

# **Tarea 6: Administración de Redes (Windows III)**

Francisco Javier Sueza Rodríguez

13 de marzo de 2023

**Centro:** IES Aguadulce  
**Ciclo Formativo:** Desarrollo Aplicaciones Web (Distancia)  
**Asignatura:** Sistemas Informáticos  
**Tema:** Tema 6 - Administración de Redes (Windows III)

# Índice

<b>1 Caso Práctico</b>	<b>4</b>
<b>2 Actividades</b>	<b>4</b>
2.1 Actividad 1: Configuración de Red Ethernet Básica y Comandos . . . . .	4
2.1.1 Enunciado . . . . .	4
2.1.2 Solución . . . . .	5
2.2 Actividad 2: Comunicar MV y Máquina Anfitriona en Red y Compartir una Carpeta . . . . .	7
2.2.1 Enunciado . . . . .	7
2.2.2 Solución . . . . .	8
2.3 Actividad 3: Establece un Servidor FTP Básico en Windows 10 . . . . .	11
2.3.1 Enunciado . . . . .	11
2.3.2 Solución . . . . .	11
2.4 Actividad 4: Servidor Web en Windows 10 . . . . .	14
2.4.1 Enunciado . . . . .	14
2.4.2 Solución . . . . .	15
2.5 Actividad 5: Utilización de Antivirus . . . . .	17
2.5.1 Enunciado . . . . .	17
2.5.2 Solución . . . . .	17
2.6 Actividad 6: Configuración de la Red Wi-Fi en un Router Inalámbrico y Conexión . . . . .	18
2.6.1 Enunciado . . . . .	18
2.6.2 Solución . . . . .	19

## Índice de figuras

2.1	Datos a configurar en la interfaz eth de la MV . . . . .	4
2.2	Cambio de valores de la interfaz Ethernet0 . . . . .	5
2.3	Información de la interfaz Ethernet0 con los datos se han cambiado . . . . .	5
2.4	Salida del comando ipconfig . . . . .	6
2.5	Salida del comando hostname . . . . .	6
2.6	Salida del comando nslookup . . . . .	6
2.7	Salida del comando ping . . . . .	7
2.8	Salida del comando tracert . . . . .	7
2.9	Estableciendo el adaptador de red de VMWare en modo bridge . . . . .	9
2.10	Configuración de la interfaz de red del invitado . . . . .	9
2.11	Configuración de la interfaz de red del anfitrión . . . . .	9
2.12	Ping desde el sistema invitado al anfitrión . . . . .	10
2.13	Ping desde el sistema anfitrión al invitado . . . . .	10
2.14	Carpeta compartida visible desde el anfitrión . . . . .	10
2.15	Archivo creado desde el sistema anfitrión abierto en el invitado . . . . .	11
2.16	Creación de carpeta raíz del servidor FTP . . . . .	12
2.17	Activación de características de Windows 10 . . . . .	12
2.18	Creación FTP: nombre y ruta . . . . .	13
2.19	Creación FTP: ip y certificado SSL . . . . .	13
2.20	Creación FTP: método y usuarios . . . . .	13
2.21	Conexión al FTP desde la máquina anfitrión en Filezilla . . . . .	14
2.22	Descarga y subida de archivos al servidor FTP desde Filezilla . . . . .	14
2.23	Código de la página web . . . . .	14
2.24	XAMPP instalado y con Apache ejecutándose . . . . .	15
2.25	Creación del fichero HTML . . . . .	16
2.26	Archivos dentro de la carpeta miweb . . . . .	16
2.27	Acceso a la página web desde el sistema anfitrión . . . . .	16
2.28	Menú contextual de la unidad USB conectada . . . . .	17
2.29	Resultado del análisis del dispositivo USB . . . . .	18
2.30	Tarea para el análisis semanal con Windows Defender programada . . . . .	18
2.31	Acceso al router con su interfaz web . . . . .	19
2.32	Cambio de contraseña de acceso al router . . . . .	20
2.33	Interfaz principal del router . . . . .	20
2.34	Cambio de contraseña de red . . . . .	20
2.35	Cambio del cifrado de la contraseña Wi-Fi . . . . .	21
2.36	Dirección MAC de un dispositivo conectado a la red . . . . .	21
2.37	Configuración del filtrado MAC . . . . .	22

## 1. Caso Práctico

María y Juan ya han terminado de administrar el sistema operativo instalado en los equipos de la empresa pero les falta configurarlos para que estén conectados a la red. Como siempre, Ada será la que les dé el visto bueno.

## 2. Actividades

### 2.1. Actividad 1: Configuración de Red Ethernet Básica y Comandos

#### 2.1.1. Enunciado

1. Configura la conexión de la interfaz de red Ethernet de la MV manualmente con los siguientes datos:

Dirección IP:	172.16.30.60
Máscara de red:	255.255.255.0
Puerta de enlace predeterminada:	172.16.30.1
DNS:	8.8.8.8 8.8.4.4

Figura 2.1: Datos a configurar en la interfaz eth de la MV

Cuando realices las capturas necesarias, y antes de proceder a ejecutar los comandos que se indican a continuación, deshaz los cambios que hayas hecho en la configuración de la interfaz de red Ethernet para asegurarte de que tienes conexión a Internet.

2. Ahora, desde la línea de comandos ejecuta los siguientes comandos, haz una captura de su salida y comenta brevemente la salida obtenida:

- a) ipconfig /all
- b) hostname
- c) nslookup <nombre\_dominio>
- d) ping <dirección\_ip>
- e) tracert <dirección\_ip>

Asegúrate de que el nombre de dominio y las direcciones IP corresponden a sitios web públicos de Internet, y no a tu dispositivo local (es decir, no uses "localhost", 127.0.0.1 o similar) o a otros dispositivos de tu red local (no vale la dirección de tu router tipo 192.168.1.1 o similares), y de que la salida de los comandos es correcta.

#### Capturas:

- Ventana donde se modifica la configuración de red (se debe indicar textualmente cómo se accede a dicha ventana).
- Muestra de que la configuración de red se ha modificado.
- Ejecución de cada uno de los comandos y salida producida.

### 2.1.2. Solución

En este primer ejercicio vamos a modificar la configuración del adaptador Ethernet de nuestra máquina virtual con Windows 10, para a continuación ejecutar diferentes comandos relacionados con redes y mostrar sus salidas.

1. Primero, vamos a cambiar la configuración del adaptador ethernet.

Para acceder a la configuración, pulsamos en **Menú Inicio —>Redes e Internet**. Se nos abrirá una ventana con diferentes configuraciones que podemos realizar, pero a nosotros no interesa la opción **Cambiar opciones de adaptador**, así que pulsamos aquí.

Esto nos abrirá la venta de **Conexiones de red**, donde se nos mostrarán todos los adaptadores de red que tenemos configurados. En nuestro caso, solo tenemos el adaptador **Ethernet0**, así que hacemos doble-click sobre este adaptador, lo que nos abrirá una ventana con información sobre su estado. En esta ventana, en la parte inferior, pulsamos en el botón **Propiedades**, lo que nos abrirá otra ventana con las propiedades del adaptador.

En esta nueva ventana, buscamos en la lista de elementos y seleccionamos **Protocolo de internet versión 4** y pulsamos en **Propiedades**. Se nos abrirá una ventana, la cual podemos ver en la siguiente captura, donde podremos cambiar la configuración IPv4 del adaptador.

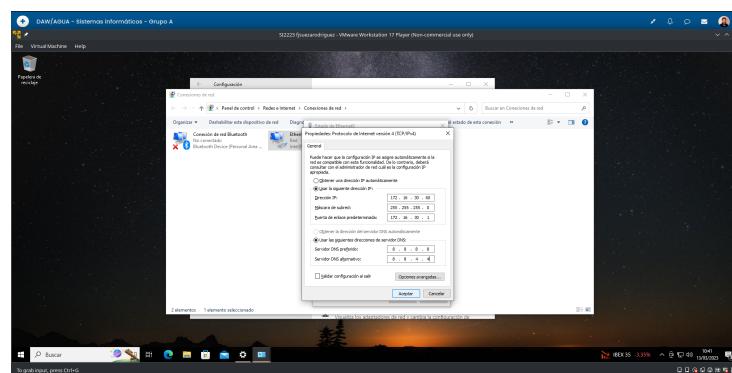


Figura 2.2: Cambio de valores de la interfaz Ethernet0

Para comprobar que se ha realizado el cambio correctamente, volvemos a la venta de **Estado de Ethernet0** y pulsamos en **Detalles**, lo que nos mostrará toda la información de red, como se ve a continuación.

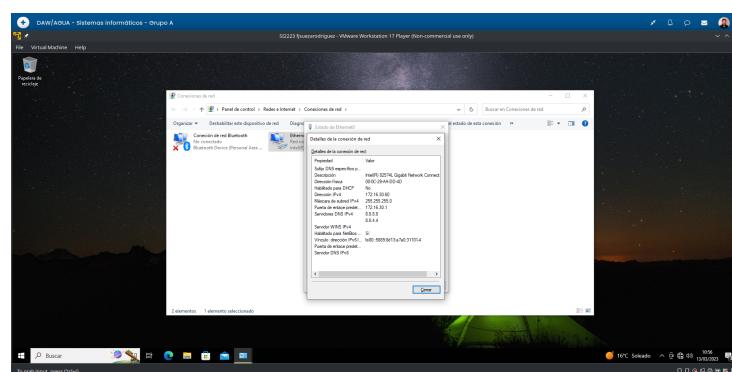


Figura 2.3: Información de la interfaz Ethernet0 con los datos se han cambiado

2. A continuación, vamos a ejecutar una serie de **comandos de red** y a mostrar y comentar su salida.

- **ipconfig /all**: este comando nos ha mostrado la configuración de red. En concreto, la configuración **IP de Windows** y la de todas las interfaces de red que tenemos en el equipo, en nuestro caso, los de la interfaces **Ethernet0** y de la interfaz **Bluetooth**, esta última sin conexión a internet.

Figura 2.4: Salida del comando ipconfig

- **hostname**: este comando simplemente nos muestra el nombre host de la máquina. En nuestro caso no hemos establecido ninguno por lo que tenemos el que establece por defecto Windows 10.

A screenshot of a Windows 10 desktop environment. A command prompt window is open in the center, displaying the command 'dir' and its output, which includes files like 'Screenshot\_1.png', 'Screenshot\_2.png', and 'Screenshot\_3.png'. The desktop background is dark. The taskbar at the bottom features the Start button, Task View, File Explorer, and other standard icons. The system tray shows battery status, signal strength, and volume controls.

Figura 2.5: Salida del comando hostname

- **nslookup**: este comando nos muestra información sobre DNS de un dominio o IP determinado. Nosotros hemos ejecutado el comando sobre **www.google.com**, mostrándonos en la salida información sobre la IP de este dominio.

Figura 2.6: Salida del comando nslookup

- **ping:** este comando se usa para comprobar si hay conexión entre nuestro ordenador y una dirección de IP remota. Nosotros hemos realizado ping sobre **www.google.com** y como vemos se hay una conexión perfecta con esta dirección, con 0 % de paquetes perdidos y una respuesta mínima de 25ms y máxima de 136ms.

```

C:\Users\joseantonio - Sistemas Informáticos - Grupo A> ping www.google.com

Pinging www.google.com [142.250.200.48] with 32 bytes of data:
Replay 1 de 4: 142.250.200.48 Tiquete-id tiempo=40ms ttl=128
Replay 2 de 4: 142.250.200.48 Tiquete-id tiempo=40ms ttl=128
Replay 3 de 4: 142.250.200.48 Tiquete-id tiempo=40ms ttl=128
Replay 4 de 4: 142.250.200.48 Tiquete-id tiempo=40ms ttl=128

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
Porcentaje de pérdida = 0.00%
Tiempo total de ida y vuelta en milisegundos
Ronda = 25ms, media = 136ms, rango = 136ms
C:\Users\joseantonio>

```

Figura 2.7: Salida del comando ping

- **tracert:** esta utilidad nos muestra todos los saltos que hay entre nuestro ordenador y una dirección ip determinada. En nuestro caso, hemos vuelto a ejecutarla sobre **www.google.com**. En nuestro caso como vemos hay **9 saltos** entre nuestra dirección y la de google, incluyendo nuestro router (192.168.1.1).

```

C:\Users\joseantonio - Sistemas Informáticos - Grupo A> tracert www.google.com

Tracert a la dirección www.google.com [142.250.200.48]
sobre un máximo de 30 saltos

  1  192.168.1.1  2 ms  14 ms  24 ms  Local máquina [192.168.1.1]
  2  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  3  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  4  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  5  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  6  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  7  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  8  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  9  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  10  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  11  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  12  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  13  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  14  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  15  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  16  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  17  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  18  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  19  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  20  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  21  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  22  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  23  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  24  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  25  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  26  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  27  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  28  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  29  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]
  30  192.168.1.1  14 ms  14 ms  14 ms  Router [192.168.1.1]

Tracert finalizado.
C:\Users\joseantonio>

```

Figura 2.8: Salida del comando tracert

## 2.2. Actividad 2: Comunicar MV y Máquina Anfitriona en Red y Compartir una Carpeta

### 2.2.1. Enunciado

Para esta actividad debes configurar la MV para que máquina anfitriona y máquina virtual puedan comunicarse a través de un entorno de red local. Puedes hacerlo de diversas maneras, las cuales serán más o menos adecuadas dependiendo de tu entorno de red. Recomendamos una de estas dos opciones:

- **Opción 1:** Estableciendo el adaptador de red de la MV en modo “puente”. En este caso el software de virtualización simulará que la MV esté conectada directamente al mismo aparato que tu máquina anfitriona. Por ejemplo, si tienes un router casero, será como si la MV estuviese conectada directamente al router con una conexión cableada y pertenecerá a su subred LAN igual que el equipo anfitrión.

- **Opción 2:** Habilitar un segundo adaptador de red en la MV y configurarlo en modo “sólo-anfitrión”. Esto simula una segunda tarjeta de red en la MV, la cual estaría conectada directamente a otra tarjeta de red en la máquina anfitriona. Para esta conexión la máquina anfitriona utiliza un adaptador de red virtual que se crea durante la instalación del software de virtualización. En el caso de VirtualBox este adaptador se llama “VirtualBox Host-Only Network” y por defecto tiene la IP 192.168.56.1/24, por lo que en la máquina virtual tendrás que asegurarte de que el segundo adaptador de red que has añadido tiene una IP que pertenezca a la misma subred. El motivo de tener dos adaptadores de red en este caso es que el primero, configurado en modo NAT (el modo por defecto), permite a la MV tener conexión externa con Internet pero no con el anfitrión, mientras que el segundo, en modo sólo-anfitrión, permite la comunicación entre anfitrión y MV pero no con Internet.

Cuando hayas configurado la MV comprueba que existe comunicación entre ambas máquinas realizando dos “ping”: uno de la MV a la máquina anfitriona y otro al contrario. Es posible que para que funcione el “ping” debas activar en las máquinas la opción de “activar el uso compartido de archivos e impresoras”, o bien una regla en el firewall de Windows que permita el tráfico de “solicitud de eco ICMP”.

Cuando compruebes que existe comunicación a través de la red entre ambas máquinas, crea una carpeta en la máquina virtual y compártela. Deberás acceder a esta carpeta desde la máquina anfitriona a través de la red y crear un documento en su interior con algún texto de ejemplo. Esta acción de compartir la carpeta no se puede realizar utilizando las herramientas que proveen los programas de virtualización para ello, debe hacerse tal como se haría si se tuviesen dos equipos conectados dentro de una red local.

#### **Capturas:**

- Configuración del adaptador de red de la máquina virtual en el software de virtualización.
- Configuración IP del adaptador de la máquina real que se vaya a usar para la comunicación.
- Configuración IP del adaptador de la máquina virtual que se vaya a usar para la comunicación.
- Ping máquina virtual >máquina anfitriona.
- Ping máquina anfitriona >máquina virtual.
- Compartición de la carpeta creada en la MV.
- Acceso desde la máquina anfitriona a la carpeta compartida en la MV.
- Creación de un documento de texto dentro de la carpeta compartida desde la máquina anfitriona.

#### **2.2.2. Solución**

En este ejercicio vamos a conectar mediante red la máquina anfitriona y la máquina visitante. Nosotros, hemos elegido la **opción 1** para conectar ambas máquinas, ya nos ha parecido más simple y ciertamente, ha sido bastante rápida y efectiva. A continuación detallamos los pasos que hemos llevado a cabo.

1. En primer lugar hemos cambiado la configuración del adaptador ethernet de VMWare, estableciendo el adaptador de red en modo **bridge** y marcando la casilla **Replicate physical network connection state**, como se puede ver en la siguiente captura.

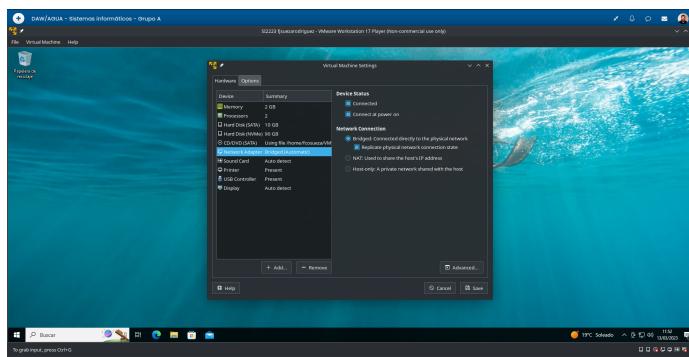


Figura 2.9: Estableciendo el adaptador de red de VMWare en modo bridge

- En este paso, **no hemos tenido** que hacer ninguna **configuración de los adaptadores** del red ni del sistema host ni del guest, ya que al establecer el adaptador de VMWare en modo bridge **el sistema invitado se conecta** a la red como **una máquina más de la red**. Aun así, aquí se muestran 2 capturas con la configuración que tiene cada una de las máquinas.

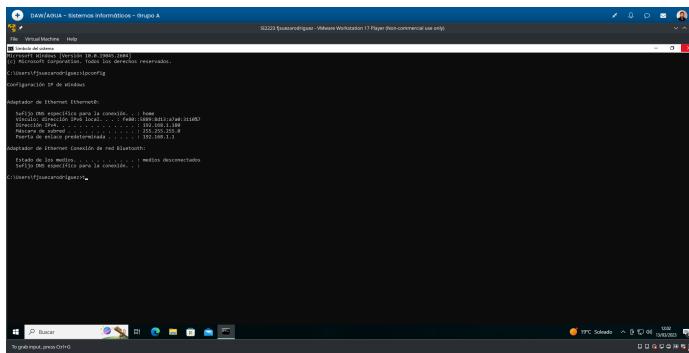


Figura 2.10: Configuración de la interfaz de red del invitado

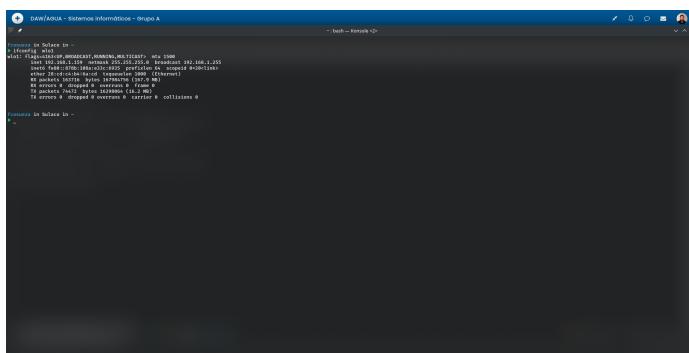


Figura 2.11: Configuración de la interfaz de red del anfitrión

- Para comprobar que se ha establecido la conexión correctamente, hemos usado el comando **ping** entre las dos máquinas. Cabe destacar que para que funcione el comando, hemos tenido que activar la opción **Activar uso compartido de archivos e impresoras** en el sistema invitado. Una vez hecho esto, las máquinas se han reconocido correctamente, como vemos en las siguientes capturas.

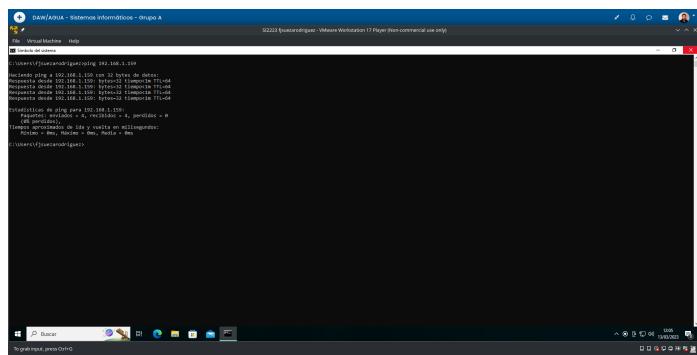


Figura 2.12: Ping desde el sistema invitado al anfitrión

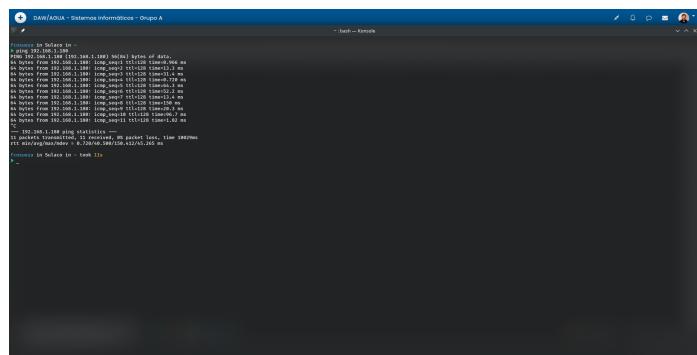


Figura 2.13: Ping desde el sistema anfitrión al invitado

4. Por último, hemos creado una carpeta compartida, que en un alarde de originalidad hemos llamado **Compartida**, en Windows 10 (sistema invitado). Pulsando en el botón derecho sobre la carpeta hemos accedido a **Propiedades**, y en la ventana que se nos abre a la pestaña **Compartir**. Hemos configurado la carpeta para que se comparta mediante la red, añadiendo permisos de escritura y lectura a todos los usuarios, entre otras cosas.

En sistema anfitrión, una **Kubuntu 22.04**, hemos tenido que instalar **samba**, para poder acceder a estas carpetas, aunque aquí no vamos a entrar en detalles. Pero como podemos ver en la siguiente captura, ya podemos visualizar y acceder a la carpeta compartida desde Windows 10.

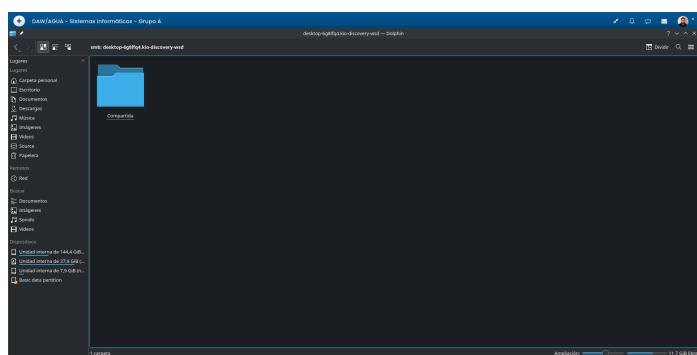


Figura 2.14: Carpeta compartida visible desde el anfitrión

A continuación hemos creado un archivo de texto desde el anfitrión y lo hemos abierto desde el

invitado, para comprobar que se había creado correctamente.

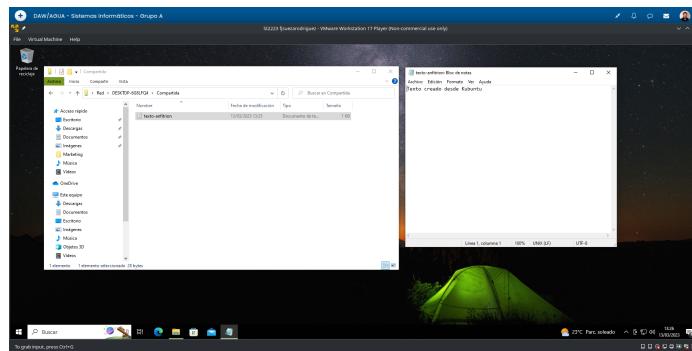


Figura 2.15: Archivo creado desde el sistema anfitrión abierto en el invitado

## 2.3. Actividad 3: Establece un Servidor FTP Básico en Windows 10

### 2.3.1. Enunciado

Instala y configura en la MV un servidor FTP con el servicio de FTP que suministra Windows, con autenticación básica y requiriendo TLS/SSL (para ello se puede utilizar un certificado autofirmado). El nombre del sitio FTP será “SI\_< inicial de tu nombre y primer apellido >”. Por ejemplo, para un alumno llamado Pablo Rodríguez Campos, el nombre de su sitio FTP será “SI\_prodriguez”. Si tienes problemas para conseguir que funcione la conexión mediante TLS/SSL utiliza el foro de la unidad para consultarla.

El acceso a dicho servidor lo realizarás desde la máquina anfitriona utilizando un cliente FTP como Filezilla. Una vez conectado al servidor realiza dos transferencias de ficheros: una descarga (MV >anfitrión) y una subida (anfitrión >MV).

Recuerda, el acceso será desde la máquina anfitriona (cliente FTP Filezilla) a la MV (servidor FTP incluido en Windows 10).

#### Capturas:

- Creación y asignación de permisos a la carpeta usada para el directorio raíz del FTP.
- Activación de las características de Windows necesarias para el servicio FTP y su configuración.
- Creación del sitio FTP incluyendo: Nombre del sitio FTP y ruta de acceso física; Dirección IP de acceso, requerimiento de SSL y certificado; Tipo de autenticación, autorización de usuarios y permisos.
- Conexión del cliente FTP con el servidor. Se debe mostrar que esta conexión es segura mediante TLS/SSL.
- Descarga y subida de un fichero. Se debe ver en la consola de Filezilla que las transferencias han sido correctas.

### 2.3.2. Solución

En este ejercicio vamos a crear un servidor FTP en la máquina invitada con Windows 10 y posteriormente acceder a este desde la máquina anfitriona usando el cliente Filezilla. Para comprobar que el servidor funciona correctamente, haremos un par de transferencias de archivos.

1. En primer lugar hemos creado la carpeta que será la raíz del servidor FTP. La carpeta creada se llama **SI\_fjsueza** y la hemos creado en el **Escritorio** de Windows. No ha sido necesario añadir permisos extra a dicha carpeta ya que vamos a usar el usuario que creamos al principio, **fjsueza-rodriguez**, para acceder al servidor FTP, el cual ya tiene todos los permisos sobre dicha carpeta.

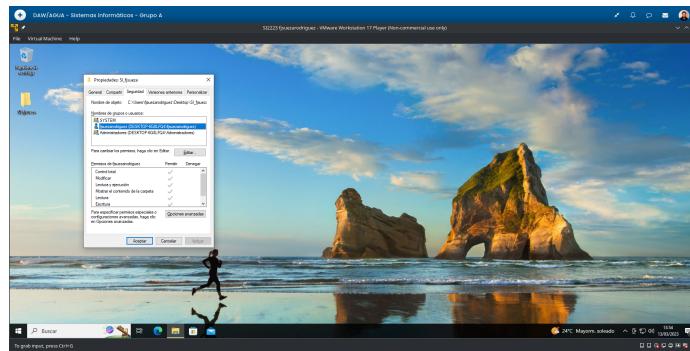


Figura 2.16: Creación de carpeta raíz del servidor FTP

2. El siguiente paso consiste en activar el **servicio de FTP** en Windows 10.

Para ello, hemos abierto el **Panel de Control** y pulsado en la opción **Programas**. En la ventana que se nos abre, hemos pulsado en la opción **Activar o desactivar características de Windows**, debajo del apartado **Programas y Características**. Se nos abrirá una nueva ventana con un conjunto de carpetas que podemos que ir desplegando y activando. En nuestro caso, nos interesa la carpeta **Internet Information Services**. Desplegamos esta carpeta y activamos **Servidor FTP**, que por defecto activará **Extensibilidad de FTP** y **Servicio FTP**. Dejaremos estas dos opciones marcadas.

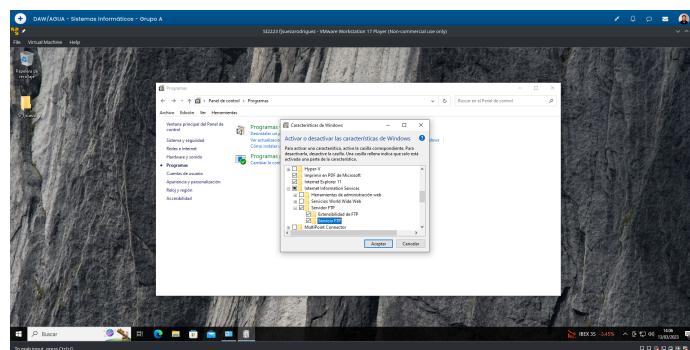


Figura 2.17: Activación de características de Windows 10

3. A continuación, vamos a crear el servidor FTP, configurando su nombre, método de autenticación, etc. Para ellos debemos acceder al **Administrador de Internet Information Services (ISS)**, al cual podemos acceder desde **Panel de Control —> Herramientas Administrativas**.

Una vez aquí, desplegamos el menú de la izquierda, donde figura el hostname de nuestro ordenador, y damos con el botón derecho sobre el elemento **Sitios**, pulsando sobre la opción **Agregar sitio FTP...** que se nos mostrará. Se nos abrirá una ventana donde nos guiarán en la creación del servidor FTP, permitiéndonos introducir todos los datos que se nos pide en el enunciado.

Cabe destacar que antes del último paso, hemos **creado un certificado SSL autofirmado** usando la opción **Certificados de servidor** del administrador de Internet Information Services.

En las siguientes capturas, podemos ver todos los datos introducidos en la creación del servidor FTP.

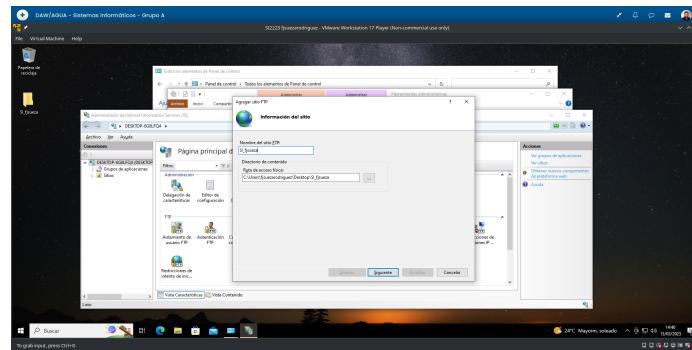


Figura 2.18: Creación FTP: nombre y ruta

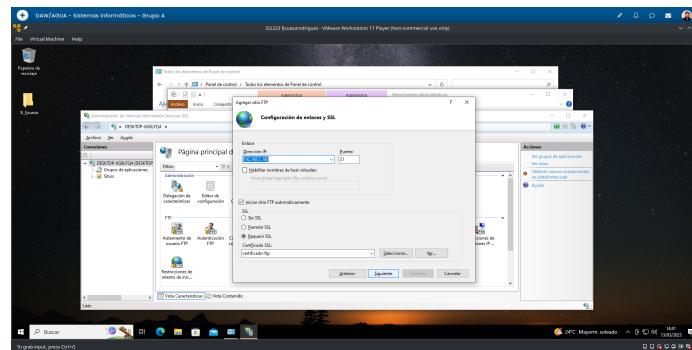


Figura 2.19: Creación FTP: ip y certificado SSL

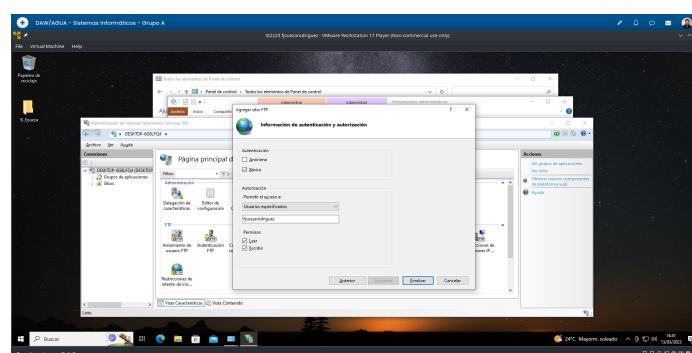


Figura 2.20: Creación FTP: método y usuarios

4. Para comprobar que el servidor se ha creado correctamente, vamos a acceder a él desde el sistema anfitrión, usando la aplicación **Filezilla**. Después de introducir los datos en Filezilla, hemos **realizado la conexión correctamente**, como podemos ver en la siguiente captura.

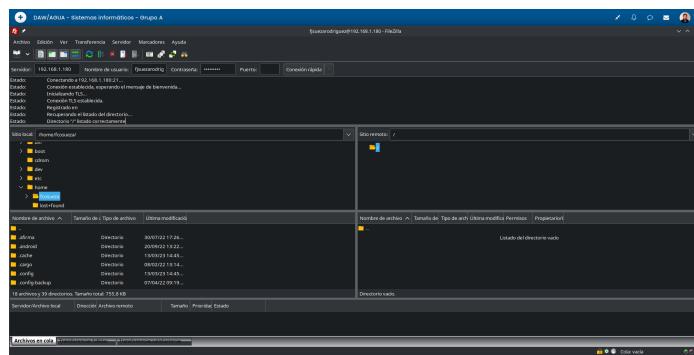


Figura 2.21: Conexión al FTP desde la máquina anfitrión en Filezilla

5. Por último, hemos creado una imagen de mapa de bits en el directorio del FTP, para descargarla con el cliente, y hemos también subido un libro al FTP. Las dos operaciones se han realizado con éxito, como podemos ver en la siguiente captura.

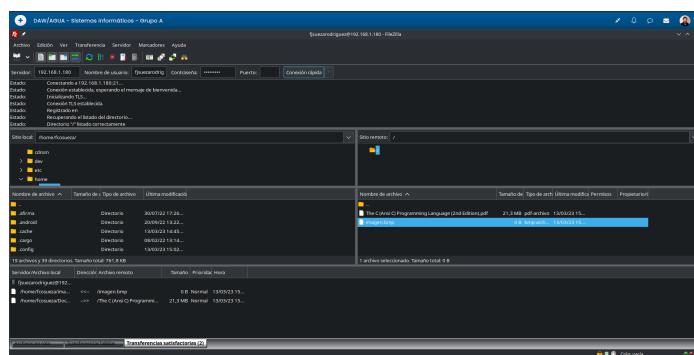


Figura 2.22: Descarga y subida de archivos al servidor FTP desde Filezilla

## 2.4. Actividad 4: Servidor Web en Windows 10

### 2.4.1. Enunciado

Instala y configura el entorno de servidor web “XAMPP” en la MV. Una vez activados los servicios, en la carpeta pública del servidor Apache (“htdocs”) crea una carpeta llamada “miweb”, en la cual guardarás una fotografía tuya y un archivo “.html” con el siguiente código:

```

1 <html lang="es">
2   <head>
3     <title>CFGSI DAW/DAM - Módulo SI - Unidad 6</title>
4     <meta charset="UTF-8">
5   </head>
6   <body>
7     <h1>Tarea 6 de Sistemas Informáticos</h1>
8     <h2>Esta es mi primera página web en código HTML.</h2>
9     
10    Realizado por - Tu Nombre y Apellidos<br>
11    Creado el dia - dd/mm/aaaa
12    <h2>Curso 2022/2023</h2>
13  </body>
14 </html>
```

Figura 2.23: Código de la página web

Para ello, abre un editor simple de texto, copia las líneas de código HTML personalizándolo con tu nombre y referenciando la imagen correctamente. Por último, guarda el archivo como “miprimeraweb.html” en la carpeta “miweb” y añade a la misma una foto tuya de tamaño carnet para que se visualice al abrir la página.

A continuación accede a dicha página web desde un navegador web en la máquina anfitriona usando esta URL: “[http://<IP\\_de\\_la\\_MV>/miweb/miprimeraweb.html](http://<IP_de_la_MV>/miweb/miprimeraweb.html)”.

Recuerda, el acceso será desde la máquina anfitriona (navegador web) a la MV (servidor web).

### Capturas:

- XAMPP instalado y con el servicio Apache en marcha.
- Creación del archivo “miprimeraweb.html” en un editor de texto (se debe ver el código HTML).
- Archivo “miprimeraweb.html” y archivo de fotografía situados en la carpeta “miweb”.
- Acceso a la página web creada desde un navegador web en la máquina anfitriona (se debe ver en la barra de direcciones la URL que se ha usado para acceder).

#### 2.4.2. Solución

En este ejercicio vamos a instalar el bundle **XAMPP**, que nos permite instalar al mismo tiempo **Apache** con **MySQL**, **PHP** y **Perl**.

1. En primer lugar, hemos descargado XAMPP desde [su página oficial](#) y hemos procedido a instalarlo, mediante el instalador que nos hemos descargado.

Una vez instalado, se ha abierto el **Panel de Control de XAMPP** y hemos activado el servidor web **Apache**, como podemos ver en la siguiente imagen.

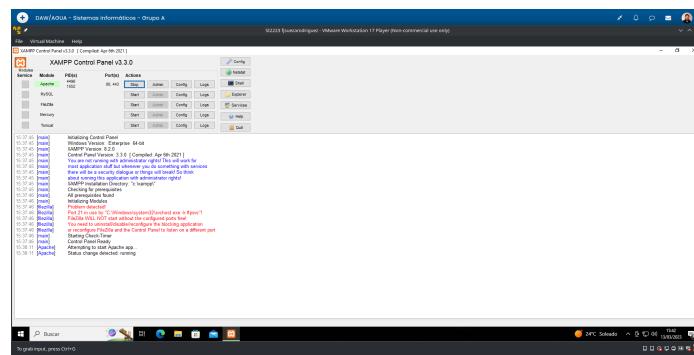


Figura 2.24: XAMPP instalado y con Apache ejecutándose

2. Una vez instalado correctamente XAMPP, hemos creado la que será nuestra página de prueba, usando para el **Notepad**, ya que es una web muy sencilla y no necesitamos editores más complejos. En la siguiente imagen se muestra el código creado en Notepad.

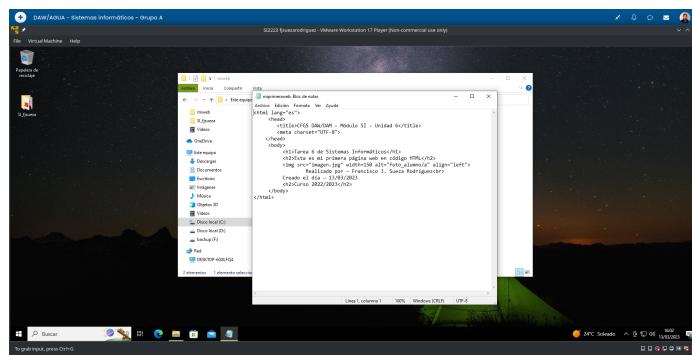


Figura 2.25: Creación del fichero HTML

3. Hemos creado un directorio dentro del directorio **htdocs**, llamado **miweb**, y hemos agregado el archivo HTML creado en el paso anterior y una imagen personal tamaño carnet.

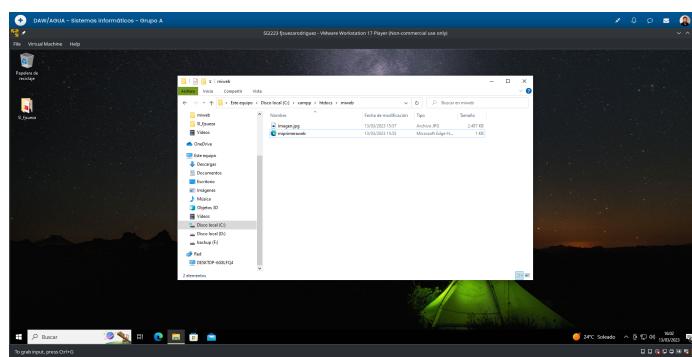


Figura 2.26: Archivos dentro de la carpeta miweb

4. Por último, hemos **accedido a la página web** creada desde el sistema anfitrión, específicamente desde el navegador web Firefox. En la siguiente captura, se puede ver el acceso a la página a través de la red.

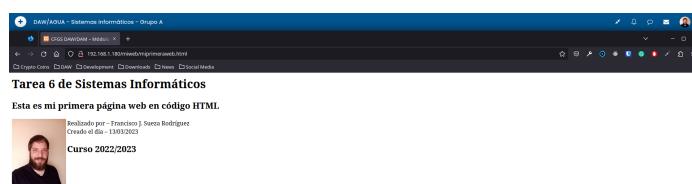


Figura 2.27: Acceso a la página web desde el sistema anfitrión

## 2.5. Actividad 5: Utilización de Antivirus

### **2.5.1. Enunciado**

Utilizando un antivirus, realiza lo siguiente:

1. Analiza una memoria USB que tengas conectada al ordenador. Comenta el resultado del análisis y qué se haría en caso de haber encontrado alguna amenaza.
  2. Configura un análisis completo programado para que se ejecute semanalmente todos los lunes a las 5:00 horas. Nombra la tarea como 'ANÁLISIS SEMANAL - <tu nombre completo y apellidos>'.

Para hacer esta actividad necesitas tener instalado un programa antivirus o puedes utilizar el propio "Windows Defender" incluido con Windows 10. Estos son algunos antivirus gratuitos que puedes instalar:

- Avast! Free Antivirus.
  - Avira Free Antivirus.
  - AVG Anti-virus Free Edition.

## Capturas:

- Acción para iniciar el análisis de la memoria USB.
  - Resultado del análisis de dicha memoria.
  - Programación del análisis semanal.

## 2.5.2. Solución

En este punto vamos a utilizar un **antivirus** para **analizar una memoria usb** y también vamos a **configurar análisis semanales** para mantener nuestro sistema seguro y libre virus. Nosotros hemos optado por usar **Windows Defender**, ya que es el software que viene por defecto en Windows 10.

1. En primer lugar hemos analizado un dispositivo USB. En nuestro caso, no contábamos con ningún pendrive, así que hemos conectado un **disco duro externo Seagate de 1 TB**.

Una vez conectado el disco, hemos abierto el **Explorador de archivos** y pulsado con el botón derecho sobre el dispositivo conectado, llamado **Multimedia** y con la letra **G** asignada. Cuando se despliega el menú contextual, podemos seleccionar la opción **Examinar con Windows Defender**, que una vez pulsada iniciará automáticamente un análisis de la unidad.

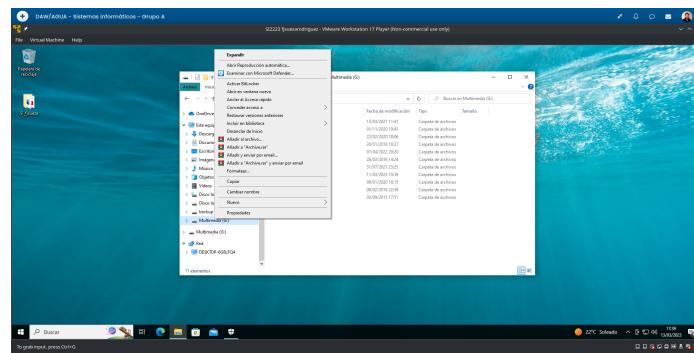


Figura 2.28: Menú contextual de la unidad USB conectada

2. Una vez realizado el examen, se nos ha notificado que **no existen amenazas**, pero en el caso de que las existieran, Windows Defender nos daría diferentes acciones a realizar, siendo las principales **eliminar los archivos infectados o poner estos en cuarentena**. En la siguiente imagen, vemos el resultado del análisis.

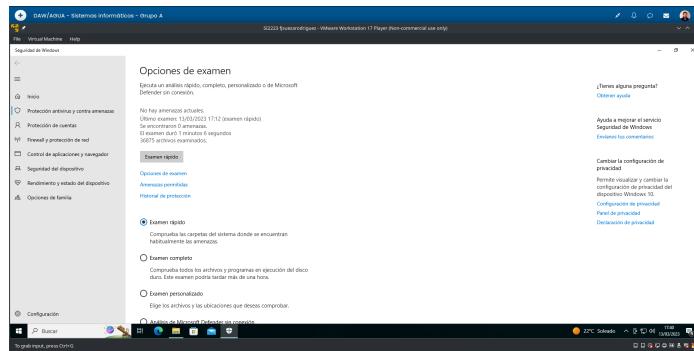


Figura 2.29: Resultado del análisis del dispositivo USB

3. Por último, vamos a **programar una tarea** para que Windows Defender realice un análisis del sistema todos **Lunes a las 5:00h**. Para ello, en primer lugar, hemos abierto el **Programador de Tareas**. En la **Biblioteca** el **Programador de Tareas** en el apartado **Microsoft**, buscamos y seleccionamos la carpeta de **Windows Defender**.

Desde aquí, podemos crear la nueva tarea, añadiendo un **desencadenador** para que se ejecute en la fecha deseada e indicando que se debe ejecutar la aplicación **Windows Defender Scheduled Scan**. Además de el resto de datos. En la siguiente imagen se puede ver la tarea ya correctamente programada.

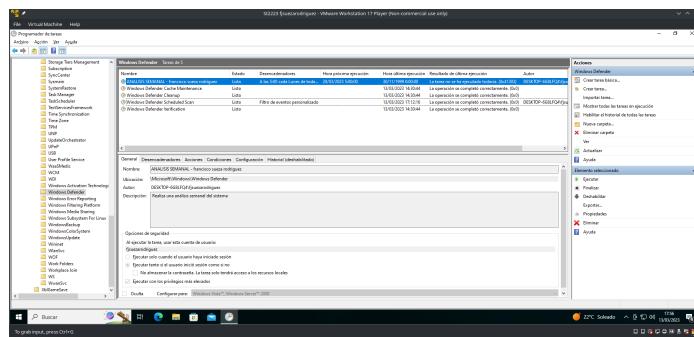


Figura 2.30: Tarea para el análisis semanal con Windows Defender programada

## 2.6. Actividad 6: Configuración de la Red Wi-Fi en un Router Inalámbrico y Conexión

### 2.6.1. Enunciado

Accede a un punto de acceso o router inalámbrico y muestra cómo se realizarían las siguientes operaciones:

1. Configuración de la clave de acceso al panel de configuración del router.
2. Configuración de la clave de red inalámbrica. Si aún no dispones de clave, establécela.
3. Configuración del tipo de cifrado. Cambia el cifrado a WPA2-Personal si no lo tienes así.

- Muestra cómo se activaría el filtrado de direcciones MAC para los equipos de tu red. Averigua la dirección MAC del equipo que estés usando o un dispositivo móvil de tu red y explica cómo se añadiría a la lista de filtrado por MAC. No es necesario que apliques y guardes estos cambios, basta con explicarlo y mostrar las ventanas donde se realiza.

#### Capturas:

- Acceso al punto de acceso inalámbrico a través de un navegador web (se debe ver la URL usada para acceder).
- Configuración de la clave de acceso al panel de configuración del router.
- Configuración de la clave de red inalámbrica.
- Configuración del cifrado en WPA2-Personal.
- Dirección MAC del equipo que estás usando o de otro equipo de tu red.
- Configuración del filtrado de direcciones MAC.
- Conexión a dicha red inalámbrica desde un cliente Windows (debe verse cómo se selecciona la red indicada).

#### 2.6.2. Solución

En esta última actividad vamos a realizar diferentes **tareas de administración** de nuestro **router Wi-Fi**. Las tareas que hemos realizado son las siguientes:

- En primer lugar nos hemos conectado al router a través de la su interfaz web. Para ello, hemos introducido la dirección **192.168.1.1** en el navegador web y a continuación hemos introducido los credenciales de acceso al router. En nuestro caso, ya habíamos cambiado la contraseña que viene por defecto, no así el usuario. Muestro router es un modelo **Sagemcom Fast 5657**.

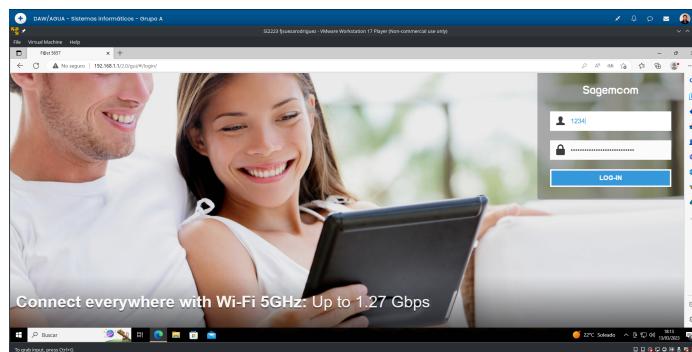


Figura 2.31: Acceso al router con su interfaz web

- El siguiente paso es sería cambiar la **contraseña de acceso** al router. En este ruter, hay que pulsar en la opción **Access Control** y después en la pestaña **User**, lo que nos desplegará un formulario con el que podremos cambiar la contraseña de acceso.

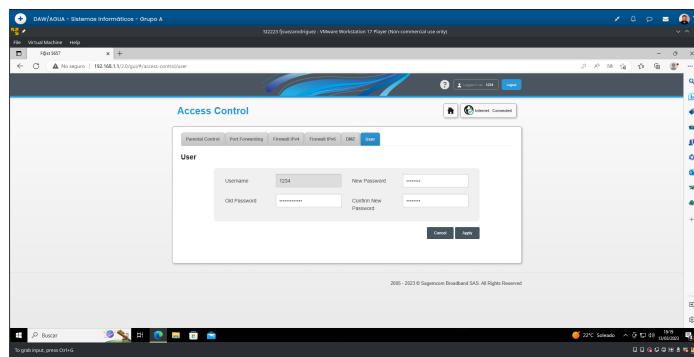


Figura 2.32: Cambio de contraseña de acceso al router

3. A continuación vamos a cambiar la **contraseña de la red inalámbrica**. Para cambiarla, debemos pulsar en el **ícono de una rueda** que aparece en la interfaz principal, al lado del nombre de la red. En la siguiente imagen, se muestra dicho ícono, que también servirá para futuros pasos.

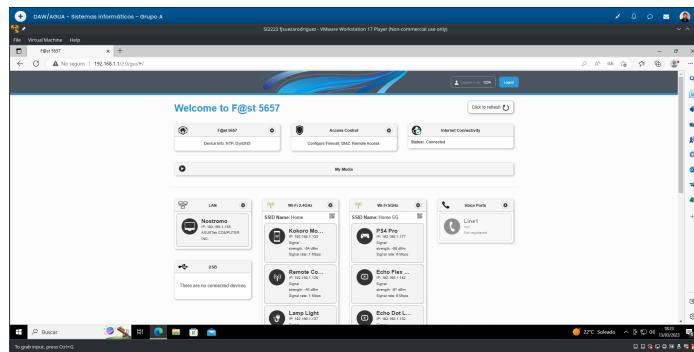


Figura 2.33: Interfaz principal del router

En la ventana que se nos carga, en la parte inferior, podemos **cambiar la contraseña de la red**. Si queremos, podemos establecer diferentes contraseñas para la red 2.4 Ghz y la 5Ghz.

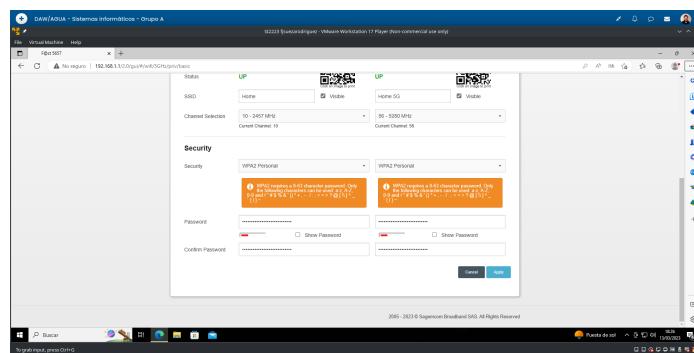


Figura 2.34: Cambio de contraseña de red

4. En la misma ventana donde nos encontrábamos en el punto anterior, podemos cambiar el **cifrado a WPA2 Personal**. Como podemos ver en la siguiente captura (y en la anterior), la contraseña ya tiene es tipo de cifrado.

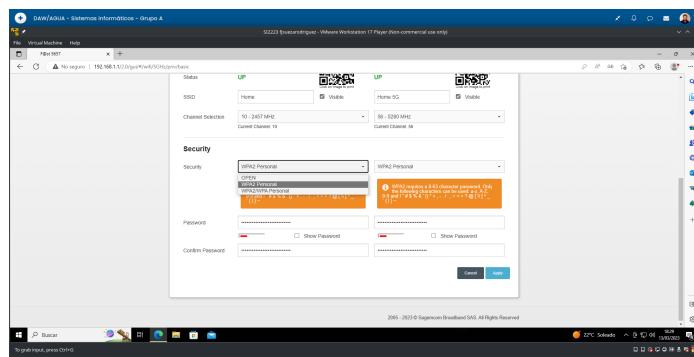


Figura 2.35: Cambio del cifrado de la contraseña Wi-Fi

5. A continuación vamos a ver la cual es la **dirección MAC** de alguno de los dispositivos conectados a la red. Desde la **interfaz principal** del router, que hemos mostrado en la **figura 2.33**, podemos pulsar en alguno de los dispositivos que se muestran conectados a la red 2.4Ghz o a la 5Ghz. Nosotros hemos pulsado en uno y se nos muestra una pantalla con información relevante al dispositivo y su conexión con el router, entre esta información, esta la dirección MAC.

En concreto, la dirección MAC del dispositivo elegido es **BC:CE:25:FB:B7:CC**, como vemos en la siguiente captura.

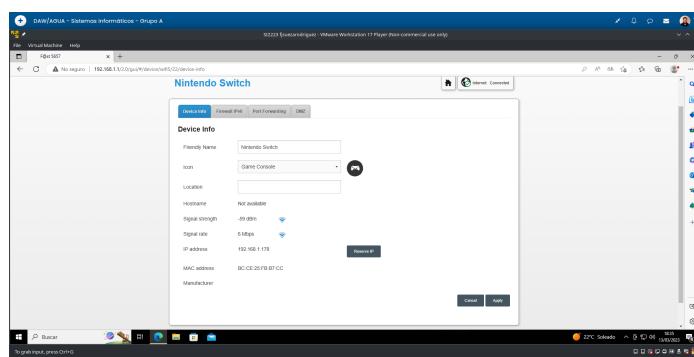


Figura 2.36: Dirección MAC de un dispositivo conectado a la red

6. Ahora vamos a usar esa dirección en el **filtrado de direcciones MAC**. Pulsamos en el icono de la rueda, al lado del nombre de alguna de las dos redes, y en la ventana que se nos carga, en la pestaña **MAC Filter**. Aquí podemos seleccionar el modo de filtrado. Si seleccionamos **Allow All**, permitirá a cualquier dispositivo conectar. En cambio si seleccionamos **Allow** solo permitirá conectarse a los dispositivos de la tabla inferior y por último si seleccionamos **Deny**, denegará el acceso a los dispositivos introducidos.

Nosotros hemos seleccionado **Deny** e introducido la dirección MAC del dispositivo del punto anterior.

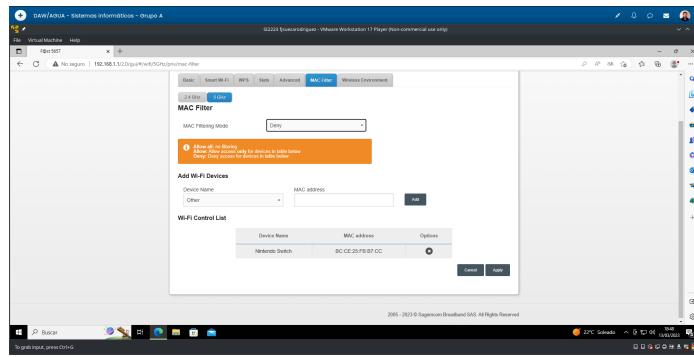


Figura 2.37: Configuración del filtrado MAC

7. Por último,, para conectar a una red Wi-Fi, solo tenemos que pulsar en icono de red, y si tenemos una tarjeta wireless, se nos mostrará el conjunto de redes detectado, pulsamos en la red seleccionada y nos pedirá que introduzcamos los credenciales. Si los tenemos, los introducimos y podremos conectar a la red.

**NOTA:** Esta captura esta realizada en Linux, pero el proceso es exactamente igual que en Windows.

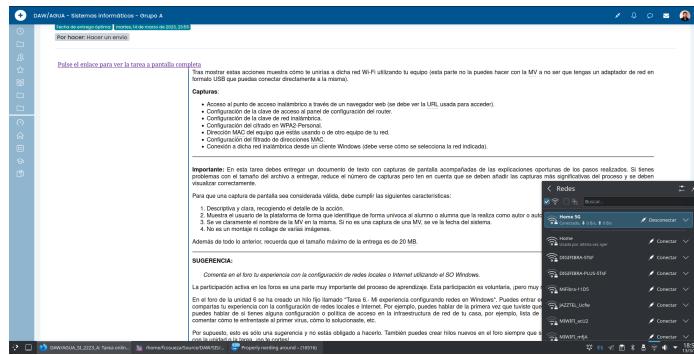


Figura 2.38: Conexión a una red inalámbrica