Que es un Firewall y como funciona. Tipos de firewall

Cada computadora conectada a internet (y, hablando más genéricamente, a cualquier red informática) es susceptible a ser **víctima de un ataque de un pirata informático.** La metodología empleada generalmente consiste en barrer la red (enviando paquetes de datos de manera aleatoria) en busca de una máquina conectada, y luego **buscar un "agujero" de seguridad,** el cual utilizará para acceder a los datos que allí se encuentren.

Esta amenaza es todavía mayor si la computadora está permanentemente conectada a Internet. Las razones son varias, incluyendo que la PC objeto se encuentre conectada sin supervisión permanente, o que no cambie, o lo haga de manera muy dilatada, la dirección IP. Afortunadamente, **para protegernos de las intrusiones de estos ciberdelincuentes, tenemos a nuestro favor una fantástica herramienta llamada Firewall.**

¿Qué es un Firewall?

Un firewall (llamado también "cortafuego"), es un sistema que permite **proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red** (expresamente de Internet). El firewall es un sistema que permite filtrar los paquetes de datos que andan por la red. Se trata de un "puente angosto" que filtra, al menos, el tráfico entre la red interna y externa.

Un firewall puede ser un programa (software) o un equipo (hardware) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas.

¿Cómo funciona un Firewall?

Un firewall funciona como una barrera entre internet u otras redes públicas y nuestra computadora. Todo el tipo de tráfico que no esté en la lista permitida por el firewall, no entra ni sale de la computadora.

Para ello, un sistema de firewall contiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión **(Allow)**
- Bloquear una conexión **(Deny)**
- Redireccionar un pedido de conexión sin avisar al emisor **(Drop).**

El conjunto de estas reglas permite instalar un método de filtración dependiente de la política de seguridad adoptada por la organización. Se distinguen habitualmente dos tipos de políticas de seguridad que permiten:

- Permitir únicamente las comunicaciones autorizadas explícitamente: **"Todo lo que no es autorizado explícitamente está prohibido".**
- Impedir cualquier comunicación que fue explícitamente prohibida.

El primer método es el más seguro, pero requiere de una definición precisa de las necesidades de comunicación de toda la red.

Tipos de firewall

Básicamente, **existen dos tipos de firewalls**, destinados a diferentes tipos de infraestructuras de datos y tamaños de red.

- **Firewall por Software** (tanto aplicaciones gratuitas como pagas)
- **Firewall por Hardware** (Es decir mediante la utilización de dispositivos)

Firewall por software

Un firewall gratuito es un software que se puede instalar y utilizar libremente, o no, en la computadora. Son también llamados **"Desktop firewall"** o **"Software firewall".**

Son firewalls básicos para pequeñas instalaciones hogareñas o de oficina que **monitorean y bloquean, siempre que necesario, el tráfico de Internet**. Casi todas las computadoras vienen con un firewall instalado independientemente del sistema operativo instalado en ellas.

Las características de un firewall por software son:

- Los gratuitos se incluyen con el sistema operativo y normalmente son para uso personal
- Pueden ser fácilmente integrados con otros productos de seguridad
- No necesita de hardware para instalarlo en la computadora

- Es muy simple de instalar, normalmente ya viene activado y el Sistema Operativo alerta cuando no tenemos ningún tipo de firewall en funcionamiento.
- Un **firewall por software es lo más básico en materia de seguridad** que debe existir en una computadora y no hay razones que justifiquen la no utilización de, por lo menos, un desktop firewall.
- Un firewall comercial funciona de la misma forma que uno gratuito, pero normalmente incluye protecciones extra y mucho más control sobre su configuración y funcionamiento.

Firewall por Hardware

Una **firewall por Hardware** viene normalmente instalado en los routers que utilizamos para acceder a Internet, lo que significa que todas las computadoras que estén detrás del router estarán protegidas por un firewall que está incluido en el dispositivo. La mayoría de los routers vienen con un firewall instalado.

La configuración de un firewall por hardware es más complicada que una instalación de un firewall por software y es normalmente realizada a través del navegador que se utiliza para acceder a Internet. Cabe destacar que la d**iferencia de precio entre un router con firewall y un router sin firewall** es muy pequeña, por eso es recomendable comprar un firewall con esta protección.

Es posible tener un **firewall por hardware** y un **firewall por software** activos simultáneamente para lograr una mayor protección, pero tenemos que tener amplios conocimientos en el tema de seguridad para que todo ello cumpla con su función correctamente sin solaparse.

La importancia de un Firewall

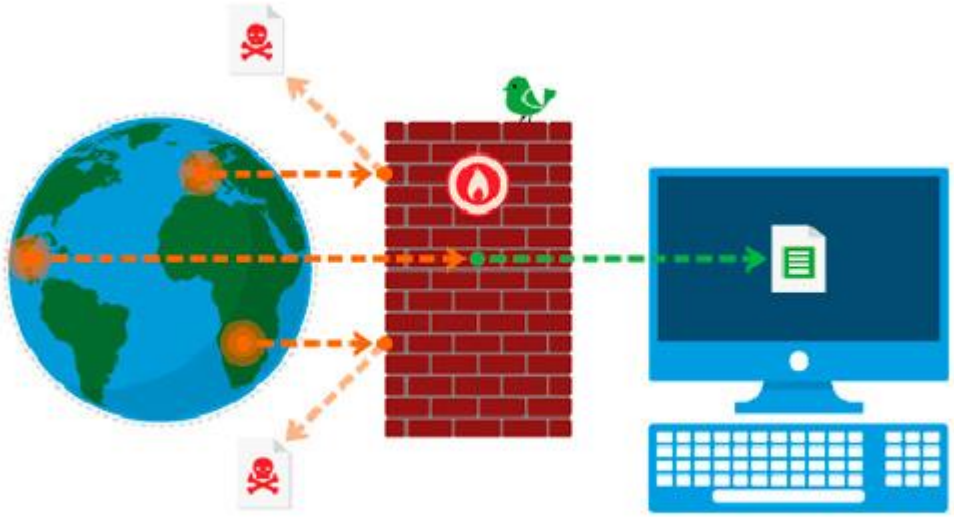
Uno de los aspectos fundamentales para **la seguridad de nuestra computadora es la instalación de un firewall junto con un antivirus de calidad.** Es importante instalar esta medida de protección cuando utiliza su computadora para el acceso a internet. El **firewall**

crea una barrera entre los datos privados de nuestra computadora y las amenazas externas que nos pueden atacar cuando estamos conectados a una red.

¿Es necesario tener un firewall?

La respuesta a este interrogante es inevitablemente sí, ya que **un firewall está diseñado para proteger nuestra PC de varios tipos de ataques, amenazas y malware** de todo tipo, incluyendo los siguientes:

- Gusanos, también denominados "worms", que se esparcen de computadora en computadora vía internet y después toman el control de su computadora.
- Los Hackers que deseen entrar en la computadora para tomar el control de la misma y hacer **"ataques disfrazados"** o robar datos personales que se encuentran en el disco rígido.
- Bloquea el tráfico de salida para no dejar que **determinados protocolos sean utilizados para esparcir los virus que pueda llegar a tener su computadora.**



Por sí sólo, **un firewall no impide todos los ataques,** pero si no tuviera ninguno instalado, basta con conectarse a Internet para que la probabilidad de ser infectado en pocos minutos sea grande. **Un firewall no protege la computadora en casos como virus, spam y spyware.** Es la última defensa cuando revelamos nuestras contraseñas, o si permitimos la entrada de agentes externos como malware en aplicaciones.

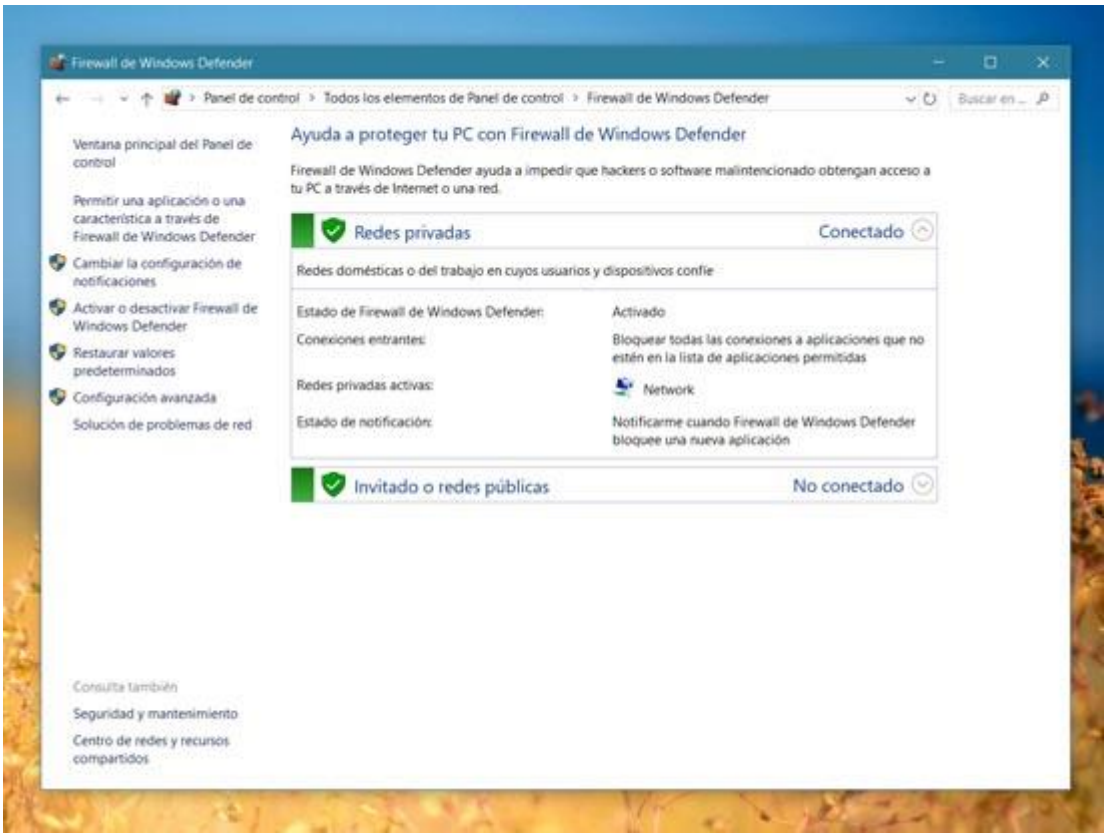
En este punto debemos tener en cuenta que **un firewall sin otro tipo de protección no garantiza una protección completa** (de hecho, actualmente nada garantiza seguridad 100% completa). Por ello, aunque nos encontremos en redes protegidas, como es el caso de

las redes empresariales y hasta de los ISP, siempre debemos activar un firewall en nuestra computadora para tener mayor protección.

Consejos para usar el Firewall en Windows 7, Windows 8 y Windows 10

En estos tiempos en que la actividad delictiva en Internet está llegando a límites insospechados, una de las mejores herramientas con la que podemos contar para **prevenirnos de cualquier ataque proveniente del exterior es la utilización de un buen Firewall.**

Si bien en el mercado existen alternativas más completas y avanzadas, lo cierto es que las versiones de Windows más modernas traen por defecto incluido **Windows Firewall,** una fantástica herramienta de seguridad que nos permitirá estar siempre protegidos cuando nos conectamos a la red de redes sin complejas configuraciones y además sin pagar extra por un software de terceros.



Una de las mejores funcionalidades con las que podemos contar es la posibilidad de **establecer de forma precisa diversos modos de** protección que nos servirán para estar a salvo en cualquier situación en la que nos encontremos trabajando, además de un muy bien trabajado centro de control con todas las opciones y accesos necesarios debidamente organizados y completamente a disposición del usuario.

Además, ahora también es posible **definir un rango de puertos o direcciones IP específicas o precisar que conexiones entrantes deben cumplir con el protocolo IPsec.**

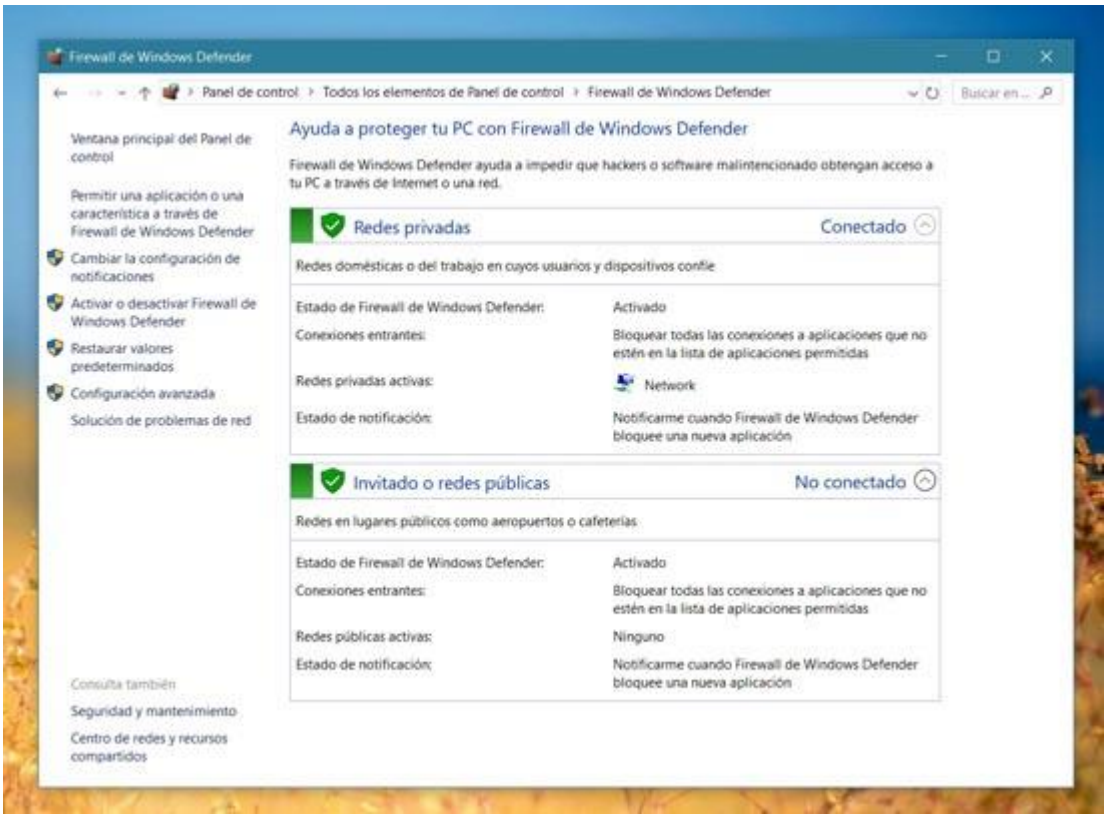
Opciones de configuración y opciones avanzadas del Firewall de Windows

Paso 1

Para lograr tener a nuestra disposición todas las opciones del Firewall de Windows, nos desplazamos hasta el menú Inicio y pulsamos sobre Panel de Control.

Paso 2

Nos dirigimos hacia el apartado “Sistema y seguridad” en donde pulsaremos sobre “Firewall de Windows”.



Paso 3

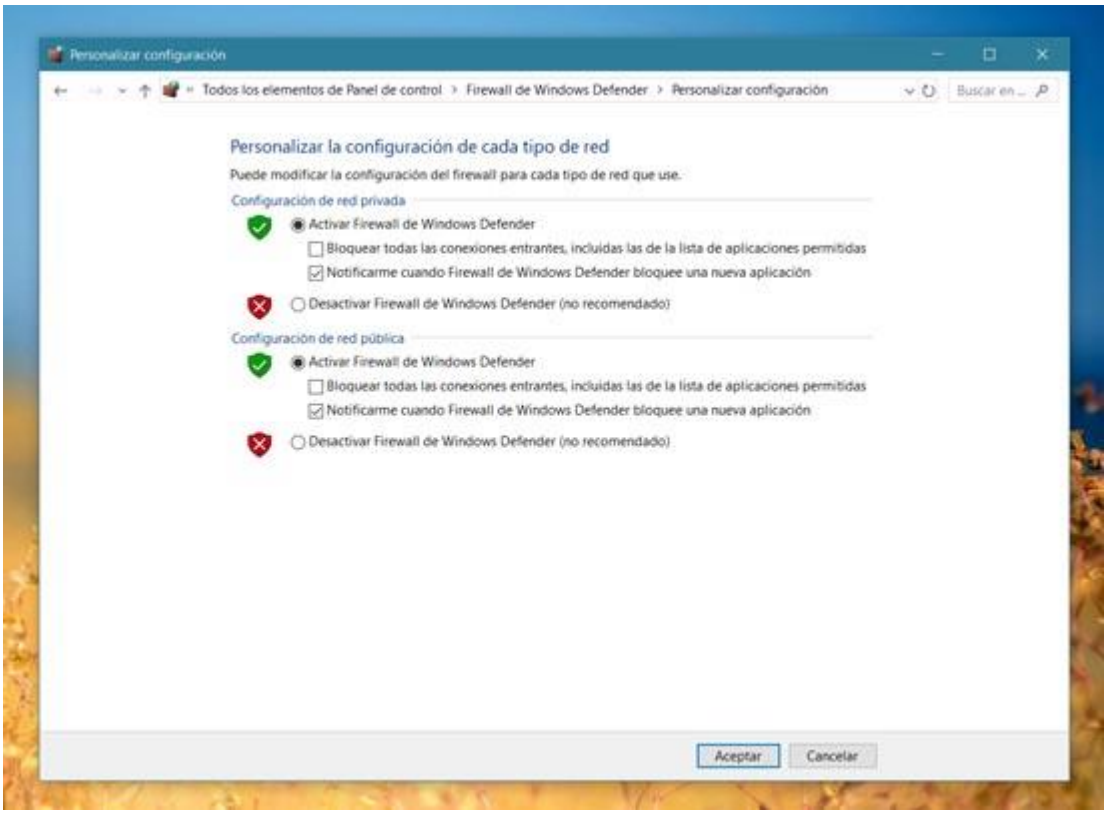
En la pantalla que se presenta tendremos a nuestra disposición las opciones para activar o desactivar el Firewall de acuerdo a la clasificación de las redes a las que nos conectamos.

Cabe destacar que el firewall de Windows ofrece cobertura para tres tipos de redes diferentes:

- Red Dominio.
- Red Pública.
- Red doméstica o de trabajo (Red Privada).

El tipo de red y los parámetros de protección serán seleccionados al momento de conectarnos a la misma.

Entre las funciones con las que podemos contar en este apartado, es importante señalar que tendremos la posibilidad de **ajustar las opciones predeterminadas por cada tipo de red por separado, además de determinar si desactivamos el Firewall,** el control de las notificaciones de bloqueo o el bloqueo en un sólo paso de todas las conexiones entrantes.



Una de las características más interesantes del **Firewall de Windows** es la posibilidad que nos brinda de emplear más de un perfil simultáneamente, es decir, si nuestra computadora se encuentra conectada a una red de trabajo y a una red del tipo pública al mismo tiempo, **el Firewall será capaz de aplicar la configuración que corresponda a las distintas conexiones entrantes,** de acuerdo al tipo de red desde la que provenga.

También una muy útil función es la posibilidad de crear nuevas reglas de conexión para cada tipo de red desde la sección del Firewall en el Panel de Control.

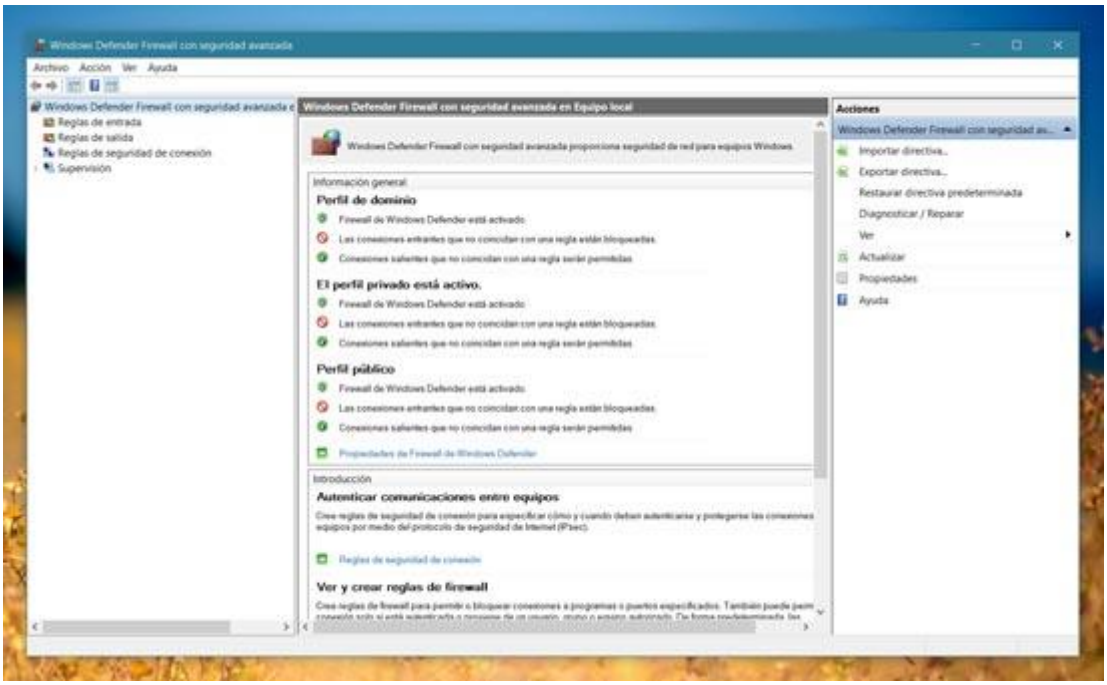
Cómo crear o modificar una regla en el Firewall de Windows

Paso 1

En Firewall de Windows, pulsamos sobre **“Configuración avanzada”.**

Paso 2

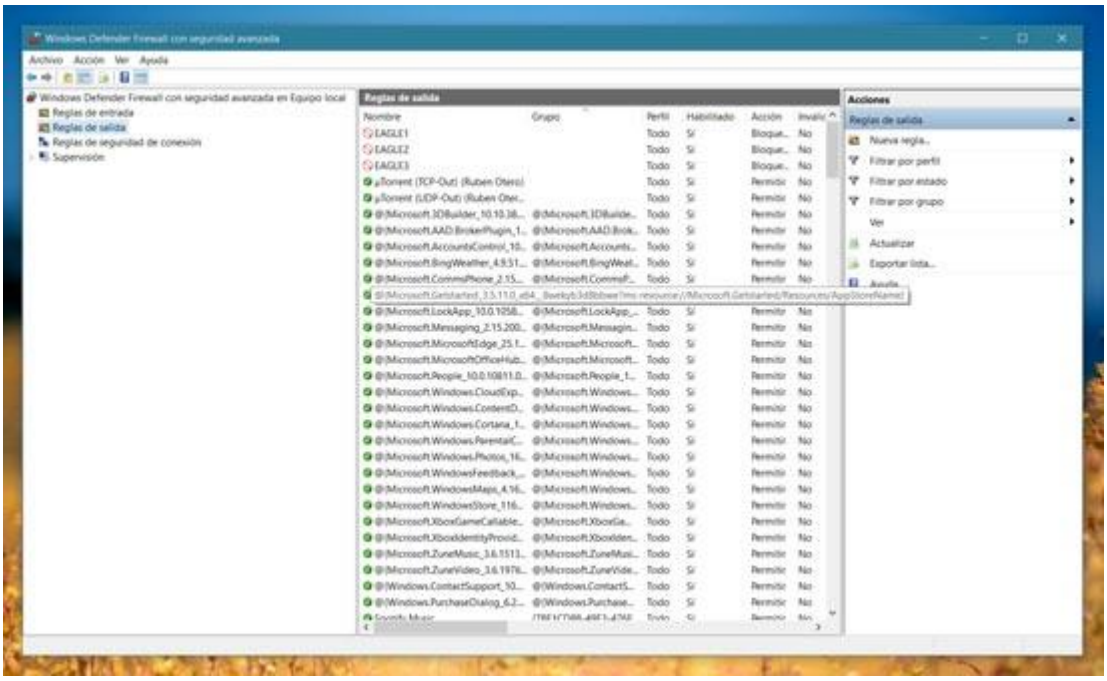
Nos desplazamos hasta el apartado **“Ver y crear reglas de Firewall”** y pulsamos sobre los ítems **“Reglas de entrada”** o en **“Reglas de salida”** para poder acceder y crear una nueva regla o modificar una existente.



Como abrir los puertos del Firewall de Windows

Como sabemos, **cualquier conexión que entra o sale desde nuestra computadora a Internet,** es gestionada mediante la utilización de los denominados Puertos, los cuales sirven para que nuestra PC interactúe con el exterior, como por ejemplo en el caso de los juegos online o los programas de intercambio P2P.

Estos puertos son absolutamente necesarios para que dichas aplicaciones funcionen y se conecten con Internet correctamente, pero **el Firewall de Windows en forma predeterminada sólo ofrece canales de entrada y salida a programas y servicios indispensables** para que el sistema operativo brinde un correcto funcionamiento.



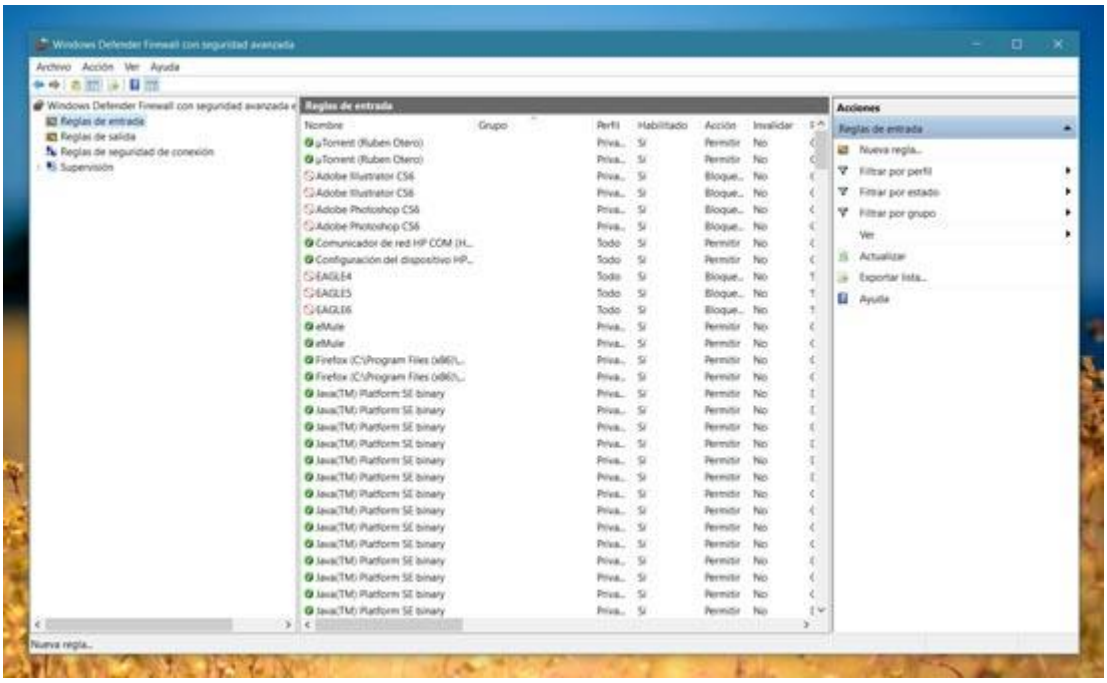
A lo largo de esta guía vamos a explicar los pasos necesarios para poder **abrir los puertos en el Firewall de Windows** para que nuestros programas se puedan conectar perfectamente.

Paso 1

En primera instancia debemos desplazarnos hasta el “Panel de Control de Windows”, “Sistema y Seguridad” y allí **ejecutar el Firewall de Windows.**

Paso 2

En el panel de la derecha, pulsamos sobre **“Configuración Avanzada”** y en la ventana que se presenta, seleccionamos **“Regla de entrada”.**

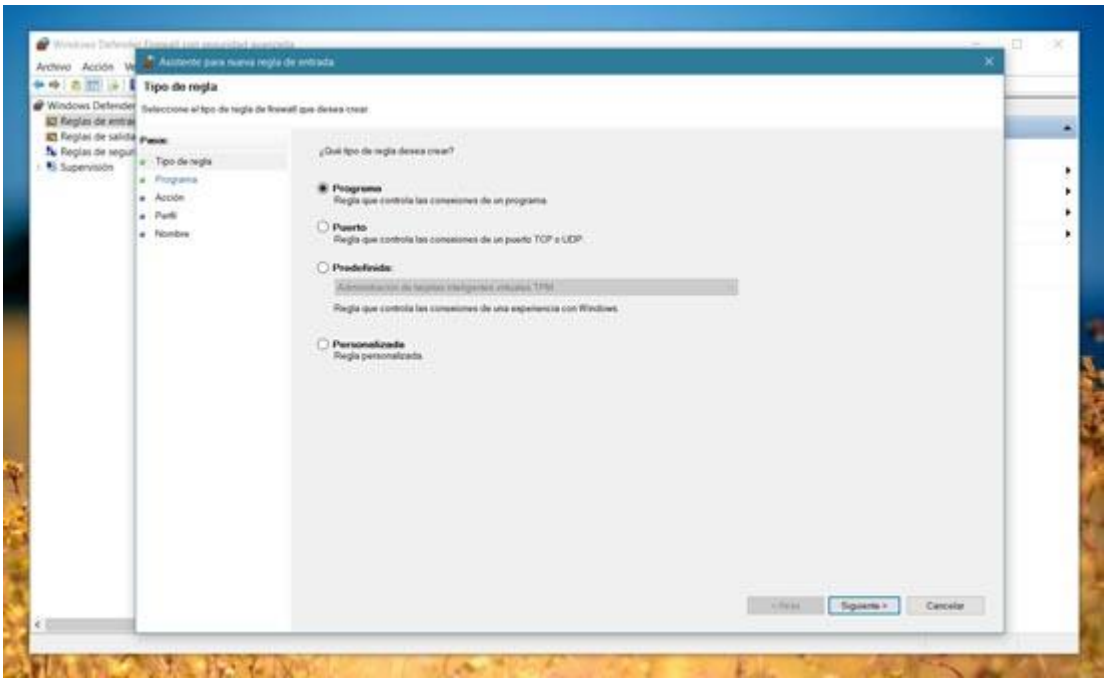


Paso 3

En este punto, el sistema nos mostrará todas las configuraciones de acceso de los **programas gestionados por el Firewall de Windows.** Cabe destacar que podemos optar por brindar acceso total a las conexiones que requiere determinada aplicación o solamente abrir los puertos que realmente son necesarios.

Paso 4

Si optamos por abrir sólo los puertos requeridos, por cierto la opción recomendada, debemos pulsar sobre el botón **“Nueva regla”,** y en la ventana que aparece pulsamos sobre **“Puertos”,** lo único que resta es **indicarle al Firewall de Windows los puertos que deseamos abrir.**



Paso 5

Asignamos un nombre al perfil y le indicamos a qué tipo de red debe ser aplicada la regla que recién acabamos de crear.

Paso 6

Pulsamos sobre **“Finalizar”** y a partir de este punto podremos disfrutar de nuestras aplicaciones preferidas debidamente conectadas a Internet.