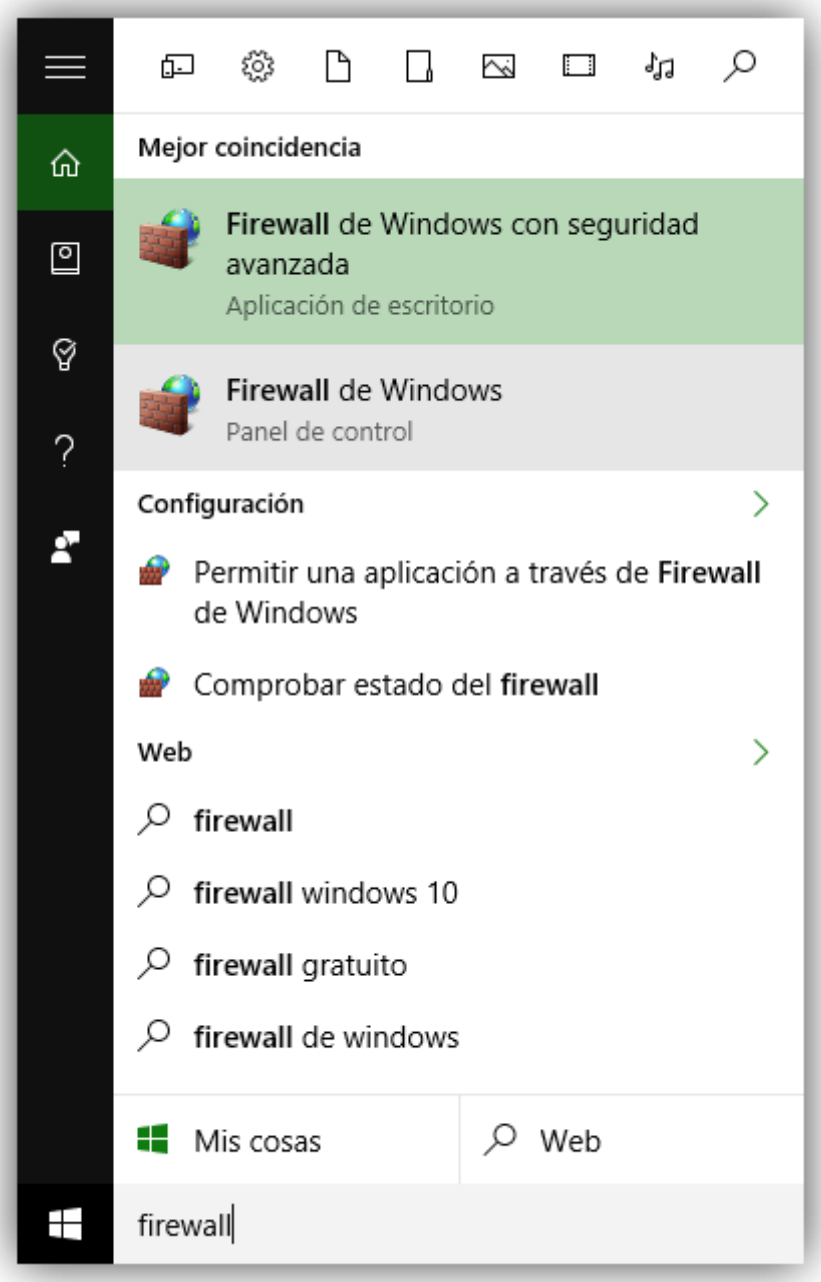
Seguridad Informática

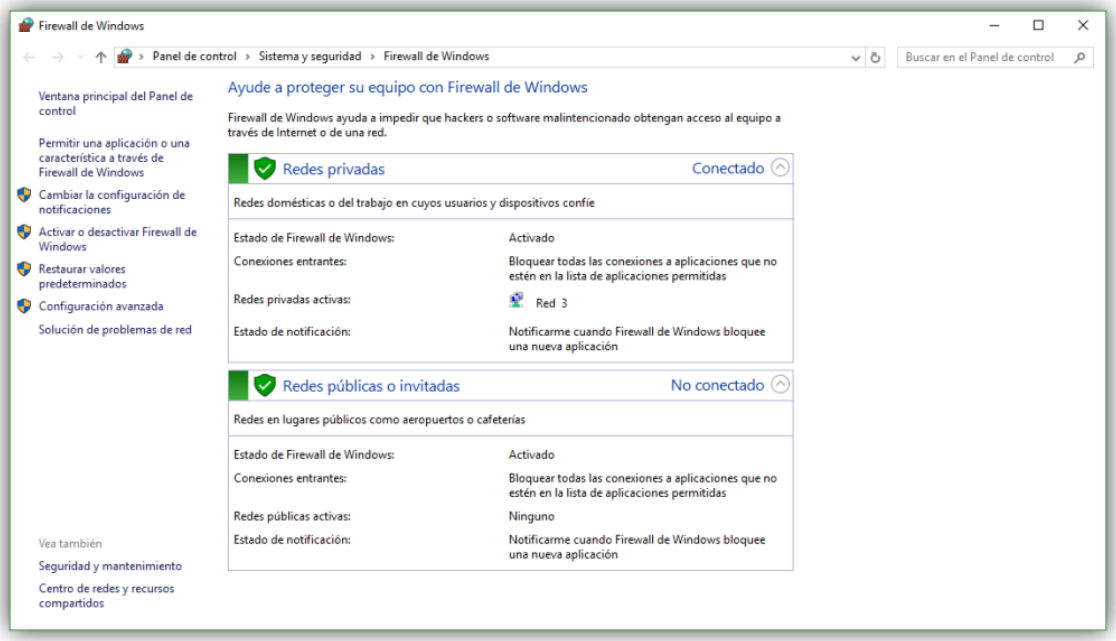
Según ya habíamos tratado en trabajos anteriores el tema de Firewall, tenemos el siguiente artículo que explica como configurar una regla de Firewall sobre Windows 10, también es perfectamente aplicable en Windows 7 y difiere en como configurar otro tipo de Firewall en algunas cosas, pero básicamente todo se trata de trabajar con puertos.

Cómo ver el estado del firewall de Windows 10 y activar o desactivar esta característica

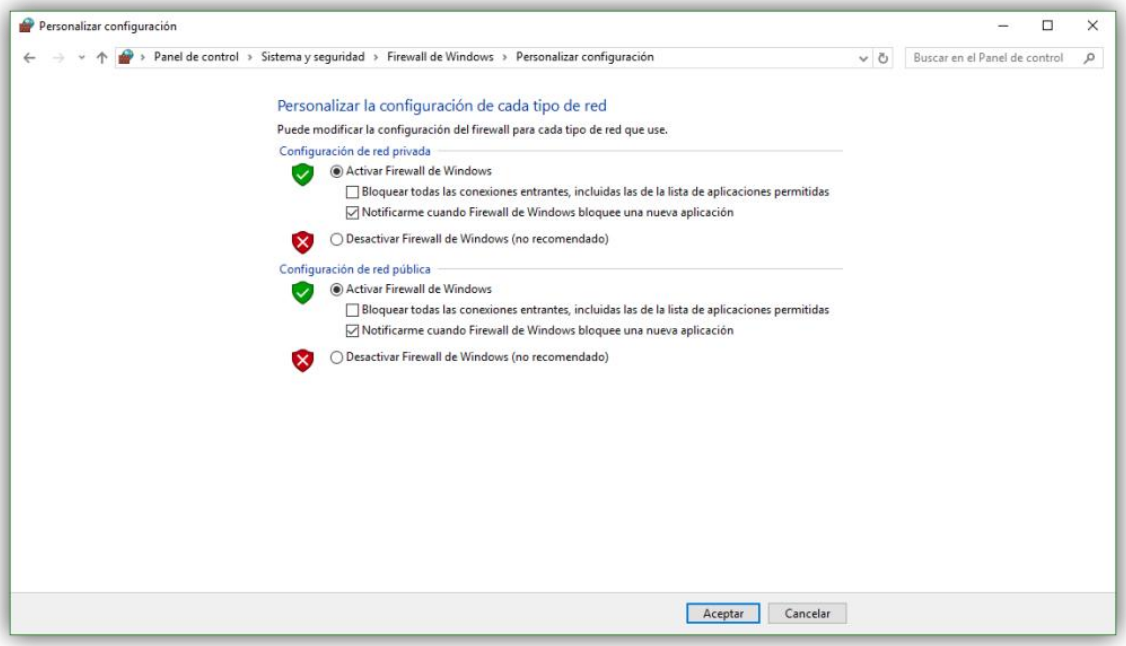
Lo primero que debemos hacer es buscar en Cortana, el nuevo buscador de Windows 10, «Firewall» para ver todos los apartados de configuración relacionados con esta herramienta de seguridad.



Pulsamos sobre «**Comprobar estado del firewall**» y veremos una ventana similar a la siguiente, donde podremos ver tanto si el cortafuegos está siendo controlado por otra aplicación (por ejemplo, una suite antivirus instalada) o si está tanto activado como desactivado para las redes públicas (las que salen a Internet) y para las privadas (redes locales).



En caso de querer cambiar esta configuración, simplemente debemos seleccionar, en el menú de opciones del lateral izquierdo, «**Activar o desactivar firewall de Windows**«. Se nos abrirá una nueva ventana como la siguiente.



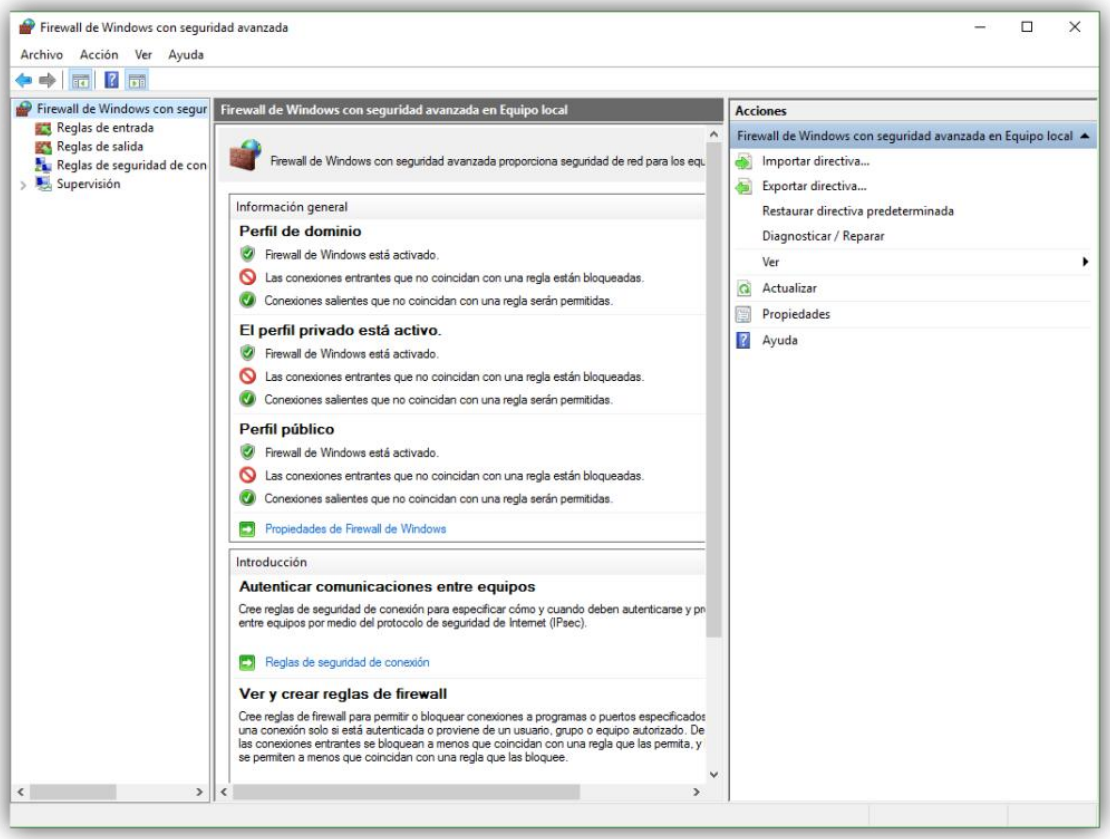
Desde aquí podemos activarlo o desactivarlo para las redes públicas y privadas, así como elegir si queremos aplicar un bloqueo global, de todas las conexiones (por ejemplo, en caso de emergencia o para

desconectarnos temporalmente de Internet) y si queremos ver notificaciones cada vez que se bloquee una conexión.

A nivel muy básico, estas son las principales opciones que nos ofrece Windows con su cortafuegos de fábrica, sin embargo, también es posible configurar los filtros de manera que si, por ejemplo, queremos que una aplicación concreta pueda salir a Internet por un solo puerto, podamos abrir dicho puerto permaneciendo cerrados los demás.

Cómo crear reglas para abrir y cerrar puertos en el firewall de Windows 10

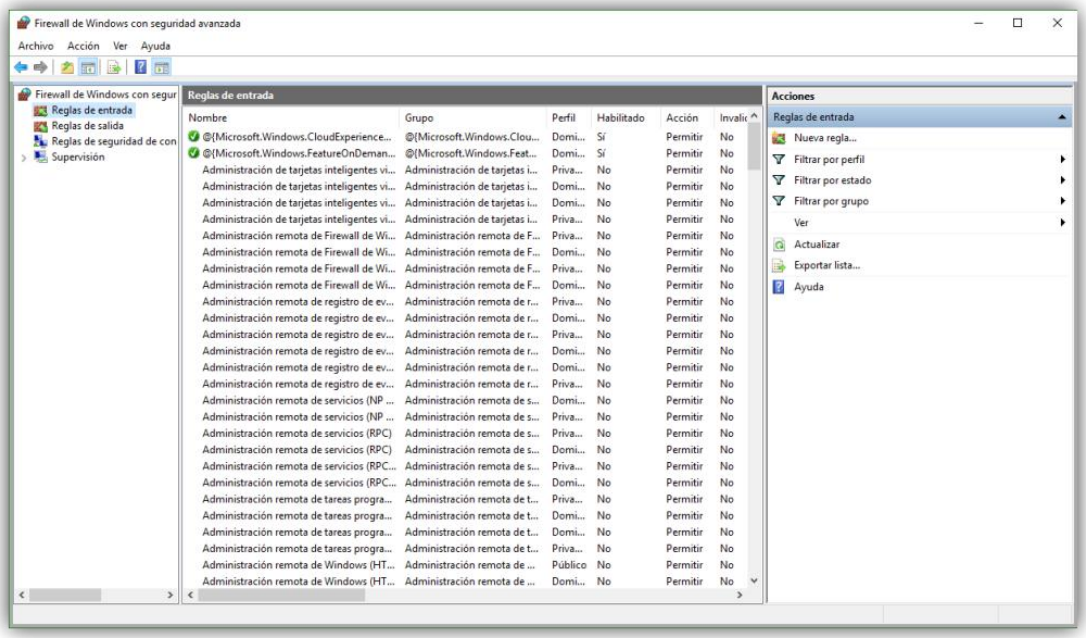
Para la creación de las reglas, en el mismo menú de la parte izquierda anterior debemos seleccionar «**Configuración avanzada**«. Veremos una ventana similar a la siguiente.



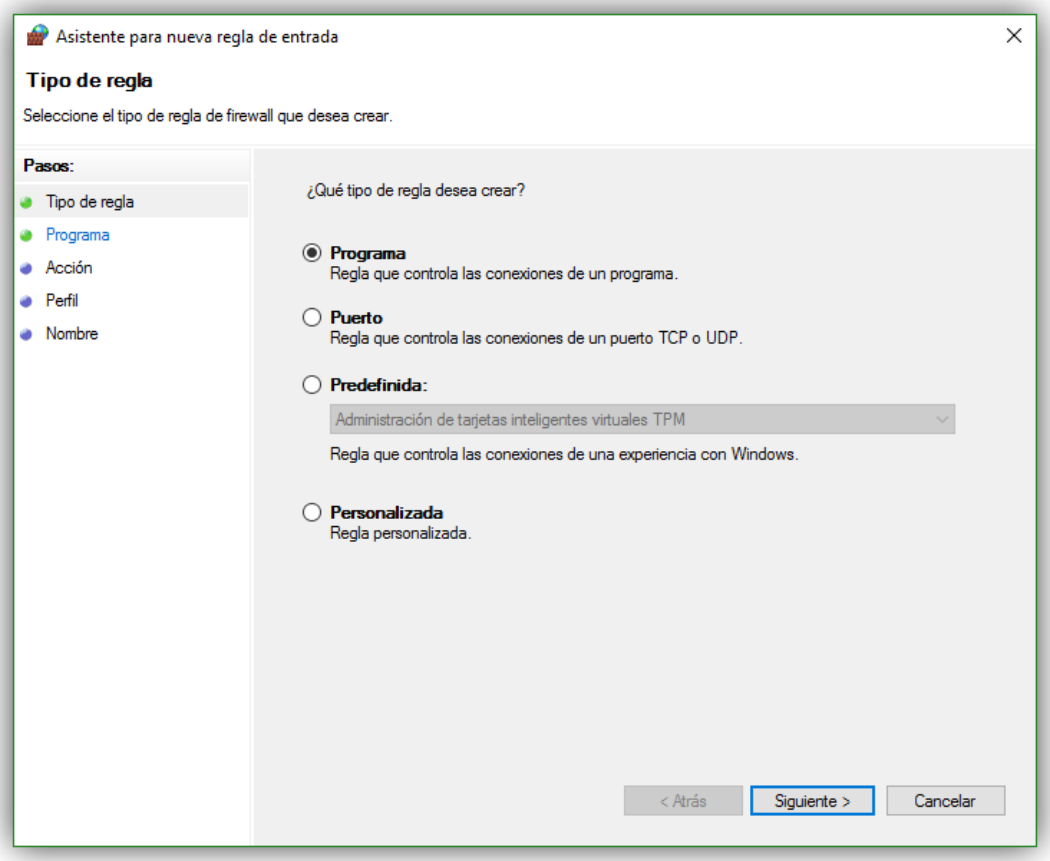
En esta ventana vamos a poder ver todas las reglas por las que se rige el cortafuegos y que hacen que el tráfico se permita o bloquee específicamente. Como podemos ver en la parte izquierda, tenemos dos tipos de reglas diferentes:

- **Reglas de entrada**: Controlan el tráfico que se permite o bloquea desde fuentes externas, es decir, las conexiones que se generan en Internet y que llegan a nuestro ordenador.
- **Reglas de salida**: Controla las conexiones que se generan en nuestro ordenador y que tienen como objetivo salir a Internet.

Seleccionamos en este panel del tipo de regla que queremos crear y, en la parte derecha, pulsamos sobre «Nueva regla».

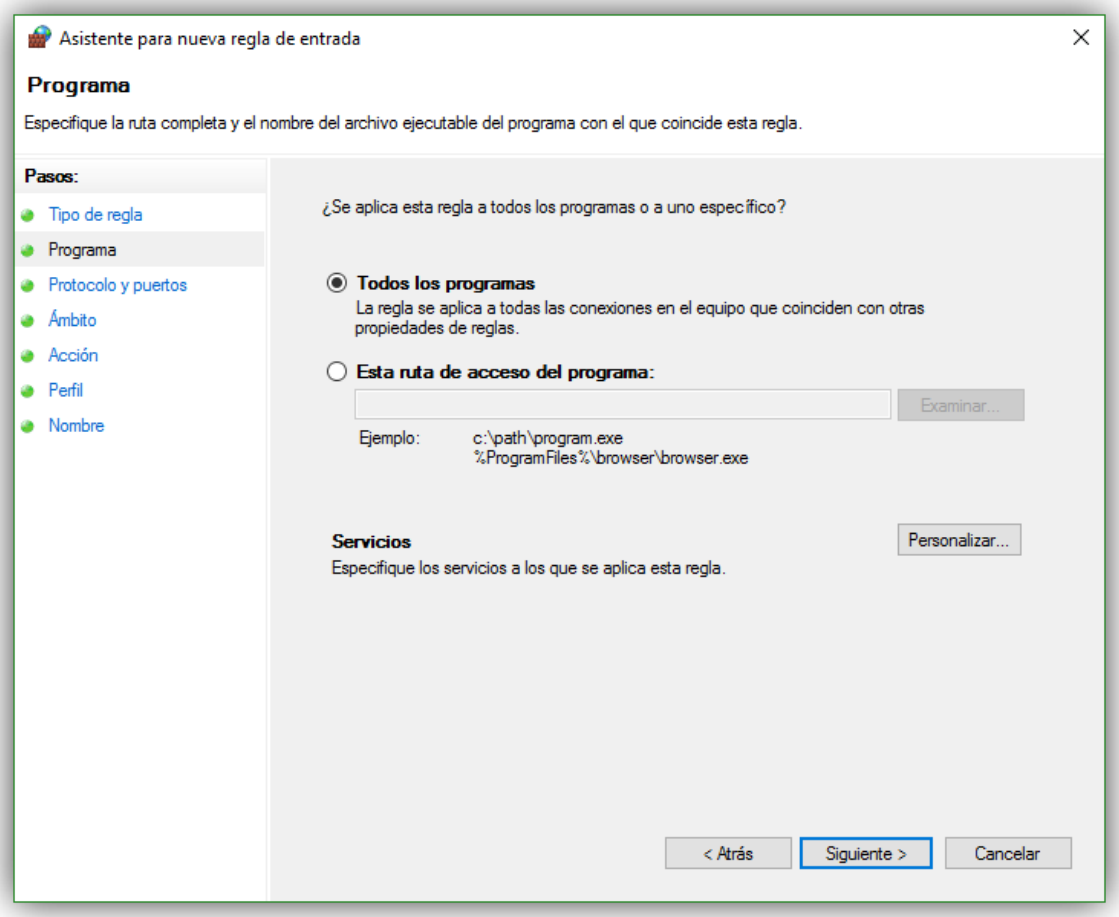


Nos aparecerá un sencillo asistente como el siguiente.



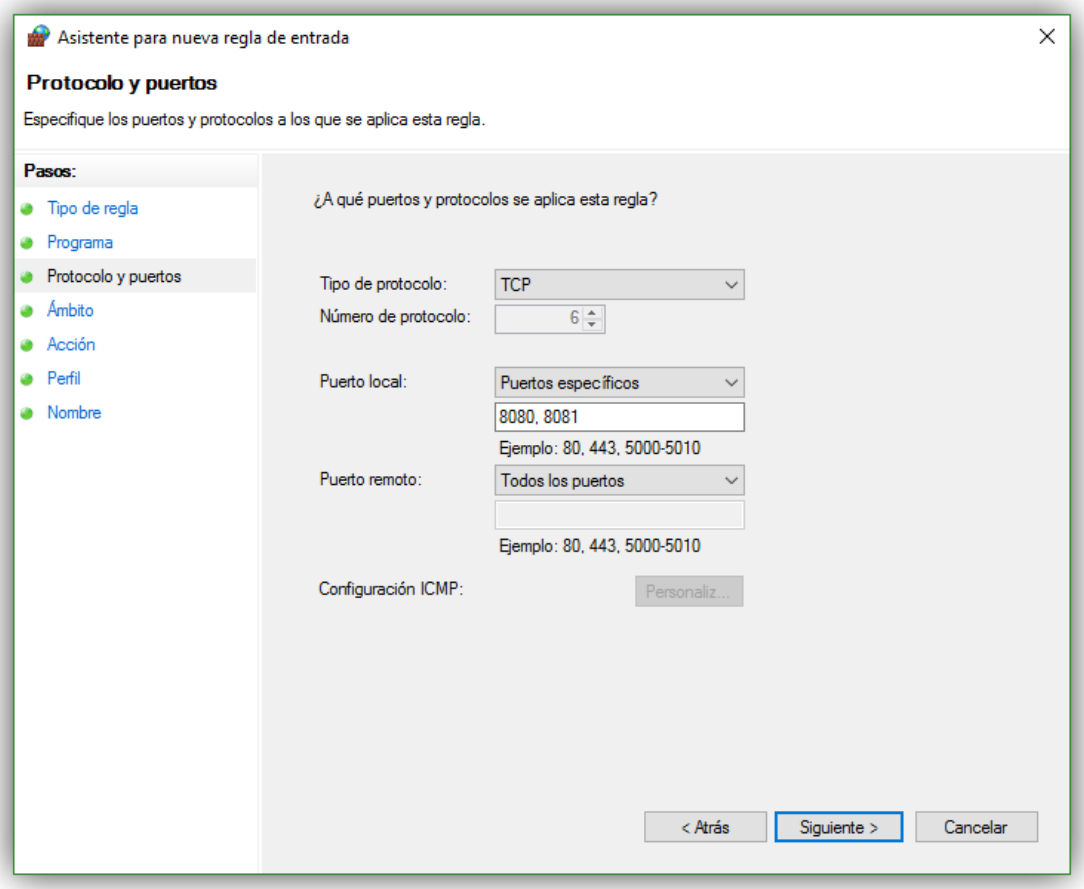
Lo primero que debemos hacer es seleccionar el tipo de regla que vamos a crear, ya sea, por ejemplo, para un programa específico (útil para abrir los puertos en el eMule o uTorrent), una regla para permitir el tráfico a través de un puerto concreto, una regla predefinida o personalizada.

La regla personalizada es la más completa y cubre tanto los apartados de una regla de programa como los de una regla de puerto, por lo que vamos a ver esta que, en resumen, nos permitirá habilitar la conexión de una aplicación específica a través de un puerto concreto.



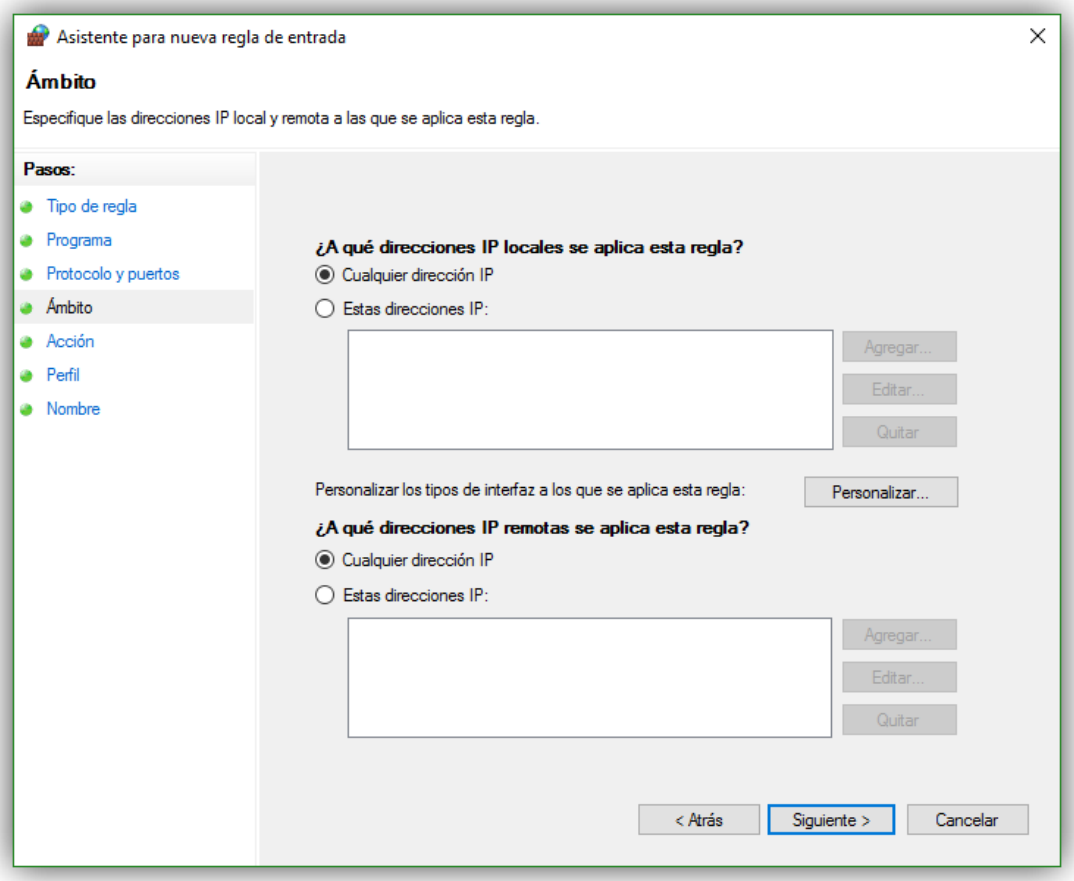
Lo primero que nos preguntará será qué programa o servicio va a verse afectado por dicha regla. Podemos elegir uno concreto o marcar la opción de «Todos los programas» para que dicha regla se aplique a todo.

En el siguiente paso tendremos que configurar el protocolo y los puertos.

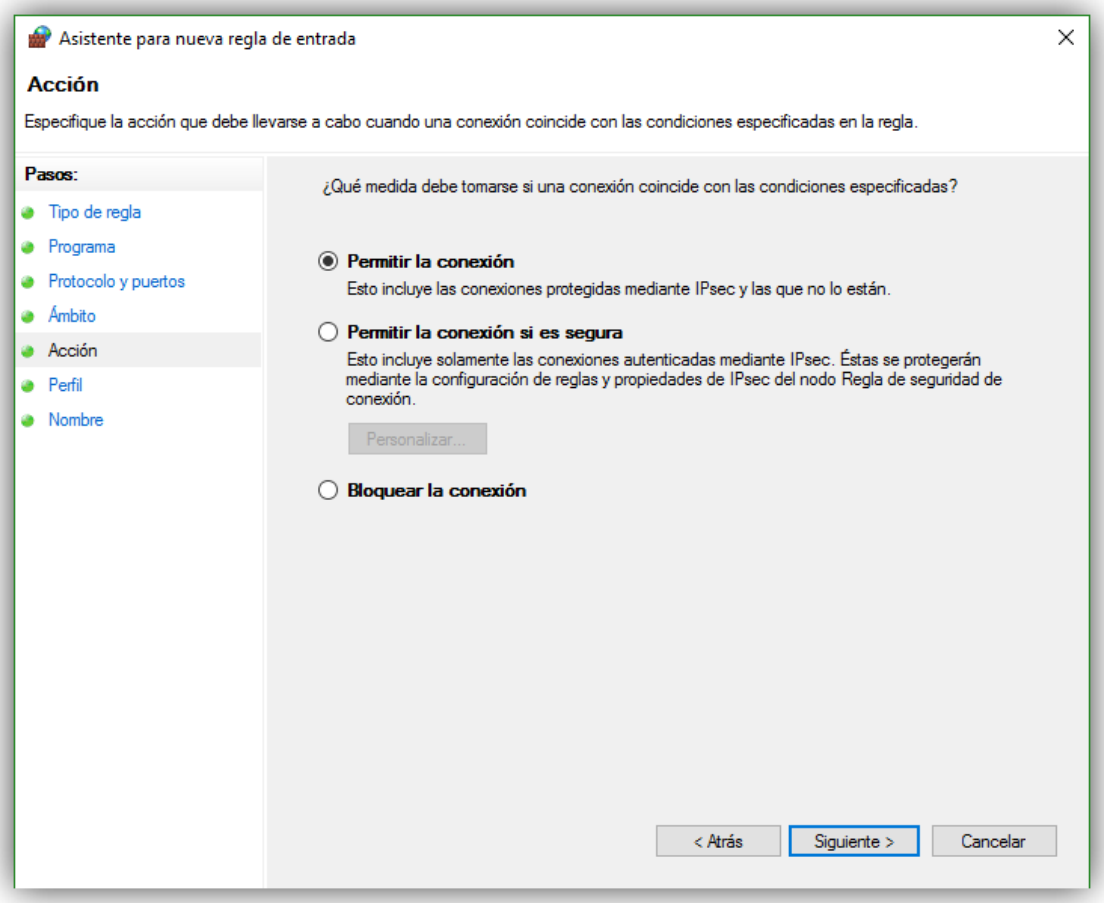


Aquí elegiremos a través de qué protocolo se hará la conexión (los más comunes con TCP y UDP) y especificar los puertos locales y remotos que queremos permitir (o bloquear).

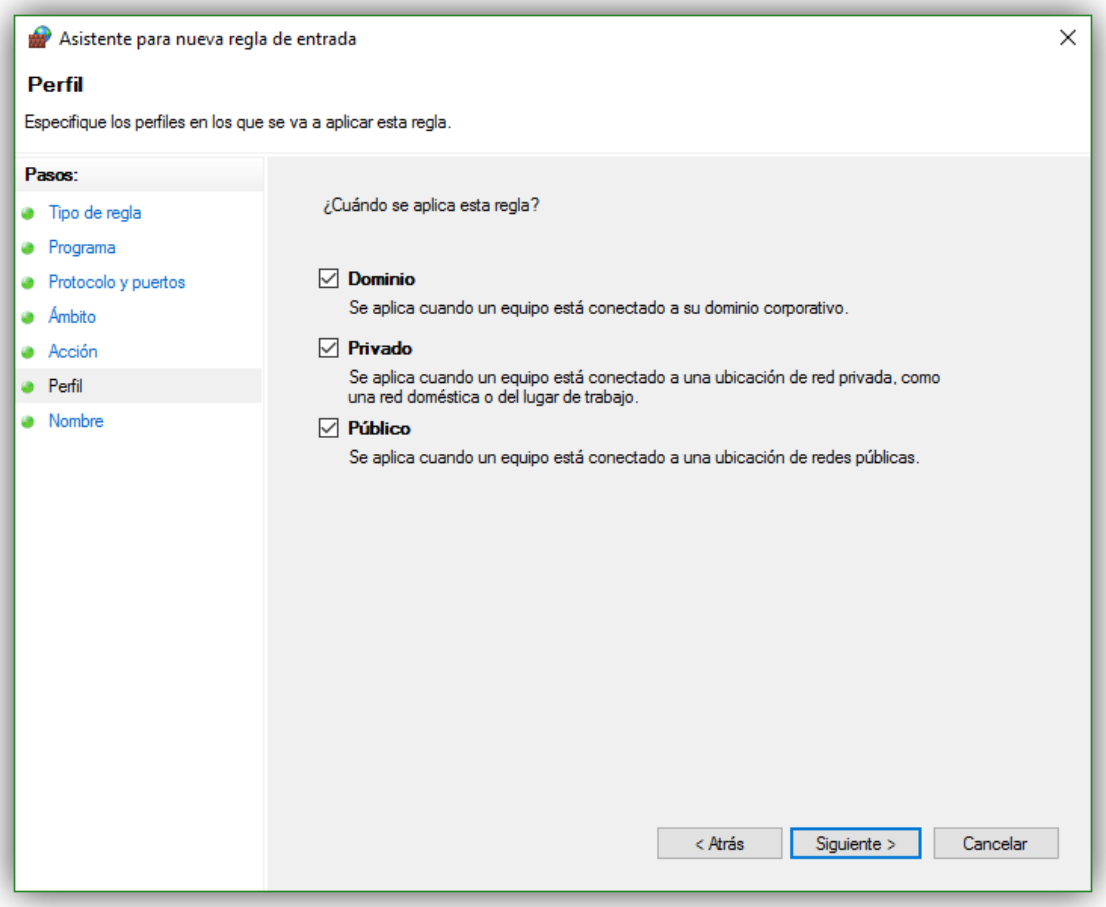
Continuamos con el asistente y a continuación podremos elegir las direcciones IP locales y remotas para las que se hará efectiva dicha regla.



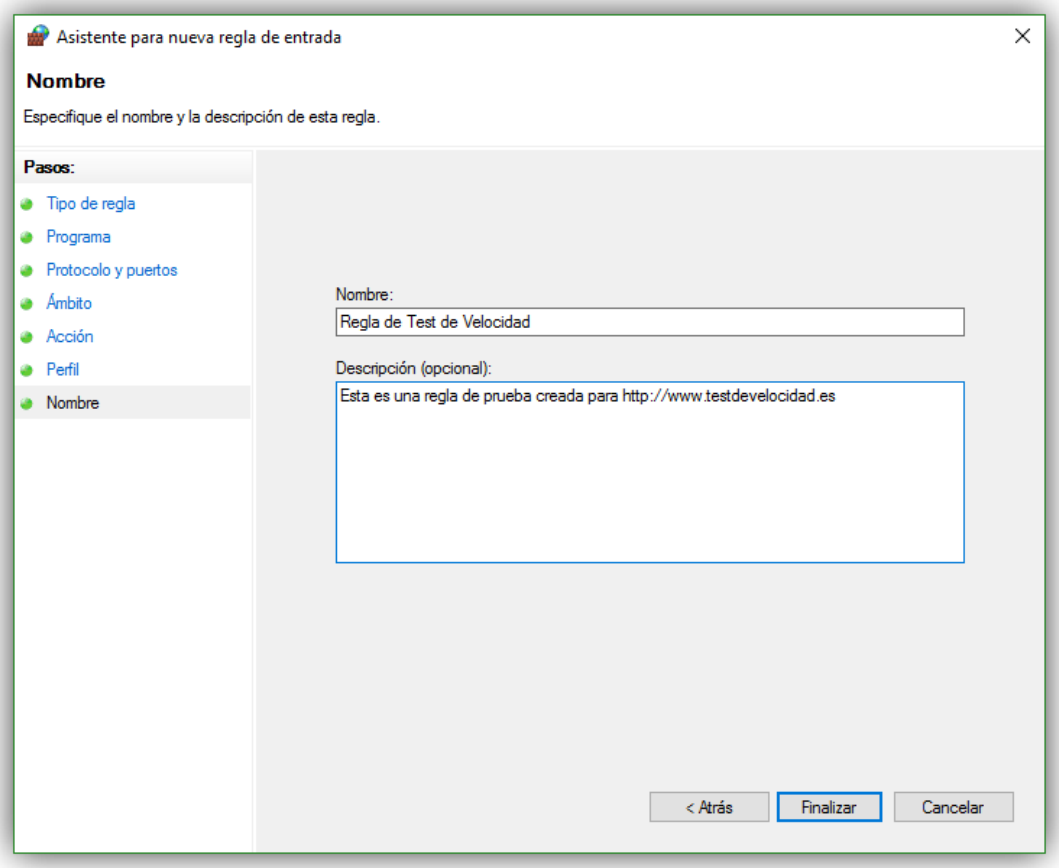
A continuación, tendremos que elegir si queremos permitir la conexión, permitirla siempre que sea a través de protocolos seguros o bloquear toda la conexión de la regla.



En el siguiente paso debemos configurar cuándo queremos que se aplique la regla, dentro de un dominio, en una red pública o en una red privada.



Por último, el asistente nos preguntará por el nombre y la descripción de dicha regla de manera que podamos identificarla en caso de tener que realizar alguna modificación en ella.



Tras finalizar el asistente, la regla se activará y empezará a funcionar en nuestro sistema operativo. A partir de ahora, todo el tráfico tendrá que cumplir las condiciones específicas para dicha regla si quiere poder transmitirse sin problemas, de no ser así, se bloqueará la conexión como medida de seguridad para evitar posibles problemas mayores.

Actividad:

- Crear una regla de entrada y una de salida que impida que los navegadores Web tengan acceso a internet en cualquier tipo de red (pública o privada).
- ¿Qué puertos tendría que bloquear en el Firewall de un router para que Whatsapp no se pueda conectar?