



## Actividad

Utilizando la herramienta de firewall de Windows se pueden crear reglas del firewall personalizadas para proteger los equipos. De la misma forma sucede con los firewalls en redes.

Para abrir el firewall los estudiantes deben ir en sus dispositivos al panel de control, luego sistema y seguridad y finalmente en firewall de Windows defender.

## Configurar una regla de entrada para permitir una aplicación específica:

- Abre el Firewall de Windows Defender con seguridad avanzada:
  - Presiona Win + R, escribe wf.msc y pulsa Enter.
- En el panel izquierdo, selecciona Reglas de entrada.
- Haz clic en **Nueva regla** en el panel derecho.
- Selecciona **Programa** y haz clic en **Siguiente**.
- Busca la aplicación que deseas permitir (por ejemplo, un navegador o una aplicación local).
- Selecciona Permitir la conexión y haz clic en Siguiente.
- Especifica los perfiles (privado, público, dominio) donde la regla será válida y haz clic en **Siguiente**.
- Asigna un nombre a la regla (por ejemplo, *Permitir Navegador*) y guarda los cambios.

Configurar una regla para bloquear un puerto específico (por ejemplo, el puerto 23):

- En el Firewall de Windows Defender con seguridad avanzada, selecciona Reglas de entrada.
- Haz clic en **Nueva regla**.







- Selecciona Puerto y haz clic en Siguiente.
- Selecciona TCP e introduce el número de puerto que deseas bloquear (por ejemplo, 23, utilizado por Telnet).
- Selecciona Bloquear la conexión y haz clic en Siguiente.
- Define los perfiles (privado, público, dominio) y haz clic en Siguiente.
- Asigna un nombre a la regla (por ejemplo, *Bloquear puerto Telnet*) y guarda los cambios.

## Verificar el funcionamiento de las reglas:

Intenta utilizar la aplicación permitida o acceder al puerto bloqueado desde otro dispositivo en la red.

Observa cómo el firewall permite o niega el acceso según las reglas configuradas.

Para mayor claridad, habilita el registro del Firewall:

En Firewall de Windows Defender con seguridad avanzada, ve a Propiedades del Firewall.

En cada perfil (Dominio, Privado, Público), habilita Registrar paquetes descartados en Registro de conexiones.

