



CFGs ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

IMPLANTACIÓN DE SISTEMAS OPERATIVOS



Ud5.- Administración de la red y cortafuegos

Índice

- 1.- Introducción.
- 2.- Configuración de la red.
- 3.- Cortafuegos.



1.- Introducción

Hoy día es muy difícil pensar en equipos aislados. En la mayoría de las ocasiones están conectados entre sí y con acceso a Internet.

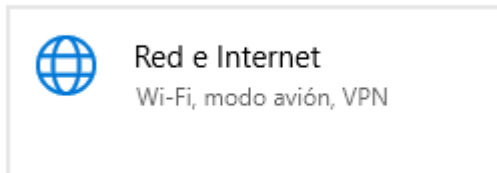
En un entorno como éste, es fundamental que el **SO** facilite la configuración de la red.





2.-Configuración de la red.

Configuración de Windows



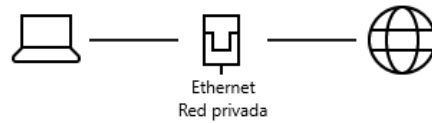


2.-Configuración de la red.



Estado

Estado de red



Estás conectado a Internet.

Si tienes un plan de datos limitado, puedes convertir esta red en una conexión de uso medido o cambiar otras propiedades.

[Cambiar las propiedades de conexión](#)

[Mostrar redes disponibles](#)

Cambiar la configuración de red



Cambiar opciones del adaptador

Visualiza los adaptadores de red y cambia la configuración de conexión.



Opciones de uso compartido

Decide qué quieres compartir en las redes a las que te conectas.



Solucionador de problemas de red

Diagnosticar y solucionar problemas de red.

[Ver las propiedades de red](#)

[Firewall de Windows](#)

[Centro de redes y recursos compartidos](#)

[Restablecimiento de red](#)



2.-Configuración de la red.

Ethernet

← Configuración

Red

Perfil de red

☐ Público

El equipo se establece como oculto para otros dispositivos de la red y no se puede usar para compartir archivos e impresoras.

☒ Privada

Para una red de confianza, como la de tu hogar o el trabajo. El equipo se establece como reconocible y se puede usar para compartir archivos e impresoras si lo configuras.



2.-Configuración de la red.

VPN

VPN



Agregar una conexión VPN

Opciones avanzadas

Permitir VPN a través de redes de uso medido



Activado

Permitir VPN en itinerancia



Activado



2.-Configuración de la red.

¿Qué es un VPN?

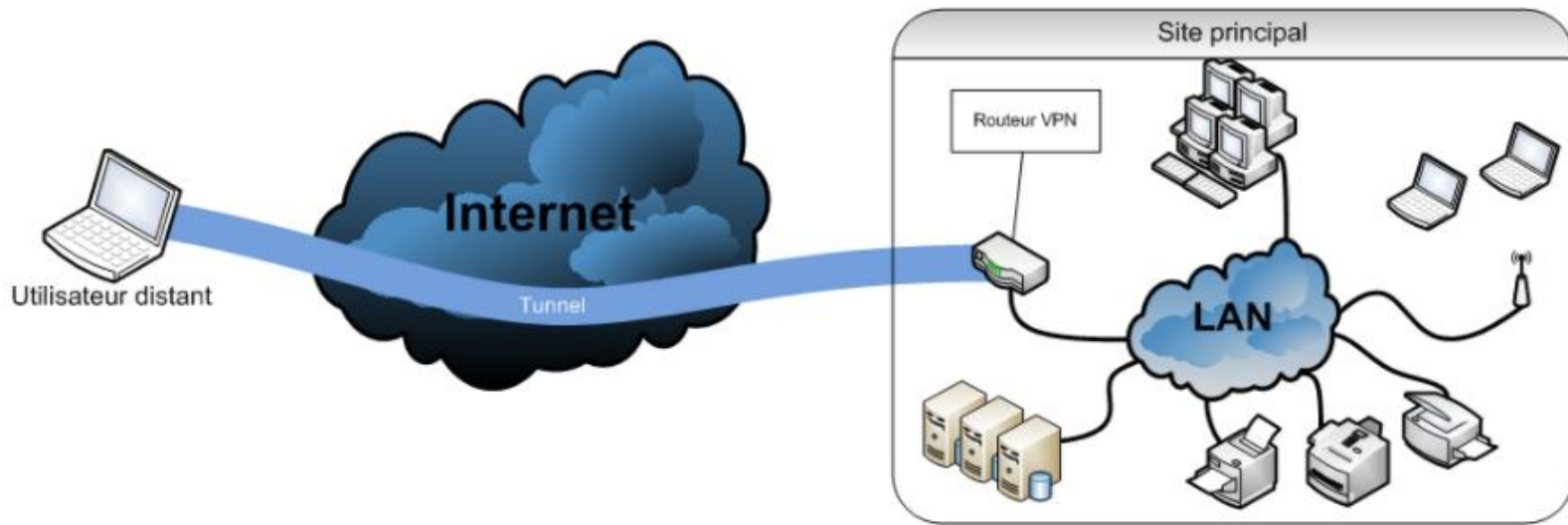
Un **VPN (Virtual Private Network)** te permite crear una conexión segura a otra red a través del Internet. Cuando conectas cualquier dispositivo a un VPN, este actúa como si estuviese en la misma red que la que tiene el VPN y todo el tráfico de datos se envía de forma segura a través del VPN.

Esto quiere decir que puedes usar el Internet como si estuvieses presente en la región que tiene la red del VPN, lo que te viene muy bien si necesitas acceso a contenido que está bloqueado por región. Por ejemplo, si quieres entrar a mirar el catálogo de un servicio exclusivo de un país concreto, con un VPN puedes hacerlo, porque una vez que entras con la conexión enmascarada, dicho servicio sólo verá que te estás conectando desde ese país, aunque en realidad no sea así.

Además el VPN es una red privada y virtual como su nombre lo dice, por lo tanto **todo el tráfico que pasa por esa red está asegurado y protegido** de ojos no deseados. Esto puede ser de mucha utilidad cuando nos conectamos a una red Wi-Fi pública.



2.-Configuración de la red.





2.-Configuración de la red.

¿Cuáles son los usos de un VPN?

- **Acceso a una red de trabajo mientras se está de viaje.** Los VPNs se usan con frecuencia para aquellos profesionales que viajan y necesitan entrar en su red de trabajo mientras están lejos. Usar este método permite que los recursos se mantengan seguros porque están en la nube.
- **Acceso a una red del hogar mientras se está de viaje.** También se puede usar para entrar al ordenador que hemos dejado en casa, como si estuviésemos usando una LAN (*Local Network Area*).
- **Esconde los datos de navegación.** Por ejemplo, si estás usando un Wi-Fi público, de esos que están disponibles sin contraseña en restaurantes y centros comerciales, todo lo que visites que no tenga conexión **HTTPS** estará visible para cualquiera que sepa dónde mirar. En cambio si tienes un VPN, lo único que podrán ver es la conexión al VPN; todo lo demás **será anónimo**.
- **Entrar en sitios con bloqueo geográfico.** Usualmente los problemas de bloqueo de región suelen pedir que estés en Estados Unidos. Esto sucede con Hulu, Pandora o el catálogo de Netflix que es más grande y completo en este país. A veces pasa también en ciertos vídeos de YouTube. Para evitar estas restricciones, sólo hay que usar un VPN que tenga localización de USA.
- **Evitar la censura en Internet.** Para aquellos gobiernos que deciden censurar ciertos sitios web, un VPN funciona muy bien para acceder a ellos sin problemas.

Vídeo: VPN



2.-Configuración de la red.

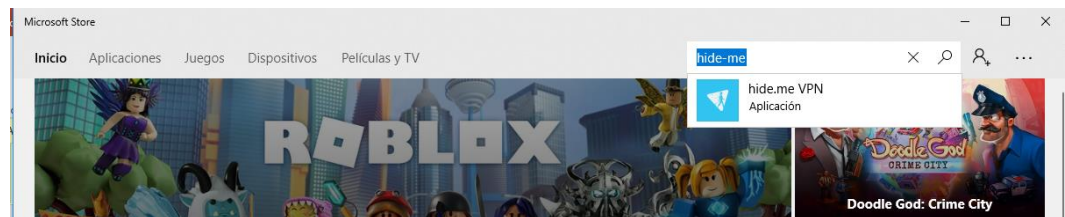
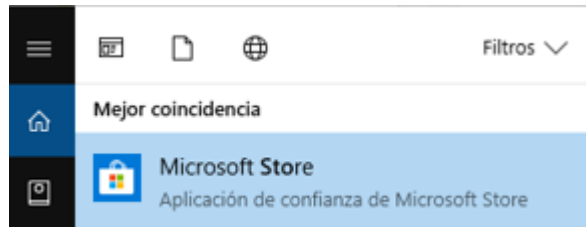
Ejercicio:

1.- Descargarte una aplicación para establecer VPN e instálala.

Hide-me → Es una aplicación que nos permite establecer una vpn

Nos la podemos descargar de Microsoft Store o de su página oficial.

Recomendamos su [página oficial](#).





2.-Configuración de la red.

Ejercicio:

2.- Nos registramos y nos logueamos.



hide.me VPN

HIDE me

mftienda

.....

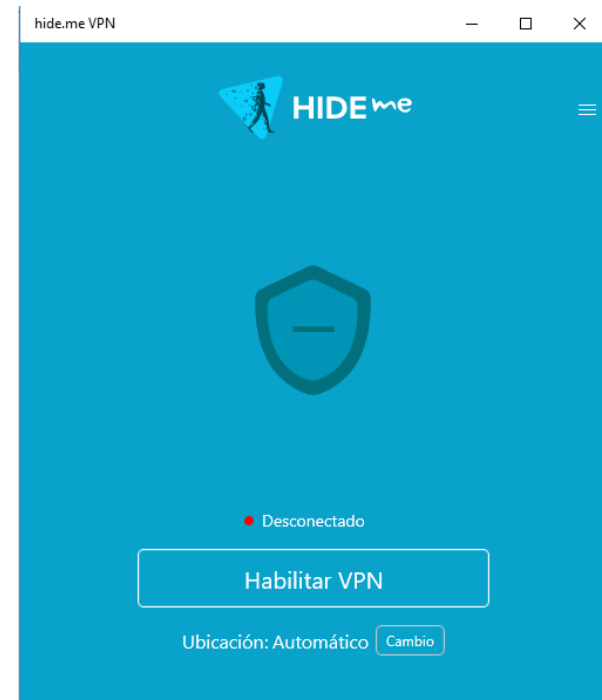
Iniciar sesión

[¿Olvidó su contraseña?](#)

o

Crear cuenta

3.- Habilitar VPN.



hide.me VPN

HIDE me

Desconectado

Habilitar VPN

Ubicación: Automático [Cambio](#)

4.- Observa la IP pública antes y después de utilizar el servicio.



2.-Configuración de la red.



Uso de datos

Uso de datos

Información general



Ethernet

6.55 GB

De los últimos 30 días

[Ver uso por aplicación](#)

Mostrar configuración para



Ethernet



Límite de datos

Windows puede ayudarte a no superar el límite de datos. Esto no cambiará el plan de datos.

[Establecer límite](#)

Datos en segundo plano

Restringe los datos en segundo plano para ayudar a reducir el uso de datos en Ethernet.

Limitar las acciones que las aplicaciones de Store y las características de Windows pueden hacer en segundo plano

☐ Siempre☒ Nunca

Ejercicio: Observa qué aplicaciones consumen más.



2.-Configuración de la red.

Proxy

Configuración automática del proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Detectar la configuración automáticamente

☒ Activado

Usar script de configuración

☐ Desactivado

Dirección de script

Guardar

Configuración manual del proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Usar servidor proxy

☐ Desactivado

Dirección

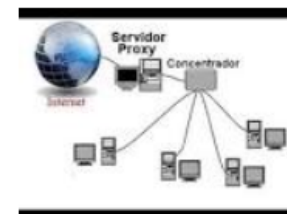
Puerto

Usar el servidor proxy excepto para direcciones que empiecen con las siguientes entradas. Usa el punto y coma (;) para separar las entradas.

☐ No usar el servidor proxy para direcciones locales (intranet)

Guardar

Servidor proxy



Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor. [Wikipedia](#)



2.-Configuración de la red.

Diagnóstico

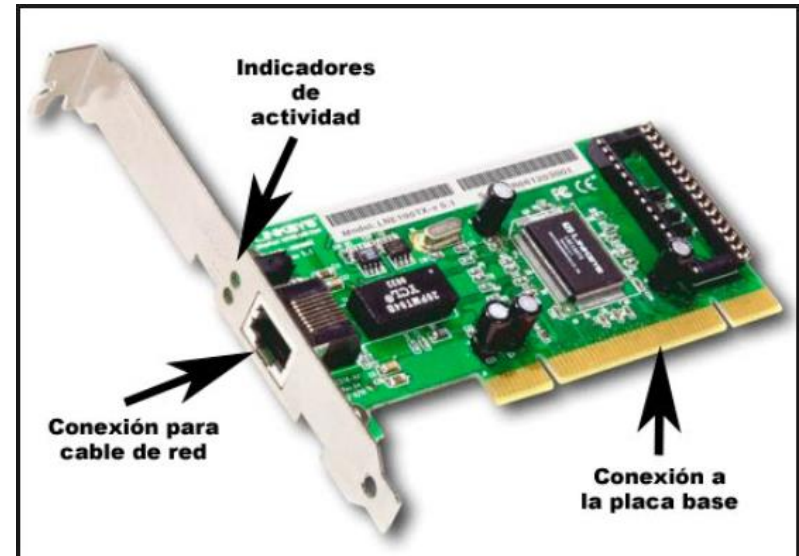
1.- Los leds de la tarjeta de red están apagados.

Diagnóstico:

Solución:



– Puerto 10/100/1000Mbps RJ45



La tarjeta de red posee dos luces indicadoras (LED):

- La luz verde corresponde a la alimentación eléctrica;
- La luz naranja (10 Mb/s) o roja (100 Mb/s) indica actividad en la red (envío o recepción de datos).



2.-Configuración de la red.

Diagnóstico

2.- Hace ping a 8.8.8.8, pero no a Google.es

Diagnóstico:

Solución.

3.-La luz verde está encendida, pero no hace ping a la puerta de enlace.

Diagnóstico:

Solución.



2.-Configuración de la red.

Diagnóstico

4.- Tengo instalado una tarjeta que soporta 1Gbps, pero mi conexión con mi router no pasa de 100Mbps.

Diagnóstico:

Solución.

Aplicaciones y características

Opciones de energía

Visor de eventos

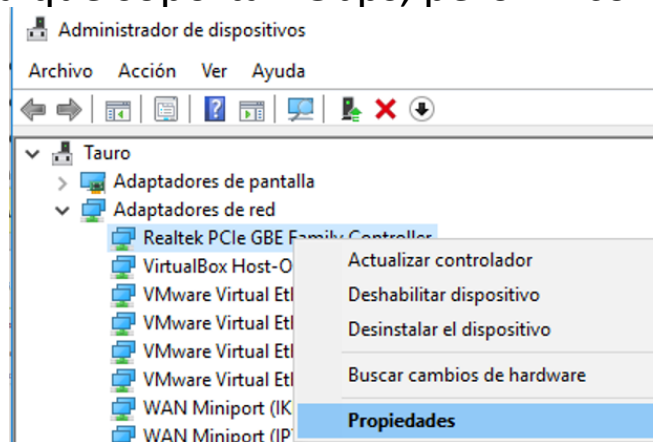
Sistema

Administrador de dispositivos

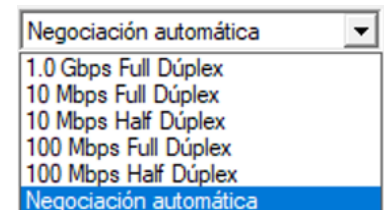
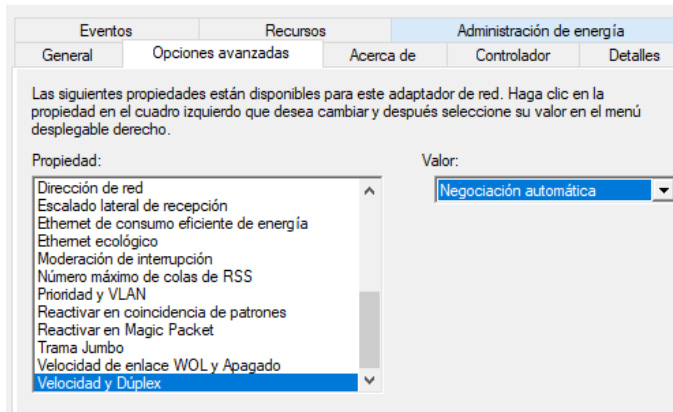
Conexiones de red

Administración de discos

Administración de equipos



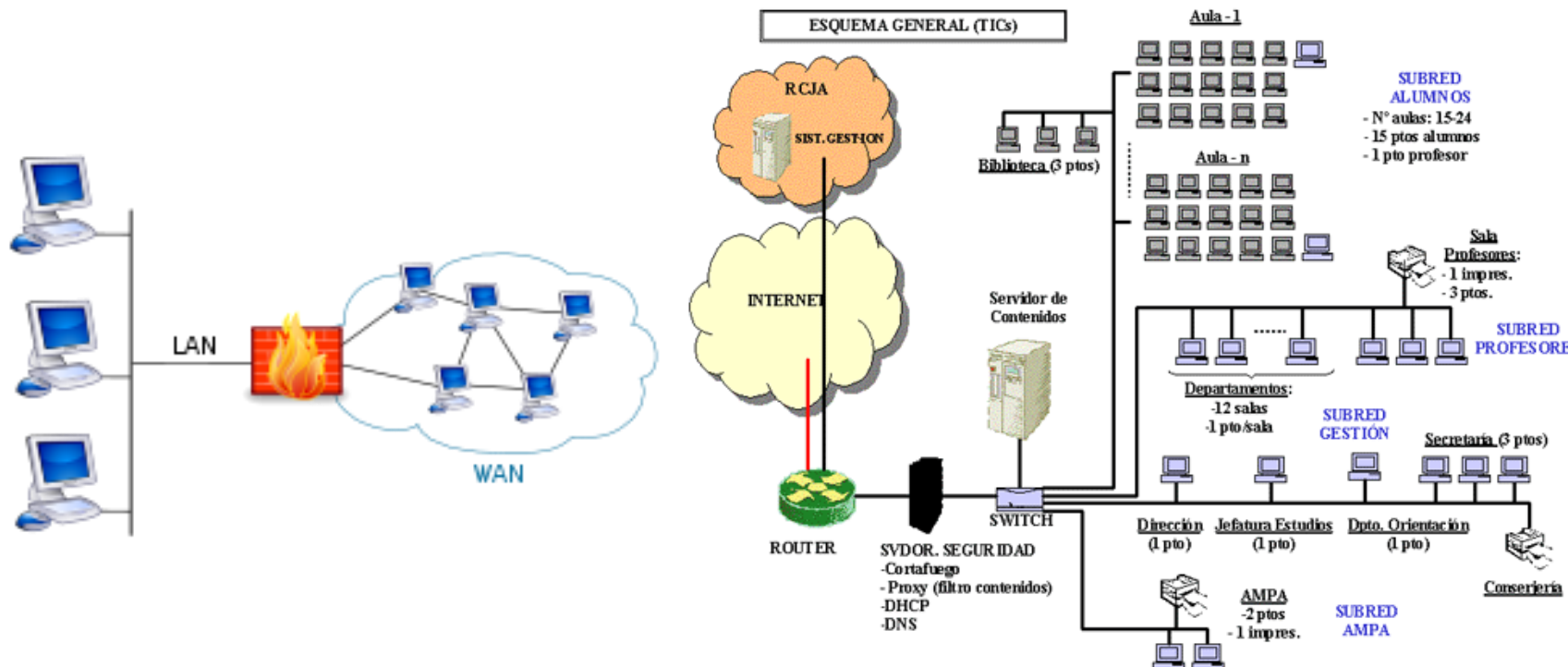
Propiedades: Realtek PCIe GBE Family Controller





3.-Cortafuegos.

Un cortafuegos (*firewall* en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.





3.-Cortafuegos.

Un Servidor Proxy es un dispositivo que:

actúa como intermediario para las solicitudes de los clientes que buscan recursos de otros servidores.

Un Firewall es un dispositivo que es:

diseñado para permitir o denegar las transmisiones de la red sobre la base de un conjunto de reglas



3.-Cortafuegos.

Un cortafuegos funciona en base a reglas. Existen dos grandes filosofías para definir las: por un lado está la **política permisiva**, que acepta todo el tráfico menos el que sea denegado expresamente y, por otro, **la política restrictiva** que deniega todo el tráfico menos lo que se acepte expresamente. Esta última política es más difícil de mantener pero más segura y es la que se debería utilizar siempre.

Regla	Acción	IP Origen	IP Destino	Proto	Puerto Origen	Puerto Destino
1	Aceptar	172.16.0.0/16	192.168.0.4	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.8	tcp	cualquiera	80
3	Aceptar	172.16.0.0/16	192.168.0.2	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Por ejemplo, podríamos tener un cortafuegos con una regla que indicase que el rango de red 172.16.0.0/16 puede acceder al servidor SMTP (puerto 25) con dirección IP 192.168.0.4 y al servicio Web (puerto 80) con dirección 192.168.0.2. Otra regla podría establecer que cualquier dirección podría tener acceso a otro servicio Web en la dirección 192.168.10.8. Lógicamente el resto de conexiones serían denegadas.




3.-Cortafuegos.


Firewall de Windows Defender

← → ↕ ↑  > Panel de control > Todos los elementos de Panel de control > Firewall de Windows Defender


Ventana principal del Panel de control

Permitir que una aplicación o una característica a través de Firewall de Windows Defender

 Cambiar la configuración de notificaciones

 Activar o desactivar el Firewall de Windows Defender




 Restaurar valores predeterminados



 Configuración avanzada

Solución de problemas de red

Ayudar a proteger el equipo con Firewall de Windows Defender

Firewall de Windows Defender puede ayudar a impedir que piratas informáticos o software malintencionado obtengan acceso al equipo a través de Internet o una red.

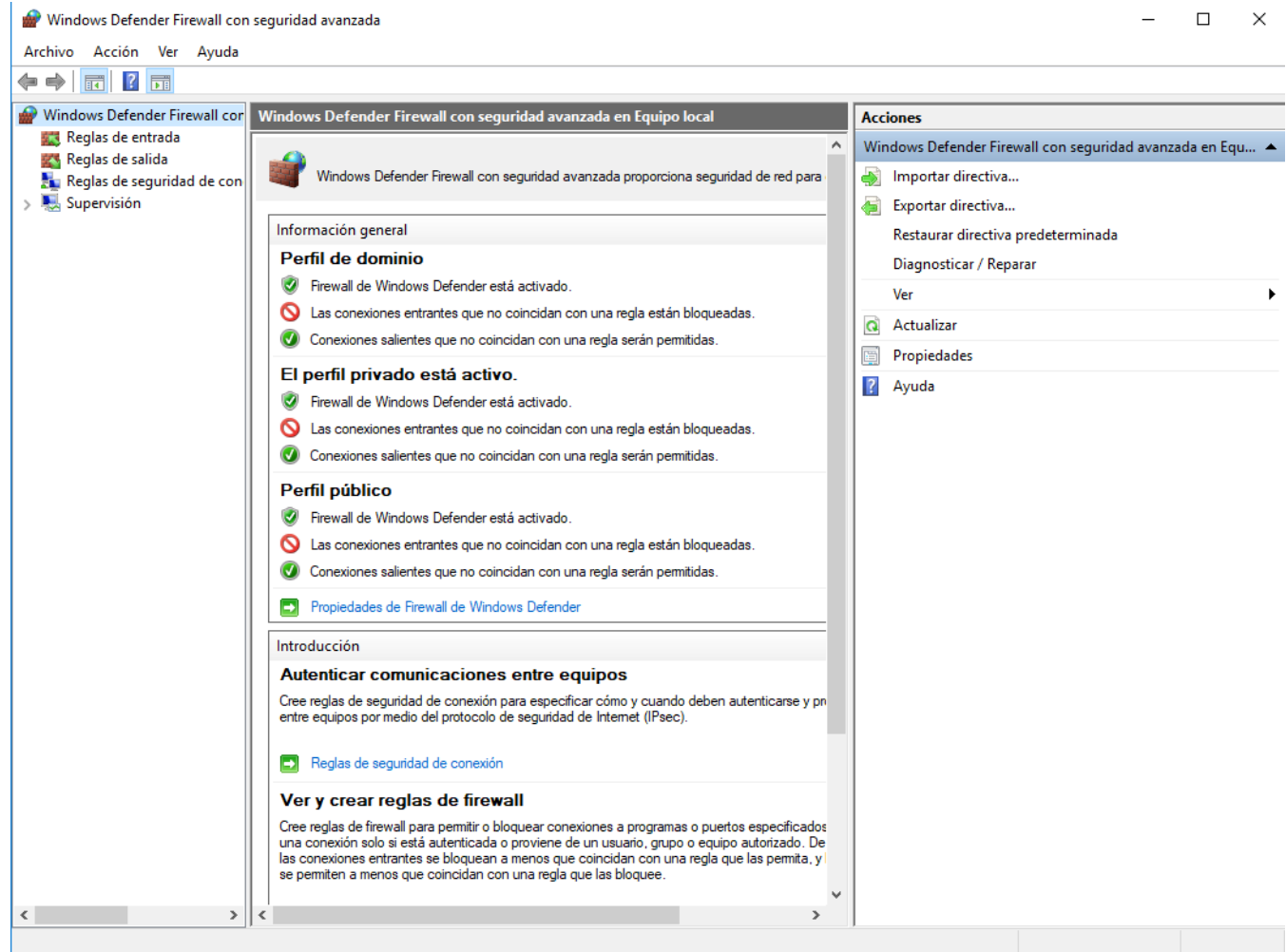
 Redes privadas Conectado 	
Redes domésticas o del trabajo en cuyos usuarios y dispositivos confíe	
Estado de Firewall de Windows Defender:	Activado
Conexiones entrantes:	Bloquear todas las conexiones a aplicaciones que no estén en la lista de aplicaciones permitidas
Redes privadas activas:	 Red
Estado de notificación:	Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación

 Redes públicas o invitadas No conectado 	
--	--



3.-Cortafuegos.

Configuración avanzada





3.-Cortafuegos.

Ejercicios: Firewall-Configuración avanzada

Bloquear la navegación para los siguientes puertos:

80 → Transferencia de páginas web.

8080 → Transferencia con servidor web Java (Tomcat)

1.- **Regla de salida** → Nueva regla → Puerto → TCP

2.- Comprueba si tienes acceso a (**Borra el historial**):

<http://www.diariosur.es>

Elpais.com

<https://www.Google.es>

3.- Elimina dicha regla.



3.-Cortafuegos.

Ejercicios: Firewall-Configuración avanzada

Bloquear la utilización de Google Chrome.

- 1.- **Regla de salida** → Nueva regla → Programa
- 2.- Comprueba si con Google y Firefox puedes navegar (**Borra el historial**).
- 3.- Elimina dicha regla.



3.-Cortafuegos.

Ejercicios: Firewall-Configuración avanzada

Bloquear entradas del tipo:

<ftp://ftp.cica.es/>

<ftp://ftp.iac.es/>



Sugerencias/mejoras del tema



Sugerencias /mejoras del tema



Referencias

- ❑ Los logotipos del Dpto de informática han sido diseñados por Manuel Guareño.