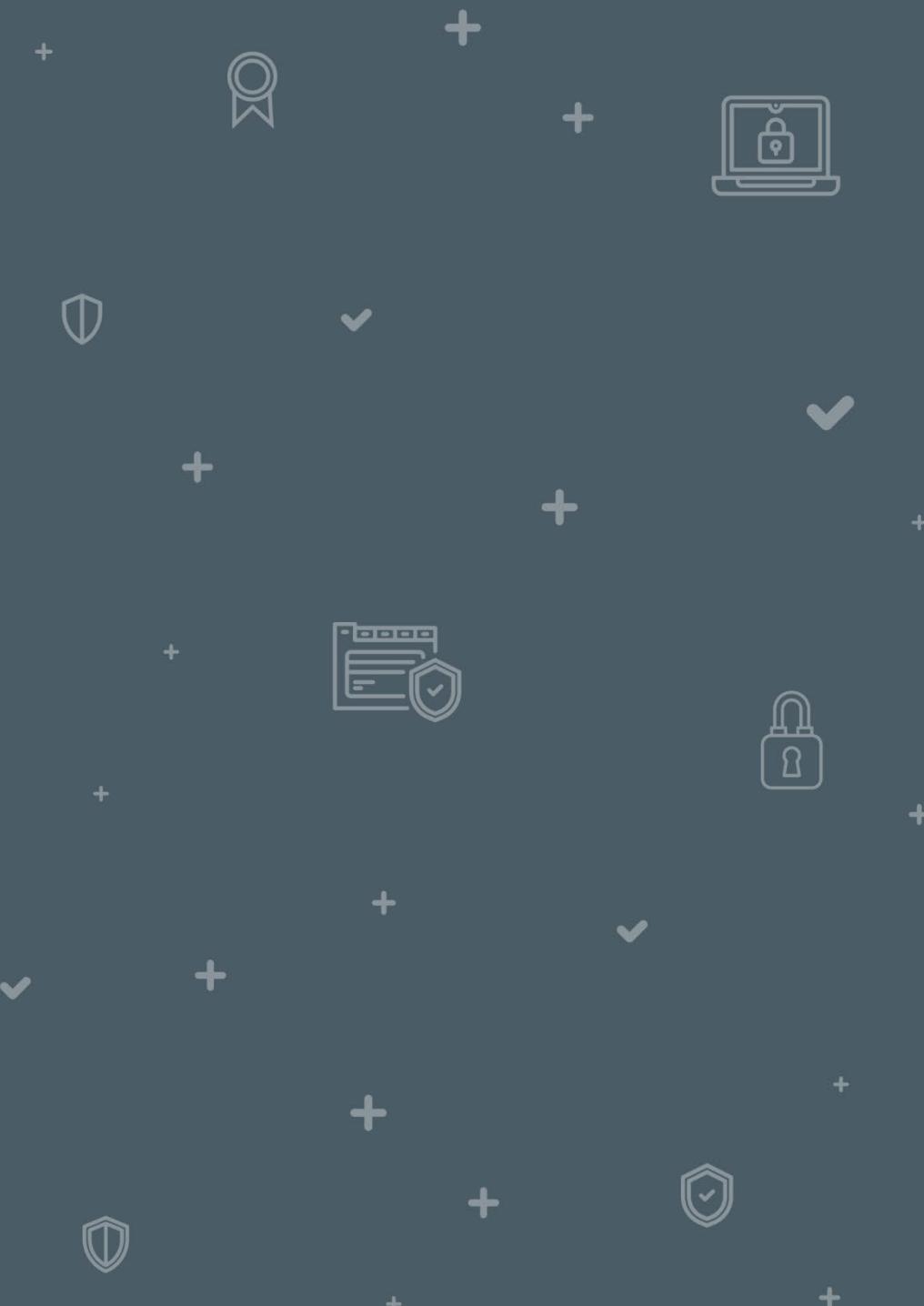
```
Entorno Industrial_Ubuntu 20.04 LTS (Ubuntu recien instalado) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 21 de feb 18:11
incibe@industrial: ~
incibe@industrial:~$ sudo apt install net-tools
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0
libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
net-tools
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 196 kB de archivos.
Se utilizarán 864 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.6.aebd88e-1ubuntu1 [196 kB]
Descargados 196 kB en 0s (441 kB/s)
Seleccionando el paquete net-tools previamente no seleccionado.
(Leyendo la base de datos ... 186246 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
.
Desempaquetando net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Configurando net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Procesando disparadores para man-db (2.9.1-1) ...
Progreso: [ 80%] [#####
CTRL DERECHA ..]
```

Ilustración 53: Instalación del paquete «*sudo apt install net-tools*».

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- 5.1 Instalación herramientas de simulación de dispositivos Siemens

5





INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

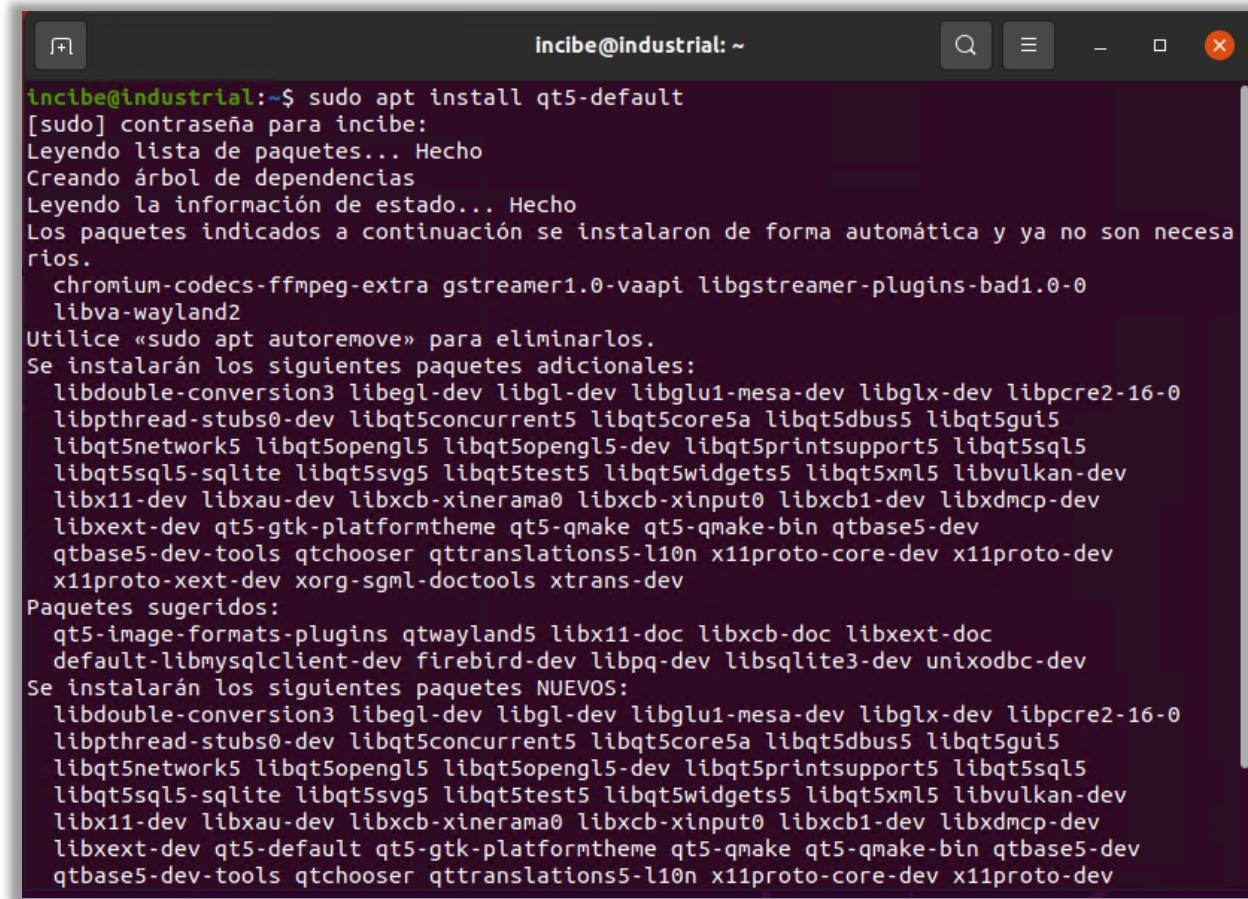
Ahora, instalarás un grupo de herramientas que te permitirán simular las comunicaciones que se generan en dispositivos que utilizan el protocolo Modbus, en concreto Modbus TCP. Estos dispositivos simularán un Maestro Modbus, que es el que realiza la petición y la consulta de la información que almacena el Esclavo Modbus, y un Esclavo Modbus que es el que recibe las peticiones y envía la información al Maestro Modbus, como haría un PLC Industrial.

- Deberás ejecutar en la terminal los siguientes comandos que instalan 2 paquetes de *software*, que forman parte del *framework* multiplataforma para desarrollar aplicaciones gráficas Qt. Estos paquetes son necesarios para poder ejecutar la aplicación QModMaster ya que se basa en el *framework* Qt.

5 INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Instala el paquete de software «qt5-default»:
 - sudo apt install qt5-default**

Ilustración 54: instalación del software «qt5-default» mediante el comando `sudo apt install qt5-default`.



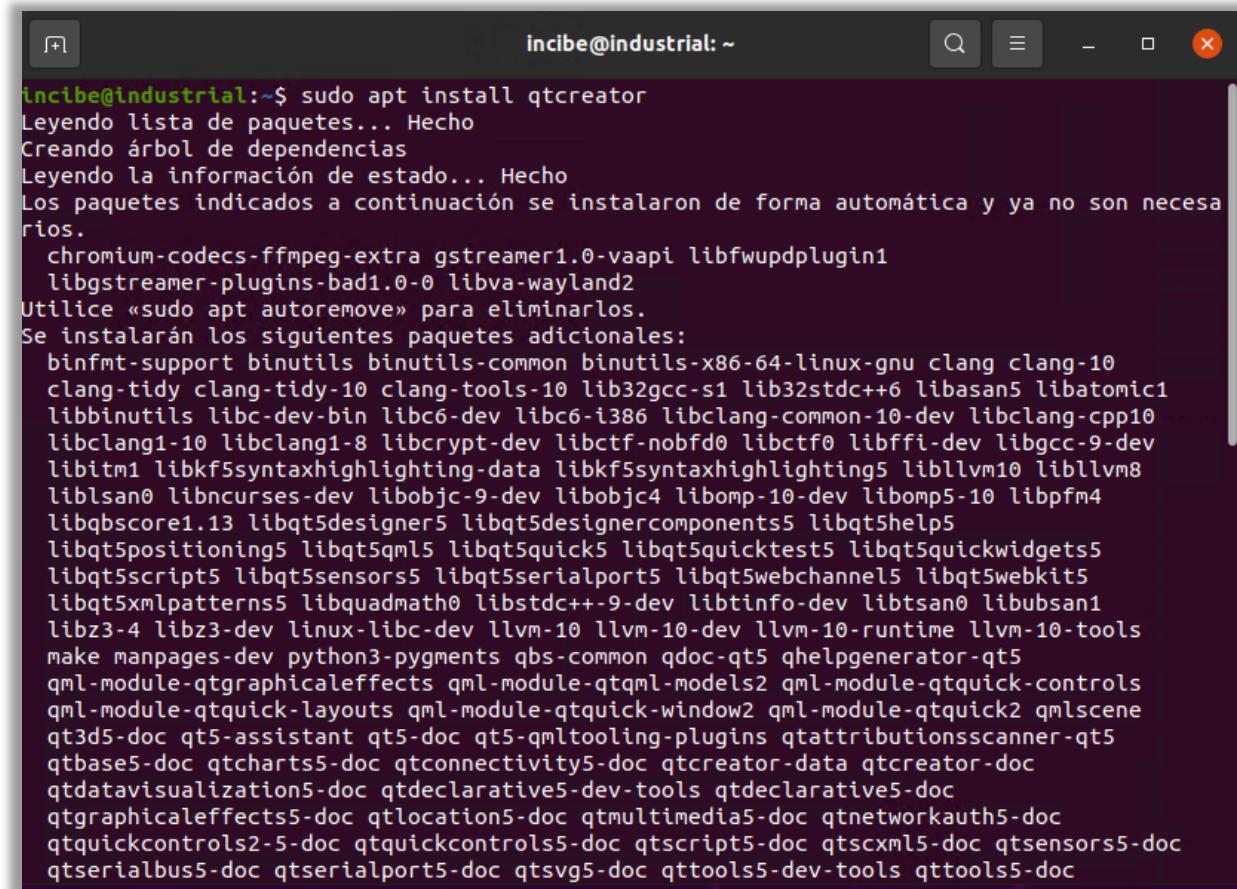
```
incibe@industrial:~$ sudo apt install qt5-default
[sudo] contraseña para incibe:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0
  libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libdouble-conversion3 libegl-dev libgl-dev libglu1-mesa-dev libglx-dev libpcre2-16-0
  libpthread-stubs0-dev libqt5concurrent5 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5network5 libqt5opengl5 libqt5opengl5-dev libqt5printsupport5 libqt5sql5
  libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5widgets5 libqt5xml5 libvulkan-dev
  libx11-dev libxau-dev libxcb-xinerama0 libxcb-xinput0 libxcb1-dev libxdmcp-dev
  libxext-dev qt5-gtk-platformtheme qt5-qmake qt5-qmake-bin qtbase5-dev
  qtbase5-dev-tools qtchooser qttranslations5-l10n x11proto-core-dev x11proto-dev
  x11proto-xext-dev xorg-sgml-doctools xtrans-dev
Paquetes sugeridos:
  qt5-image-formats-plugins qtwayland5 libxcb-doc libxext-doc
  default-libmysqlclient-dev firebird-dev libpq-dev libsqli3-dev unixodbc-dev
Se instalarán los siguientes paquetes NUEVOS:
  libdouble-conversion3 libegl-dev libgl-dev libglu1-mesa-dev libglx-dev libpcre2-16-0
  libpthread-stubs0-dev libqt5concurrent5 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5network5 libqt5opengl5 libqt5opengl5-dev libqt5printsupport5 libqt5sql5
  libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5widgets5 libqt5xml5 libvulkan-dev
  libx11-dev libxau-dev libxcb-xinerama0 libxcb-xinput0 libxcb1-dev libxdmcp-dev
  libxext-dev qt5-default qt5-gtk-platformtheme qt5-qmake qt5-qmake-bin qtbase5-dev
  qtbase5-dev-tools qtchooser qttranslations5-l10n x11proto-core-dev x11proto-dev
```

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Ahora instala el paquete de software «qtcreator»:
 - **sudo apt install qtcreator**

Ilustración 55: Instalación del paquete de software «qtcreator» mediante el comando comando `sudo apt install qtcreator`.

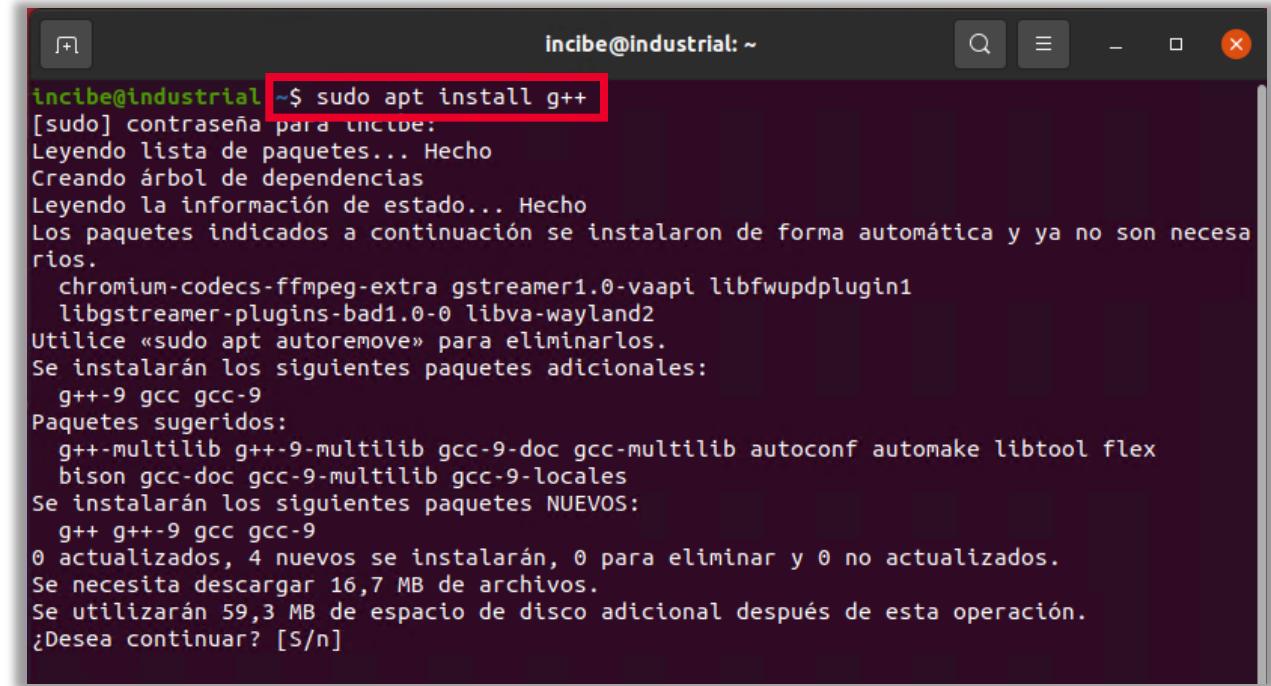


```
incibe@industrial:~$ sudo apt install qtcreator
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
binfmt-support binutils binutils-common binutils-x86-64-linux-gnu clang clang-10
clang-tidy clang-tidy-10 clang-tools-10 lib32gcc-s1 lib32stdc++6 libasan5 libatomic1
libbinutils libc-dev-bin libc6-dev libc6-i386 libclang-common-10-dev libclang-cpp10
libclang1-10 libclang1-8 libcrypt-dev libctf-nobfd0 libctf0 libffi-dev libgcc-9-dev
libitm1 libkf5syntaxhighlighting-data libkf5syntaxhighlighting5 libllvm10 libllvm8
liblsan0 libncurses-dev libobjc-9-dev libobjc4 libomp-10-dev libomp5-10 libpfm4
libqbscore1.13 libqt5designer5 libqt5designercomponents5 libqt5help5
libqt5positioning5 libqt5qml5 libqt5quick5 libqt5quicktest5 libqt5quickwidgets5
libqt5script5 libqt5sensors5 libqt5serialports5 libqt5webchannel5 libqt5webkit5
libqt5xmlpatterns5 libquadmath0 libstdc++-9-dev libtinfo-dev libtsan0 libubsan1
libz3-4 libz3-dev linux-libc-dev llvm-10 llvm-10-dev llvm-10-runtime llvm-10-tools
make manpages-dev python3-pygments qbs-common qdoc-qt5 qhelpgenerator-qt5
qml-module-qtgraphicaleffects qml-module-qtqml-models2 qml-module-qtquick-controls
qml-module-qtquick-layouts qml-module-qtquick-window2 qml-module-qtquick2 qmlscene
qt3d5-doc qt5-assistant qt5-doc qt5-qmltooling-plugins qtattributionsscanner-qt5
qtbase5-doc qtcharts5-doc qtconnectivity5-doc qtcreator-data qtcreator-doc
qtdatavisualization5-doc qtdeclarative5-dev-tools qtdeclarative5-doc
qtgraphicaleffects5-doc qtlocation5-doc qtmultimedia5-doc qtnetworkauth5-doc
qtquickcontrols2-5-doc qtquickcontrols5-doc qtscript5-doc qtscxml5-doc qtsensors5-doc
qtserialbus5-doc qtserialport5-doc qtsvg5-doc qttools5-dev-tools qttools5-doc
```

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Por último, instala el paquete de software «g++» (compilador de C++ de GNU):
 - **sudo apt install g++**
 - Cuando pregunte confirmación escribir «s» y pulsar intro.



```
incibe@industrial:~$ sudo apt install g++
[sudo] contraseña para incibe:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  g++-9 gcc gcc-9
Paquetes sugeridos:
  g++-multilib g++-9-multilib gcc-9-doc gcc-multilib autoconf automake libtool flex
  bison gcc-doc gcc-9-multilib gcc-9-locales
Se instalarán los siguientes paquetes NUEVOS:
  g++ g++-9 gcc gcc-9
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 16,7 MB de archivos.
Se utilizarán 59,3 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Ilustración 56: Instalación del paquete de software «g++» mediante el comando `sudo apt install g++`.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Una vez instalados los paquetes necesarios para la aplicación [QModMaster](#) (que simula un dispositivo Maestro Modbus), accede a su página web para descargarlo, haciendo clic en el icono Firefox para abrir el navegador y acceder a su página web.

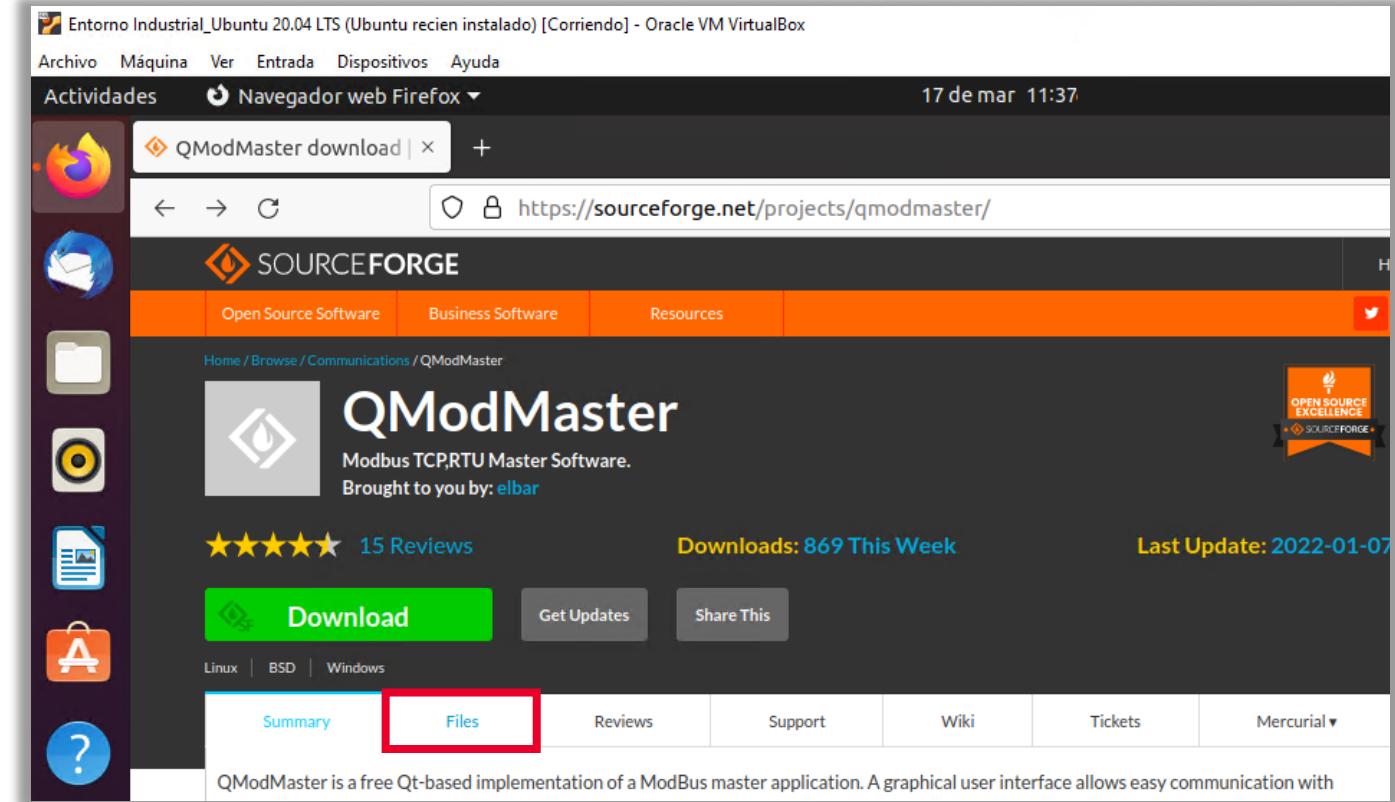


Ilustración 57: Página de descarga la aplicación QModMaster.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Haz clic en la pestaña «Files» y después haz clic en la entrada «**qModMaster-code-0.5.2-3.zip**» para descargar el archivo que corresponde a Linux.

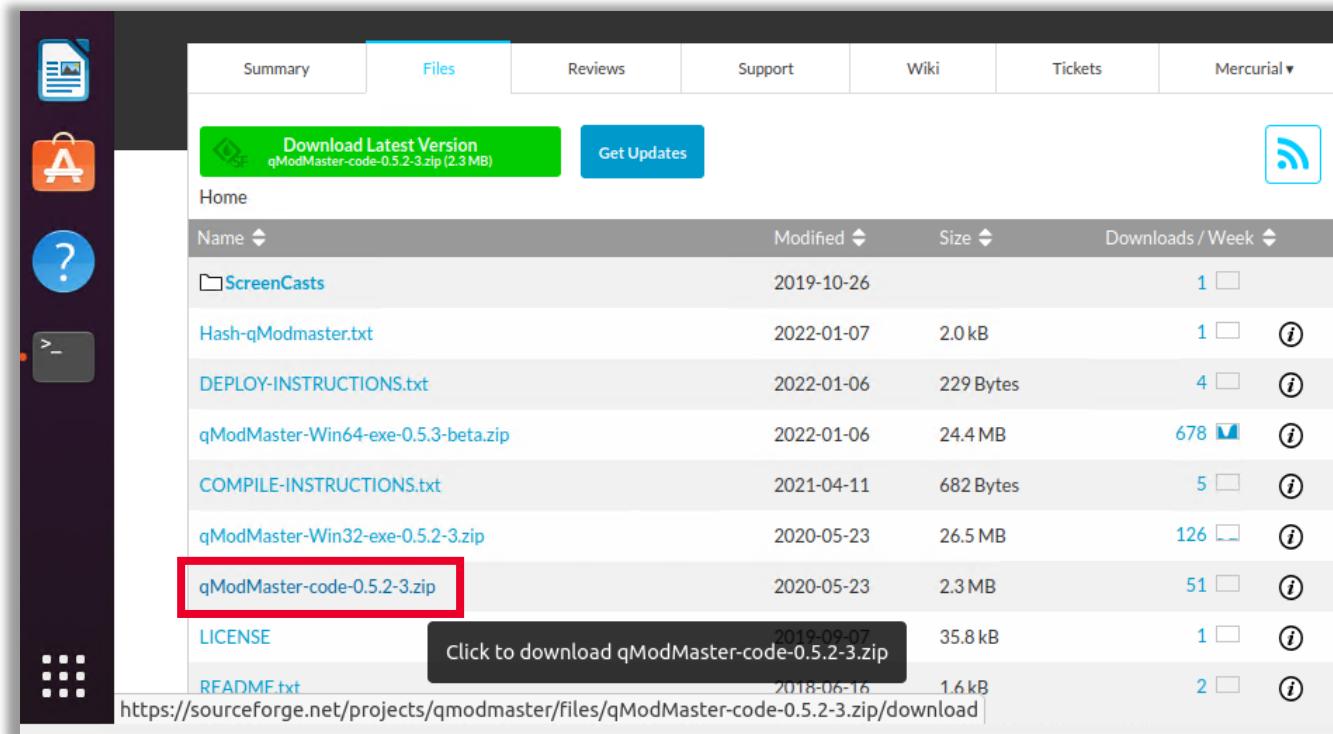


Ilustración 58: Acceso a la pestaña la pestaña «Files» y clic en la entrada «**qModMaster-code-0.5.2-3.zip**» para descargar el archivo.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

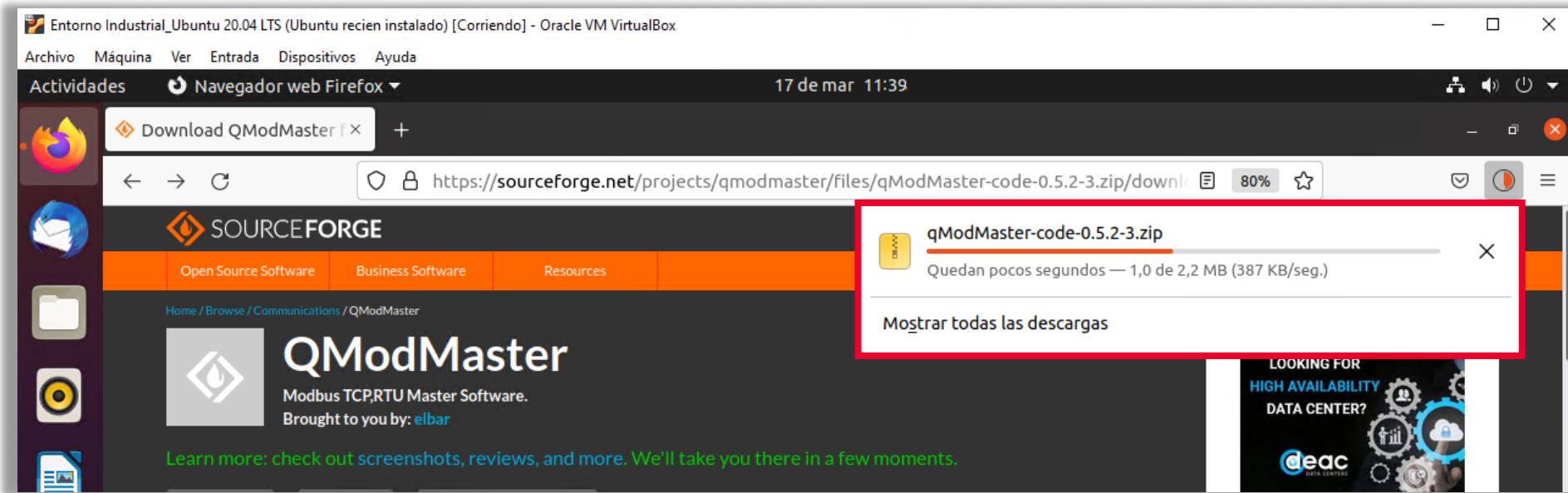


Ilustración 59: Imagen del progreso de la descarga del archivo «qModMaster-code-0.5.2-3.zip».



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Desde la terminal, (si es necesario, abre una nueva) copia el archivo descargado a la carpeta «Documentos» con el siguiente comando.

Para que el comando de copia funcione, debes asegurar que estás en la carpeta de usuario incibe. Si no estás en dicha carpeta, antes de ejecutar el comando de copia, ejecuta el comando **cd** para acceder directamente a la carpeta del usuario incibe:

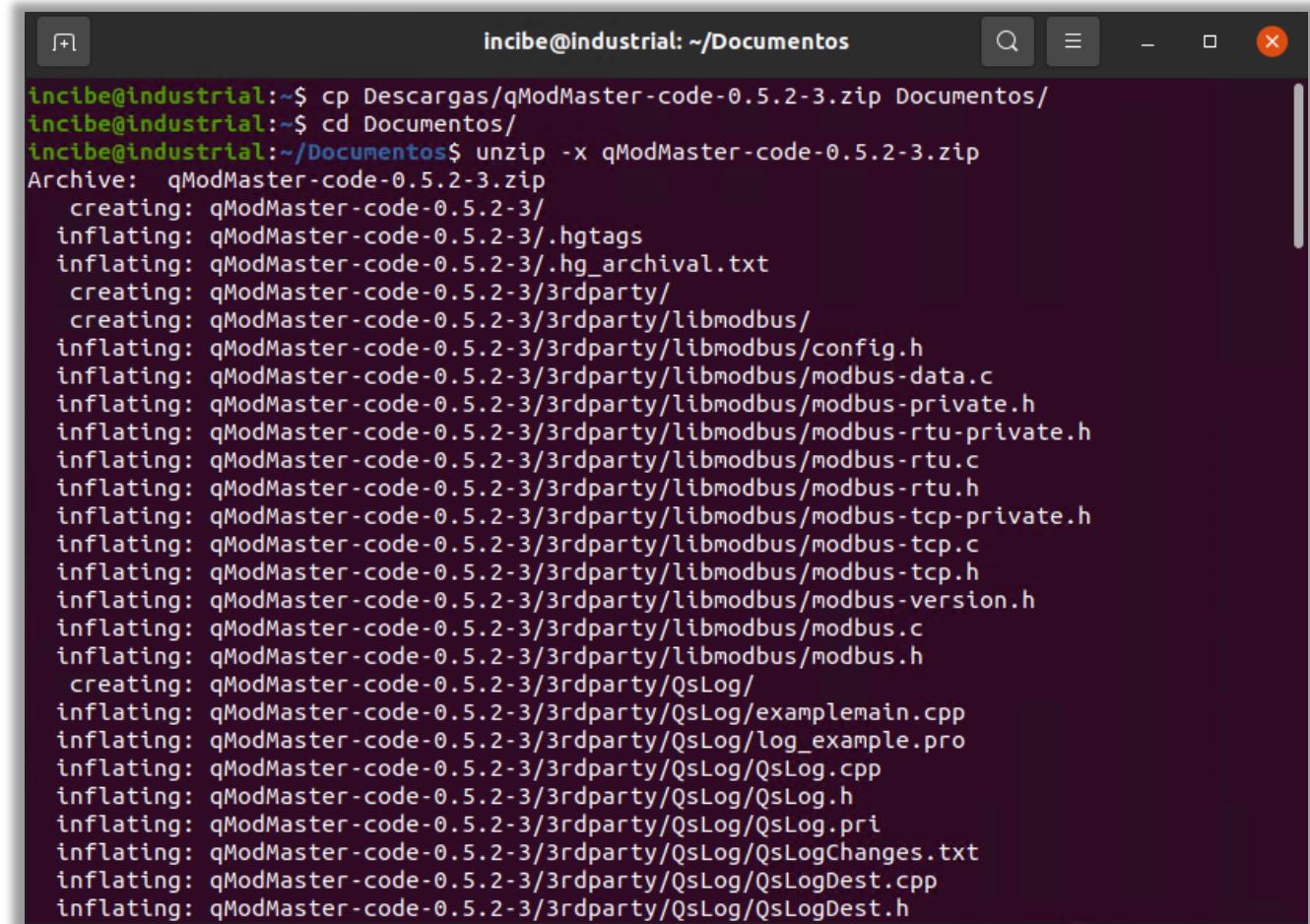
- **cp Descargas/qModMaster-code-0.5.2.3.zip Documentos/**

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Accede a la carpeta donde has copiado el archivo que has descargado y descomprime el archivo ZIP:
 - **cd Documentos/**
 - **unzip -x qModMaster-code-0.5.2-3.zip**

Ilustración 60: Ejecución desde el terminal del comando **cp Descargas/qModMaster-code-0.5.2.3.zip Documentos/**



A screenshot of a terminal window titled "incibe@industrial: ~/Documentos". The window shows the command "unzip -x qModMaster-code-0.5.2-3.zip" being run, followed by a detailed list of files being extracted from the archive. The output includes "creating:" for directory creation and "inflating:" for individual files like "hgtags", "hg_archival.txt", "3rdparty/", "libmodbus/", "config.h", "modbus-data.c", "modbus-private.h", "modbus-rtu-private.h", "modbus-rtu.c", "modbus-rtu.h", "modbus-tcp-private.h", "modbus-tcp.c", "modbus-tcp.h", "modbus-version.h", "modbus.modbus.c", "modbus.h", "QsLog/", "examplemain.cpp", "log_example.pro", "QsLog/QsLog.cpp", "QsLog/QsLog.h", "QsLog/QsLog.pri", "QsLog/QsLogChanges.txt", "QsLog/QsLogDest.cpp", and "QsLog/QsLogDest.h".

```
incibe@industrial:~/Documentos$ cp Descargas/qModMaster-code-0.5.2-3.zip Documentos/
incibe@industrial:~/Documentos$ cd Documentos/
incibe@industrial:~/Documentos$ unzip -x qModMaster-code-0.5.2-3.zip
Archive: qModMaster-code-0.5.2-3.zip
  creating: qModMaster-code-0.5.2-3/
  inflating: qModMaster-code-0.5.2-3/.hgtags
  inflating: qModMaster-code-0.5.2-3/.hg_archival.txt
  creating: qModMaster-code-0.5.2-3/3rdparty/
  creating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/config.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-data.c
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-private.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-rtu-private.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-rtu.c
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-rtu.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-tcp-private.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-tcp.c
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-tcp.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus-version.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus.modbus.c
  inflating: qModMaster-code-0.5.2-3/3rdparty/libmodbus/modbus.h
  creating: qModMaster-code-0.5.2-3/3rdparty/QsLog/
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/examplemain.cpp
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/log_example.pro
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/QsLog.cpp
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/QsLog.h
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/QsLog.pri
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/QsLogChanges.txt
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/QsLogDest.cpp
  inflating: qModMaster-code-0.5.2-3/3rdparty/QsLog/QsLogDest.h
```

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Una vez finalizada la descompresión del archivo ZIP, accede a la carpeta que ha generado la descompresión, y en ella crea una carpeta nueva de nombre «*build*», después accede a esta nueva carpeta:
 - cd qModMaster-code-0.5.2-3/
 - mkdir build
 - cd build/

```
inflating: qModMaster-code-0.5.2-3/translations/qModMaster_zh_TW.qm
inflating: qModMaster-code-0.5.2-3/translations/qModMaster_zh_TW.ts
inflating: qModMaster-code-0.5.2-3/translations/translations.qrc
incibe@industrial:~/Documentos$ cd qModMaster-code-0.5.2-3/
incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3$ mkdir build
incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3$ cd build/
incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3/build$
```

Ilustración 61: Creación de la carpeta «*build*» tras descomprimir el archivo.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Ejecuta los comandos de compilación del paquete de software QModMaster.
 - Con el primer comando, generas el archivo «Makefile» en la carpeta que te encuentras, «build», utilizando el comando **qmake** que pertenece al *framework* Qt.
 - Los archivos Makefile son utilizados por el programa make para construir programas ejecutables a partir del código fuente. Los makefiles que produce qmake se adaptan a la plataforma particular desde la que se ejecuta, basándose en los archivos de proyecto de qmake.
 - Los dos puntos «..» antes de /qModMaster.pro hacen referencia a que el archivo se va a generar en la carpeta superior a la ubicación actual.
 - **qmake ..//qModMaster.pro**

5

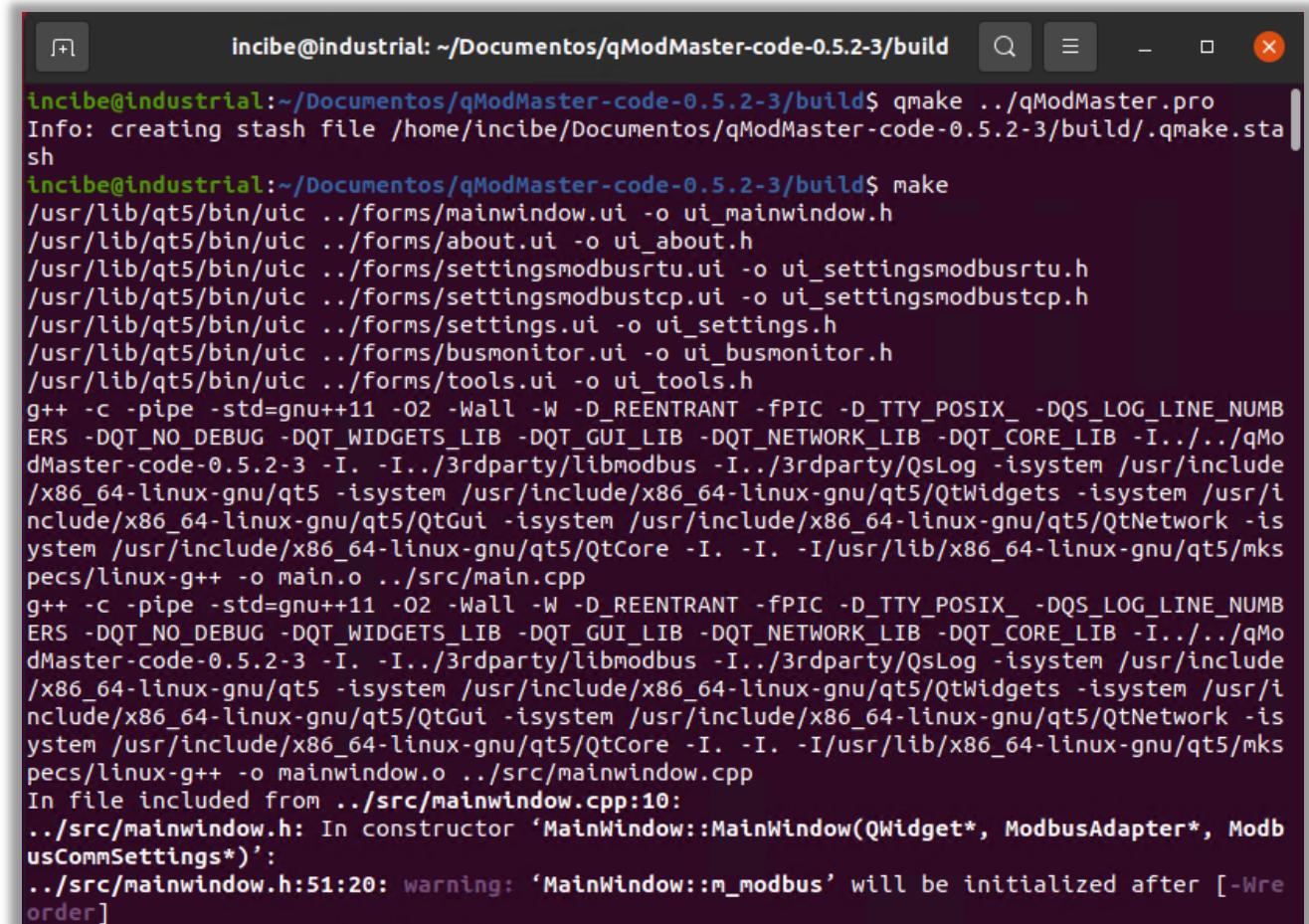
INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Con este segundo comando ejecutas el proceso de compilación que va a generar el archivo ejecutable de la aplicación

QModMaster:

- make

Ilustración 62: Ejecuta los comandos de compilación del paquete de software QModMaster.

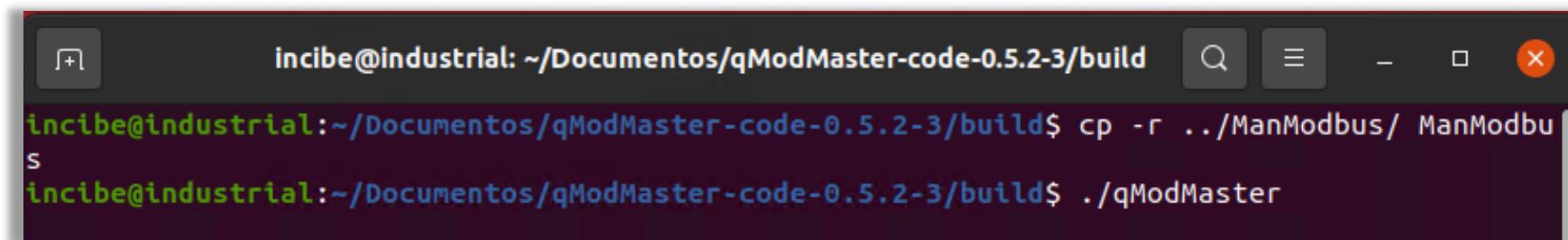


The screenshot shows a terminal window titled "incibe@industrial: ~/Documentos/qModMaster-code-0.5.2-3/build". The user has run the command "qmake ..\qModMaster.pro" followed by "make". The terminal output shows the compilation of multiple files, including UI files (mainwindow.ui, about.ui) and logic files (settingsmodbusrtu.ui, settingsmodbustcp.ui, settings.ui), using g++ with various flags. It also includes the linking of Qt libraries and system headers. A warning message at the end indicates that a variable will be initialized after its declaration.

```
incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3/build$ qmake ..\qModMaster.pro
Info: creating stash file /home/incibe/Documentos/qModMaster-code-0.5.2-3/build/.qmake.stash
incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3/build$ make
/usr/lib/qt5/bin/uic ..\forms/mainwindow.ui -o ui_mainwindow.h
/usr/lib/qt5/bin/uic ..\forms/about.ui -o ui_about.h
/usr/lib/qt5/bin/uic ..\forms/settingsmodbusrtu.ui -o ui_settingsmodbusrtu.h
/usr/lib/qt5/bin/uic ..\forms/settingsmodbustcp.ui -o ui_settingsmodbustcp.h
/usr/lib/qt5/bin/uic ..\forms/settings.ui -o ui_settings.h
/usr/lib/qt5/bin/uic ..\forms/busmonitor.ui -o ui_busmonitor.h
/usr/lib/qt5/bin/uic ..\forms/tools.ui -o ui_tools.h
g++ -c -pipe -std=gnu++11 -O2 -Wall -W -D_REENTRANT -fPIC -D_TTY_POSIX_ -DQS_LOG_LINE_NUMBERS -DQT_NO_DEBUG -DQT_WIDGETS_LIB -DQT_GUI_LIB -DQT_NETWORK_LIB -DQT_CORE_LIB -I../../qModMaster-code-0.5.2-3 -I. -I../3rdparty/libmodbus -I../3rdparty/QsLog -isystem /usr/include/x86_64-linux-gnu/qt5 -isystem /usr/include/x86_64-linux-gnu/qt5/QtWidgets -isystem /usr/include/x86_64-linux-gnu/qt5/QtGui -isystem /usr/include/x86_64-linux-gnu/qt5/QtNetwork -isystem /usr/include/x86_64-linux-gnu/qt5/QtCore -I. -I. -I/usr/lib/x86_64-linux-gnu/qt5/mkspecs/linux-g++ -o main.o ..\src\mainwindow.cpp
g++ -c -pipe -std=gnu++11 -O2 -Wall -W -D_REENTRANT -fPIC -D_TTY_POSIX_ -DQS_LOG_LINE_NUMBERS -DQT_NO_DEBUG -DQT_WIDGETS_LIB -DQT_GUI_LIB -DQT_NETWORK_LIB -DQT_CORE_LIB -I../../qModMaster-code-0.5.2-3 -I. -I../3rdparty/libmodbus -I../3rdparty/QsLog -isystem /usr/include/x86_64-linux-gnu/qt5 -isystem /usr/include/x86_64-linux-gnu/qt5/QtWidgets -isystem /usr/include/x86_64-linux-gnu/qt5/QtGui -isystem /usr/include/x86_64-linux-gnu/qt5/QtNetwork -isystem /usr/include/x86_64-linux-gnu/qt5/QtCore -I. -I. -I/usr/lib/x86_64-linux-gnu/qt5/mkspecs/linux-g++ -o mainwindow.o ..\src\mainwindow.cpp
In file included from ..\src\mainwindow.cpp:10:
..\src\mainwindow.h: In constructor 'MainWindow::MainWindow(QWidget*, ModbusAdapter*, ModbusCommSettings*)':
..\src\mainwindow.h:51:20: warning: 'MainWindow::m_modbus' will be initialized after [-Wreorder]
```

5 INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Copia el contenido de la ayuda (carpeta ManModbus) a la carpeta actual «*build*», ejecuta la aplicación qModMaster y comprueba cómo aparece la ventana del simulador qModMaster.
 - Ejecuta el comando **cp** con el parámetro **-r** para que copie la carpeta ManModbus, así como todo su contenido de forma recursiva:
 - **cp -r ..\ManModbus/ ManModbus**
 - Para poder ejecutar el archivo, escribe delante del comando **./**:
 - **./qModMaster**



A screenshot of a terminal window titled "incibe@industrial: ~/Documentos/qModMaster-code-0.5.2-3/build". The window shows three lines of command-line text:
1. "incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3/build\$ cp -r ..\ManModbus/ ManModbu
s"
2. "incibe@industrial:~/Documentos/qModMaster-code-0.5.2-3/build\$./qModMaster"
3. An empty line at the bottom.

Ilustración 63: Copia del contenido de la ayuda (carpeta ManModbus) a la carpeta actual «*build*», ejecutando la aplicación qModMaster y comprobando como aparece la ventana del simulador qModMaster.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- En esta vista se puede observar la ventana de la aplicación QModMaster.

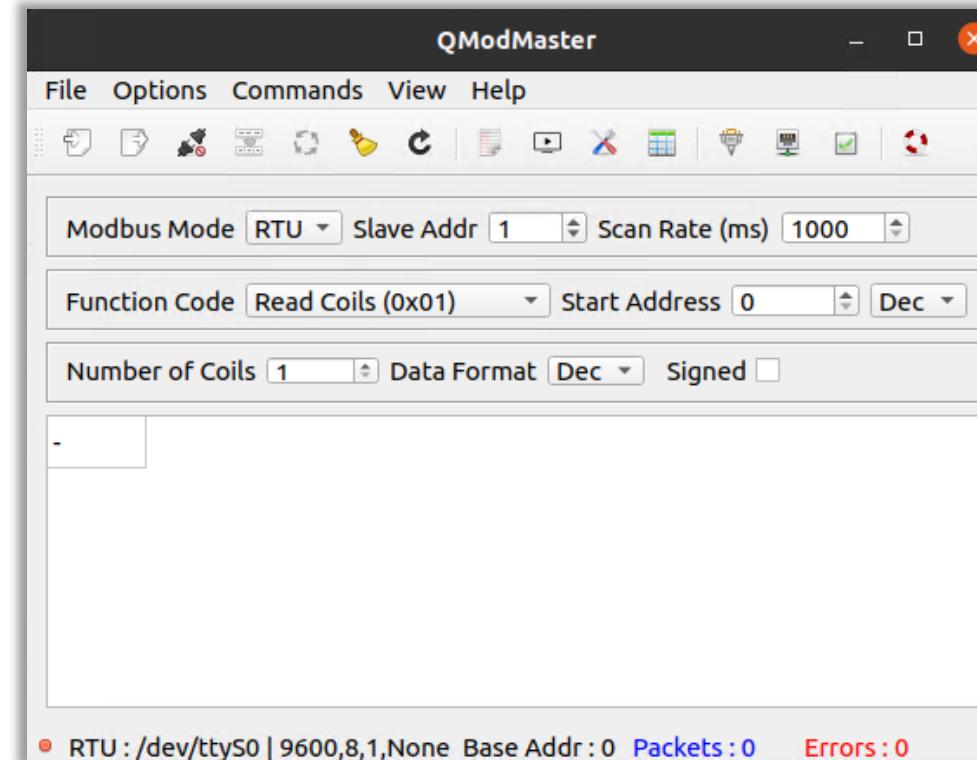


Ilustración 64: Vista de la ventana de la aplicación QModMaster.

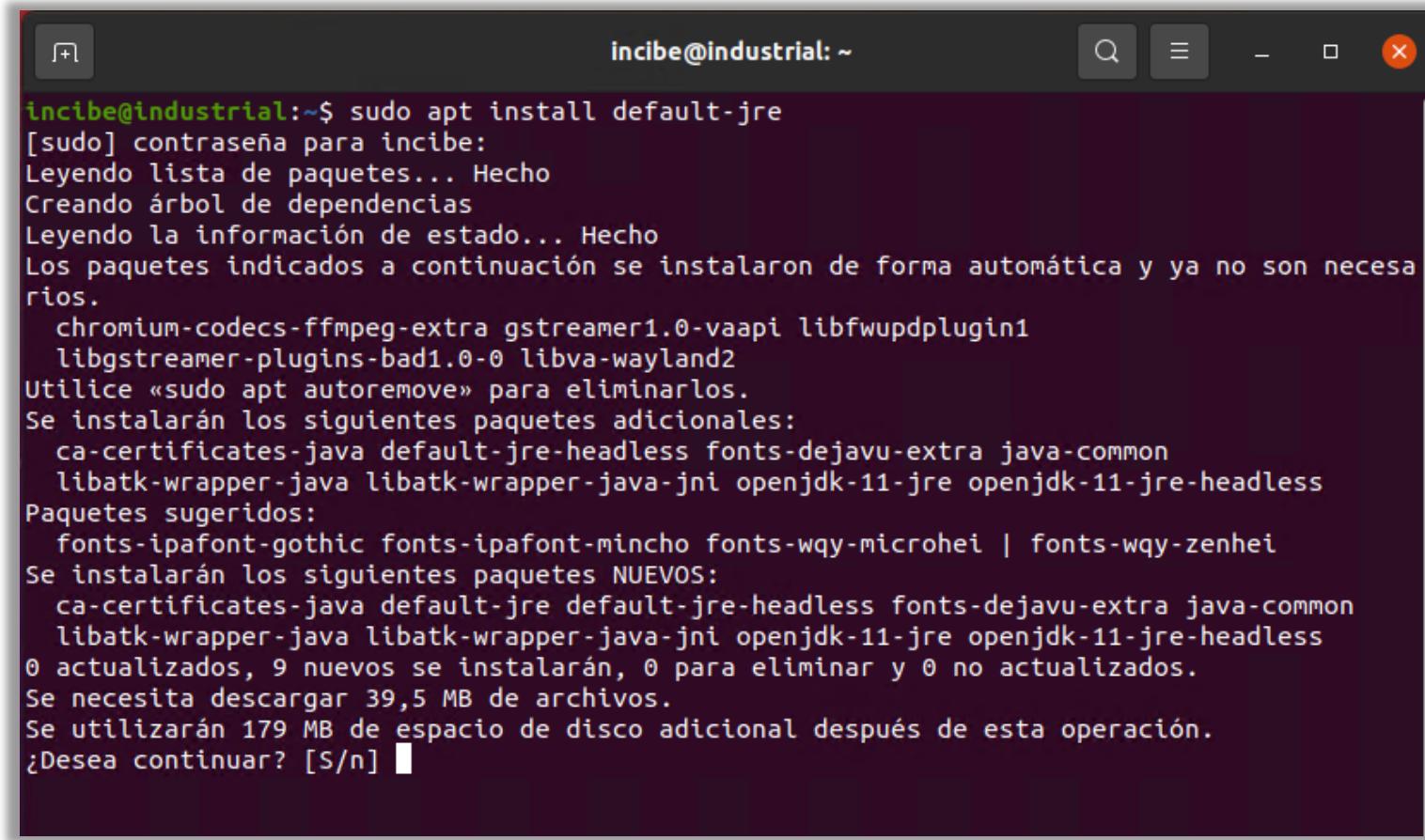


INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- La ventana de esta aplicación QModMaster no la cierres, ya que la necesitas para la realización de los siguientes apartados y volverás a trabajar sobre ella.
- Por otro lado, abre una nueva terminal, como te hemos explicado anteriormente y ejecuta el comando de instalación del paquete de software de la máquina virtual de Java:
 - **sudo apt install default-jre**
- Una vez termine de ejecutarse el comando, te aparecerá la pregunta «¿Desea continuar?». Para continuar pulsa «enter» o escribe la letra «s» y «enter».

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS



```
incibe@industrial:~$ sudo apt install default-jre
[sudo] contraseña para incibe:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
ca-certificates-java default-jre-headless fonts-dejavu-extra java-common
libatk-wrapper-java libatk-wrapper-java-jni openjdk-11-jre openjdk-11-jre-headless
Paquetes sugeridos:
fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei
Se instalarán los siguientes paquetes NUEVOS:
ca-certificates-java default-jre default-jre-headless fonts-dejavu-extra java-common
libatk-wrapper-java libatk-wrapper-java-jni openjdk-11-jre openjdk-11-jre-headless
0 actualizados, 9 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 39,5 MB de archivos.
Se utilizarán 179 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] ■
```

Ilustración 65: Ejecución del comando de instalación del paquete de software de la máquina virtual de Java.

5 INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Abre el navegador web Firefox, haciendo clic en su ícono y accede a la página web del simulador del dispositivo Modbus de tipo esclavo introduciendo <https://sourceforge.net/projects/modbuspal/>
Después, haz clic en el botón «Download» para que nos descargue la última versión de ModbusPal.

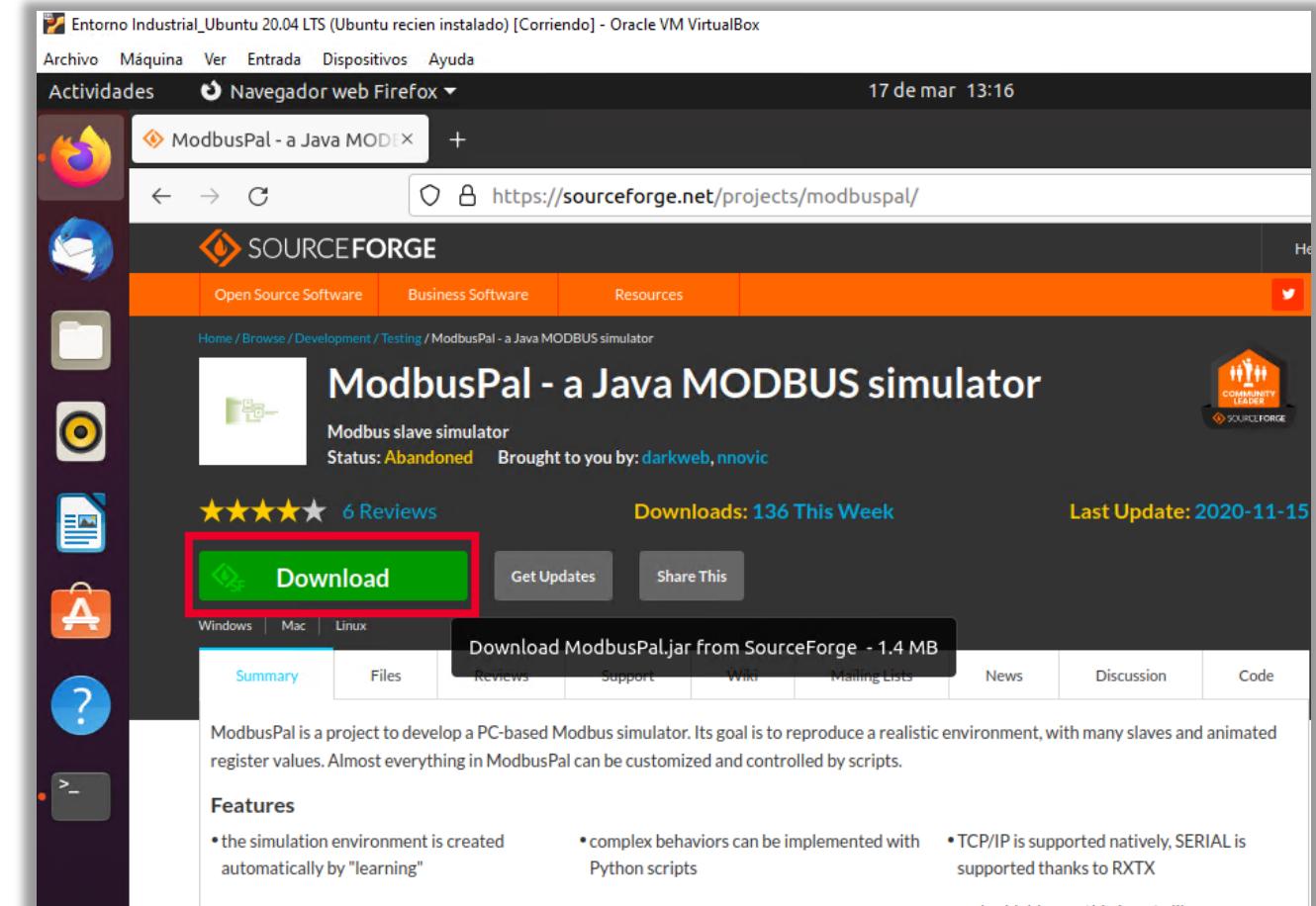


Ilustración 66: Imagen de la ventana de descarga de ModbusPal.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

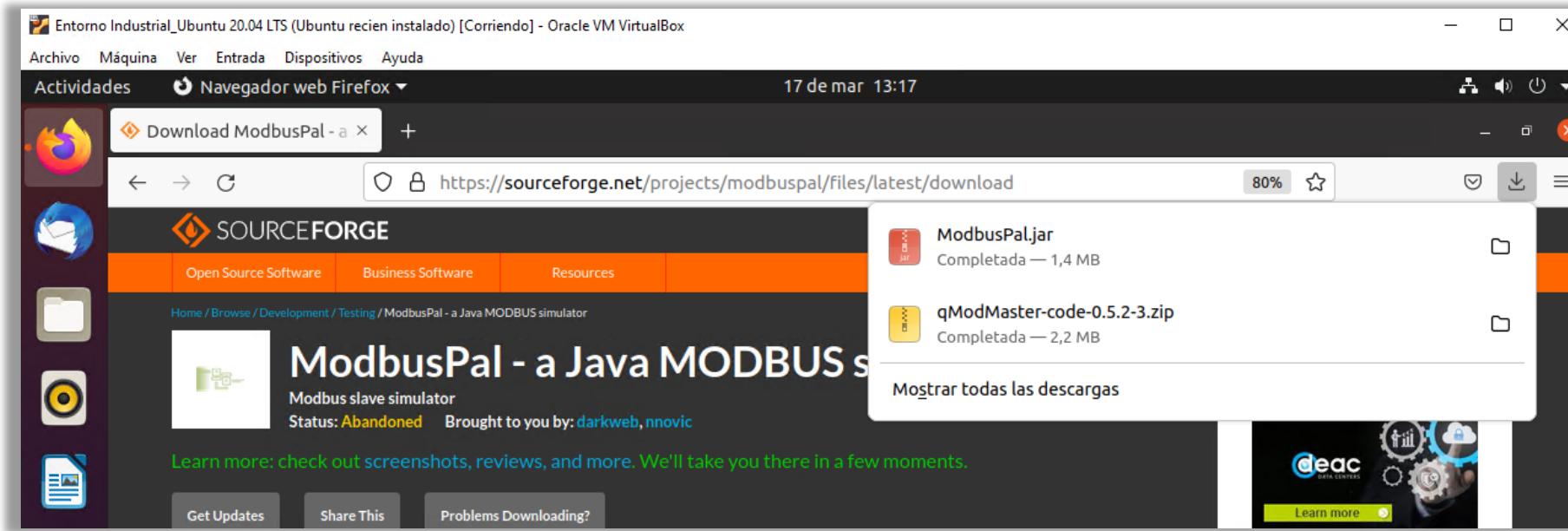


Ilustración 67: Imagen de estado de la descarga.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Desde la terminal anterior (o si la has cerrado, abre una nueva), crea la carpeta «modbuspal» en la carpeta «Documentos» y copia el archivo que acabas de descargar a la carpeta recién creada.
 - **mkdir Documentos/modbuspal**
 - **cp Descargas/ModbusPal.jar Documentos/modbuspal/**
- Despues accede a la carpeta modbuspal y ejecuta el comando **Java** indicándole con el parámetro **-jar** el nombre del archivo que queremos ejecutar (que es el archivo «ModbusPal.jar»).
 - **cd Documentos/modbuspal/**
 - **sudo java -jar ModbusPal.jar**



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

```
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
done.
incibe@industrial:~$ mkdir Documentos/modbuspal
incibe@industrial:~$ cp Descargas/ModbusPal.jar Documentos/modbuspal/
incibe@industrial:~$ cd Documentos/modbuspal/
incibe@industrial:~/Documentos/modbuspal$ sudo java -jar ModbusPal.jar
```

Ilustración 68: Creación de la carpeta «modbuspal» en la carpeta «Documentos» y copia del archivo que descargado en la carpeta recién creada.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

- Comprueba que aparece la ventana del simulador del dispositivo ModbusPal, desde la que más adelante crearemos nuestros esclavos.
- La ventana de esta aplicación ModbusPal no la cierres, ya que la necesitas para la realización de los siguientes apartados y volverás sobre ella.

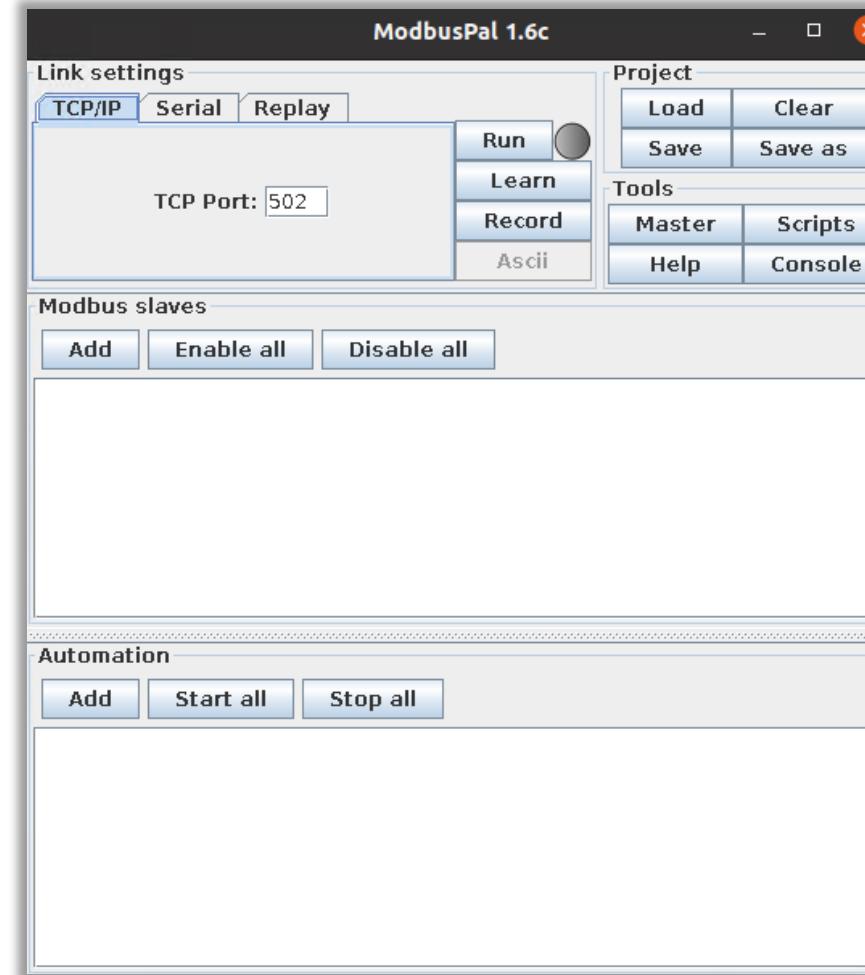


Ilustración 69: Comprobación de que la ventana del simulador del dispositivo Modbus de tipo Esclavo.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

Ahora, instalarás las herramientas necesarias para simular un dispositivo PLC Siemens, con el paquete de *software* Snap7.

Este paquete de *software* está formado por dos aplicaciones de tipo cliente/servidor y ambas en conjunto simulan el funcionamiento de un dispositivo PLC Siemens. La primera de ellas es la aplicación Snap7 Server Demo y es la que desempeña el rol de dispositivo PLC y suministra los datos cuando le son solicitados.

La segunda aplicación es la encargada de interactuar con este PLC a modo de cliente e interfaz para mostrar toda la información del mismo. Esta aplicación se denomina Snap7 Client Demo.

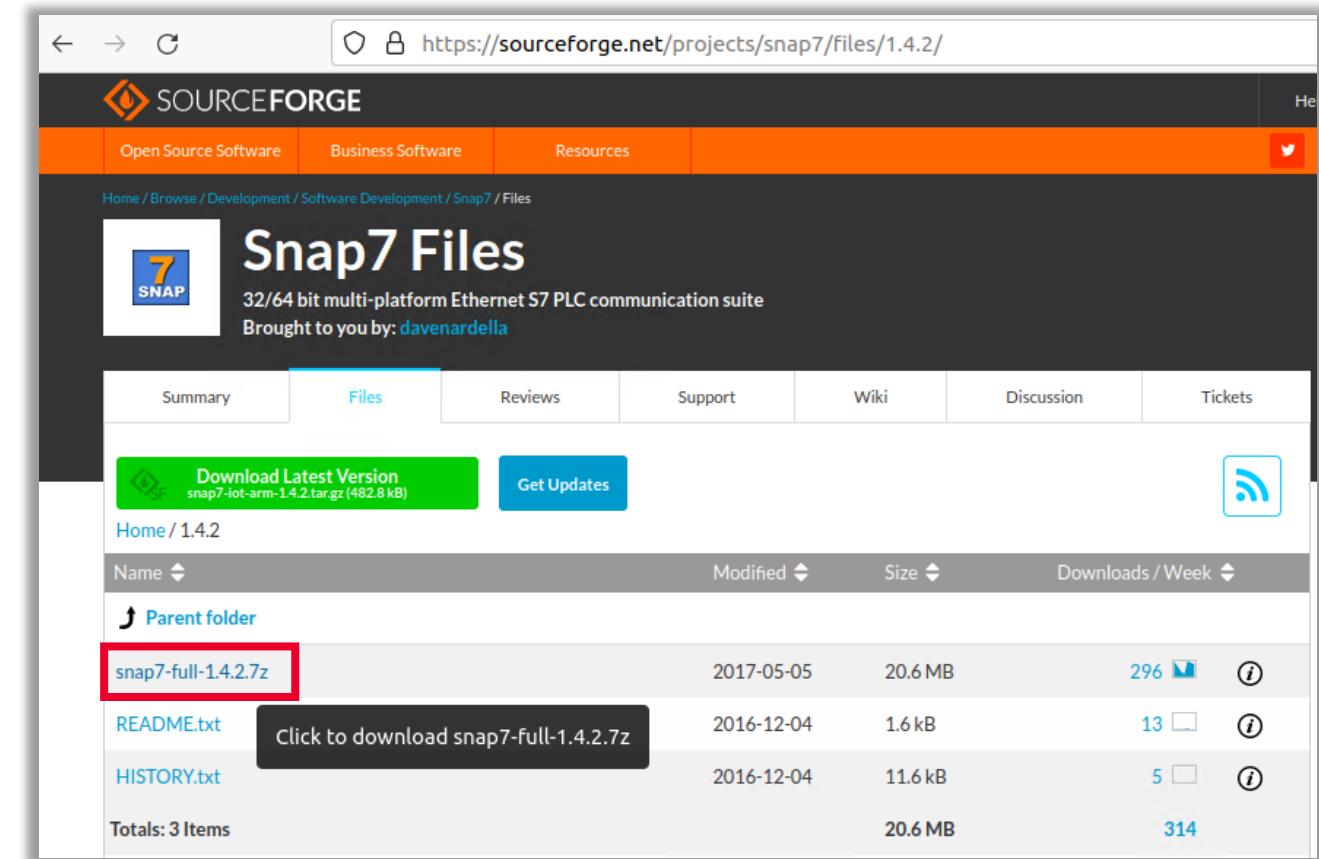
5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Descarga el paquete de software Snap7, desde el navegador Firefox de la MV Ubuntu.
- Haz clic en la entrada «snap7-full-1.4.2.7z» para descargar el paquete de software Snap7 para Linux.

Ilustración 70: Página de descarga del paquete de software Snap7 para Linux.



5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Haz clic en el icono en forma de carpeta, al lado del archivo que se acaba de descargar en Firefox, para que abra la carpeta contenedora del archivo descargado.

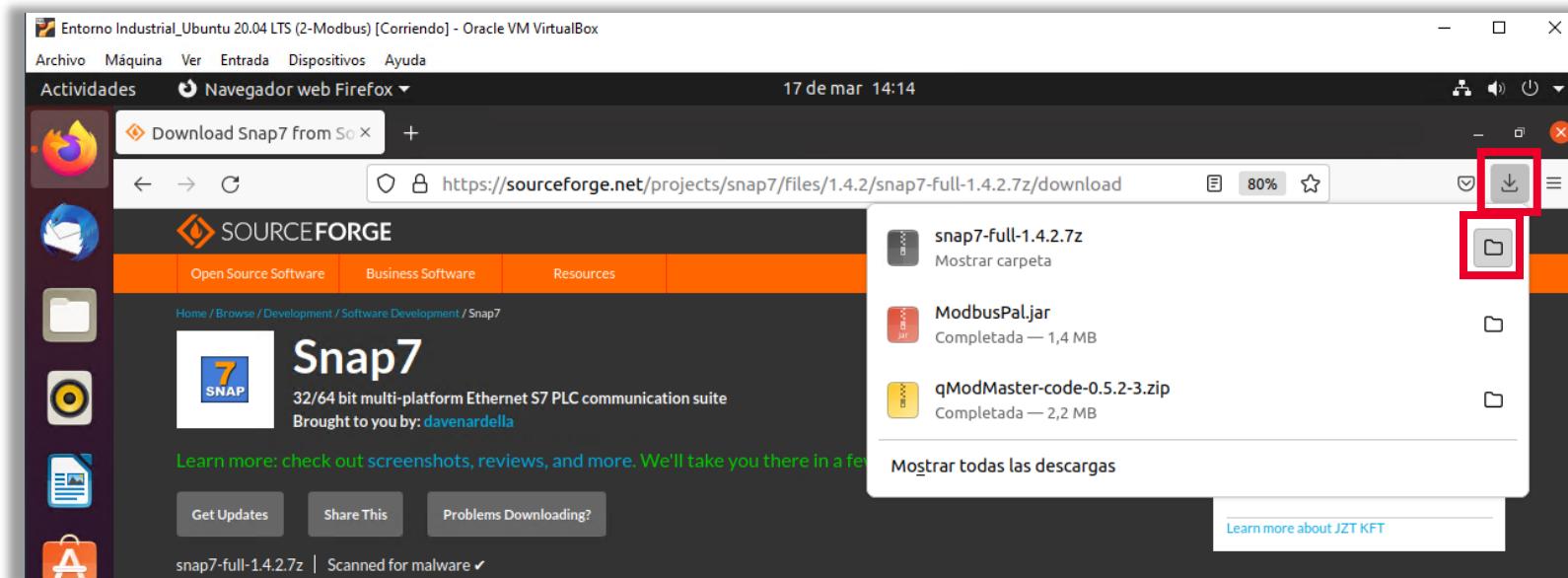


Ilustración 71: Carpeta al lado del archivo descargado para que se abra la carpeta contenedora del archivo descargado.

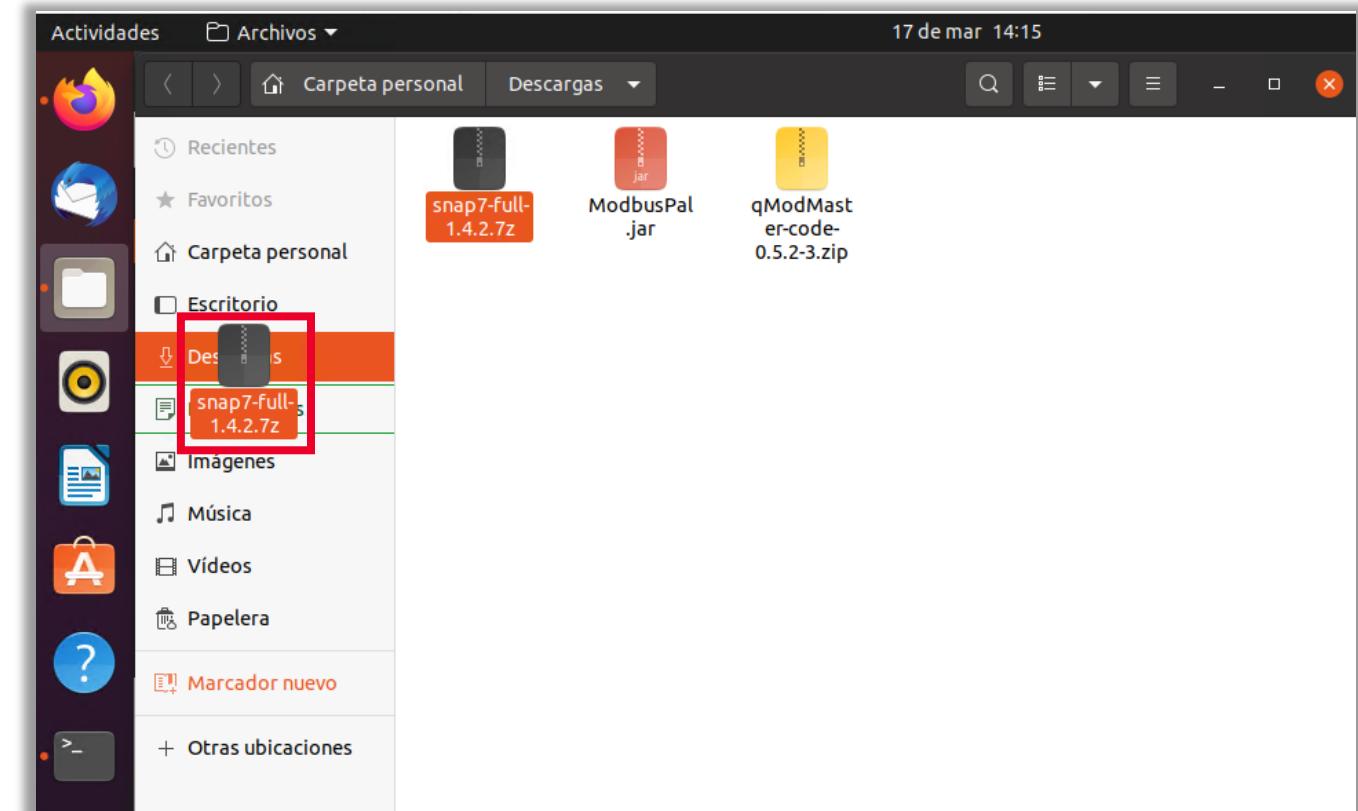
5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Selecciona el archivo «snap7-full-1.4.2.7z» y, sin soltar el botón izquierdo del ratón, arrástralolo a la ubicación que aparece debajo de la carpeta «Descargas», (que es la carpeta «Documentos») y suéltalo allí para copiarlo de esta forma utilizando la interfaz gráfica.

Ilustración 72: Selección del archivo «snap7-full-1.4.2.7z» y copiar en la carpeta «Documentos».



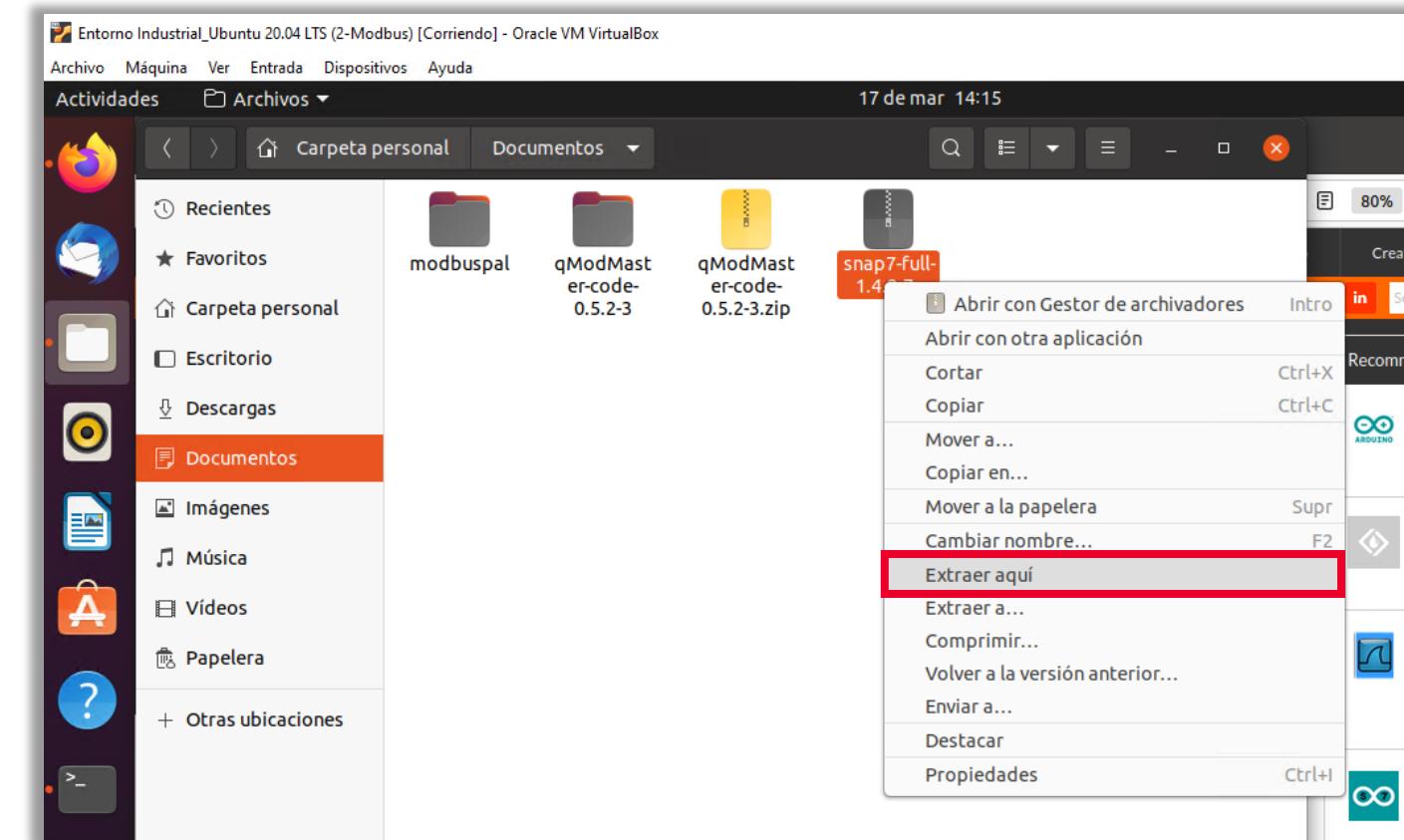
5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Haz clic en la entrada «Documentos» para acceder a esta carpeta, y selecciona el archivo que has copiado anteriormente. Haz clic con el botón izquierdo del ratón y selecciona la opción del menú desplegable «Extraer aquí», para que extraiga el contenido del archivo comprimido en formato 7Z, en la carpeta de nombre «snap7-full-1.4.2».

Ilustración 73: Descompresión del archivo en la carpeta de nombre «snap7-full-1.4.2».



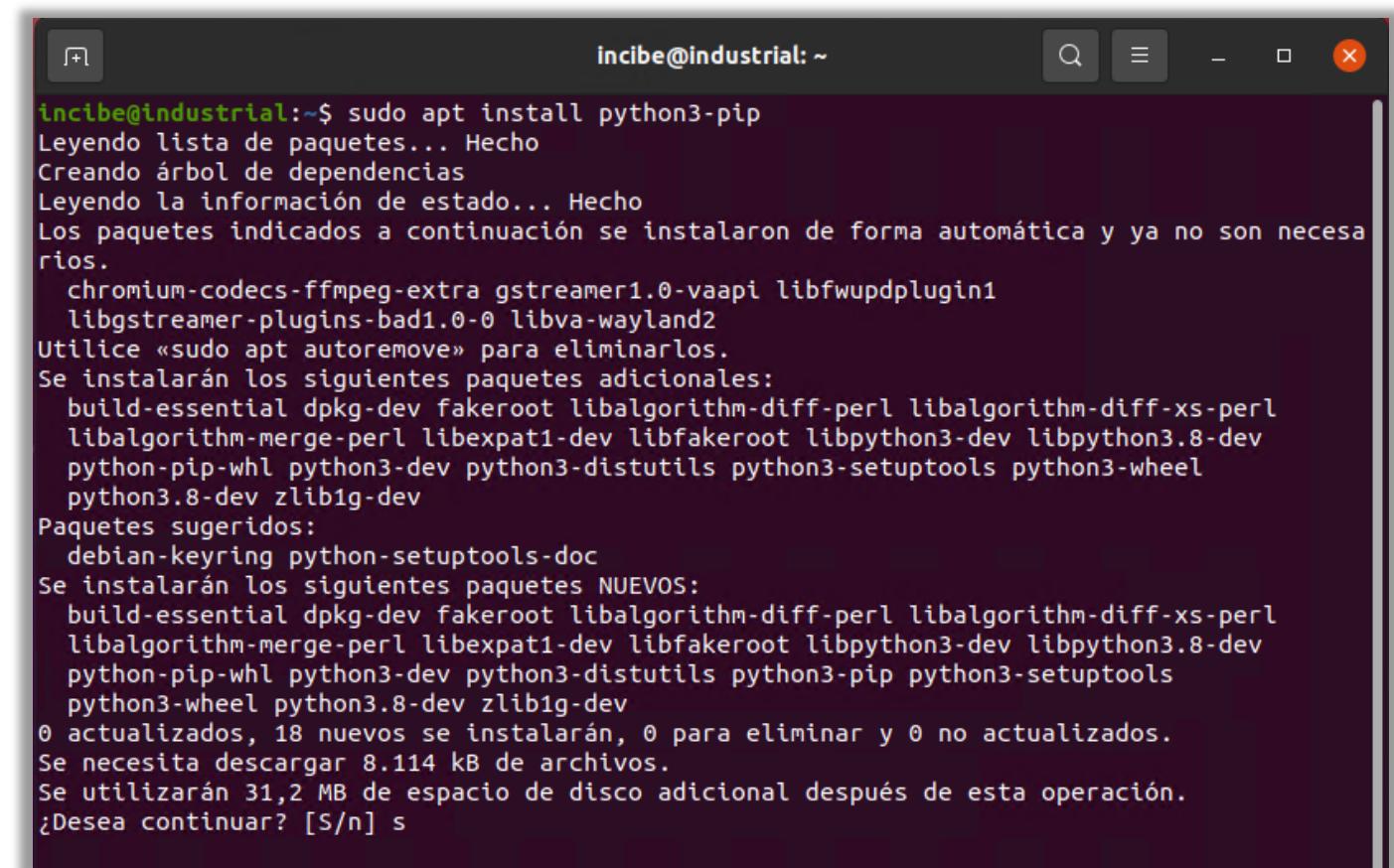
5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Desde la terminal, instala el gestor de paquetes para python 3 pip, que es necesario para instalar el paquete de software python-snap7:
 - **sudo apt install python3-pip**
- Pulsa «enter» o introduce la letra «s» y luego pulsa «enter» para continuar.

Ilustración 74: Instalación del gestor de paquetes para python 3 pip.



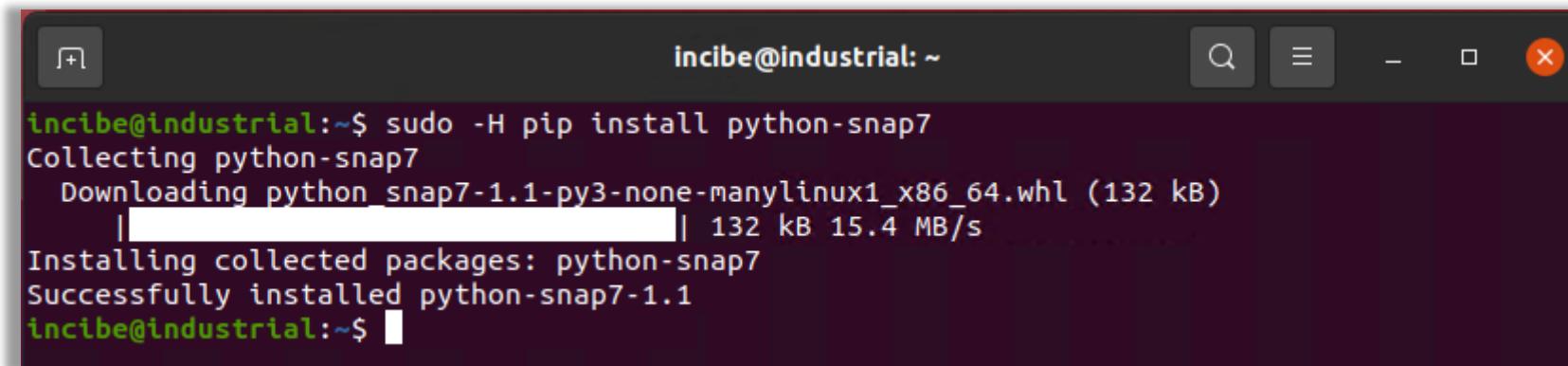
```
incibe@industrial:~$ sudo apt install python3-pip
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  build-essential dpkg-dev fakeroot libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libexpat1-dev libfakeroot libpython3-dev libpython3.8-dev
  python-pip-whl python3-dev python3-distutils python3-setuptools python3-wheel
  python3.8-dev zlib1g-dev
Paquetes sugeridos:
  debian-keyring python-setuptools-doc
Se instalarán los siguientes paquetes NUEVOS:
  build-essential dpkg-dev fakeroot libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libexpat1-dev libfakeroot libpython3-dev libpython3.8-dev
  python-pip-whl python3-dev python3-distutils python3-pip python3-setuptools
  python3-wheel python3.8-dev zlib1g-dev
0 actualizados, 18 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 8.114 kB de archivos.
Se utilizarán 31,2 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Con el gestor de paquetes pip (que acabas de instalar), instala el paquete python-snap7:
 - **sudo -H pip install python-snap7**
- La barra blanca que ves en la imagen, es la barra de descarga del programa.



```
incibe@industrial:~$ sudo -H pip install python-snap7
Collecting python-snap7
  Downloading python_snap7-1.1-py3-none-manylinux1_x86_64.whl (132 kB)
|████████████████████████████████████████████████████████████████| 132 kB 15.4 MB/s
Installing collected packages: python-snap7
Successfully installed python-snap7-1.1
incibe@industrial:~$
```

Ilustración 75: Proceso de instalación el paquete python-snap7 con el gestor instalado.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

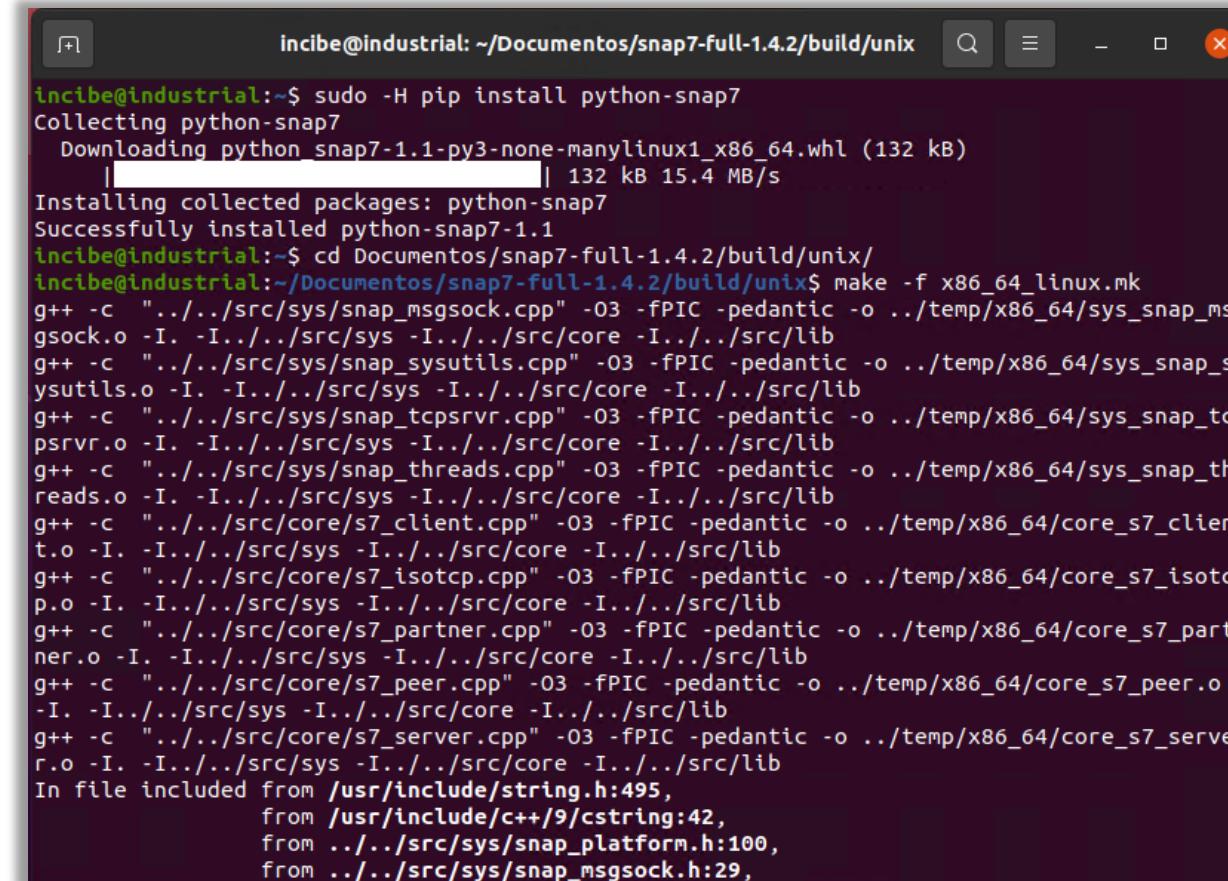
5.1 Instalación herramientas de simulación de dispositivos Siemens

- Accede a la carpeta donde se encuentran los archivos del código fuente que tienes que compilar para la versión de Linux de 64 *bits*, con el siguiente comando:
 - **cd Documentos/snap7-full-1.4.2/build/unix/**
- Despues invoca el comando de compilación, con **make** y el parámetro **-f**, donde le especificamos que **x86_64_linux.mk** es el archivo de nuestro sistema Linux de 64 *bits* que vamos a compilar:
 - **make -f x86_64_linux.mk**

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens



```
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/unix$ sudo -H pip install python-snap7
Collecting python-snap7
  Downloading python_snap7-1.1-py3-none-manylinux1_x86_64.whl (132 kB)
    |████████| 132 kB 15.4 MB/s
Installing collected packages: python-snap7
Successfully installed python-snap7-1.1
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/unix$ make -f x86_64_linux.mk
g++ -c "../../../src/sys/snap_msgsock.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/sys_snap_ms
gsock.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/sys/snap_sysutils.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/sys_snap_s
ysutils.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/sys/snap_tcpsrvr.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/sys_snap_tc
psrvr.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/sys/snap_threads.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/sys_snap_th
reads.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/core/s7_client.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/core_s7_clien
t.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/core/s7_isotcp.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/core_s7_isotc
p.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/core/s7_partner.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/core_s7_part
ner.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/core/s7_peer.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/core_s7_peer.o
-I. -I../../../src/sys -I../../../src/core -I../../../src/lib
g++ -c "../../../src/core/s7_server.cpp" -O3 -fPIC -pedantic -o ../../temp/x86_64/core_s7_serve
r.o -I. -I../../../src/sys -I../../../src/core -I../../../src/lib
In file included from /usr/include/string.h:495,
                 from /usr/include/c++/9/cstring:42,
                 from ../../../src/sys/snap_platform.h:100,
                 from ../../../src/sys/snap_msgsock.h:29,
```

Ilustración 76: Acceso a la carpeta donde se encuentran los archivos del código fuente que es necesario compilar para la versión de Linux de 64 bits.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

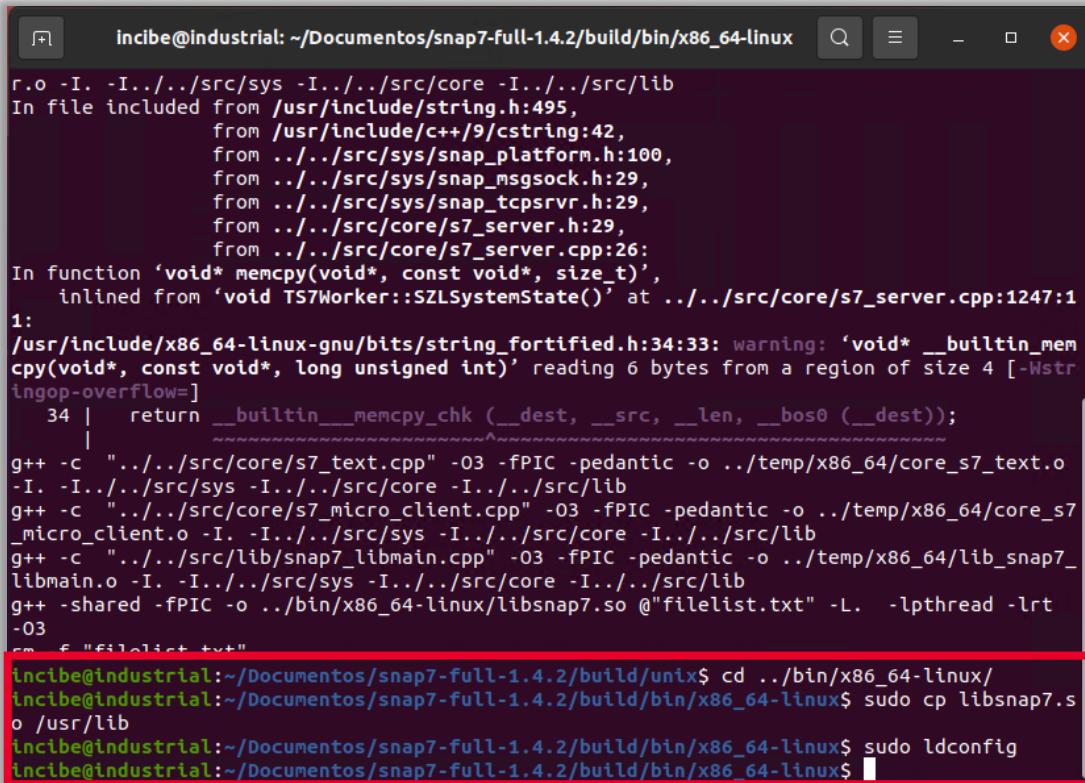
5.1 Instalación herramientas de simulación de dispositivos Siemens

- Accede a la carpeta donde se acaba de generar la librería que necesita Linux Ubuntu para poder ejecutar el paquete de software Snap7 con:
 - **cd .../bin/x86_64-linux/**
- Copia la librería a la ubicación de las librerías del sistema. Como lo vas a hacer con sudo, te pedirá que introduzcas la contraseña del súper usuario. Si no la pide, es porque ya la tiene almacenada por haberla introducido previamente en esta terminal:
 - **sudo cp libsnap7.so /usr/lib**
- Ejecuta **ldconfig**, para crear los vínculos necesarios para las bibliotecas compartidas:
 - **sudo ldconfig**

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens



The terminal window shows the compilation of the snap7 library. The user is in the directory ~/Documentos/snap7-full-1.4.2/build/bin/x86_64-linux. The compilation command is:

```
r.o -I../../src/sys -I../../src/core -I../../src/lib  
In file included from /usr/include/string.h:495,  
     from /usr/include/c++/9/cstring:42,  
     from ../../src/sys/snap_platform.h:100,  
     from ../../src/sys/snap_msgsock.h:29,  
     from ../../src/sys/snap_tcpsrvr.h:29,  
     from ../../src/core/s7_server.h:29,  
     from ../../src/core/s7_server.cpp:26:  
In function 'void* memcp(void*, const void*, size_t)',  
  inlined from 'void TS7Worker::S7SystemState()' at ../../src/core/s7_server.cpp:1247:1  
1:  
/usr/include/x86_64-linux-gnu/bits/string_fortified.h:34:33: warning: 'void* __builtin_mem  
cpy(void*, const void*, long unsigned int)' reading 6 bytes from a region of size 4 [-Wstr  
ingop-overflow]  
  34 |   return __builtin_memcpy_chk (__dest, __src, __len, __bos0 (__dest));  
   |  
   |  
g++ -c "../../src/core/s7_text.cpp" -O3 -fPIC -pedantic -o ./temp/x86_64/core_s7_text.o  
-I. -I../../src/sys -I../../src/core -I../../src/lib  
g++ -c "../../src/core/s7_micro_client.cpp" -O3 -fPIC -pedantic -o ./temp/x86_64/core_s7  
_micro_client.o -I. -I../../src/sys -I../../src/core -I../../src/lib  
g++ -c "../../src/lib/snap7_libmain.cpp" -O3 -fPIC -pedantic -o ./temp/x86_64/lib_snap7  
_libmain.o -I. -I../../src/sys -I../../src/core -I../../src/lib  
g++ -shared -fPIC -o ./bin/x86_64-linux/libsnap7.so @"filelist.txt" -L. -lpthread -lrt  
-O3  
cm -f "filelist.txt"  
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/unix$ cd ..//bin/x86_64-linux/  
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/bin/x86_64-linux$ sudo cp libsnap7.s  
o /usr/lib  
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/bin/x86_64-linux$ sudo ldconfig  
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/bin/x86_64-linux$
```

A large grey arrow points from the bottom of the terminal window towards the right side of the slide.

Ilustración 77: Imagen del proceso de copia de las librerías.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

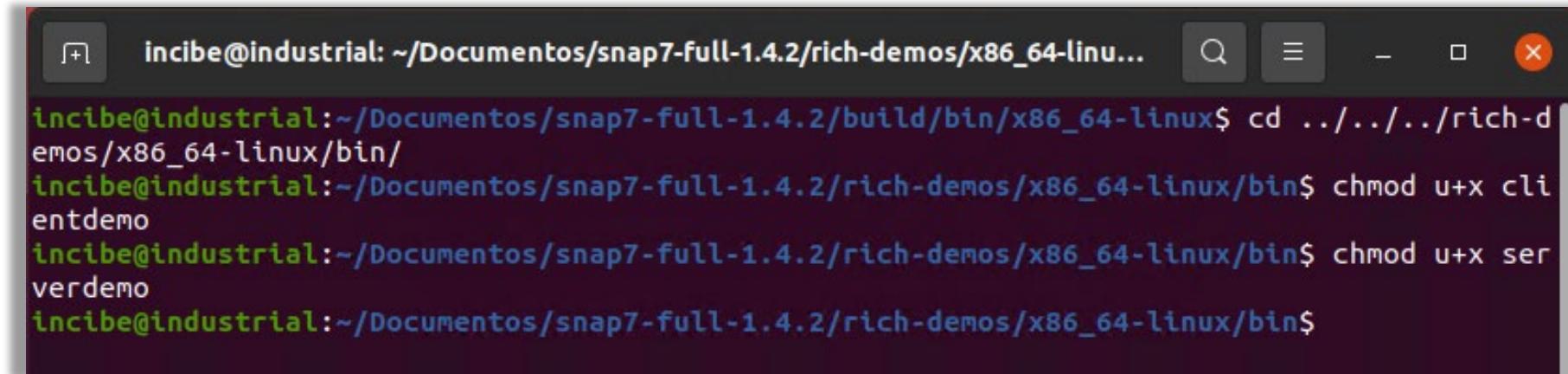
5.1 Instalación herramientas de simulación de dispositivos Siemens

- Accede a la carpeta donde se encuentran los archivos binarios de las aplicaciones que se han generado tras finalizar el proceso anterior de compilación, y asigna permisos de ejecución a los 2 archivos de nuestras aplicaciones Snap7. Esto se hace con los siguientes comandos:
 - **cd ../../rich-demos/x86_64-linux/bin/**
 - **chmod u+x clientdemo**
 - **chmod u+x serverdemo**
- Los comandos **chmod** permiten otorgar permisos.
 - «u» hace referencia a usuario (el propietario del archivo) y «x» hace referencia a permisos de ejecución.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens



```
incibe@industrial: ~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linu... 
incibe@industrial:~/Documentos/snap7-full-1.4.2/build/bin/x86_64-linux$ cd ../../rich-demos/x86_64-linux/bin/
incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$ chmod u+x clientdemo
incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$ chmod u+x serverdemo
incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$
```

Ilustración 78: Proceso de acceso a la carpeta donde se encuentran los archivos binarios de las aplicaciones y asignación de permisos.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

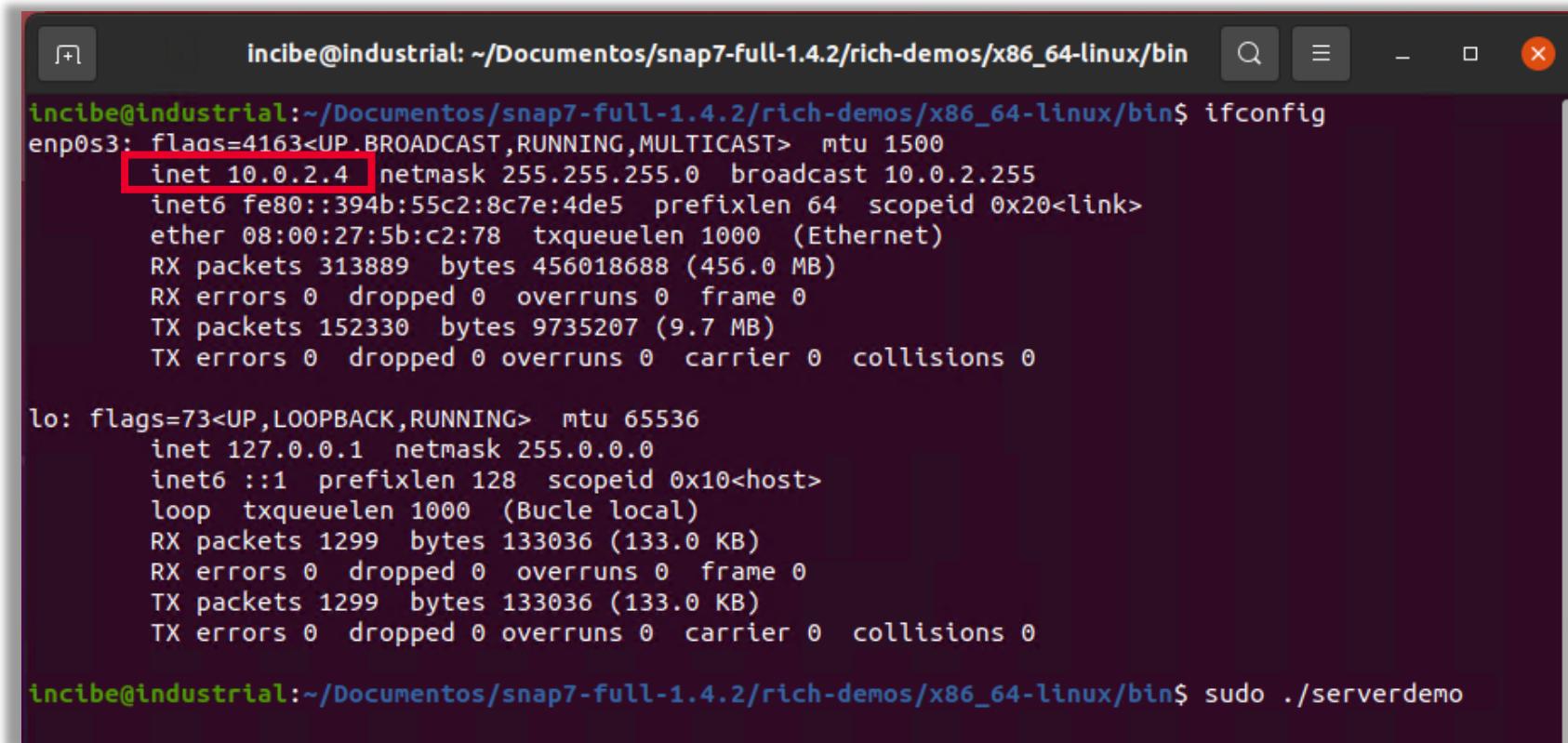
5.1 Instalación herramientas de simulación de dispositivos Siemens

- Ejecuta el comando **ifconfig** para averiguar la IP del adaptador de red de la MV Ubuntu. En nuestro caso la dirección IP es la 10.0.2.4, si a ti te sale una dirección IP diferente, deberás indicar la que a ti te aparezca. Esta IP es la que vas a configurar en la aplicación Snap7 Server Demo:
 - **Ifconfig**
- Ejecuta la aplicación «serverdemo»:
 - **sudo ./serverdemo**

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens



```
incibe@industrial: ~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 brd 10.0.2.255 netmask 255.255.255.0
        broadcast 10.0.2.255
        inet6 fe80::394b:55c2:8c7e:4de5 brd fe80::ff:fe:8c7e:4de5/64 scopeid 0x20<link>
            ether 08:00:27:5b:c2:78 txqueuelen 1000 (Ethernet)
            RX packets 313889 bytes 456018688 (456.0 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 152330 bytes 9735207 (9.7 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

    lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 brd ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Bucle local)
            RX packets 1299 bytes 133036 (133.0 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1299 bytes 133036 (133.0 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$ sudo ./serverdemo
```

Ilustración 79: Ejecución del comando ifconfig para averiguar la IP del adaptador de red de la MV Ubuntu.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Aparecerá la ventana de la aplicación Snap7 Server Demo, lo que indica que la aplicación se ha compilado e instalado adecuadamente. Esta aplicación simula un PLC Siemens.
 - Establece la IP de nuestro servidor Snap7, haciendo clic en el cuadro de texto «*Local Address*» e introduce la IP, en nuestro caso la 10.0.2.4., Después de esto pulsa en el botón «*Start*» para arrancar nuestro servidor Snap7.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

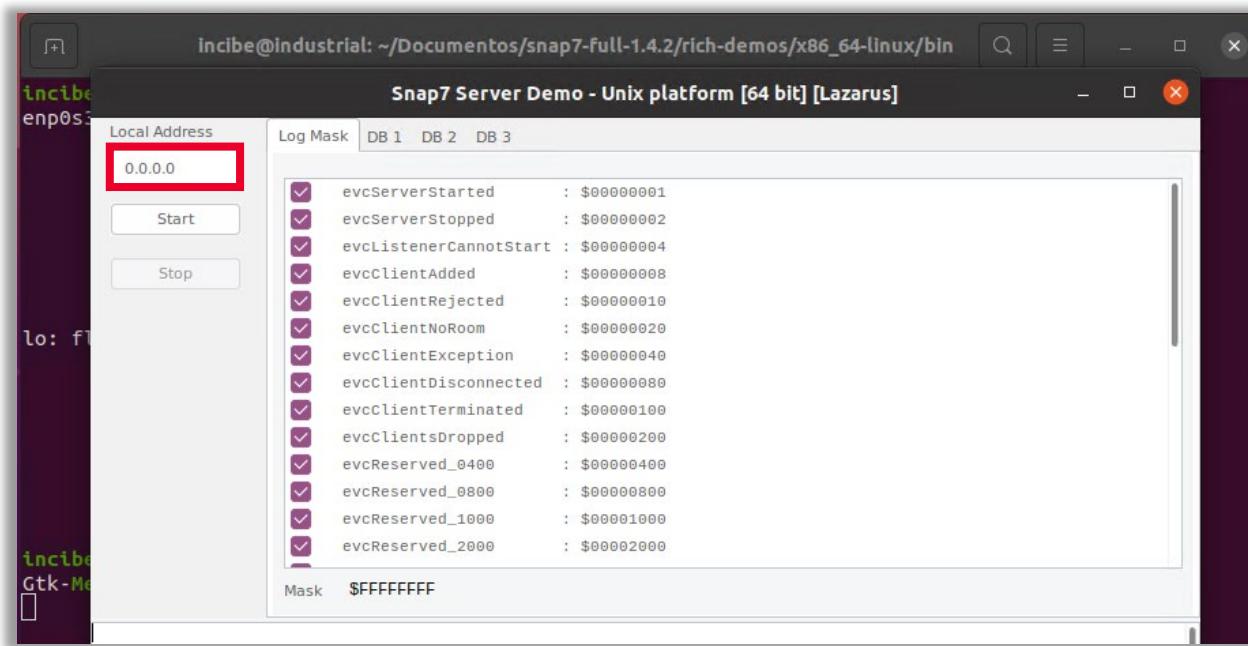


Ilustración 80: Ventana de la aplicación Snap7 Server Demo que simula un PLC Siemens. Destacado en rojo dónde se debe indicar la dirección IP.

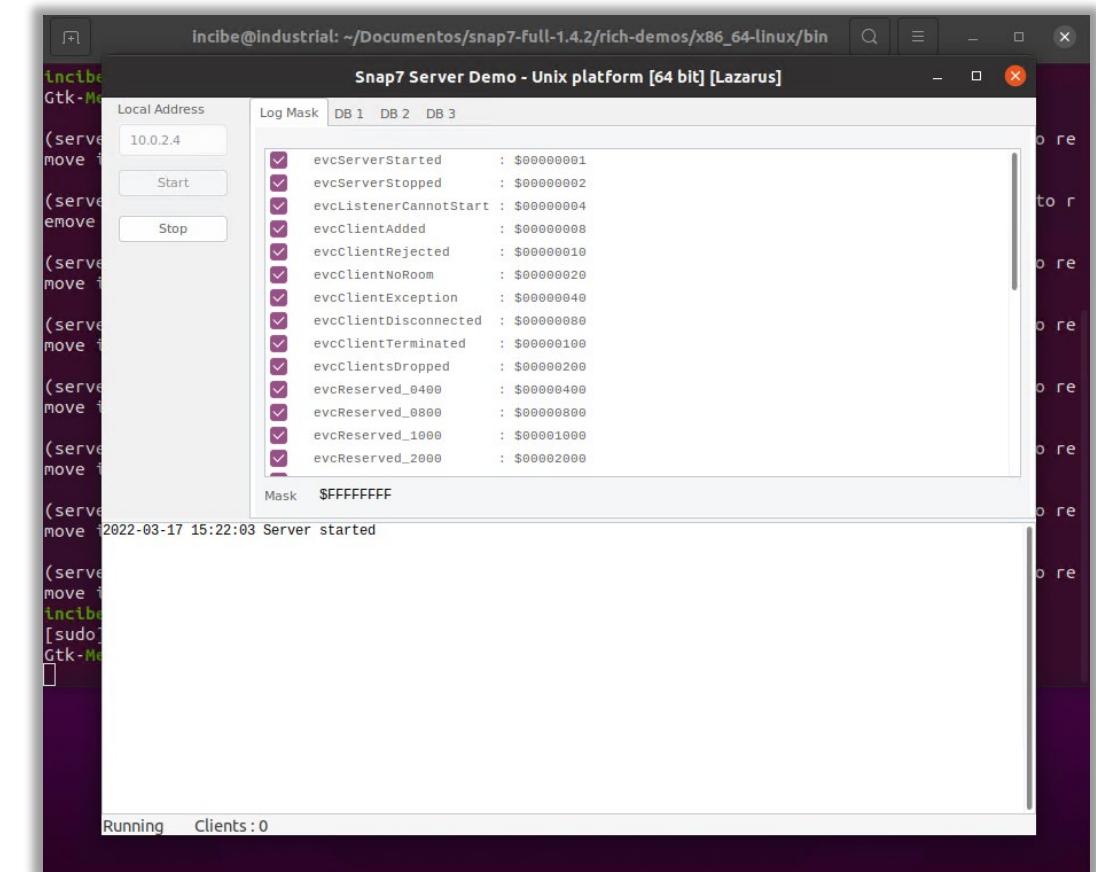


Ilustración 81: Establecimiento de la dirección IP del servidor Snap7.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Abre una nueva terminal haciendo clic en el icono de la terminal que aparece en el *dock* o barra de herramientas (se denominan de cualquiera de estas formas) de Ubuntu y selecciona la entrada «Ventana Nueva».

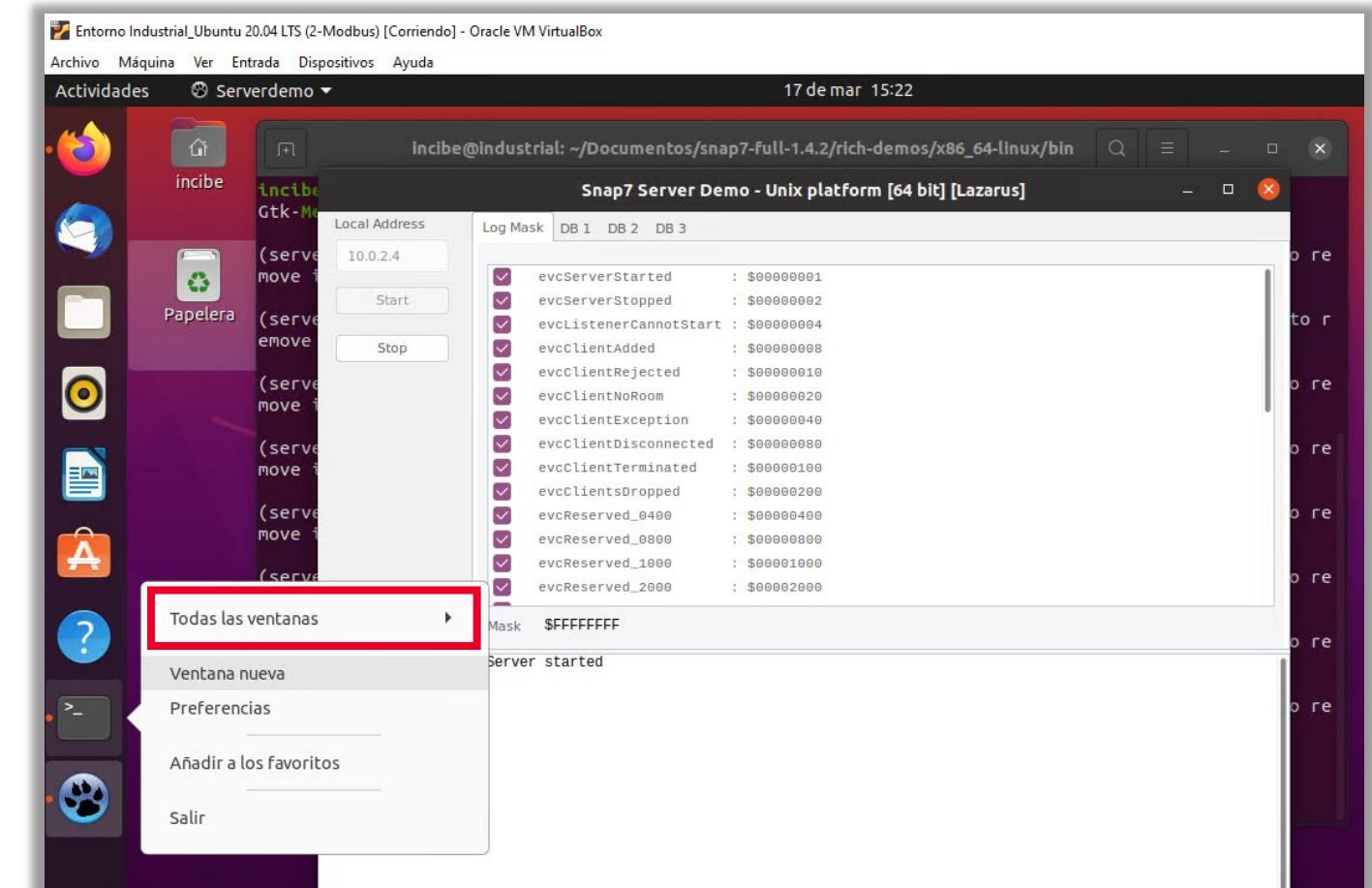


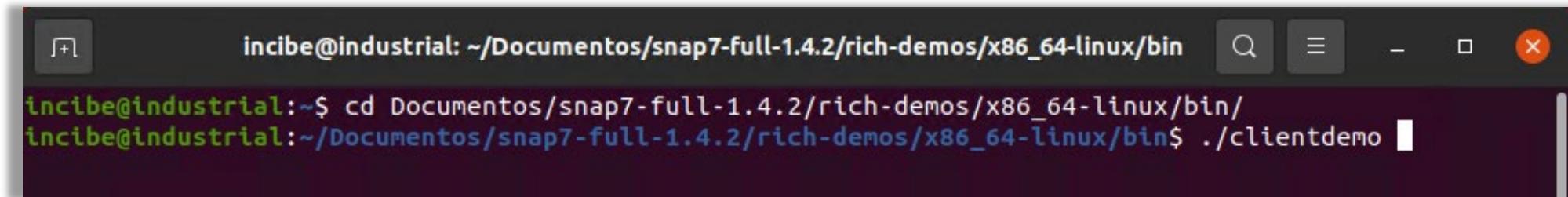
Ilustración 82: Apertura de nuevo terminal y selección de «Ventana Nueva».

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- En esta nueva terminal, accede a la carpeta donde has ejecutado la aplicación Snap7 Server Demo:
 - **cd Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin/**
- Ejecuta la aplicación «clientdemo»:
 - **./clientdemo**



A screenshot of a terminal window titled "incibe@industrial: ~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin". The terminal shows two commands being run: "cd Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin/" and "./clientdemo". The output of the second command is visible at the bottom of the terminal window.

```
incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin
incibe@industrial:~$ cd Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin/
incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$ ./clientdemo
```

Ilustración 83: Acceso a la carpeta de la aplicación Snap7 Server Demo y ejecución de «clientdemo».



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Aparece la ventana de la aplicación Snap7 Client Demo, lo que indica que la aplicación se ha compilado e instalado adecuadamente. Esta aplicación es el cliente que nos permite interactuar con el Servidor Siemens Snap7 Server Demo.
 - Establece la IP a la que te vas a conectar que, en nuestro caso, es la 10.0.2.4.
 - En la entrada «Connect as», elegimos S7 BASIC. Pulsa el botón «Connect» y, así, establecemos conexión con el servidor.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

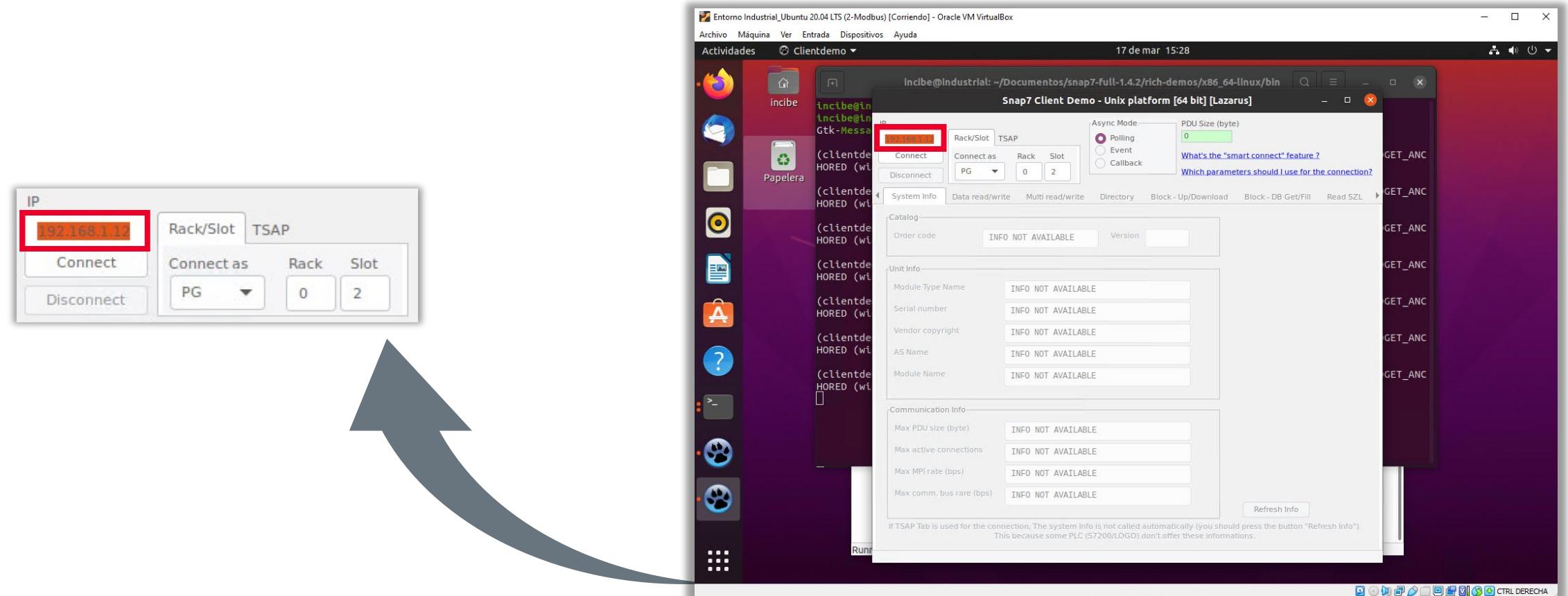


Ilustración 84: Imagen de la ventana de Snap7 Client Demo indicando que la aplicación se ha compilado e instalado correctamente.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

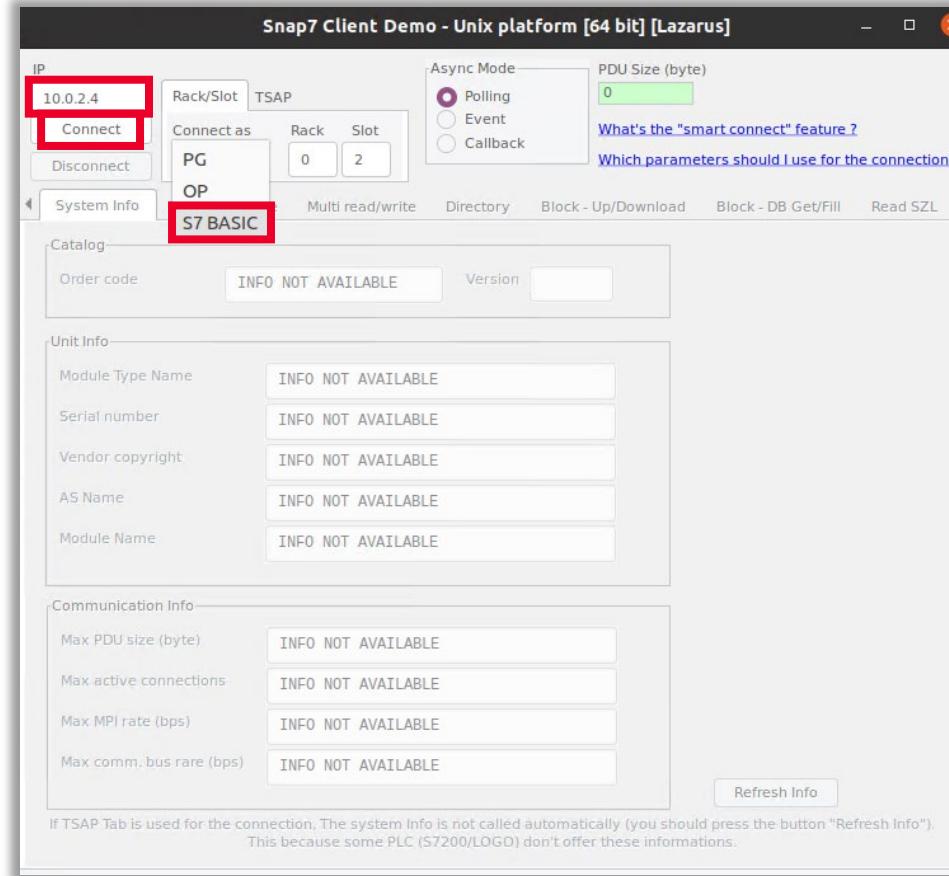


Ilustración 85: Establecimiento de la IP de la aplicación Snap7 Server Demo y elección de «S7 BASIC» en la entrada «Connect as».

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- La aplicación Snap7 Client Demo cuenta con una serie de pestañas a las que puedes acceder directamente. Si haces clic en la flecha derecha al final de la fila de pestañas accede a la pestaña «*Date/Time*» que muestra la fecha y hora establecida en el PLC que estas simulando con la aplicación Snap7 Server Demo.

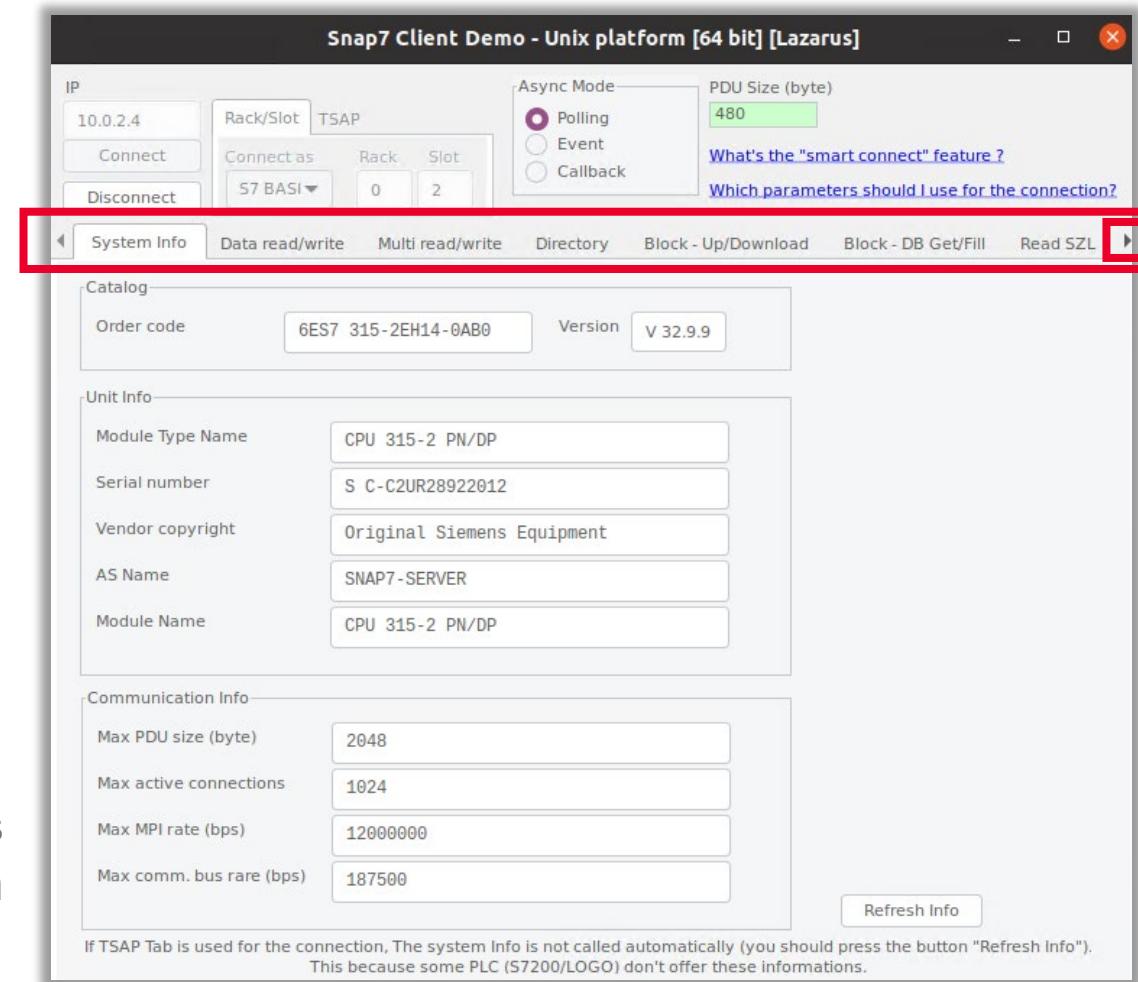


Ilustración 86: Imagen de las pestañas de la aplicación Snap7 Client Demo.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

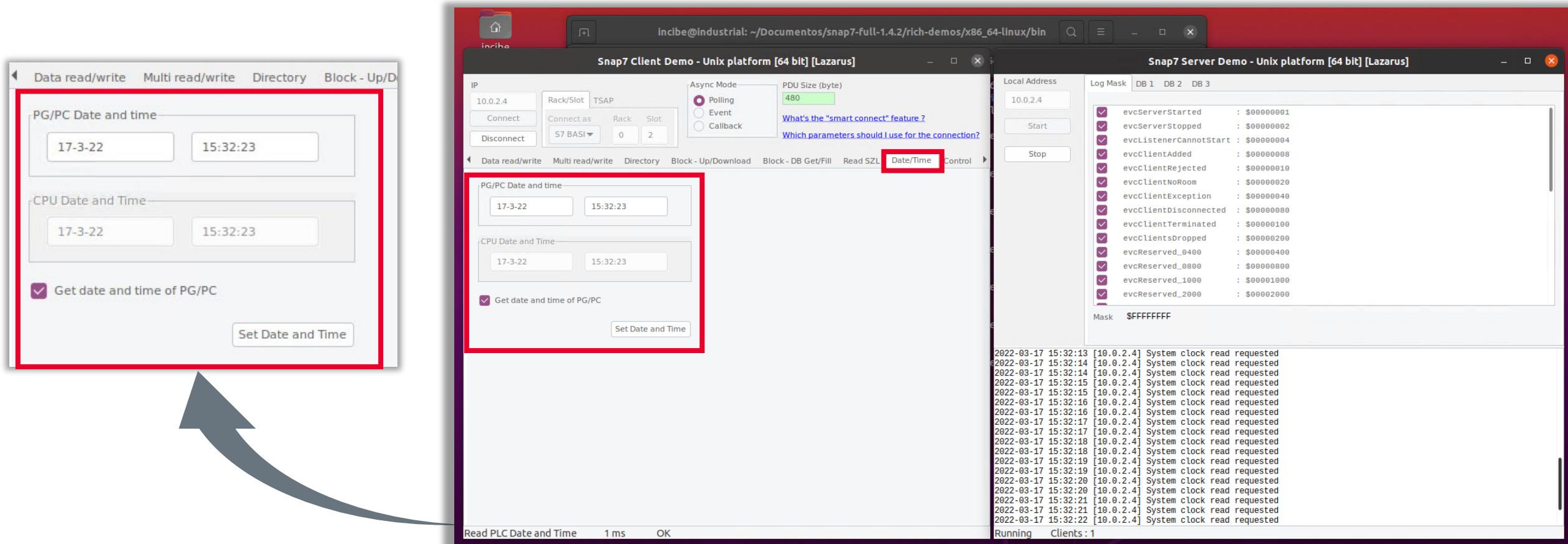


Ilustración 87: Imagen de la pestaña «Date/Time» que muestra la fecha y hora establecida en el PLC simulado con la aplicación Snap7 Server Demo.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- La pestaña «Control», es la parte más interesante de la aplicación Snap7 Client Demo ya que nos va a permitir realizar operación de parada del PLC (*Stop*) y arranque del PLC (*Start*).
 - En nuestro caso el PLC está en ejecución (en «*Run*»).

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

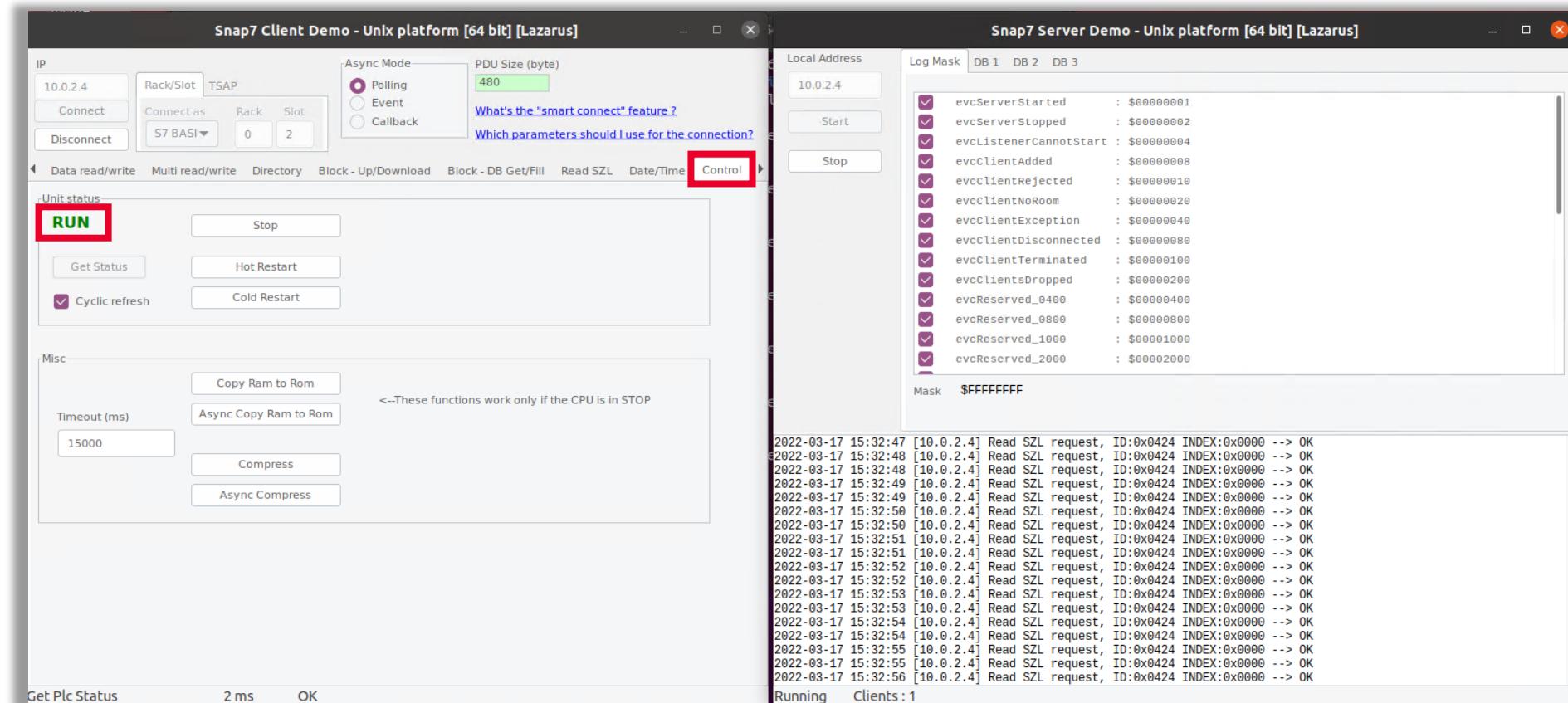


Ilustración 88: Pestaña «Control» que permite realizar operación de parada y arranque del PLC.



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Para parar el PLC, haz clic en el botón «Stop». Para confirmar que se ha detenido, haz clic en el botón «Get Status» y nos muestra que el estado del PLC ahora es *STOP*.

En la ventana de la aplicación Snap7 Server Demo podemos comprobar cómo aparece el registro de la orden recibida de CPU Control.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

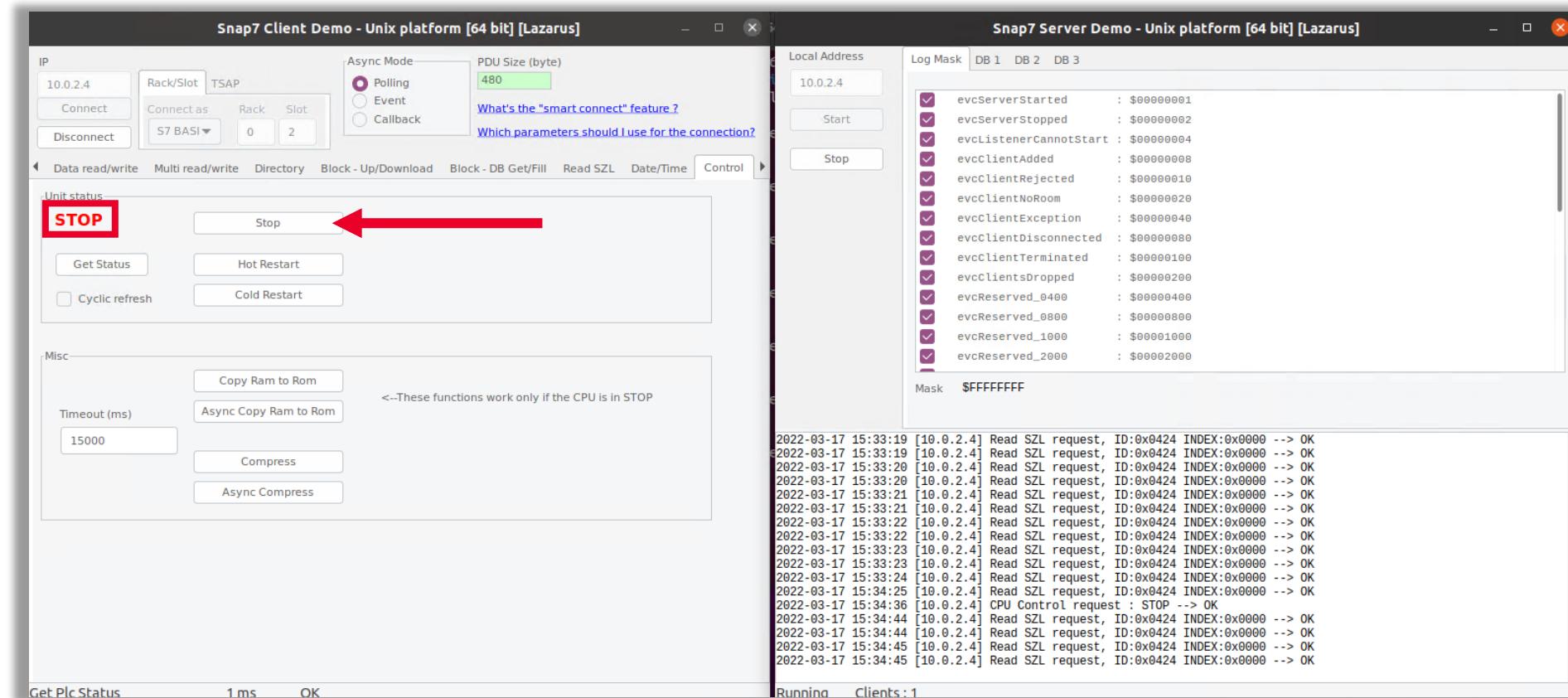


Ilustración 89: Confirma la parada del PLC mediante el botón «stop».



INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Para arrancar el PLC de nuevo, pulsa en el botón «*Hot Restart*». Si en este caso seleccionas la casilla de verificación «*Cyclic refresh*», vemos que automáticamente nos indica que la unidad del PLC está en ejecución, «*RUN*», y en la ventana de la aplicación Snap7 Server Demo podemos comprobar cómo aparece la orden recibida de CPU Control (*Warm Start*), así como se muestra el registro de órdenes recibidas desde la aplicación Snap7 Client Demo.

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

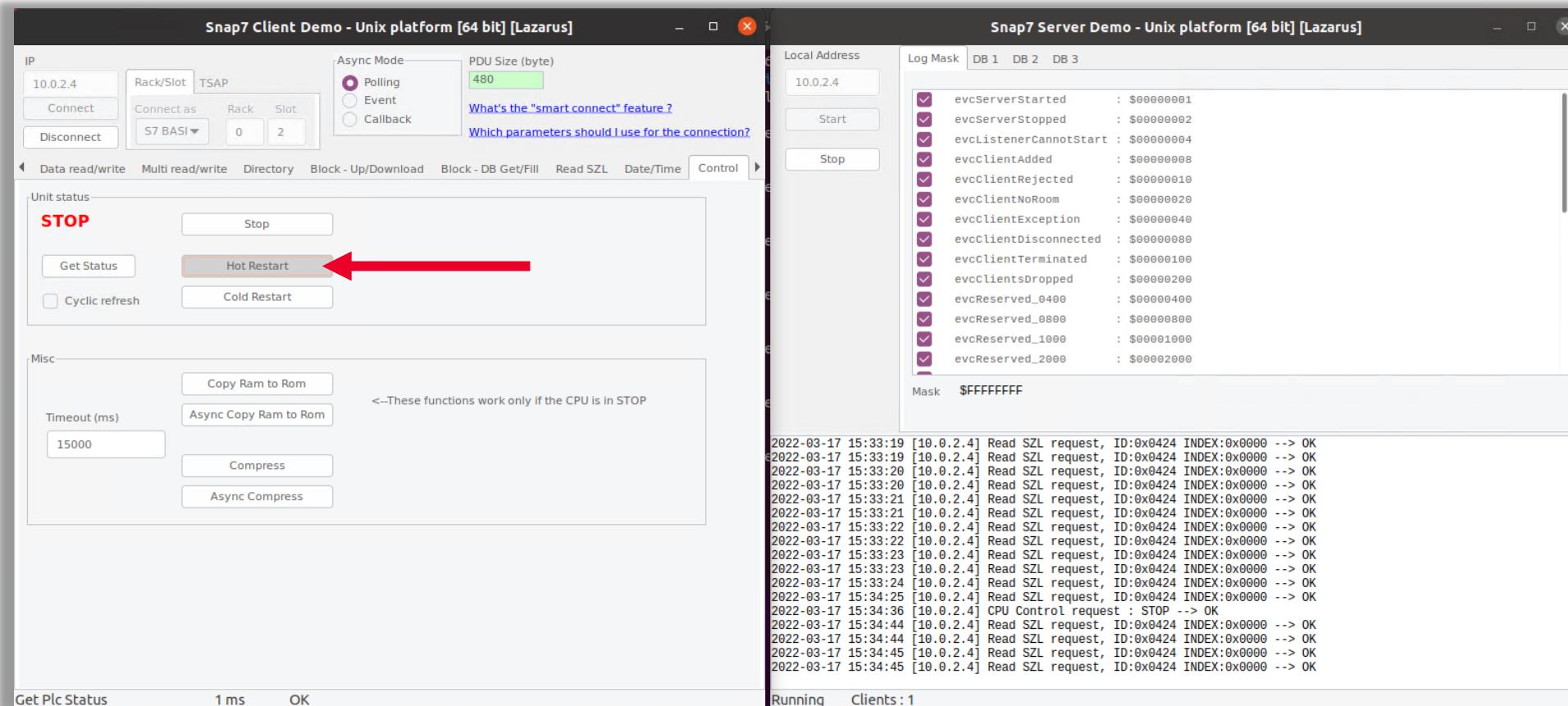


Ilustración 90: Arranque del PLC mediante el botón «Hot Restart».

5

INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

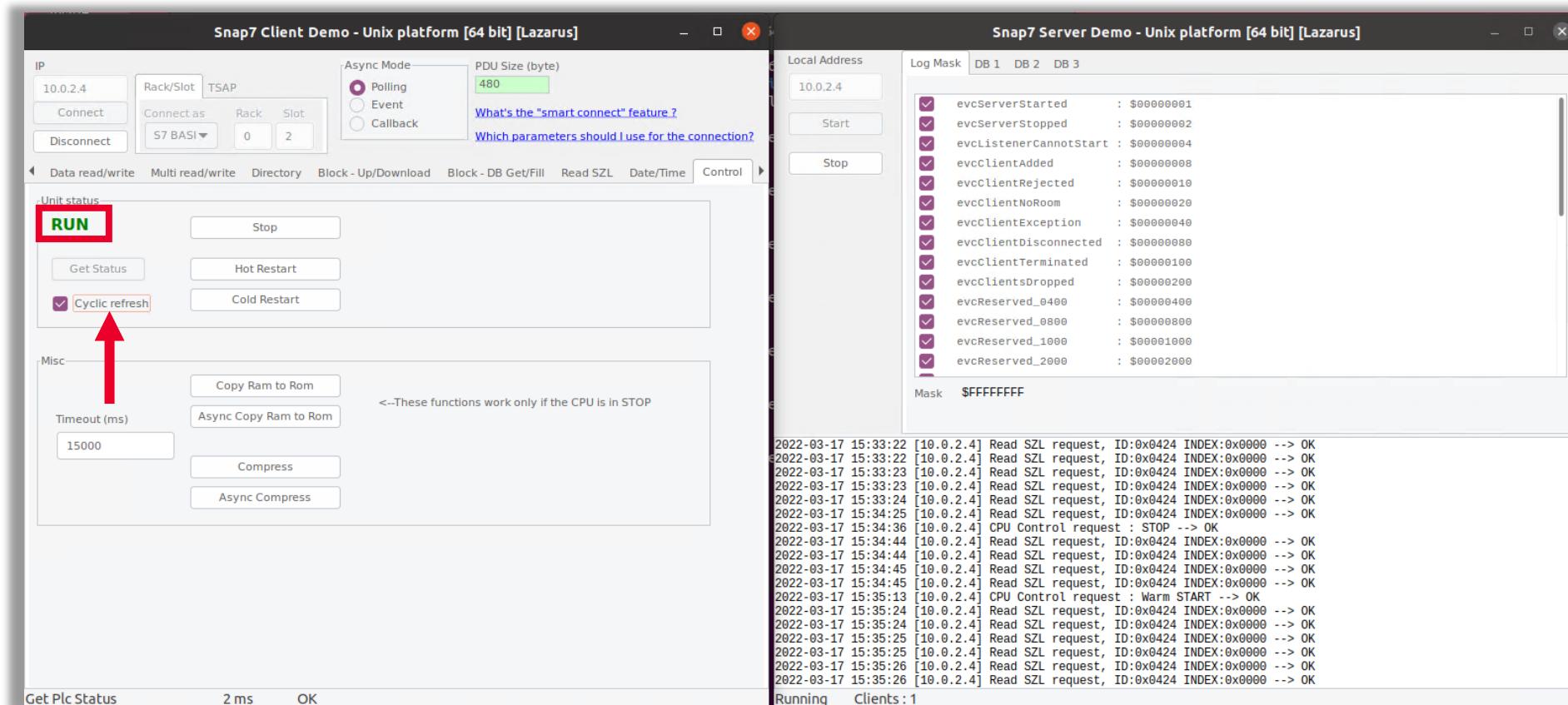


Ilustración 91: Selección de la casilla de verificación «*Cyclic refresh*» que confirma que la unidad del PLC está en «*RUN*».



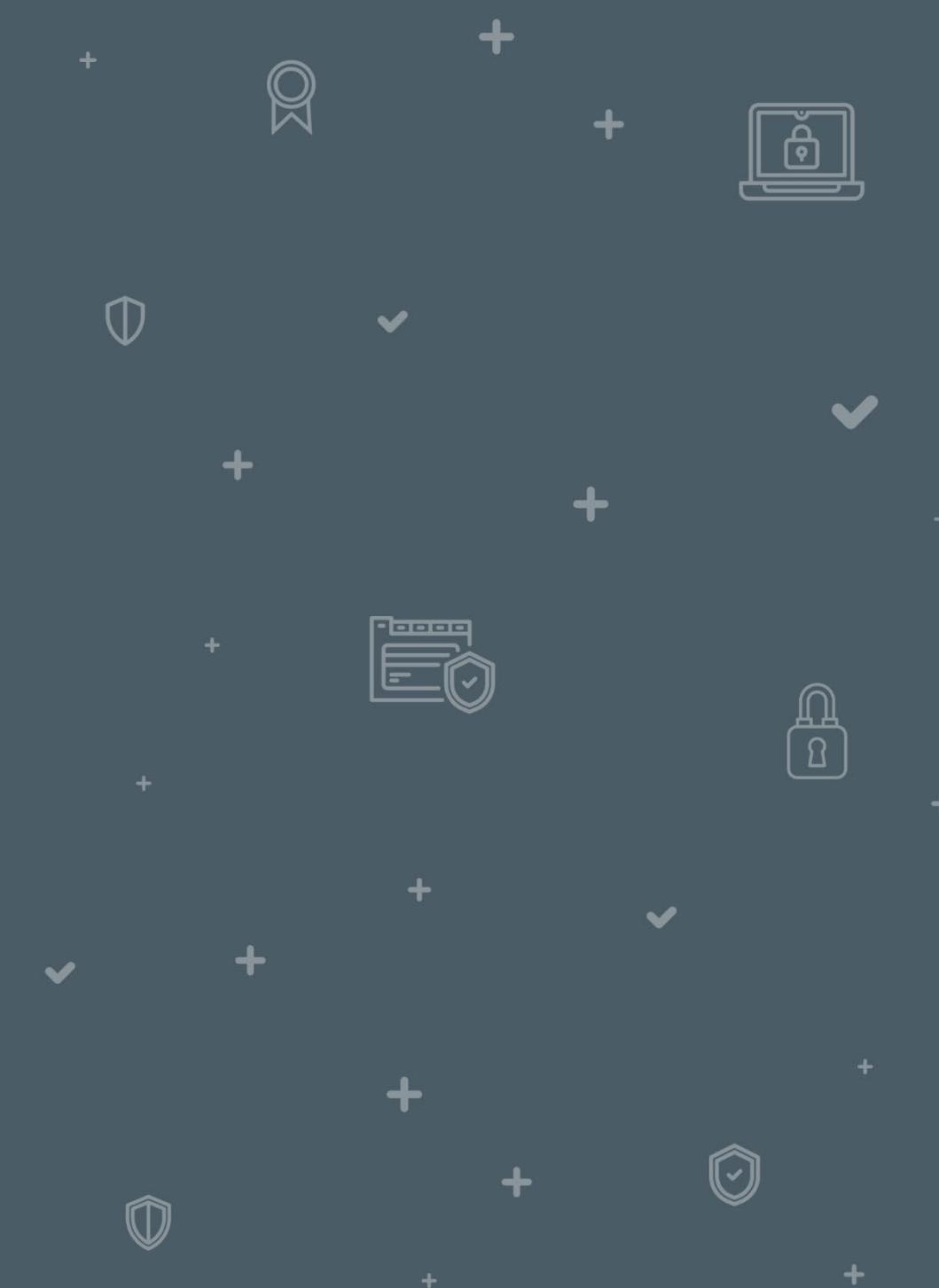
INSTALACIÓN DE HERRAMIENTAS DE SIMULACIÓN DEL PROTOCOLO DE COMUNICACIÓN MODBUS

5.1 Instalación herramientas de simulación de dispositivos Siemens

- Las ventanas de estas dos aplicaciones del paquete de software Snap7, no las cierres ya que volveremos sobre ellas en los siguientes apartados, aunque si pulsas en este orden en el botón de «Disconnect» (en la aplicación Snap 7 Client Demo) y «Stop» (en la aplicación Snap 7 Server Demo).

INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEO DE ACTIVOS: NMAP Y PLCCAN

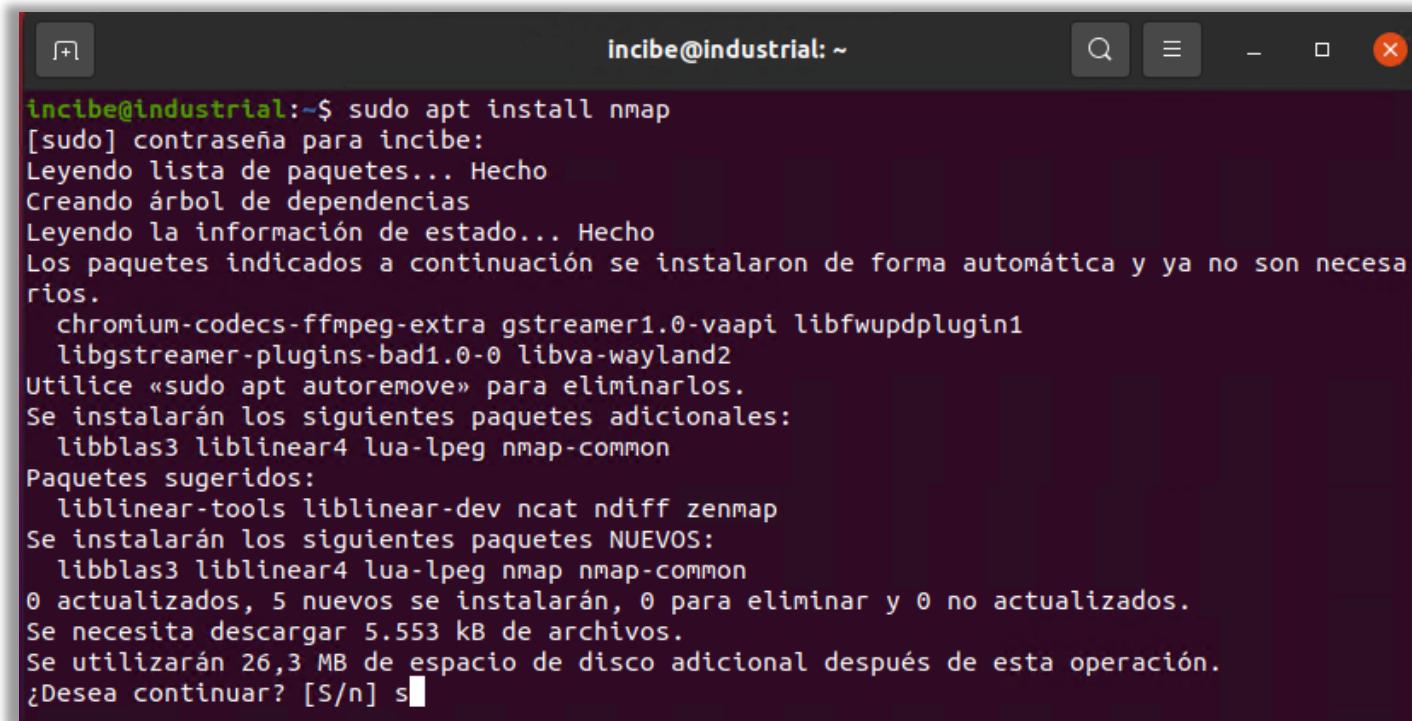
6



6

INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEOS DE ACTIVOS: NMAP Y PLCCAN

- Abre una terminal e instala el paquete de software Nmap.
 - **sudo apt install nmap**



```
incibe@industrial:~$ sudo apt install nmap
[sudo] contraseña para incibe:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libblas3 liblinear4 lua-lpeg nmap-common
Paquetes sugeridos:
  liblinear-tools liblinear-dev ncat ndiff zenmap
Se instalarán los siguientes paquetes NUEVOS:
  libblas3 liblinear4 lua-lpeg nmap nmap-common
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 5.553 kB de archivos.
Se utilizarán 26,3 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Ilustración 92: Instalación de las herramientas de escaneo de activos Nmap y PLCScan.

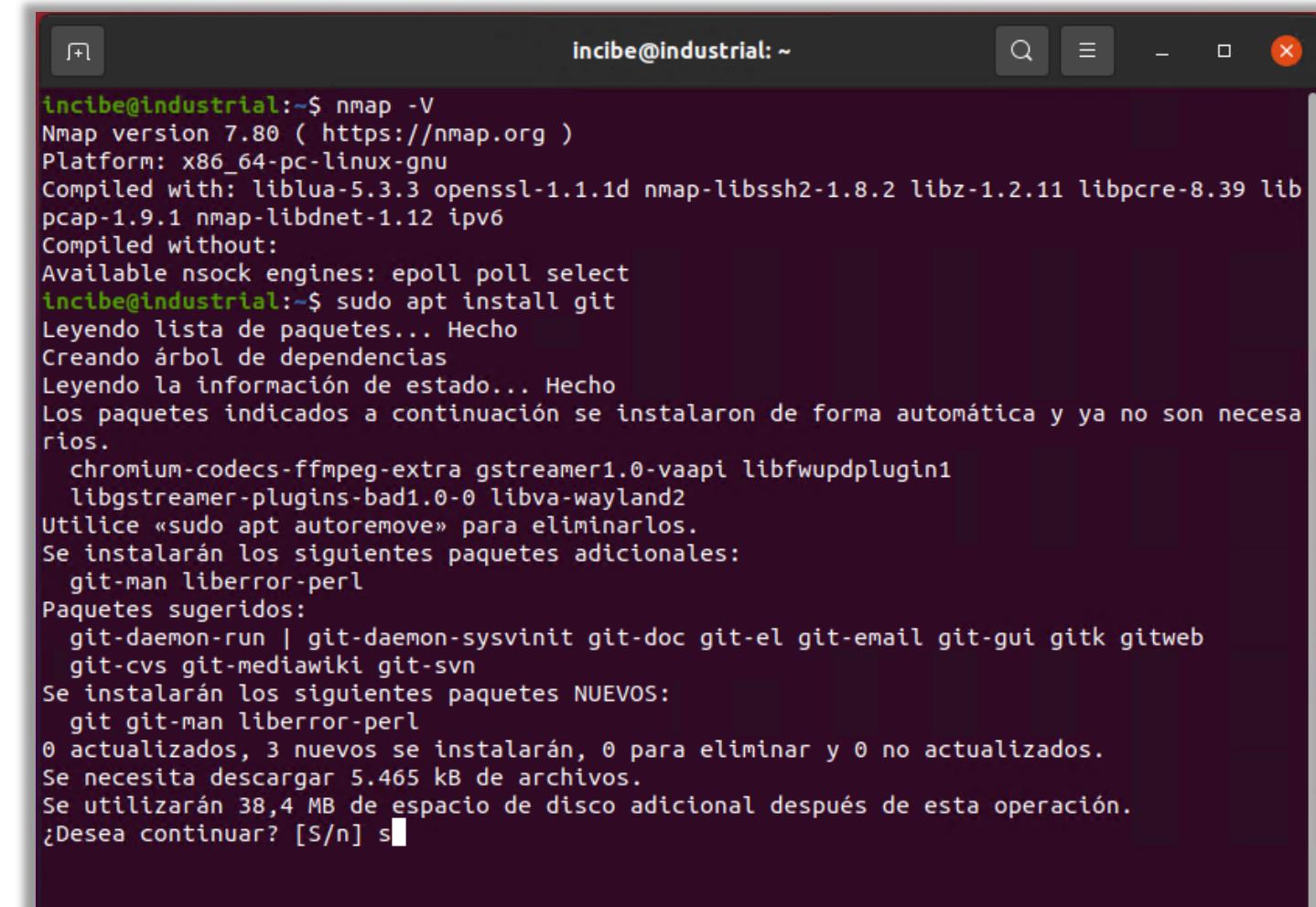
6

INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEOS DE ACTIVOS: NMAP Y PLCCAN

- Tras la instalación, comprueba la versión instalada de la herramienta Nmap (para verificar que se ha instalado correctamente) e instala el paquete de *software git* (de control de versiones), que nos valdrá para descargarnos los repositorios (clonar) de las herramientas que necesiten este tipo de instalación.

- nmap -V**
- sudo apt install git**

Ilustración 93: La versión instalada de la herramienta Nmap e instalación del paquete de *software git*.



```
incibe@industrial:~$ nmap -V
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1d nmap-libssh2-1.8.2 libz-1.2.11 libpcre-8.39 libpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
incibe@industrial:~$ sudo apt install git
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  git-man liberror-perl
Paquetes sugeridos:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk gitweb
  git-cvs git-mediawiki git-svn
Se instalarán los siguientes paquetes NUEVOS:
  git git-man liberror-perl
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 5.465 kB de archivos.
Se utilizarán 38,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```



INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEOS DE ACTIVOS: NMAP Y PLCCAN

- Accede a la carpeta «Documentos», ahí clonarás el repositorio de la herramienta PLCcan. Clonar un repositorio consiste en extraer una copia integral de todos los datos del mismo que existe en GitHub en dicho momento. GitHub es un portal que permite alojar el código de las aplicaciones o proyectos utilizando un sistema de control de versiones. Es uno de los repositorios más conocidos e importantes, donde cualquier persona puede guardar sus proyectos.
 - **cd Documentos/**
 - **git clone https://github.com/meeas/plcscan**



INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEOS DE ACTIVOS: NMAP Y PLCCAN

```
incibe@industrial: ~/Documentos
Se utilizarán 38,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 liberror-perl all 0.17029-1 [26
,5 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 git-man all 1:2.25.1-1u
buntu3.2 [884 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 git amd64 git 1:2.25.1-1ubu
ntu3.2 [4.554 kB]
Descargados 5.465 kB en 10s (575 kB/s)
Seleccionando el paquete liberror-perl previamente no seleccionado.
(Leyendo la base de datos ... 201317 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../liberror-perl_0.17029-1_all.deb ...
Desempaquetando liberror-perl (0.17029-1) ...
Seleccionando el paquete git-man previamente no seleccionado.
Preparando para desempaquetar .../git-man_1%3a2.25.1-1ubuntu3.2_all.deb ...
Desempaquetando git-man (1:2.25.1-1ubuntu3.2) ...
Seleccionando el paquete git previamente no seleccionado.
Preparando para desempaquetar .../git_1%3a2.25.1-1ubuntu3.2_amd64.deb ...
Desempaquetando git (1:2.25.1-1ubuntu3.2) ...
Configurando liberror-perl (0.17029-1) ...
Configurando git-man (1:2.25.1-1ubuntu3.2) ...
Configurando git (1:2.25.1-1ubuntu3.2) ...
Procesando disparadores para man-db (2.9.1-1) ...
incibe@industrial:~$ cd Documentos/
incibe@industrial:~/Documentos$ git clone https://github.com/meeas/plcscan
Clonando en 'plcscan'...
remote: Enumerating objects: 51, done.
remote: Total 51 (delta 0), reused 0 (delta 0), pack-reused 51
Desempaquetando objetos: 100% (51/51), 25.90 KiB | 616.00 KiB/s, listo.
incibe@industrial:~/Documentos$
```

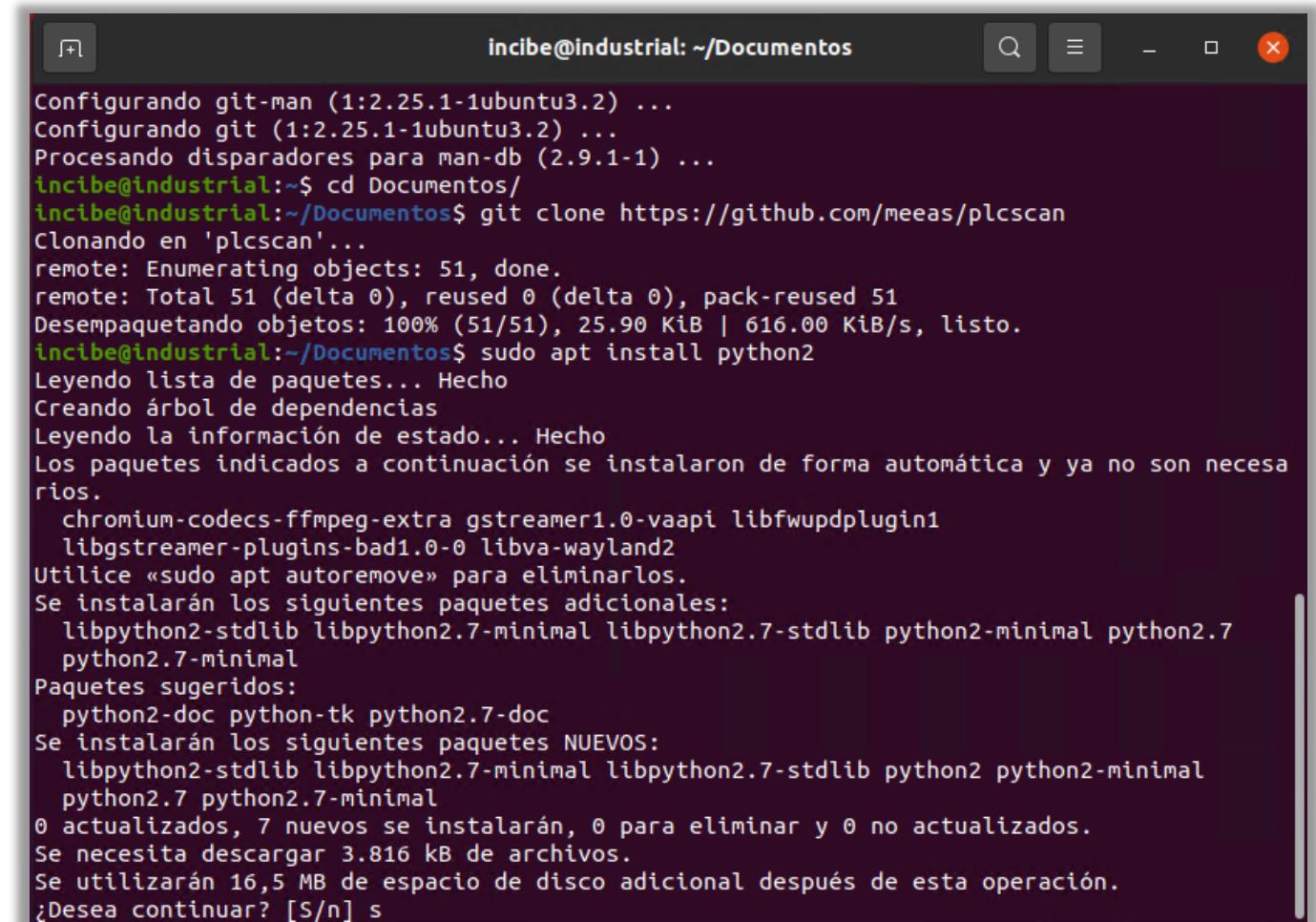
Ilustración 94: Clonación del repositorio de la herramienta PLCcan en la carpeta «Documentos».

6

INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEOS DE ACTIVOS: NMAP Y PLCCAN

- Instala el paquete de software python2 que necesitamos para poder ejecutar la herramienta PLCcan:
 - sudo apt install python2**

Ilustración 95: Instalación del paquete de software python2 necesario para poder ejecutar la herramienta PLCcan.

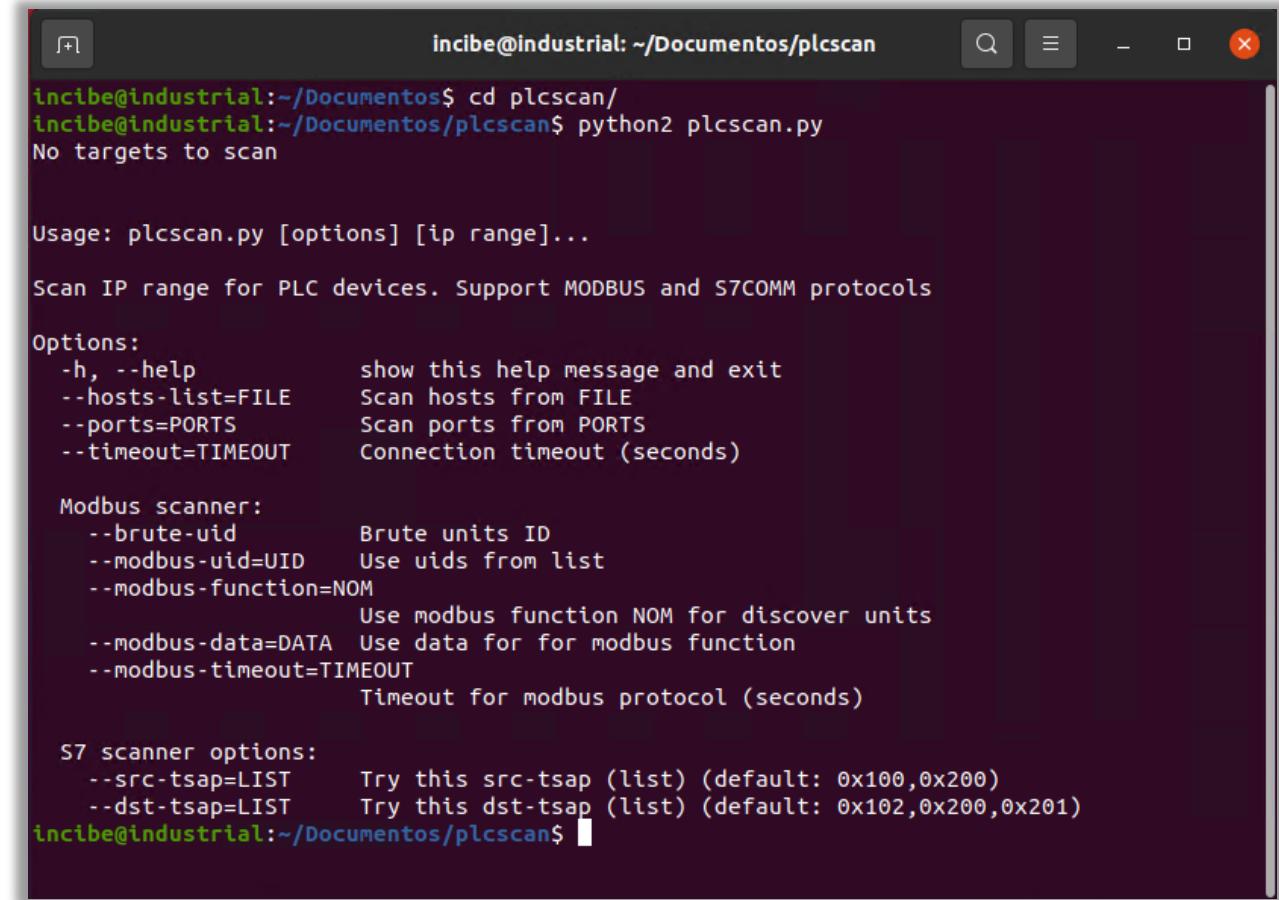


```
incibe@industrial: ~/Documentos
Configurando git-man (1:2.25.1-1ubuntu3.2) ...
Configurando git (1:2.25.1-1ubuntu3.2) ...
Procesando disparadores para man-db (2.9.1-1) ...
incibe@industrial:~/Documentos$ cd Documentos/
incibe@industrial:~/Documentos$ git clone https://github.com/meeas/plcscan
Clonando en 'plcscan'...
remote: Enumerating objects: 51, done.
remote: Total 51 (delta 0), reused 0 (delta 0), pack-reused 51
Desempaquetando objetos: 100% (51/51), 25.90 KiB | 616.00 KiB/s, listo.
incibe@industrial:~/Documentos$ sudo apt install python2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libfwupdplugin1
libgstreamer-plugins-bad1.0-0 libva-wayland2
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
 libpython2.7-stdlib libpython2.7-minimal libpython2.7-stdlib python2-minimal python2.7
 python2.7-minimal
Paquetes sugeridos:
 python2-doc python-tk python2.7-doc
Se instalarán los siguientes paquetes NUEVOS:
 libpython2.7-stdlib libpython2.7-minimal libpython2.7-stdlib python2 python2-minimal
 python2.7 python2.7-minimal
0 actualizados, 7 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 3.816 kB de archivos.
Se utilizarán 16,5 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

6

INSTALACIÓN Y CONFIGURACIÓN DE HERRAMIENTAS DE ESCANEOS DE ACTIVOS: NMAP Y PLCCAN

- Accede a la carpeta PLCScan que nos ha creado la herramienta Git y donde se ha almacenado todo el contenido del repositorio que has clonado anteriormente.
- Ejecuta con python2 el archivo PLCScan.py y comprueba que la herramienta se ejecuta correctamente:
 - **cd plcsan/**
 - **python2 plcsan.py**
- Esta terminal no la cerramos, ya que la necesitamos para la realización de los siguientes apartados y volveremos sobre ella.



A terminal window titled "incibe@industrial: ~/Documentos/plcscan". The user runs "cd plcscan/" followed by "python2 plcscan.py". The output shows the usage information for the script, which scans IP ranges for PLC devices using MODBUS and S7COMM protocols. It details options for hosts, ports, timeout, and specific Modbus and S7 scanner parameters.

```
incibe@industrial:~/Documentos/plcscan$ cd plcscan/
incibe@industrial:~/Documentos/plcscan$ python2 plcscan.py
No targets to scan

Usage: plcscan.py [options] [ip range]...

Scan IP range for PLC devices. Support MODBUS and S7COMM protocols

Options:
-h, --help          show this help message and exit
--hosts-list=FILE   Scan hosts from FILE
--ports=PORTS        Scan ports from PORTS
--timeout=TIMEOUT   Connection timeout (seconds)

Modbus scanner:
--brute-uid         Brute units ID
--modbus-uid=UID    Use uids from list
--modbus-function=NOM
                     Use modbus function NOM for discover units
--modbus-data=DATA   Use data for for modbus function
--modbus-timeout=TIMEOUT
                     Timeout for modbus protocol (seconds)

S7 scanner options:
--src-tsap=LIST      Try this src-tsap (list) (default: 0x100,0x200)
--dst-tsap=LIST      Try this dst-tsap (list) (default: 0x102,0x200,0x201)
incibe@industrial:~/Documentos/plcscan$
```

Ilustración 96: Comprobación que la herramienta se funciona correctamente ejecutando con python2 el archivo PLCcan.py.

7

CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

- 7.1 Ejecución de aplicaciones QModMaster y ModbusPal
- 7.2 Creación del esclavo nº1
- 7.3 Establecer comunicación entre Modbus TCP y lectura de datos

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

En este apartado vamos a crear un esclavo en la aplicación ModbusPal y vamos a establecer la comunicación Modbus TCP con la aplicación QModMaster para la lectura de los datos. Para que puedas realizar y comprender estas prácticas es importante que sepas que podemos encontrar diferentes tipos de datos:

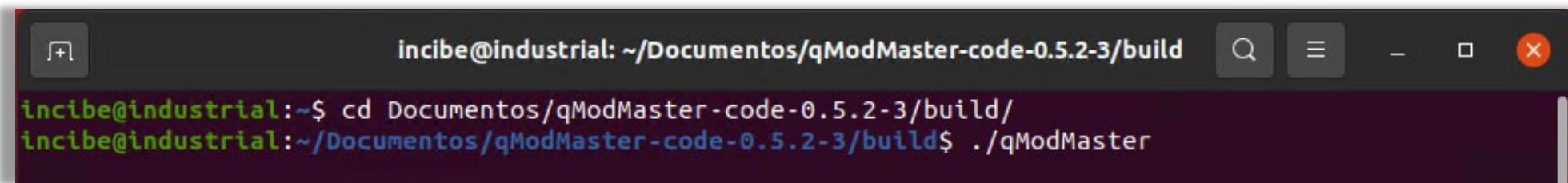
- Las *coils* son nombres de direcciones de memoria, es decir, son registros o nombres de variables predefinidas de tipo booleano (esto es, aquel que puede representar valores de lógica binaria, es decir, 2 valores, que suelen asociarse con verdadero o falso, siendo 1 verdadero y 0 falso), y que pueden ser leídas o escritas.
- Los *holding registers*, al igual que las *coils*, son nombres de direcciones de memoria que permiten almacenar datos de tipo integer (esto es, números enteros).

Si tienes la ventana de la aplicación ModbusPal abierta, avanza directamente al apartado «[7.2 Creación del esclavo nº1](#)».

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.1 Ejecución de aplicaciones QModMaster y ModbusPal

- Si has cerrado la ventana de la aplicación QModMaster, abre una nueva terminal y sitúate en la carpeta «*build*» que creamos anteriormente, ahí ejecuta la aplicación QModMaster, como ya has aprendido:
 - **cd Documentos/qModMaster-code-0.5.2.3/build/**
 - **./qModMaster**



A screenshot of a terminal window titled "incibe@industrial: ~/Documentos/qModMaster-code-0.5.2-3/build". The window shows two command-line entries: "cd Documentos/qModMaster-code-0.5.2-3/build/" and "./qModMaster". The terminal interface includes standard window controls (minimize, maximize, close) and a search bar.

Ilustración 97: Ejecución de la aplicación QModMaster en la carpeta «*build*».

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.1 Ejecución de aplicaciones QModMaster y ModbusPal

- Si has cerrado la ventana de la aplicación ModbusPal, abre una nueva terminal y ejecuta los siguientes comandos para acceder a la carpeta donde se encuentra la aplicación ModbusPal y ejecutar la aplicación (con el comando sudo, que nos fuerza a que introduzcamos la contraseña de súper usuario):
 - **cd /Documentos/modbuspal**
 - **sudo java -jar ModbusPal.jar**

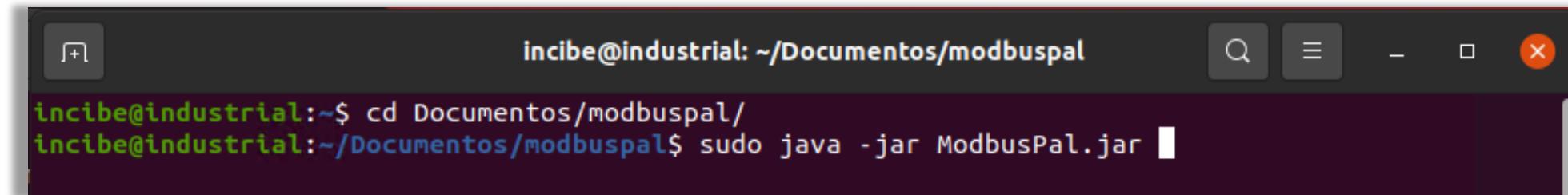


Ilustración 98: Consola donde se ejecuta la aplicación ModbusPal.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- Deberás tener ambas aplicaciones QModMaster y ModbusPal ejecutándose, como se muestran en la imagen:

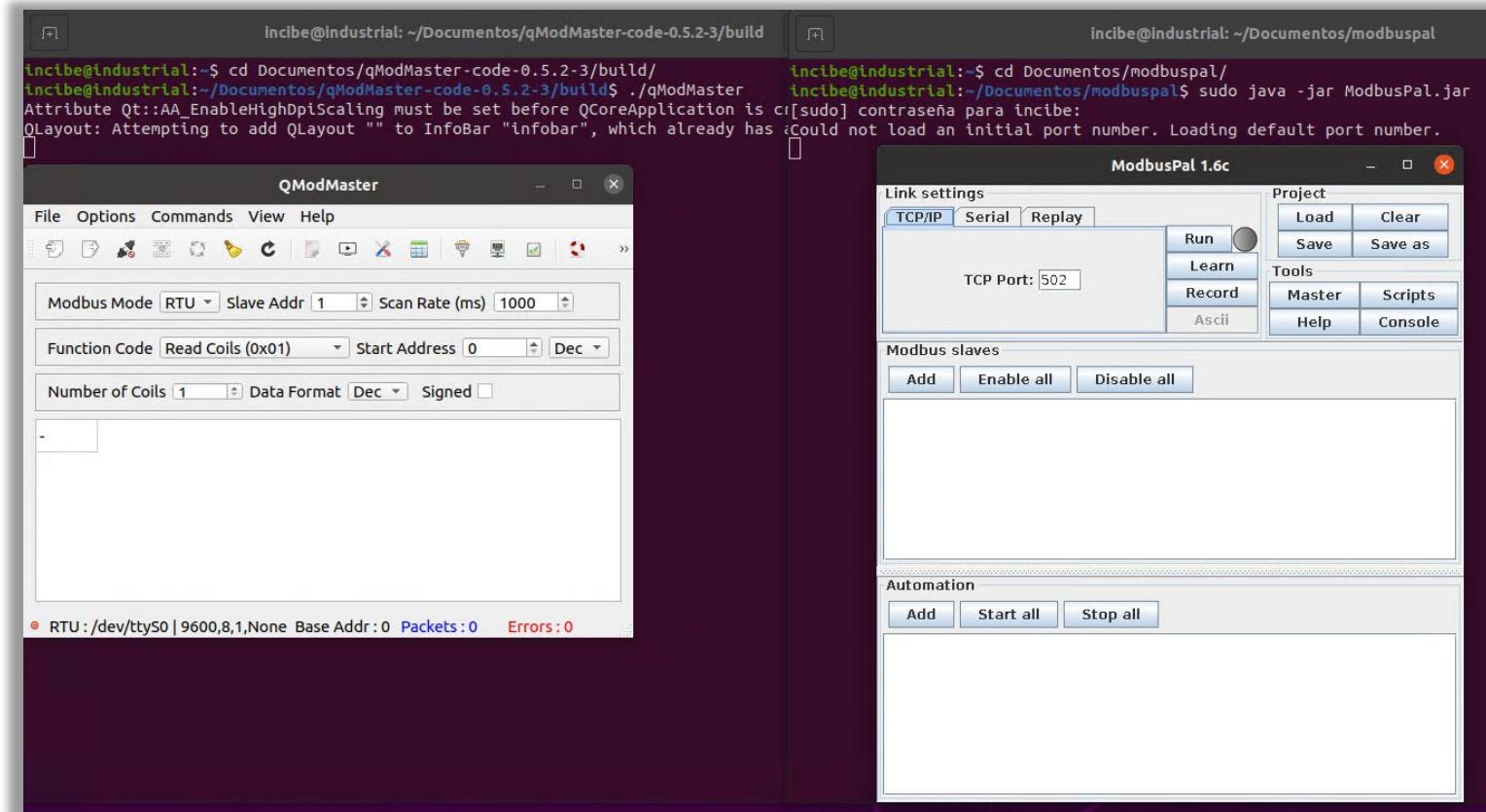


Ilustración 99: Aplicaciones QModMaster y ModbusPal ejecutándose.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- En ModbusPal vamos a añadir un nuevo esclavo.
Lo haremos pulsando en el botón «Add».

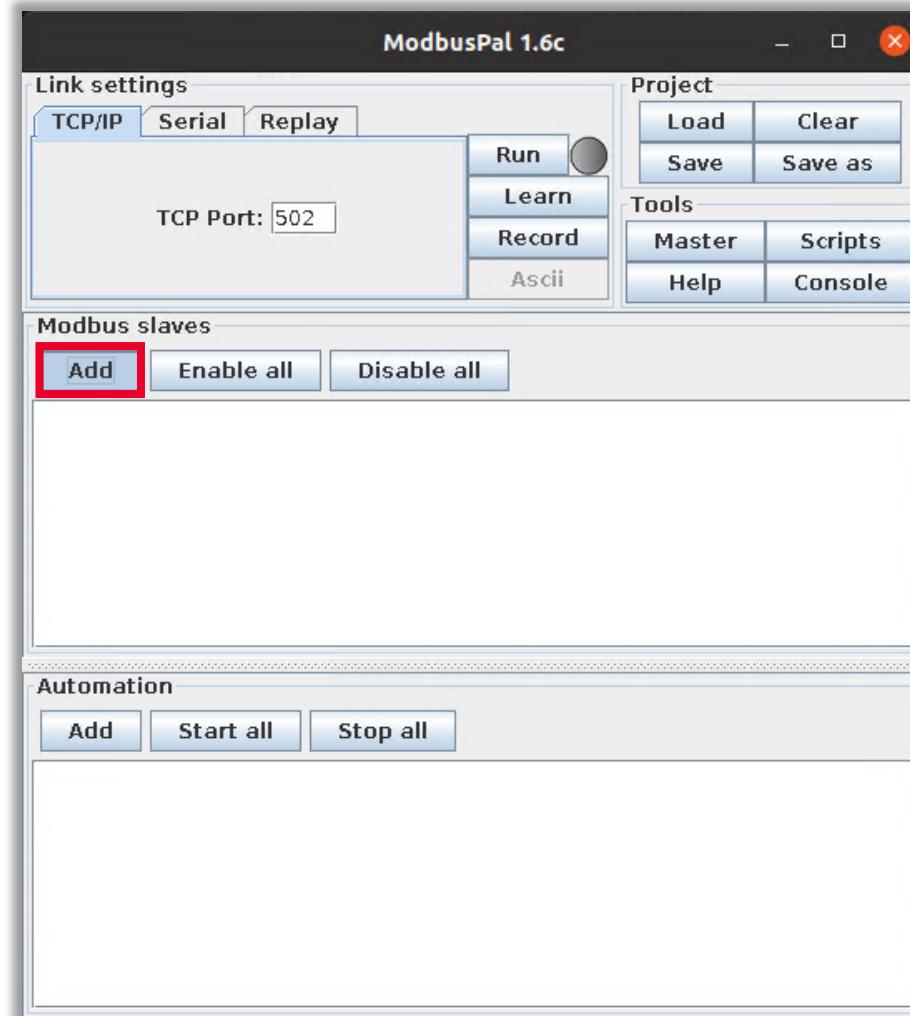


Ilustración 100: Añadir un nuevo esclavo en ModbusPal mediante el botón «Add».

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- En la ventana emergente que nos aparece, rellenamos los siguientes campos, como se muestra en la imagen, y pulsa en el botón «Add»:
 - En el campo «Add slave» siempre tenemos que escribir un número.
 - En el campo «Slave name» escribimos un nombre identificativo.

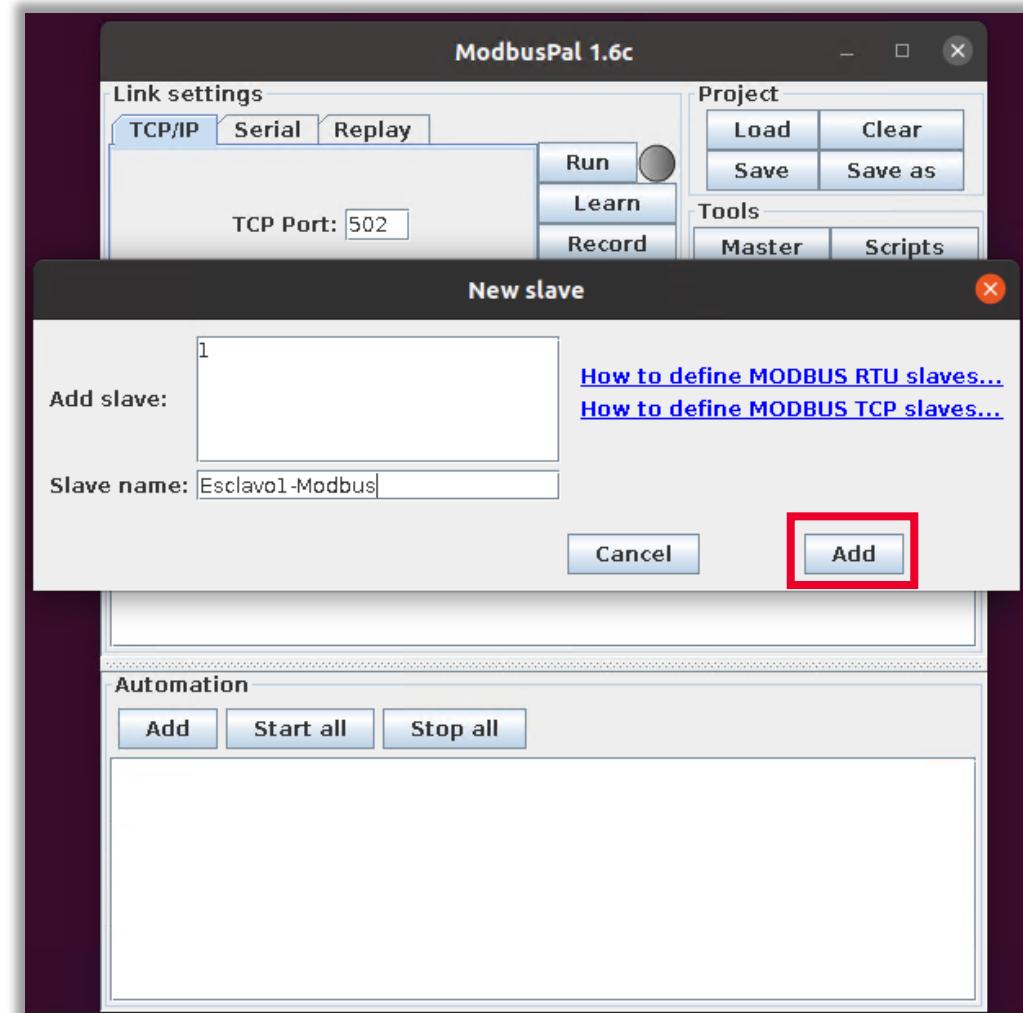


Ilustración 101: Añadir nuevo esclavo.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- Para editar el esclavo, pulsa sobre el icono que representa a un ojo que aparece en la entrada del esclavo que acabamos de crear.

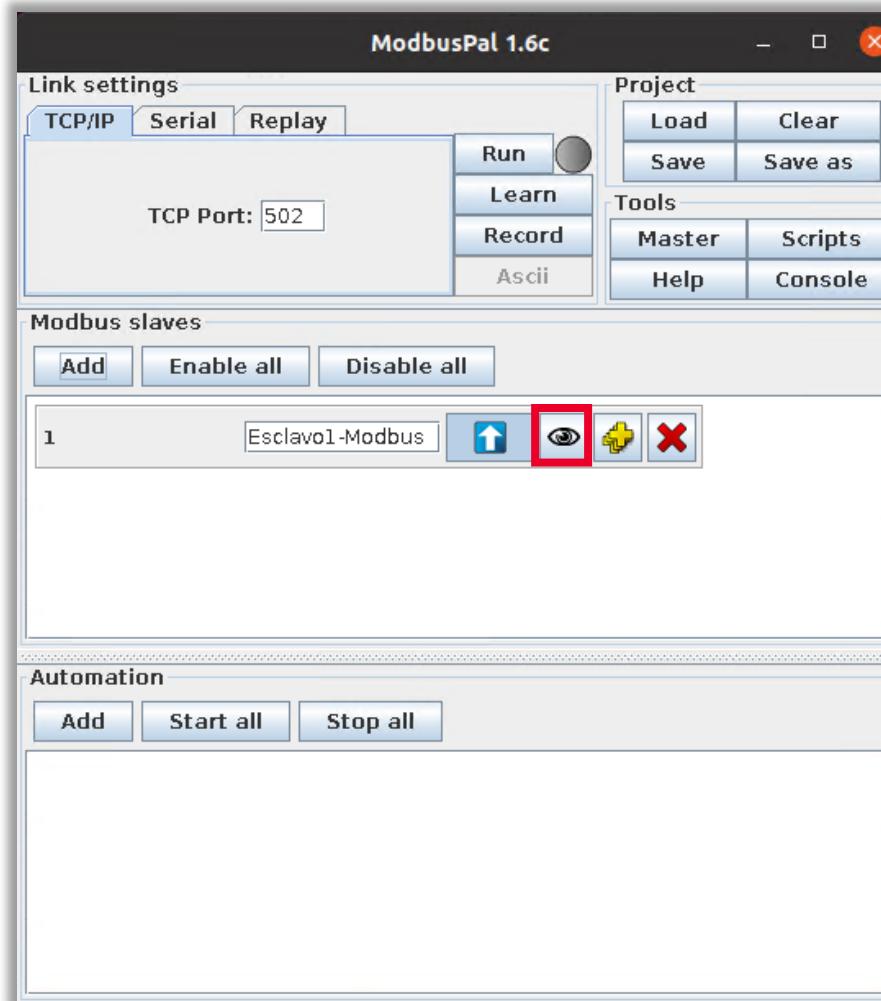


Ilustración 102: Edición del esclavo.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- En la ventana emergente que nos aparece, pulsa la pestaña «*Coils*», y después pulsa sobre el botón «*Add*».

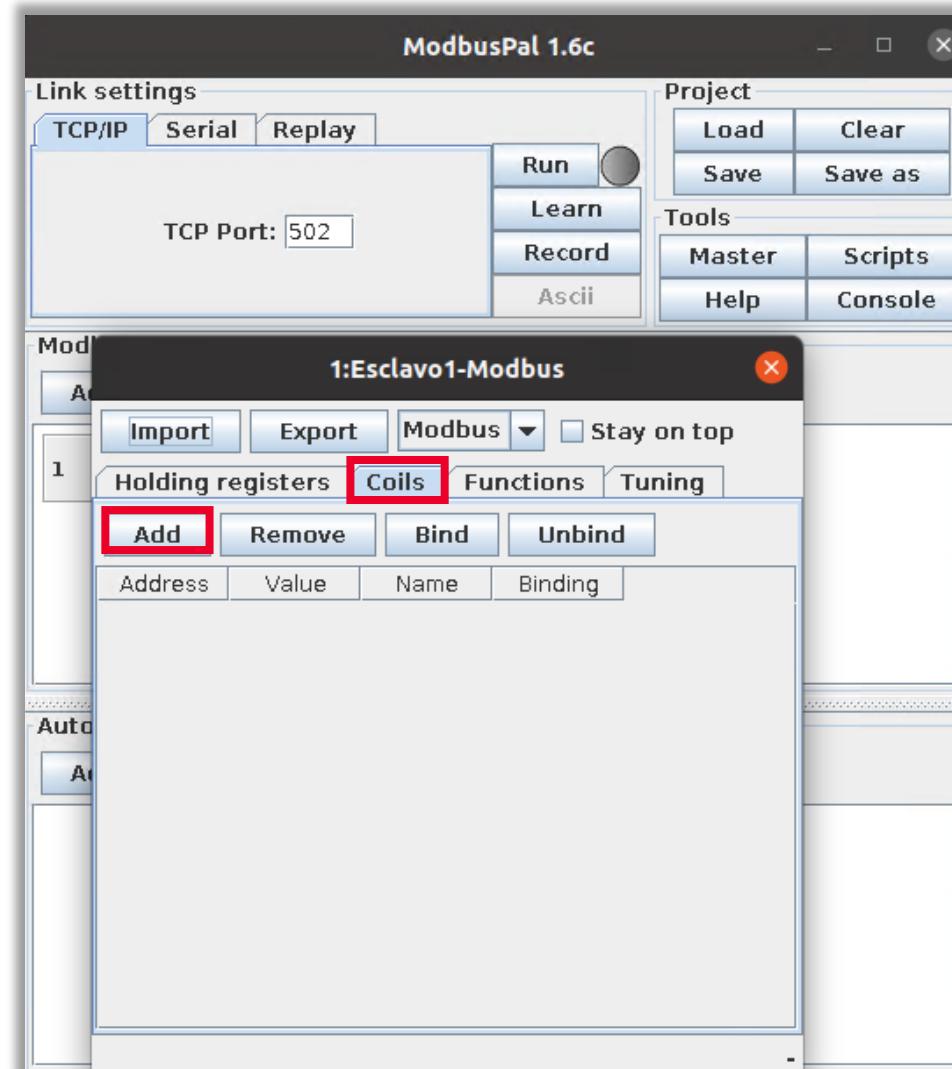


Ilustración 103: Ventana emergente donde hay que acceder a la pestaña «*Coils*», y pulsar sobre el botón «*Add*».

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

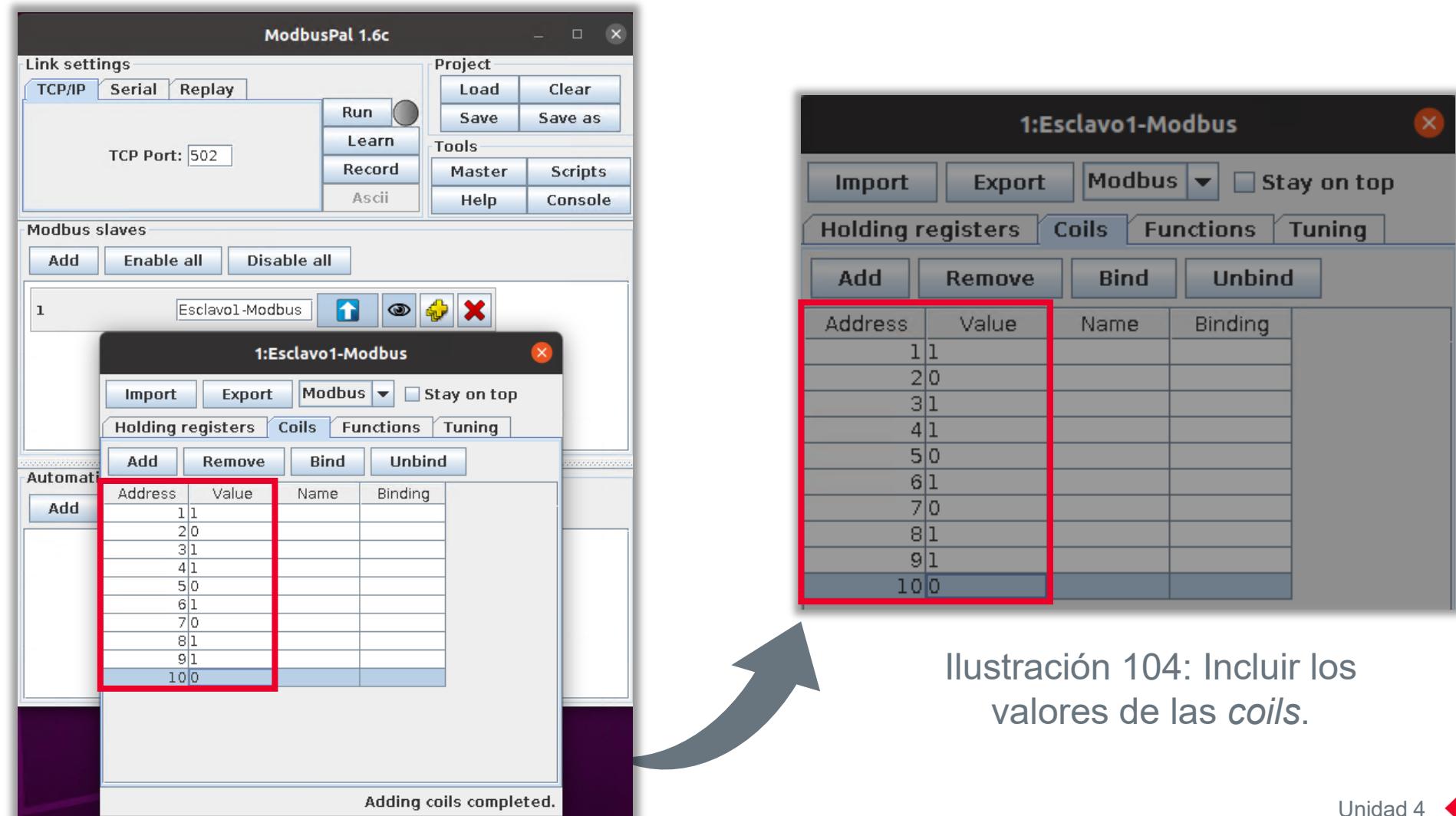
7.2 Creación del esclavo nº1

- Nos aparece una nueva ventana emergente y para añadir diez columnas (tomamos este valor como ejemplo representativo) rellenamos los campos con los siguientes valores:
 - From: 1.
 - To: 10.
- Después editamos los valores de las *coils* como aparece en la imagen de la siguiente diapositiva.

Nota: estos valores son inventados, puedes elegir los que quieras, sin embargo, recomendamos seguir estos pasos para que puedas ver cómo se desarrolla todo con los mismos valores y evitar posibles confusiones.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1



7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- En la pestaña «*Holding registers*», pulsa sobre el botón «*Add*».

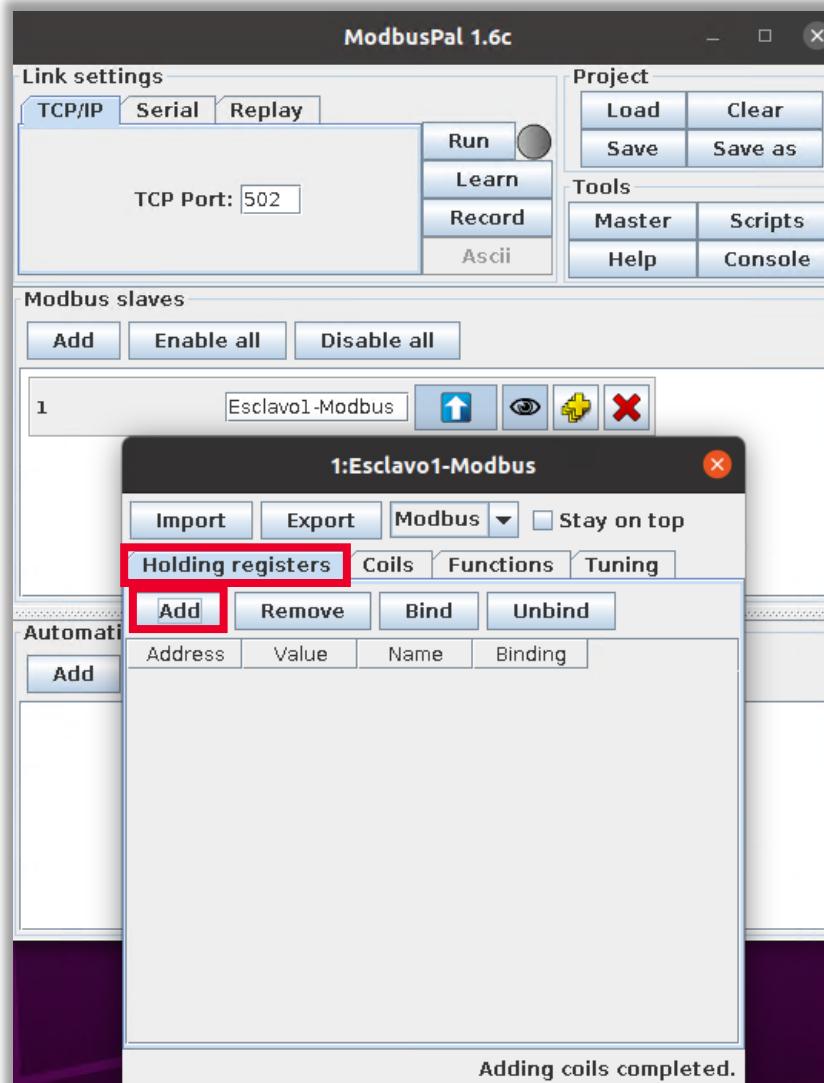


Ilustración 105: Pestaña «*Holding registers*».

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- Añadimos los siguientes registros según aparece en la imagen.

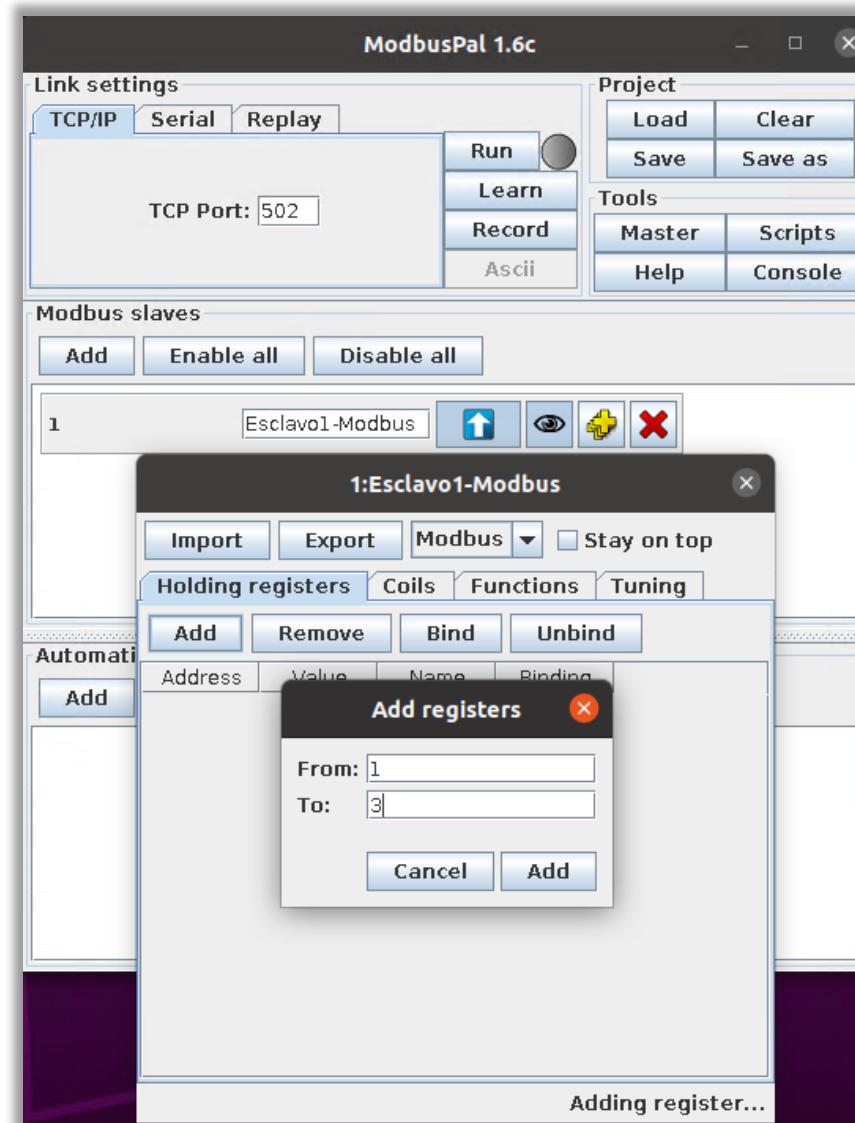


Ilustración 106: Introducir los parámetros «From: 1» y «To: 3».

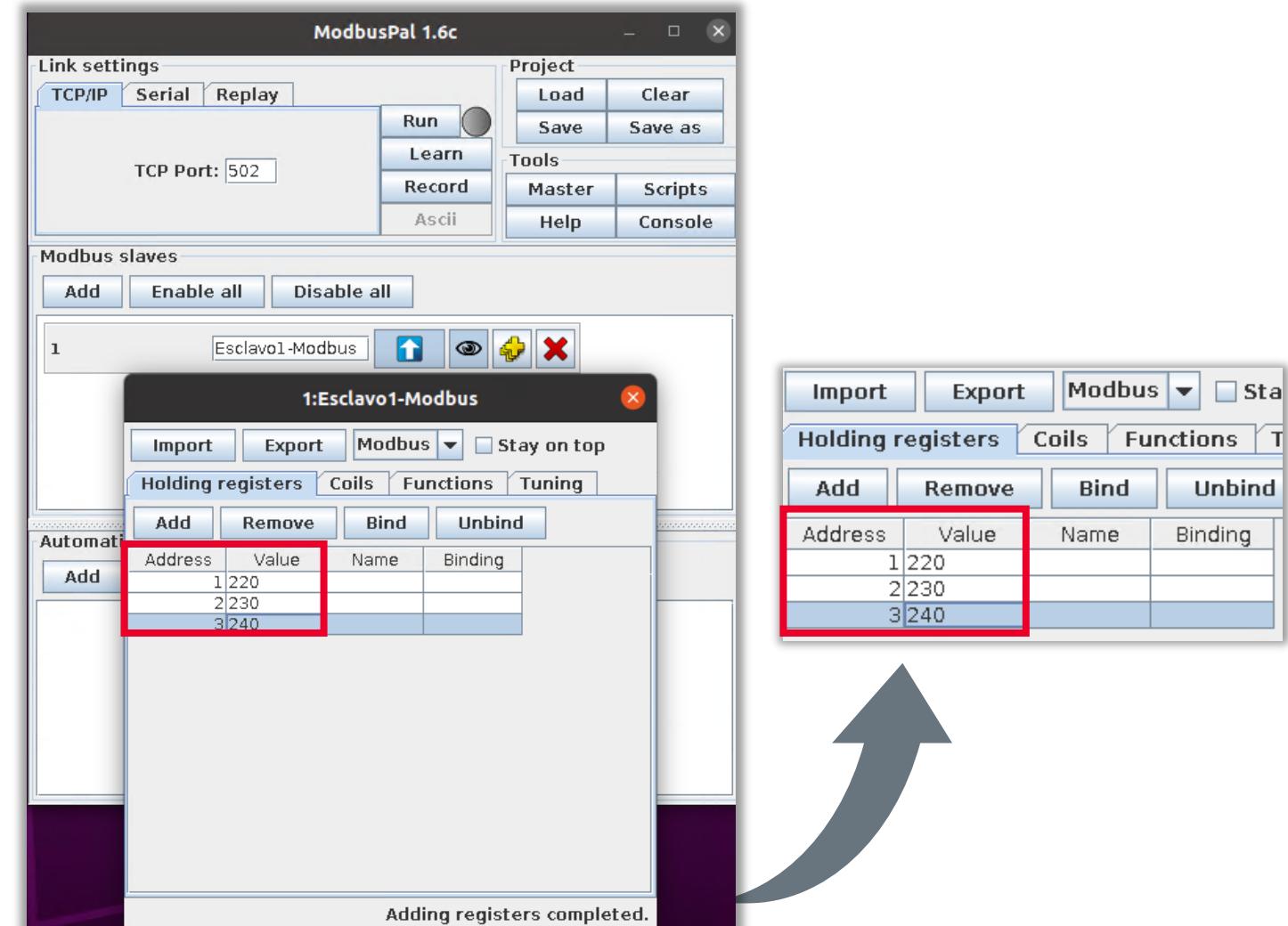
7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.2 Creación del esclavo nº1

- Editamos los valores de los campos de los tres *Holding registers* como aparece en la siguiente imagen (utilizamos estos valores como ejemplo):

Nota: de nuevo, estos valores son inventados, pero recomendamos al alumno que los siga.

Ilustración 107: Edición de los valores de los campos de los tres *Holding registers*.



7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- En la aplicación QModMaster, selecciona en el menú «Options > Modbus TCP».

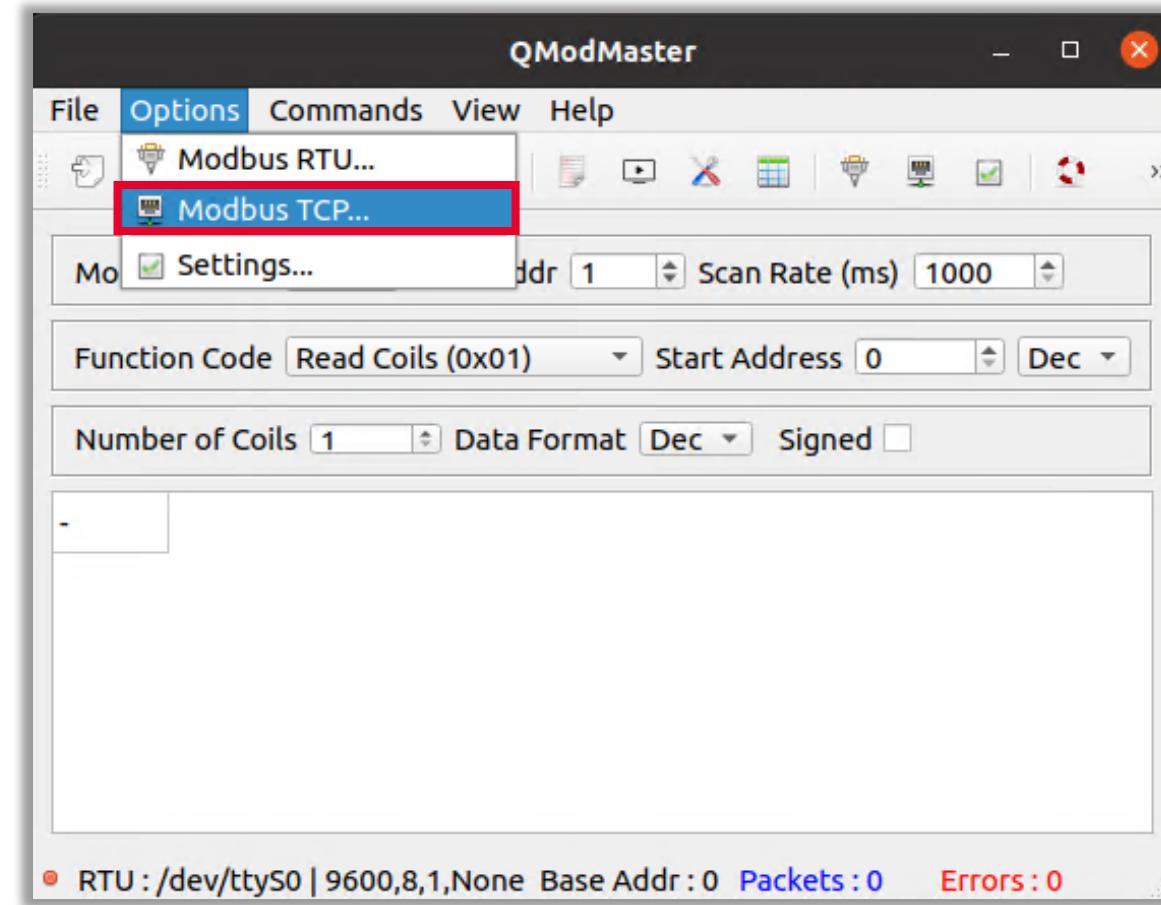


Ilustración 108: Selección de «Modbus TCP» en el menú «Options» en la aplicación QModMaster.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- Nos aparece una ventana que nos muestra los valores por defecto para establecer la comunicación Modbus TCP.
 - La dirección IP que aparece es la del esclavo (la dirección IP 127.0.0.1 es la de *localhost* que hace referencia a la dirección IP de nuestro propio equipo) a la que se va a conectar la aplicación QModMaster y el puerto TCP que aparece es el 502 que es el puerto que se utiliza para el protocolo Modbus TCP.

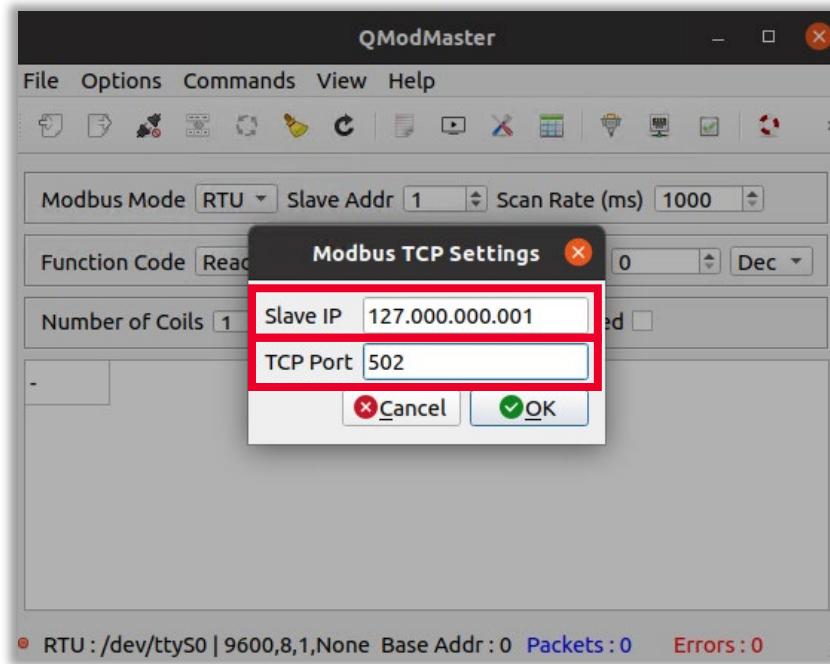


Ilustración 109: Dirección IP a la que se va a conectar la aplicación QModMaster.

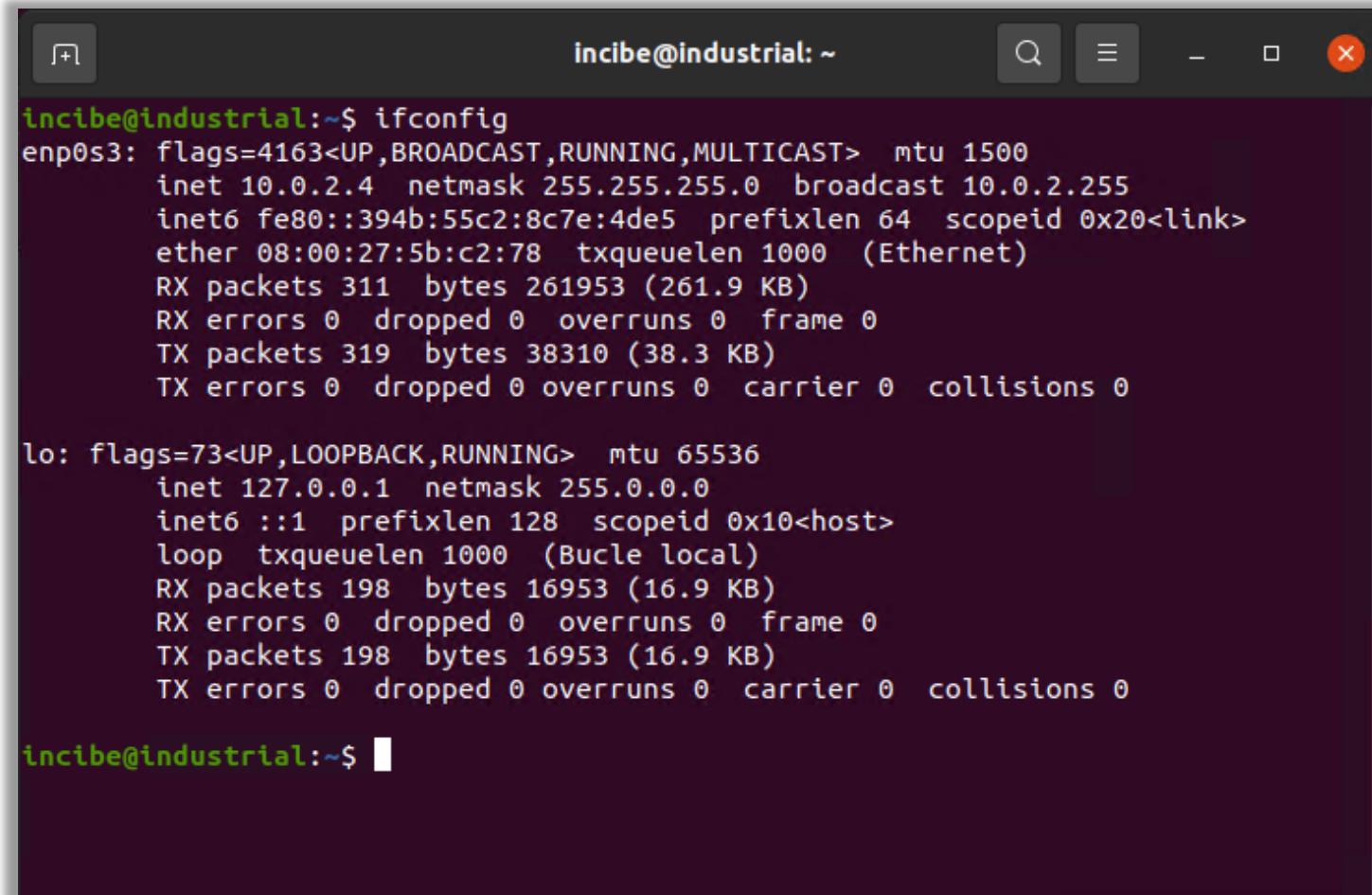
7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- Aunque podríamos dejar el valor que aparece por defecto en el campo Slave IP, vamos a introducir la dirección IP que tiene asignada nuestro equipo, distinta a la de *localhost*.
- Para refrescar este dato (porque ya lo conocíamos previamente), abre una nueva terminal, y ejecuta el comando:
 - **Ifconfig**
- En nuestro caso, la dirección IP que buscamos es la que nos aparece en la entrada `enp0s3` que es nuestra interfaz de red que tiene la dirección IP asignada de 10.0.2.4.

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos



A terminal window titled "incibe@industrial: ~" displaying the output of the "ifconfig" command. The output shows two network interfaces: "enp0s3" and "lo". The "enp0s3" interface has an IP address of 10.0.2.4 and a netmask of 255.255.255.0, with a broadcast address of 10.0.2.255. The "lo" interface is a loopback interface with an IP address of 127.0.0.1 and a netmask of 255.0.0.0.

```
incibe@industrial:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
                inet6 fe80::394b:55c2:8c7e:4de5  prefixlen 64  scopeid 0x20<link>
                  ether 08:00:27:5b:c2:78  txqueuelen 1000  (Ethernet)
                    RX packets 311  bytes 261953 (261.9 KB)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 319  bytes 38310 (38.3 KB)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopeid 0x10<host>
                  loop  txqueuelen 1000  (Bucle local)
                    RX packets 198  bytes 16953 (16.9 KB)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 198  bytes 16953 (16.9 KB)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

incibe@industrial:~$
```

Ilustración 110: Comando ifconfig para actualizar la dirección IP.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- De nuevo regresamos a la aplicación «QModMaster > Options > ModbusTCP» e introducimos los siguientes valores en los campos:

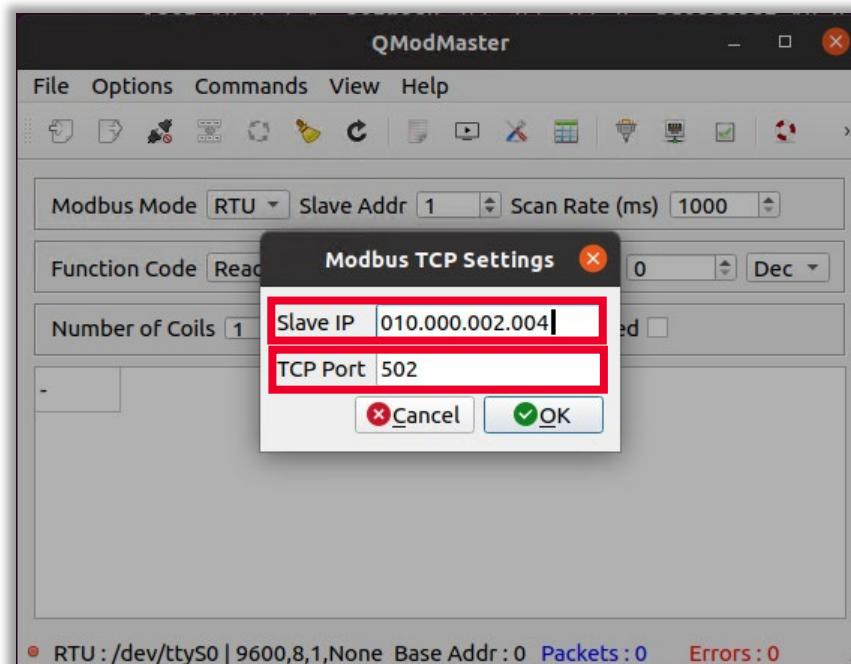


Ilustración 111: Introducción de valores «slave IP» y «TCP Port» en los ajustes de Modbus TCP en QModMaster.

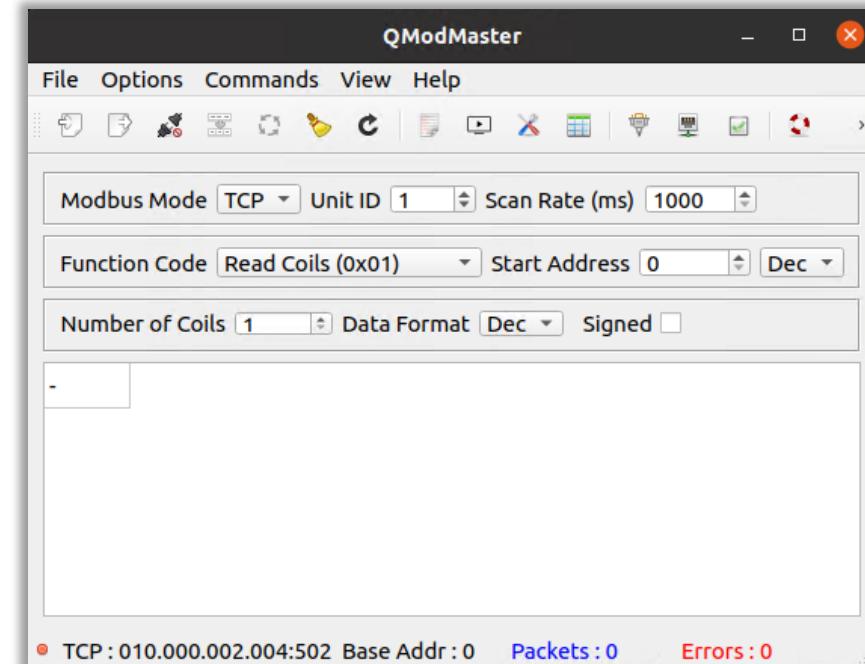


Ilustración 112: QModMaster tras los valores aplicados.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- Ahora volvemos a la aplicación ModbusPal, y pulsa el botón «Run». Esto es necesario para que posteriormente se pueda establecer la comunicación Modbus TCP desde la aplicación QModMaster.

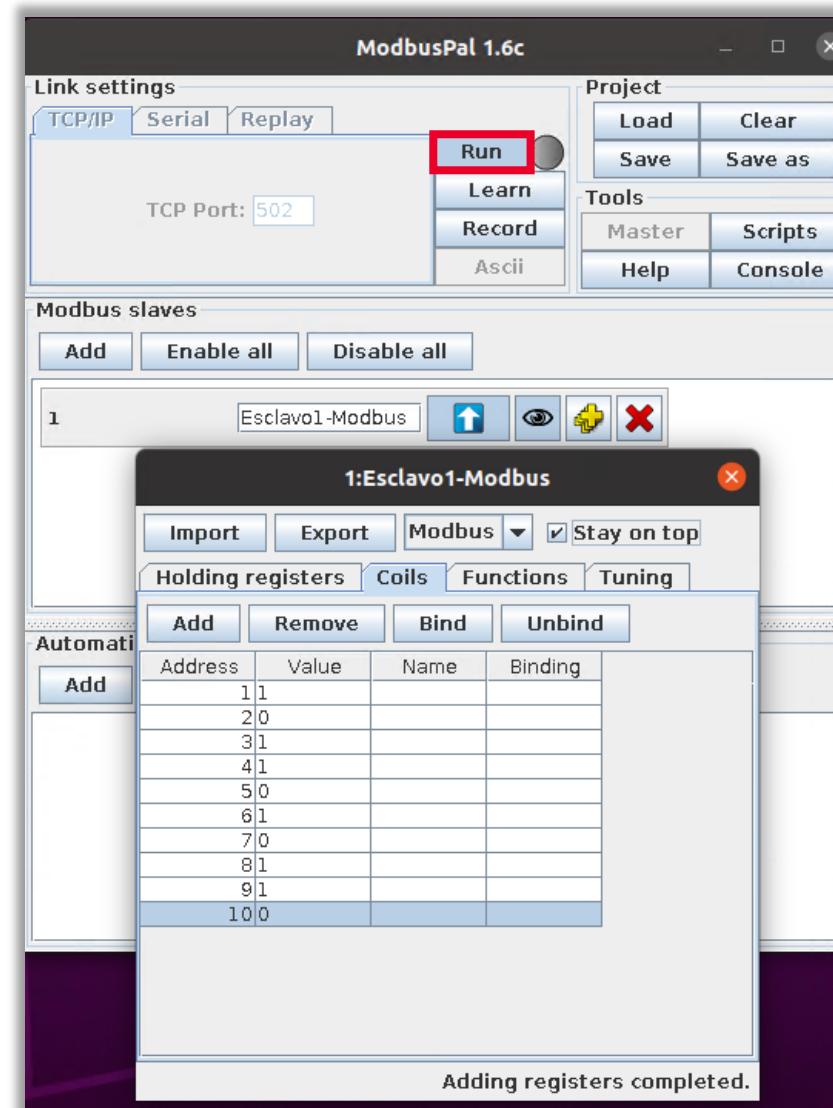


Ilustración 113: Botón «Run» en la aplicación ModbusPal.

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- De nuevo en la aplicación QModMaster, aunque ya podríamos establecer la comunicación con el esclavo nº1 que está ejecutándose en la aplicación ModbusPal, vamos a realizar los ajustes necesarios para poder leer los datos de este esclavo nº1.
- En la imagen de la siguiente diapositiva observarás que en el campo «*Unit ID*» indica el número del esclavo, en nuestro caso, el 1. «*Start Address*» es el campo que representa la dirección del esclavo desde la que queremos leer los datos, la dejamos en 0. En «*Modbus Mode*» debe estar seleccionada la opción de TCP. Por último, el campo «*Number of Coils*» debe de coincidir con el número de *coils* que queremos leer en el esclavo, en nuestro caso incrementamos el valor hasta el número 10.
 - El campo «*Function Code*», por defecto está establecido en «*Read Coils (0x01)*», que es la función que vamos a utilizar para leer los valores de las *coils* en el esclavo.

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

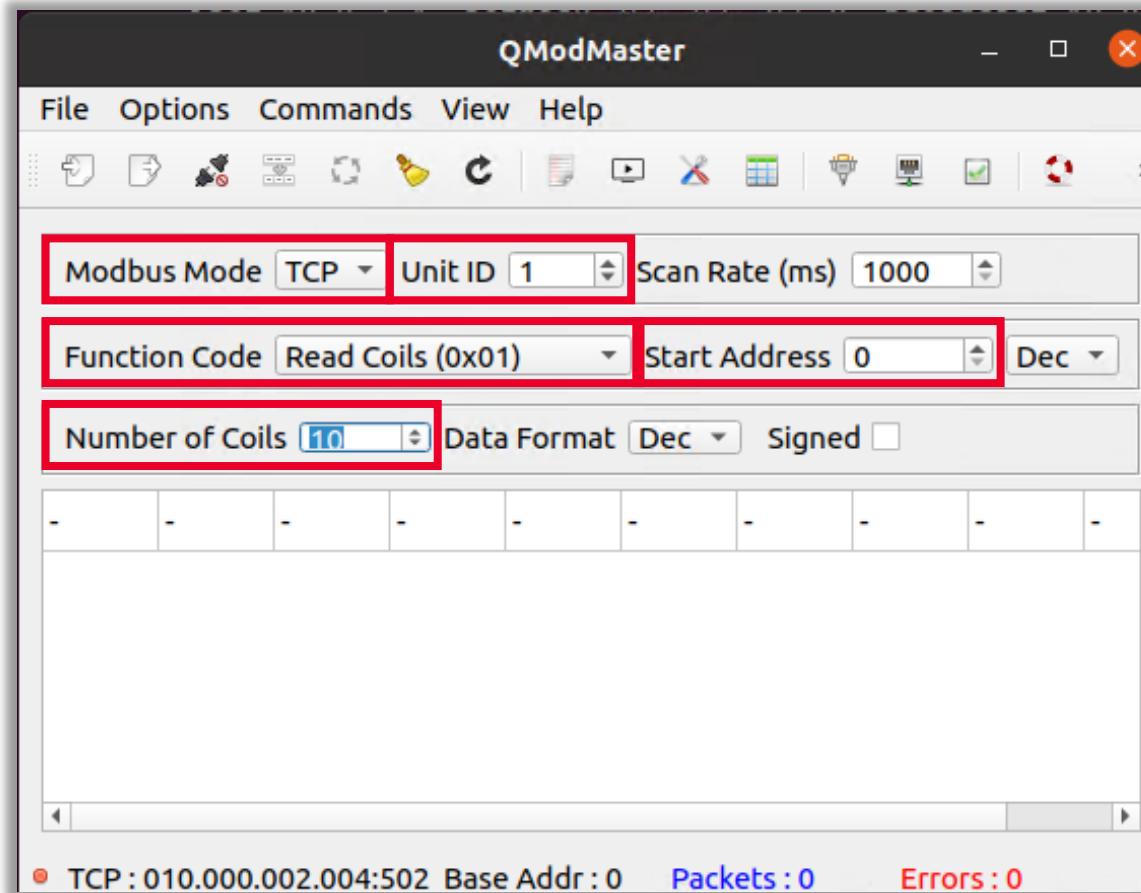


Ilustración 114: Parámetros: *Unit ID*: 1; *Start Address*: 0; *Number of Coils* debe ser el número de *coils* que se quieren leer en el esclavo; *Modbus Mode*: TCP.



7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- Pulsa sobre el botón representado por dos enchufes en la fila de botones, tercer botón empezando por la izquierda, (que es el botón utilizado para conectar y desconectar la comunicación), con esto establecemos la conexión Modbus TCP.
 - Una vez establecida la conexión, solo nos queda llevar a cabo la lectura de las *coils* del esclavo nº1 desde la aplicación QModMaster. Pulsa sobre el cuarto botón de la fila de botones, empezando por la izquierda (que es el botón utilizado para realizar operaciones de lectura/escritura).

7 CREACIÓN DEL ESCLAVO N°1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

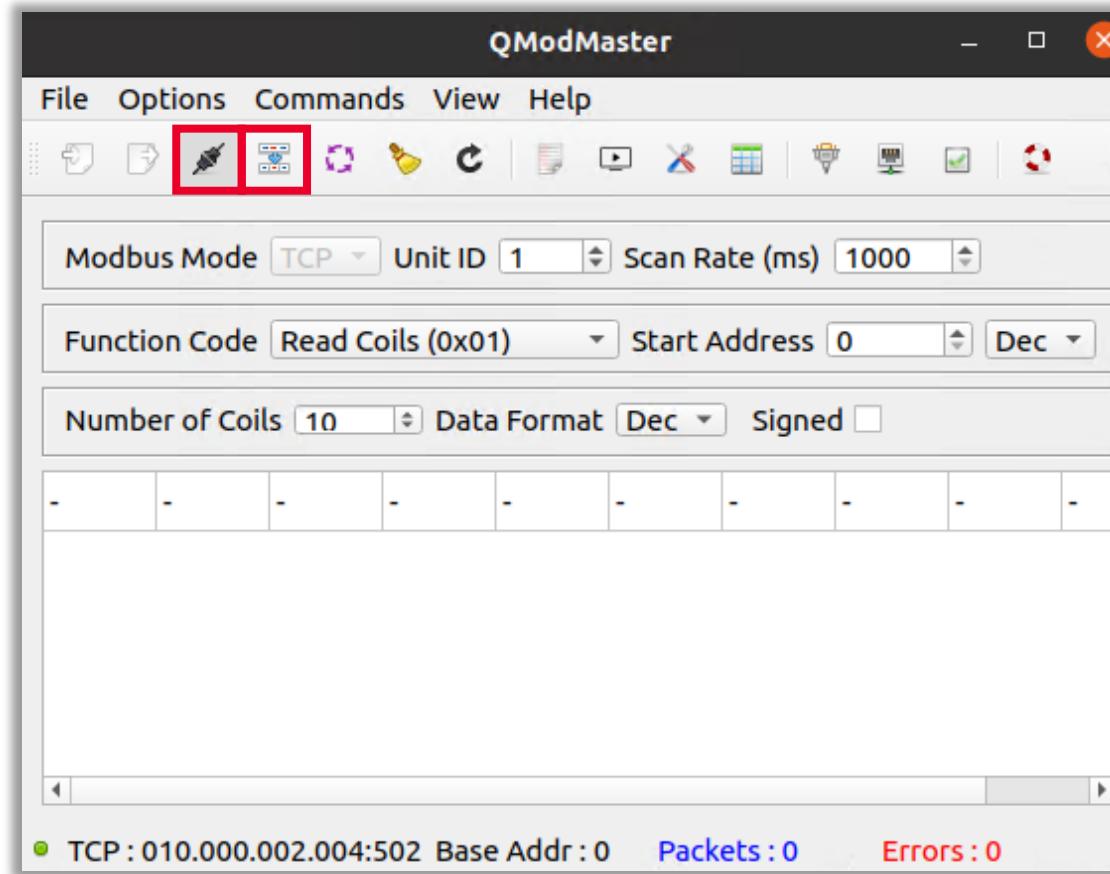


Ilustración 115: Ventana desde la que se realiza la conexión.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- Tras esto, comprueba el resultado de lectura de las 10 *coils* del esclavo nº1, teniendo ambas ventanas de las dos aplicaciones QModMaster y ModbusPal a la vista.
- Como podemos ver en la imagen, se ha producido la lectura de las *coils*. Si comprobamos en QModMaster aparecen los 10 mismos resultados que los valores de las *coils* de ModbusPal.

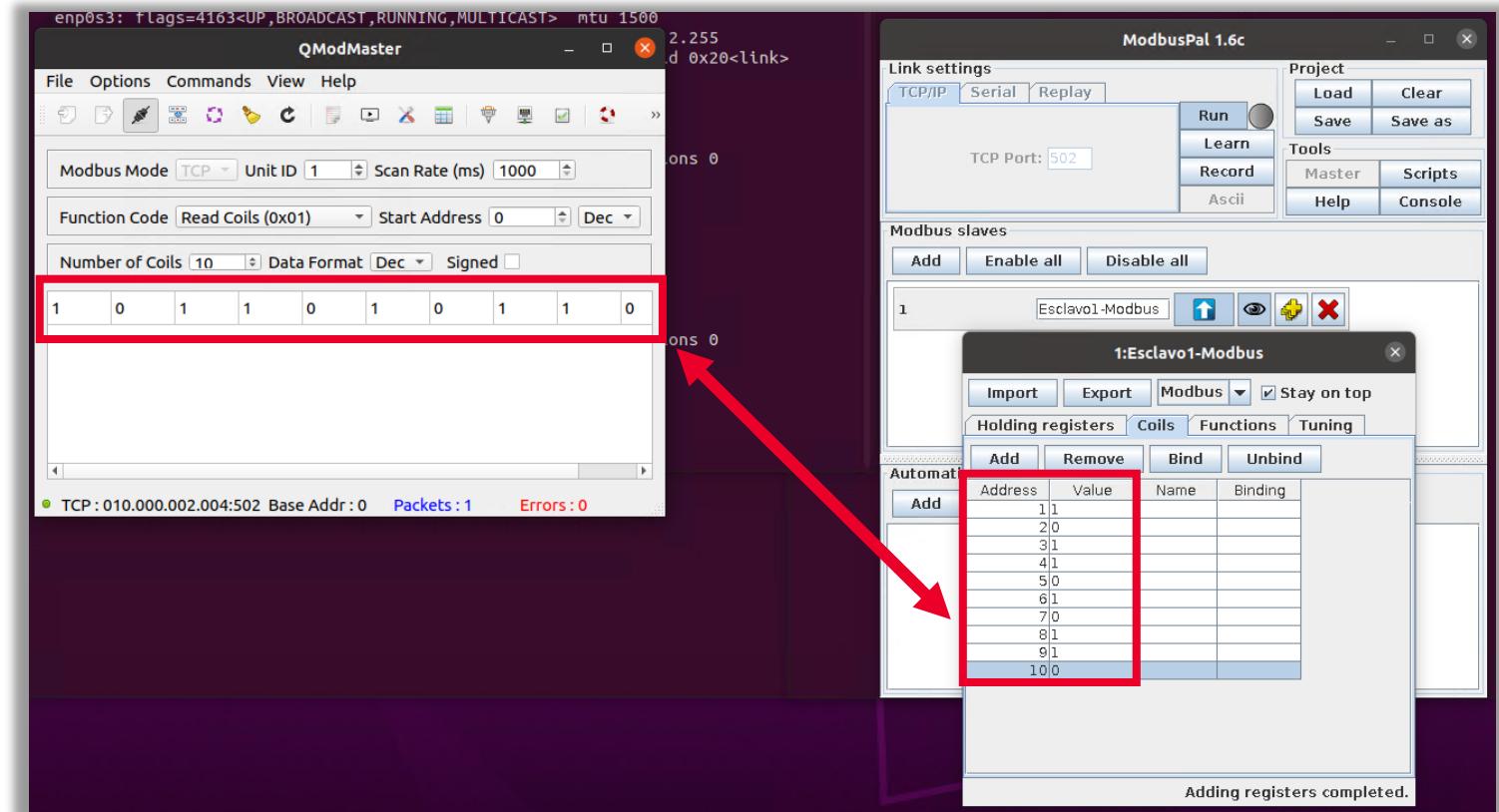


Ilustración 116: Comprobación del resultado de lectura de las *coils* del esclavo, con las ventanas de las dos aplicaciones QModMaster y ModbusPal abiertas.

7 CREACIÓN DEL ESCLAVO Nº1 MODBUS Y LECTURA DE COILS

7.3 Establecer comunicación entre Modbus TCP y lectura de datos

- Para finalizar este apartado, debes desconectar primero la conexión de la aplicación QModMaster y después desactivar el botón «Run» de la aplicación ModbusPal.
 - Desde la aplicación QModMaster, pulsa el mismo botón que has utilizado anteriormente para establecer la conexión (tercer botón empezando por la izquierda).
 - Desde la aplicación ModbusPal, pulsa sobre el botón «Run».

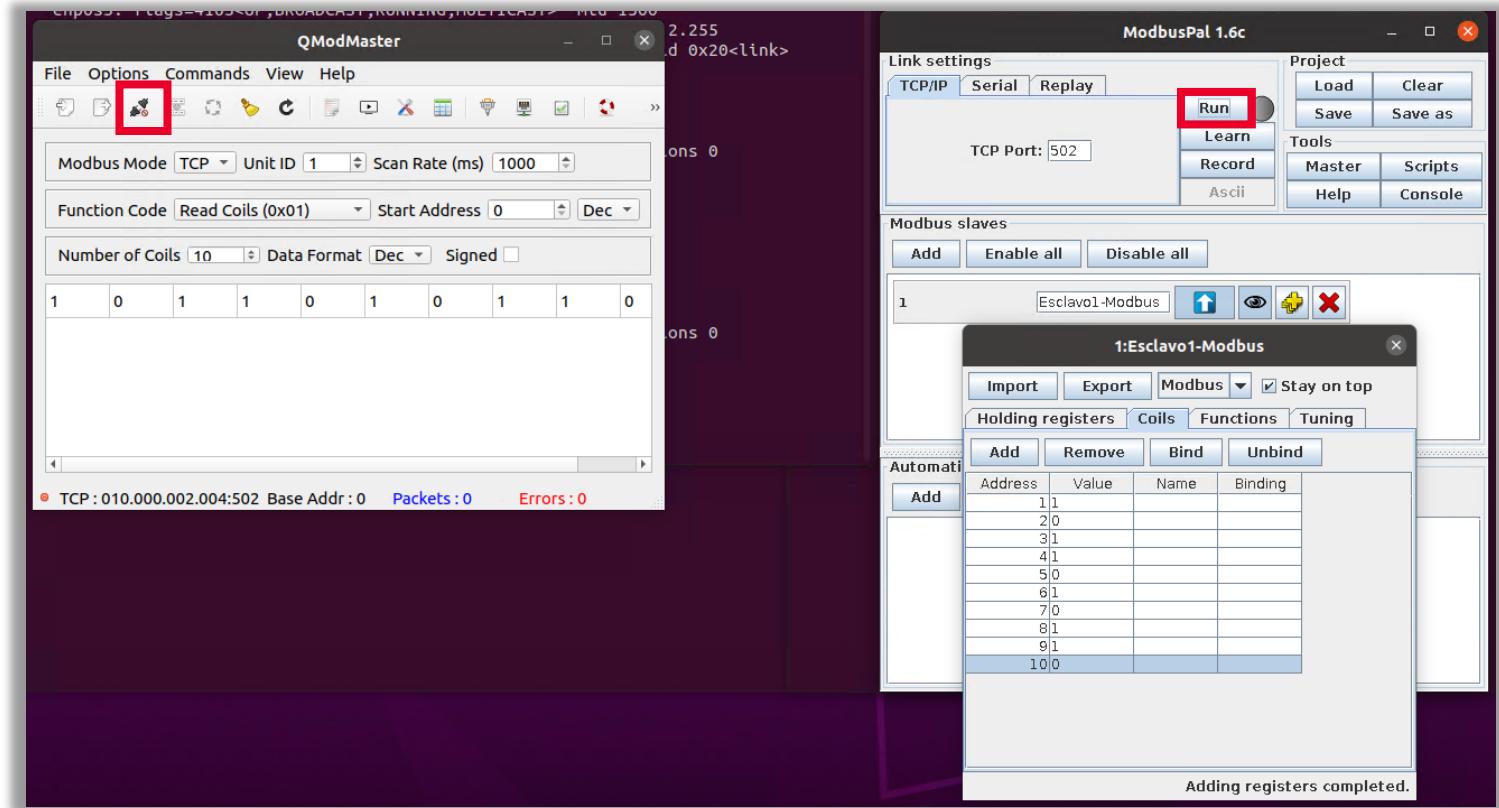


Ilustración 117: Cómo hacer la desconexión. Primero desde QModMaster y después desactivando el botón «Run» de la aplicación ModbusPal.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE *HOLDING* *REGISTERS*

- 8.1 Establecer comunicación entre Modbus TCP y lectura de datos del esclavo nº17.2 Creación del esclavo nº1
- 8.2 Lectura de datos del esclavo nº2

8

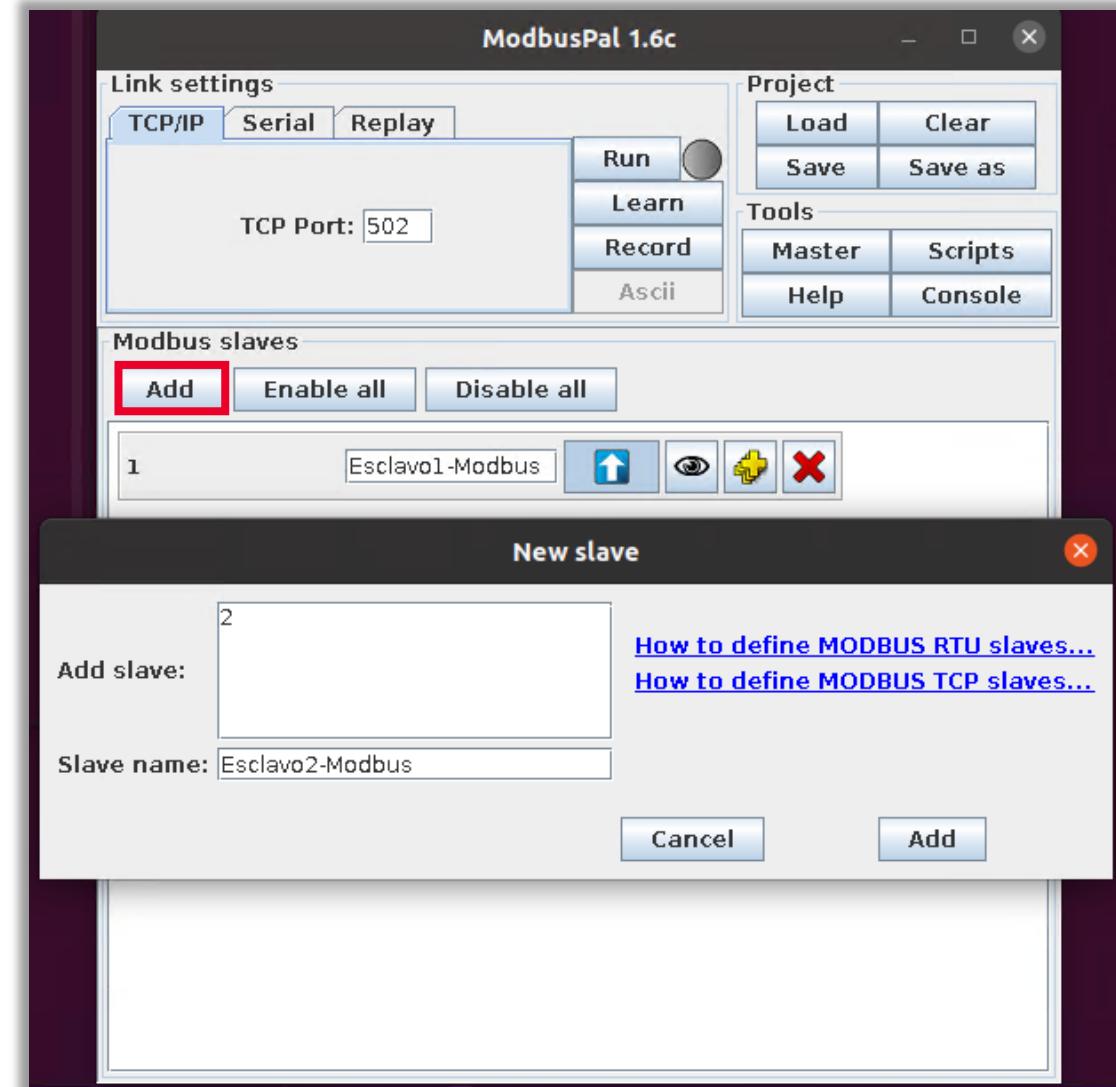
CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE *HOLDING REGISTERS*

En este apartado se va a crear un segundo esclavo con la aplicación Modbuspal (como has visto anteriormente) y se va a establecer la comunicación Modbus TCP con la aplicación QModMaster para la lectura de los datos del *Holding register* del esclavo nº1 que has creado anteriormente y de un nuevo

Holding register que vamos a crear en el esclavo nº2.

- Añadimos un nuevo esclavo en ModbusPal pulsando el botón «Add», como has hecho anteriormente.

Ilustración 118: Añadir nuevo esclavo en ModbusPal.



8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE *HOLDING REGISTERS*

- Una vez lo has añadido, pulsa en el icono que representa un ojo para editar este segundo esclavo.

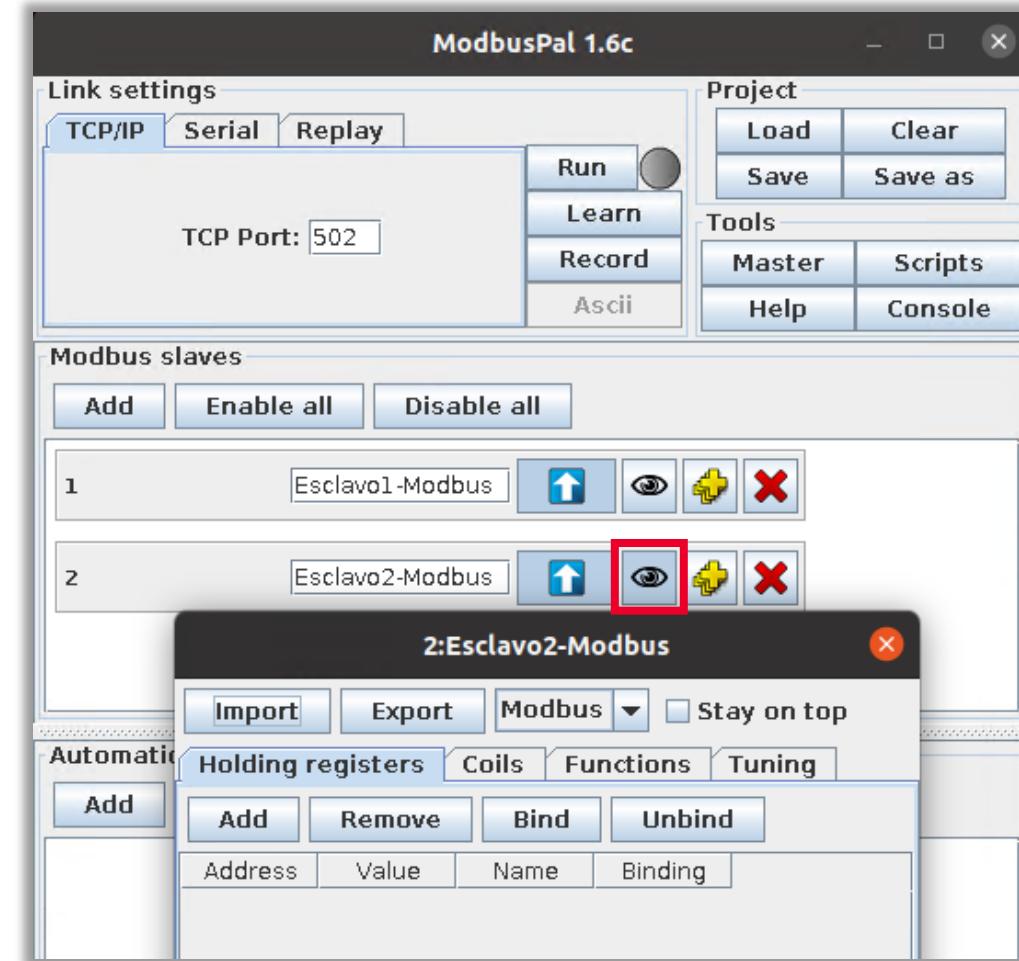


Ilustración 119: Edición del segundo esclavo.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE *HOLDING REGISTERS*

- En la pestaña «*Holding registers*», pulsa el botón «*Add*» y añadimos seis (6) *Holding registers*.

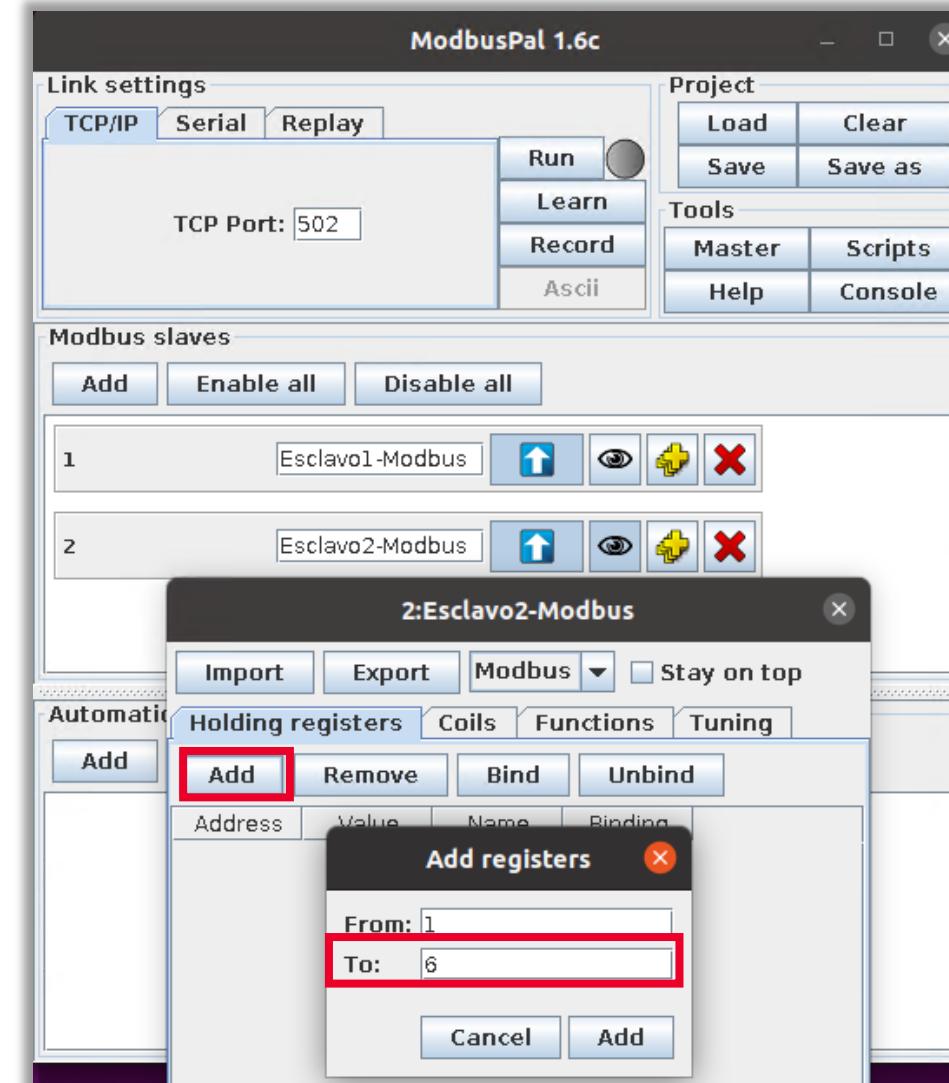


Ilustración 120: Añadir seis *Holding registers*.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE *HOLDING REGISTERS*

- Editamos sus valores, como aparecen en la siguiente imagen:

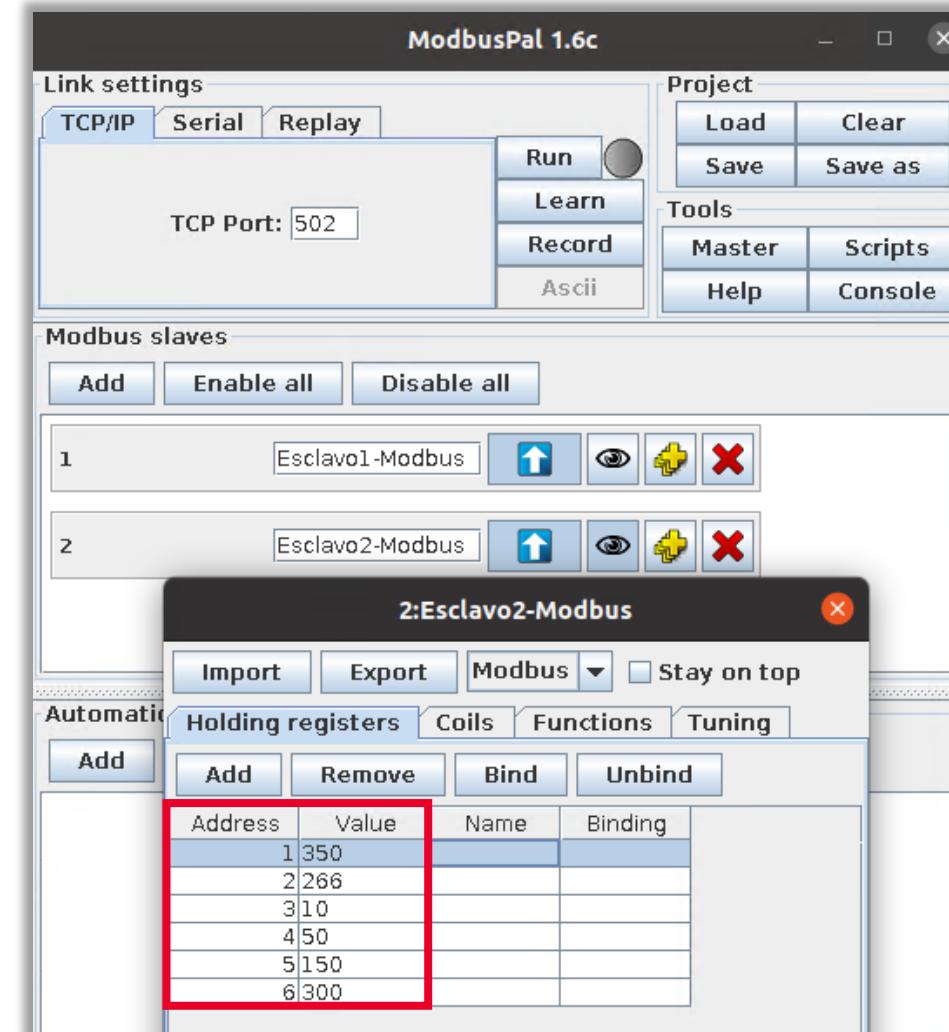


Ilustración 121: Añadir valores al esclavo.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE *HOLDING REGISTERS*

- Ahora pulsa en el botón «Run».

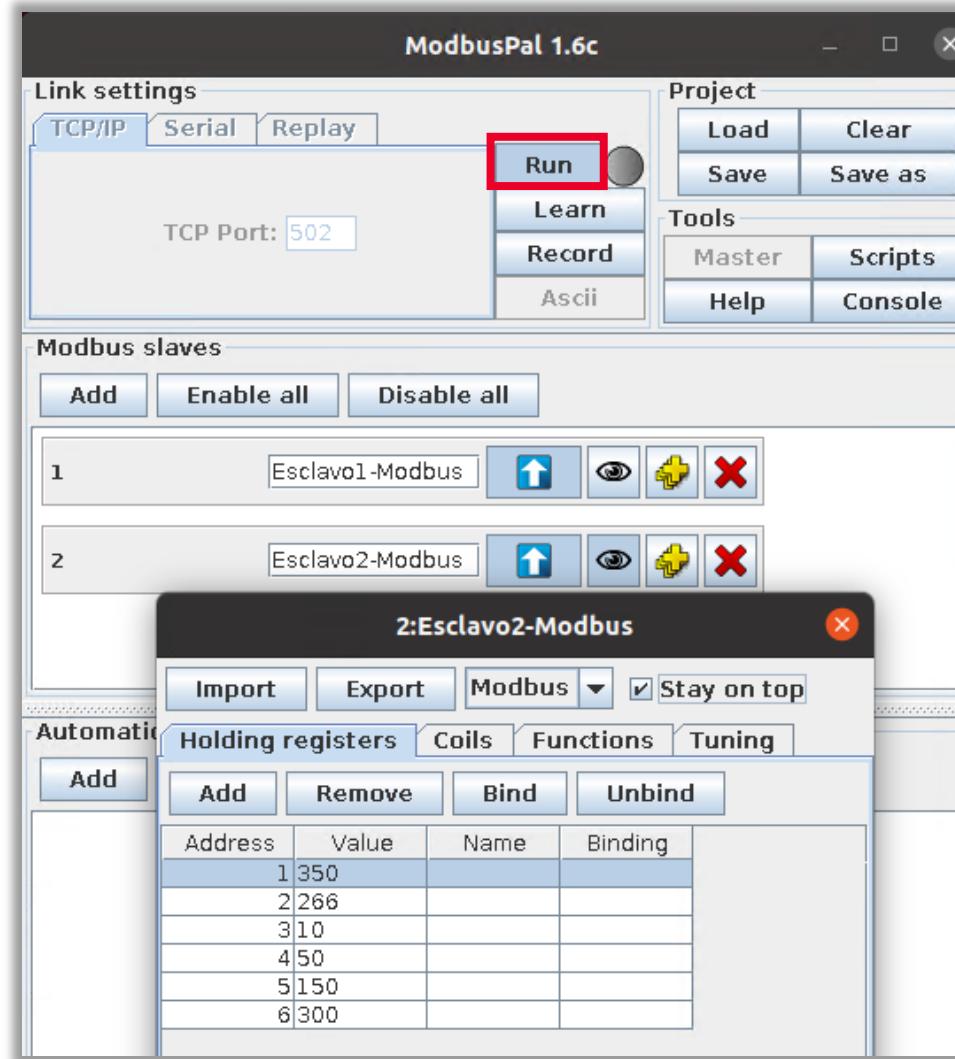


Ilustración 122: Lanzamiento del esclavo mediante el botón «Run».

8

CREACIÓN DEL ESCLAVO Nº2 MODBUS Y LECTURA DE *HOLDING REGISTERS*

- Podemos ver ahora que tenemos nuestros dos esclavos creados.

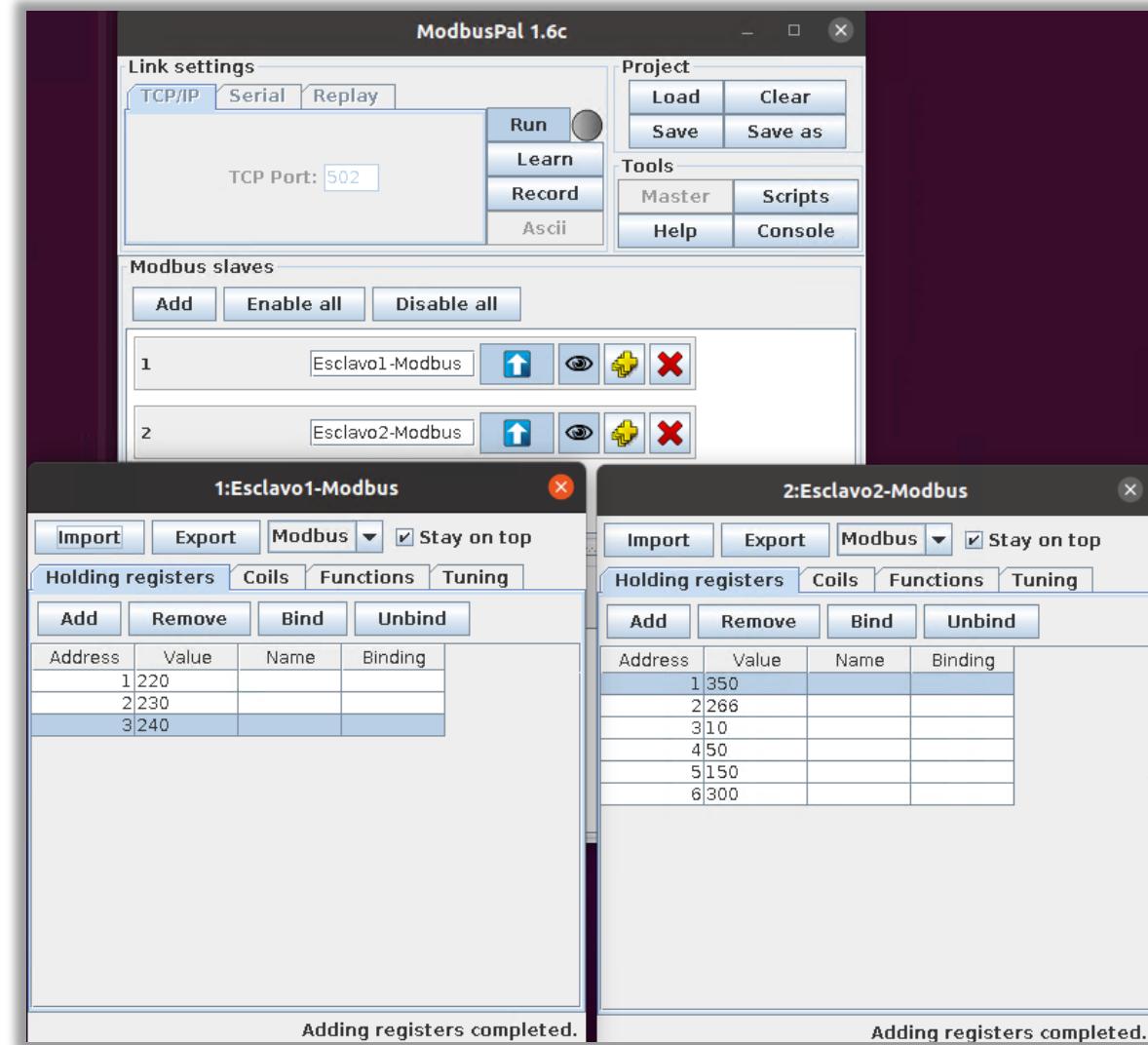


Ilustración 123: Dos discos esclavos creados.

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.1 Establecer comunicación entre Modbus TCP y lectura de datos del esclavo nº1

- Ahora vamos a nuestra aplicación QModMaster.
- Si la ventana de la aplicación QModMaster no la habíamos cerrado anteriormente, nos aparecerá la última lectura realizada de las *coils* como vemos en la siguiente imagen:

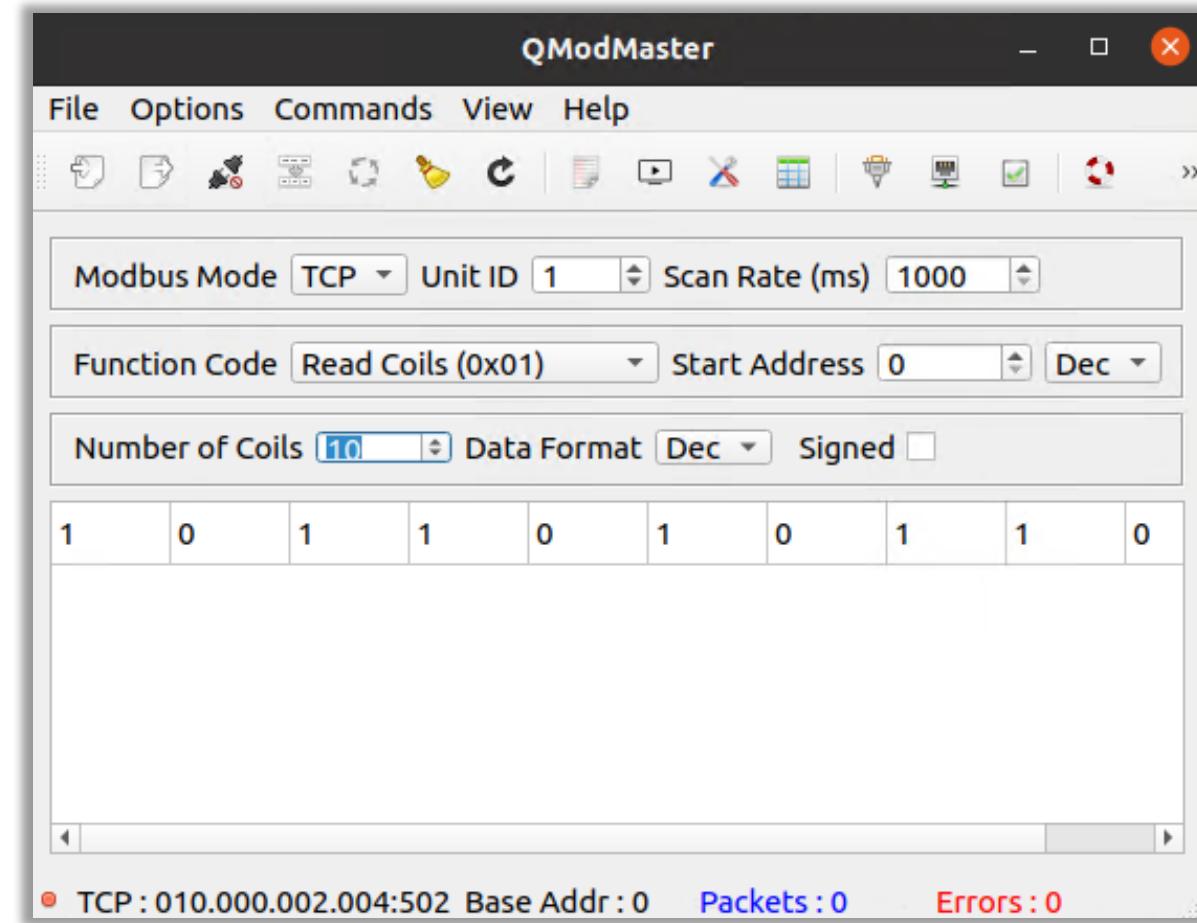


Ilustración 124: Última lectura de *coils*.

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.1 Establecer comunicación entre Modbus TCP y lectura de datos del esclavo nº1

- Para configurar los parámetros de lectura de nuestro esclavo Modbus, en «*Function Code*», seleccionaremos la opción «*Read Holding registers*», ya que en este caso vamos a utilizar la función de lectura de los *Holding registers*.

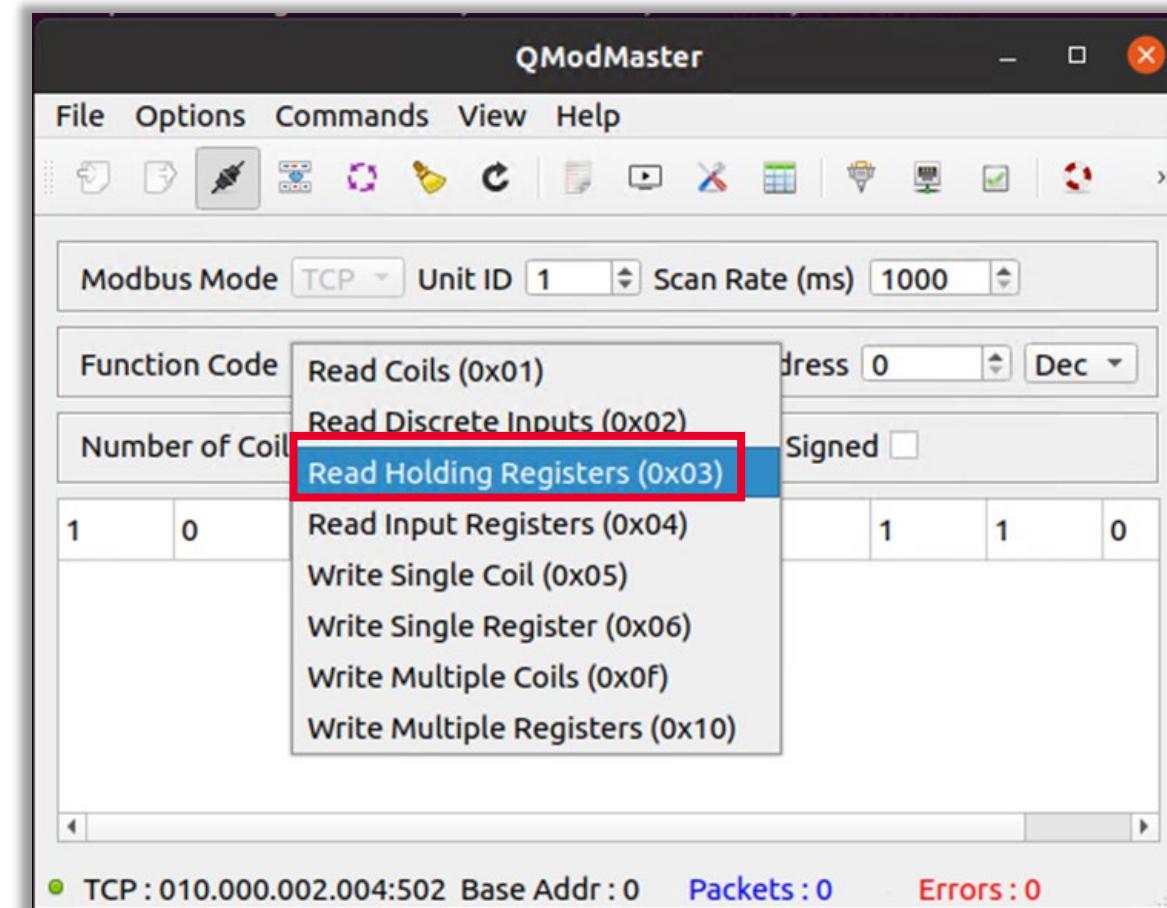


Ilustración 125: Selección de la opción «*Read Holding registers*» para configurar los parámetros de lectura del disco.



CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.1 Establecer comunicación entre Modbus TCP y lectura de datos del esclavo nº1

- Configuramos los valores del esclavo nº1 como aparecen en la imagen siguiente, estableciendo el número de registros (*Number of Registers*) en 3. Después pulsa el botón «*Connect*» (tercer botón empezando por la izquierda) y una vez se ha establecido la conexión, pulsa en el botón «*Read/Write*», para ejecutar la operación de lectura de los tres *Holding Register*.
- Ahora, en el botón del menú superior que está al lado de los cables, pulsaremos para ejecutar.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.1 Establecer comunicación entre Modbus TCP y lectura de datos del esclavo nº1

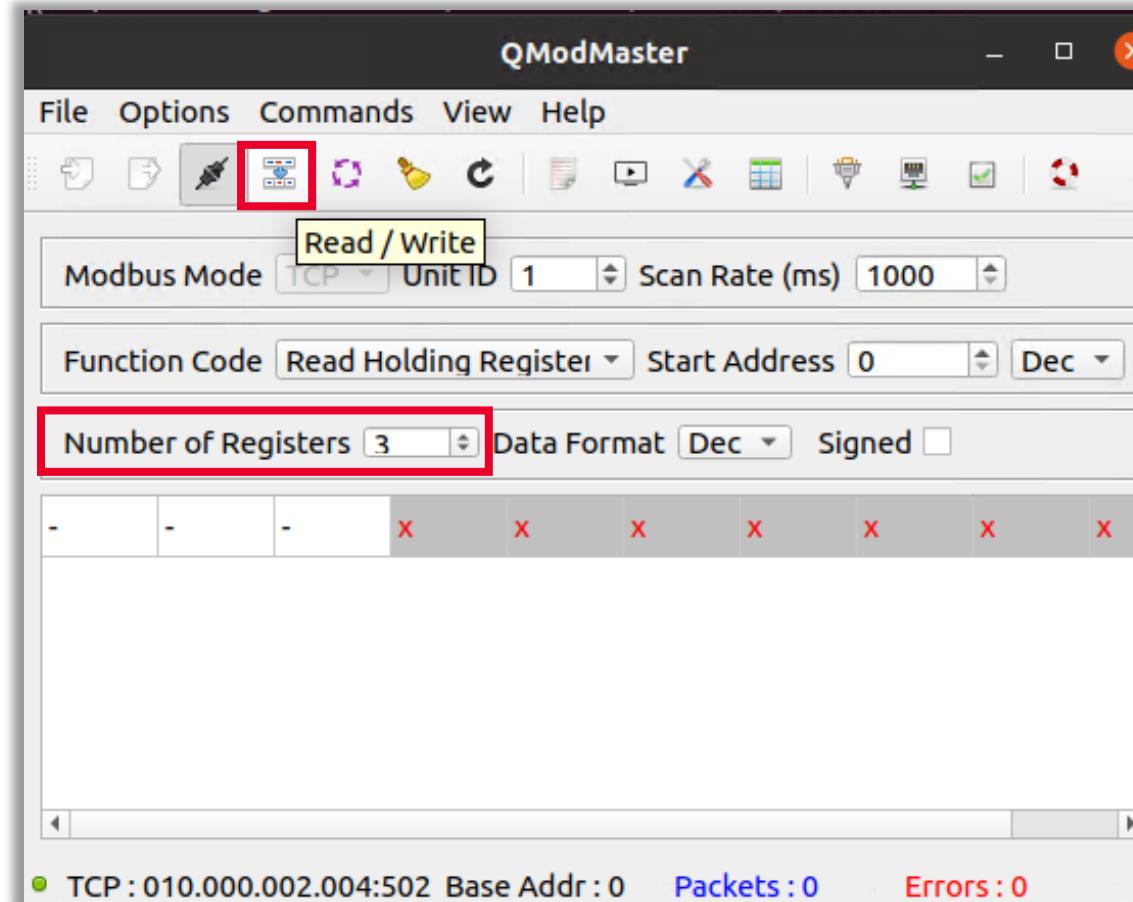


Ilustración 126: Ejecución de la configuración.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.1 Establecer comunicación entre Modbus TCP y lectura de datos del esclavo nº1

- Como podemos observar en la imagen siguiente, la aplicación QModMaster nos ha devuelto la lectura de los tres *Holding Register* del esclavo nº1.

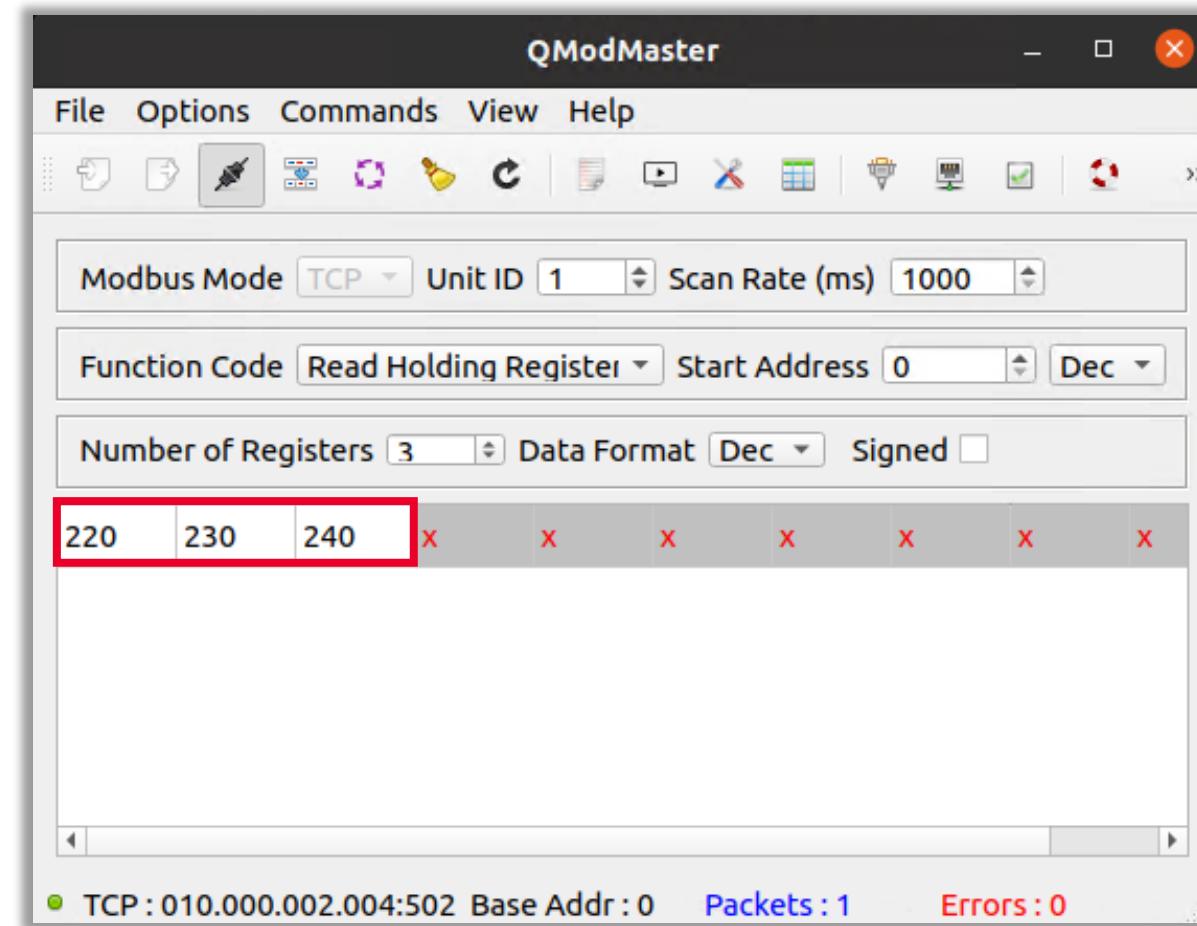


Ilustración 127: Aplicación QModMaster donde confirma la lectura de los tres Holding Register del esclavo 1.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.2 Lectura de datos del esclavo nº2

- Para proceder a la lectura de los datos del esclavo nº2, establecemos los campos con los valores que aparecen en la siguiente imagen, y pulsaremos en el botón «Read/Write».

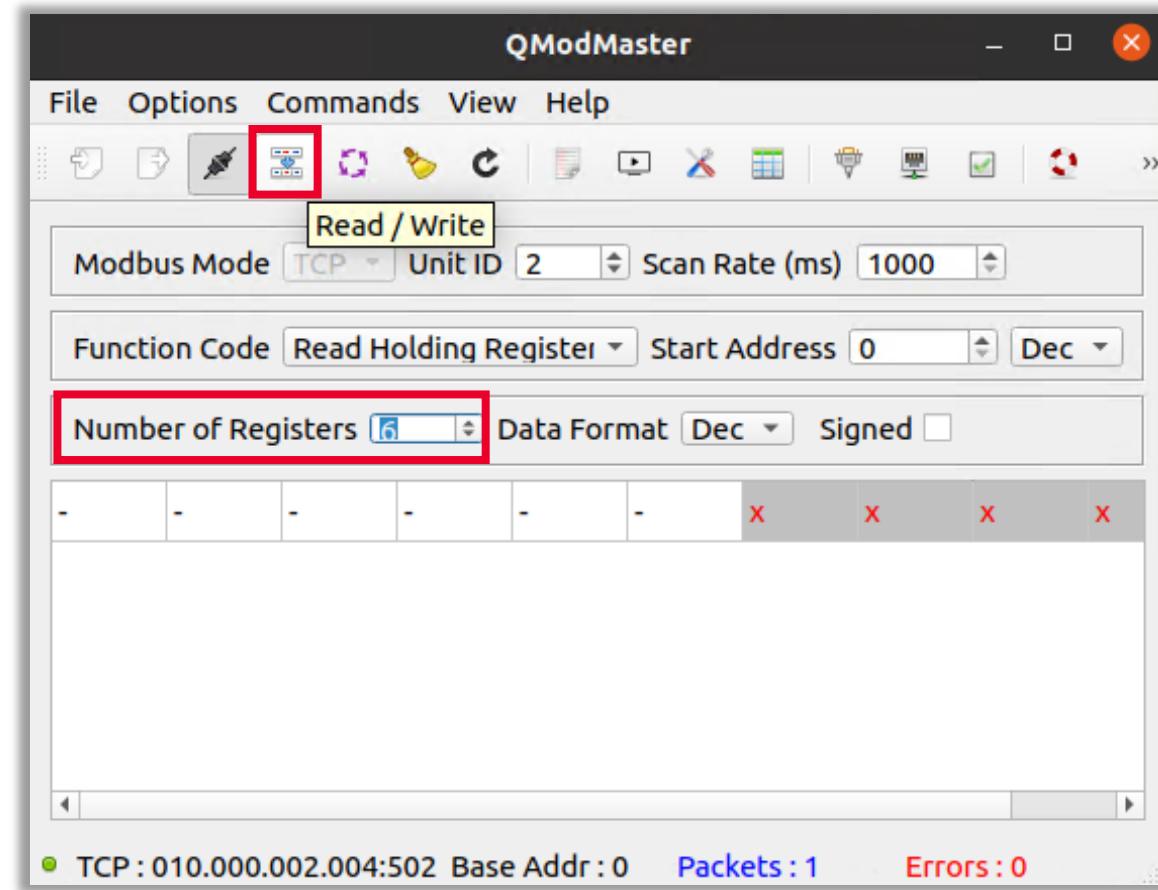


Ilustración 128:
Campos del esclavo 2.

8

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.2 Lectura de datos del esclavo nº2

- Como podemos observar de nuevo en la imagen siguiente, la aplicación QModMaster nos ha devuelto la lectura de los seis *Holding Registers* del esclavo nº2.

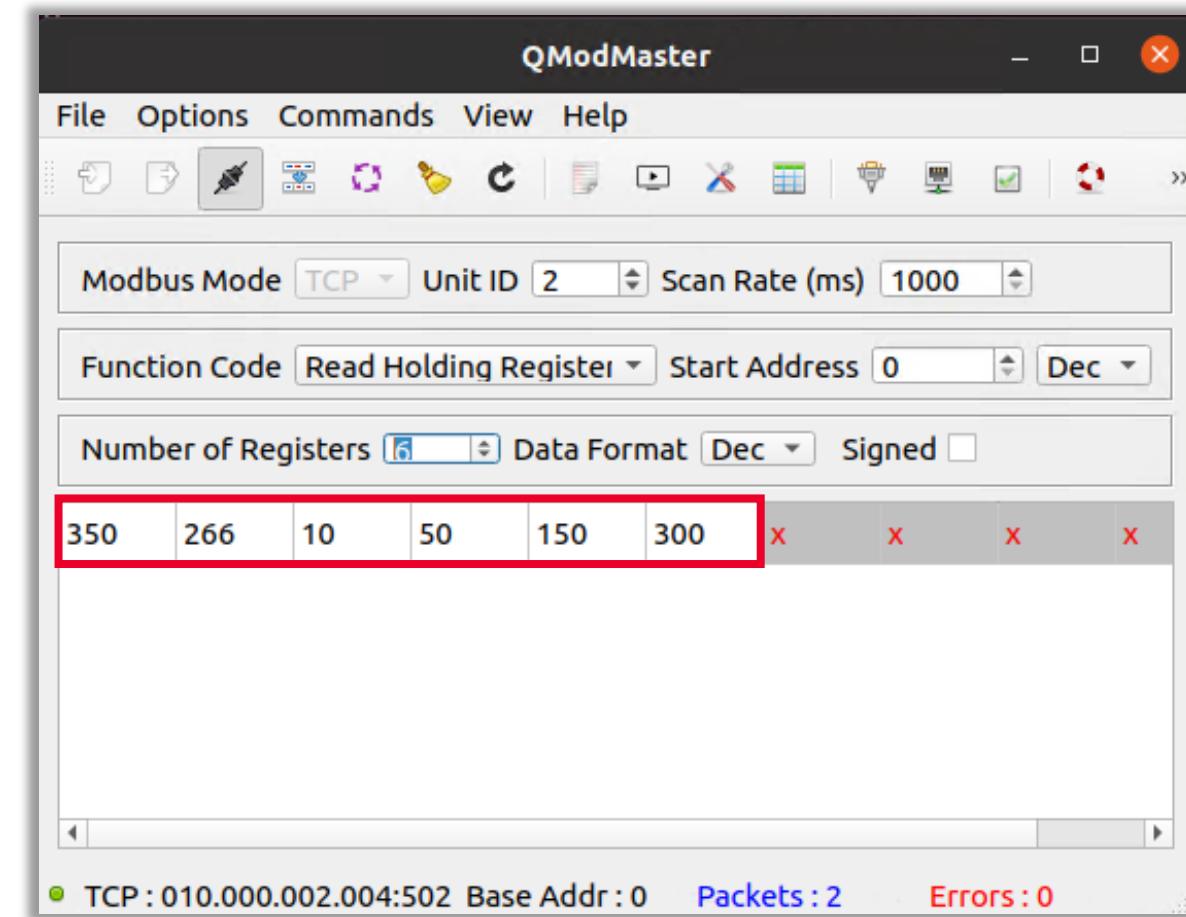


Ilustración 129: Aplicación QModMaster donde confirma la lectura de los seis *Holding Register* del esclavo 2.

CREACIÓN DEL ESCLAVO N°2 MODBUS Y LECTURA DE HOLDING REGISTERS

8.2 Lectura de datos del esclavo n°2

- En esta vista se puede observar la ejecución de la aplicación QModMaster, y la aplicación ModbusPal incluyendo las ventanas de los dos esclavos.

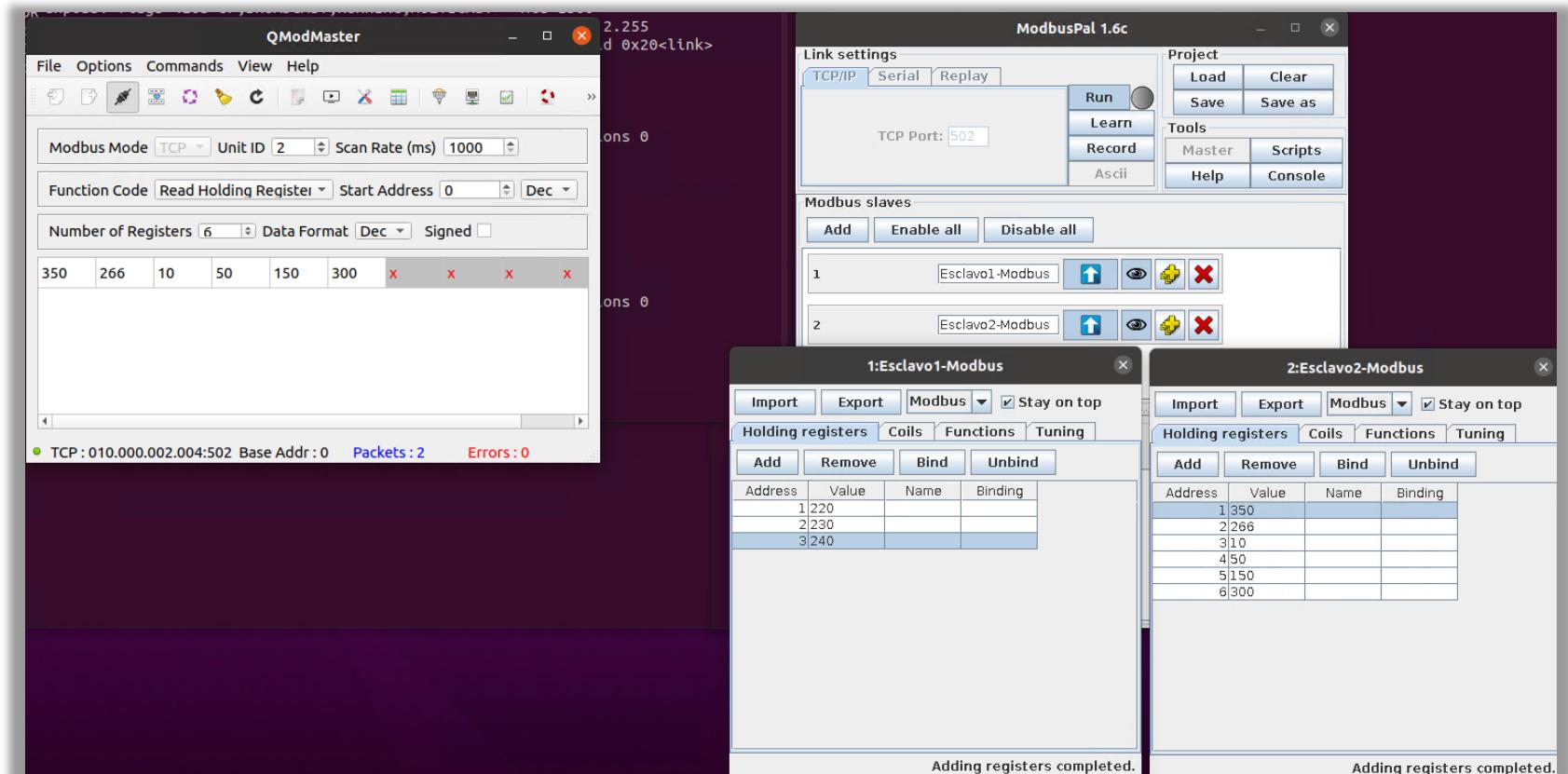


Ilustración 130: Aplicaciones QModMaster y ModbusPal incluyendo las ventanas de los dos esclavos.

9

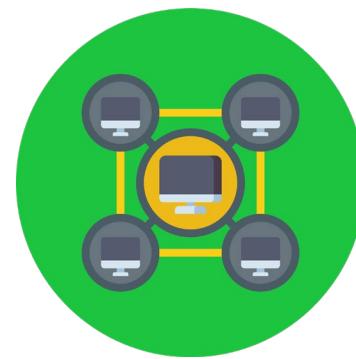
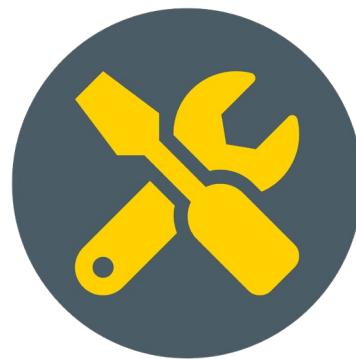
HERRAMIENTA PLCSCAN

- 9.1 Escaneo de dispositivos que utilizan el protocolo Modbus
- 9.2 Ejecución de la aplicación Snap7 Server Demo
- 9.3 Ejecución de la aplicación Snap7 Client Demo
- 9.4 Escaneo de dispositivos Siemens



HERRAMIENTA PLCSCAN

En este apartado se va a utilizar la herramienta PLCScan para realizar la identificación de dispositivos que utilizan el protocolo Modbus TCP, así como los dispositivos Siemens que utilizan el protocolo de comunicación s7comm.



9 HERRAMIENTA PLCSCAN

9.1 Escaneo de dispositivos que utilizan el protocolo Modbus

- Para la identificación de dispositivos que utilizan el protocolo de comunicación Modbus TCP haremos lo siguiente:
 - Si no cerraste la terminal donde se ejecuta anteriormente la aplicación PLCScan, accede a ella y obvia este paso.
En caso contrario abre una nueva terminal en la MV y sitúate en la carpeta PLCScan con el siguiente comando:
 - **cd Documentos/plcscan/**
- Una vez situados en la carpeta, ejecuta los siguientes comandos para realizar los diferentes escaneos (estos comandos se ejecutan a través de la aplicación de consola python2 que ejecuta a su vez el archivo PLCScan.py).
 - Primero ejecuta la herramienta invocando la ayuda de PLCScan con el parámetro **-h**, para ver todas las opciones que nos posibilita la herramienta:
 - **python2 plcscan.py -h**



HERRAMIENTA PLCSCAN

9.1 Escaneo de dispositivos que utilizan el protocolo Modbus

- Ahora realiza un primer escaneo indicando la dirección IP de la MV donde estamos ejecutando la aplicación ModbusPal:
 - **python2 plcscan.py 10.0.2.4**
- Como veremos en la imagen de la siguiente diapositiva el resultado que nos ha devuelto la herramienta no indica que haya detectado un dispositivo Modbus, por lo que ejecuta la herramienta utilizando el parámetro **--modbus-uid** para indicarle que el esclavo que queremos escanear es el nº1.
 - **python2 plcscan.py --modbus-uid=1 10.0.2.4**
- Ahora como aparece en la imagen, el resultado de la ejecución de la herramienta ya nos ha identificado correctamente que hay un dispositivo Modbus y que el nº de esclavo es el 1.

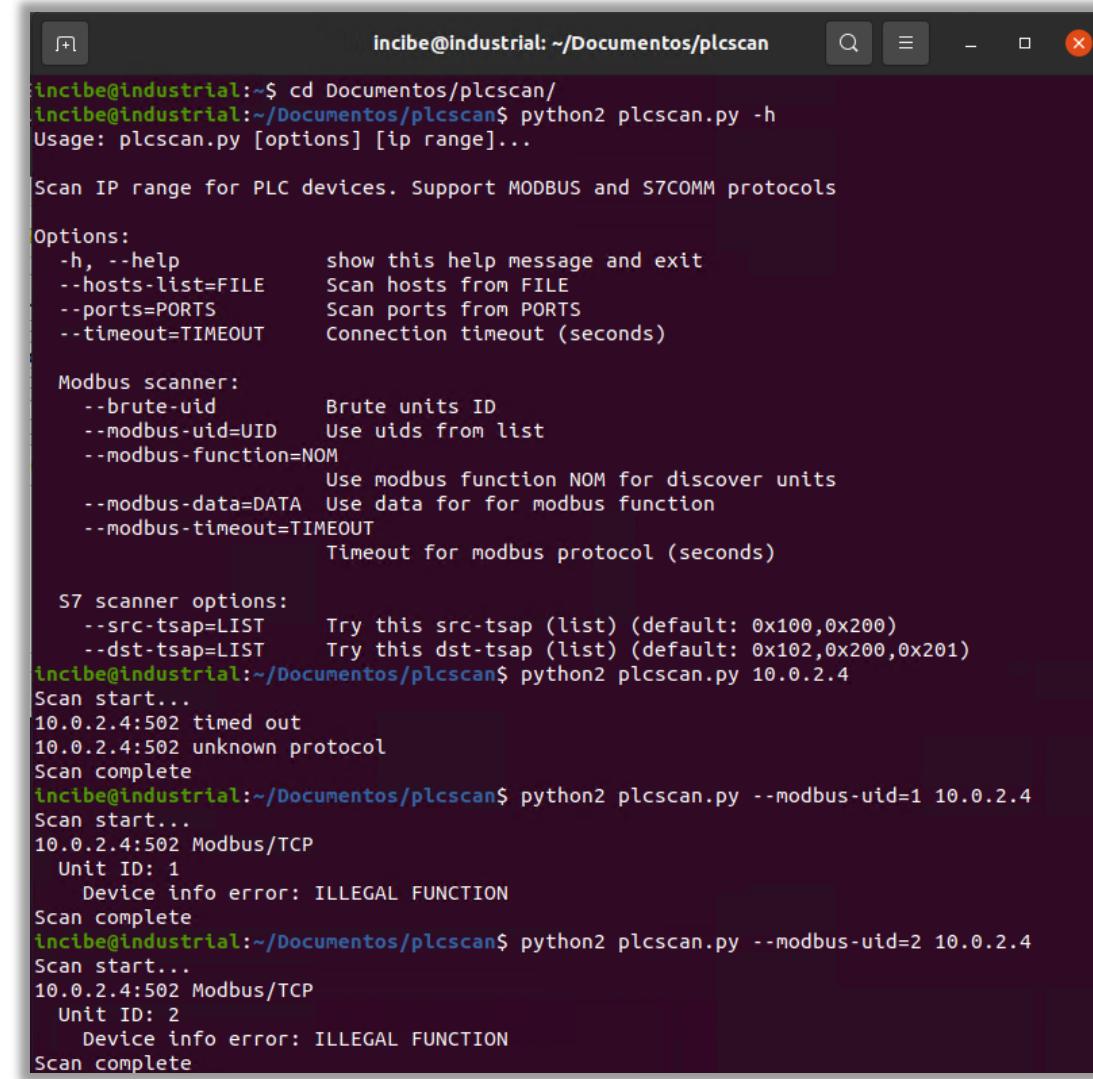
9

HERRAMIENTA PLCSCAN

9.1 Escaneo de dispositivos que utilizan el protocolo Modbus

- Ejecuta de nuevo la herramienta PLCScan pero indicando esta vez en el parámetro que el nº del esclavo es el 2:
 - python2 plcscan.py --modbus-uid=2**
- 10.0.2.4**
- Comprueba de nuevo en la imagen el resultado de la ejecución.

Ilustración 131: Identificación de dispositivos que utilizan el protocolo de comunicación Modbus TCP.



```
incibe@industrial:~/Documentos/plcscan$ cd Documentos/plcscan/
incibe@industrial:~/Documentos/plcscan$ python2 plcscan.py -h
Usage: plcscan.py [options] [ip range]...
Scan IP range for PLC devices. Support MODBUS and S7COMM protocols

Options:
-h, --help      show this help message and exit
--hosts-list=FILE Scan hosts from FILE
--ports=PORTS   Scan ports from PORTS
--timeout=TIMEOUT Connection timeout (seconds)

Modbus scanner:
--brute-uid     Brute units ID
--modbus-uid=UID Use uids from list
--modbus-function=NOM
                  Use modbus function NOM for discover units
--modbus-data=DATA Use data for for modbus function
--modbus-timeout=TIMEOUT
                  Timeout for modbus protocol (seconds)

S7 scanner options:
--src-tsap=LIST  Try this src-tsap (list) (default: 0x100,0x200)
--dst-tsap=LIST  Try this dst-tsap (list) (default: 0x102,0x200,0x201)
incibe@industrial:~/Documentos/plcscan$ python2 plcscan.py 10.0.2.4
Scan start...
10.0.2.4:502 timed out
10.0.2.4:502 unknown protocol
Scan complete
incibe@industrial:~/Documentos/plcscan$ python2 plcscan.py --modbus-uid=1 10.0.2.4
Scan start...
10.0.2.4:502 Modbus/TCP
Unit ID: 1
Device info error: ILLEGAL FUNCTION
Scan complete
incibe@industrial:~/Documentos/plcscan$ python2 plcscan.py --modbus-uid=2 10.0.2.4
Scan start...
10.0.2.4:502 Modbus/TCP
Unit ID: 2
Device info error: ILLEGAL FUNCTION
Scan complete
```



HERRAMIENTA PLCSCAN

9.1 Escaneo de dispositivos que utilizan el protocolo Modbus

- Dejamos esta terminal abierta, para continuar con la ejecución de esta herramienta posteriormente.
 - Para la identificación de dispositivos que utilizan el protocolo de comunicación s7comm utilizados por los dispositivos Siemens seguiremos las instrucciones que aparecen en los siguientes apartados.

9.2 Ejecución de la aplicación Snap7 Server Demo

- Accede a la ventana de la aplicación Snap 7 Server Demo que dejamos ejecutándose anteriormente y pulsa en el botón «*Start*».
- Si teníamos cerrada esta ventana procedemos como sigue:
 - Abre una nueva terminal y ejecuta el siguiente comando para tomar nota de la dirección IP asignada (en nuestro caso es la IP 10.0.2.4):
 - **ifconfig**
- Tras esto nos situamos en la carpeta «bin» de Snap7 que has descargado previamente con el siguiente comando:
 - **cd Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin/**
- Ejecuta de nuevo la aplicación Snap7 Server Demo:
 - **sudo ./serverdemo**



HERRAMIENTA PLCSCAN

9.2 Ejecución de la aplicación Snap7 Server Demo

```
incibe@industrial: ~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin
incibe@industrial:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::394b:55c2:8c7e:4de5 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:5b:c2:78 txqueuelen 1000 (Ethernet)
            RX packets 134731 bytes 189969260 (189.9 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 68586 bytes 4772550 (4.7 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Bucle local)
            RX packets 3150 bytes 298272 (298.2 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3150 bytes 298272 (298.2 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

incibe@industrial:~$ cd Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin/
incibe@industrial:~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin$ sudo ./serverdemo
```

Ilustración 132: Nueva terminal y se ejecuta el comando para tomar nota de la dirección IP asignada.

9

HERRAMIENTA PLCSCAN

9.2 Ejecución de la aplicación Snap7 Server Demo

- En la ventana que nos aparece, establecemos de nuevo la IP de la aplicación Snap7 Server Demo, rellenando el campo «Local Address» con la dirección IP que has obtenido ejecutando el comando **ifconfig**. Tras esto pulsa el botón «Start» para arrancar el servidor, como se puede ver en la siguiente imagen.

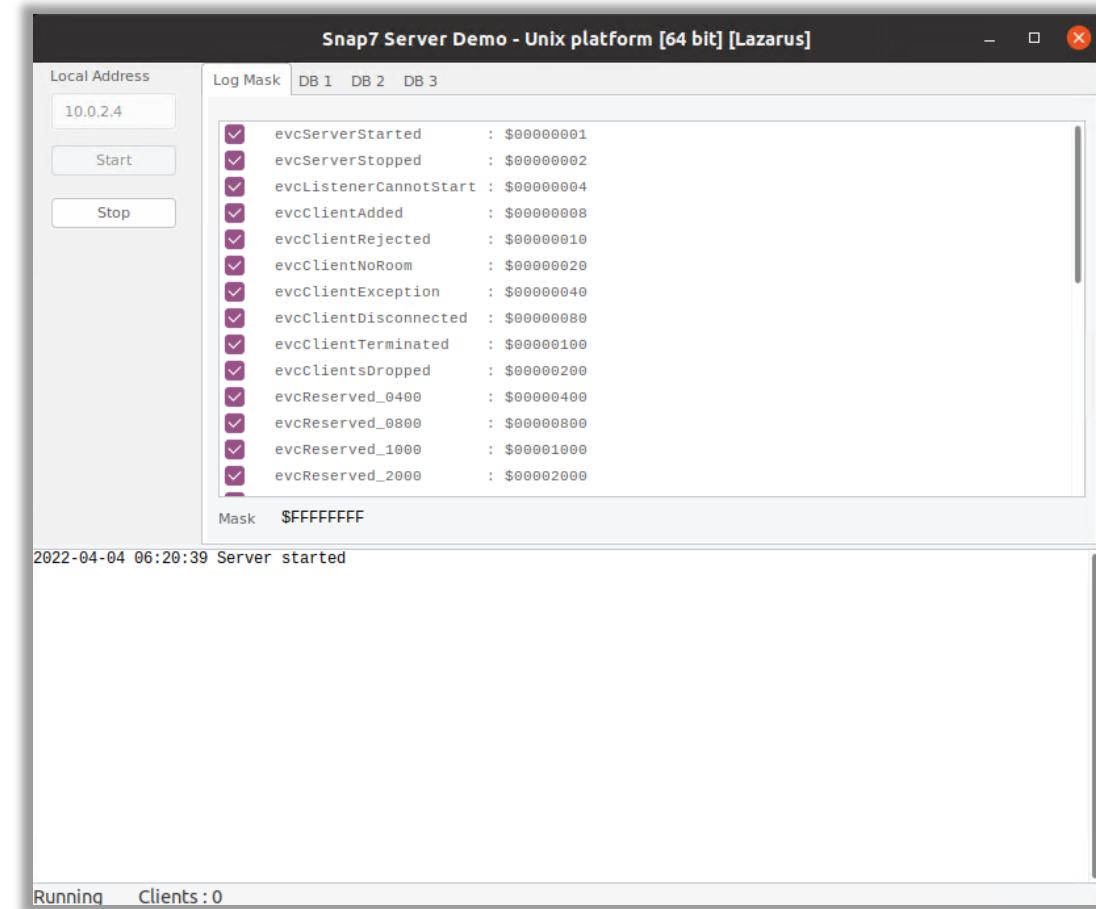


Ilustración 133: IP de la aplicación Snap7 Server Demo.

9.3 Ejecución de la aplicación Snap7 Client Demo

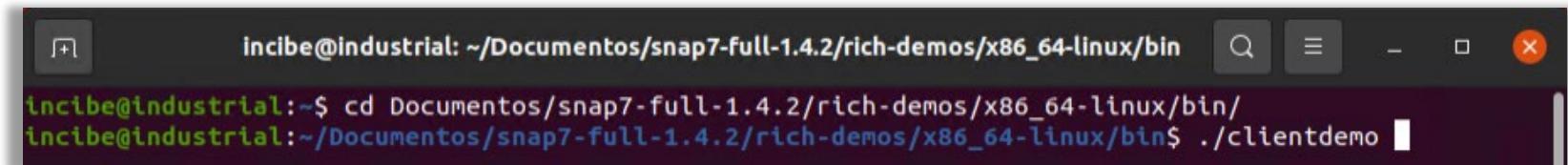
- Accede a la ventana de la aplicación Snap 7 Client Demo que dejamos ejecutándose anteriormente y pulsa en el botón «Connect».
- Si teníamos cerrada esta aplicación procedemos como sigue:
 - En una nueva terminal, nos situaremos en la carpeta «bin» de Snap7 que has descargado previamente con el siguiente comando:
 - **cd Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin/**

9

HERRAMIENTA PLCSCAN

9.3 Ejecución de la aplicación Snap7 Client Demo

- Ejecuta el cliente denominado Snap7 Client Demo para que nos muestre la interfaz del PLC:
 - ./clientdemo**



The screenshot shows a terminal window with a dark background and light-colored text. The window title is "incibe@industrial: ~/Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin". The terminal prompt is "incibe@industrial:~\$". The user has navigated to the directory "Documentos/snap7-full-1.4.2/rich-demos/x86_64-linux/bin" and is executing the command "../clientdemo". The command is shown in blue, indicating it is being typed or has just been run.

Ilustración 134: Ejecución de aplicación Snap7 Client Demo.

9

HERRAMIENTA PLCSCAN

9.3 Ejecución de la aplicación Snap7 Client Demo

- En la entrada «Connect as», elegimos «S7 BASIC». Pulsa el botón «Connect» y establece la conexión con nuestra aplicación Snap7 Server Demo, para de esta forma poder interactuar con el PLC.

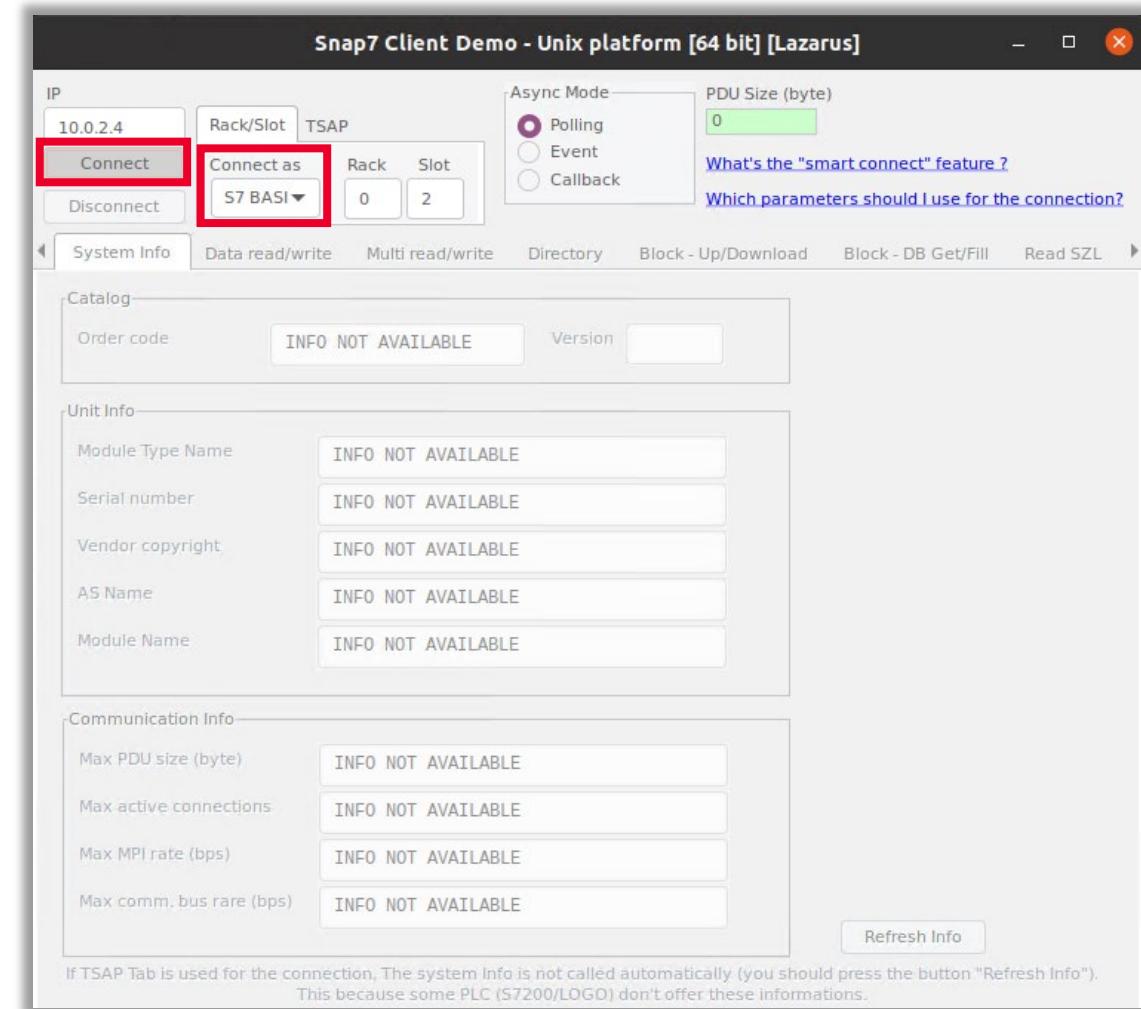


Ilustración 135: Establecimiento de la conexión con la aplicación Snap7 Server Demo.

9

HERRAMIENTA PLCSCAN

9.3 Ejecución de la aplicación Snap7 Client Demo

- Una vez hemos pulsado el botón de «Connect», nos aparece la siguiente información del sistema del PLC al conectarnos con él. No tenemos que tocar o cambiar nada.

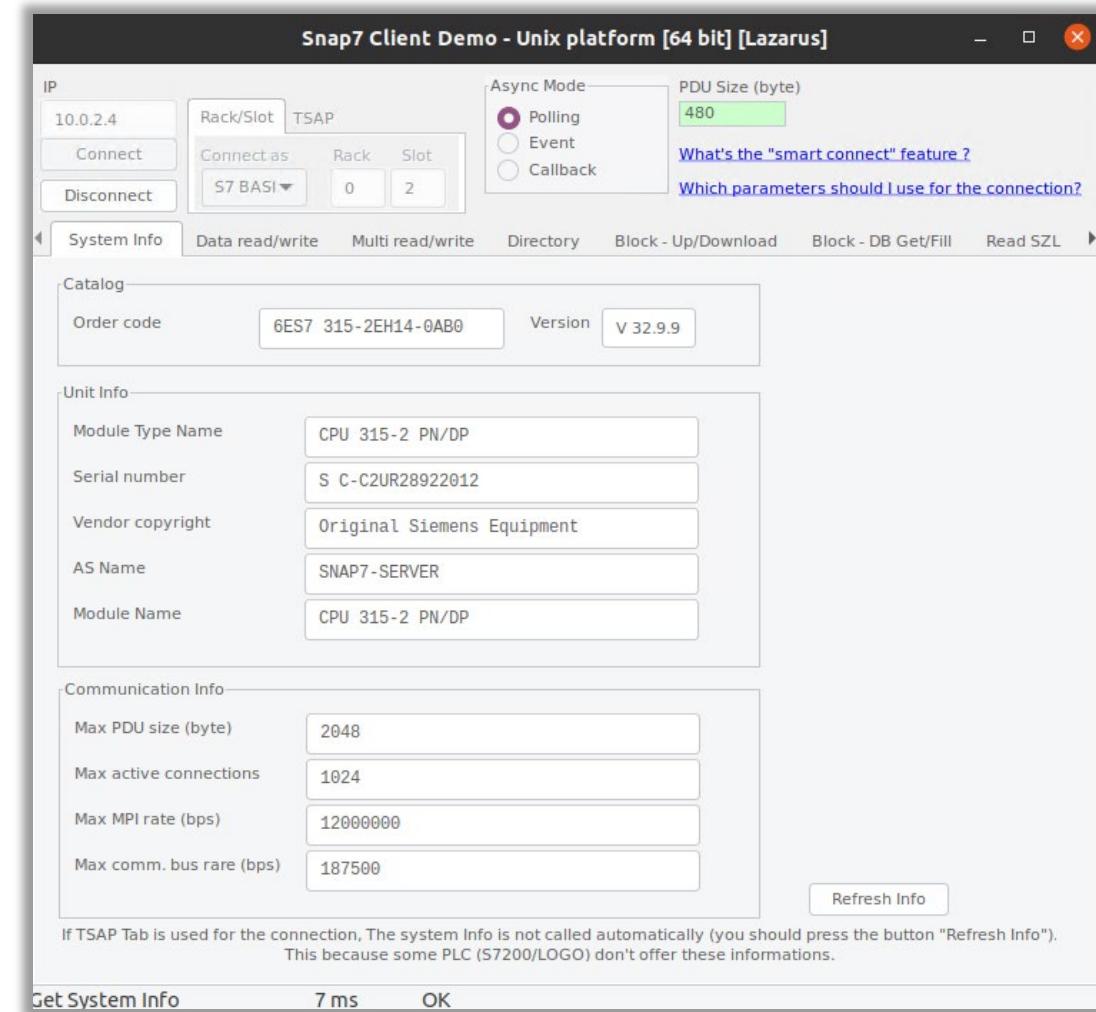


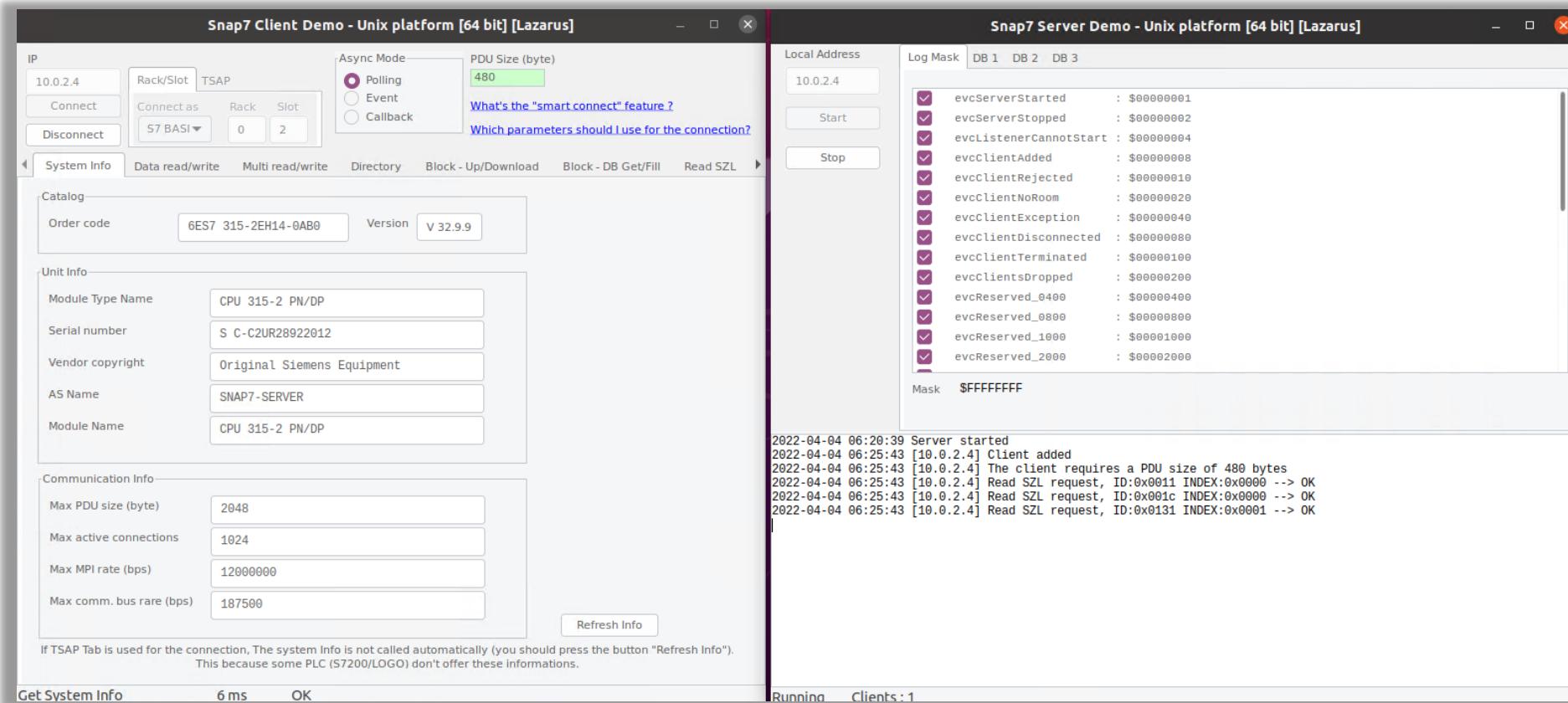
Ilustración 136: Establecimiento de la conexión con la aplicación Snap7 Server Demo.

9

HERRAMIENTA PLCSCAN

9.3 Ejecución de la aplicación Snap7 Client Demo

- Ahora deberíamos tener ambas pantallas, la del servidor y la del cliente, como se muestra en la siguiente imagen:



9.4 Escaneo de dispositivos Siemens

- Si has cerrado la terminal de PLCScan que utilizamos anteriormente, abre una nueva terminal y accede a la carpeta de la aplicación PLCScan con el comando:
 - **cd Documentos/plcscan**
- Si ya tienes abierta la terminal, ejecuta la herramienta PLCScan nuevamente, pero esta vez vamos a realizar un escaneo de dispositivos Siemens en un rango de direcciones IP (suponiendo el caso de que no conociéramos exactamente la dirección IP donde podría estar ejecutándose el dispositivo Siemens).

9 HERRAMIENTA PLCSCAN

9.4 Escaneo de dispositivos Siemens

- Ejecuta el comando indicado a continuación. La dirección IP se pondrá como 10.0.2.0/28 donde estamos indicando que nos realice un escaneo en las 16 primeras direcciones IP, es decir, de la 10.0.2.0 a la 10.0.2.17. Se debe tener en cuenta que cuanto menor es el valor de la máscara de red, mayor es el número de direcciones IP a escanear, y, por tanto, más tiempo tardará en realizar el escaneo. Por ello hemos escogido un rango muy limitado para realizar esta práctica.
 - **python2 plcscan.py 10.0.2.0/28**
- En las imágenes siguientes vemos primero la ejecución del comando cuando aún continúa realizando el escaneo de dispositivos Siemens en el rango de direcciones IP y después cuando ha finalizado su ejecución.

9 HERRAMIENTA PLCSCAN

9.4 Escaneo de dispositivos Siemens

Ilustración 138: Inicio del escaneo de dispositivos Siemens.

9 HERRAMIENTA PLCSCAN

9.4 Escaneo de dispositivos Siemens

Ilustración 139: Finalización del escaneo de dispositivos Siemens.

9 HERRAMIENTA PLCSCAN

9.4 Escaneo de dispositivos Siemens

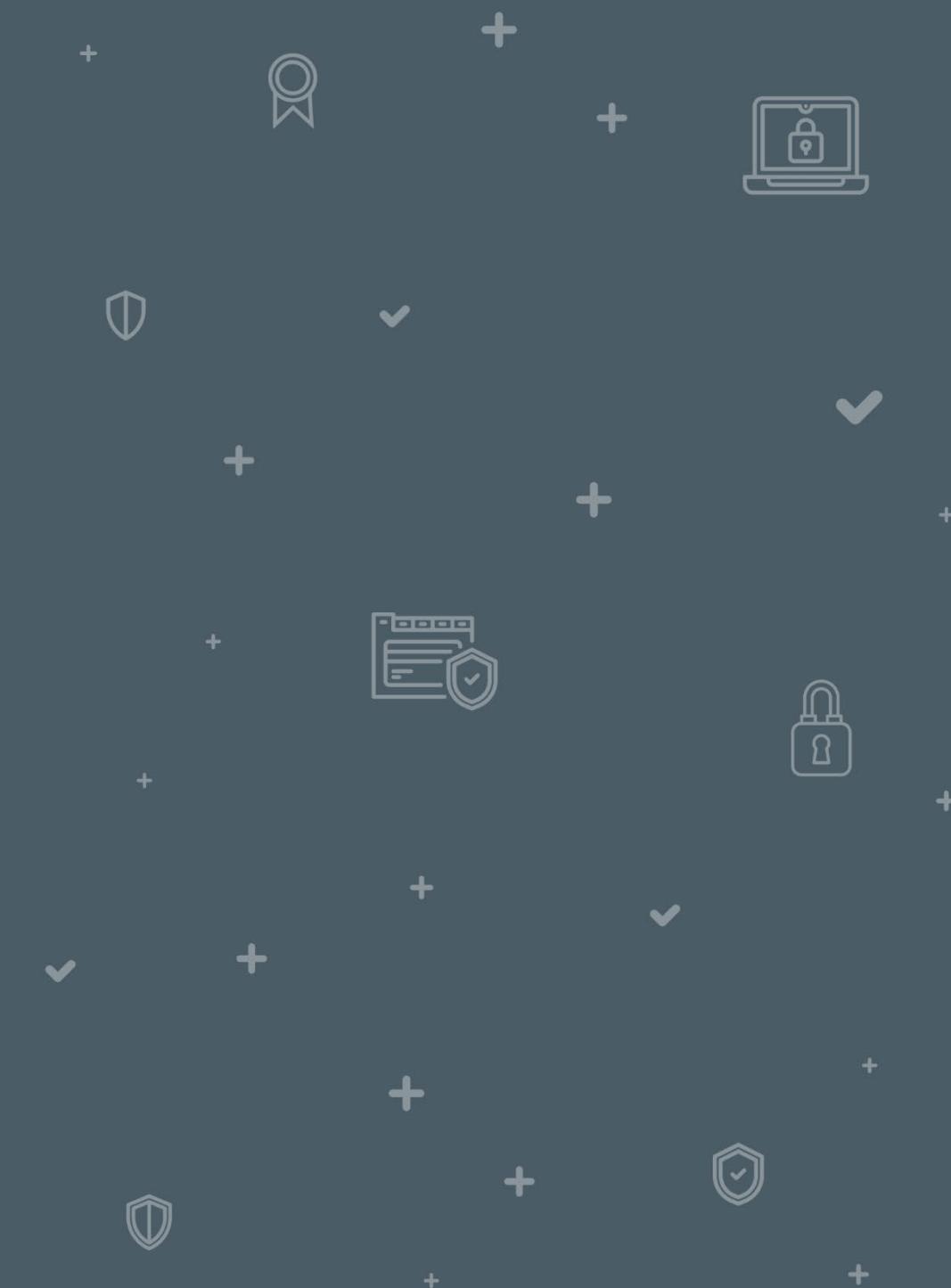
- Como se puede ver en la imagen siguiente, se ha detectado un dispositivo PLC Siemens en la dirección IP 10.0.2.4 y del que nos muestra diferente información, como el tipo y versión de *hardware* y *firmware*, el nombre del PLC que es SNAP7 – Server, el nombre y número de serie del módulo, etc.
- De esta forma has realizado un escaneo de dispositivos PLC Siemens en un rango de direcciones IP, has identificado la presencia de uno de estos dispositivos y has obtenido abundante información del mismo.

```
incibe@industrial:~/Documentos/plcscan$ python2 plcscan.py 10.0.2.0/28
Scan start...
10.0.2.4:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                  : 6ES7 315-2EH14-0AB0  v.0.4      (364553)
  Basic Hardware          : 6ES7 315-2EH14-0AB0  v.0.4      (364553)
  Basic Firmware          :                               v.3.2.6    (202020)
  Unknown (129)           : Boot Loader             A          (426f6f)
  Name of the PLC          : SNAP7-SERVER          (534e41)
  Name of the module        : CPU 315-2 PN/DP       (435055)
  Plant identification      :                               (000000)
  Copyright                : Original Siemens Equipment (4f7269)
  Serial number of module  : S C-C2UR28922012      (532043)
  Module type name          : CPU 315-2 PN/DP       (435055)
  Serial number of memory card: MMC 267FF11F      (4d4d43)
  Manufacturer and profile of a CPU module:  *
  OEM ID of a module        :
  Location designation of a module:
Scan complete
incibe@industrial:~/Documentos/plcscan$
```

Ilustración 140: Detección de dispositivo PLC Siemens.

AGRUPACIÓN DE MÁQUINAS

10



10 AGRUPACIÓN DE MÁQUINAS

En este apartado, vas a crear un grupo para organizar la MV Entorno Industrial_Ubuntu 20.04 LTS, dentro de VirtualBox.

- Apaga la máquina virtual, pulsando en el icono de «encender/apagar» de la esquina superior derecha.

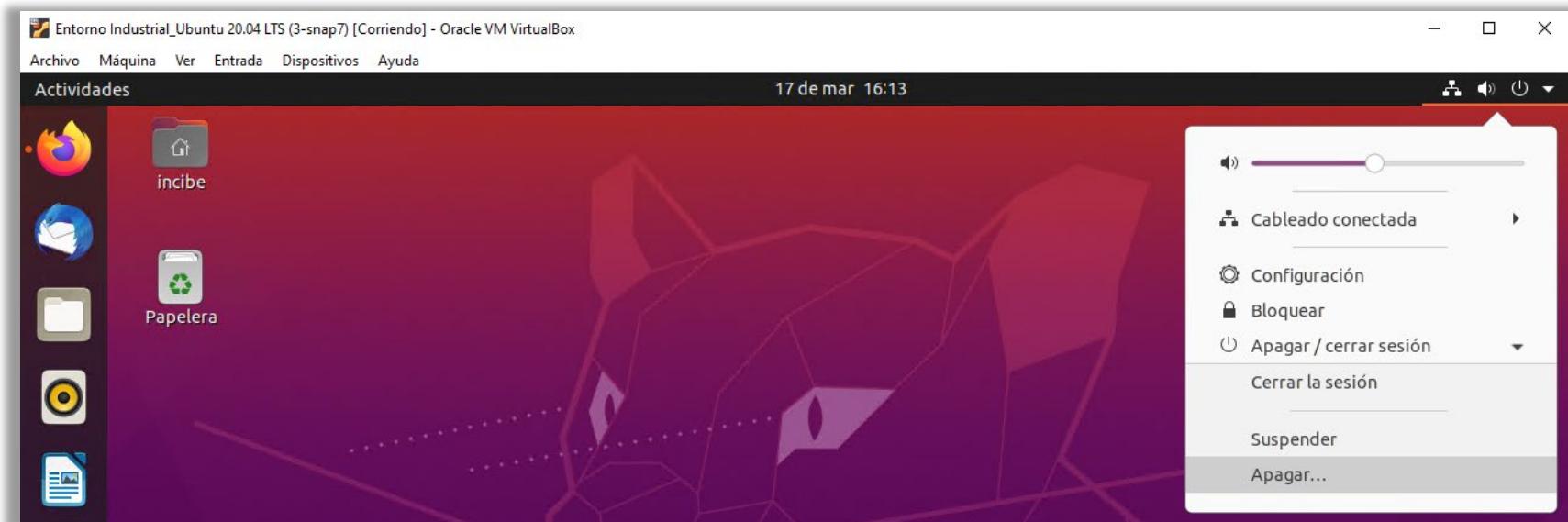


Ilustración 141: Ubicación de apagado de la máquina.

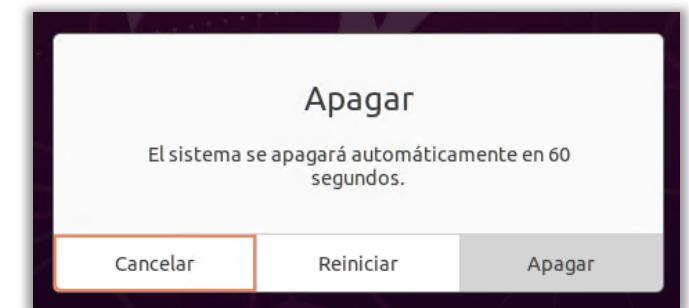


Ilustración 142: Mensaje de confirmación de apagar la máquina.

10 AGRUPACIÓN DE MÁQUINAS

- Con la máquina apagada, haz clic en su entrada y selecciona la opción agrupar.

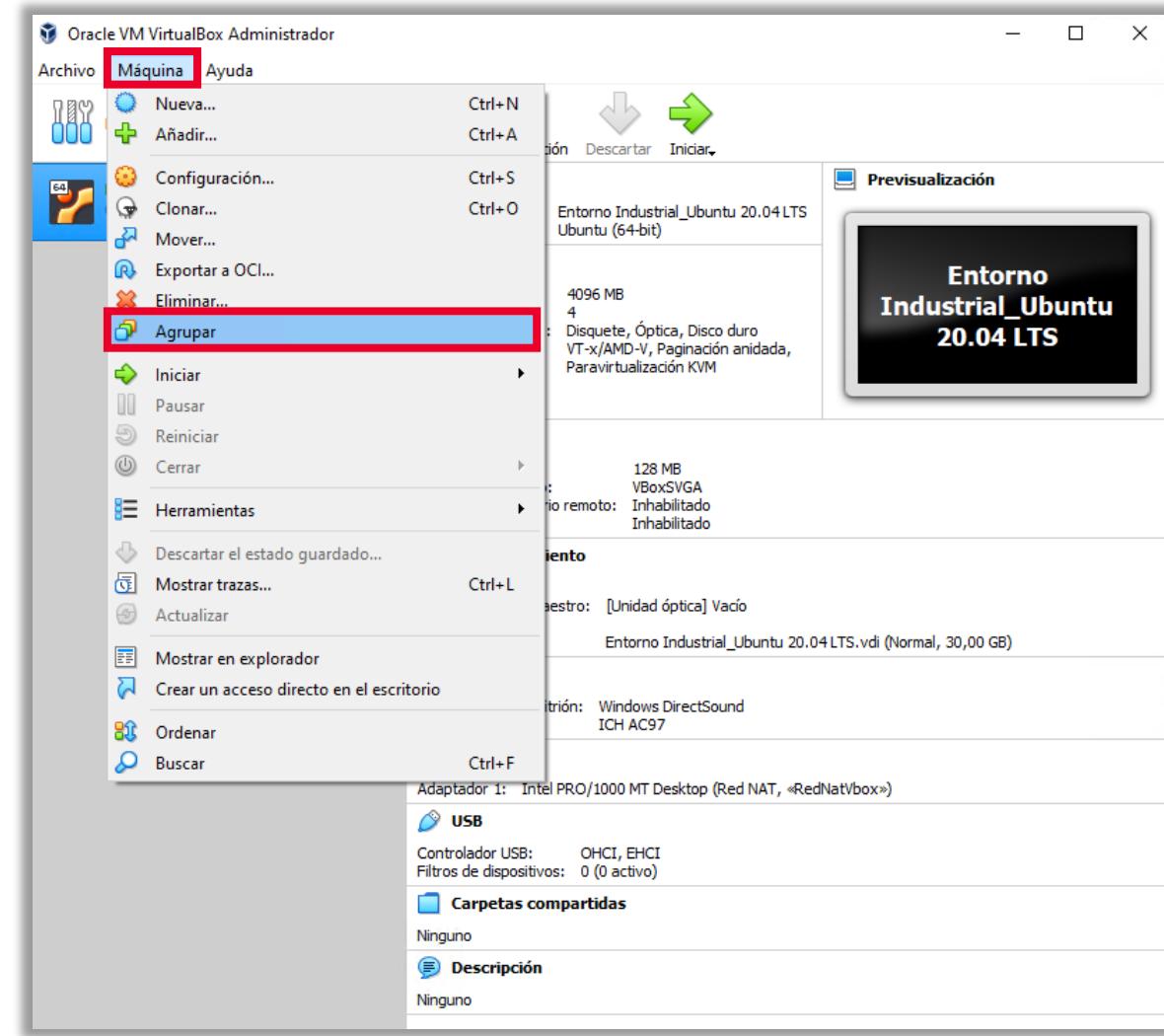


Ilustración 143: Inicio de la máquina.

10 AGRUPACIÓN DE MÁQUINAS

- Selecciona la entrada «Nuevo grupo» (que se nos acaba de crear), haz clic con el botón derecho del ratón y selecciona «Renombrar grupo». Establecemos el nombre «PLANTA INDUSTRIAL».

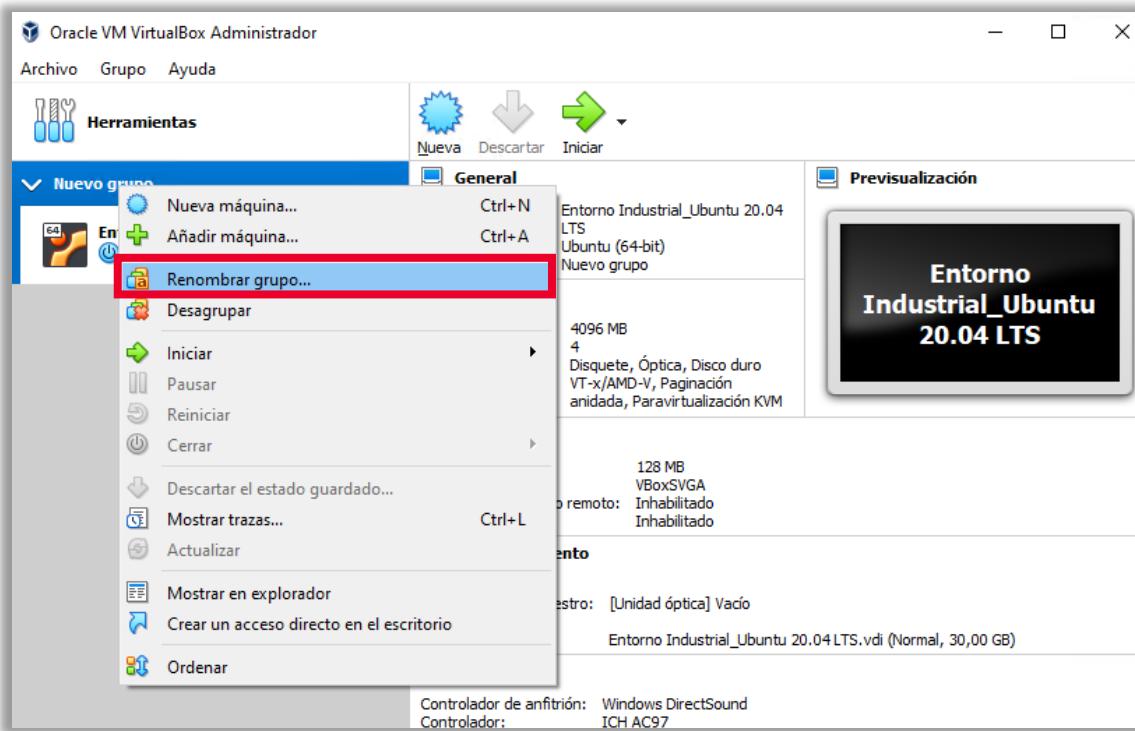


Ilustración 144: Renombrar grupo en la nueva máquina.

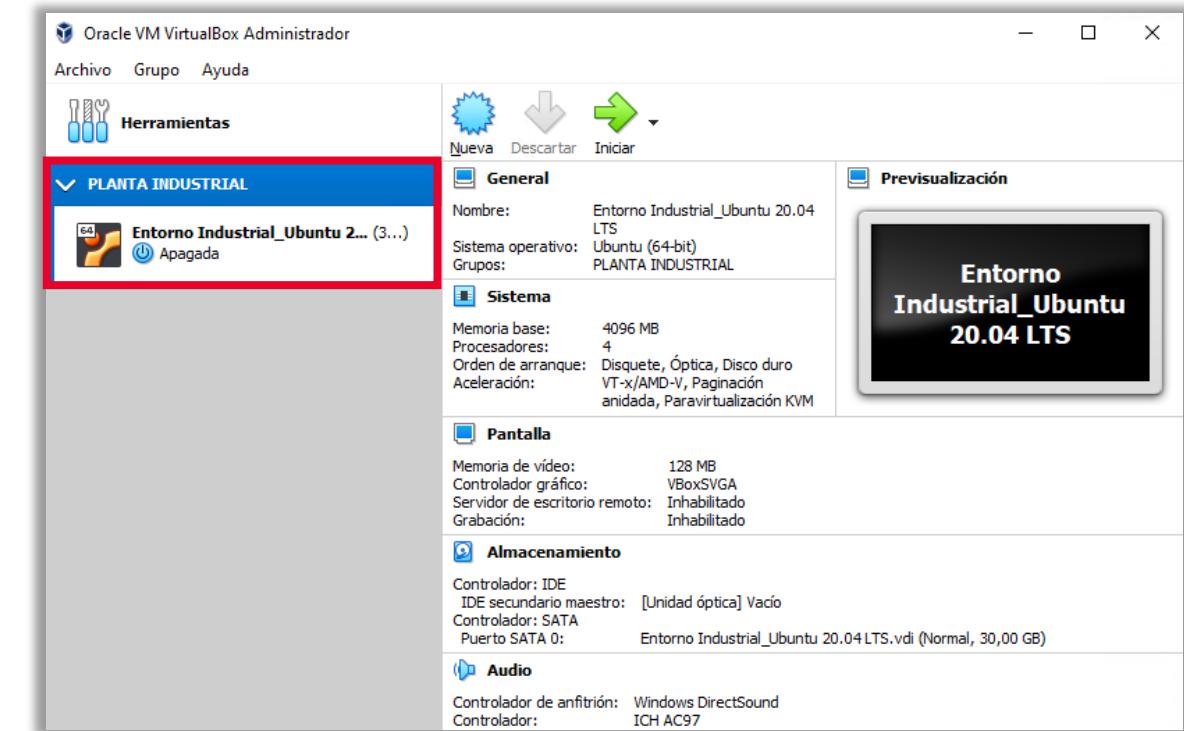


Ilustración 145: Nuevo grupo con la máquina apagada.

¡Enhorabuena!

Ya tenemos nuestro entorno
industrial virtual listo.



¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 incibe

INSTITUTO NACIONAL DE CIBERSEGURIDAD

