WILCOMP

S.A.S.

Firewall (Cortafuegos de Windows)

---

a. Contenido

- **Activación y verificación del Firewall de Windows Defender.**
- **Comprensión de las redes privadas vs. públicas.**
- **Permiso manual de aplicaciones a través del firewall.**
- **Restauración de valores predeterminados.**
- **Bloqueo de entrada de conexiones no solicitadas.**

---

b. Introducción

El Firewall (cortafuegos) es una barrera de seguridad que controla el tráfico de red que entra y sale de su computadora. Actúa como un filtro: permite la comunicación de programas confiables (como su navegador web) y bloquea intentos de conexión no autorizados (como un virus que intenta enviar sus datos a un atacante).

Windows 10 y 11 incluyen un firewall potente y gratuito llamado Windows Defender Firewall. Este tutorial le enseñará a verificar que esté activo, a permitir aplicaciones legítimas cuando sea necesario, y a restaurar la configuración si algo deja de funcionar correctamente. No necesita instalar ningún programa adicional.

---

c. Paso a Paso

1. Acceder a la configuración del Firewall

1. **En la barra de búsqueda junto al botón Inicio, escriba: firewall.**
2. **De los resultados, seleccione Firewall y protección de red (también puede aparecer como "Windows Defender Firewall").**
3. **Se abrirá una ventana con tres secciones principales: Red de dominio, Red privada y Red pública.**

2. Verificar el estado del firewall

1. **En cada una de las tres secciones, verifique que el texto indique "Firewall de Windows Defender activado".**

- **Red privada: Úsela cuando esté en su hogar o en una red de confianza.**
- **Red pública: Úsela cuando esté en aeropuertos, cafeterías, centros comerciales, etc. Nunca desactive el firewall en redes públicas.**

2. **Si alguna dice "Desactivado", haga clic sobre esa red y luego en el botón "Activar firewall de Windows Defender".**
3. **Asegúrese de que "Bloquear todas las conexiones entrantes, incluso en la lista de aplicaciones permitidas" esté DESACTIVADO a menos que se encuentre en un entorno de alto riesgo. Esta opción es útil para máxima seguridad, pero puede impedir el uso de impresoras o dispositivos en la red local.**

3. Permitir una aplicación a través del firewall

A veces un programa confiable (un juego, una impresora en red, un software de videollamadas) no puede conectarse a Internet porque el firewall lo bloquea. Para solucionarlo:

1. **En la pantalla principal de "Firewall y protección de red", haga clic en "Permitir una aplicación a través del firewall" (ubicado en la parte inferior).**
2. **Se abrirá una ventana con una lista de aplicaciones. Presione el botón "Cambiar configuración" (necesitará permisos de administrador).**
3. **Busque la aplicación que desea autorizar. Marque las casillas según corresponda:**
   - **Privado: Marque esta opción si la aplicación necesita funcionar en su red doméstica (por ejemplo, para compartir archivos o usar una impresora).**
   - **Público: Marque esta opción si necesita usar la aplicación cuando está fuera de su casa (por ejemplo, un servicio de VPN o un juego en línea).**
4. **Si la aplicación no aparece en la lista, haga clic en "Permitir otra aplicación...", luego en "Examinar" y busque el archivo ejecutable (.exe) de la aplicación en su disco duro. Una vez seleccionado, haga clic en "Agregar" y luego marque las casillas correspondientes.**
5. **Presione Aceptar para guardar los cambios.**

4. Restaurar valores predeterminados del firewall

Si ha realizado muchos cambios y nota comportamientos extraños (por ejemplo, que la computadora no responde o que ciertas funciones de red dejaron de funcionar), puede restaurar el firewall a su estado original.

1. **En la pantalla principal de “Firewall y protección de red”, haga clic en “Restaurar firewalls a los valores predeterminados”.**
2. **Se abrirá una nueva ventana. Haga clic en “Restaurar valores predeterminados”.**
3. **Confirme la operación cuando el sistema se lo solicite.**
4. **Esto no eliminará sus archivos personales, pero borrará todas las reglas personalizadas que haya creado. Las aplicaciones que había permitido manualmente tendrán que volver a configurarse.**

5. Bloqueo de entrada avanzado (opcional)

Si desea un control más granular, puede crear reglas de entrada y salida:

1. **En la pantalla principal, haga clic en “Configuración avanzada” (en el menú lateral izquierdo).**
2. **Se abrirá una ventana de “Firewall de Windows Defender con seguridad avanzada”. Aquí puede crear reglas específicas para puertos, protocolos o direcciones IP.**
3. **Recomendación: Para un usuario doméstico, esta sección no es necesaria. Limítese a las opciones básicas descritas en los pasos anteriores para evitar bloqueos accidentales.**

---

d. Conclusión

El Firewall de Windows es su primera línea de defensa contra accesos no autorizados. Al mantenerlo activo y gestionar correctamente las aplicaciones permitidas, logra un equilibrio entre seguridad y funcionalidad.

Puntos clave para recordar:

- **Nunca desactive el firewall completamente, incluso si un programa no funciona. En su lugar, permita solo ese programa.**
- **Diferencie entre red privada (su hogar) y red pública (lugares con desconocidos). En redes públicas, sea más restrictivo.**
- **Si un programa confiable deja de funcionar después de una actualización de Windows, verifique primero en “Permitir aplicaciones” antes de pensar en desactivar el firewall.**

- **Mantenga activadas las notificaciones del firewall para saber cuándo se bloquea una conexión.**