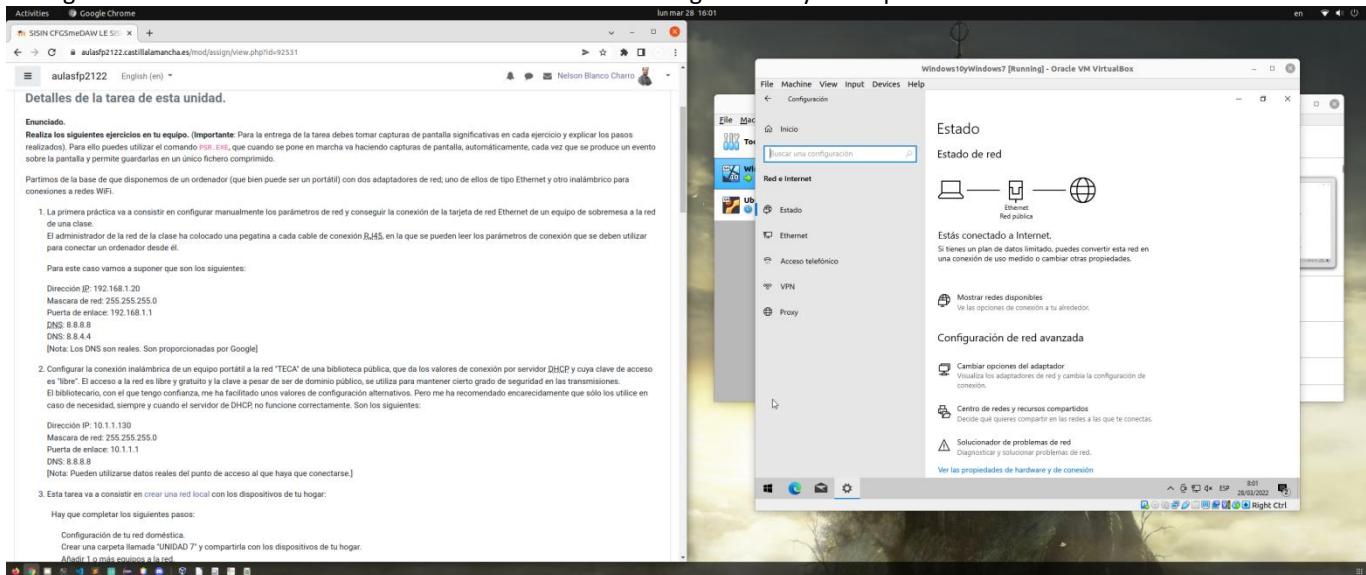


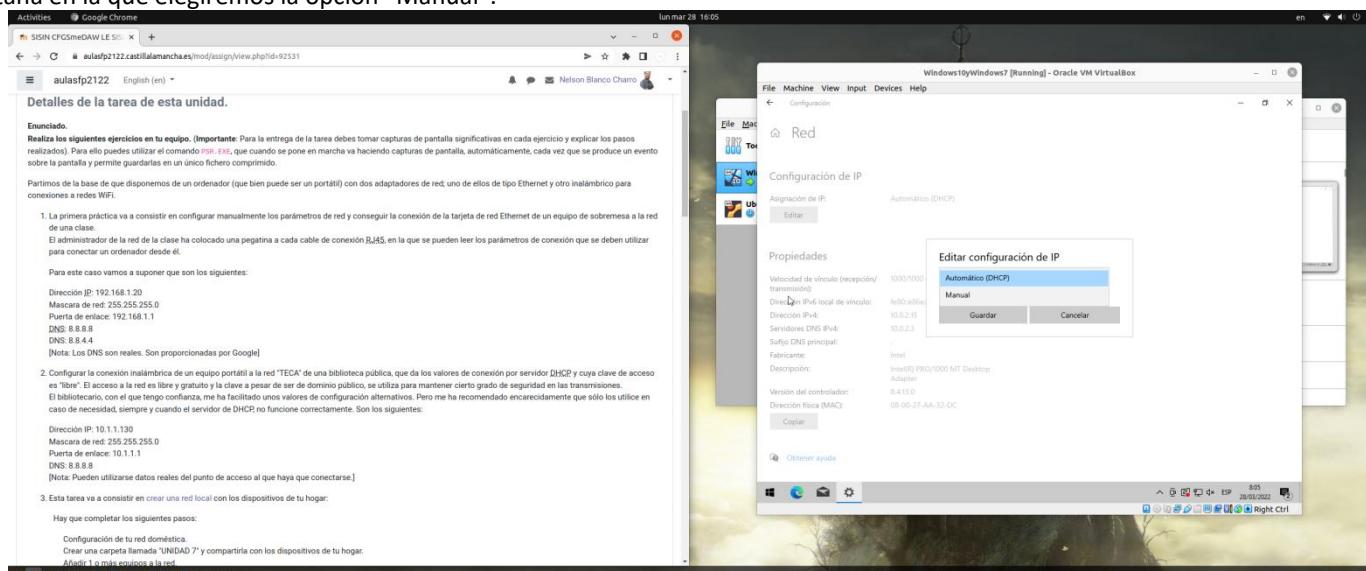
Actividad 1

La primera práctica va a consistir en configurar manualmente los parámetros de red y conseguir la conexión de la tarjeta de red Ethernet de un equipo de sobremesa a la red de una clase. El administrador de la red de la clase ha colocado una pegatina a cada cable de conexión RJ45, en la que se pueden leer los parámetros de conexión que se deben utilizar para conectar un ordenador desde él.

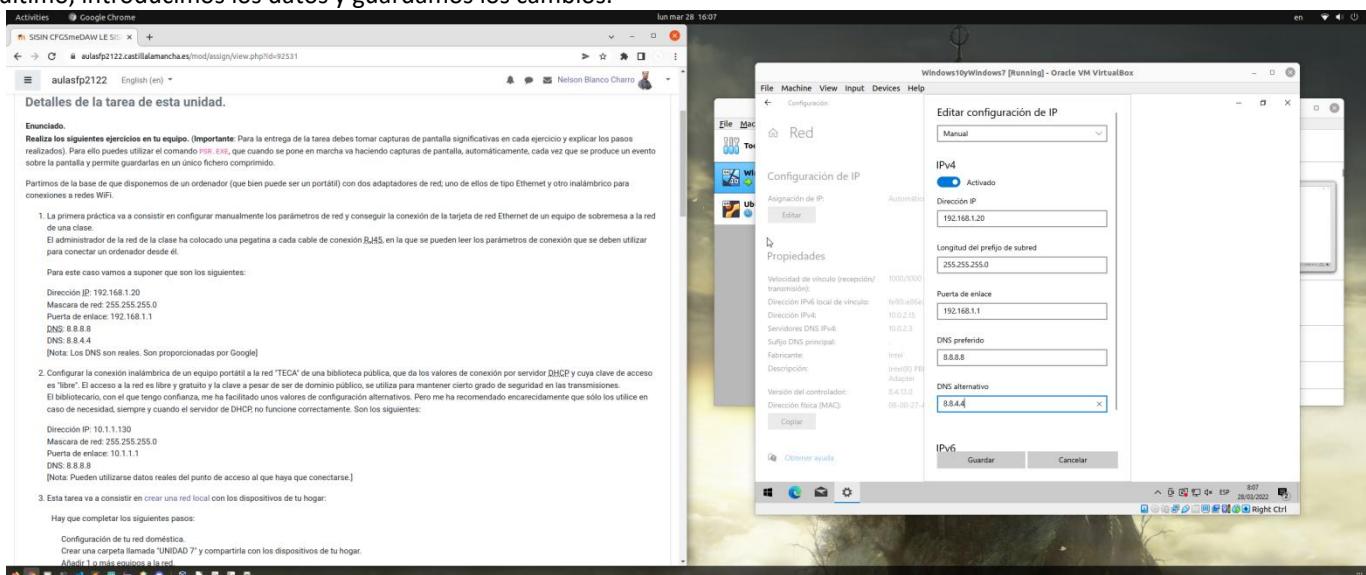
Para configurar manualmente una red Ethernet debemos ir a “Configuración” y a la opción “Red e internet”



A continuación, en la pestaña “Ethernet” seleccionamos la red y hacemos clic en “Editar” en la configuración de IP. Nos aparecerá una ventana en la que elegiremos la opción “Manual”.



Por último, introducimos los datos y guardamos los cambios.

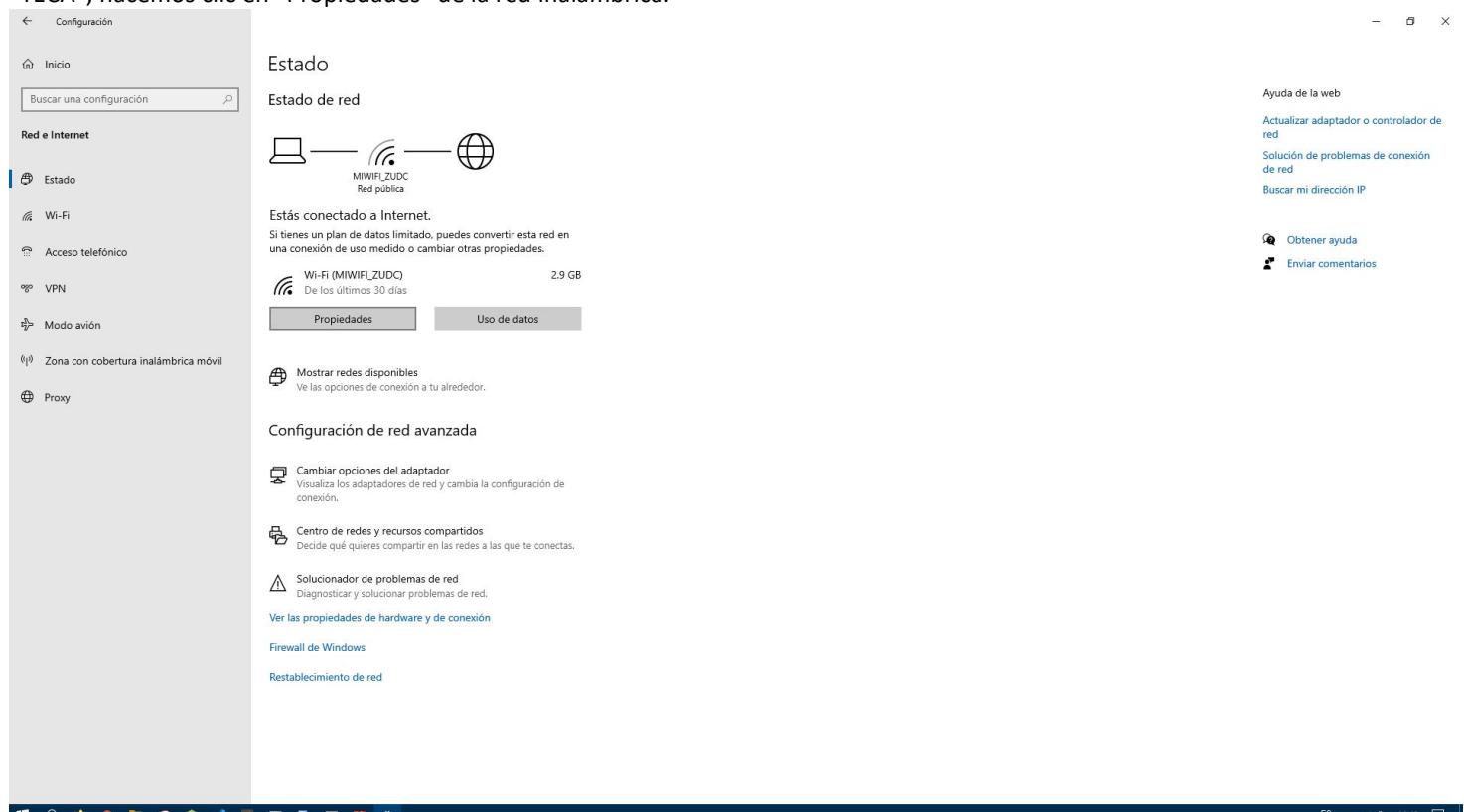


Actividad 2

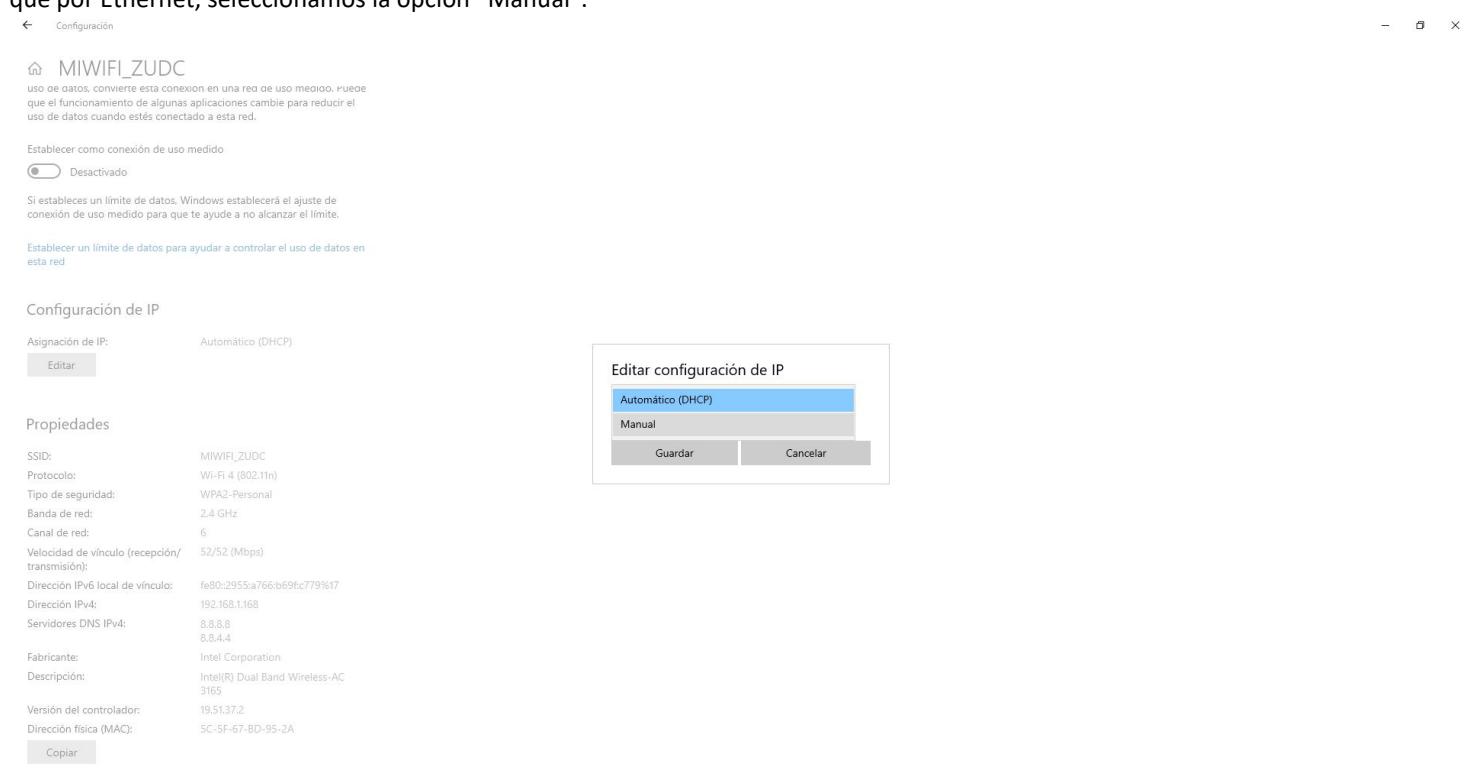
Configurar la conexión inalámbrica de un equipo portátil a la red "TECA" de una biblioteca pública, que da los valores de conexión por servidor DHCP y cuya clave de acceso es "libre". El acceso a la red es libre y gratuito y la clave a pesar de ser de dominio público, se utiliza para mantener cierto grado de seguridad en las transmisiones.

El bibliotecario, con el que tengo confianza, me ha facilitado unos valores de configuración alternativos. Pero me ha recomendado encarecidamente que sólo los utilice en caso de necesidad, siempre y cuando el servidor de DHCP, no funcione correctamente.

Para realizar la configuración, nos situamos en la configuración del apartado anterior, en "Red e internet". Una vez conectados a la red "TECA", hacemos clic en "Propiedades" de la red inalámbrica.



Nos aparecerá la configuración de la red, navegamos hasta "Configuración de IP" y hacemos clic en la opción "Editar". Del mismo modo que por Ethernet, seleccionamos la opción "Manual".



Por último, introducimos los datos facilitados por el bibliotecario y guardamos la configuración.

← Configuración

- ⌂ ×

MIWIFI_ZUDC

uso de datos: convierte esta conexión en una red de uso medio. Puede que el funcionamiento de algunas aplicaciones cambie para reducir el uso de datos cuando estés conectado a esta red.

Establecer como conexión de uso medio

Desactivado

Si estableces un límite de datos, Windows establecerá el ajuste de conexión de uso medio para que te ayude a no alcanzar el límite.

Establecer un límite de datos para ayudar a controlar el uso de datos en esta red

Configuración de IP

Asignación de IP: Automático (DHCP)

[Editar](#)

Propiedades

SSID:	MIWIFI_ZUDC
Protocolo:	Wi-Fi 4 (802.11n)
Tipo de seguridad:	WPA2-Personal
Banda de red:	2.4 GHz
Canal de red:	6
Velocidad de vínculo (recepción/transmisión):	52/52 (Mbps)
Dirección IPv6 local de vínculo:	fe80::2955:a766:b69fc779%17
Dirección IPv4:	192.168.1.168
Servidores DNS IPv4:	8.8.8 8.8.4
Fabricante:	Intel Corporation
Descripción:	Intel(R) Dual Band Wireless-AC 3165
Versión del controlador:	19.51.37.2
Dirección física (MAC):	5C-5F-67-8D-95-2A

[Copiar](#)

Editar configuración de IP

Manual

IPv4

Activado

Dirección IP: 10.1.1.130

Longitud del prefijo de subred: 255.255.255.0

Puerta de enlace: 10.1.1.1

DNS preferido: 8.8.8.8

DNS alternativo: 8.8.4.4

IPv6

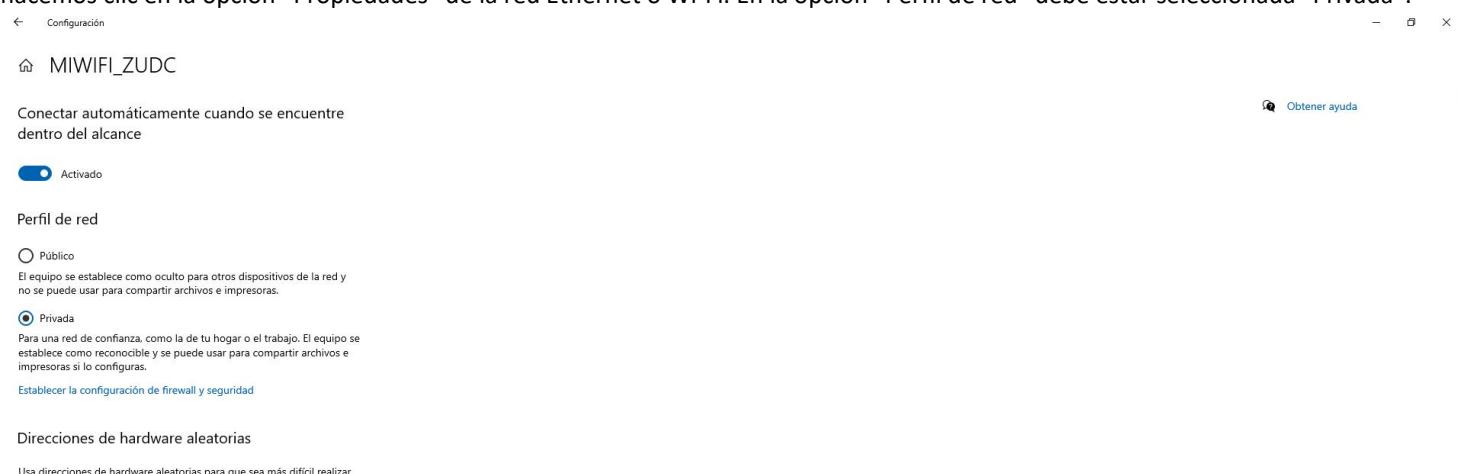
Guardar Cancelar



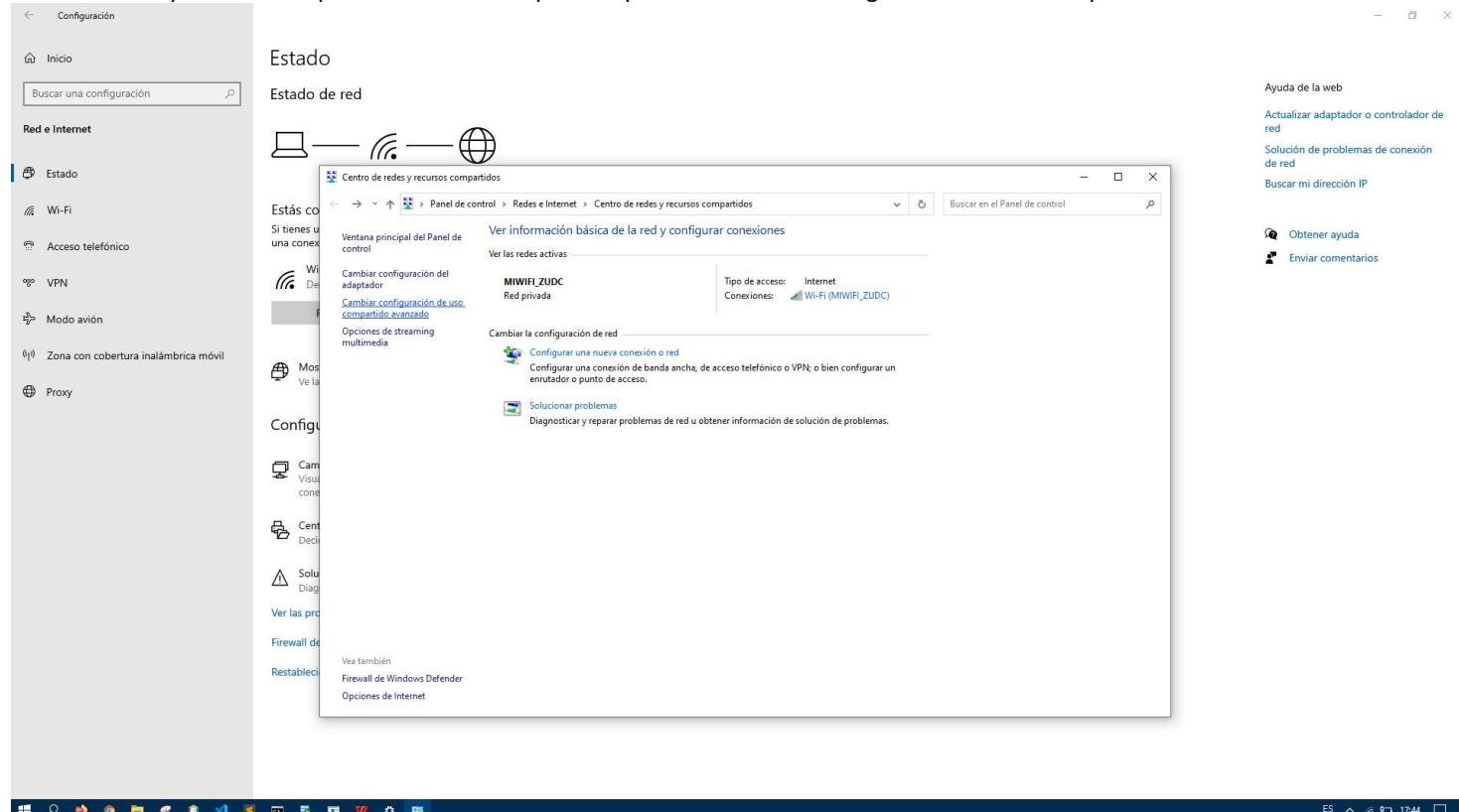
Actividad 3

Esta tarea va a consistir en crear una red local con los dispositivos de tu hogar.

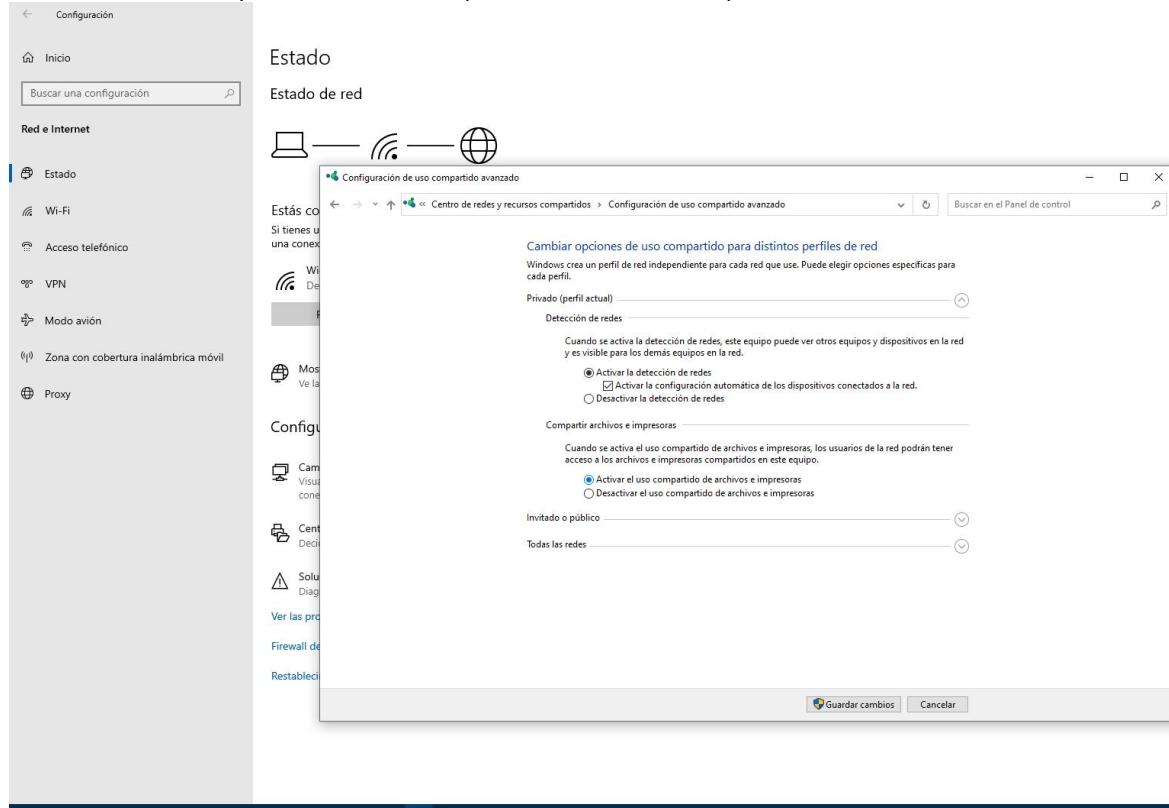
Primero debemos asegurarnos que nuestro equipo esté configurado como perfil privado. Para comprobarlo, en “Red e internet” hacemos clic en la opción “Propiedades” de la red Ethernet o Wi-Fi. En la opción “Perfil de red” debe estar seleccionada “Privada”.



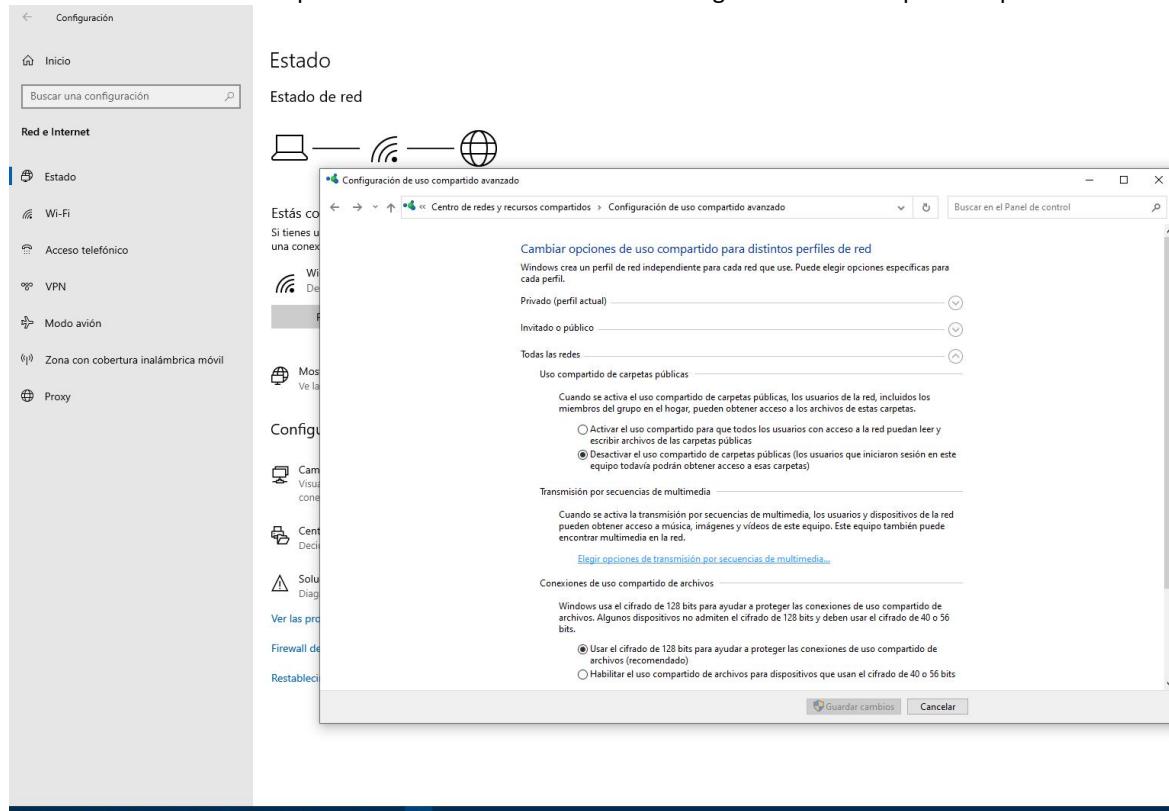
Volvemos a “Red e internet” y en la pestaña “Estado” hacemos clic en “Centro de redes y recursos compartidos”. Nos aparecerá una ventana en la que tenemos que hacer clic en la opción izquierda “Cambiar configuración de uso compartido avanzado”.



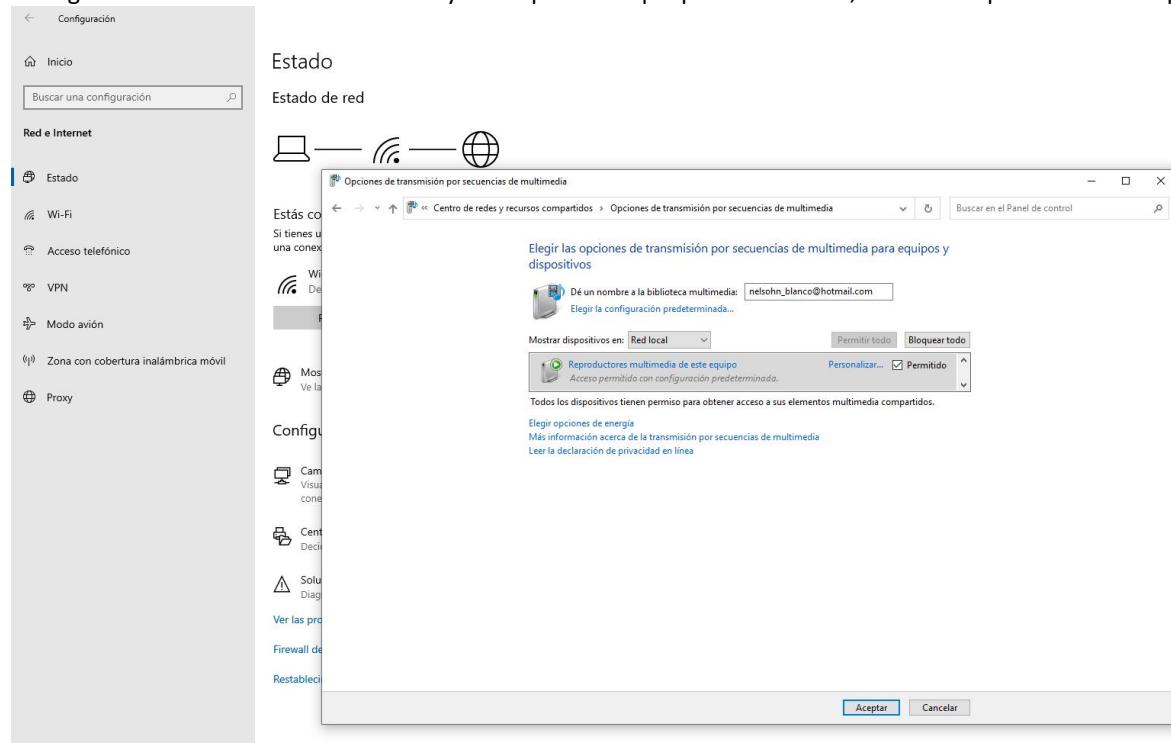
En la ventana que aparece tenemos que tener marcada las opciones “Activar la configuración automática de los dispositivos conectados a la red” y “Activar el uso compartido de archivos e impresoras”.



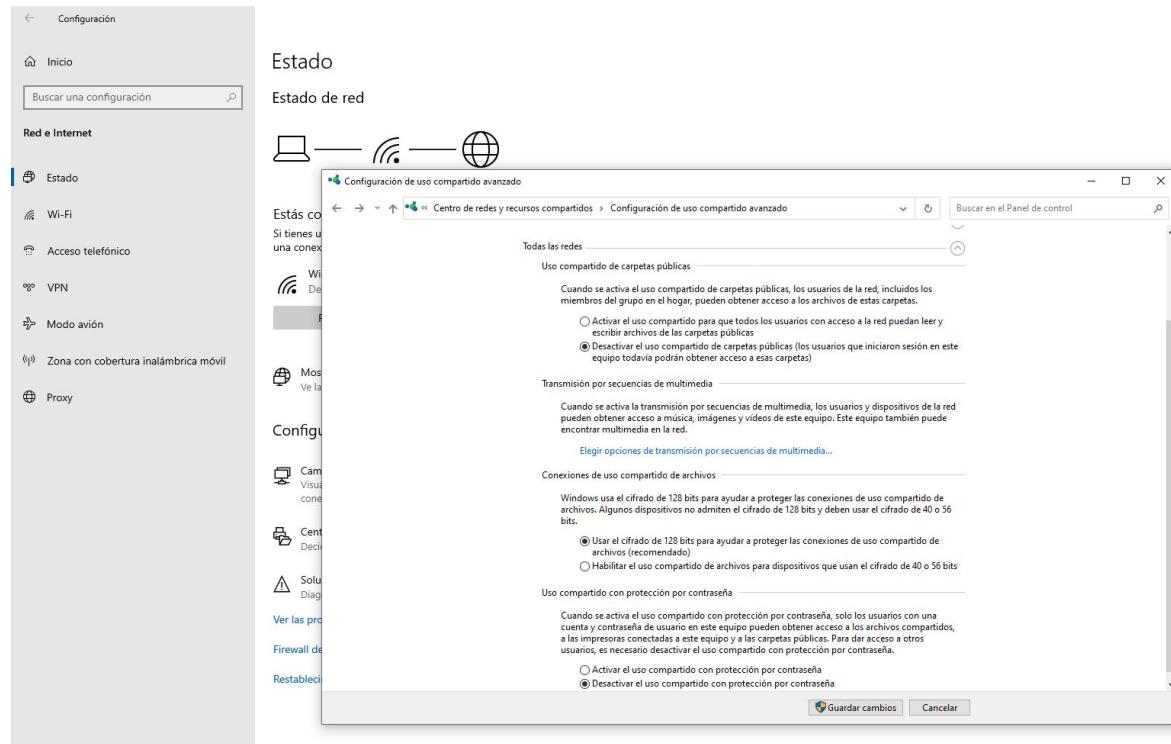
Desplegamos la última opción “Todas las redes” y hacemos clic en “Elegir opciones de transmisión por secuencias de multimedia” y “Activamos la transmisión por secuencias de multimedia ” en la siguiente ventana que nos aparece.



Configuramos el nombre del ordenador y los dispositivos que podrán acceder, finalmente pulsamos en aceptar.

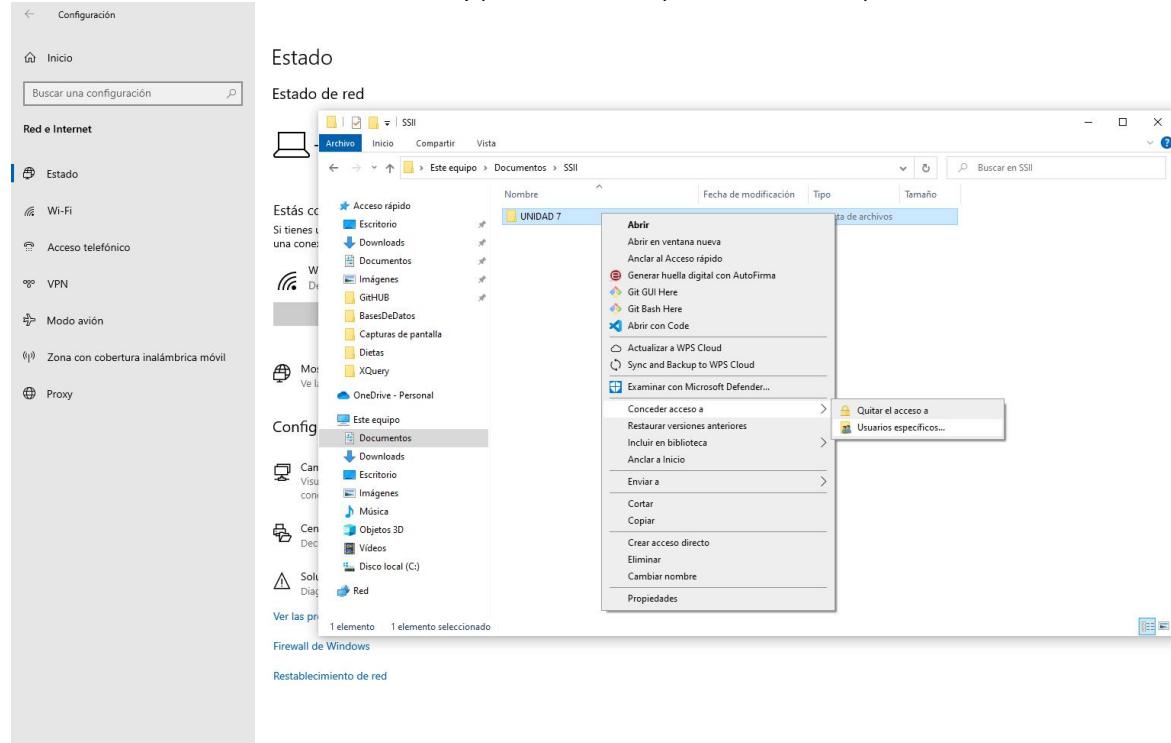


Como último paso, en el desplegable “Todas las redes” debemos marcar la opción “Desactivar el uso compartido con protección por contraseña”.

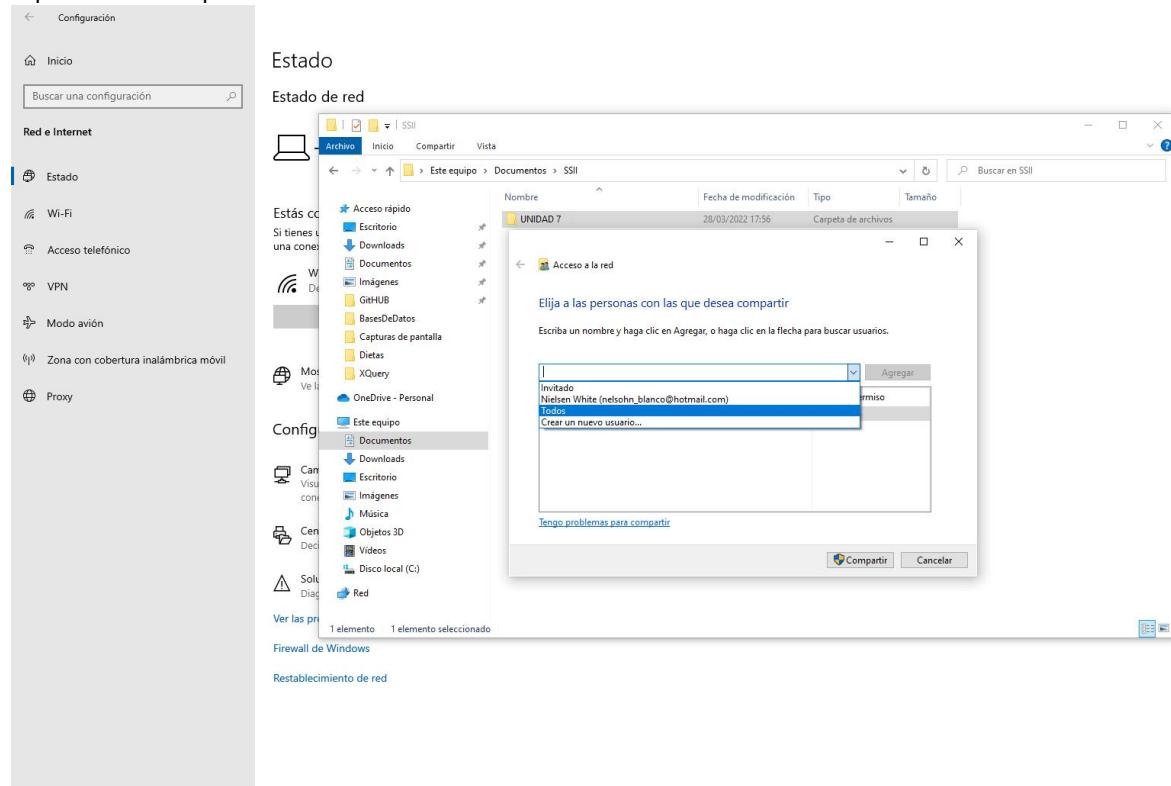


Guardamos cambios y tendremos configurada la red doméstica.

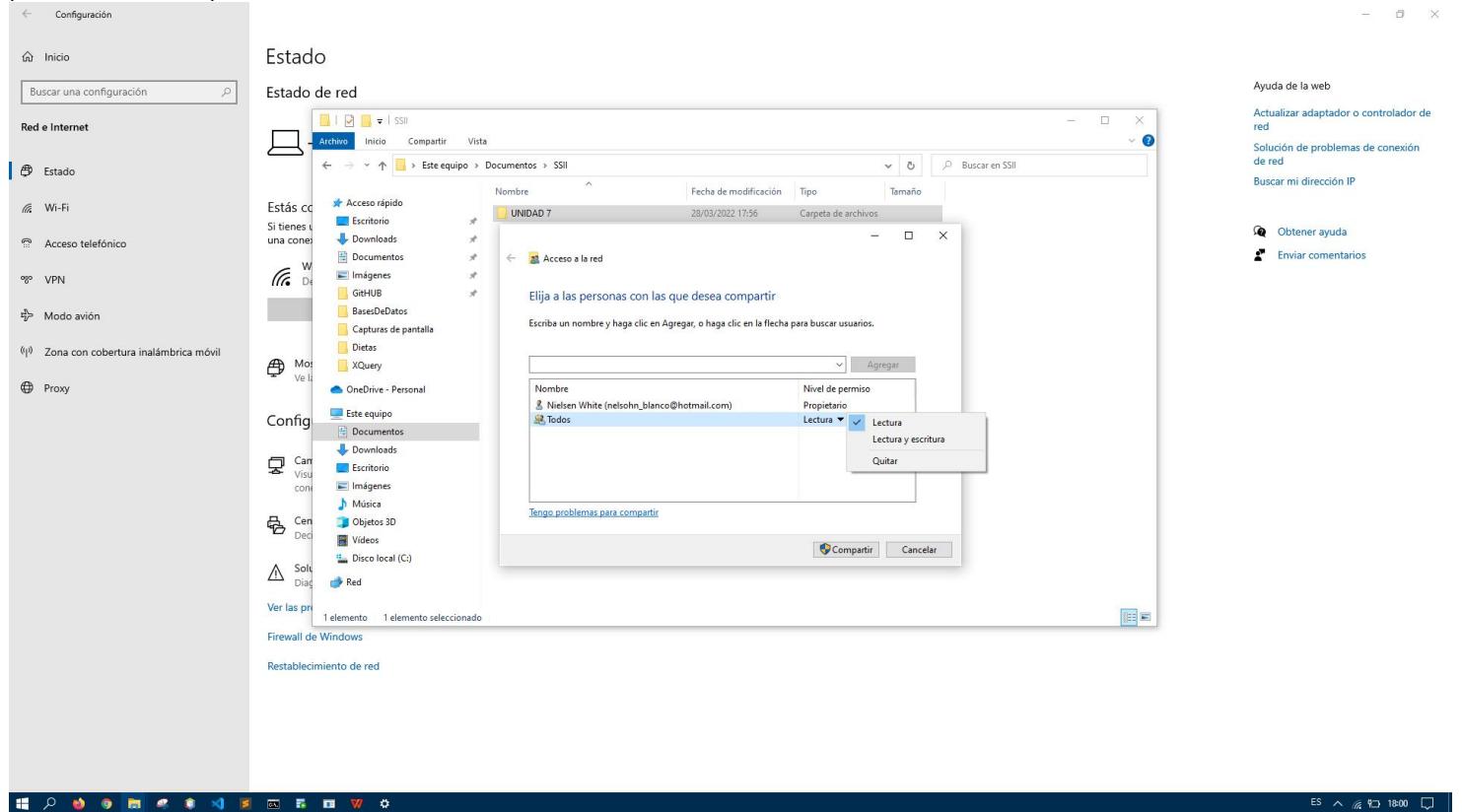
Creamos una carpeta llamada “UNIDAD 7” para compartirla en la red doméstica. Para ello hacemos clic derecho sobre la carpeta, accedemos al menú “Conceder acceso a” y pulsamos en la opción “Usuarios específicos”.



Nos aparecerá una ventana en la que debemos elegir las personas con las que compartir la carpeta en la red. Podemos elegir usuarios específicos o compartirla con “Todos”.



Una vez agregado el usuario o usuario, debemos seleccionar el nivel de permiso si es de “lectura” o de “lectura y escritura”. Finalmente, pulsamos en “Compartir”.

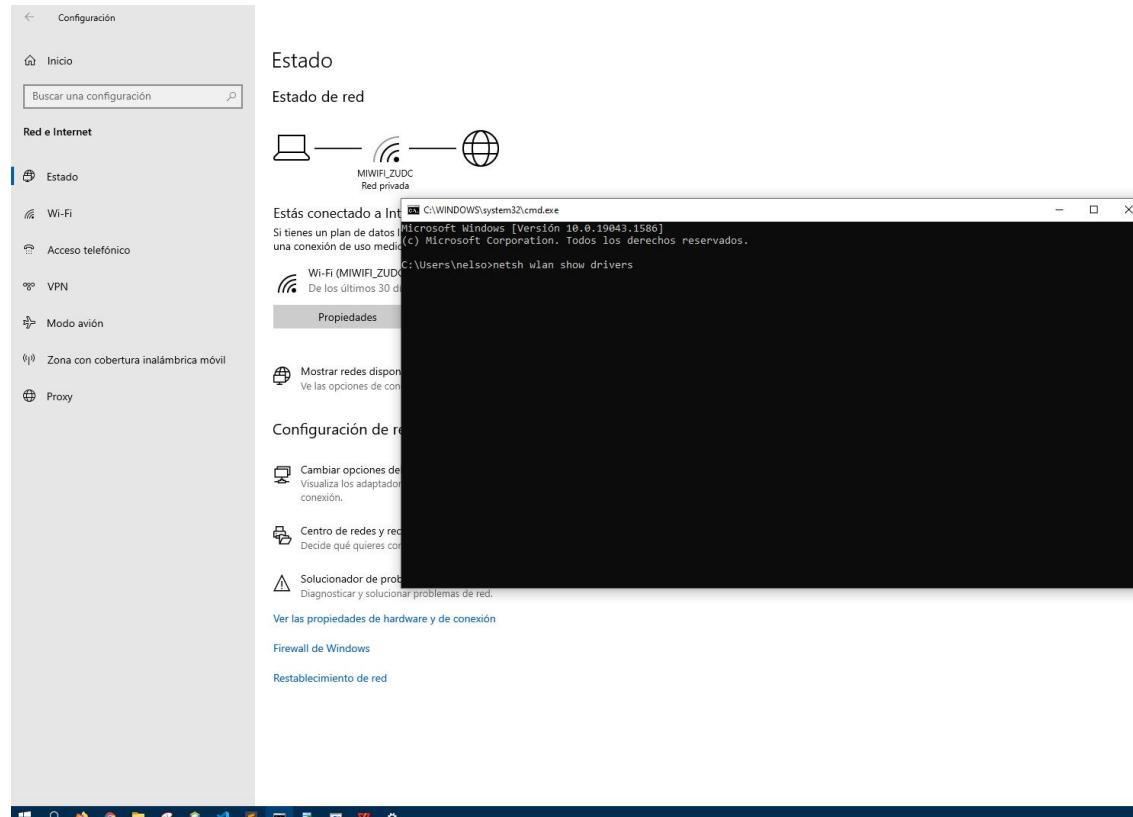


De éste modo se habrá compartido por la red local la carpeta con todos los archivos en ella en modo lectura, es decir, no se permite modificar los archivos solo verlos o copiarlos.

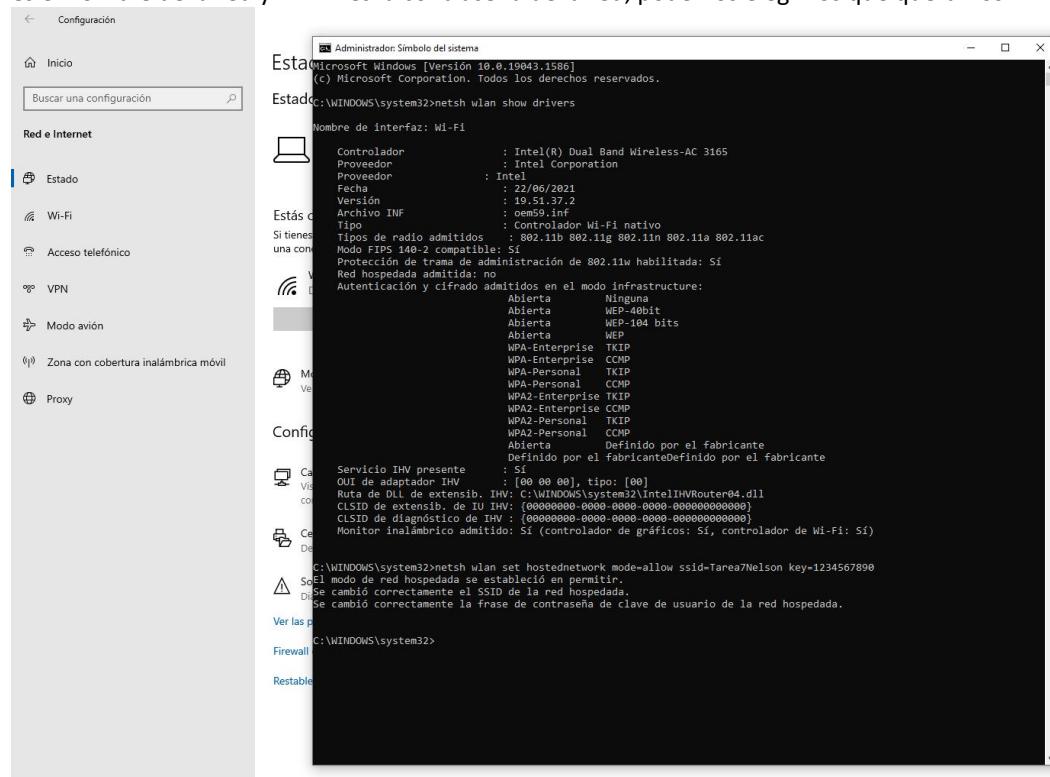
Actividad 4

Crear una conexión AD-HOC para traspasar de un ordenador a otro el extenso contenido de una carpeta concreta, por ejemplo: la carpeta "Mis proyectos". Es necesario utilizar este tipo de conexión por ser la única alternativa viable y disponible.

Para crear una conexión AD-HOC en Windows 10 utilizaremos el terminal, para ello pulsamos la tecla Windows + R, a continuación tecleamos "cmd" y pulsamos intro. Nos aparecerá el terminal en el que tenemos que introducir el siguiente comando "netsh wlan show drivers".



A continuación, introducimos el siguiente comando "netsh wlan set hostednetwork mode=allow ssid=XXXXXX key=YYYYYY". Donde XXXXXX es el nombre de la red y YYYYYY es la contraseña de la red, podemos elegir los que queramos.



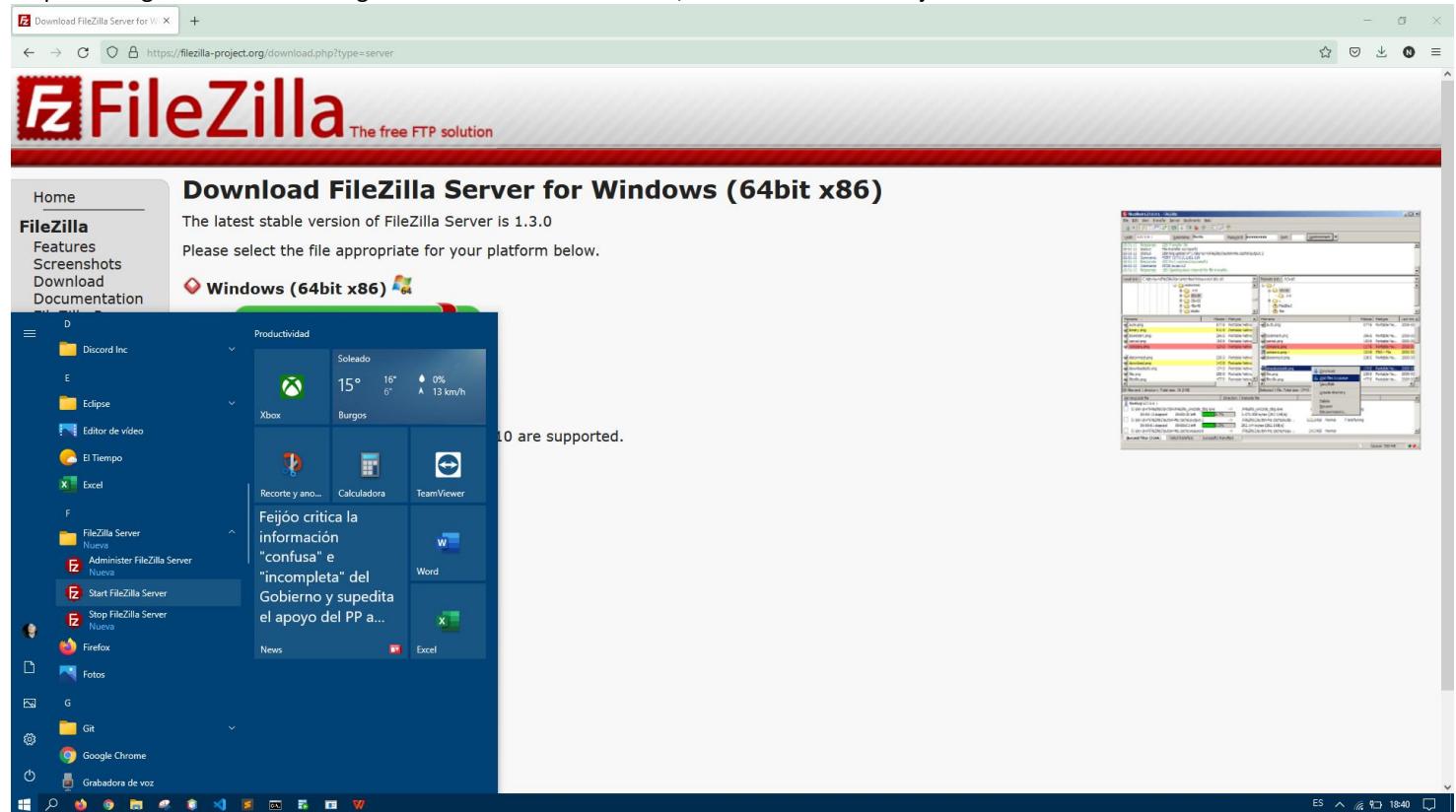
Finalmente, introducimos la sentencia "netsh wlan start hostednetwork" para activar la red ad-hoc. Para verificar que se ha creado correctamente, en el otro ordenador nos debería aparecer el Wi-Fi "Tarea7Nelson" que en éste caso es la red ad-hoc creada.

Actividad 5

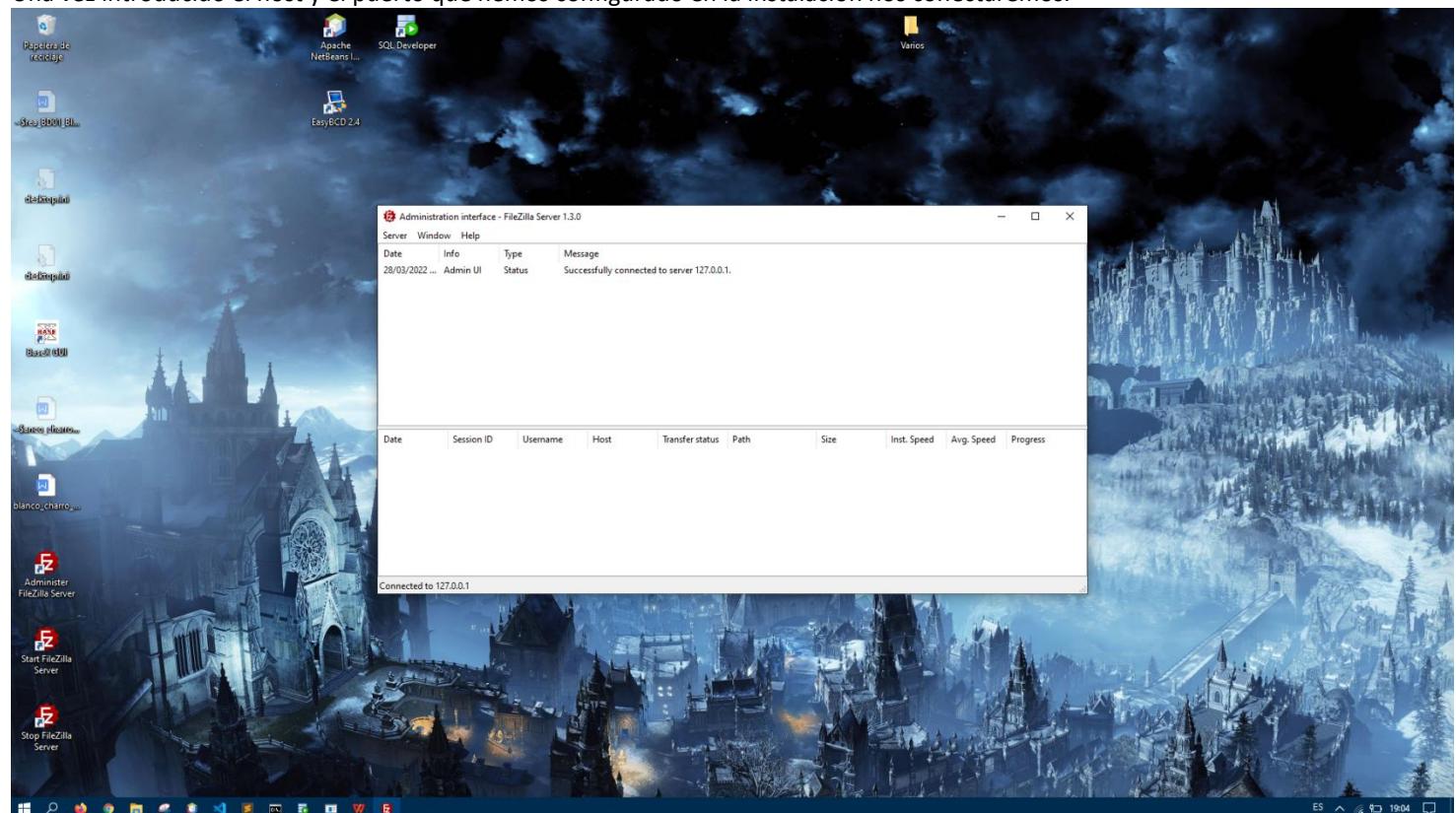
Realiza la configuración de los siguientes servidores:

a. Instala y configura un servidor FTP con el servicio de FTP que suministra Windows 10 (con autenticación básica y permitiendo SSL). Para el cliente utiliza el programa Filezilla. El nombre del sitio FTP será `damsi_<initial_de_tu_nombre_y_primer_apellido>`.

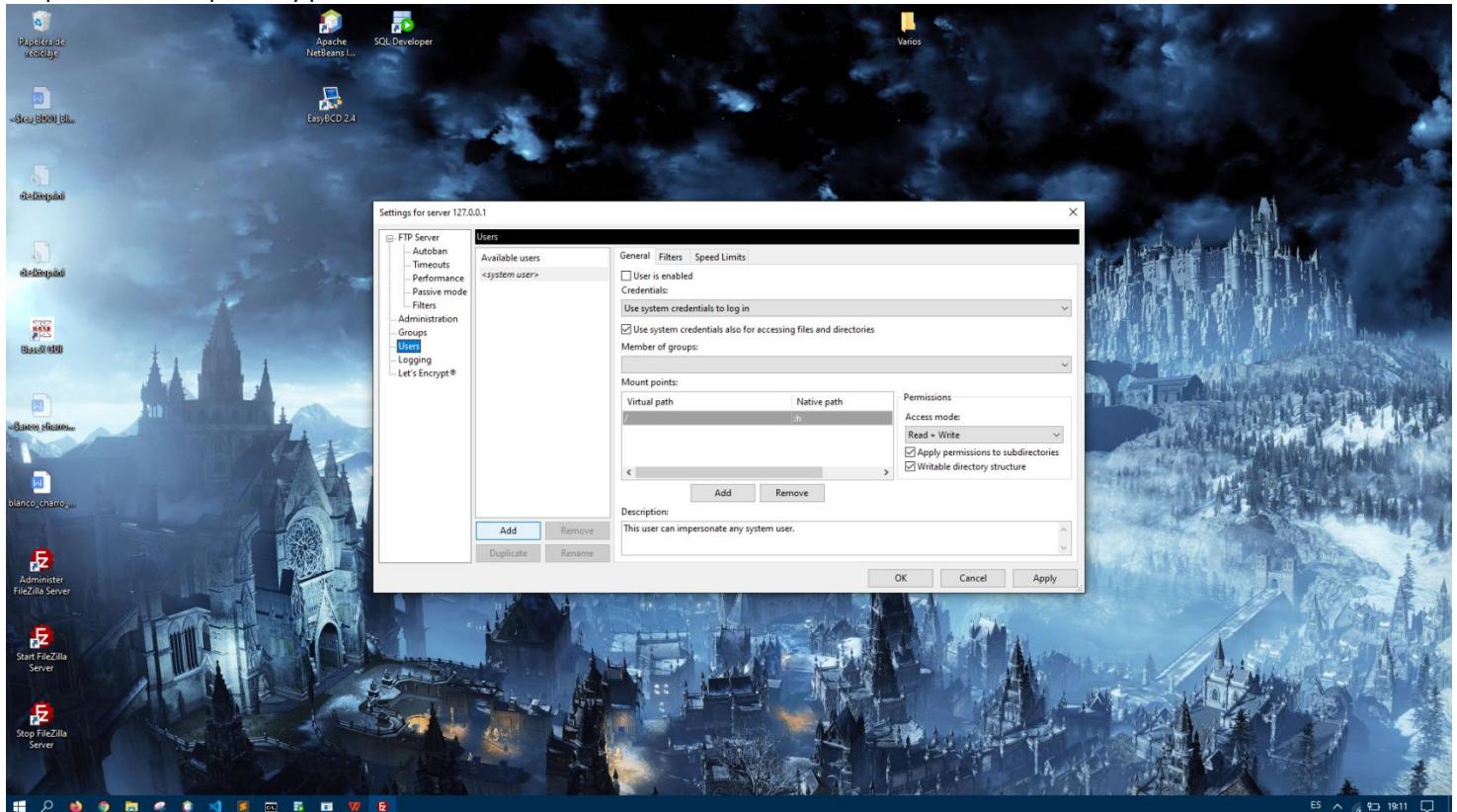
En primer lugar debemos descargar e instalar "FileZilla Server", una vez instalado lo ejecutamos como administrador.



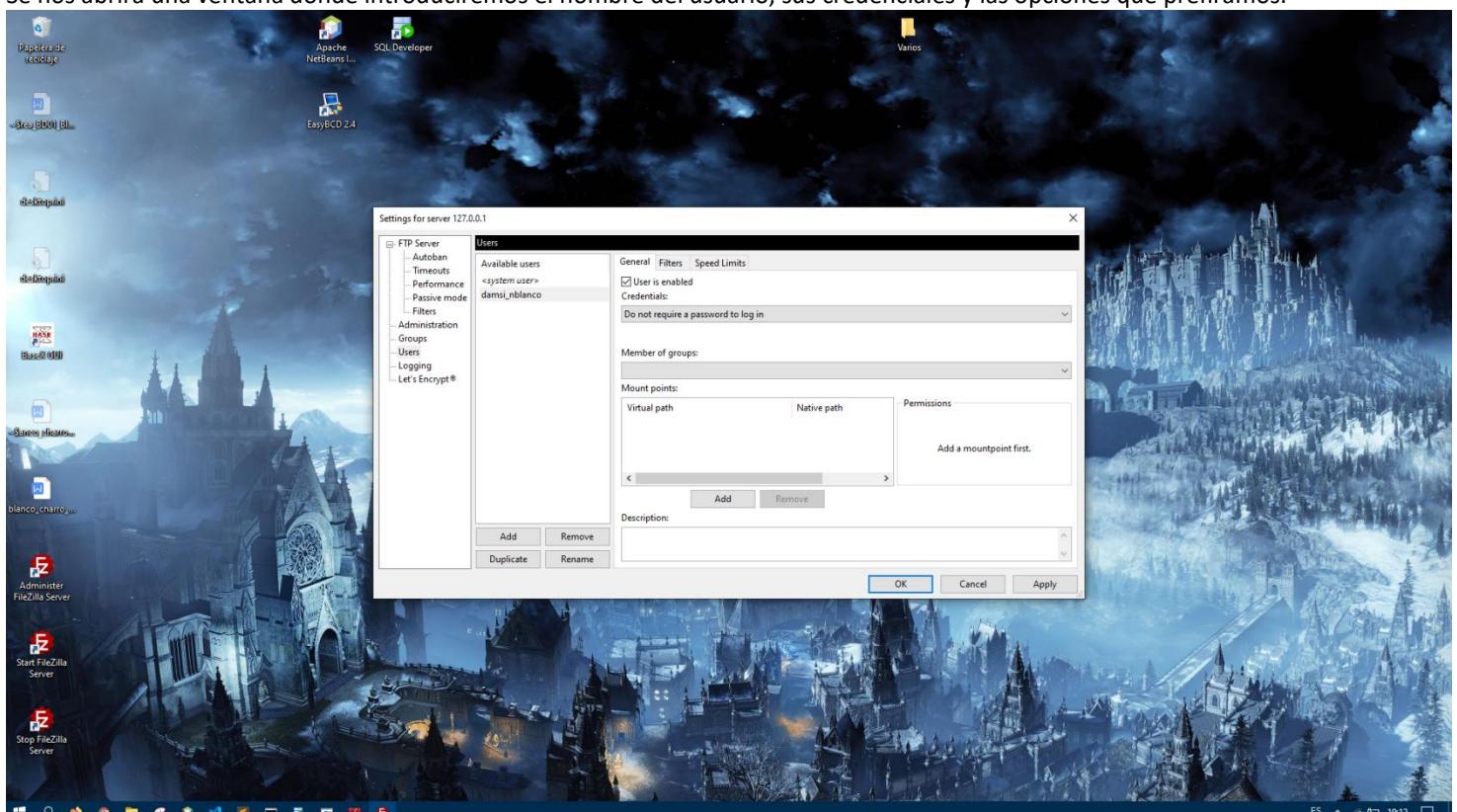
Una vez introducido el host y el puerto que hemos configurado en la instalación nos conectaremos.



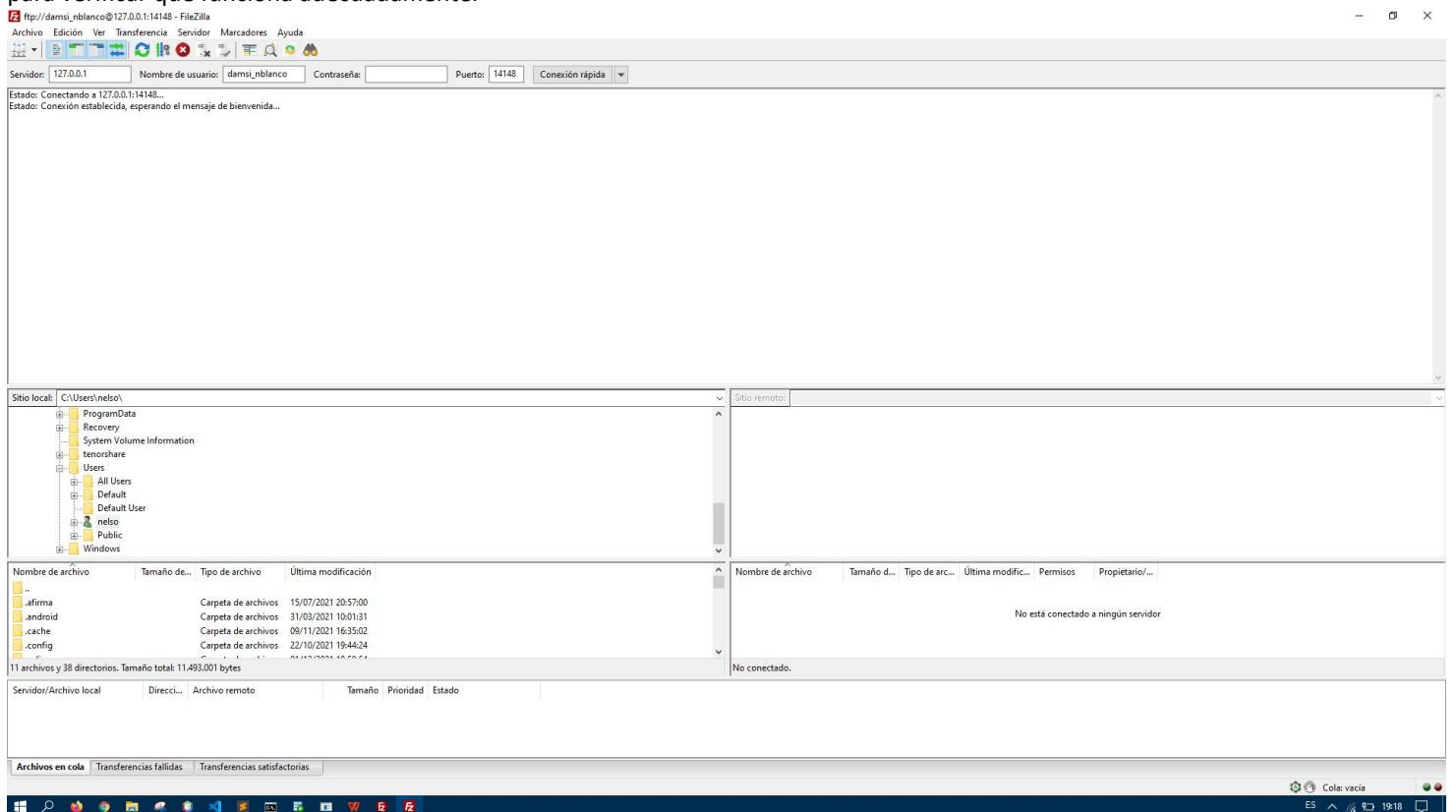
A continuación, crearemos un usuario llamado “damsi_nblanco”, para ello hacemos clic en la pestaña “Server” y en la opción “Configure”. Nos aparecerá una ventana con las configuraciones del servidor FTP creado. Para crear el usuario hacemos clic en “Users” del panel lateral izquierdo y pulsamos en “Add”.



Se nos abrirá una ventana donde introduciremos el nombre del usuario, sus credenciales y las opciones que prefiramos.

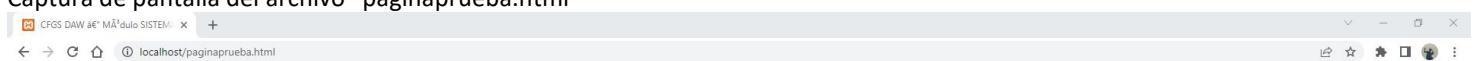


Para probar la conexión debemos descargar e instalar FileZilla Client. Cuando lo tengamos instalado, lo ejecutamos y nos aparecerá una ventana, para probar que el servidor funciona correctamente lo que haremos será loggearnos con el usuario creado anteriormente para verificar que funciona adecuadamente.

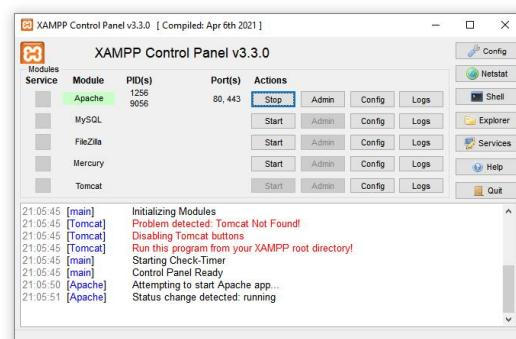


b. Instala y configura un servidor web en tu equipo con el programa XAMPP. Una vez activados los servicios, en la carpeta pública del servidor Apache guarda un archivo html con el siguiente código.

Captura de pantalla del archivo “página prueba.html”



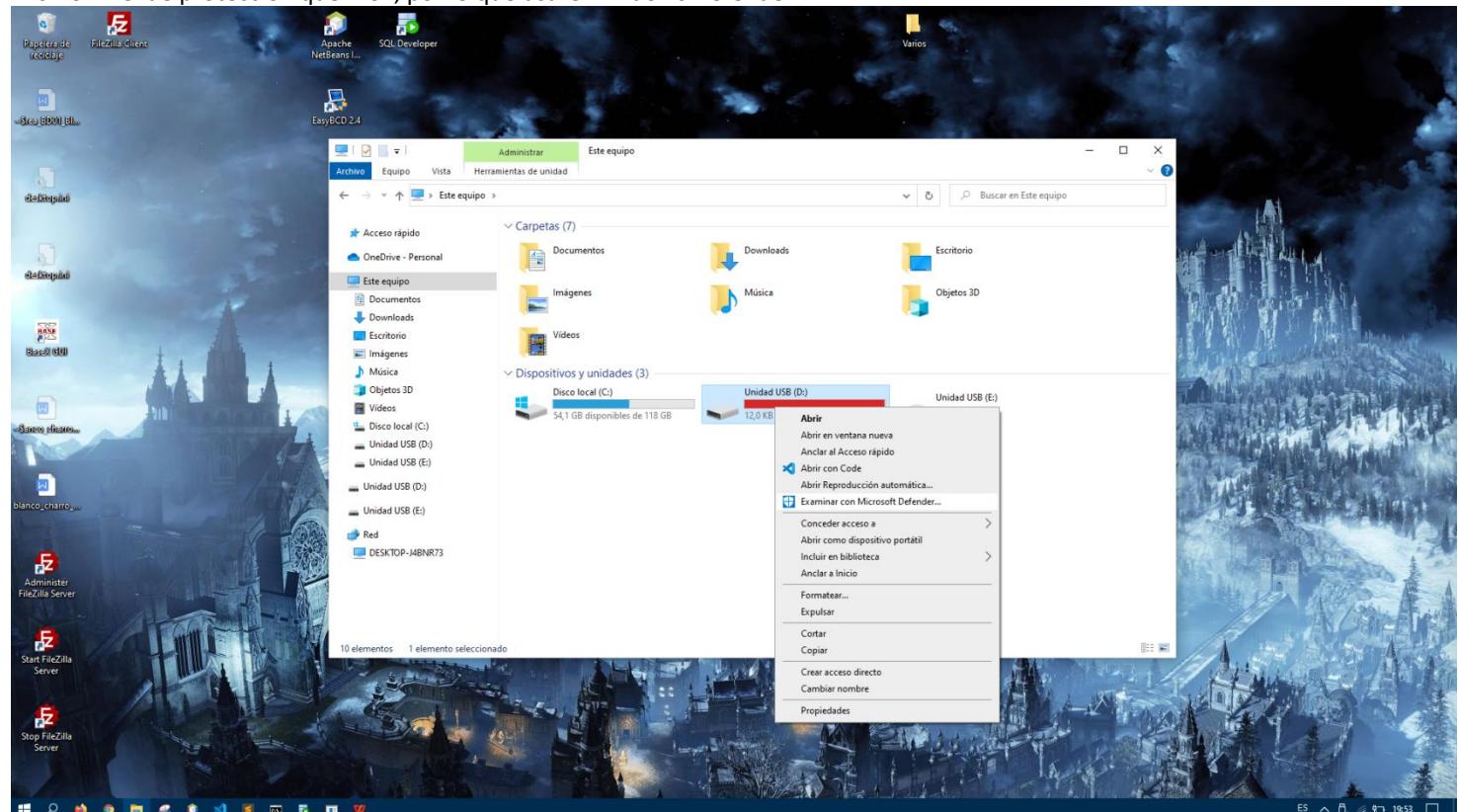
Tarea 7: Esta es una página de prueba para el servidor web realizado en la Tarea 7 de Sistemas Informáticos



Actividad 6

a. Realizar un análisis de una unidad extraible que tengas conectada al ordenador y una captura de pantalla del proceso y otra del resultado del análisis. ¿Se ha detectado alguna amenaza? En caso afirmativo, ¿de qué tipo? ¿qué acciones has tomado (eliminar, ignorar alerta, poner en cuarentena el archivo)? Razona tu respuesta.

Al intentar instalar Microsoft Security Essentials, Windows 10 me dice que ya tengo instalado Windows Defender que proporciona el mismo nivel de protección que MSE, por lo que usaré Windows Defender.



Captura del proceso de análisis del USB extraible.

A screenshot of the Windows Security app. On the left, a sidebar lists navigation options: Inicio, Protección antivirus y contra amenazas, Protección de cuentas, Firewall y protección de red, Control de aplicaciones y navegador, Seguridad del dispositivo, Rendimiento y estado del dispositivo, and Opciones de familia. The main area shows a progress bar for a 'Ejecutando examen completo...' (Running full scan...) with a time estimate of '00:00:00' and '1893 archivos examinados' (1893 files examined). Below the progress bar, there's a 'Cancelar' (Cancel) button. To the right, there's a sidebar with links: '¿Tienes alguna pregunta?' (Do you have any questions?), 'Obtener ayuda' (Get help), 'Ayuda a mejorar el servicio Seguridad de Windows' (Help improve Windows Security service), 'Envíanos tus comentarios' (Send us your comments), 'Cambiar la configuración de privacidad' (Change privacy settings), 'Permitir visualizar y cambiar la configuración de privacidad del dispositivo Windows 10' (Allow viewing and changing the privacy settings of the Windows 10 device), 'Configuración de privacidad' (Privacy settings), 'Panel de privacidad' (Privacy panel), and 'Declaración de privacidad' (Privacy statement). At the bottom, there's a 'Configuración' (Configuration) button and a taskbar with various icons.

Captura del análisis finalizado

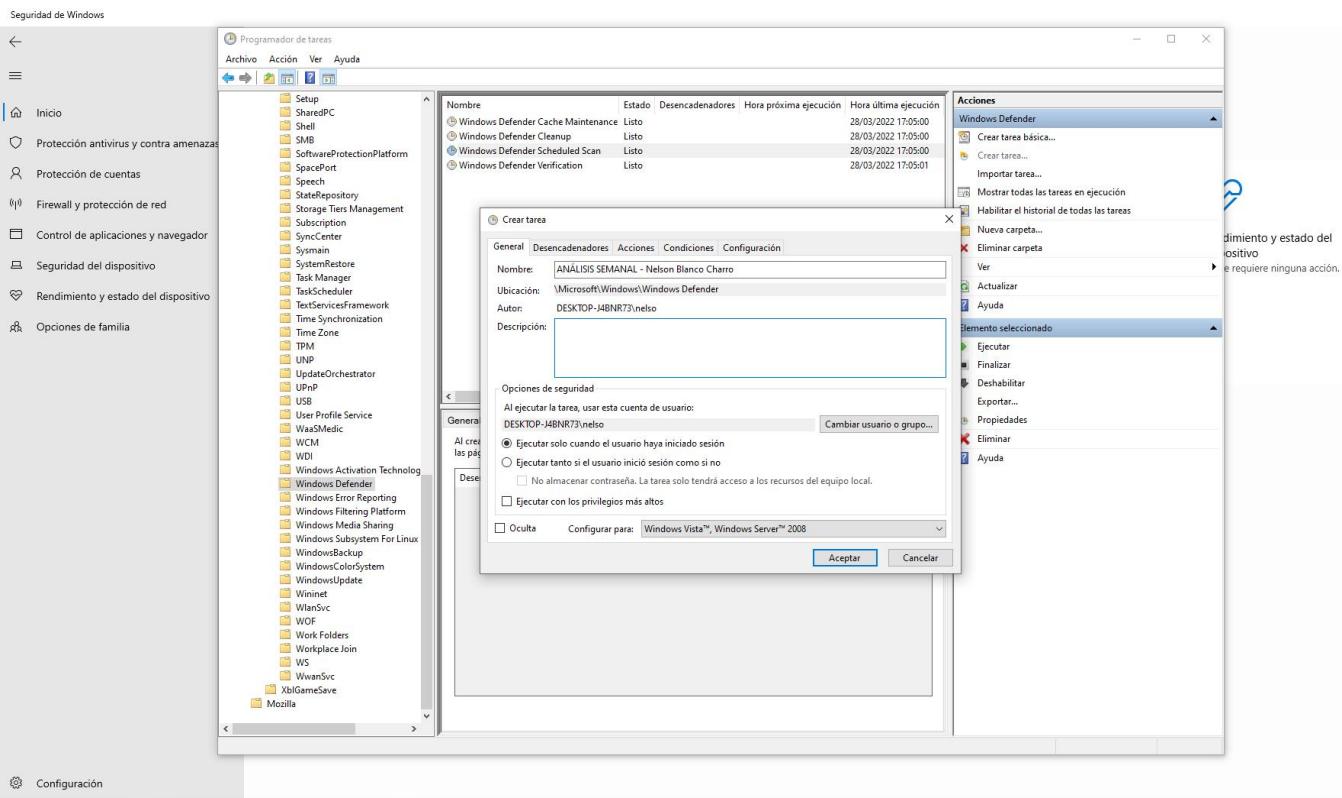
The screenshot shows the Windows Security app interface. On the left, a sidebar lists various security features: Inicio, Protección antivirus y contra amenazas, Protección de cuentas, Firewall y protección de red, Control de aplicaciones y navegador, Seguridad del dispositivo, Rendimiento y estado del dispositivo, and Opciones de familia. The main area displays a threat analysis report for a file named "PUABundler:Win32/uTorrent_BundleInstaller" from 19/03/2022 21:50 (Activado). The file is categorized as "Baja" (Low) risk. Below the file details, there are sections for "Amenazas permitidas" and "Historial de protección". A large button labeled "Iniciar acciones" is prominently displayed. To the right, there are links for "Ayuda a mejorar el servicio Seguridad de Windows", "Envíanos tus comentarios", "Cambiar la configuración de privacidad", "Configuración de privacidad", "Panel de privacidad", and "Declaración de privacidad". At the bottom, a "Examinar ahora" button is visible.

Se ha detectado una amenaza de riesgo bajo, la recomendación es poner el archivo en cuarentena pero el USB es un instalador de Ubuntu Server, por lo que confío en el creador y selecciono la opción “Permitir en dispositivo”.

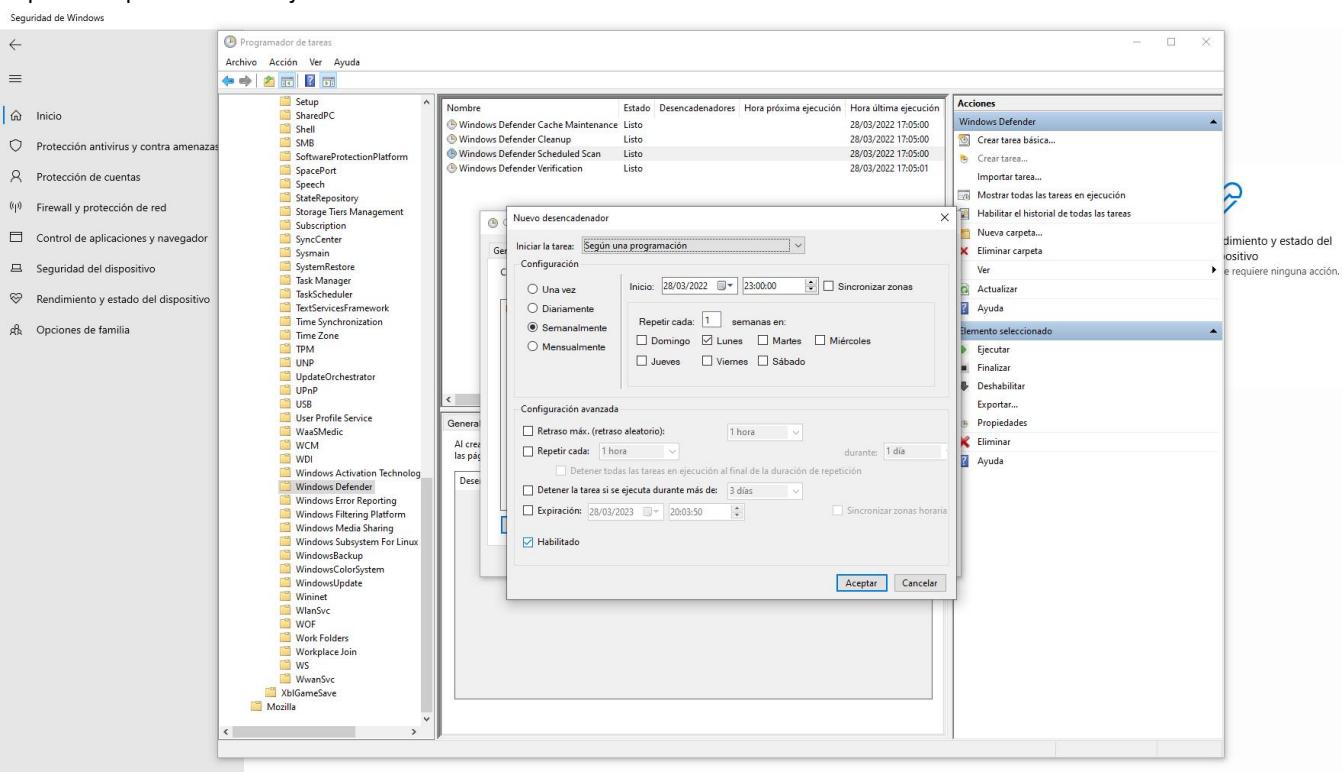
This screenshot shows the same Windows Security app interface as the previous one, but with a different selection in the "Opciones de acción:" dropdown. The "Permitir en dispositivo" option is now selected, while "Poner en cuarentena" and "Quitar" are unselected. The rest of the interface, including the sidebar, threat details, and other configuration links, remains identical to the first screenshot.

b. A continuación, configura un análisis programado para que se ejecute semanalmente a las 23:00 horas y que revise todos las unidades de disco y la memoria. Nombra la tarea como 'ANÁLISIS SEMANAL - <Tu Nombre y Apellidos>'. Realiza una captura de pantalla de la configuración de la programación.

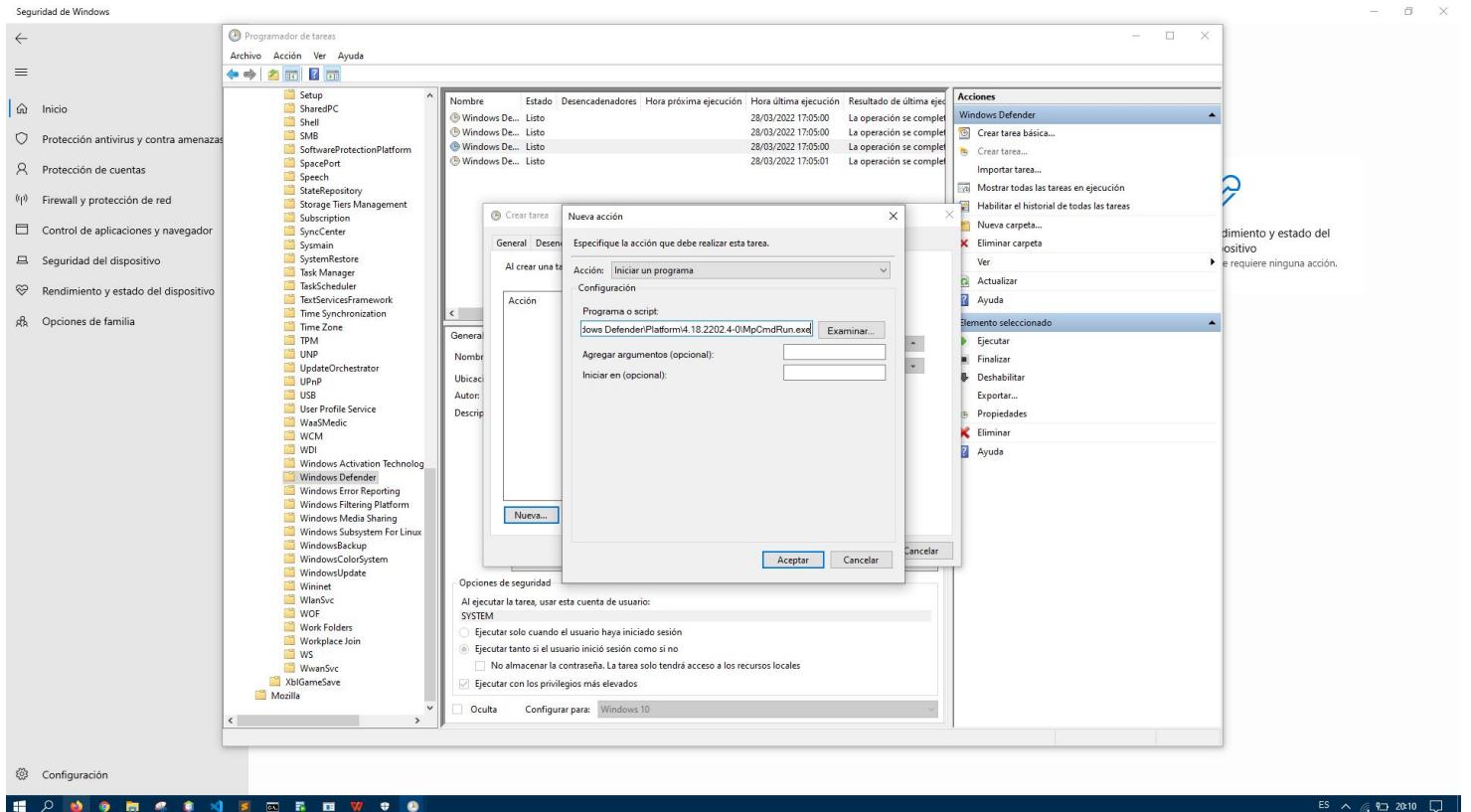
Captura de pantalla del nombre de la tarea de análisis



Captura de pantalla de la ejecución semanal a las 23:00



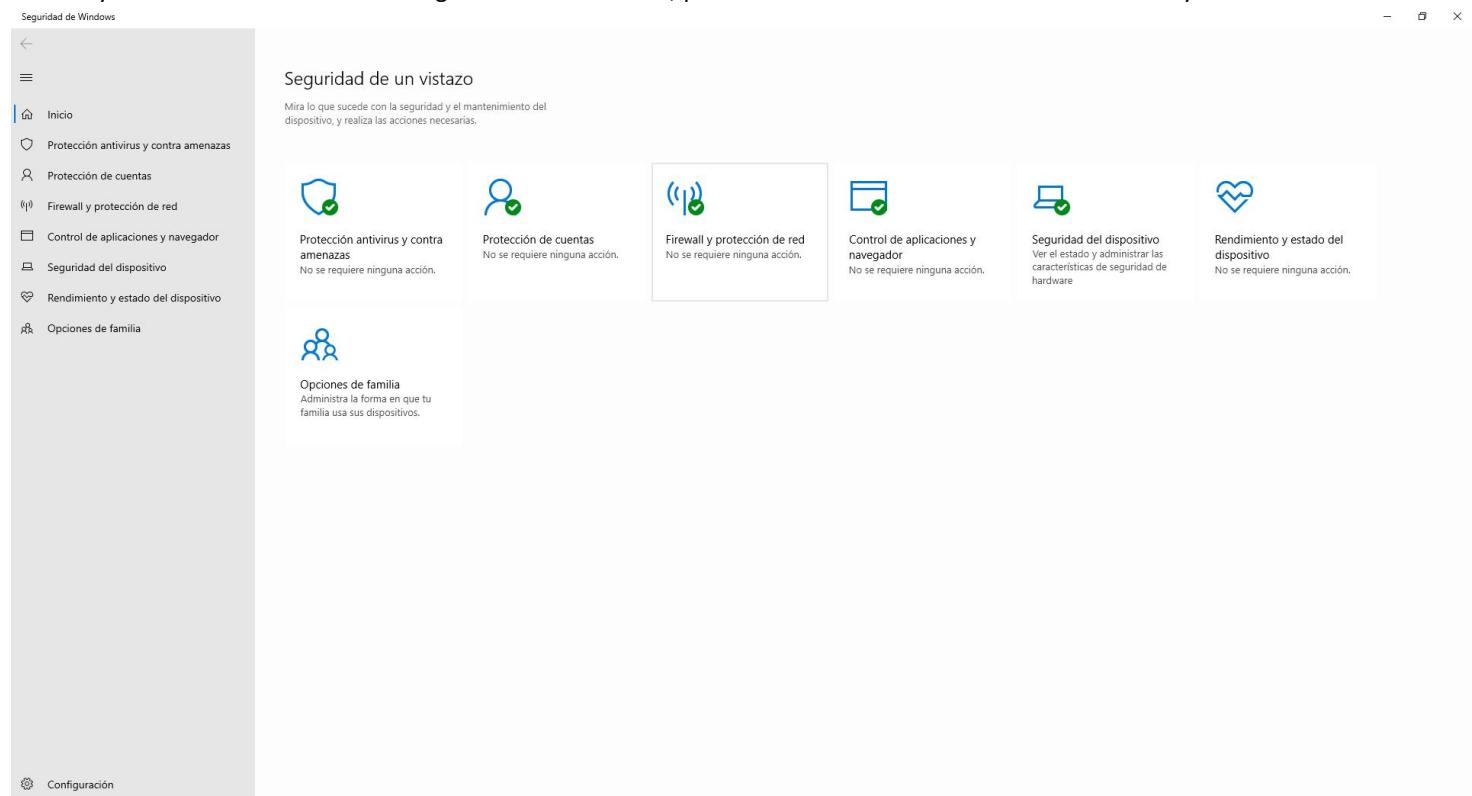
Acciones a realizar: revisar todos los archivos y carpetas mediante la acción de Windows Defender.



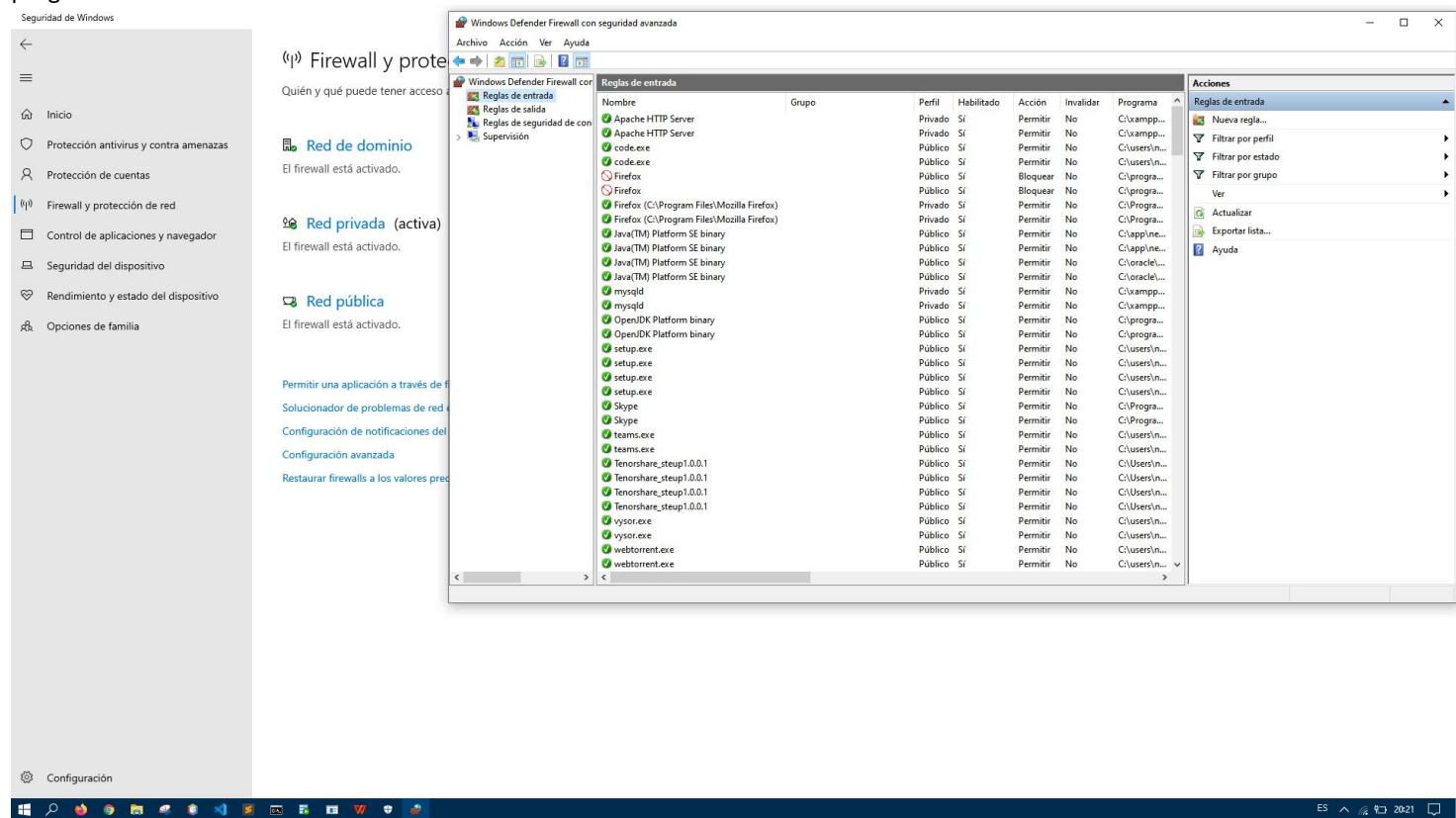
Actividad 7

Realiza un tutorial con capturas de pantalla y texto descriptivo donde se describa el proceso de instalación y configuración de un cortafuegos concreto paso a paso.

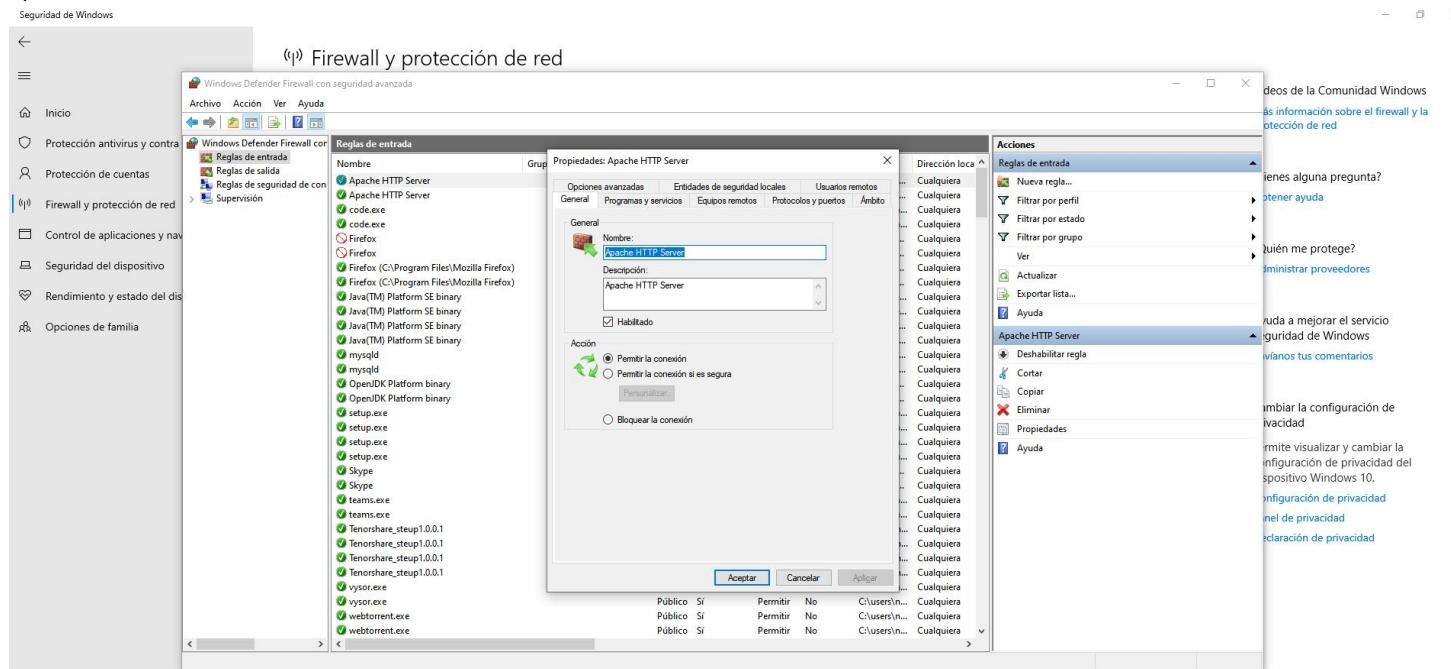
En el caso de Windows 10, por defecto trae un cortafuegos o firewall al que se puede acceder a su configuración si hacemos clic en "Inicio" y a continuación tecleamos "Seguridad de Windows", por lo cual no es necesario instalar nada a mayores.



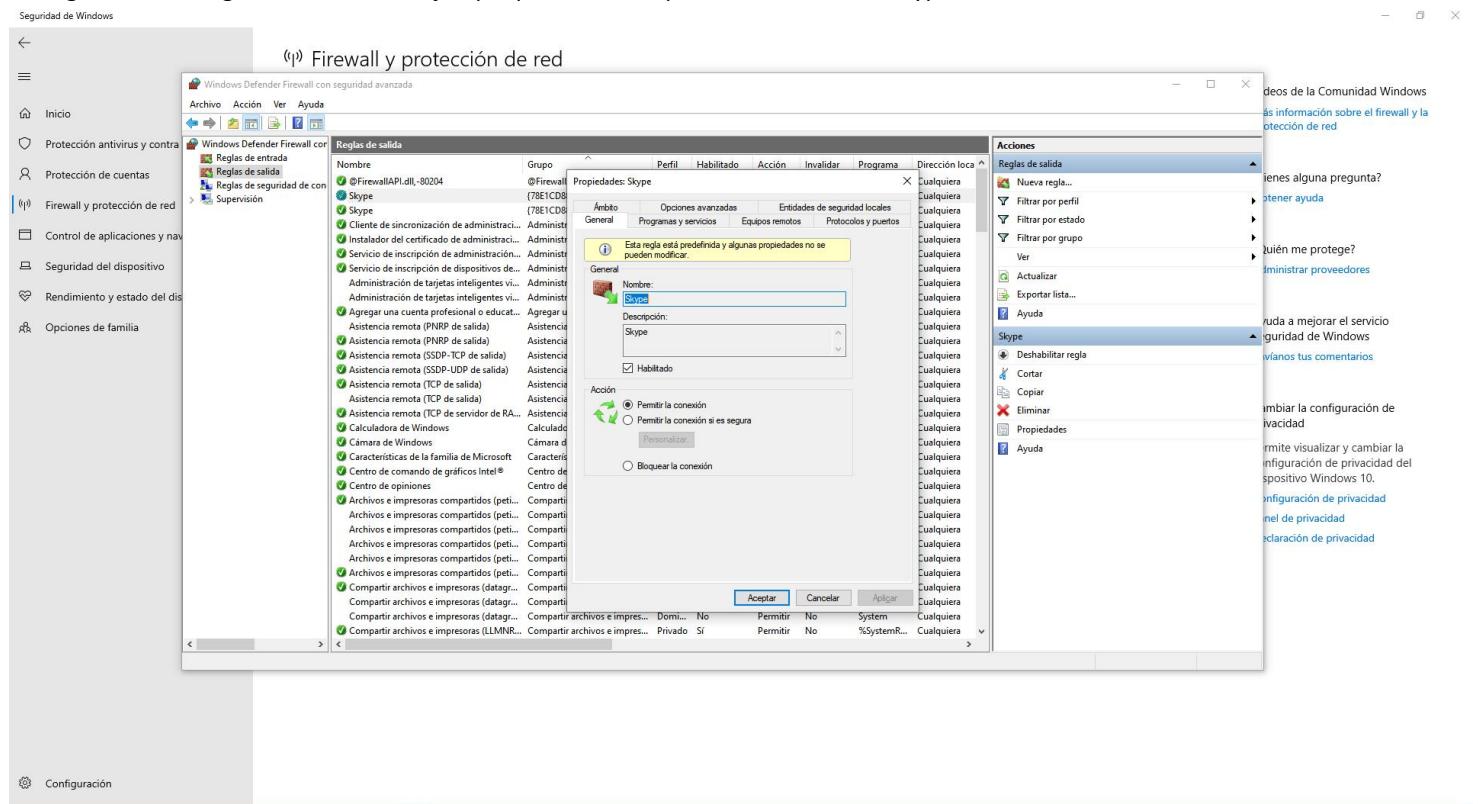
Para ver las opciones del cortafuegos de Windows, hacemos clic en la opción "Configuración avanzada", nos aparecerá una ventana con un resumen de las configuraciones, y seleccionando en el panel lateral izquierdo podemos activar o bloquear los distintos programas o llamadas.



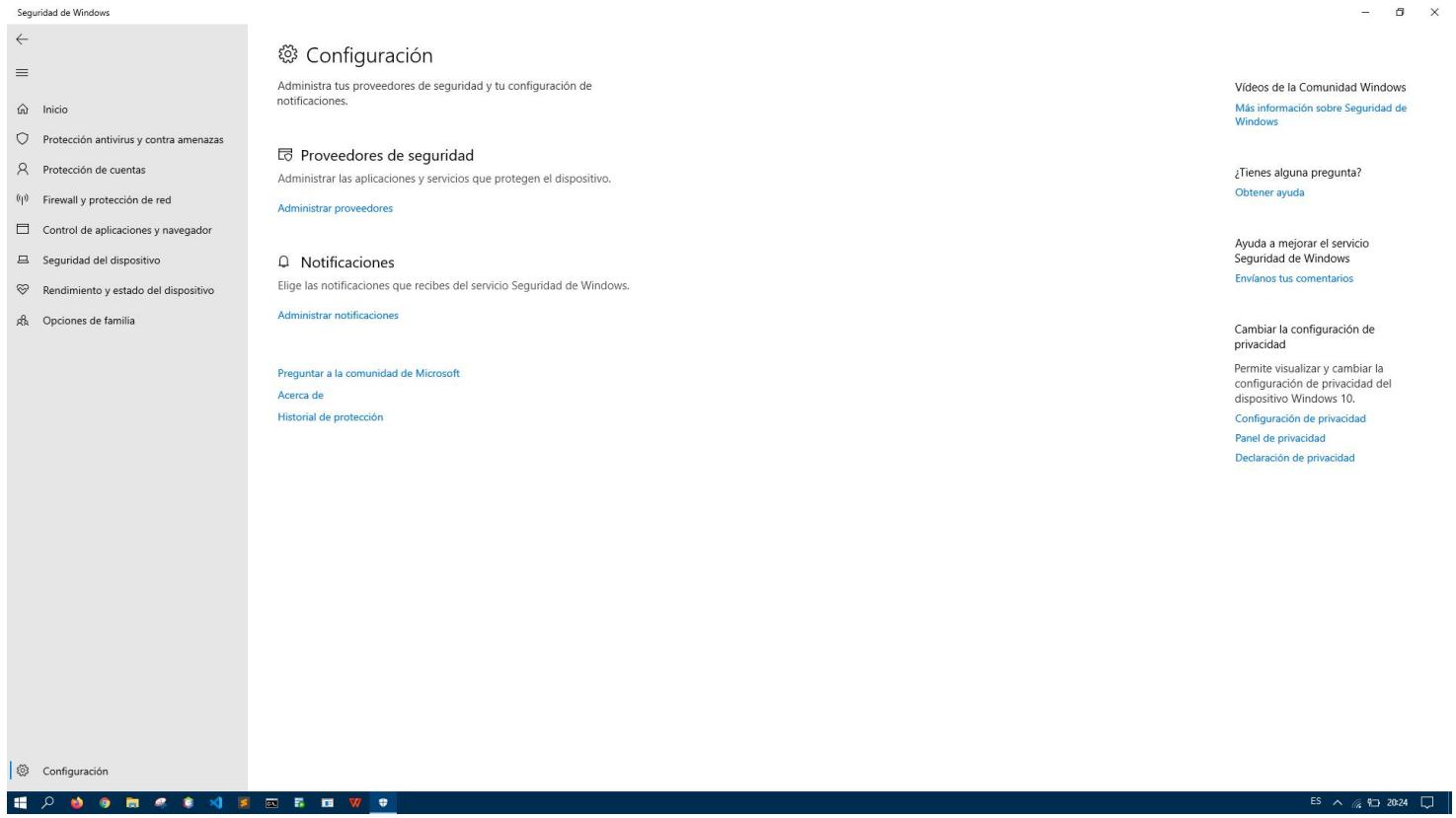
Configuración de reglas de entrada. Por ejemplo podemos no permitir la conexión a ApacheHTTPServer que hemos instalado en el apartado 5b.



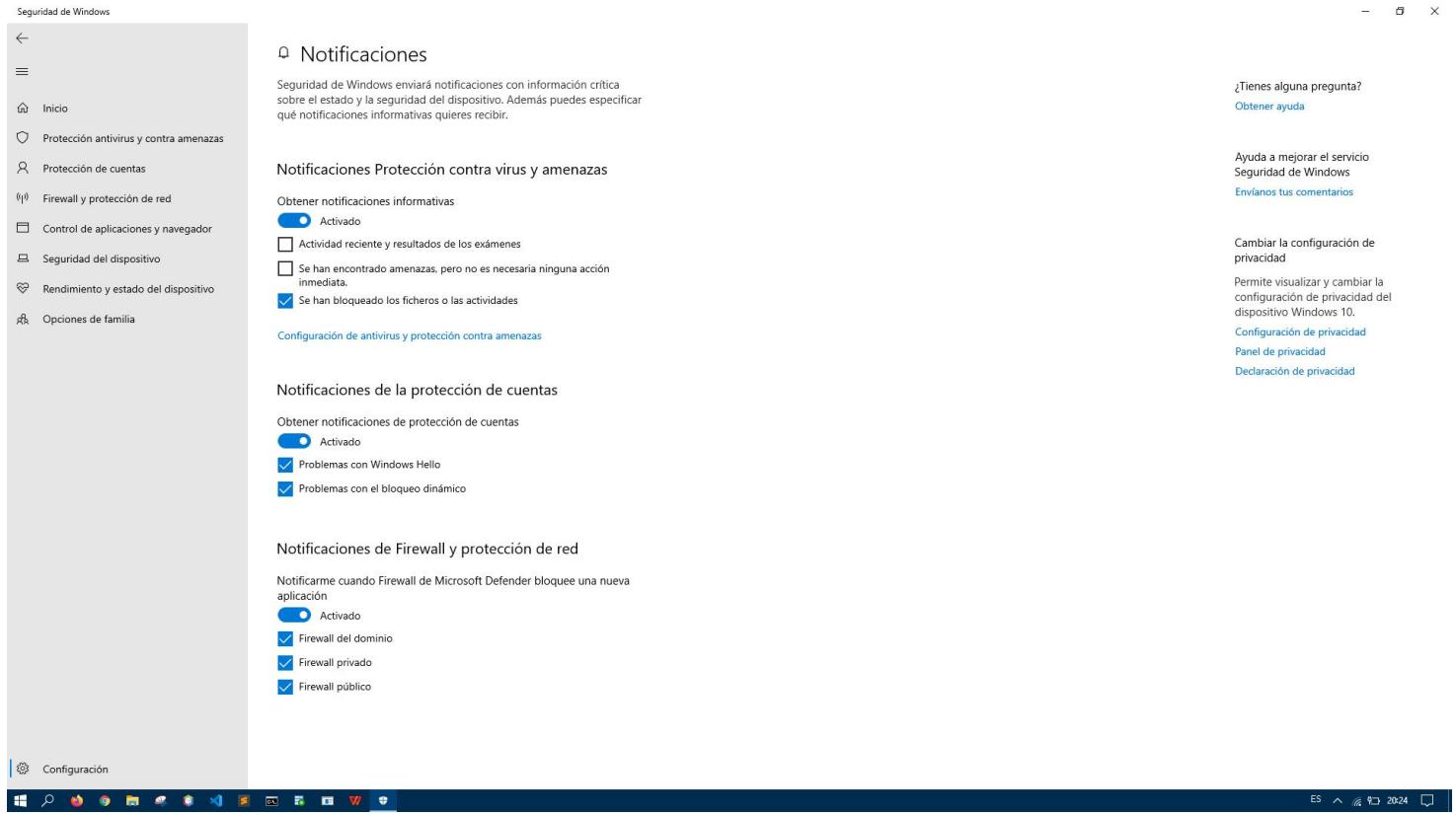
Configuración de reglas de salida. Por ejemplo podemos bloquear la conexión de Skype.



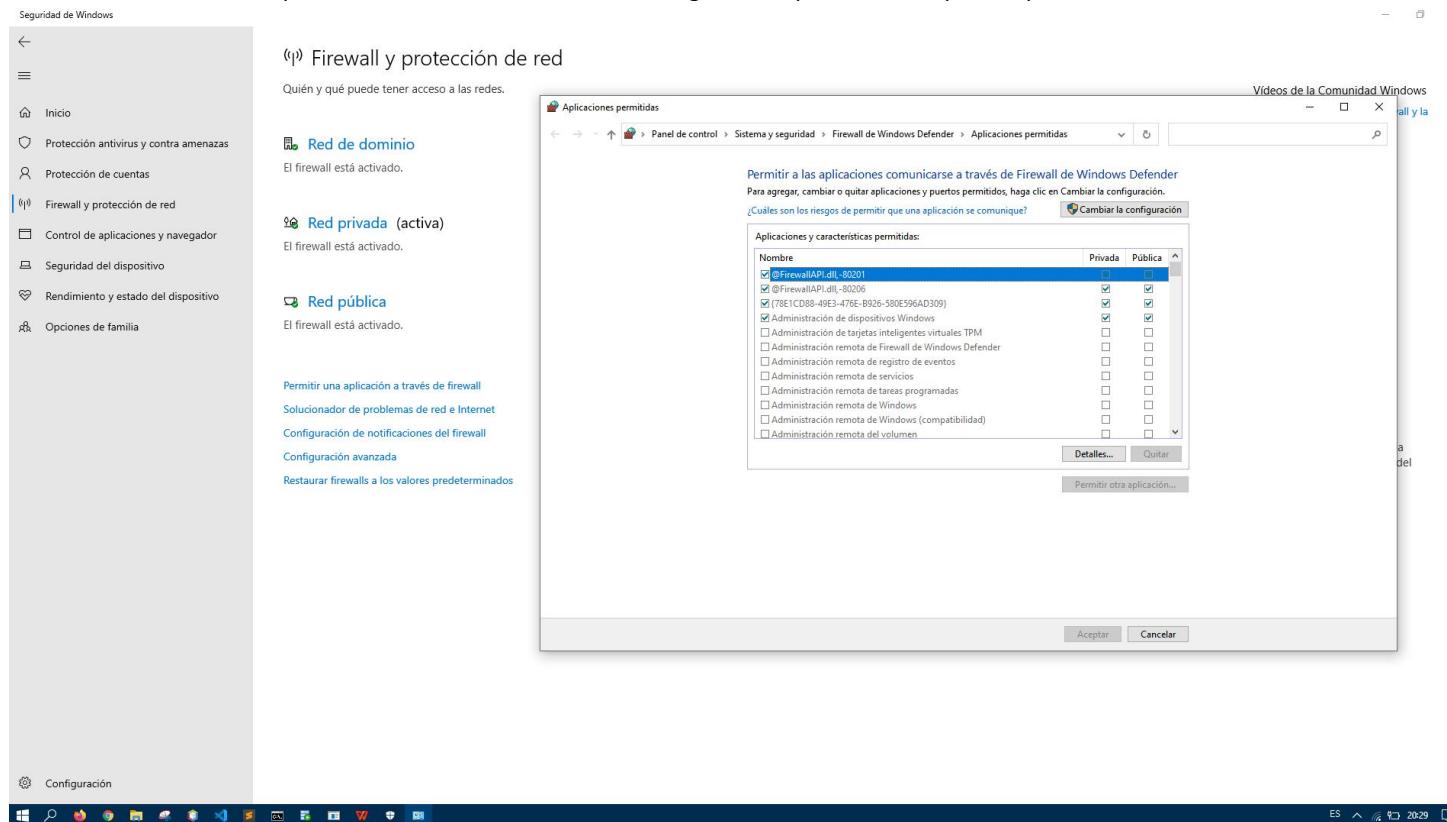
Para configurar las alertas, en la ventana principal encima de la configuración avanzada tenemos que hacer clic en “Configuración de notificaciones de firewall”, a continuación nos aparecerá un menú en el que debemos seleccionar “Administrar notificaciones”.



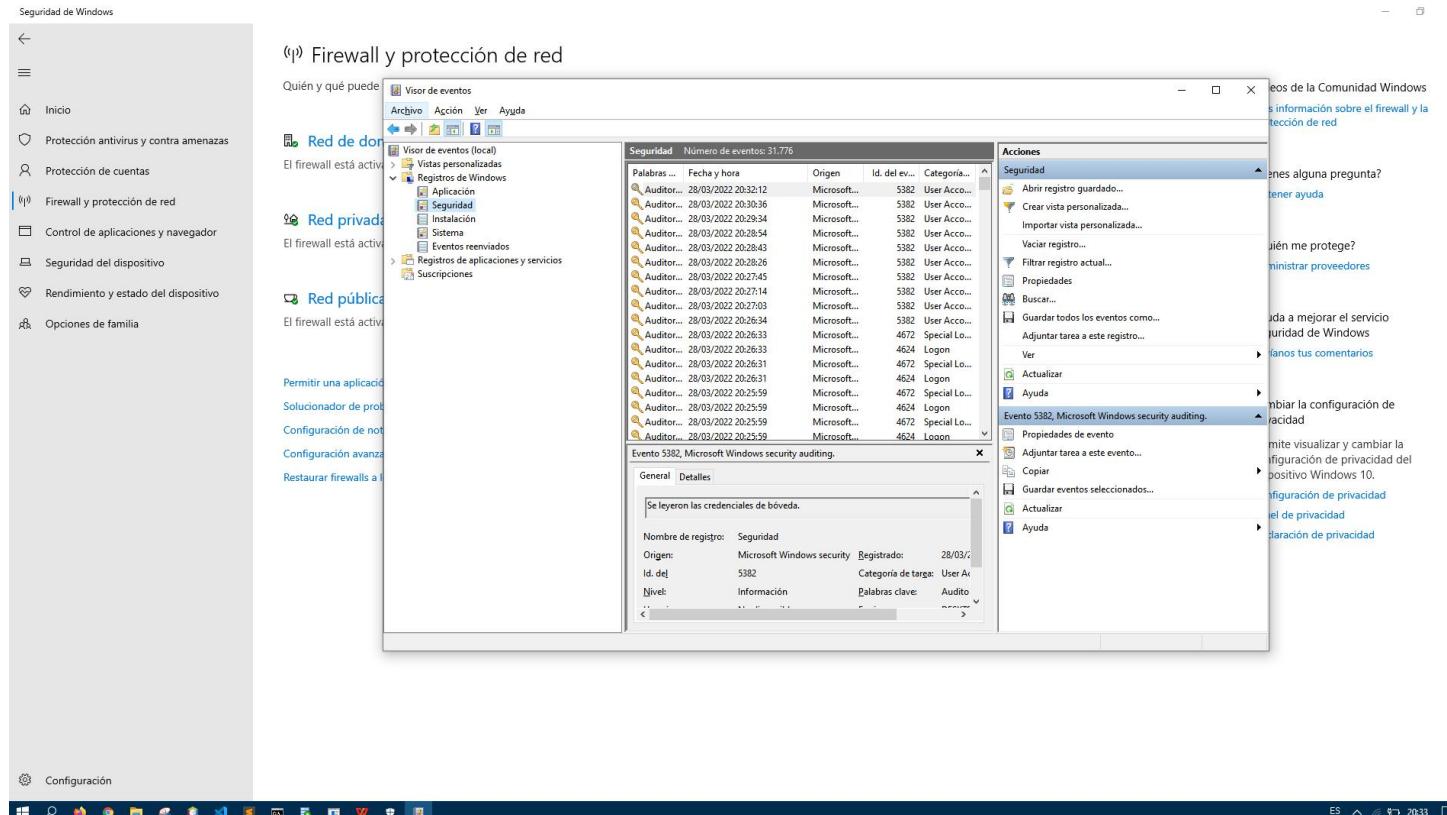
Nos aparecerá otro menú en el que podemos modificar la configuración de notificaciones del firewall.



Para permitir o bloquear que los programas puedan acceder a internet, debemos seleccionar la opción “Permitir una aplicación a través de firewall”. Para que de este modo, cambiando la configuración, podamos bloquear o permitir su acceso.



Para ver los eventos registrados por el cortafuegos de Windows 10, debemos hacer clic en Inicio y buscar el programa “Visor de eventos”, a continuación abrimos el desplegable llamado “Registros de Windows” y seleccionamos “Seguridad”. De éste modo podremos ver los eventos admitidos y denegados por el firewall de Windows.



Actividad 8

Si tienes acceso a un punto de acceso o router inalámbrico localiza dónde se encuentran las opciones de seguridad vistas en la unidad y realiza capturas de pantalla de las opciones.

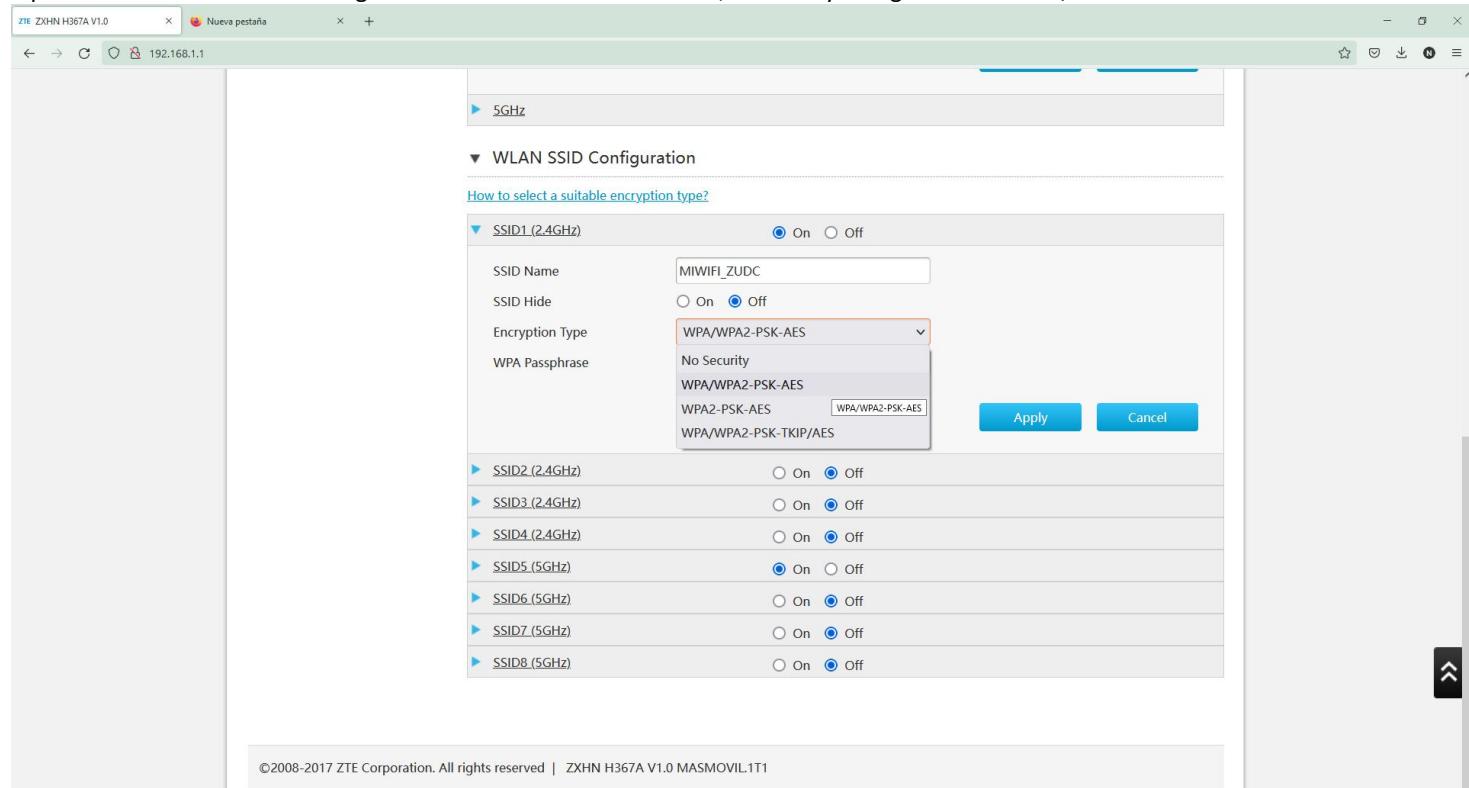
Clave del router. Es la clave que nos permite acceder a la configuración propia del Router, con la que configurar las distintas redes Wi-Fi o Ethernet, el cifrado MAC o la seguridad de la red.

The screenshot shows the ZTE ZXHN H367A V1.0 Management & Diagnosis interface. On the left, there's a sidebar with links for Status, Account Management (which is selected), Idle Timeout, System Management, and Network Diagnosis. The main content area is titled "Page Information" and describes the function of web account parameter(s) configuration. A sub-section titled "User Account Management" is expanded, showing fields for Username (1234), Old Password, New Password, and Confirmed Password. At the bottom right of this section are "Apply" and "Cancel" buttons. The footer of the page includes the copyright notice "©2008-2017 ZTE Corporation. All rights reserved | ZXHN H367A V1.0 MASMOVIL.1T1".

Clave de red. Es la clave que nos permite conectarnos al router para tener acceso a internet, no permite configurar el router, solo da acceso a la red.

The screenshot shows the ZTE ZXHN H367A V1.0 Management & Diagnosis interface. The sidebar shows the "Account Management" link is selected. The main content area is titled "WLAN SSID Configuration" and provides instructions on how to select a suitable encryption type. It lists several SSID configurations: SSID1 (2.4GHz) is active (On) with name MIWIFI_ZUDC, hide off, encryption type WPA/WPA2-PSK-AES, and passphrase Tarea7Nelson. Other SSIDs listed are SSID2 (2.4GHz), SSID3 (2.4GHz), SSID4 (2.4GHz), SSID5 (5GHz), SSID6 (5GHz), SSID7 (5GHz), and SSID8 (5GHz), all currently set to Off. At the bottom right are "Apply" and "Cancel" buttons. The footer includes the copyright notice "©2008-2017 ZTE Corporation. All rights reserved | ZXHN H367A V1.0 MASMOVIL.1T1".

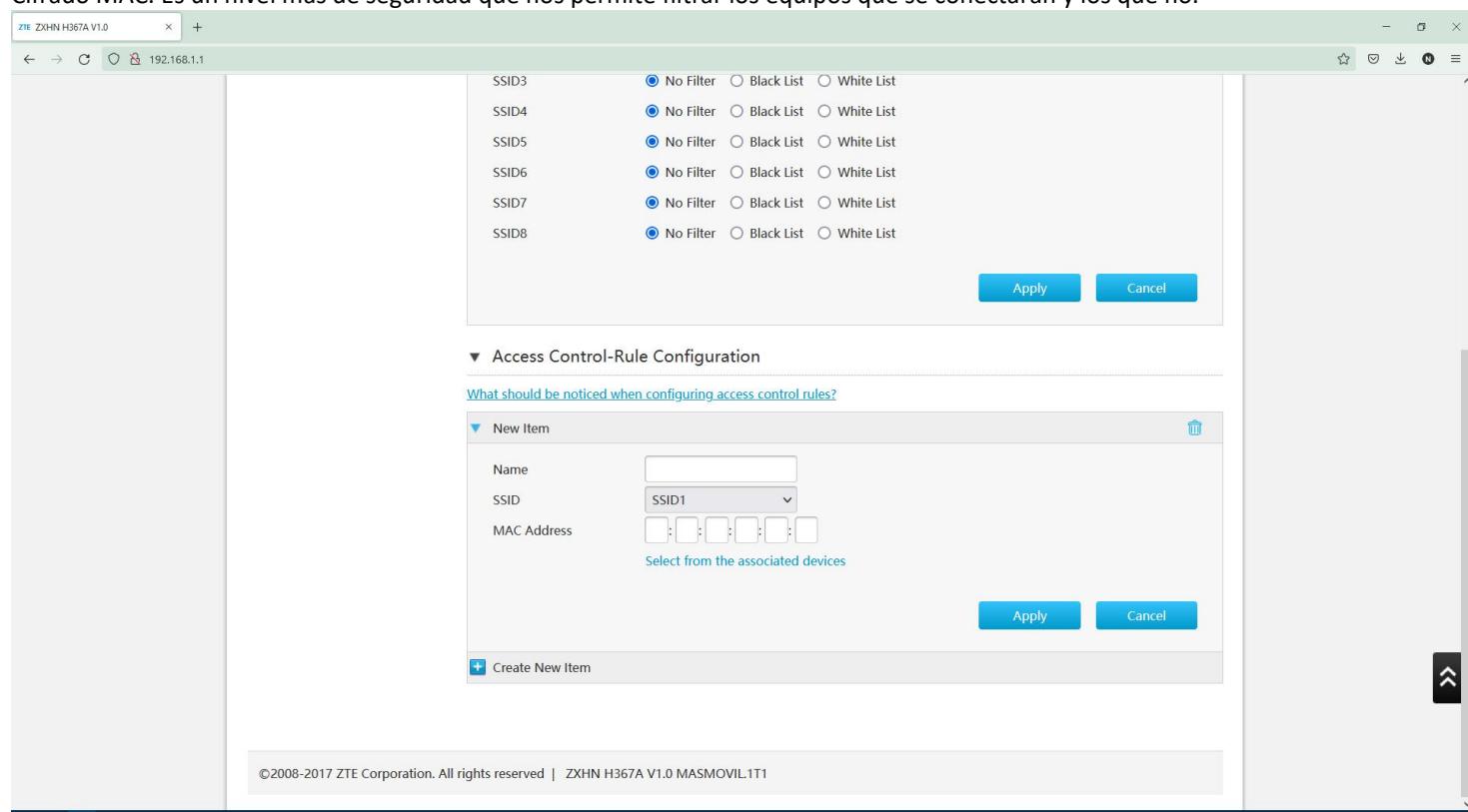
Tipo de cifrado. Es el nivel de seguridad de la contraseña de Wi-Fi, el de mayor seguridad es WPA/WPA2-PSK-AES



The screenshot shows the 'WLAN SSID Configuration' section. A dropdown menu for 'Encryption Type' under 'SSID1 (2.4GHz)' is open, displaying options: 'No Security', 'WPA/WPA2-PSK-AES', 'WPA2-PSK-AES', and 'WPA/WPA2-PSK-TKIP/AES'. The 'WPA/WPA2-PSK-AES' option is selected. Other SSIDs listed include SSID2 (2.4GHz), SSID3 (2.4GHz), SSID4 (2.4GHz), SSID5 (5GHz), SSID6 (5GHz), SSID7 (5GHz), and SSID8 (5GHz). The 'Apply' and 'Cancel' buttons are visible at the bottom right.

©2008-2017 ZTE Corporation. All rights reserved | ZXHN H367A V1.0 MASMOVIL.1T1

Cifrado MAC. Es un nivel más de seguridad que nos permite filtrar los equipos que se conectarán y los que no.



The screenshot shows the 'Access Control-Rule Configuration' section. It lists eight SSIDs (SSID3 to SSID8) with their respective MAC address filtering options: 'No Filter', 'Black List', or 'White List'. The 'Black List' option is selected for all SSIDs. The 'Apply' and 'Cancel' buttons are visible at the bottom right.

▼ Access Control-Rule Configuration

What should be noticed when configuring access control rules?

New Item

Name	SSID	MAC Address
	SSID1	[Select from the associated devices]

Apply Cancel

Create New Item

©2008-2017 ZTE Corporation. All rights reserved | ZXHN H367A V1.0 MASMOVIL.1T1