



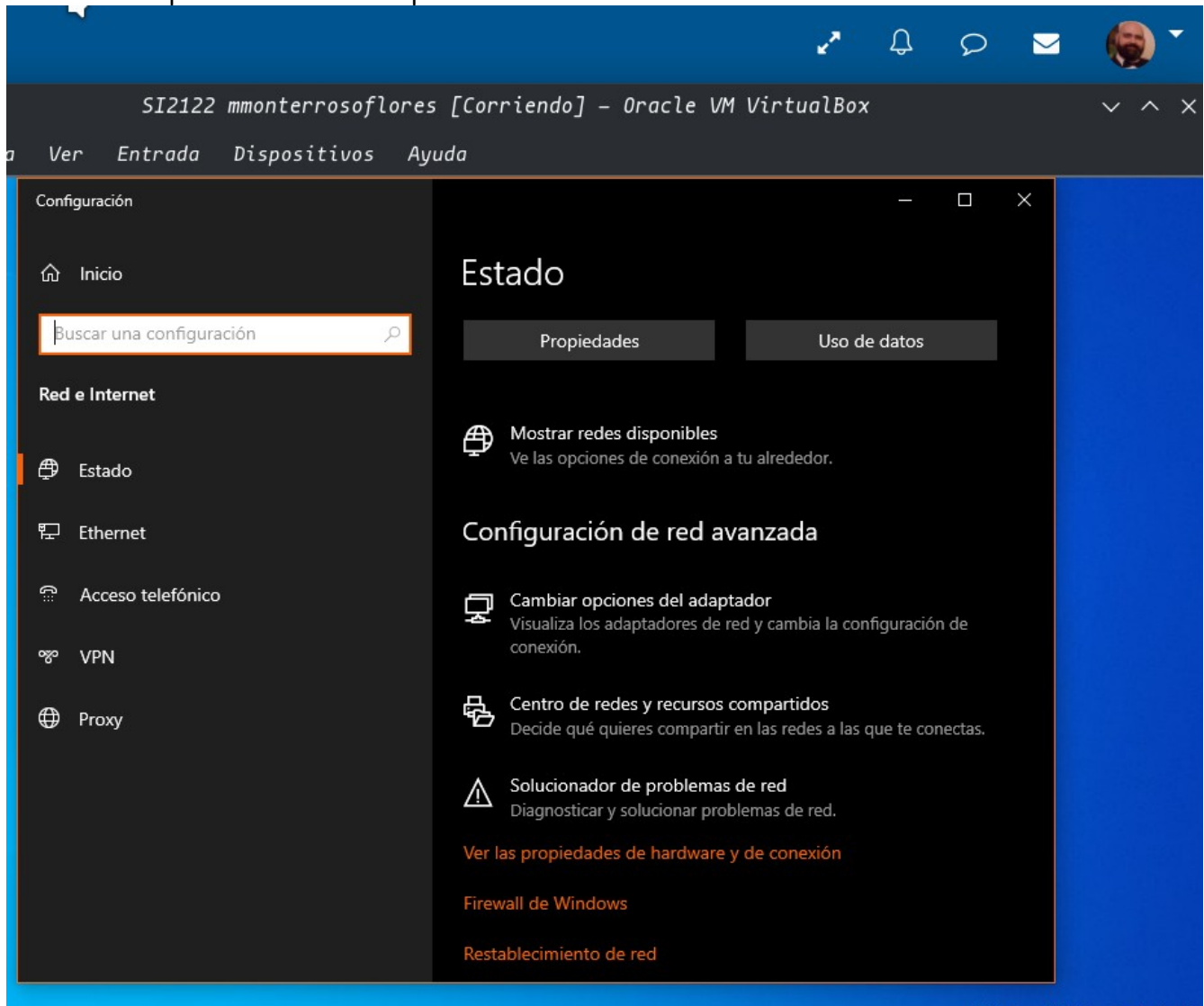
ADMINISTRACIÓN DE REDES EN WINDOWS 10 EN UNA MÁQUINA VIRTUAL

***Manuel Monterroso
Flores***

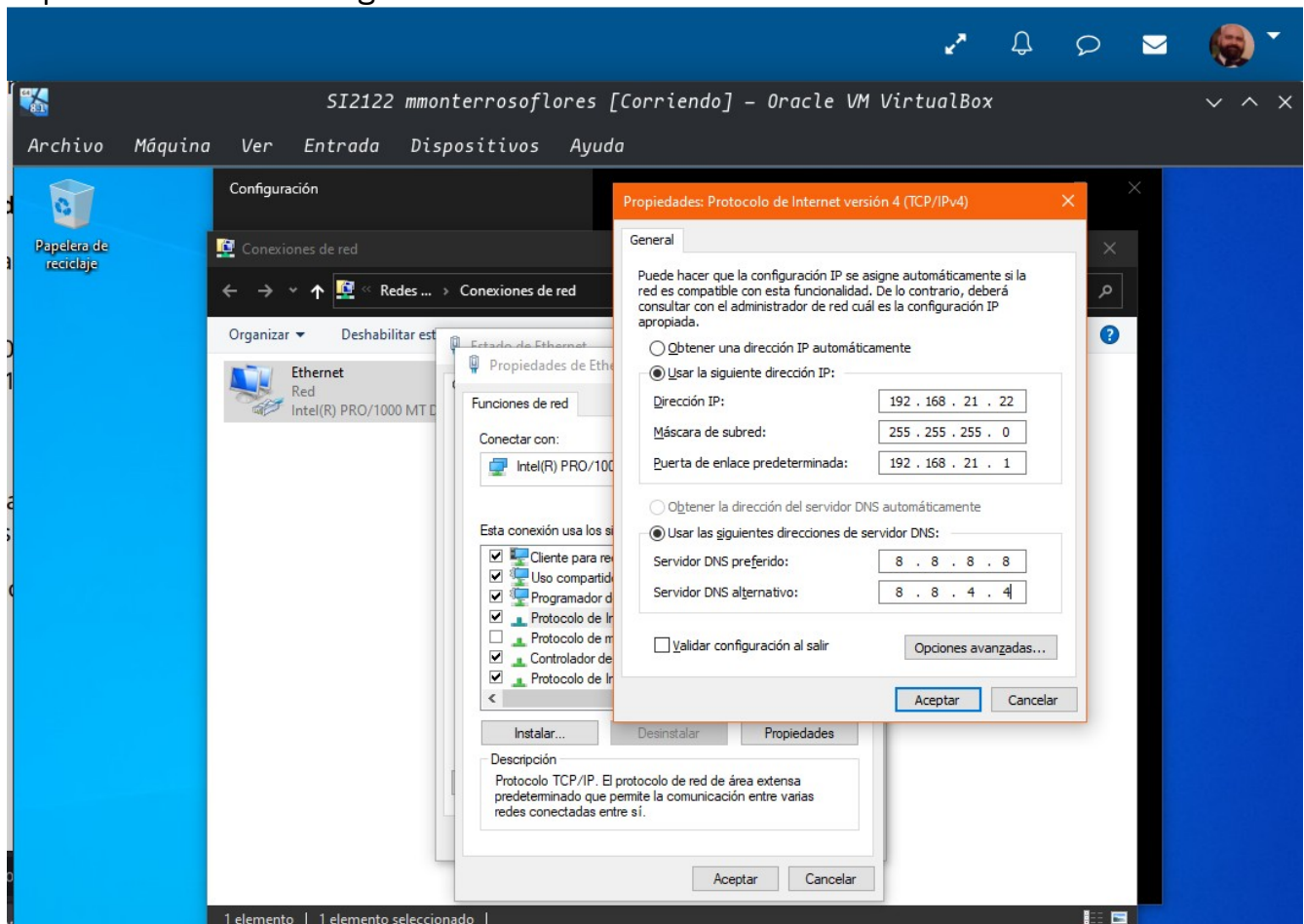
ÍNDICE:

ACTIVIDAD 01.....	03
ACTIVIDAD 02.....	08
ACTIVIDAD 03.....	09
ACTIVIDAD 04.....	14
ACTIVIDAD 05.....	16
ACTIVIDAD 06.....	20
ACTIVIDAD 07.....	23

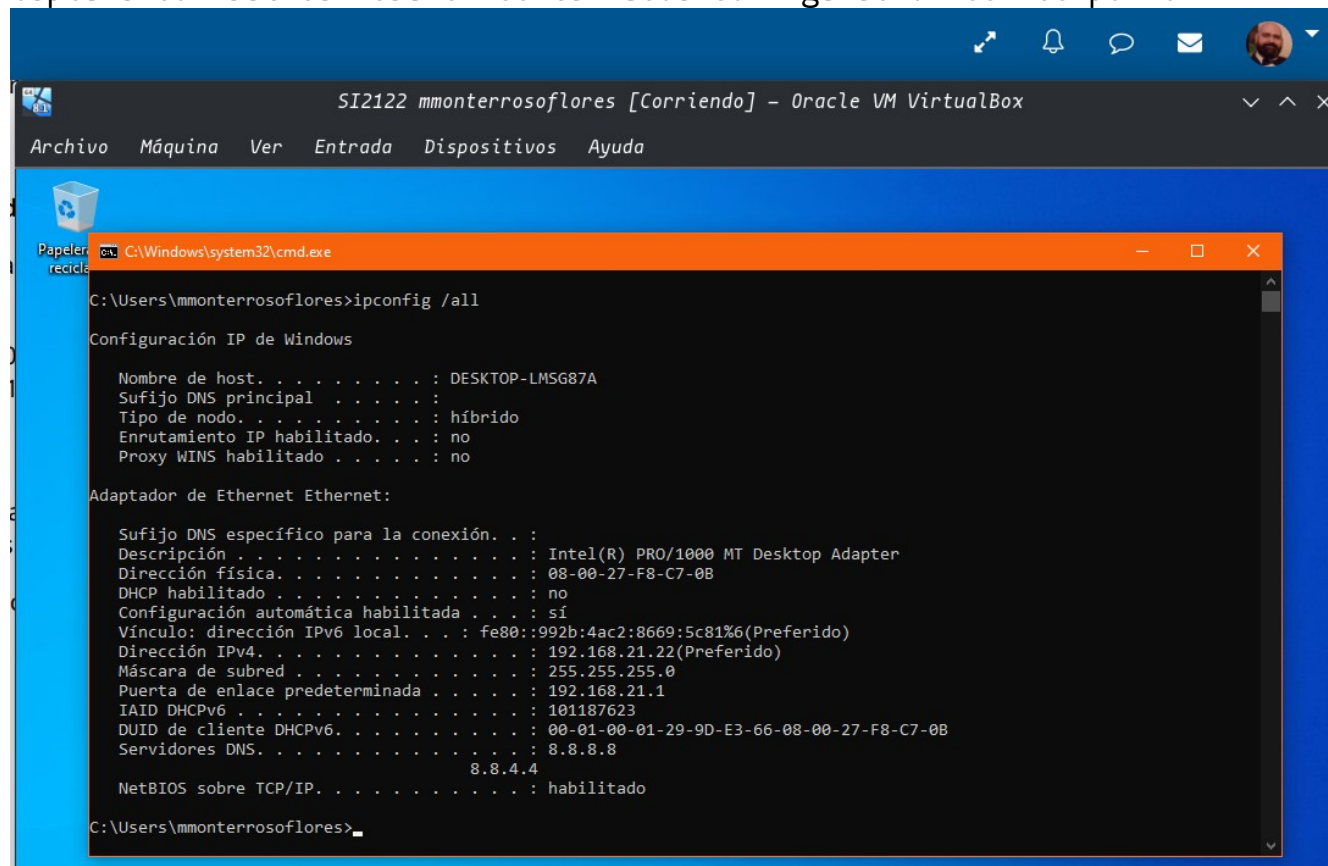
Actividad 1.- Configuración de red Ethernet y comandos básicos.
Pulsando con el botón derecho del ratón sobre el icono de red que está al lado del reloj saldrá dos opciones y nos introduciremos en “Abrir configuraciones de red e internet”.
Nos saldrá una nueva ventana en donde nos introduciremos en la opción “Cambiar opciones del adaptador”.



Luego nos introducimos dentro de las opciones del adaptador dando doble clic sobre él y nos introducimos en configuración de IP4 y ahí configuraremos las rutas como piden en la tarea. Captura con la configuración.



Captura con salida resumen de la nueva configuración de red por CMD.



```
C:\Windows\system32\cmd.exe

C:\Users\mmonterrosflores>ipconfig /all

Configuración IP de Windows

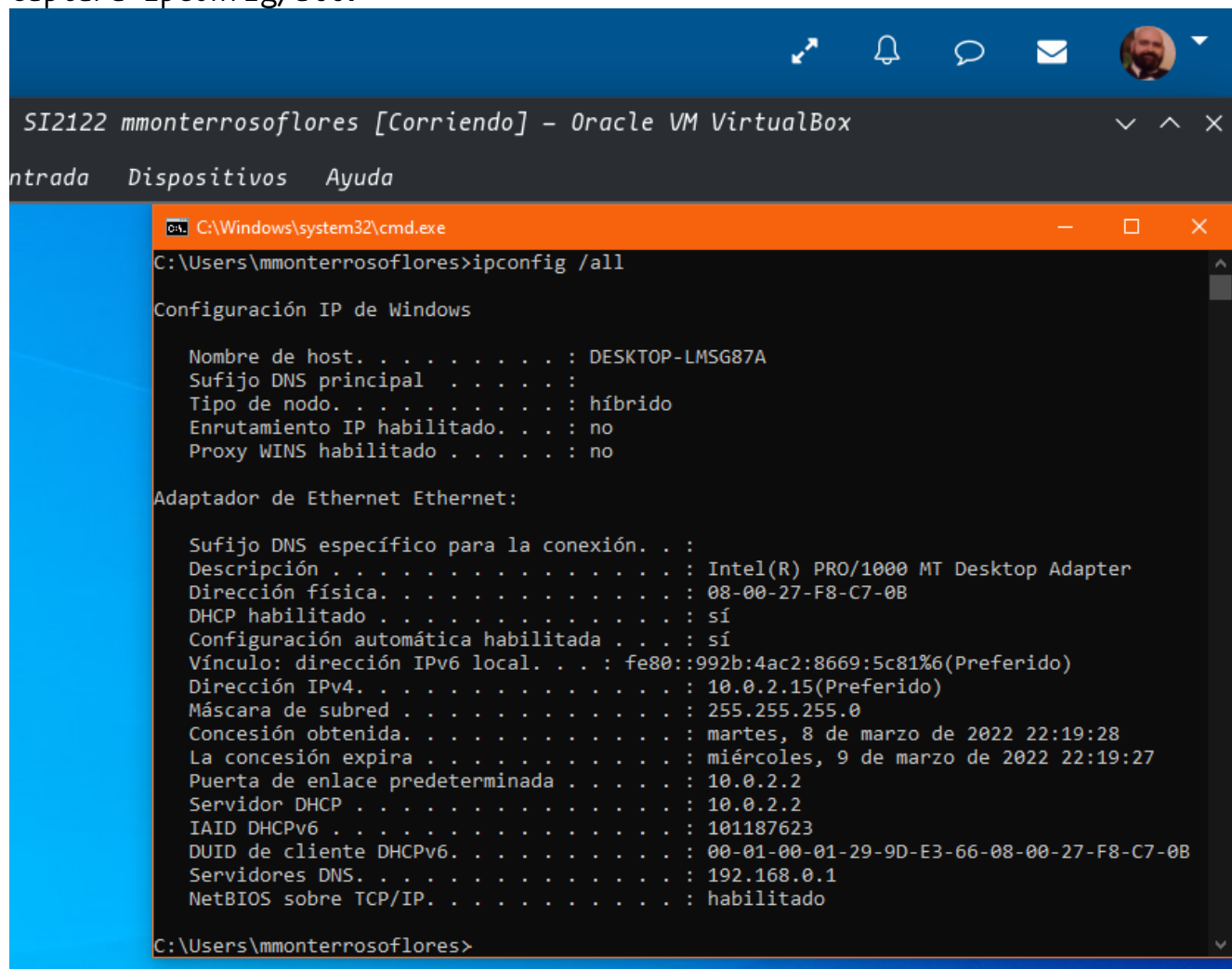
Nombre de host. . . . . : DESKTOP-LMSG87A
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-F8-C7-0B
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::992b:4ac2:8669:5c81%6(Preferido)
Dirección IPv4. . . . . : 192.168.21.22(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.21.1
IAID DHCPv6 . . . . . : 101187623
DUID de cliente DHCPv6. . . . . : 00-01-00-01-29-9D-E3-66-08-00-27-F8-C7-0B
Servidores DNS. . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS sobre TCP/IP. . . . . : habilitado

C:\Users\mmonterrosflores>
```

Segundo apartado, ejecutamos los comandos que nos piden la tarea tras volver a la configuración de la configuración del adaptador.
Captura ipconfig/all.



The screenshot shows a Windows command prompt window titled "SI2122 mmonterrosoflores [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Entrada", "Dispositivos", and "Ayuda". The command prompt shows the execution of the command `ipconfig /all` from the directory `C:\Users\mmonterrosoflores`. The output displays the Windows IP configuration and the Ethernet adapter details.

```
C:\Users\mmonterrosoflores>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : DESKTOP-LMSG87A
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-F8-C7-0B
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::992b:4ac2:8669:5c81%6(Preferido)
Dirección IPv4. . . . . : 10.0.2.15(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 8 de marzo de 2022 22:19:28
La concesión expira . . . . . : miércoles, 9 de marzo de 2022 22:19:27
Puerta de enlace predeterminada . . . . . : 10.0.2.2
Servidor DHCP . . . . . : 10.0.2.2
IAID DHCPv6 . . . . . : 101187623
DUID de cliente DHCPv6. . . . . : 00-01-00-01-29-9D-E3-66-08-00-27-F8-C7-0B
Servidores DNS. . . . . : 192.168.0.1
NetBIOS sobre TCP/IP. . . . . : habilitado

C:\Users\mmonterrosoflores>
```

Captura hostname, nslookup y ping.

```
SI2122 mmonterrosoflores [Corriendo] - Oracle VM VirtualBox
Entrada Dispositivos Ayuda

C:\Windows\system32\cmd.exe

C:\Users\mmonterrosoflores>hostname
DESKTOP-LMSG87A

C:\Users\mmonterrosoflores>nslookup www.wikipedia.com
Servidor: dlinkrouter
Address: 192.168.0.1

Respuesta no autoritativa:
Nombre: ncredir-lb.wikimedia.org
Addresses: 2620:0:862:ed1a::3
           91.198.174.194
Alias: www.wikipedia.com

C:\Users\mmonterrosoflores>ping www.wikipedia.com

Haciendo ping a ncredir-lb.wikimedia.org [91.198.174.194] con 32 bytes de datos:
Respuesta desde 91.198.174.194: bytes=32 tiempo=75ms TTL=127
Respuesta desde 91.198.174.194: bytes=32 tiempo=77ms TTL=127
Respuesta desde 91.198.174.194: bytes=32 tiempo=72ms TTL=127
Respuesta desde 91.198.174.194: bytes=32 tiempo=72ms TTL=127

Estadísticas de ping para 91.198.174.194:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 72ms, Máximo = 77ms, Media = 74ms

C:\Users\mmonterrosoflores>
```

Captura con tracert.

```
SI2122 mmonterrosoflores [Corriendo] - Oracle VM VirtualBox
Entrada Dispositivos Ayuda

C:\Windows\system32\cmd.exe

C:\Users\mmonterrosoflores>tracert www.wikipedia.com

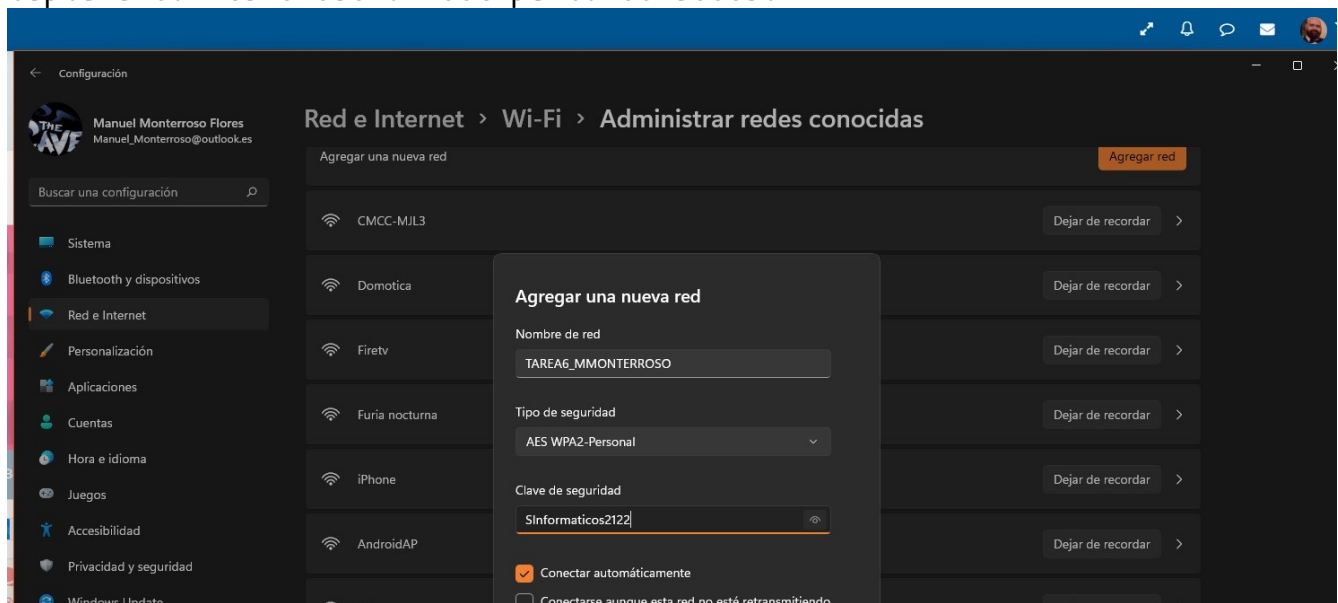
Traza a la dirección ncredir-lb.wikimedia.org [91.198.174.194]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms    10.0.2.2
 2  1 ms     1 ms     1 ms     dlinkrouter [192.168.0.1]
 3  1 ms     <1 ms    <1 ms     uisp.lan [192.168.10.1]
 4  4 ms     5 ms     5 ms     20.3.9.1
 5  50 ms    43 ms    41 ms    10.5.0.1
 6  46 ms    46 ms    51 ms    86.106.0.137
 7  *        *        *        Tiempo de espera agotado para esta solicitud.
 8  51 ms    59 ms    51 ms    be2324.ccr31.bio02.atlas.cogentco.com [154.54.61.129]
 9  72 ms    64 ms    63 ms    be2315.ccr41.par01.atlas.cogentco.com [154.54.61.114]
10  71 ms    75 ms    134 ms   be12265.ccr41.ams03.atlas.cogentco.com [130.117.2.141]
11  74 ms    74 ms    74 ms    be2434.agr21.ams03.atlas.cogentco.com [130.117.2.241]
12  72 ms    70 ms    73 ms    149.11.65.174
13  74 ms    74 ms    76 ms    po-4.fbx-r3.leaseweb.net [87.255.32.121]
14  71 ms    75 ms    74 ms    87.255.35.66
15  76 ms    80 ms    76 ms    ncredir-lb.esams.wikimedia.org [91.198.174.194]

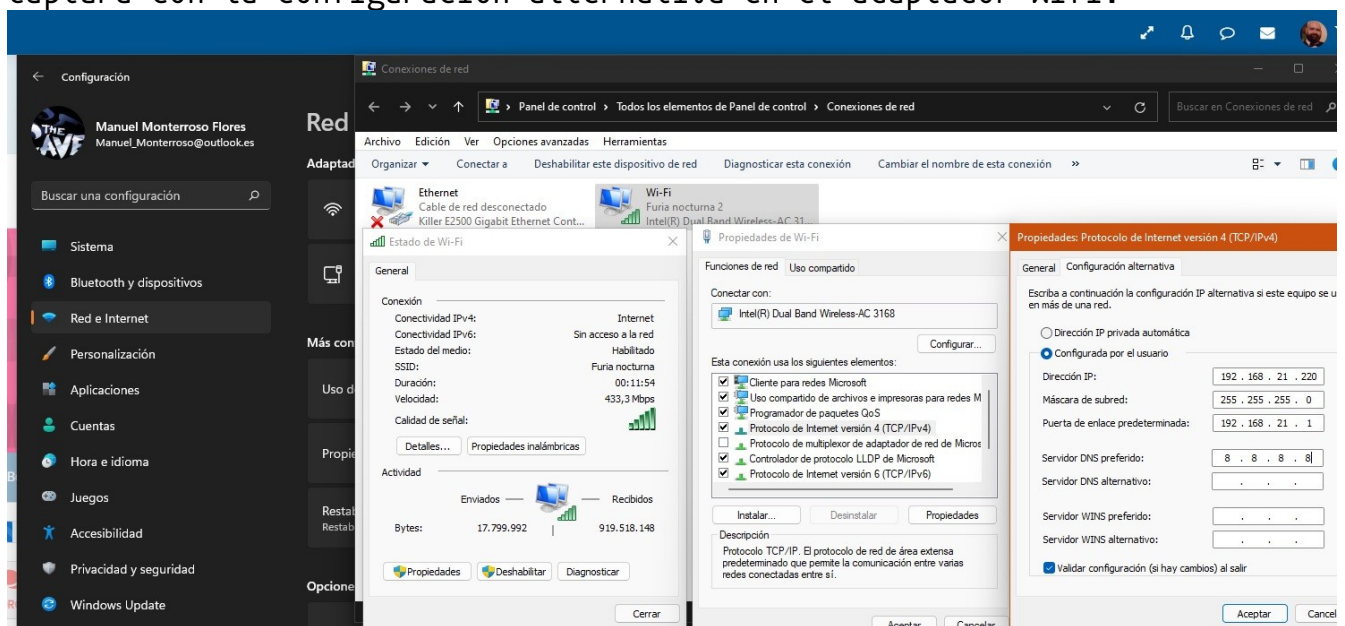
Traza completa.

C:\Users\mmonterrosoflores>
```

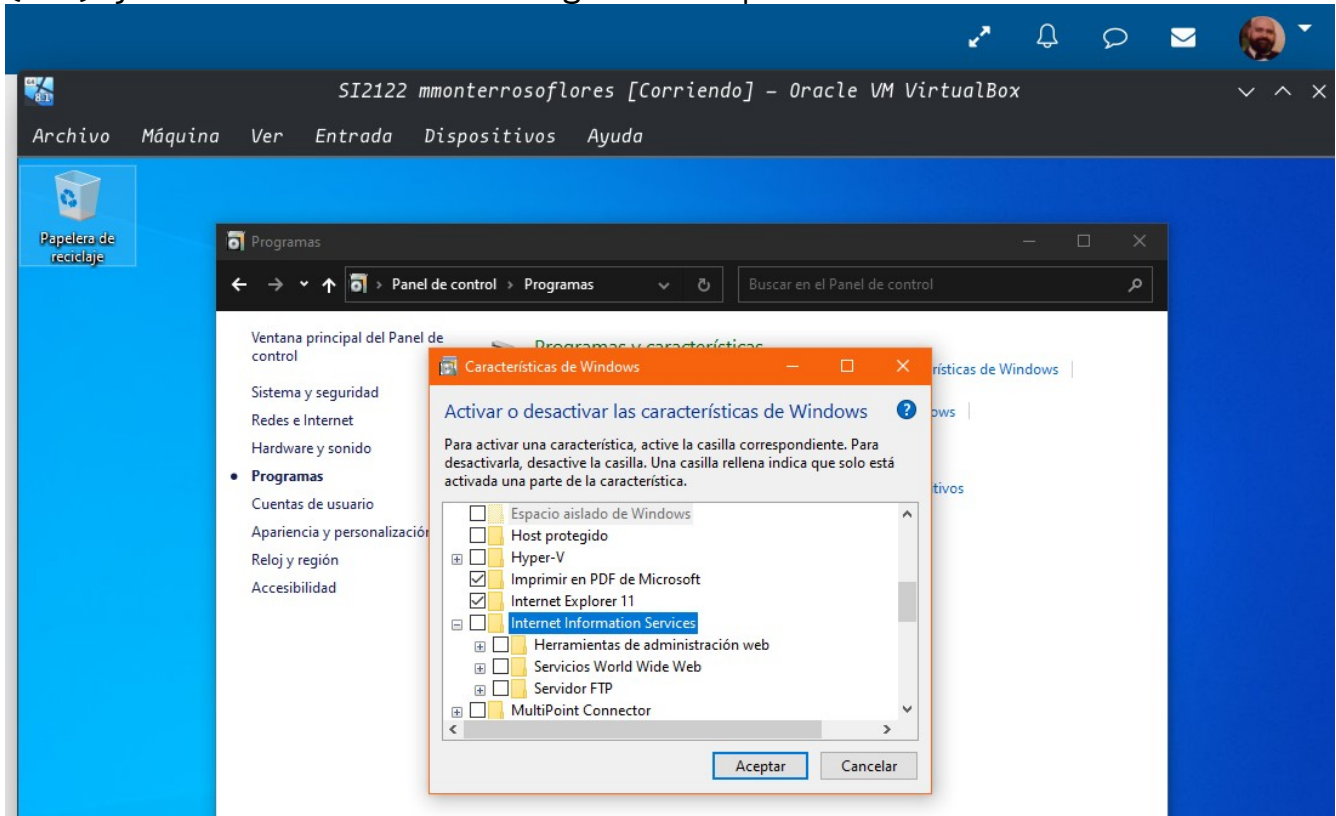

Actividad 2.- Configuración de red Wi-Fi. Captura con la creación del punto de acceso.



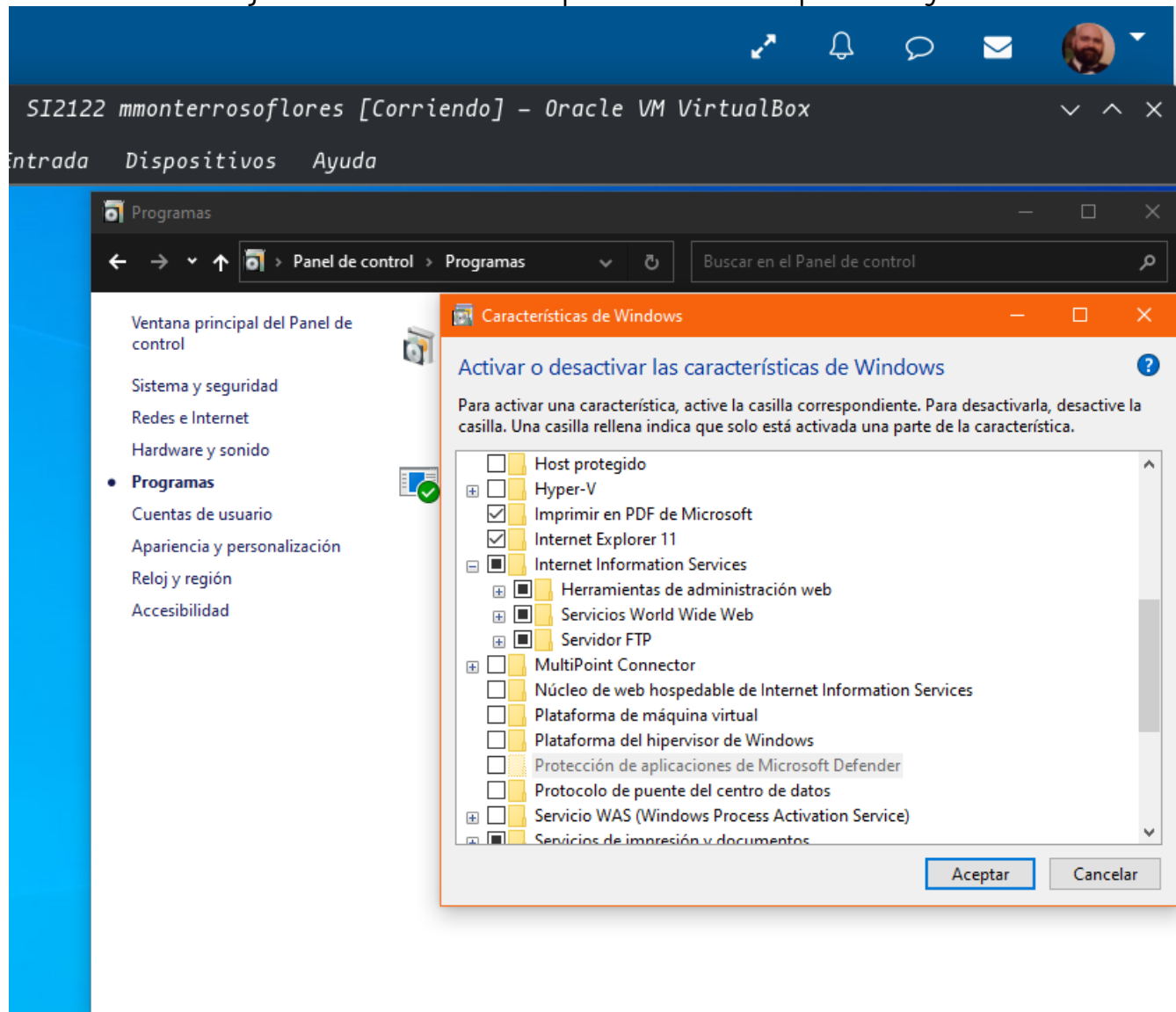
Captura con la configuración alternativa en el adaptador wifi.



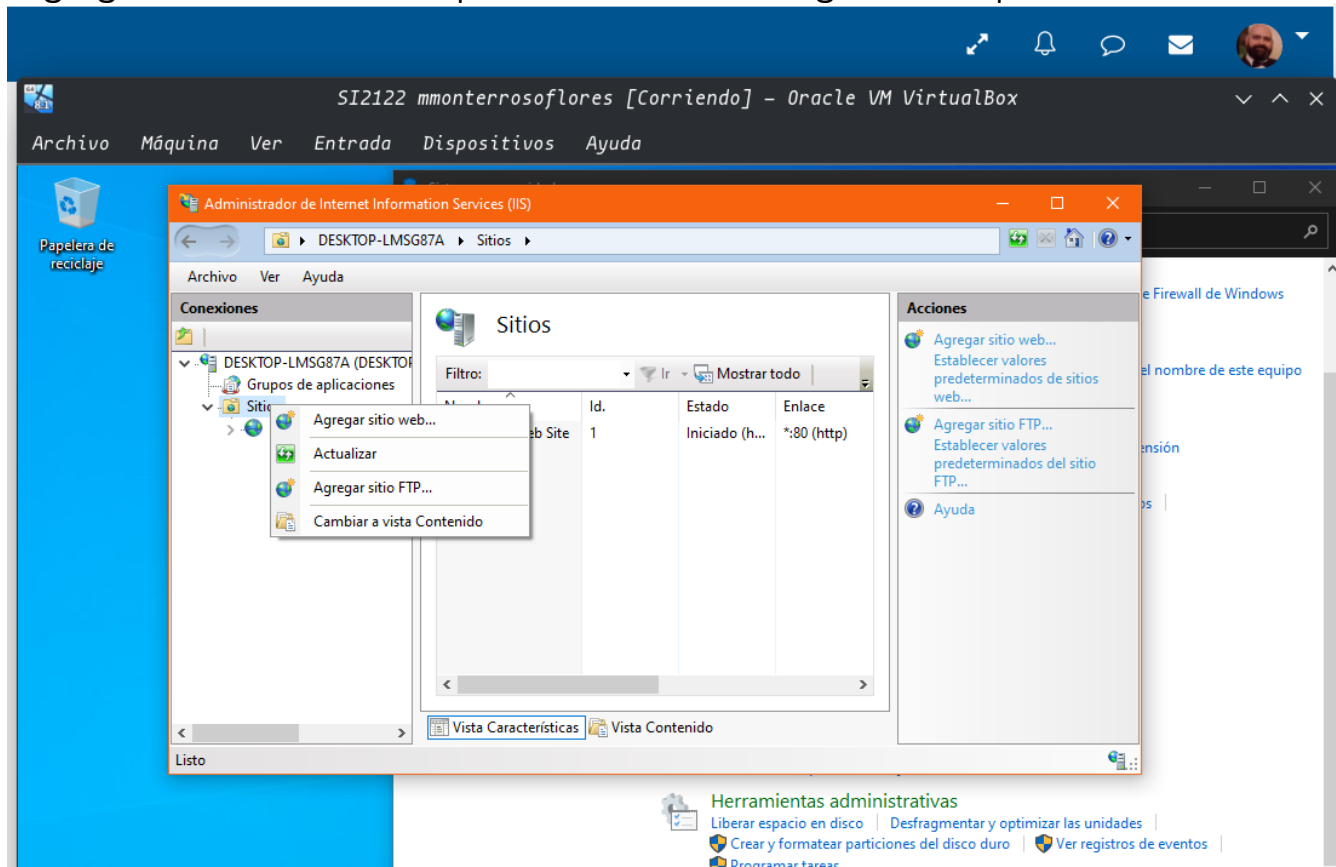
Actividad 3.- Establecer un servidor FTP básico en Windows 10.
Primero tendremos que activar el servidor FTP en windows, eso se realiza entrando en panel de control y dentro buscamos el apartado “Programas” y dentro seleccionamos “Activar o desactivar las características de Windows” y dentro buscamos la opción “Internet Information Services (IIS)”, como mostramos en la siguiente captura.



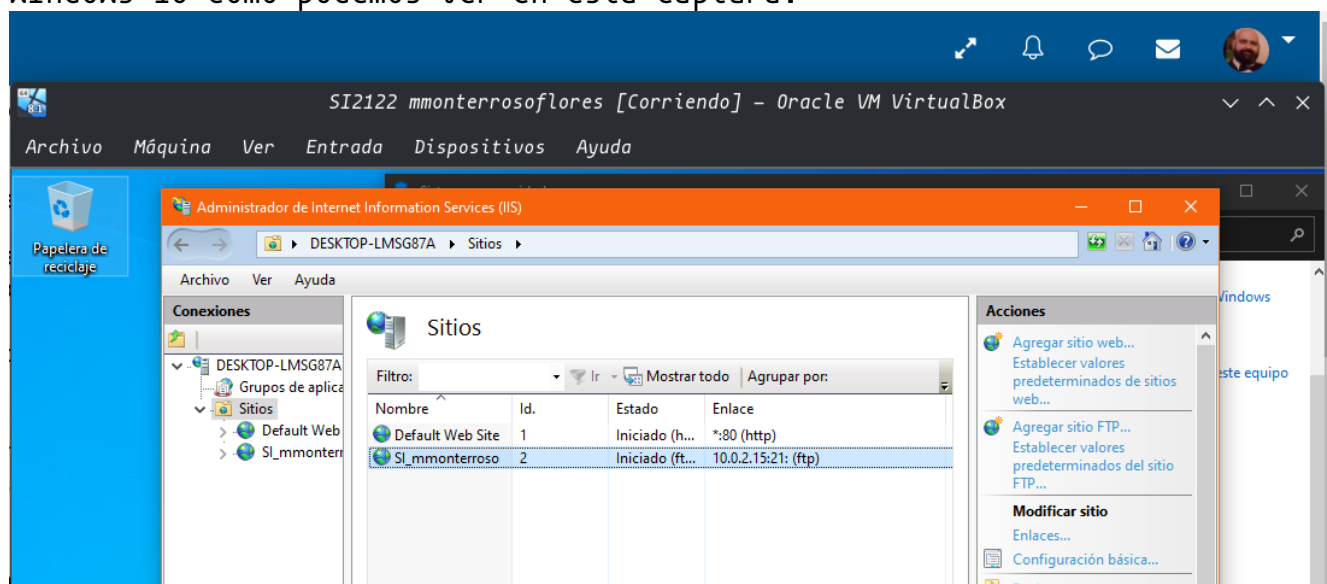
Y en este apartado activamos la opción en si misma pero luego deberemos de señalar el del servidor de FTP porque no lo hará al seleccionar la opción Padre y le daremos a aceptar y esperamos que se instale las nuevas características, ahora mostramos captura con las opciones ya activadas.



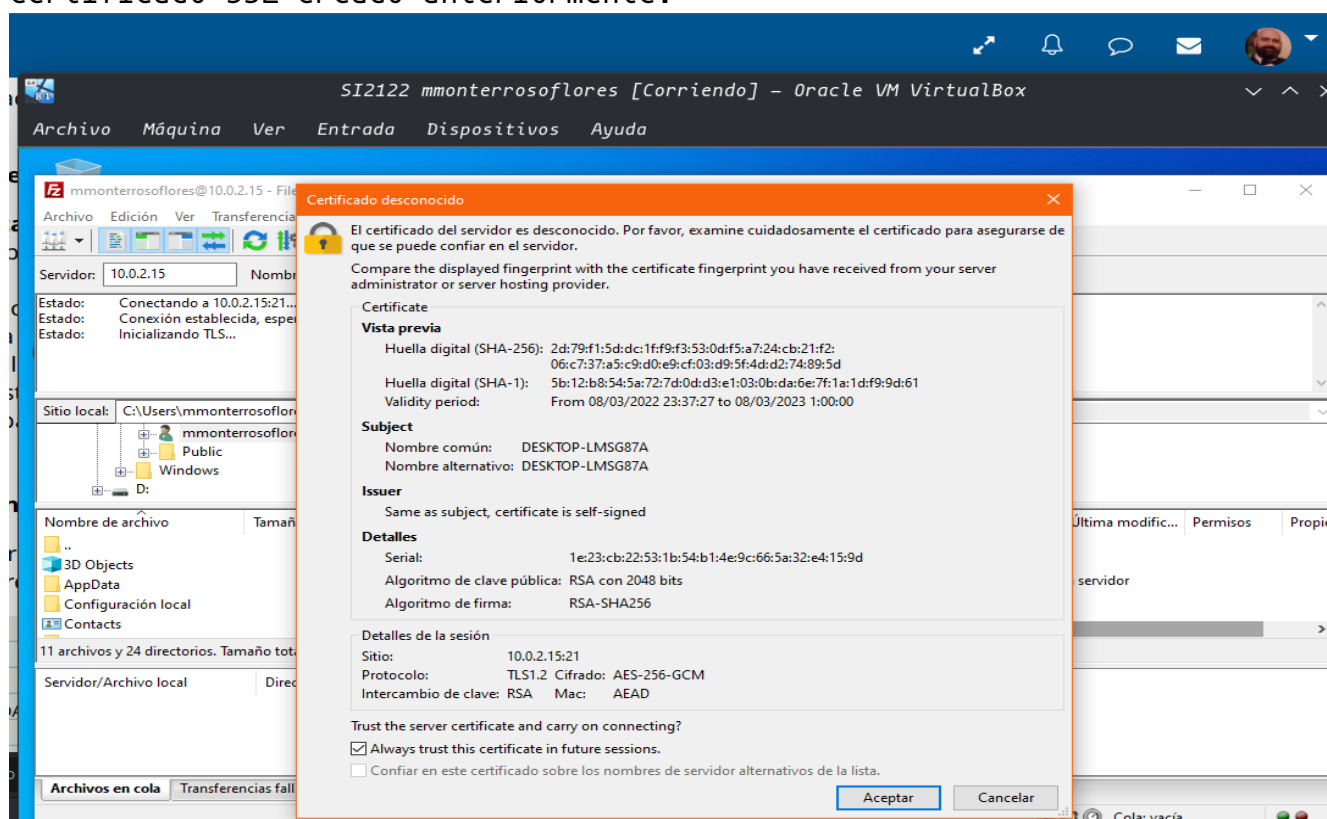
Ahora volvemos al panel de control y entramos en la opción “Sistema y Seguridad” y dentro le damos a “Herramientas Administrativas”, dentro de la nueva ventana en la parte de la derecha buscamos la opción “Administrador IIS”, dentro primero crearemos un certificado SSL en la opción de IIS y luego tras crear el certificado SSL volvemos a la pantalla principal y en la parte de la izquierda le damos con el botón derecho del ratón sobre la opción “Sitios” y del menú seleccionamos “Agregar sitio FTP” como podemos ver en la siguiente captura.



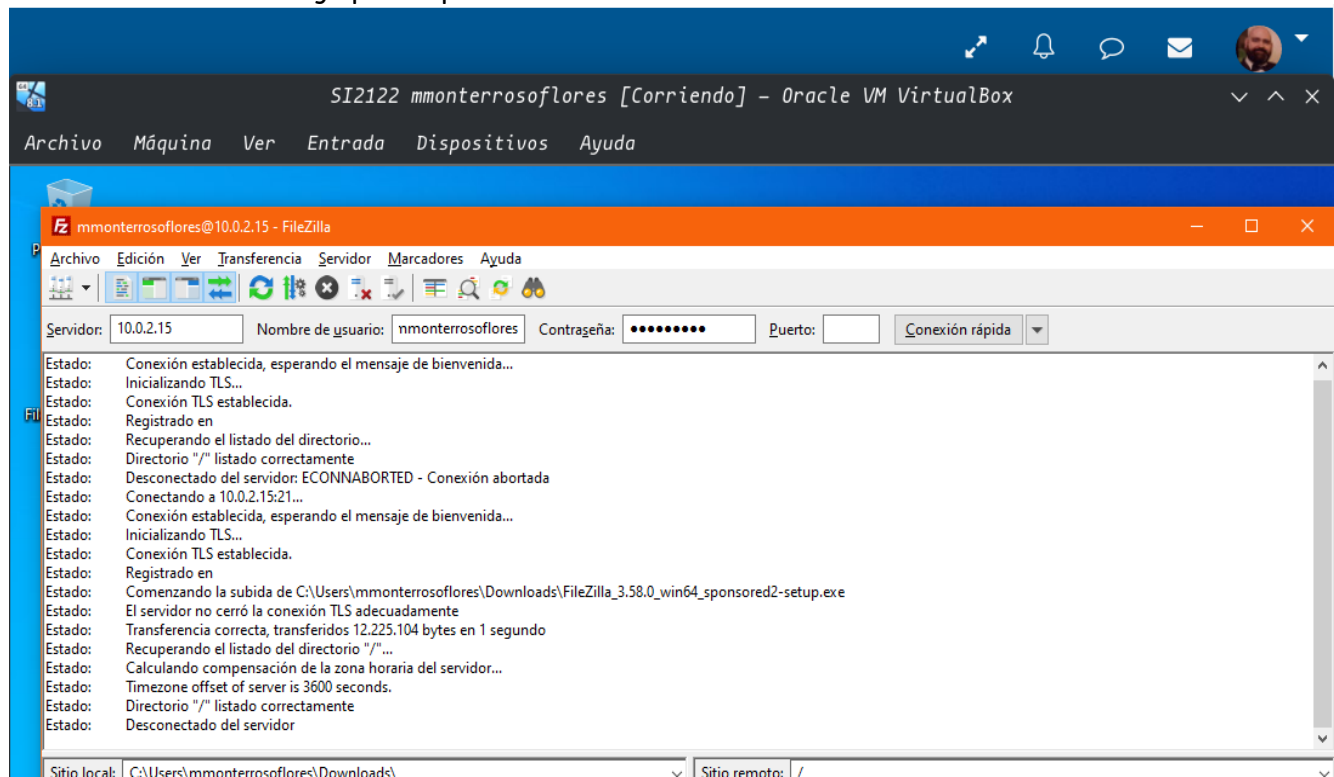
Rellenamos todos los datos y cuando pidan certificado seleccionamos el que hemos creado y ya con esto tenemos creado el servidor FTP dentro de windows 10 como podemos ver en esta captura.



Para probar la configuración vamos a instalar el programa Filezilla. Captura que al intentar entrar en el servidor FTP pide que aceptemos el certificado SSL creado anteriormente.

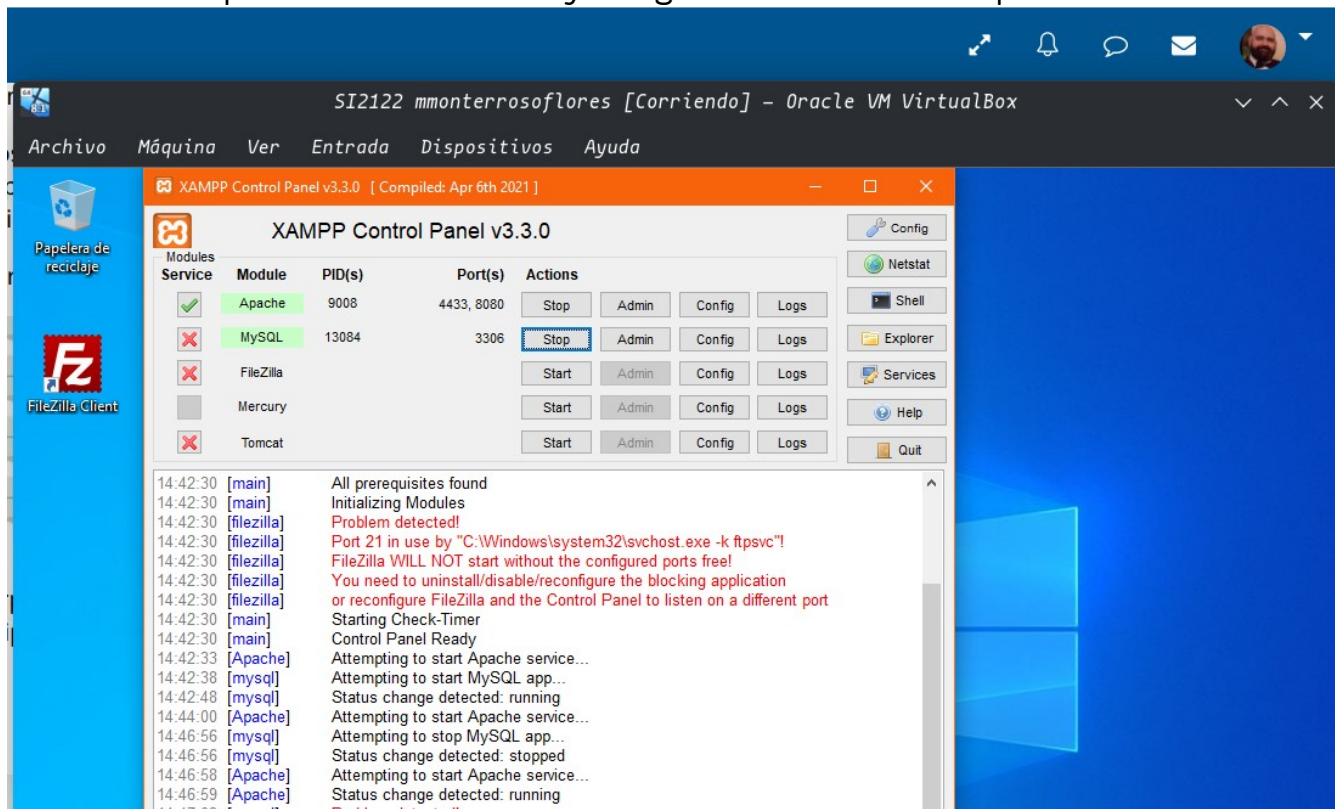


Captura donde se puede comprobar la conexión con el usuario de windows y con conexión TLS y para probar he transferido un archivo.



Actividad 4.- Servidor web en Windows 10.

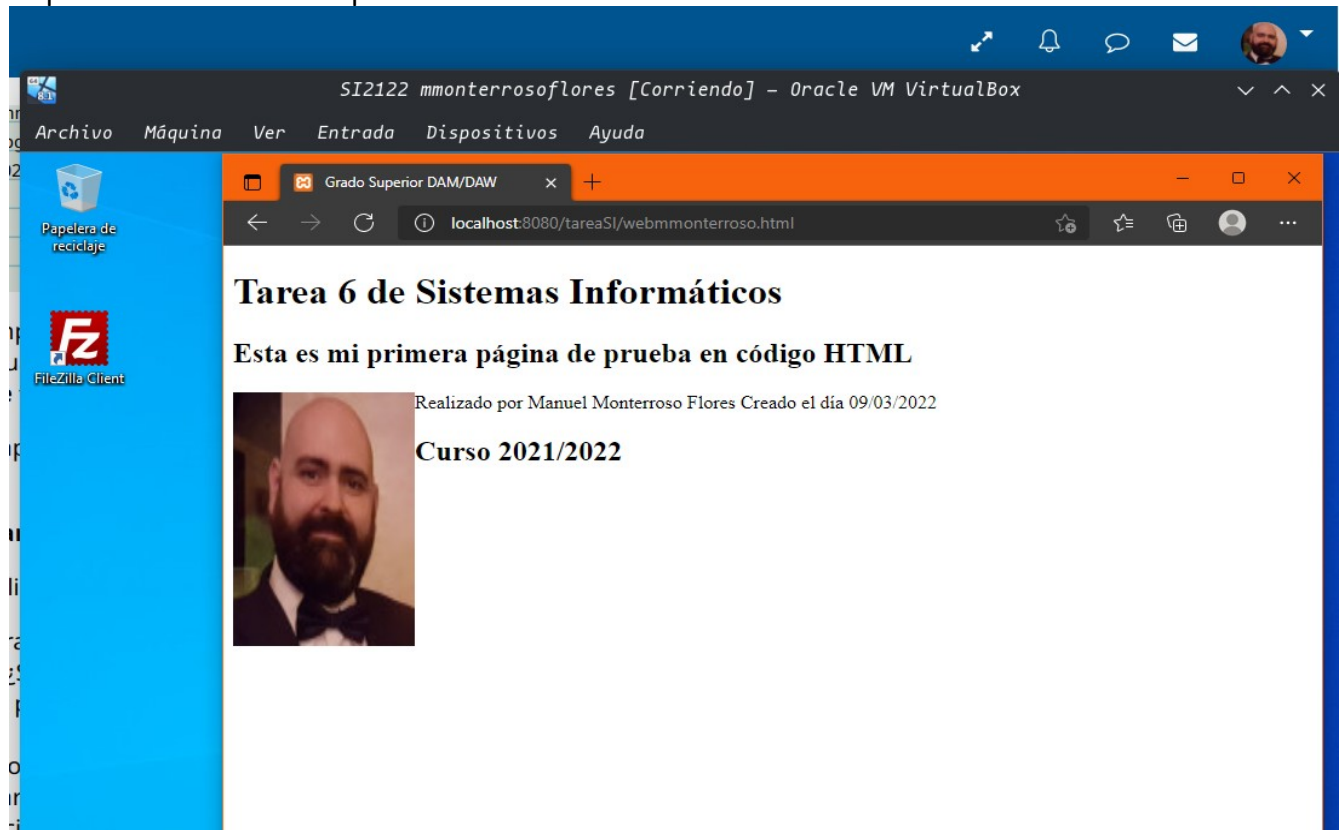
Nos descargamos el programa XAMPP y lo instalamos, tras instalarlo cambiamos el puerto predeterminado, el 80, por el puerto , tras ello creamos un archivo de texto con el código que nos pone en la tarea modificando por los datos míos y lo guardamos en la carpeta



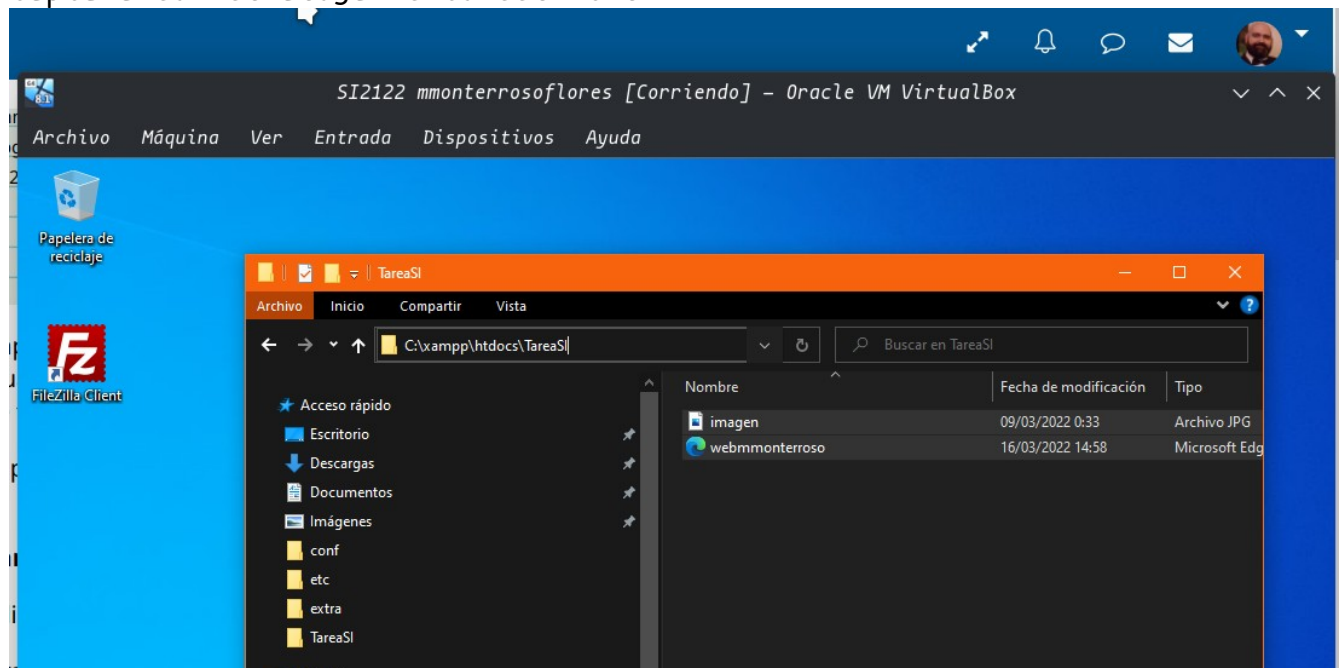
Captura con la web de XAMPP en el localhost y el puerto 8080.



Captura con la web personal iniciada.



Captura con el alojamiento del html.

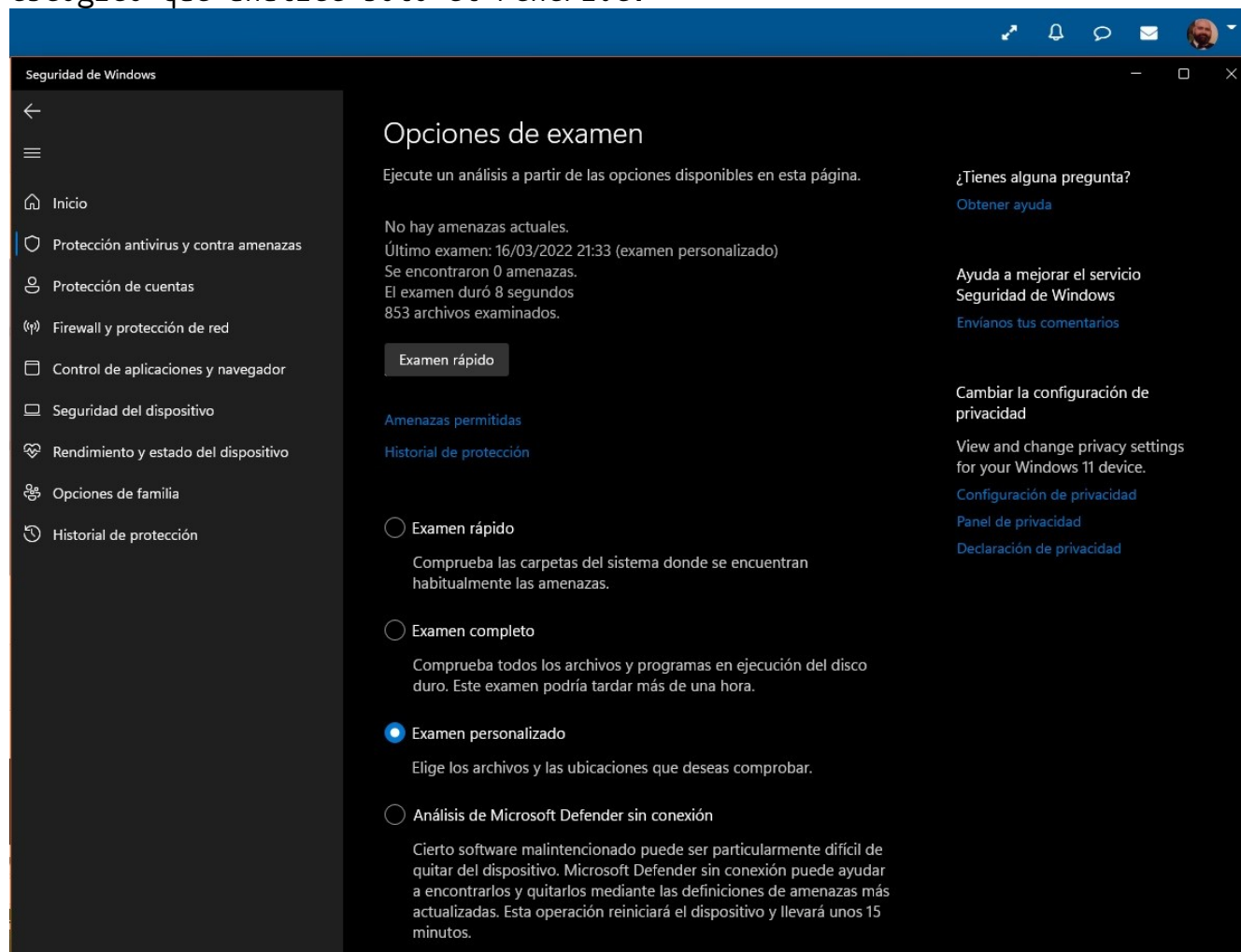


Actividad 5.- Utilización de Antivirus.

Para esta actividad vamos a utilizar el propio antivirus de Microsoft que viene instalado en el propio Windows 11, Windows Defender.

Uso la versión de Windows 11 porque soy Insiders y además del canal alpha por tanto siempre tengo la última versión de este SO.

Captura con el análisis de un Pendrive con Windows Defender, para realizar este análisis he escogido la opción de Examen personalizado y he escogido que analice solo el Pendrive.



Vemos en este análisis que no se ha encontrado ningún tipo de amenaza, pero si hubiera salido alguna siempre te saldrán distintas opciones que son permitir (no se borra la amenaza y no se vuelve a analizar), que se escogería por ejemplo para archivos que nosotros mismos sepamos que no son peligrosos como por ejemplo un analizador de red wifi que pueda cree el antivirus que es un analizador de equipos como un troyano, la siguiente opción sería poner en cuarentena (que no borra el archivo pero el antivirus lo sigue analizando y sobre todo sus cambios o los cambios que

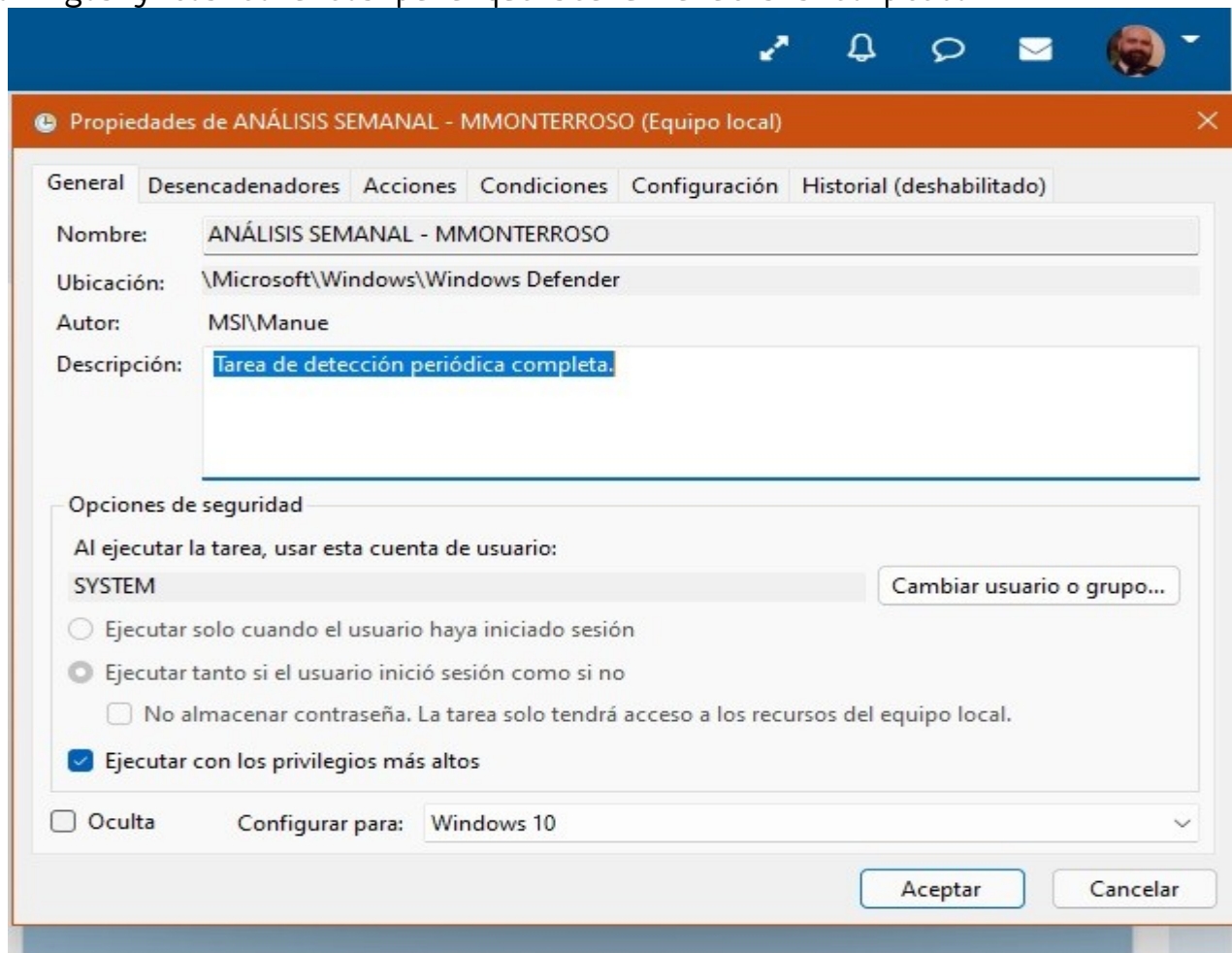
pueda hacer en el equipo), que lo haremos para archivos que no sepamos si son inofensivos o si son peligrosos y que creamos que son necesarios para cualquier programa o plugin y por último tenemos la opción de eliminar (borrar la amenaza), que lo que hará es borrar el archivo si sabemos que puede ser peligroso.

Fuente para el segundo apartado:

<https://www.thewindowsclub.com/schedule-scans-in-windows-defender>

En la fuente se puede ver que en el planificador de tareas de Windows se puede configurar cuando queremos que pase el análisis y también el tipo porque un análisis completo incluye tanto las memorias externas conectadas como todos los discos duros del equipo.

Capturas con el análisis programado para que sea semanal, todos los domingos y los comandos para que sea un análisis completo.



Propiedades de ANÁLISIS SEMANAL - MMONTERROSO (Equipo local)

General

Desencadenadores

Acciones

Condiciones

Configuración

Historial (deshabilitado)

Cuando se crea una tarea, se pueden especificar las condiciones que la activarán.

Editar desencadenador

Iniciar la tarea: Según una programación

Configuración

☐ Una vez

☐ Diariamente

☒ Semanalmente

☐ Mensualmente

Inicio:

16/03/2022

5:00:00

☐ Sincronizar zonas

Repetir cada:

1

semanas en:

☒ Domingo

☐ Lunes

☐ Martes

☐ Miércoles

☐ Jueves

☐ Viernes

☐ Sábado

Configuración avanzada

☐ Retraso máx. (retraso aleatorio):

1 hora

☐ Repetir cada:

1 hora

durante:

1 día

☐ Detener todas las tareas en ejecución al final de la duración de repetición

☐ Detener la tarea si se ejecuta durante más de:

3 días

☐ Expiración:

16/03/2023

22:51:27

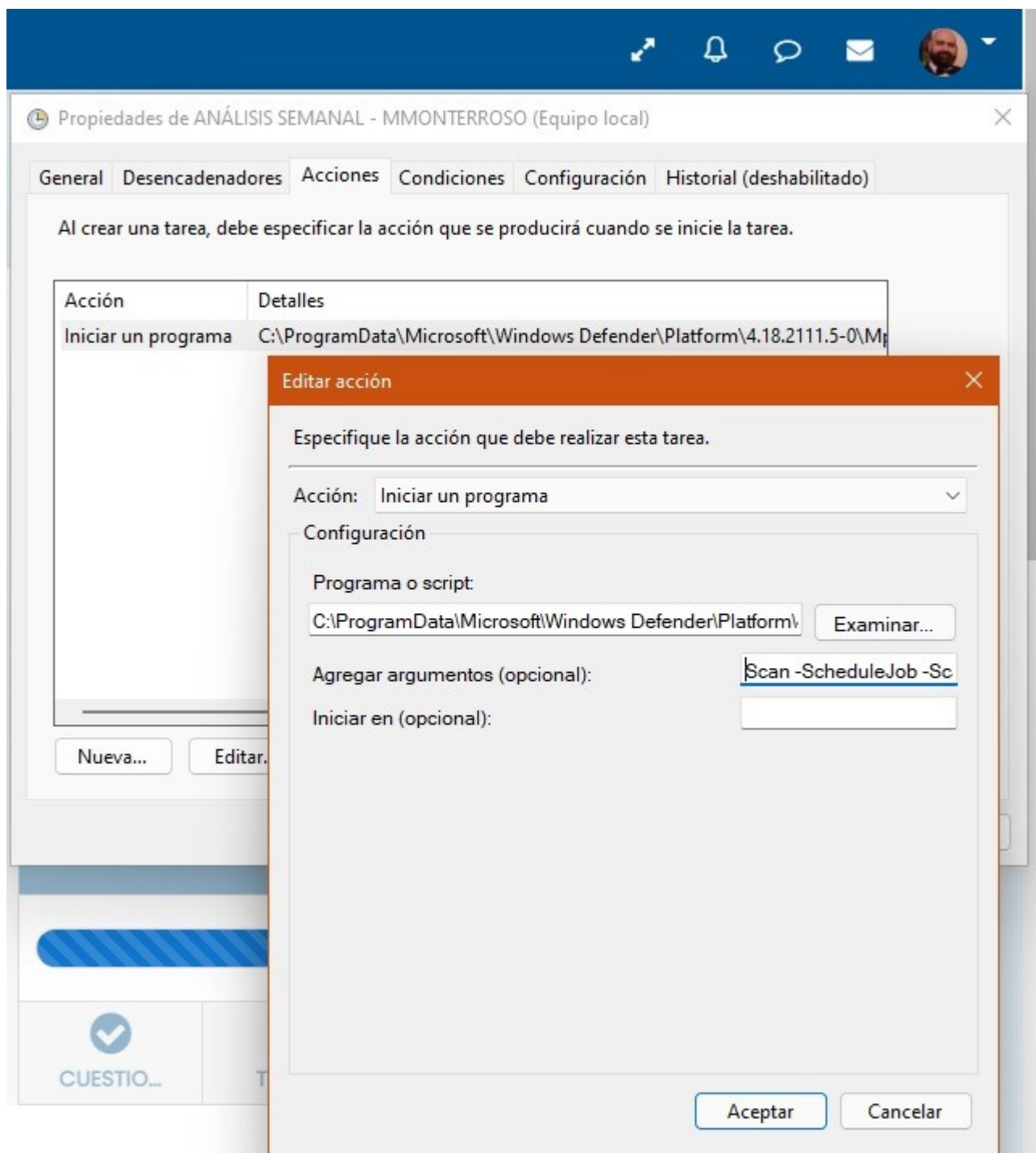
☐ Sincronizar zonas horaria

☒ Habilitado

Aceptar

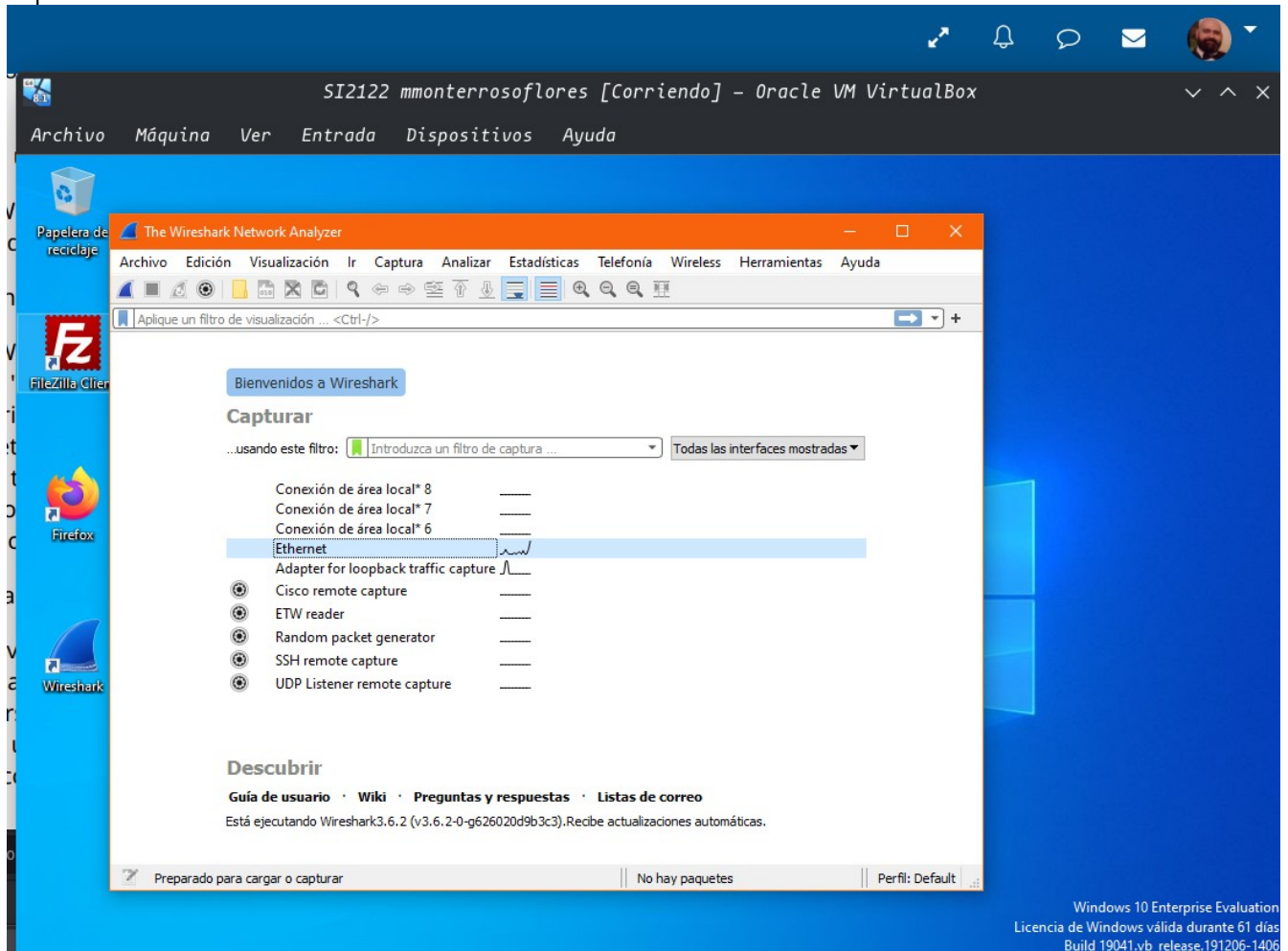
Cancelar

18

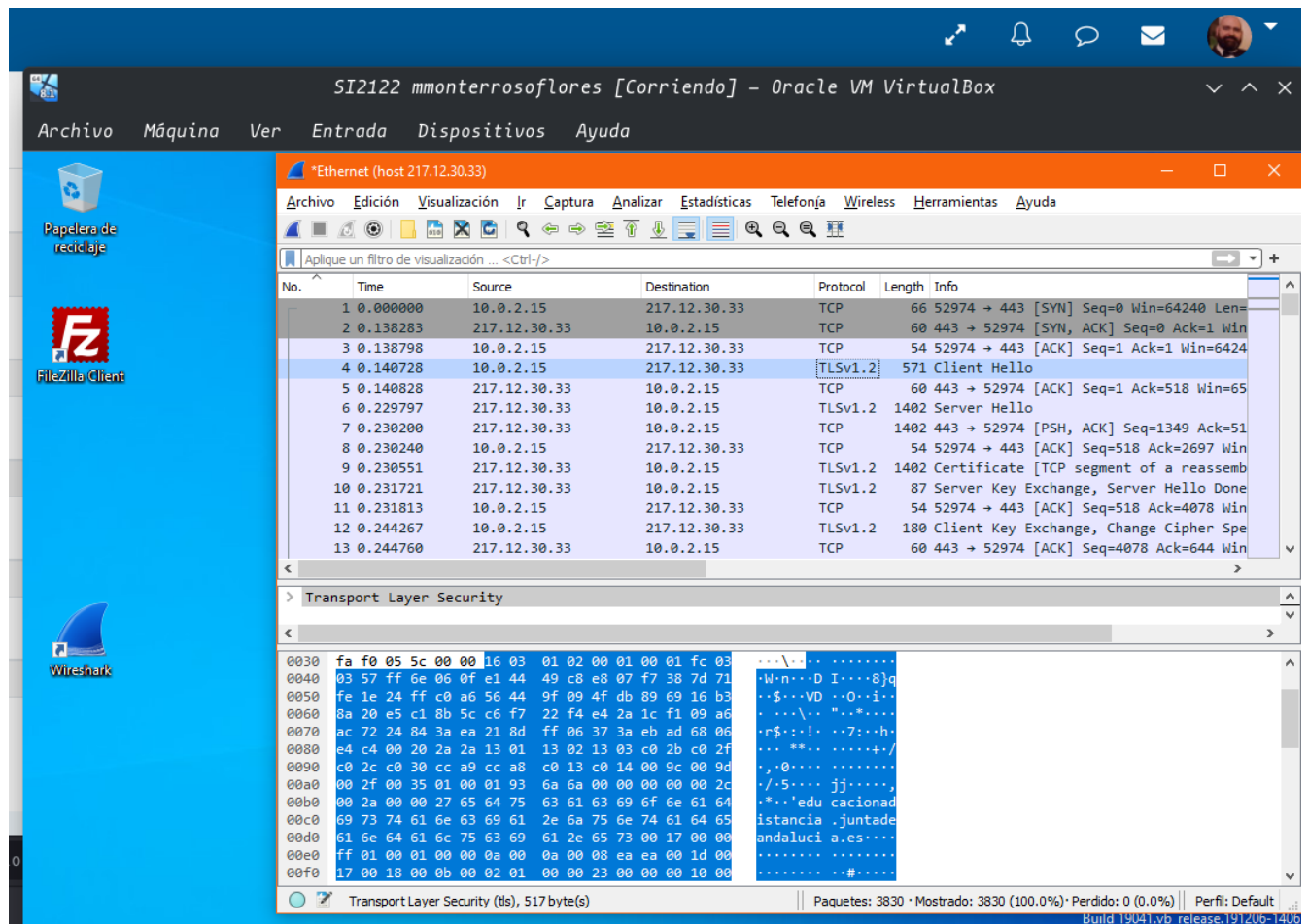


Actividad 6 .- Monitorización usando Wireshark.

Captura con Wireshark recién iniciado tras la instalación.



Captura con el inicio de la conversión entre el equipo y la página de la JA.



Captura con el filtro ip.addr == 217.12.30.33

SI2122 mmonterrosoflores [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Ethernet (host 217.12.30.33)

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 217.12.30.33

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	217.12.30.33	TCP	66	52974 → 443 [SYN] Seq=0 Win=64240 Len=
2	0.138283	217.12.30.33	10.0.2.15	TCP	60	443 → 52974 [SYN, ACK] Seq=0 Ack=1 Win=
3	0.138798	10.0.2.15	217.12.30.33	TCP	54	52974 → 443 [ACK] Seq=1 Ack=1 Win=6424
4	0.140728	10.0.2.15	217.12.30.33	TLSv1.2	571	Client Hello
5	0.140828	217.12.30.33	10.0.2.15	TCP	60	443 → 52974 [ACK] Seq=1 Ack=518 Win=65
6	0.229797	217.12.30.33	10.0.2.15	TLSv1.2	1402	Server Hello
7	0.230200	217.12.30.33	10.0.2.15	TCP	1402	443 → 52974 [PSH, ACK] Seq=1349 Ack=51
8	0.230240	10.0.2.15	217.12.30.33	TCP	54	52974 → 443 [ACK] Seq=518 Ack=2697 Win=
9	0.230551	217.12.30.33	10.0.2.15	TLSv1.2	1402	Certificate [TCP segment of a reassemb
10	0.231721	217.12.30.33	10.0.2.15	TLSv1.2	87	Server Key Exchange, Server Hello Done
11	0.231813	10.0.2.15	217.12.30.33	TCP	54	52974 → 443 [ACK] Seq=518 Ack=4078 Win=
12	0.244267	10.0.2.15	217.12.30.33	TLSv1.2	180	Client Key Exchange, Change Cipher Spe
13	0.244760	217.12.30.33	10.0.2.15	TCP	60	443 → 52974 [ACK] Seq=4078 Ack=644 Win=

Transport Layer Security

0030 fa f0 05 5c 00 00 16 03 01 02 00 01 00 01 fc 03
0040 03 57 ff 6e 06 0f e1 44 49 c8 e8 07 f7 38 7d 71 ...W-n...D I...8}q
0050 fe 1e 24 ff c0 a6 56 44 9f 09 4f db 89 69 16 b3 ...\$.~VD .0..i
0060 8a 20 e5 c1 8b 5c c6 f7 22 f4 e4 2a 1c f1 09 a6 ".*....
0070 ac 72 24 84 3a ea 21 8d ff 06 37 3a eb ad 68 06 ...r\$.:!.~:7:..h
0080 e4 c4 00 20 2a 2a 13 01 13 02 13 03 c0 2b c0 2f +./
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ... ,.0....
00a0 00 2f 00 35 01 00 01 03 6a 6a 00 00 00 00 00 2c .../.5.... jj.....
00b0 00 2a 00 00 27 65 64 75 63 61 63 69 6f 6e 61 64'edu cacionad
00c0 69 73 74 61 6e 63 69 61 2e 6a 75 6e 74 61 64 65 ...istancia .juntade
00d0 61 6e 64 61 6c 75 63 69 61 2e 65 73 00 17 00 00 ...andaluci a.es....
00e0 ff 01 00 01 00 00 0a 00 0a 00 08 ea 00 1d 00
00f0 17 00 18 00 0b 00 02 01 00 00 23 00 00 00 10 00 #....

Transport Layer Security (tls), 517 byte(s)

Paquetes: 3830 · Mostrado: 3830 (100.0%) · Perdido: 0 (0.0%) · Perfil: Default

¿Crees que la conversación entre la MV y el servidor web del aula virtual está encriptada? ¿Por qué?

Si, porque la conexión entre el equipo y la página se realiza a través del protocolo TLSv1.2 que es el que se utiliza en las páginas protegidas con el protocolo HTTPS, este protocolo es una actualización del antiguo protocolo SSL.

Actividad 7.- Configuración de la red Wi-Fi en un router inalámbrico.

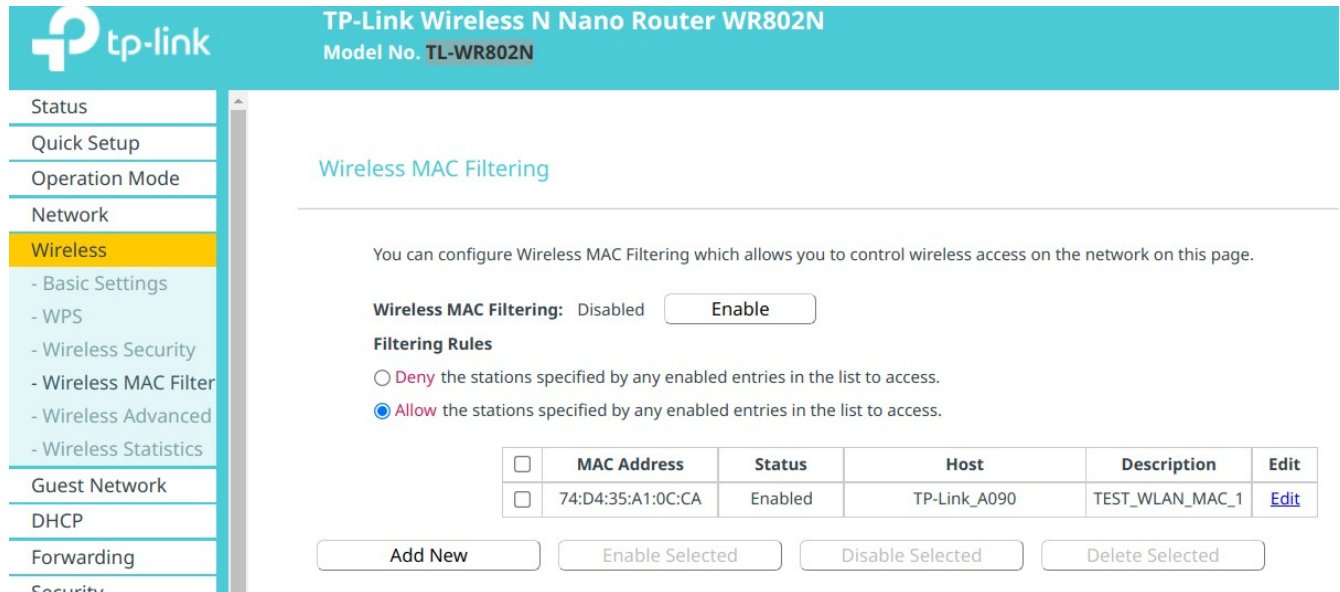
Captura con la configuración de la contraseña de acceso al panel de control del router.

The screenshot shows the TP-Link Wireless N Nano Router WR802N web interface. The left sidebar contains a menu with the following items: Wireless, Guest Network, DHCP, Forwarding, Security, Parental Controls, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, IPv6, System Tools (highlighted in yellow), and - Time Settings. The main content area is titled "Password" and contains a warning message: "Username and password can contain between 1 - 15 characters and may not include spaces." Below this, there are five input fields: "Old User Name:", "Old Password:", "New User Name:", "New Password:", and "Confirm password:". At the bottom right, there are two buttons: "Save" and "Clear All".

Captura de la clave para la configuración del wifi, además realizado con la protección WPA2.

The screenshot shows the TP-Link Wireless N Nano Router WR802N web interface. The left sidebar contains a menu with the following items: Status, Quick Setup, Operation Mode, Network, Wireless (highlighted in yellow), - Basic Settings, - WPS, - Wireless Security, - Wireless MAC Filter, and - Wireless Advanced. The main content area is titled "Wireless Security" and contains a note: "Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled. For network security, it is strongly recommended to enable wireless security and select WPA2-PSK AES encryption." Below this, there are two radio buttons: "Disable Wireless Security" and "WPA/WPA2 - Personal(Recommended)" (selected). To the right of the selected radio button, there are three dropdown menus: "Version:" with "WPA2-PSK" selected, "Encryption:" with "AES" selected, and "Wireless Password:" with "12811441" entered. Below these, there is a "Group Key Update Period:" field with "0" entered. At the bottom, there is a radio button for "WPA/WPA2 - Enterprise".

Capturas con el filtrado de dirección por MAC, como lo estoy haciendo por un emulador, y no se guardan los cambios, en la primera captura pondré la pagina principal de esta opción en el Router y en la segunda captura pondré como se pondría la dirección que nos piden en la tarea.



TP-Link Wireless N Nano Router WR802N
Model No. TL-WR802N

Status
Quick Setup
Operation Mode
Network
Wireless
- Basic Settings
- WPS
- Wireless Security
- Wireless MAC Filter
- Wireless Advanced
- Wireless Statistics
Guest Network
DHCP
Forwarding
Security

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

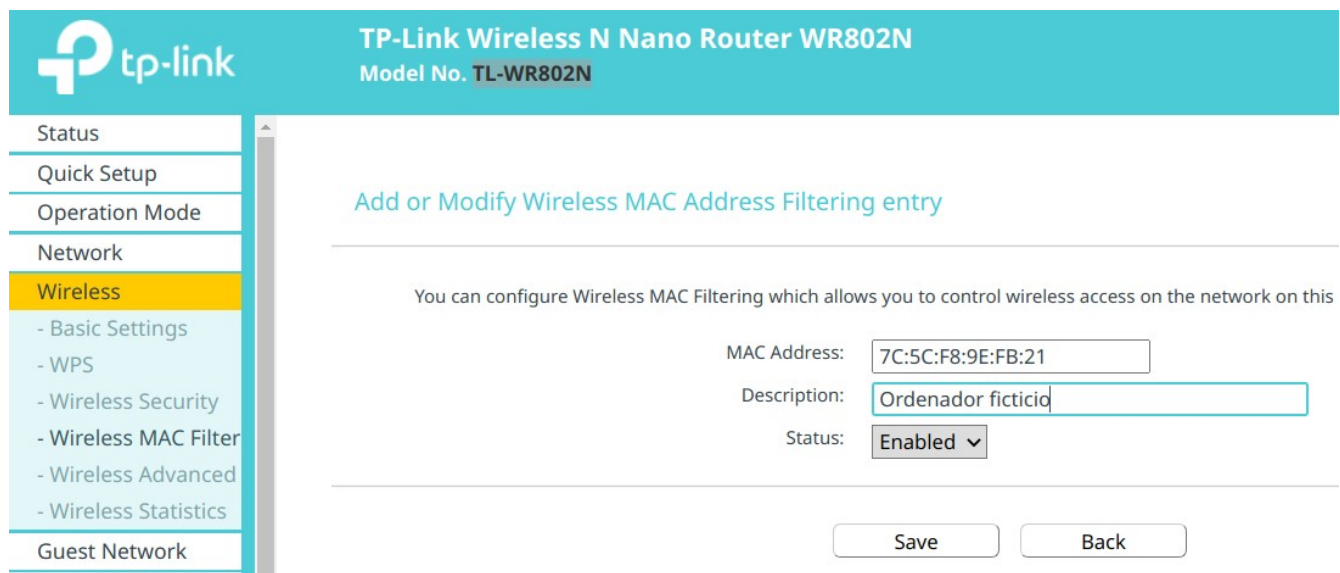
Wireless MAC Filtering: Disabled

Filtering Rules

☐ Deny the stations specified by any enabled entries in the list to access.

☒ Allow the stations specified by any enabled entries in the list to access.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	74:D4:35:A1:0C:CA	Enabled	TP-Link_A090	TEST_WLAN_MAC_1	Edit



TP-Link Wireless N Nano Router WR802N
Model No. TL-WR802N

Status
Quick Setup
Operation Mode
Network
Wireless
- Basic Settings
- WPS
- Wireless Security
- Wireless MAC Filter
- Wireless Advanced
- Wireless Statistics
Guest Network

Add or Modify Wireless MAC Address Filtering entry

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this

MAC Address:

Description:

Status:

Con la opción Allow lo que estamos haciendo es decir al router que solo se podrán conectar los equipos que posean las MACs que estén en esa lista, lo bueno de este método de seguridad es que se supone que cada equipo de conexión a internet posee una dirección MAC única, pero esto en realidad se puede saltar porque se puede emular estas direcciones y

saltarse este método de seguridad si se puede obtener la MAC de los equipos permitidos.