# LABORATORIO 3: CONFIGURACIÓN DEL FIREWALL DE WINDOWS

Realizado por: Jesús Padilla Crespo

# Laboratorio 3: Configuración del Firewall de Windows

## Introducción

En esta práctica de laboratorio, se explora el Firewall de Windows y se configuran algunos parámetros avanzados.

## Equipo recomendado

- Dos computadoras con Windows conectadas directamente o través de la red
- Las computadoras deben estar en el mismo grupo de trabajo y en la misma red
- RECOMENDACIÓN: →Configuraciones firewall ICMP (en las 2 máquinas tanto en entrada como en salida)
- Firewall/config avanzada/crear regla/personalizada/todos los programas/ icmpv4/siguiente todo el rato

## Instrucciones

## Paso 1: Cree y comparta una carpeta en PC-1.

a. Inicie sesión en **PC-1** como miembro del grupo de administradores. Pídale al instructor el nombre de usuario y contraseña.

b. Verifique que pueda hacer ping a **PC-2**.

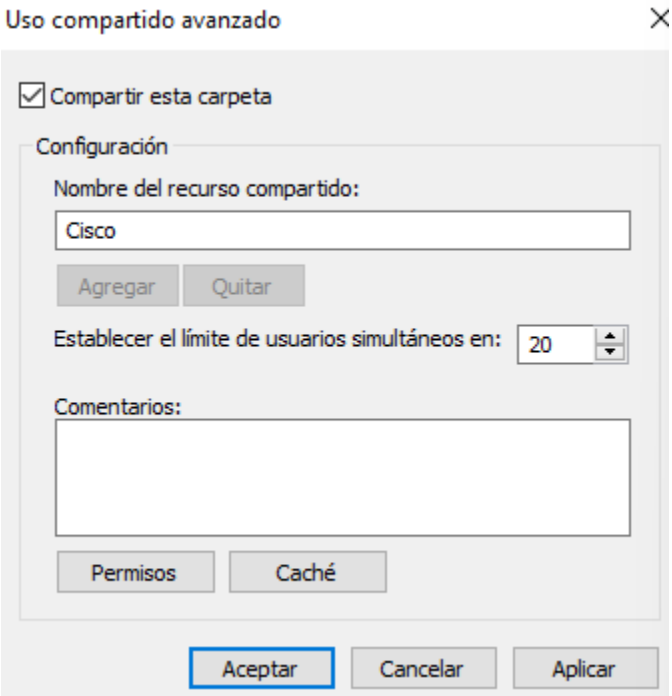
```
C:\Users\asir27>ping 192.168.1.118

Haciendo ping a 192.168.1.118 con 32 bytes de datos:
Respuesta desde 192.168.1.118: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.118: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.118: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.118: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.118:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

c. En **PC-1**, haga clic con el botón secundario en el escritorio y seleccione **Nuevo y Carpeta**. Asígnele a la carpeta el nombre **Cisco**.

d. Haga clic con el botón secundario del mouse en la carpeta Cisco y, luego, seleccione **Propiedades, Uso compartido** y **Uso compartido avanzado**. Se abre la ventana **Uso compartido avanzado**. Haga clic en **Compartir esta carpeta** y utilice el nombre predeterminado **Cisco**. Haga clic en **Aceptar**. Cierre la ventana **Propiedades de Cisco**.




## Paso 2: Utilice el Explorador de archivos o Windows Explorer para ver la carpeta compartida de PC-1.

a. Inicie sesión en **PC-2** como miembro del grupo de administradores. Pídale al instructor el nombre de usuario y contraseña.

b. Abra el **Explorador de archivos** o **Windows Explorer**. En el panel izquierdo, en **Red**, expanda **PC-1**.

Pregunta:

En PC-1, ¿puede ver la carpeta compartida **Cisco**?

**→Sí, puedo verla**

**Nota**: Si la respuesta es no, solicite ayuda al instructor.

c. Cierre el Explorador de archivos o Windows Explorer.

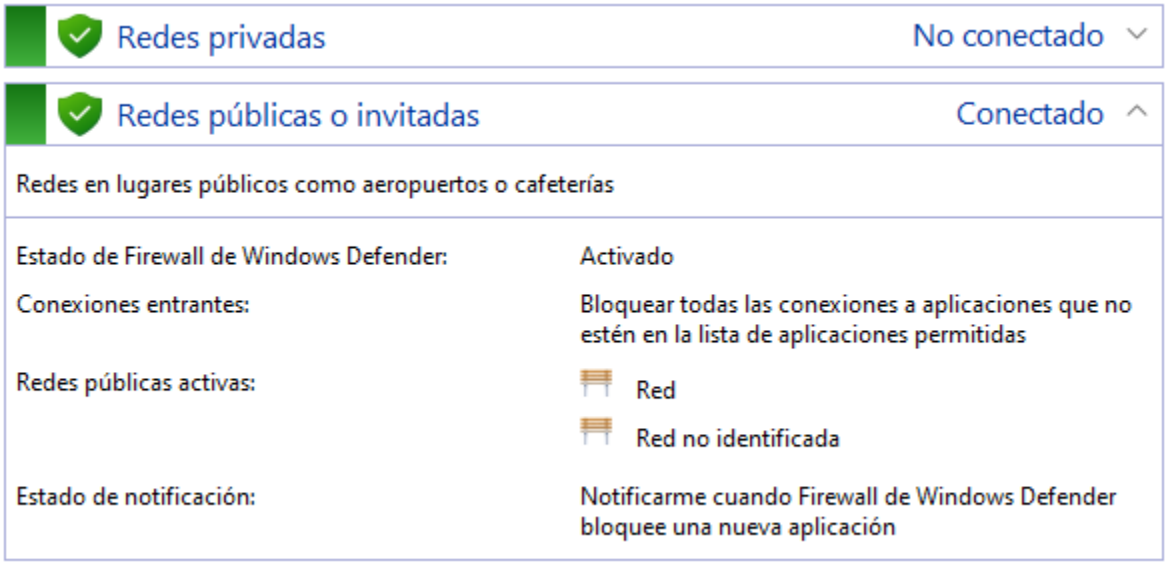
## Paso 3: Abra el Firewall de Windows en PC-1.

**Nota**: Utilice **PC-1** para el resto de la práctica de laboratorio, a menos que se indique lo contrario.

a. Para abrir la ventana Firewall de Windows, haga clic en Panel de control > Sistema y seguridad > Firewall de Windows Defender o Firewall de Windows.

b. El estado normal del Firewall de Windows es **Activado**.




Pregunta:

¿Cuáles son los beneficios del Firewall de Windows?

**→Mayor seguridad para solicitudes entrantes y salientes de la red que puedan dañar a nuestro equipo ya sea por ataque directo de un usuario que por aplicaciones dañinas.**

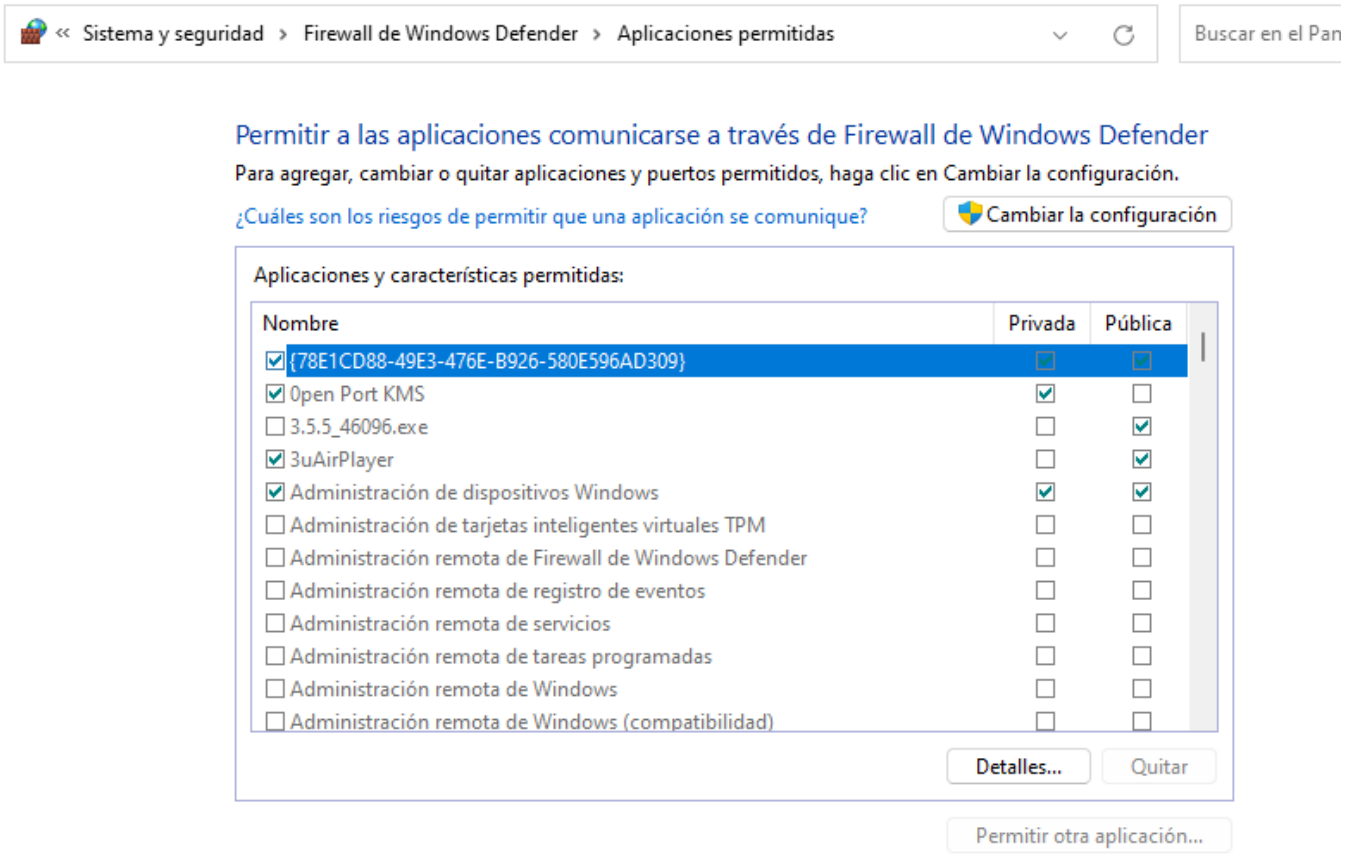
## Paso 4: Investigar la función Programas permitidos del Firewall de Windows.

a. Haga clic en Permitir una aplicación o una característica a través de Firewall de Windows Defender o Permitir que las aplicaciones se comuniquen a través del Firewall de Windows.

b. Se abre la ventana **Aplicaciones permitidas**. Los programas y servicios que el Firewall de Windows no bloquea se indican con una marca de verificación. Haga clic en **¿Cuáles son los riesgos de permitir que una aplicación se comunique?** o**¿Cuáles son los riesgos de permitir que un programa se comunique?**

**Nota**: Puede agregar aplicaciones a esta lista. Esto puede ser necesario si tiene una aplicación que requiere comunicaciones externas pero, por alguna razón, el Firewall de Windows no puede realizar la configuración automáticamente.

La creación de demasiadas excepciones en el archivo Programas y servicios puede tener consecuencias negativas.




Describa una consecuencia negativa de tener demasiadas excepciones.

**→Al crear excepciones ,creamos sin ser conscientes una pequeña brecha en nuestro "muro" y al abrir muchas brechas la consistencia de ese muro disminuye mucho, pues bien, eso mismo sucede con nuestro firewall, creamos pequeñas oberturas en nuestra defensa exponiendo esas vulnerabilidades a la red en la que podemos ser víctimas.**

c. Cierre la ventana Ayuda y soporte técnico de Windows.

## Paso 5: Configure la función aplicaciones permitidas de Firewall de Windows.

a. En la ventana **Aplicaciones permitidas**, haga clic en **Cambiar configuración**. Elimine la marca de verificación de **Compartir archivos e impresoras**. Haga clic en **Aceptar**.

b. En **PC-2**, mediante el **Explorador de archivos** o **Windows Explorer**, intente abrir la red para conectarse a **PC-1**.

Pregunta:

¿Puede conectarse con PC-1 y ver la carpeta compartida de Cisco?

**→No, no he podido acceder a la carpeta**

¿Recibió un mensaje de error en PC-2? Si es así, ¿cuál fue el mensaje de error?

**Sí, Windows no ha podido acceder al otro pc.**

c. Cierre todas las ventanas abiertas en **PC-2**.

d. En **PC-1**, agregue una marca de verificación a **Uso compartido de archivos e impresoras**. Haga clic en **Aceptar**.

**Nota**: Debe poder agregar la marca de verificación sin tener que hacer clic en **Cambiar configuración**.

e. En **PC-2**, vuelva a abrir el Explorador de archivos o Windows Explorer e intente conectarse a **PC-1**.

Pregunta:

¿Puede conectarse a PC 1? Explique.

**→Sí, porque la función Compartir archivos e impresoras de PC-1 ya no está bloqueada por el firewall.**

f. Cierre todas las ventanas abiertas en **PC-2** y cierre la sesión.

g. Cierre todas las ventanas de **PC-1**.

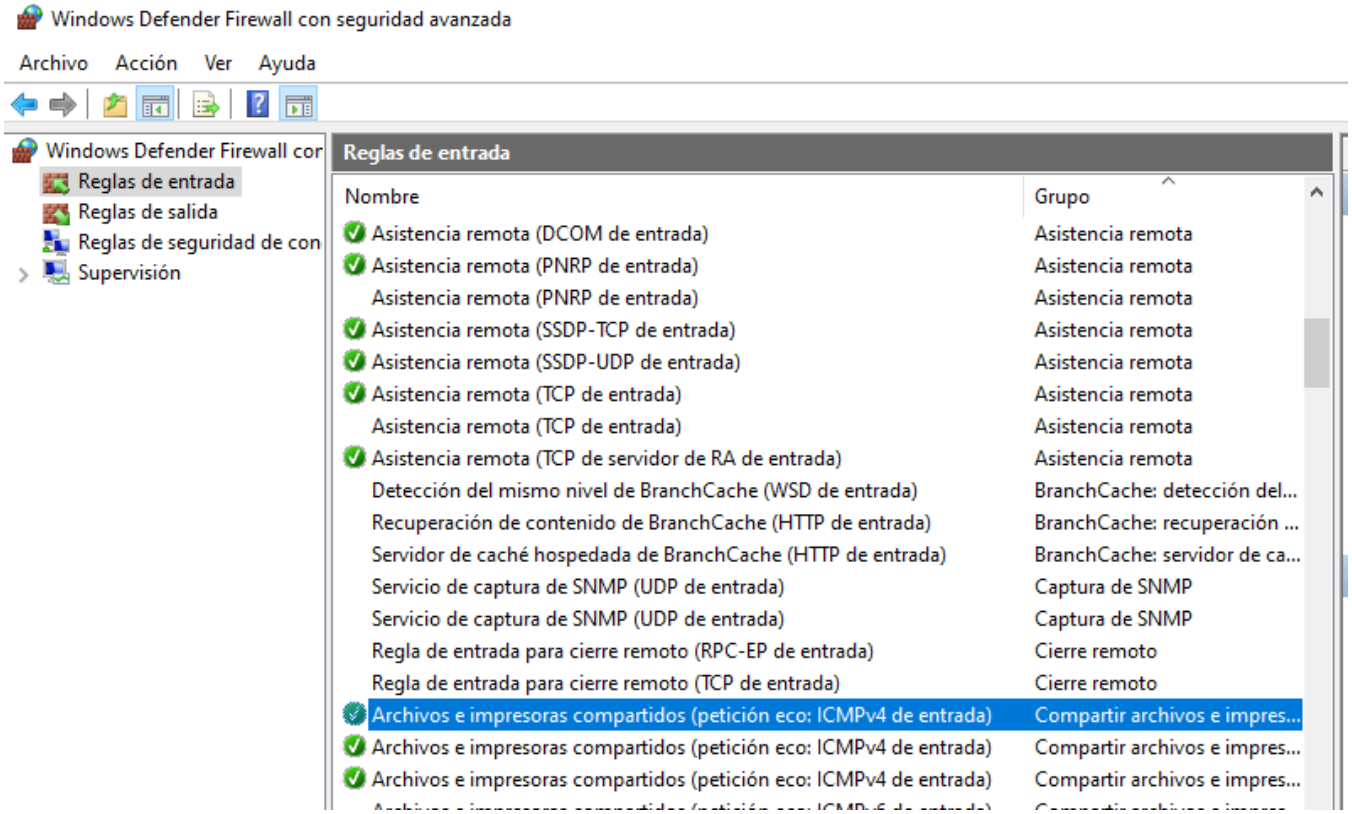
## Paso 6: Explore las funciones de seguridad avanzada en Firewall de Windows.

**Nota**: Utilice **PC-1** para el resto de esta práctica de laboratorio.

a. En la vista de iconos pequeños, haga clic en **Panel de control**, **Herramientas administrativas**, **Firewall de Windows Defender con seguridad avanzada** o **Firewall de Windows con seguridad avanzada**.

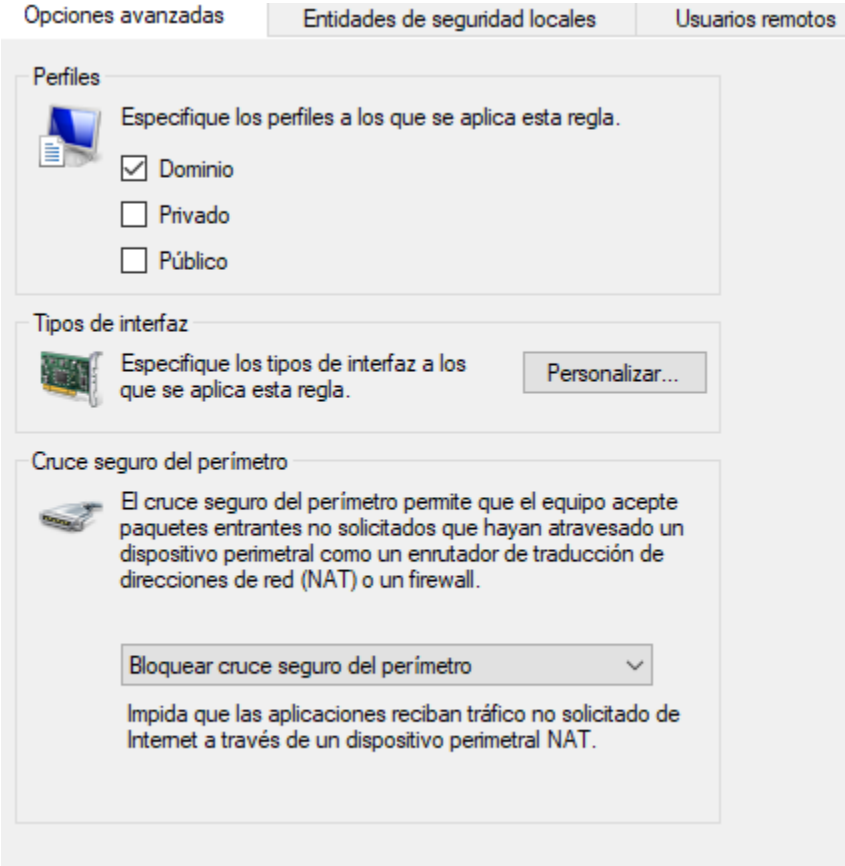
b. En el panel izquierdo de la ventana **Firewall de Windows Defender con seguridad avanzada** o **Firewall de Windows con seguridad avanzada**, puede seleccionar elementos para configurar **Reglas de entrada**, **Reglas de salida** o **Reglas de seguridad de conexión.** También puede hacer clic en **Supervisar** para ver el estado de reglas configuradas. Haga clic en **Reglas entrantes**.

c. En el panel central, desplácese hacia abajo hasta encontrar la regla de entrada denominada **Compartir archivos e impresoras (Echo Request – ICMPv4-In)**. Haga clic con el botón secundario del mouse en la regla y seleccione **Propiedades**, luego seleccione la pestaña **Opciones avanzadas**.

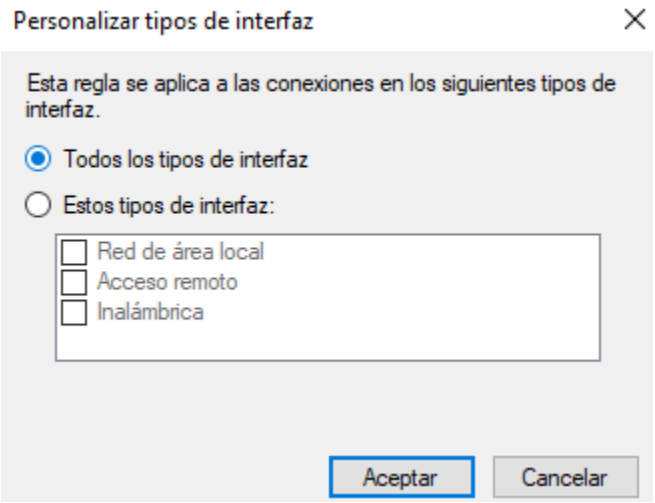


d. La pestaña **Opciones avanzadas** muestra los perfiles que utiliza la computadora. Haga clic en **Personalizar** en el área **Tipos de interfaz** de la ventana.




e. La ventana **Personalizar tipos de interfaz** muestra las distintas conexiones configuradas para la computadora. Deje seleccionada la opción **Todos los tipos de interfaz**, luego, haga clic en **Aceptar**.




f. Haga clic en la pestaña **Programas y servicios**. En la sección **Servicios**, haga clic en **Configuración...**.

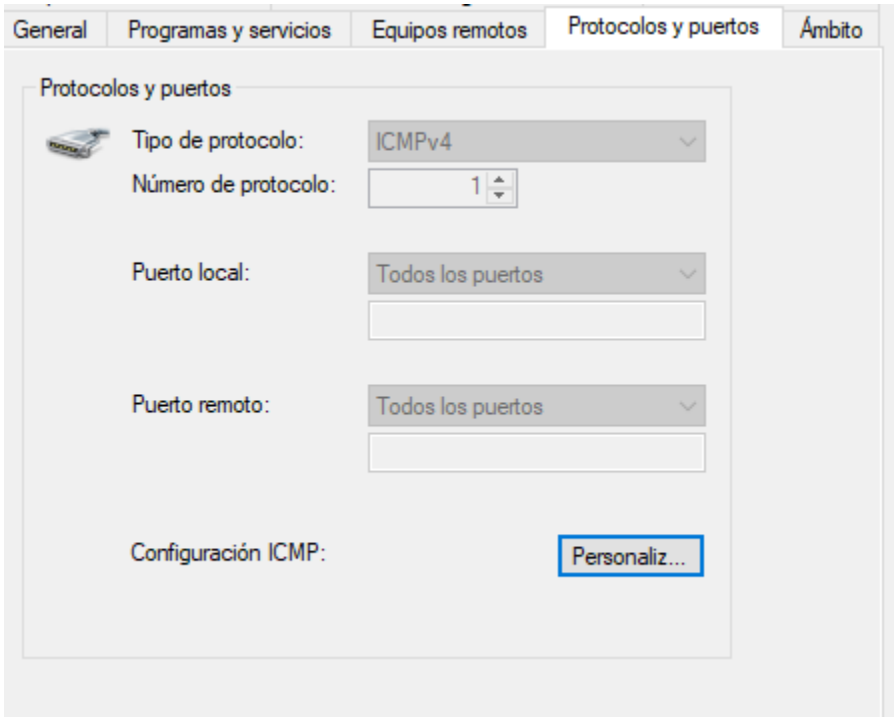
Indique el nombre corto de cuatro servicios que estén disponibles en la ventana **Personalizar configuración de servicios**.

***Escriba sus respuestas aquí.***

g. Haga clic en **Cancelar** para cerrar la ventana **Personalizar configuración de servicios**.

h. Haga clic en la pestaña **Protocolos y puertos**.




**Nota**: Existen numerosas aplicaciones que los usuarios generalmente no ven y que también necesitan pasar por el Firewall de Windows para acceder a la computadora. Se trata de los programas de nivel de red que dirigen el tráfico de la red y de Internet.

i. En la configuración de ICMP, haga clic en **Personalizar**.

j. Se abre la ventana **Personalizar configuración de ICMP**. La opción permitir solicitud de eco entrante es la que permite que los usuarios de la red hagan ping a su computadora para determinar si está presente en la red.

Enumere cuatro tipos específicos de ICMP.

**→Petición ECO/Anuncio de enrutador/S.Quench y Redirección**

k. Cierre todas las ventanas abiertas en **PC-1**.

l. Haga clic con el botón secundario del mouse en la carpeta **Cisco** en el escritorio, luego seleccione **Eliminar**.

## Pregunta de reflexión

¿Cuáles son algunas de las razones posibles por las que deba realizar cambios de firewall?

**→Pues como éste mismo ejercicio, una posible conexión de red para compartir archivos, pero hay que modificar algunas reglas para ceder el permiso. Otra es por ejemplo una aplicación que para poder aprovechar su potencial debemos configurar el Firewall. (eso sí, debemos estar seguros y confiar 100% tanto en la aplicación como de la fuente que se ha obtenido, si no, los resultados pueden ser todo lo contrario a lo que buscamos).**