MICROAREA

Firewall de Windows

Guía para configurar el cortafuegos de Windows y trabajar en red

MANUAL PARA LA CONFIGURACIÓN DEL FIREWALL DE WINDOWS

MICROAREA DESARROLLOS INFORMÁTICOS, S.L.U.

info@microareanext.com | www.microarea.es

Índice General

Consideraciones previas

El presente manual será de aplicación únicamente a los usuarios que trabajen exclusivamente en red. Aquellos cuya configuración sea del tipo monopuesto (servidor) o trabajan en un solo ordenador no será de utilidad puesto que no será necesario configurar el cortafuegos para trabajar con normalidad.

El programa necesita una base de datos donde guardar los datos introducidos y poder interactuar con ellos (en nuestro caso el motor de base de datos es el SQL Server desarrollado por Microsoft). Dicha información estará almacenada físicamente en un ordenador, que será el que actúe como servidor[1] y éste será el que proporcionará y gestionará esos datos a los distintos ordenadores que pueda haber en la red, denominados clientes[2], de forma que todos puedan tratar con la información almacenada.

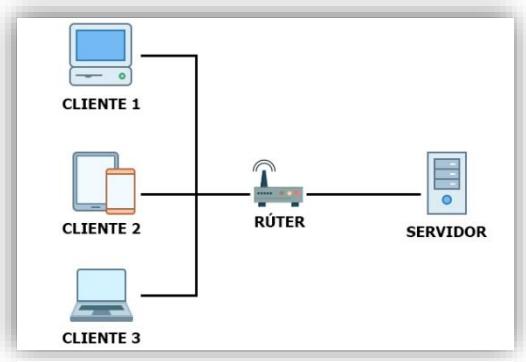

Ilustración 1: Funcionamiento del programa (Arquitectura Cliente-Servidor).

En términos informáticos, esta característica, o forma de trabajar, se denomina «Arquitectura Cliente-Servidor». Técnicamente hablando, los ordenadores clientes, mediante el uso de la red (interna o externa, privada o pública) y una conexión TCP/IP a un puerto determinado del ordenador actuante como servidor, realizan una petición (de lectura, escritura, modificación o eliminación) el cual la gestiona y ejecuta. En la *ilustración 1*, podemos ver una representación gráfica del funcionamiento general de esta forma de trabajo.

Por este motivo, ya que para poder acceder a la información el cliente ha de conectarse contra el servidor y a la base de datos instalada allí, **el** ordenador que actúa como **servidor siempre deberá estar encendido** (no hace falta que esté iniciada la sesión).

Por cuestiones relacionadas con la seguridad, de forma predeterminada todos los Windows (sin importar la versión) tienen bloqueadas las conexiones a la base de datos (para prevenir un posible ataque fraudulento no autorizado). Esto producirá un error de conexión cuando los ordenadores clientes se conecten al servidor, por lo que resulta mandatorio realizar una configuración previa dejando acceso a la base de datos. El encargado de establecer este control es el cortafuegos de Windows (o cualquier software de seguridad que asuma su función[3]).

La conexión a la base de datos **no tiene nada que ver** con **tener acceso** a las **carpetas compartidas**. De hecho, son dos formas totalmente distintas de acceder a diferentes recursos del servidor. Las carpetas compartidas son básicamente un repositorio de ficheros, mientras que, en caso del programa, debe establecerse una conexión bidireccional a una base de datos. Por tanto, por el mero hecho de poder compartir ficheros en la red, no implica necesariamente que podamos trabajar en red con el programa automáticamente.

AVISO IMPORTANTE:

Aunque es preferible disponer de conocimientos genéricos informáticos, no son realmente exigibles, dado que la configuración del cortafuegos de Windows no es una cuestión realmente complicada. No obstante, siempre podrá contar con la asistencia de su informático de confianza.

[1] Se denomina servidor no porque sea un Windows Server, sino porque será el que «servirá» la información a otros ordenadores.

[2] Necesitan de un ordenador que actúe como servidor para poder obtener acceso a los datos almacenados.

[3] Aunque en el presente manual solo nos centraremos en el cortafuegos del propio Windows.

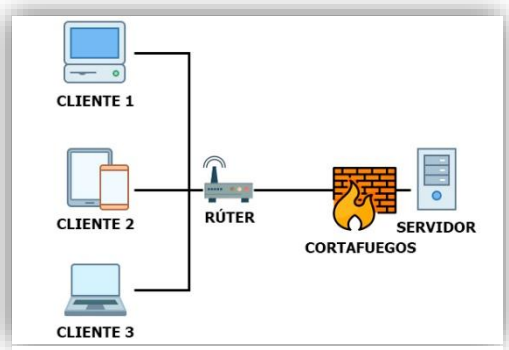

Ilustración 2: Funcionamiento de un Firewall (Cortafuegos) en una red local.

En la *ilustración 2*, podemos ver esquematizado en una gráfica cual es el funcionamiento exacto de un cortafuegos. Como su nombre indica, no es más que un programa informático que actúa de «frontera» o «barrera [4] » controlando el acceso al ordenador «protegido» de forma que puede discriminar, aceptar y declinar el «tráfico[5]» permitiendo o denegando el acceso a recursos compartidos (como carpetas y documentos) o a programas y aplicaciones instaladas (como en este caso, la base de datos).

Por tanto, el motivo de este manual es configurar debidamente el cortafuegos de Windows para permitir el acceso de los puestos de red (clientes) a la base de datos/servidor y poder trabajar con uno o varios programas de Microarea (Magest, Maconta, EosWin, Winlab o Expedientes). **Esta configuración solo deberá hacerse en el servidor**, dado que en los puestos de red/clientes no es necesario.

¿Cómo configurar el Firewall de Windows?

Básicamente la configuración es muy sencilla, dar acceso a la base de datos mediante la inclusión de dos aplicaciones, pertenecientes a ésta, en la lista blanca (lista de aplicaciones permitidas) del cortafuegos.

No obstante, antes de poder empezar y configurar como tal el cortafuegos, hay que averiguar dónde está instalada la base de datos (SQL Server) y por tanto donde se encontrarán los ficheros necesarios para poder incluirlos en la citada lista blanca. Además, también deberemos determinar el tipo de red que se le asignó a Windows, puesto que en las especificaciones del cortafuegos será un dato totalmente necesario y obligatorio.

¿Dónde está el SQL Server instalado?

Para localizar la ubicación de la base de datos habrá que acceder a los servicios de Windows y encontrar la entrada "SQL Server (XXX[6])". La forma más sencilla y rápida será pulsando la tecla Windows (⊞), y mientras se mantiene pulsada, apretar la tecla "R". Esto hará que aparezca en pantalla una ventana emergente denominada «Ejecutar». En ella escribiremos «services.msc» (sin comillas) tal y como se muestra en la *ilustración 3*.

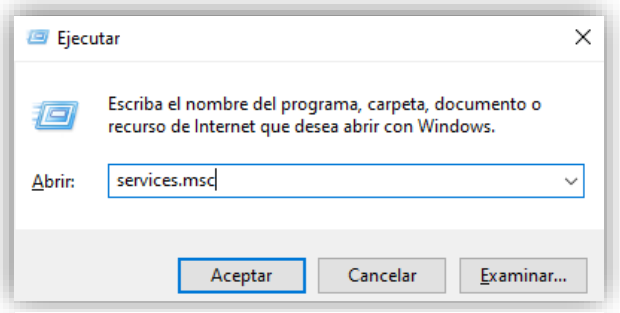

Ilustración 3: Ventana ejecutar para ver los servicios.

[4] Traducido literalmente «pared de fuego».

[5] Las peticiones, conexiones o cualquier solicitud, entrantes o salientes de un ordenador.

[6] Nombre de la instancia, podrá ser ICAM, ICAV o ICAB para las versiones de los colegios de abogados de Madrid, Valencia o Barcelona o bien MSSQLSERVER para las versiones comerciales.

Tras pulsar sobre el botón «Aceptar» se abrirá otra ventana con la lista de los servicios de Windows, *ilustración 4*. Es posible que, dependiendo de las características del ordenador, pueda demorarse la visualización un poco, por lo que si tarda en aparecer no representará ningún problema.

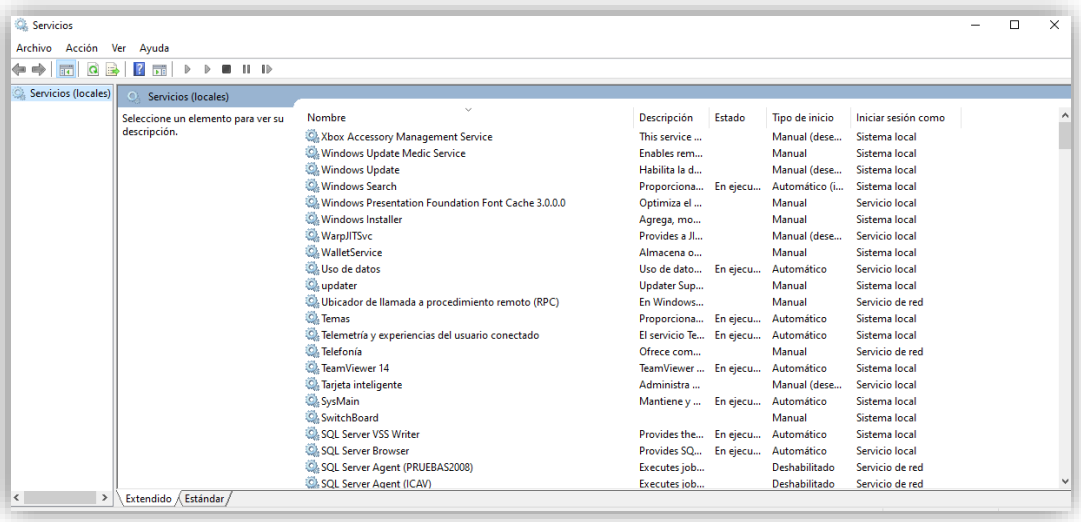

Ilustración 4: Servicios de Windows.

A continuación, se localizrá la fila comentada en el párrafo anterior, esto es «SQL Server (XXX)». Para mejorar la búsqueda, es posible pulsar sobre el título de la columna, en este caso «Nombre», para que la lista sea ordenada alfabéticamente y permita una búsqueda más sencilla.

Ilustración 5: Ejemplo de servicio del SQL Server, en este caso, se trata de la versión ICAM.

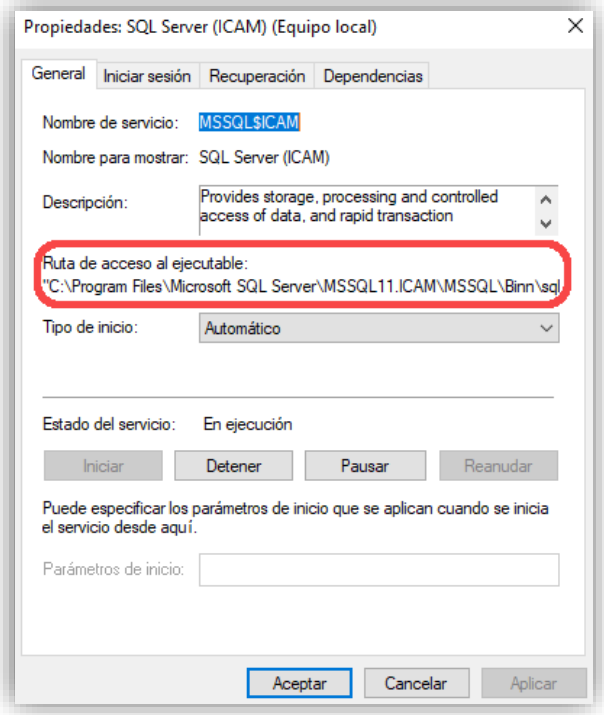

Ilustración 6: Ruta donde está instalado el SQL Server.

Cuando localicemos la línea, solo habrá que hacer clic derecho ( ) sobre ella y en la ventana que habrá aparecido por pantalla con un menú, hacer clic izquierdo ( ) sobre la opción «Propiedades». A continuación, localizaremos el texto «Ruta de acceso al ejecutable», situado en la parte central de la ventana, tal y como se muestra en la *ilustración 6*.

En esa sección de la ventana, estará la ubicación, o ruta, exacta de la instalación de la base de datos. Por tanto, tendremos que anotar o recordar dicha ruta, pues será necesaria en el paso siguiente.

Para facilitar la tarea, la ventana permitirá copiar el texto si éste previamente es seleccionado con el ratón. Una vez seleccionado, podría ser copiado, bien haciendo clic derecho ( ) y «copiar» o

bien usando los atajos del teclado (Control + C). Para recuperarla, por ejemplo, sería posible abrir un bloc de notas o un Word y pegar lo copiado.

¿Qué ficheros deben ser permitidos?

Dos son los ejecutables que deben ser añadidos a la lista de aplicaciones permitidas en el cortafuegos. El motor de base de datos (SQLBrowser) y la propia base de datos (SQLServ):

Sqlbrowser.exe

Función: Gestionar el acceso al SQL en la red interna o pública.

Ubicación: C:\Program Files (x86)\Microsoft SQL Server\90\Shared[7]

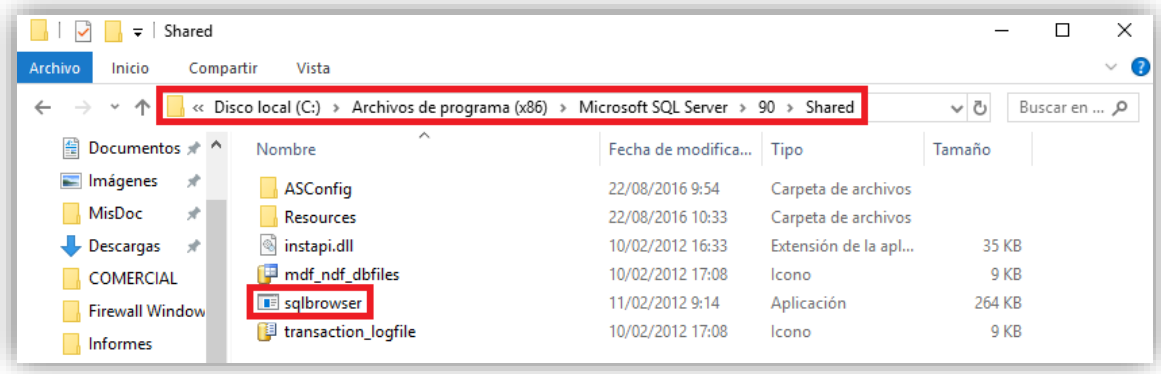

Ilustración 7: Ubicación de la aplicación "SQL Browser".

Sqlservr.exe

Función: Trabajar con la información almacenada en la base de datos.

Ubicación: Ruta de acceso al ejecutable, para más información, ver ¿Dónde tengo el SQL instalado?.

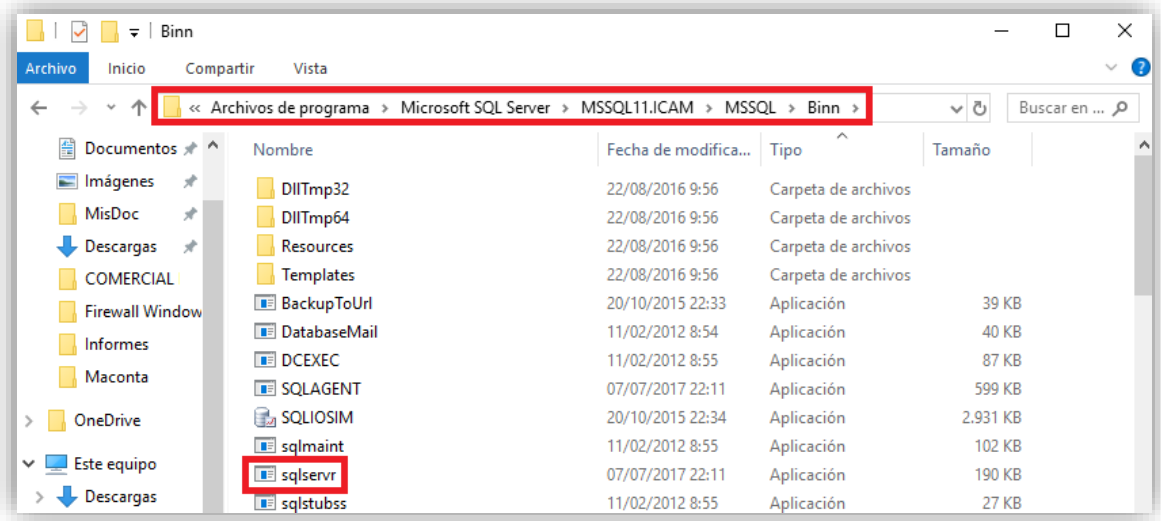

Ilustración 8: Ejemplo ubicación de la aplicación "SQL Server".

[7] Program Files es el nombre de la carpeta que Windows le da a «Archivos de Programa» en los Windows anteriores a Windows 8 o que están en inglés.

Tipos de redes locales (Windows)

Para poder crear la excepción en el cortafuegos, es necesario saber el tipo de red que está establecido en cada ordenador de la red en la que se está trabajando (cliente) y en el servidor, pues será un dato indispensable en la configuración del propio cortafuegos. Técnicamente, deberían tener todos los ordenadores de la red local, el mismo tipo de red configurada para evitar problemas de red.

La primera vez que Windows se conecta a una red, ya sea por cable o Wifi, Windows solicita que se le indique el tipo de red que es, en otras palabras, nos solicita información sobre las propiedades y características de la misma. De esta manera, podrá aplicar cierto nivel de privacidad y seguridad de forma automática predeterminando, limitando o incluso desactivando automáticamente algunas opciones de red. Por ejemplo, si nos conectamos a una red abierta (como un punto Wifi gratis sin contraseña) o pública (como la de un restaurante con contraseña) estableciendo, consecuentemente, la red como tipo pública, la detección de redes, las carpetas y recursos compartidos estarán desactivados, protegiendo nuestro ordenador del resto, sin que la navegación por internet se vea afectada. No obstante, no conviene olvidar que, aunque «aislados» no significa que se esté totalmente protegido contra cualquier eventualidad o que el ordenador no sea accesible desde la red por otros métodos. Simplemente se trata de una primera línea de defensa.

Los dos únicos tipos de red son:

Red privada: Aquellas de confianza, como pudiera ser la red de casa o de la oficina.

Red Pública: Redes de acceso público o libre de dudosa confianza, como un bar o restaurante.

Ilustración 9: Tipos de red antiguos.

No obstante, en versiones anteriores a Windows 8 y 8.1, la denominación de red privada recibía un nombre diferente, se dividía entre red doméstica (u hogar) y red de trabajo. Ambas funcionaban de manera casi idénticas, únicamente variaba en la ubicación, permitiendo así una diferenciación a la hora de la configuración del cortafuegos. De esta forma, podrían crearse reglas y excepciones a tres niveles, red doméstica (privada), trabajo (privada) o pública.

Si trabajásemos con un Windows Server, seguramente tendremos un tipo de red más, la denominada «dominio». Esta es una red exclusiva de los servidores dedicados que gestiona todos los ordenadores/usuarios de la red formando un dominio con características y peculiaridades específicas para obtener el máximo rendimiento y eficiencia de una red. No obstante, generalmente este tipo de redes son gestionados por un informático, por lo que sería este quien debería gestionar la lista blanca del cortafuegos.

¿Es importante tener bien configurado el tipo de red?

Evidentemente es un factor importante, aunque no tanto decisivo en la seguridad, puesto que, aunque el tipo de red determina unas características y funcionalidades, no constituye la defensa del ordenador, por lo que no podrá asumir las funciones de un antivirus o cortafuegos. No obstante, de cara al uso del programa, es determinante puesto que en la configuración del cortafuegos es un dato para configurar.

DUDA: ¿Cómo sé si la red es pública o privada?

Dependerá de la opción que se eligió cuando se hizo la primera conexión a la red. Para poder saber qué tipo de red marcó, podrá hacerlo desde panel de control y «Centro de redes y recursos compartidos». Allí verá las conexiones de red existentes y el tipo de cada una de ellas.

Una vez clarificada la diferencia entre un tipo de red y otra, no resta más que identificar el tipo de red que tenemos en el ordenador.

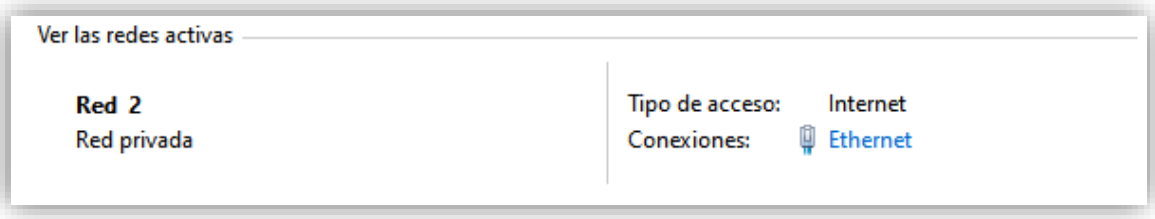

Ilustración 10: Ejemplo tipo de red.

Por ejemplo, en la *ilustración 10*, queda patente que la red «Red 2» es de tipo privada, adicionalmente se nos informa que la conexión a la red (y por tanto a internet) se realiza mediante cable (Ethernet). Si nos hubiéramos conectado a una red inalámbrica, indicaría «Wifi».

Configuración del Firewall

Una vez ya tenemos claro qué programas debemos agregar a las exclusiones (lista blanca) y el tipo de red establecido, ya es posible configurar correctamente el cortafuegos. Recuerde que operará y **configurará** el **cortafuegos bajo su** total **responsabilidad** y que únicamente deberá seguir estos pasos en el PC servidor.

Para lanzar la configuración del cortafuegos deberemos ir al panel de control y desde allí elegir la opción «Firewall de Windows Defender»:

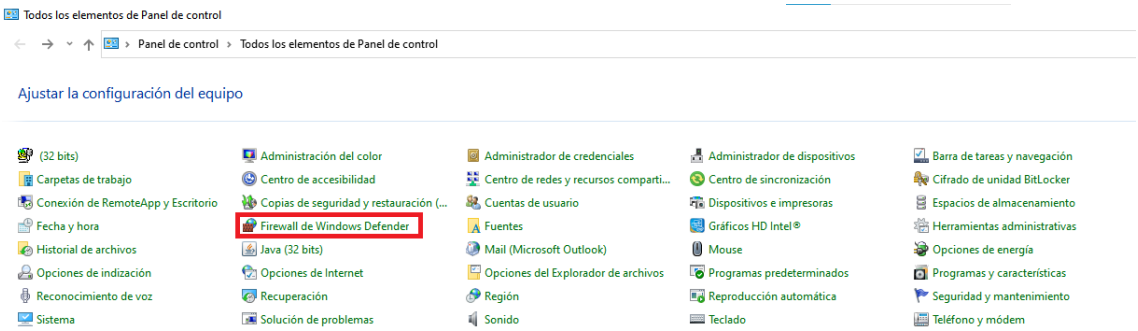

Ilustración 11: Diferentes opciones que componen el panel de control.

Otra forma de acceder y quizás más fácil, es hacer clic ( ) en la búsqueda de Windows[8].

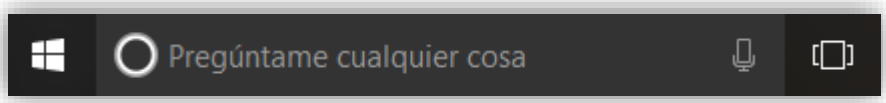

Ilustración 12: Barra de búsqueda de Windows 10.

[8] En este caso, al tratarse de Windows 10 u 11 la búsqueda aparecerá en la barra de tareas. En Windows 7 y 8 aparecerá la barra de búsqueda al pulsar sobre la tecla "Inicio" ( ).

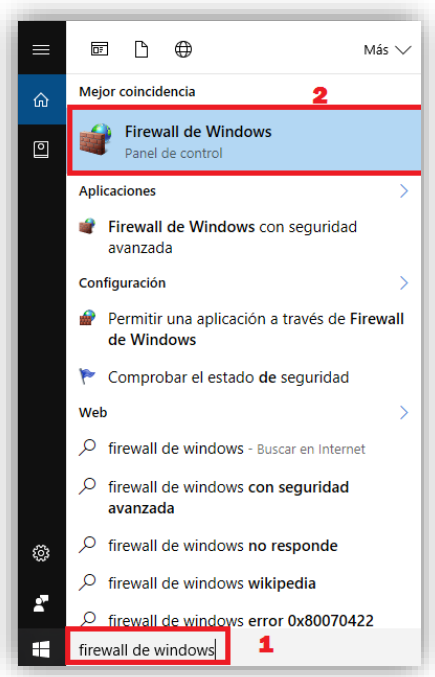

Ilustración 13: Resultado de la búsqueda.

y, a continuación, en el área habilitada para realizar las búsquedas, generalmente en forma de caja de texto, escribir «Firewall de Windows» (sin las comillas) para que comience la búsqueda (Punto **1**, *ilustración 13*). Conforme vaya escribiendo se irá actualizando la lista de resultados, de forma que es posible que aparezca el resultado antes de completar todas las palabras. En versiones de Windows antiguas (Windows 7 y posteriores) el mecanismo de búsqueda es posible que difiera y haya que pulsar alguna tecla o botón para ejecutar la búsqueda.

En cualquier caso, una vez la búsqueda ha sido completada, y por tanto aparezca «Firewall de Windows» como «aplicación» o «Panel de Control», pulsaremos sobre el resultado tal y como queda ilustrado en el punto **2**.

Es posible que obtenga más de un resultado de búsqueda, e incluso resultados que pudieran estar relacionados, como accesos directos que nos lleven a ventanas de configuración específica que más tarde podrían ser de interés. No obstante, por motivos evidentes deberemos ceñirnos estrictamente a los pasos aquí indicados.

En cualquier caso, se abrirá la ventana con el menú principal del cortafuegos. Como puede observarse, aparecerá indicado, de forma bastante llamativa, el estado del firewall (**verde** activo, **rojo** desactivado) para cada tipo de red, puesto que Windows, tiene un cortafuegos por cada una de ellas. Tan sólo habrá que hacer los cambios en la red indicada en la sección anterior (En caso de tener algún ordenador de la red con un tipo diferente de red, habrá que unificar criterio y tener todos bajo el mismo tipo de red).

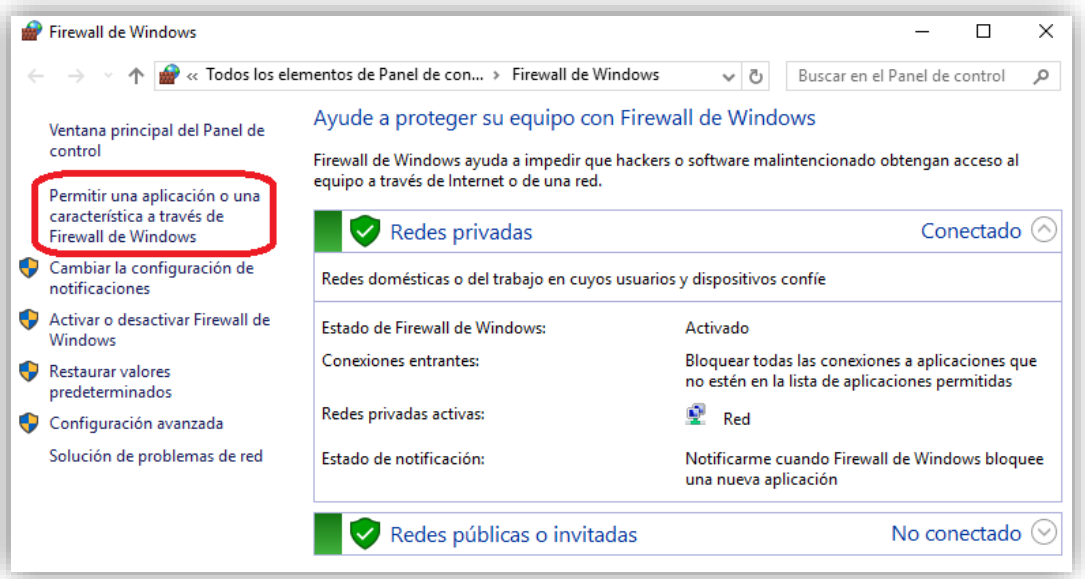

Ilustración 14: Cortafuegos (Firewall) de Windows.

Nótese que puede tener instalado un antivirus y este puede estar controlando el cortafuegos, como el aviso ilustrado en la *ilustración 15*, en tal caso deberá contactar con el departamento de soporte del

antivirus, o con su informático, puesto que no podrá alterar el funcionamiento del cortafuegos de Windows. No obstante, los elementos a indicar en la lista blanca no varían.

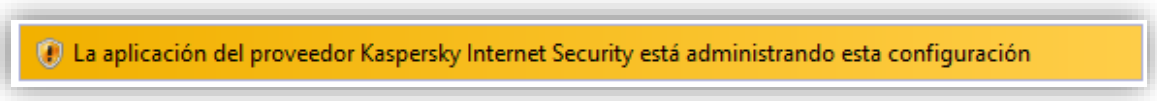

Ilustración 15: Aviso indicando que el cortafuegos está siendo controlado por un antivirus externo a Windows.

AVISO IMPORTANTE:

Es posible que se le esté notificando que la gestión del cortafuegos está derivada a su antivirus (*ilustración superior*). En ese caso, no continúe con el manual y póngase en contacto con el soporte técnico del antivirus (o su informático) para comentarle la necesidad de poder conectar un puesto de red, mediante una conexión SQL Server, al servidor y de esta manera puedan solventar la situación.

Para añadir las aplicaciones en la lista blanca, habrá que pulsar sobre la opción «Permitir una aplicación o una característica a través de Firewall de Windows», como se indica en la *ilustración 14*.

En la nueva ventana, aparecerá una lista con todas las aplicaciones, con regla propia, permitidas por el cortafuegos, delimitando su acceso en función del tipo de red (Privada y/o Pública). Por defecto, no será posible realizar ningún cambio dado que las opciones están deshabilitadas, no obstante, no hay de qué preocuparse, al pulsar sobre el botón «Cambiar configuración» se habilitarán todas las opciones de la ventana.

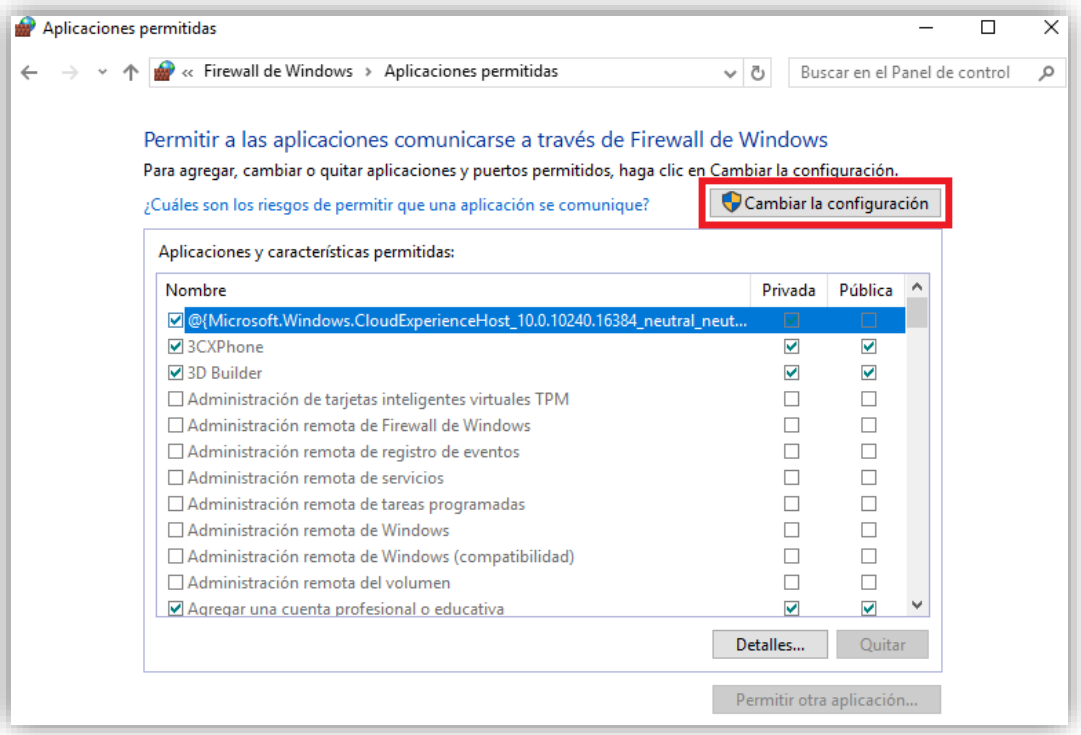

Ilustración 16: Lista blanca (Aplicaciones permitidas) del Firewall.

El funcionamiento básico de esta lista blanca podría compararse, a modo de burdo símil, con un evento social de gran magnitud (como un preestreno de cine o asistir a una gala benéfica), solo aquellos que tuvieran debidamente acreditada la asistencia estarían autorizados a acceder al recinto y al evento.

Como ya vimos, existen dos tipos de redes y por tanto sendos tipos de cortafuegos. En relación con esto, pudiera darse la situación que, tras configurar el cortafuegos (o existiendo una previa) aún no pudiera conectarse contra el servidor. Esto podría deberse a que el tipo de red marcado no es el correcto, es decir, está marcado «privada» cuando la red se definió como «pública» (o viceversa), por tanto, el bloqueo persiste. Para solventar el problema, solo habría que comprobar qué tipo de red es la que se tiene definida (lo ideal es que todos los ordenadores tengan la misma) y corregir el tipo de red, ya sea en el cortafuegos o en el ordenador problemático.

NOTA INFORMATIVA:

Recuerde, para realizar cualquier cambio será necesario disponer de los permisos de Windows avanzados (administrador) por lo que deberá hacer los ajustes con un usuario que disponga de ellos.

El siguiente paso, será pulsar sobre el botón «Permitir otra aplicación» para añadir las aplicaciones a la lista de aplicaciones permitidas y especificar a qué tipo de red tendrá acceso o se permitirán las conexiones.

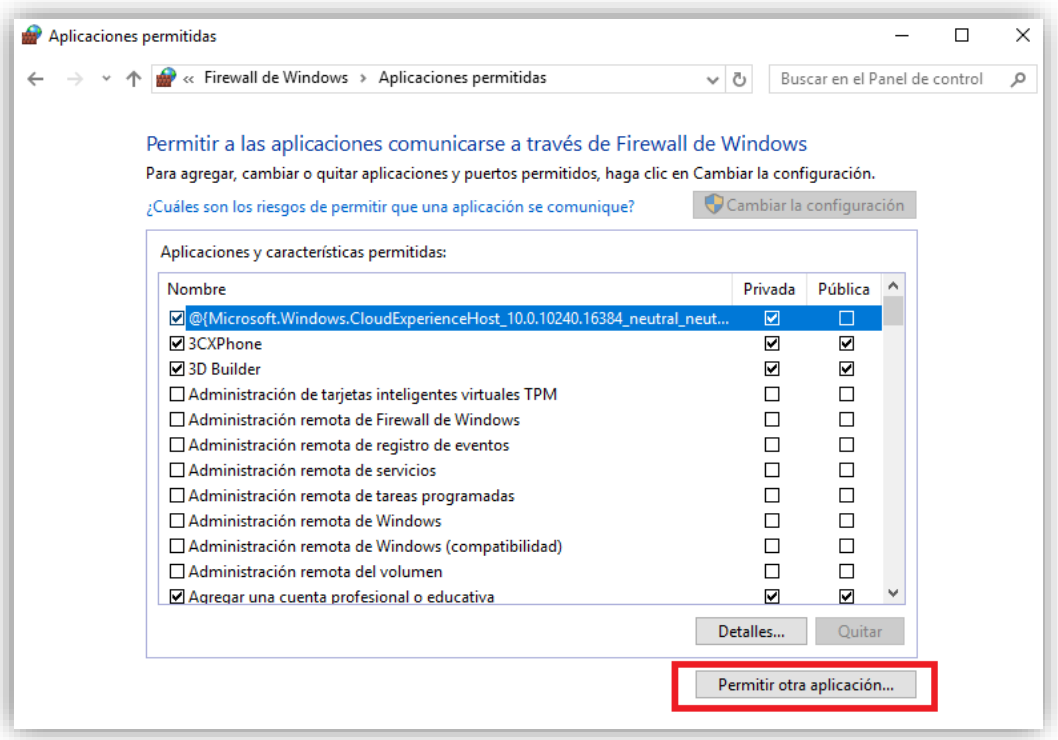

Ilustración 17: Modificación de la lista blanca (Aplicaciones permitidas).

Se abrirá una ventana, en la que habrá que pulsar sobre el botón de «Examinar» para buscar los dos ejecutables necesarios:

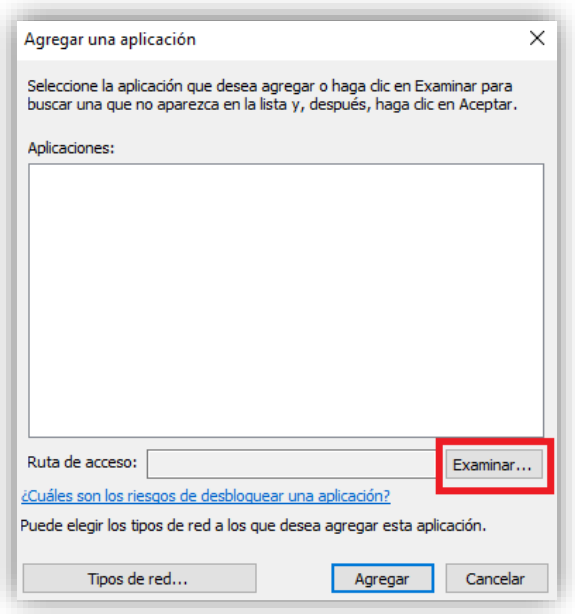

Ilustración 18: Cuadro de diálogo para la inclusión de una aplicación.

El primer fichero para buscar será el «sqlbrowser.exe», si no recuerda la ruta, consulte ¿Dónde está el SQLBrowser?. Únicamente habrá que localizar y clicar sobre el ejecutable. Seguidamente, para finalizar, habrá que pulsar sobre el botón «Abrir», tal y como se muestra en la *ilustración 19*.

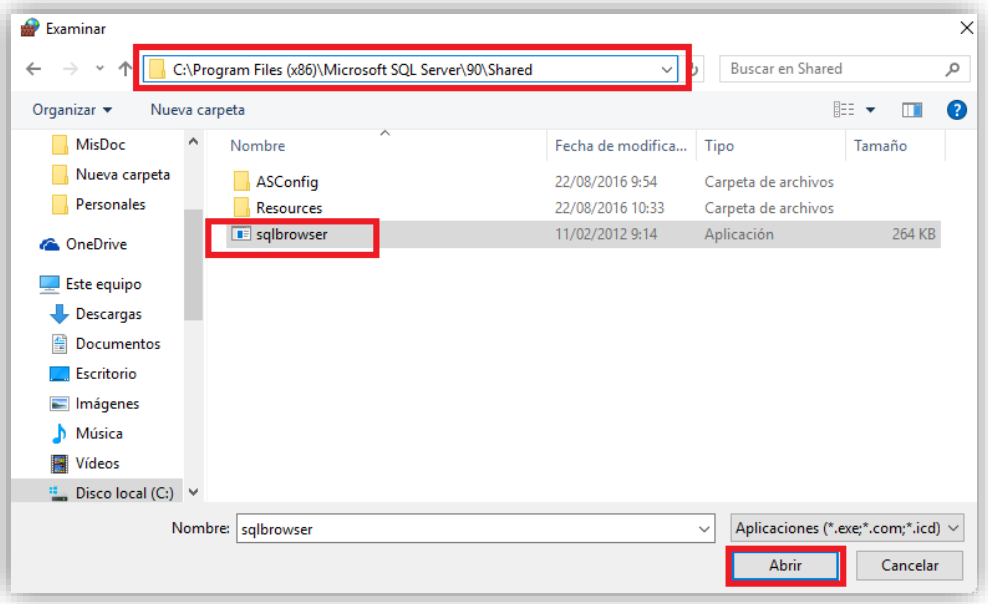

Ilustración 19: Cuadro de diálogo para la selección de la aplicación.

A continuación, tendremos en pantalla un resumen de la aplicación seleccionada, deberemos pulsar sobre el botón «Agregar» para añadir la excepción a la lista.

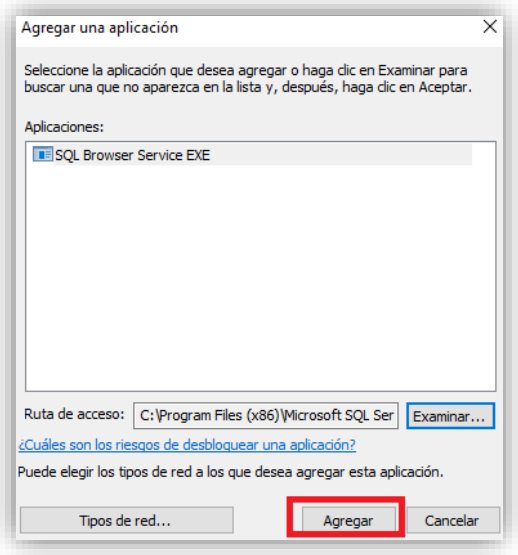

Ilustración 20: Cuadro de diálogo para agregar la aplicación.

Tras haber acepado, la pantalla inicial de la configuración volverá a ser mostrada, pero esta vez con la lista con los programas permitidos actualizada. Haciendo clic (para seleccionar) sobre la línea del elemento agregado, sólo restará marcar sobre el tipo de red [9] correspondiente. De esta forma, habremos acabado con el primer ejecutable que tenemos que agregar a la lista de aplicaciones permitidas.

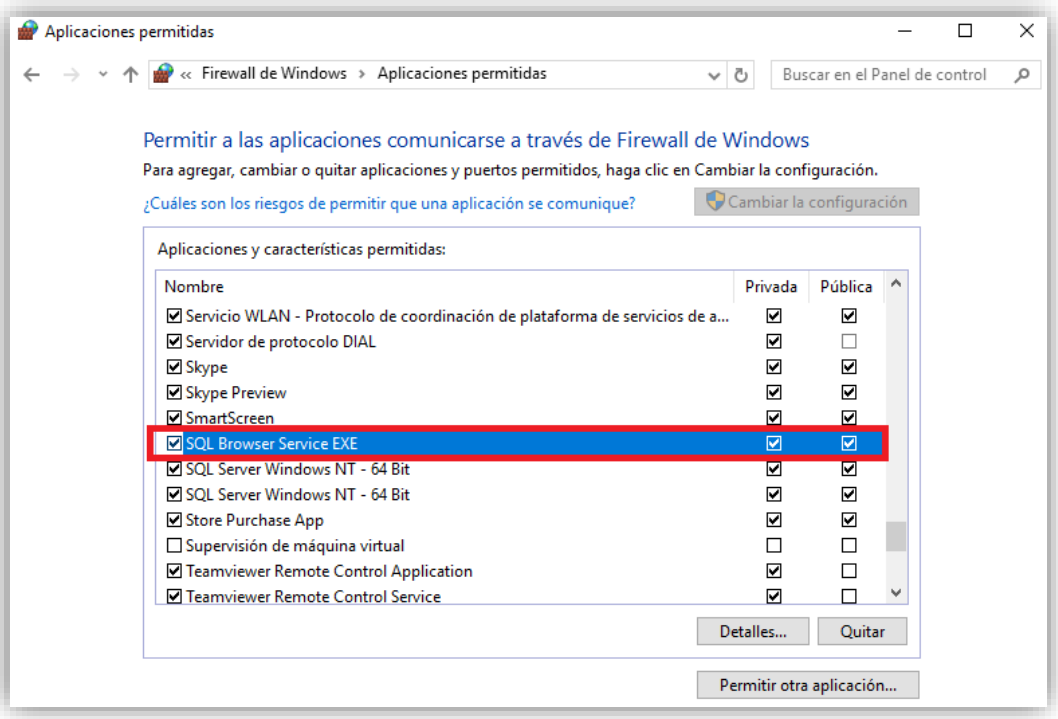

Ilustración 21: Lista blanca (Aplicaciones permitidas) en modo edición.

[9] Es posible marcar todas las opciones, es decir «Privada» y «Pública».

Por último, habrá que repetir los pasos anteriores, pero con el «Sqlserv.exe», recordemos que podemos saber en qué ruta está si consultamos la entrada pertinente del manual, ¿Dónde está el SqlServ.exe?.

Deberemos volver a pulsar sobre «Permitir otra aplicación», para poder buscarlo y agregarlo a la lista de aplicaciones permitidas:

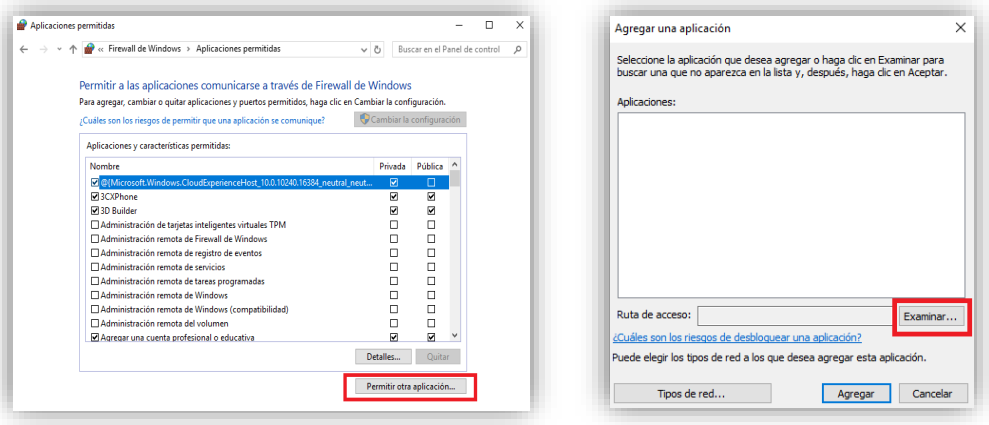

Ilustración 22: Ventana para agregar nueva aplicación y su búsqueda.

En la típica ventana de exploración de ficheros de Windows, deberemos «navegar» hasta encontrar la aplicación «Sqlserv.exe» y seleccionarlo, para pulsar sobre el botón «Abrir».

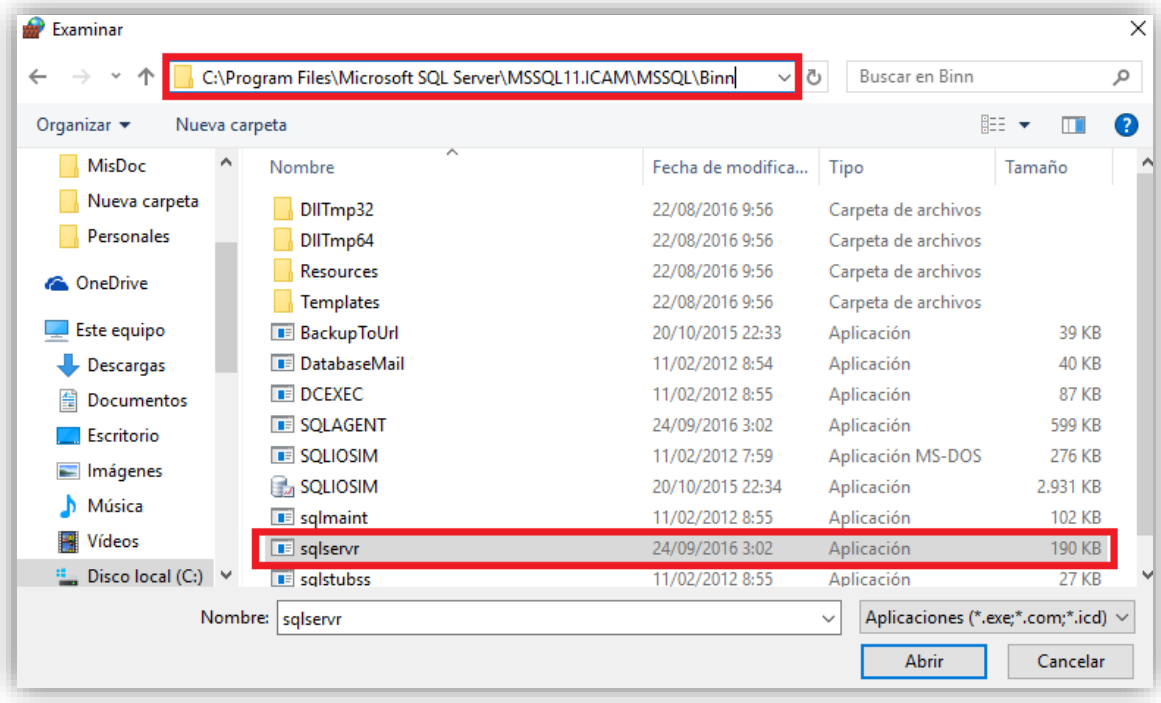

Ilustración 23: Cuadro de diálogo para la búsqueda de la aplicación a permitir.

Como en la ocasión anterior, tras completar los pasos, volveremos a la lista de aplicaciones permitidas. Una vez más deberemos, con la línea seleccionada, especificar a qué tipo de red debería tener acceso.

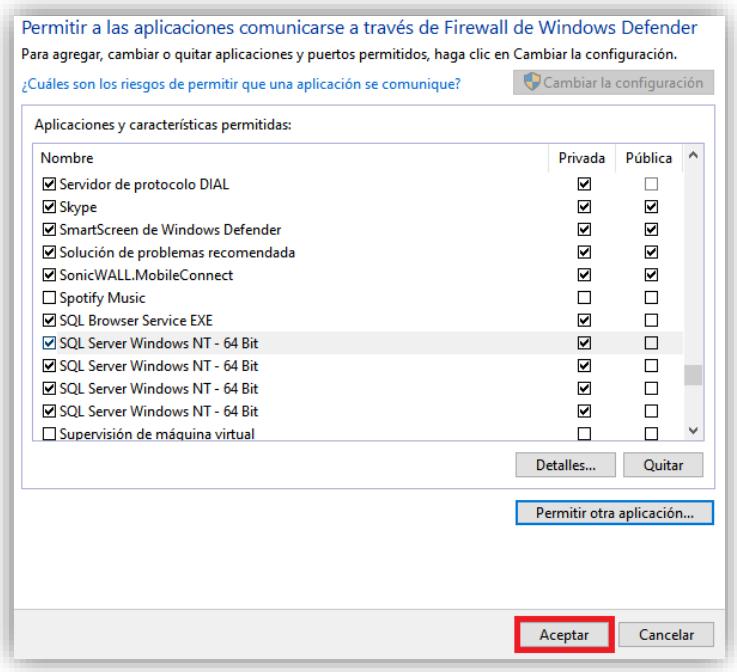

Ilustración 24: Aceptando los cambios aplicados en la lista blanca.

Una vez completado el proceso, aceptaremos todos los cambios pulsando sobre el botón «Aceptar», situado en la parte inferior de la ventana y cerraremos todas las ventanas abiertas de la configuración del cortafuegos, dando así por finalizado el proceso. Desde este momento, podrá trabajar en red con total normalidad y sin incidencias.

NOTA INFORMATIVA: Trabajando con dominios

Si la red de la oficina, o donde se esté trabajando, está configurada mediante un dominio, un tipo de red llamado dominio aparecerá en la configuración del cortafuegos de Windows. Tendrá que ser marcada, además de aplicar todo lo anteriormente explicado. Adicionalmente deberá contactar con su departamento informático o administrador de redes para que realicen los cambios oportunos que permitan a su perfil, y/o perfiles de usuarios de los compañeros, conectarse contra la base de datos alojada en el servidor. Dicha configuración escapa, por cuestiones de implementación de seguridad y configuración, a la competencia de cualquiera de nuestros técnicos y manuales, quedando exclusivamente en manos de los usuarios y sus informáticos.

Consideraciones finales

Esta configuración del cortafuegos en el ordenador que actúa como servidor únicamente es válida para redes locales, es decir, los ordenadores que pudiéramos tener físicamente en una misma ubicación o lugar. Para otro tipo de conexiones, como el uso de una VPN desde una red externa o conectarnos desde casa mediante internet (por poner un ejemplo), no sería suficiente, por lo que deberíamos consultar el manual específico para este tipo de conexiones.

Preguntas frecuentes

No puedo desactivar/configurar el firewall

Si las opciones están desactivadas o deshabilitadas, y no utiliza otro programa para la gestión del cortafuegos, no tendrá los permisos necesarios (Windows) para realizar alterar la configuración del cortafuegos. Deberá utilizar un usuario de Windows que disponga permisos de administrador o contacte con su informático y coméntele la situación.

Desactivé el cortafuegos (privado y público) y aún así no puedo conectar

Aunque no es recomendable desactivar totalmente el firewall, si ambos cortafuegos están deshabilitados y aún así persiste el problema de conexión, revise el nombre del equipo servidor/IP introducido, que el ordenador cliente esté conectado a la red local y que el PC que actúa como servidor esté encendido o que no tenga instalado algún otro programa que está limitando la conectividad.

El firewall está gestionado por el antivirus y no puedo realizar cambios.

Si tiene instalado un programa de seguridad, léase antivirus o similar, y este gestiona el cortafuegos, deberá realizar los cambios desde el propio antivirus. Si tiene algún problema con las opciones o la configuración, deberá ponerse en contacto con el soporte técnico del antivirus.

Seguí los pasos de configuración, pero no logro conectar con el servidor

Si tras revisar la configuración el problema persistiera, compruebe que está introduciendo correctamente el nombre del equipo/IP del servidor, que están ambos ordenadores conectados a la misma red local (si trabaja en una oficina/despacho), que esté encendido el ordenador que actúa como servidor y que no exista ningún otro programa instalado que esté bloqueando la conexión.

Ayer pude trabajar con normalidad, pero hoy no puedo conectarme contra el servidor

Algo en la configuración del servidor o del puesto de red ha cambiado. En algunas ocasiones al actualizarse Windows es posible que se haya aplicado alguna configuración extra por seguridad y haya reestablecido o alterado la configuración del cortafuegos, deberá revisarlo. También es posible que el nombre o la IP del equipo servidor haya cambiado, compruébelo.

¿Debo poner \ICAM o \ICAV antes del nombre del servidor/IP? (sólo versión colegios)

Si, por defecto será obligatorio indicarlo para poder establecer la conexión contra el servidor, aunque únicamente cuando trabajemos en una red local (despacho/oficina).

La red está gestionada por un dominio ¿Tendré algún problema?

No existe problema alguno, no obstante, al tratarse de un dominio deberán realizarse ciertas configuraciones adicionales que deberán ser establecidas por el propio administrador de dominio, las cuales quedan fuera del alcance del presente manual.

Si cambio de ordenador o instalo el programa ¿Debo hacer alguna modificación?

Si el ordenador afectado es el servidor, deberá configurar de nuevo el cortafuegos, por el contrario, si lo que se ha cambiado es un puesto de red, o se ha instalado el programa en nuevos ordenadores de la oficina/despacho, generalmente no deberá realizar ninguna acción más, puesto que con la configuración ya realizada en el servidor es suficiente.

¿Problemas?

Si por algún motivo tuviera algún problema o alguna duda, podrá llamar al teléfono de soporte técnico gratuito[10] 96 338 79 21 de 9:00 a 14:00 y de 16:00 a 19:00 de lunes a viernes o enviar un correo a soporte.tecnico@microareanext.com, indicando claramente el motivo o la causa del problema/duda.

[10] Únicamente disponible para clientes con mantenimiento en vigor.

Glosario

Base de datos	*Información almacenada en un soporte físico para poder ser tratada por uno o más usuarios.*
Cable (conexión red)	*La conexión a la red se hace directamente mediante un cable RJ45 al rúter o switch.*
Cliente (Informático)	*Ordenador que se conecta a otro (servidor), mediante la red, para trabajar con la información almacenada en una base de datos.*
Cliente-Servidor	*Modelo de diseño de software ideado para trabajar en red, especialmente con bases de datos, de tal manera que un ordenador (servidor) provea la información a los demandantes (clientes).*
Dominio (red)	*Gestión de la seguridad, credenciales y recursos de la red mediante la auditoria de un servidor especializado.*
Ethernet	*Denominación técnica para referirse a una red local.*
Firewall o Cortafuegos	*Herramienta informática, integrada o no en el sistema operativo, diseñado para bloquear el acceso no autorizado al ordenador o a la red, permitiendo el mismo a los sistemas autorizados. A modo de símil, funcionaria como una frontera política.*
Lista blanca (Firewall)	*Conjunto de aplicaciones con privilegios especiales excluidas de las reglas del cortafuegos permitiendo así su uso sin limitaciones.*
Lista negra (Firewall)	*Conjunto de aplicaciones que están bloqueadas por el cortafuegos para impedir su uso.*
Microsoft	*Empresa tecnológica internacional con sede en EE. UU. conocida por desarrollar el sistema operativo «Windows» o el paquete ofimático «Office».*
Monopuesto	*Configuración de nuestro programa para trabajar en un único ordenador.*
Puerto (Informático)	*Conexión y medio de transporte de la información entre equipos informáticos.*
Puesto de red	*Véase «Cliente».*
Red (Informático)	*Conjunto de ordenadores conectados entre sí mediante un medio (normalmente un rúter o Switch) cuya finalidad es compartir información y recursos.*
Red privada	*Red de confianza o segura, como pudiera ser la red de casa o de la oficina.*
Red pública	*Red abierta o protegida en la que no puede garantizarse un mínimo de seguridad. Un ejemplo sería el Wifi de un establecimiento de comida o la de un aeropuerto.*
Router	*Anglicismo para rúter.*
Rúter	*Dispositivo informático que permite la conexión de una red interna a internet.*
Servicios (Windows)	*Programa informático relativo al propio Sistema Operativo que se ejecuta en segundo plano dedicado a una tarea específica.*
Servidor	*Ordenador que por sus características provee de información a otros dentro de la red. Puede ser un tipo de PC dedicado o no.*
Sistema Operativo (SO)	*Software básico y principal cuya finalidad es permitir la interactuación entre el usuario y el sistema informático (Como, por ejemplo, Windows, MAC OS o Android).*
SQL Server	*Base de datos diseñada por Microsoft.*
Software	*Combinación de rutinas y procesos necesarios para que el PC funcione, como, por ejemplo, el sistema operativo o los programas informáticos (antivirus, Office, etc.).*
Switch	*También conocido como «Conmutador», es un dispositivo informático que permite enlazar o interconectar redes internas entre sí.*

TCP/IP	*Protocolo informático especializado en la comunicación de servicios en la red.*
Tipo de red (Windows)	*La identificación dada a la conexión de red existente en Windows, ésta puede ser de dos tipos, privada o pública.*
Wifi (conexión red)	*Conexión a la red mediante un dispositivo inalámbrico (como un rúter o móvil).*
Windows	*Sistema operativo para PC creado y desarrollado por Microsoft.*

Información de Utilidad

Información general

Teléfono Soporte Técnico: 96 338 79 20

Teléfono Departamento Comercial: 96 338 79 21

Correo Soporte Técnico: soporte.tecnico@microareanext.com

Correo Departamento Comercial: info@microareanext.com

Redes sociales:

Descarga de responsabilidad

AVISO IMPORTANTE:

Microarea no se hará responsable de los posibles daños, alteraciones o pérdidas de información acaecidos en el/los ordenadores, así como en la red debidos a la manipulación y/o alteración del programa, el Firewall de Windows o cualquier otro software relacionado.

Notas

Notas

Notas


microarea®
software