MICROAREA

CONFIGURACIÓN AVAST

Guía para usar el antivirus Avast con nuestras aplicaciones informáticas

microarea® software

MANUAL PARA CONFIGURACIÓN DEL ANTIVIRUS “AVAST”

MICROAREA DESARROLLOS INFORMÁTICOS, S.L.U.

info@microareanext.com | www.microarea.es

Índice General

Preámbulo

Es posible que, tras instalar el antivirus Avast o actualizarse el mismo, algún programa informático (aplicación) o algún recurso de red (unidades de red, carpetas compartidas, etc.) deje de funcionar, o por lo menos, no lo haga con normalidad. Esto podrá ser debido a la actuación del propio antivirus.

Cualquier programa que se dedique a prevenir, buscar, detectar y eliminar virus o amenazas informáticas basan su actividad en la búsqueda por concordancias (bases de datos con los virus conocidos), análisis heurístico (patrón de conducta de un virus ya conocido) y métodos de comportamiento (el antivirus intenta predecir el funcionamiento del archivo). Es precisamente a causa de ese último método de detención, profusamente extendido en los últimos tiempos debido a la proliferación de ataques informáticos en la red (correos electrónicos maliciosos, descarga de ficheros infectados, etc.), cuando pueden producirse problemas de conexión en una red local (casa, oficina o despacho) e incluso el impedimento de la ejecución de un programa correctamente instalado y completamente válido. El **antivirus bloqueará** automáticamente la **ejecución** del programa que considere potencialmente peligroso, aunque sea totalmente legítimo, sin interacción del usuario, aunque es posible que lance primero un aviso por pantalla. Este bloqueo se denomina “**Falso positivo**”.

El ”Falso positivo”, como se ha indicado, se produce debido a la propia inteligencia del programa de seguridad, el cual intentará predecir la naturaleza del fichero escaneado basándose en la posibilidad “de” y no en la certeza de infestación o amenaza, clasificando el fichero como infectado o malicioso, aunque esté totalmente libre de virus o amenaza alguna, aplicando la máxima “*Más vale prevenir que lamentar*” si piensa que podría ser dañino para el ordenador.

AVISO IMPORTANTE:

La manipulación del antivirus requerirá de ciertos conocimientos informáticos básicos, por lo que, en caso de carecer de ellos, sería recomendable contar con la asistencia de un técnico informático.

Consideraciones previas

Puesto que el antivirus se instala en cada uno de los equipos de forma independiente, si tuviéramos algún problema con el antivirus, podríamos tenerlo tanto en el servidor como en el puesto de red, por lo que el presente manual servirá tanto para uno, como para el otro.

Así mismo, aunque en esta guía se centre en el programa Winlab (Gestión de Nóminas) para ejemplificar las actuaciones, es totalmente válido para cualquiera de las demás aplicaciones de Microarea, tan solo habrá que elegir el programa que corresponda.

De la misma manera, tampoco hay que olvidar que el antivirus, en especial su cortafuegos, podría gestionar el acceso a la red (local o internet), por lo que, en caso de problema con la conexión contra el servidor, debería revisarse también la configuración den Avast en relación con el SQL Server (Base de datos).

NOTA INFORMATIVA:

Una forma sencilla de averiguar si el antivirus, y su cortafuegos, es el causante de los problemas de conexión o de inicio del programa es desactivarlo momentáneamente y comprobar que de esta forma el programa funciona correctamente. Lógicamente, la prueba deberá ser hecha bajo un entorno controlado y bajo su total responsabilidad.

¿Es necesario algún conocimiento previo para manipular el antivirus?

La manipulación de cualquier programa informático requiere de ciertas nociones, al menos básicas, sobre computadoras. Adicionalmente, sería aconsejable conocer los fundamentos elementales de seguridad informática, como pudiera ser qué es un virus o un cortafuegos.

No obstante, en caso de necesidad, siempre podría contactar con su técnico informático habitual para ayudarle en el proceso, o en caso de no disponer de uno, usar el soporte técnico del propio antivirus (foro, correo, teléfono, etc.) para que puedan solventarle el problema, o al menos, indicarle como hacerlo.

¿Es posible que un técnico de soporte realice los cambios?

Por normal general no, nuestros operadores de soporte técnico no estarían autorizados, y por tanto no podrían asumir la responsabilidad añadida para realizar o efectuar modificaciones, cambios o alteraciones de un software (programa) que no fuera de su competencia (y tampoco podrían dar soporte del mismo), especialmente aquellos dedicados a la integridad, solidez o seguridad de los sistemas informáticos (incluyendo la configuración de la red local). No obstante, sí que podrían, al igual que el alcance de esta guía, intentar ayudarle, en todo aquello que esté en su alcance, para que no tuviera problemas con el programa en relación con el antivirus.

Primer escaneo del programa

Cuando se ejecuta cualquier aplicación por primera vez, o se inicia tras haber aplicado una actualización, el antivirus Avast escaneará el ejecutable en busca de posibles amenazas, en el ejemplo Winlab (aunque pudiera ser el Magest, Maconta, EosWin, LexNext o Gestión Expedientes en cualquiera de sus versiones), mostrando el aviso por pantalla e impidiendo momentáneamente la ejecución del mismo.

Ilustración 1: Escaneando el programa.

De este escaneo, puede acontecer dos cosas totalmente distintas, que detecte que el programa es totalmente legítimo y está libre de amenaza:

Ilustración 2: Resultado del escaneo negativo.

O que “entienda” que pudiera ser peligroso y bloquee el archivo identificándolo como amenaza, pudiendo enviarlo directamente a la cuarentena (o baúl de virus). Sin embargo. Generalmente dejará a disposición del usuario la posibilidad de elección:

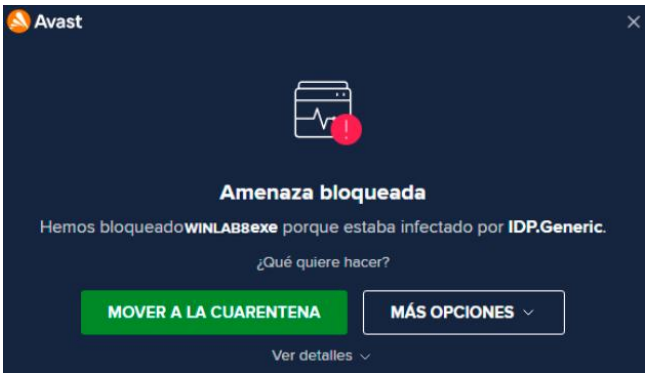


Ilustración 3: Resultado del escaneo positivo.

Fijémonos que, en el caso de haber detectado una posible infección, no ha sabido identificar exactamente que amenaza es, y simplemente ha clasificado el fichero como “amenaza genérica IDP.Generic”. Nos encontramos ante una falso positivo de libro. El antivirus entiende que el fichero puede ser potencialmente peligroso, pero no ha sido capaz de especificar la amenaza.

En este caso, dado que los programas de Microarea son escaneados y publicados libres de virus, no hay que “mover el fichero a la cuarentena” o proceder a su “eliminación”. Deberemos pulsar sobre “Más opciones” y elegir la elección de “permitir” el fichero para que pueda trabajar con la aplicación.

El propio antivirus recordará la opción elegida y no volverá a lanzar la ventana de escaneo hasta la próxima actualización del programa, si no lo añadió a la lista blanca, al entender que el fichero original ha sido cambiado (actualizado[1]).

Revisando la configuración del antivirus

El antivirus está en constante ejecución “observando” todo lo que acontece en el ordenador. A causa de este comportamiento puede tratar de múltiples maneras la relación, y forma de interactuar, entre las aplicaciones instaladas y el propio Sistema Operativo/Red (local o internet) y, por tanto, limitar o bloquear el uso de las aplicaciones o funciones de red, impidiendo su uso al asumir su papel de protector. Adicionalmente, mediante la configuración específica del antivirus, podría limitarse este comportamiento para evitar el exceso de celo en la protección del ordenador.

En caso de problemas, o haber interferido el antivirus en el correcto funcionamiento del programa, deberemos revisar la configuración del programa de seguridad y adecuarlo a nuestras necesidades mediante la creación de excepciones o reglas, que permitan identificar como software legítimo, y por tanto benévolas, las aplicaciones interferidas incluyéndolas en la lista blanca, impidiendo de esta forma el bloqueo de las mismas por parte del antivirus.

En términos generales, existen dos tipos de excepciones/reglas básicas, las que funcionan a nivel de antivirus y las que se rigen por las reglas del cortafuegos (pues, aunque el antivirus y el cortafuegos estén en la misma aplicación de seguridad, son componentes totalmente diferentes y por tanto su comportamiento, reglas y configuración, independientes). Las primeras solo afectarán al ordenador en cuestión y de forma local. Por el contrario, las segundas, afectarán a la comunicación del PC con la red.

[1] Muchos antivirus consideran una actualización de un programa como posible amenaza, pues puede entender que se está intentando reemplazar un fichero legítimo por otro que quizás no lo sea.

El antivirus Avast permite gestionar de forma rápida y sencilla la red a la que se conectó tipificándola y, en función del tipo indicado, establecer un nivel de seguridad u otro de forma predeterminada, llegando al punto de poder generar problemas de conectividad entre ordenadores de una misma red o impidiendo el acceso a la base de datos.

Excepción antivirus (control de escudos y Cybercapture)

Para crear una excepción a nivel de antivirus únicamente hay que pulsar sobre el icono del “menú” en la pantalla principal del antivirus:

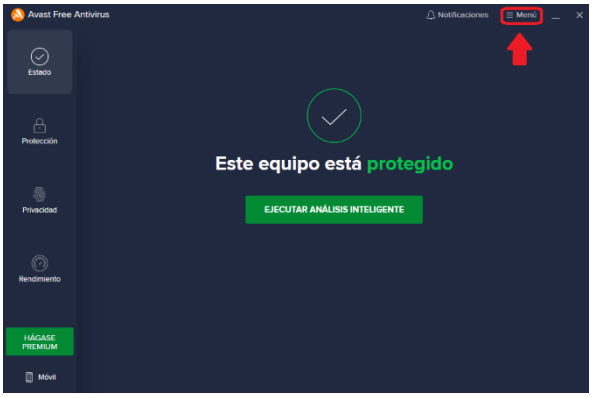


Ilustración 4: Ubicación del menú principal del Avast.

Tras haber pulsado sobre el icono, aparecerá, de forma emergente, el propio menú con varias opciones:

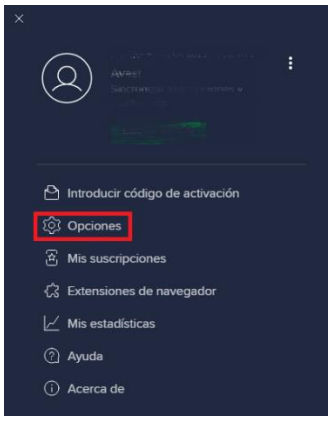


Ilustración 5: Opciones del menú.

Deberemos pulsar sobre “Opciones”, indicado por el símbolo de la rueda dentada. Este hecho, abrirá una nueva ventana:

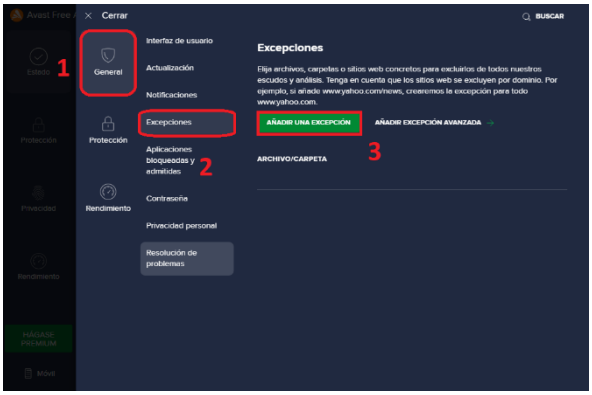


Ilustración 6: Insertando excepciones.

Primero deberemos pulsar sobre “General” (**1**), a continuación, sobre “Excepciones” (**2**). Si hubiera alguna excepción ya creada, aparecería en forma de lista en la parte inferior de la ventana. Para crear una nueva excepción, pulsaremos sobre el botón verde creado exprofeso para tal fin (**3**):

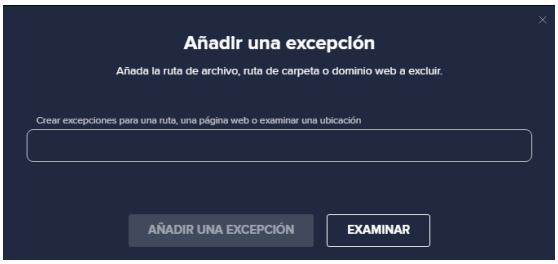


Ilustración 7: Creando una excepción.

Llegados a este punto, solo deberemos pulsar sobre el botón “Examinar” para localizar el fichero:

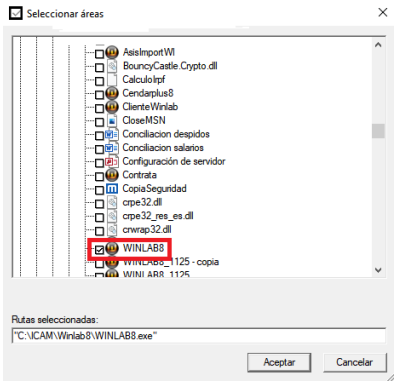


Ilustración 8: Selección del fichero a excluir.

En nuestro caso, como se trata del programa de nóminas “Winlab”, deberemos buscar en la carpeta de instalación del programa (dependerá de la versión instalada[2]) el fichero de la aplicación “Winlab8.exe[3]” y “Aceptar” la selección:

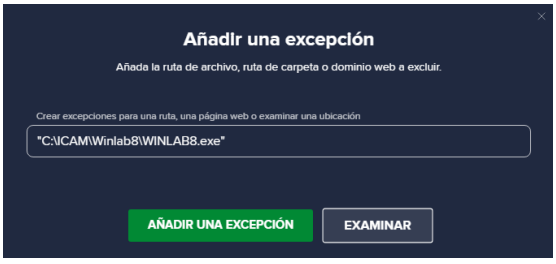


Ilustración 9: Añadiendo una excepción.

NOTA INFORMATIVA:

Una forma fácil de saber la ubicación del ejecutable del programa es hacer clic derecho sobre el acceso directo (generalmente situado en el escritorio) y pulsar sobre la opción “Abrir ubicación del archivo”. Automáticamente se abrirá en el explorador de archivos la carpeta donde está instalado el programa. Solo habrá que anotarse la dirección y el nombre del fichero para buscarlo y encontrarlo en el propio antivirus.

[2] En la carpeta raíz C:\ podrá aparecer ICAM, ICAV, ICAB o Microarea.

[3] O “Winlab8”, es posible que tenga configurado Windows para que no se muestren las extensiones de los ficheros.

Tras pulsar el botón verde para confirmar la inclusión del fichero en la lista blanca de excepciones:

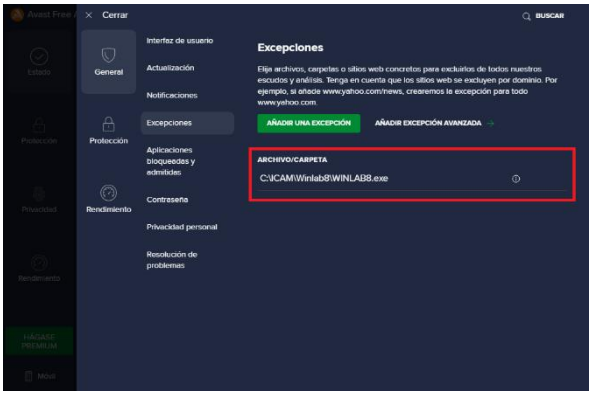


Ilustración 10: Excepción creada.

Volveremos a la pantalla inicial de exclusiones, pero esta vez la lista estará rellena con el programa en cuestión. Si fuera necesario, podría excluirse toda la carpeta entera (incluyendo subcarpetas) y no solo la aplicación para evitar los mismos problemas en cualquier otra parte del programa, como pudiera ser el componente específico que se encarga de las actualizaciones o el cálculo de IRPF.

Excepciones (reglas) del cortafuegos

Por defecto, las reglas del cortafuegos están establecidas de forma autónoma, en lo que denomina el propio Avast, como “modo inteligente”. Esto es, conforme se vayan usando las aplicaciones se irán gestionando y estableciendo las reglas automáticamente en función de unos varemos preestablecidos. Por tanto, deberemos gestionar las excepciones y revisar las lista negra o blanca del cortafuegos. Para ello, deberemos acceder al menú principal pulsando sobre “Menú” y posteriormente pulsar sobre “Opciones”, indicada esta opción con una rueda dentada.

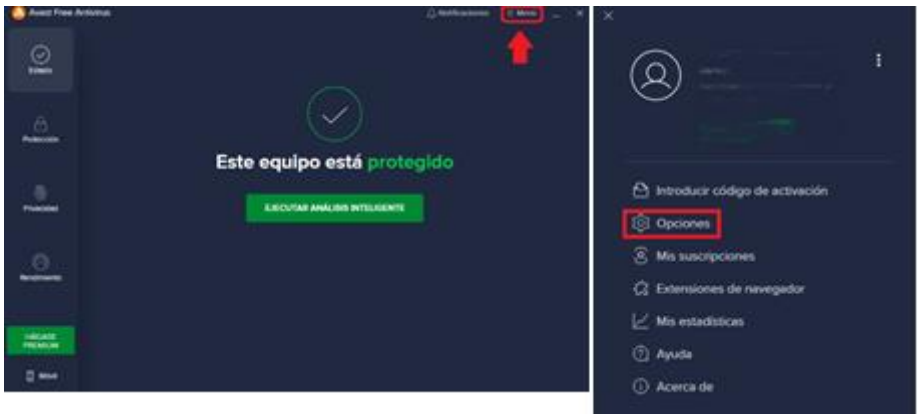


Ilustración 11: Localización del menú y las opciones de configuración.

Una vez en las opciones, habrá que elegir “Protección” (**1**) y después en “Cortafuegos” (**2**)

Ilustración 12: Localizando las reglas del cortafuegos (nótese el “modo inteligente” activo).

Tras actualizarse la pantalla, la opción “Ver reglas del cortafuegos” (**3**) estará activa. Deberemos pulsar sobre ella para cambiar de pantalla y ver las reglas activas.

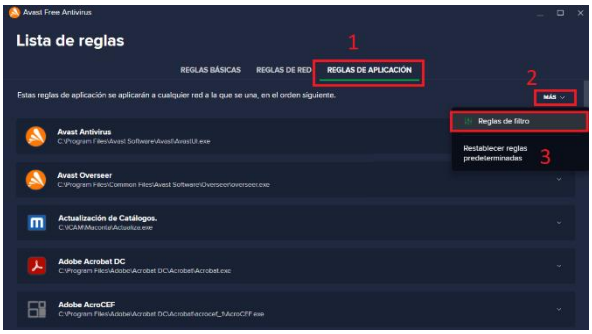


Ilustración 13: Reglas de aplicación.

En esta nueva ventana, deberemos pulsar sobre “Reglas de aplicación” (**1**). A continuación, haremos clic sobre “Más” (**2**) y “Reglas de Filtro” (**3**):

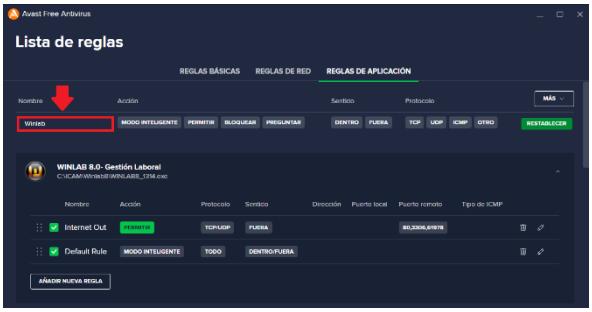


Ilustración 14: Localizando las reglas por aplicación.

Únicamente deberíamos buscar la aplicación que tuviera el problema (sin olvidarnos del SQL Server, o la base de datos) introduciendo el nombre en el recuadro rojo y revisar que no tuviera nada bloqueado (de color rojo). Si así fuera, deberíamos pulsar sobre el botón con forma de lápiz “Edición” y cambiar la opción a “Permitir” (en verde).

Para más información sobre las reglas del cortafuegos y la base de datos (SQL Server) puede consultar el manual específico sobre el cortafuegos genérico de Windows.

Aplicaciones bloqueadas (Cortafuegos)

El cortafuegos, al igual que el antivirus, dispone de una lista de aplicaciones bloqueadas (lista negra). Esta lista se empleará como referencia para bloquear cualquier tipo de ejecución de cualquier aplicación que esté incluida. De esta forma, aunque quisiéramos abrir el programa, este no se ejecutaría, pues le habríamos indicado al antivirus que no es un programa de confianza y previene su ejecución accidental.

Que esté algún programa incluido en dicha lista dependerá de la configuración del antivirus y/o de la interacción humana (es posible que el propio programa de seguridad pregunte qué hacer con X aplicación en algún momento dado, pudiendo elegir entre permitir o bloquear, y se haya seleccionado bloquear). Por dicho motivo, deberemos revisar que no tengamos alguna de nuestras aplicaciones o la propia base de datos (SQL Server) bloqueada en la lista y ésta sea la causa del problema.

Para acceder a las aplicaciones bloqueadas del cortafuegos deberemos ir a la opción “Protección” y “Cortafuegos”.

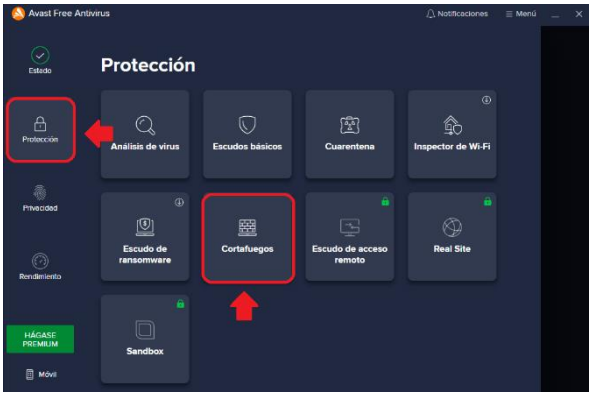


Ilustración 15: Accediendo al estado de cortafuegos.

En la nueva ventana deberemos pulsar sobre “Aplicaciones”. Por defecto será la opción que se abrirá, no obstante, nos cerciooraremos de que sea esta la elegida.

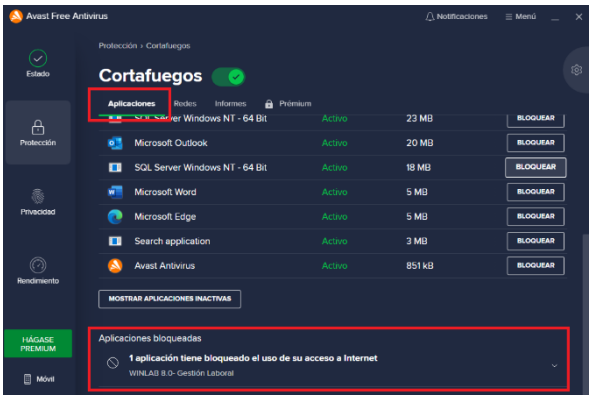
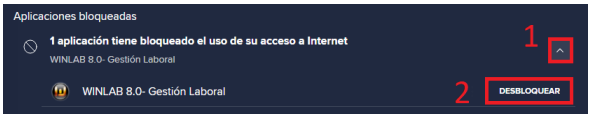


Ilustración 16: Lista blanca y lista negra del cortafuegos.

Se abrirán dos listados de aplicaciones, en la lista superior estarán las permitidas (en verde) que recibirá el nombre de lista blanca. Si desplazamos hacía abajo la ventana, veremos la otra lista, las aplicaciones bloqueadas o llista negra.

En el caso que nos concierne, Winlab aparecerá en esta última lista, por lo que no podríamos trabajar con el programa de nóminas. Para desbloquear la aplicación, o cualquiera que esté en la lista y sea necesario quitar, pulsaremos sobre el símbolo “˅” (**1**):



Completaremos la acción haciendo clic sobre la opción “Desbloquear” (**2**). De esta forma se eliminará de la lista negra y pasará a formar parte de la lista blanca, permitiendo así, el uso del programa.

Tipo de red

Como se comentó en la introducción del capítulo, y al igual que hace Windows, el antivirus permite “etiquetar” la red conectada con un tipo. En función de este, se determinarán una serie de características y funcionalidades de seguridad automáticamente, las cuales indicarán como deberá comportarse el antivirus/cortafuegos, llegando incluso al bloqueo total o parcial de aplicaciones y funciones de red.

Por tanto, si tenemos problemas de conexión, ya sea desde un puesto de red o desde el mismo servidor, es posible que esté mal configurado el tipo de red y esté impidiendo que el programa funcione como debería.

Podremos revisar el tipo de red, pulsando sobre la opción “Protección” y después en “Cortafuegos”:

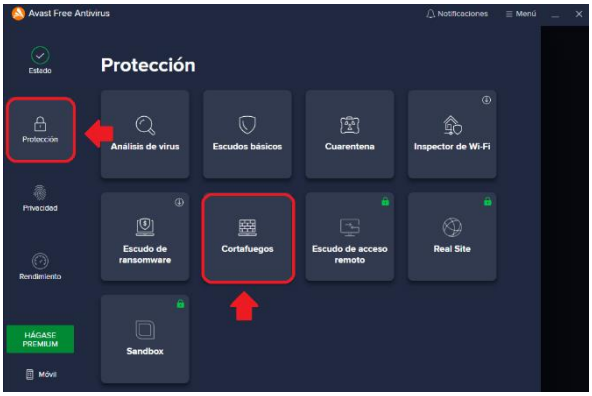


Ilustración 17: Ubicación del estado del cortafuegos.

En la nueva ventana que se habrá abierto, deberemos pulsar sobre la opción “Redes” y aparecerán tanto la red a la que estamos conectados (especificando el tipo) como las redes en las que se conectó recientemente.

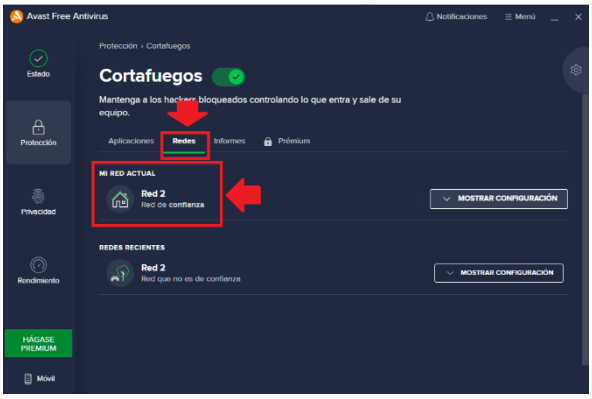


Ilustración 18: Tipo de red establecida para la red conectada.

Si la red conectada, en el ejemplo “Red 2”, está identificada como “Red de confianza” no debería haber problemas, sin embargo, si estuviera identificada como “Red que no es de confianza” el propio antivirus aplicaría reglas específicas agresivas de protección para, precisamente, proteger el ordenador lo máximo posible, pues se le está indicando que estamos conectados a una red en la que no tenemos control sobre ella, en la que no se sabe quién se conecta, que cifrado utiliza o no es posible gestionar la seguridad de la misma. Sería el caso, por citar algunos ejemplos, de una red pública o privada, pero de uso público, como un hotel, cafetería o restaurante, donde se está expuesto a cualquier tipo de amenaza. Por tanto, si estamos conectados a una red que es totalmente de confianza (como el despacho u oficina), deberíamos cambiar el tipo de red a “Red de confianza”.

NOTA INFORMATIVA: Sobre redes públicas o privadas de uso público

La propia Oficina de Seguridad Internauta (OSI), perteneciente al Instituto Nacional de Ciberseguridad (INCIBE), dependiente orgánicamente del Ministerio de Asuntos Económicos y Transformación Digital (MINECO), especifica en sus consejos de protección en la red evitar al máximo el uso de dichas redes, no obstante, en caso de necesidad nos ofrece una serie de pautas y recomendaciones para minimizar el riesgo de sufrir algún problema de seguridad. Puede consultar dicha guía aquí.

Preguntas frecuentes

A continuación, se detallarán las preguntas más habituales que suelen darse en relación con en el antivirus/cortafuegos y alguno de nuestros programas.

El programa no se abre (no se encuentra el fichero)

Si el programa ya no abre, es decir, hacemos doble clic sobre el acceso directo, pero no se abre o aparece el siguiente aviso por pantalla:

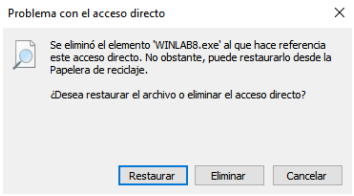


Ilustración 19: Problema con el acceso directo, el programa no existe.

Es debido a que el programa ha sido eliminado, o por lo menos movido de sitio, generalmente puede haber ocurrido dos situaciones:

El fichero fue movido a la cuarentena

Si se mandó el fichero a la cuarentena/baúl de virus, bien por una acción manual o el propio antivirus lo hizo automáticamente. Sea como fuera, no importa, deberemos abrir el antivirus y de la cuarentena/baúl de virus recuperar el fichero. Generalmente la cuarentena se encuentra en el menú de “protección”:

Ilustración 20: Ubicación de la cuarentena.

Una vez se abrió la cuarentena, no hay más que buscar el fichero del programa de la lista y posicionar el curso sobre él para que se active el menú de acciones. A continuación, haremos clic en el botón gris con tres puntos al final de la línea:

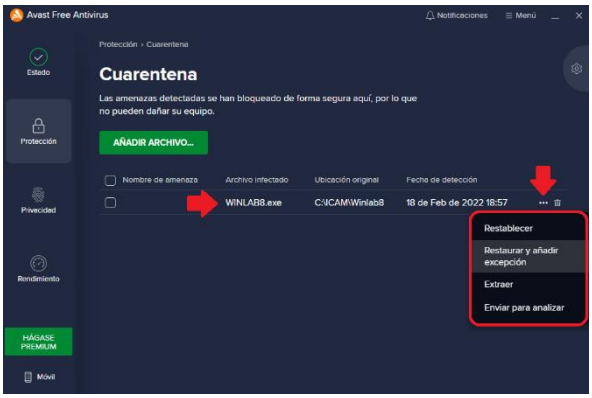


Ilustración 21: Recuperando el programa de la cuarentena.

Con la finalidad que no sea bloqueado de nuevo en el futuro, la mejor opción no es solo “restaurar” el fichero, sino que deberemos elegir, y por tanto pulsar, sobre la opción “Restaurar y añadir excepción”. De esta forma, automáticamente, el antivirus devolverá el fichero a su lugar de origen (permitiendo volver a entrar al programa) y creará una regla o excepción que posibilitará que, por descuido, error o de forma autónoma, el fichero no vuelva a ser movido a la cuarentena.

El fichero fue eliminado

Si el fichero fue movido a la cuarentena y pasó más de periodo de tiempo máximo (dependerá de la configuración), su peso[4] era superior a x tamaño (también dependerá de la configuración) o directamente fue eliminado (bien pulsando directamente sobre la opción o de forma automática al realizar algún análisis) lamentablemente no habrá nada que poder recuperar o restaurar. El fichero no estará en el disco duro, por lo que la única solución será ponerse en contacto con el departamento de soporte técnico o reinstalar/reparar el programa.

El programa se abre, pero no inicia

Si accedemos a la pantalla de inicio del programa, esto eso, la ventana donde indicamos el servidor, usuario y contraseña, pero tras identificarnos e intentar acceder al programa este no se abriera (la ventana de inicio si se cerrará), es síntoma inequívoco que el antivirus está bloqueando la correcta ejecución del programa.

Ilustración 22: Pantalla de inicio del programa o de sesión (Winlab).

En tal caso, deberíamos crear una excepción en el propio antivirus para evitar el bloqueo o pausar protección del mismo, bajo su total responsabilidad, por lo menos hasta poder entrar al programa, momento en el cual debería restaurarse la protección (esta última opción sería la menos recomendable).

El programa se abre, pero no se conecta

Ejecutamos el programa, introducimos los datos para iniciar la sesión, pero no se abre el programa. Se queda la ventana de inicio “atascada” y se bloquea. Señal es irrefutable del bloqueo de la base de datos (SQL Server, no del programa) por parte del cortafuegos de Avast. Es decir, el antivirus sí que permite la ejecución del programa, pero no la conexión a la base de datos, por lo que el programa se queda a la espera de poder recibir información hasta que el tiempo máximo de espera llega a su fin y Windows interpreta que el programa no funciona correctamente.

[4] En informática, el peso equivale al tamaño del fichero el cual es generalmente expresado en megas (megabyte MB).

Ilustración 23: Esperando el inicio de la base de datos (modo espera).

Para evitarlo, deberemos crear una excepción/regla en el propio Avast, revisar en el mismo el tipo de red, o desactivar los controles de escudos al menos hasta poder iniciar la aplicación. Esta última opción no es la más correcta y deberá ejecutarla bajo su responsabilidad plena, por lo que no se recomienda.

A pesar de todo, los problemas persisten

Recuerde que, nosotros no podemos dar soporte de una aplicación que no es de nuestra competencia, aunque con la presente guía intentemos ayudarle con la gestión del antivirus en relación con nuestras aplicaciones, por lo que sí, tras seguir las indicaciones de este manual, los problemas persistieran, debería contactar con el soporte técnico del propio Avast para solventar el problema.

Información de utilidad

Teléfonos y correos electrónicos

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:

Glosario

Aplicación	*Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.*
Base de datos	*Información almacenada en un soporte físico para poder ser tratada por uno o más usuarios.*
Baúl de virus	*Zona de contención del antivirus donde una aplicación potencialmente peligrosa es enviada para evitar su funcionamiento y por tanto su ejecución en el ordenador.*
Cable (conexión red)	*La conexión a la red se hace directamente mediante un cable RJ45 al rúter o switch.*
CD-Key	*Conjunto de caracteres alfanuméricos que posibilita activar un programa informático.*
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).*
Control remoto	*Programa informático que se instala en dos dispositivos y permite el control de uno mediante el otro.*
Cuarentena	*Véase Baúl de virus.*
Dispositivo	*Equipo informático, como pudiera ser un ordenador, portátil, Tablet, teléfono o impresora, por ejemplo.*
Dominio (red)	*Gestión de la seguridad, credenciales y recursos de la red mediante la auditoria de un servidor especializado.*
Ejecución (aplicación)	*Inicio de la aplicación informática.*
Ejecutable (aplicación)	*Archivo con extensión .exe que abre o inicia el programa o aplicación.*
Escritorio remoto	*Control remoto propio, e integrado en algunas versiones, de Windows de forma nativa.*
Ethernet	*Denominación técnica para referirse a una red local.*
Extensión (archivo)	*Cadena de caracteres precedidos por un punto que determina el tipo de fichero o archivo.*
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.*
Instancia (SQL Server)	*Agrupación centralizada de las bases de datos del usuario que utiliza el programa.*
IP	*El identificador único de un dispositivo en la red.*
IP privada	*El identificador de cada dispositivo en la red local.*
IP pública	*El identificador de nuestro rúter en internet.*
ISP	*Proveedor de Internet (Orange, Vodafone, Jazztel, etc.)*
Latencia	*El tiempo que tarda la información en ir y volver en la red, ya sea local o en internet.*
Local (Red LAN)	*Conexión de red entre varios ordenadores generalmente ubicados en la misma ubicación física (como un hogar o una oficina)*
Local (Localhost)	*El propio ordenador donde se está trabajando.*
Lista blanca (Cortafuegos)	*Conjunto de aplicaciones con privilegios especiales excluidas de las reglas del cortafuegos permitiendo así su uso sin limitaciones.*
Lista negra (Cortafuegos)	*Conjunto de aplicaciones que han sido incluidas en las reglas del cortafuegos específicamente para ser bloqueadas y no puedan ser ejecutadas.*
Mega (Megabyte)	*Expresado en MB, unidad de información (almacenamiento) estándar.*
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.*
Nube	*Espacio de almacenamiento y procesamiento de datos y archivos ubicado en internet, al que puede acceder el usuario desde cualquier dispositivo.*
Programa (informático)	*Ver aplicación.*
Puerto (Informático)	*Punto de conexión por el que la información fluye entre dispositivos o una web.*
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 pero que no puede garantizarse un mínimo de seguridad. Un ejemplo sería el Wifi de un establecimiento de comida o la de un aeropuerto.*
Router	*Término anglosajón para rúter.*
Rúter	*Dispositivo informático que permite la conexión a internet a una red interna y gestiona la misma.*
Servicios (Windows)	*Programa interno informático 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 interactuar con el sistema informático (Como, por ejemplo, Windows, MAC OS o Android, entre otros).*
SQL Server	*Gestor de bases de datos diseñada por Microsoft y usada por nuestras aplicaciones.*
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.*
Tamaño (fichero)	*Cantidad de espacio real que ocupa (pesa) un fichero en el disco duro. Se expresa en byte, aunque generalmente en unidades que superiores como Kilobyte (KB), megabyte (MB) o gigabyte (GB).*
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.*
VPN	*Tecnología de red capaz de conectar un ordenador externo de la red local a la misma mediante internet (requiero de la instalación de un programa).*
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.*

Copia de seguridad

Cualquier sistema informático está expuesto a multitud de factores de riesgo, internos y externos, directos e indirectos, que podrían poner en peligro la integridad lógica y física de los datos hasta el punto de poder sufrir una pérdida total e irremediable. Robos, incendios, inundaciones, golpes, roturas, problemas eléctricos, infecciones de virus, ataques cibernéticos, …son sólo algunos de los problemas que tristemente pueden darse. Por todo ello, la copia de seguridad debe ser un pilar fundamental en el que se base la seguridad de la empresa. Tal es la importancia de las copias de seguridad, que existe el día internacional de la copia de seguridad, el cual se celebra cada 31 de mayo, para recordarnos los beneficios de disponer de una copia en caso de emergencia.

Por esta misma razón, todas nuestras aplicaciones disponen de una herramienta totalmente gratuita que, bajo interacción del usuario, realizará la copia de seguridad (accesible desde el menú “Utilidades”, “Copias de Seguridad”). Dicho asistente, además servirá para restaurar las copias de seguridad, si fuera necesario.

Adicionalmente, si lo prefiere y para mayor comodidad, **es posible automatizar** el proceso mediante la adquisición del módulo especialmente diseñado para programar la realización de las copias de seguridad.

Podrá obtener más información contactando con nuestro departamento comercial o llamando al 96 338 79 21 en horario de oficina (de 9 a 14 h y de 16 a 19 h).

Para más información, puede consultar el documento “Manual para la copia de seguridad y su posible restauración” aquí.

Descarga de responsabilidad

AVISO IMPORTANTE:

El usuario es, y será, el único responsable de la seguridad de su ordenador, u ordenadores, y su red, y, por tanto, de las posibles consecuencias derivadas de las actuaciones o manipulaciones del software instalado o cualquier otro tipo de proceder relacionado con la actividad informática. Microarea no se hace responsable de los posibles daños, alteraciones, ataques o pérdidas de información acaecidos en el servidor, puesto de red, y en general en algún ordenador o en la red debido a la manipulación del software de seguridad (Antivirus).

Notas

Notas

Notas


microarea®
software