

## Guía del usuario de Outpost Network Security

### Bienvenido

¡Felicidades por haber descubierto Outpost Network Security Client, y por utilizar el cortafuegos más avanzado de la actualidad, que es a la vez, accesible para todos los usuarios!

Para facilitar su comprensión, esta guía ha sido dividida en tres grandes grupos:

- [Para todos los usuarios](#)
- [Para usuarios avanzados](#)
- [Información adicional](#)

### Para todos los usuarios

- [Guía del usuario I](#)
  - **Cómo empezar**
    - Cómo iniciar Outpost Network Security Client
    - Cómo detener Outpost Network Security Client
    - Las alertas de Outpost Network Security Client
  - **Una orientación**
    - El icono de la bandeja de sistema
    - La ventana principal de Outpost Network Security Client
    - Los paneles
    - La barra de herramientas
    - Los botones en la barra de herramientas
- [Guía del usuario II](#)
  - **Configuración de Outpost Network Security Client**
    - Información básica
    - Configuraciones iniciales
    - Cómo seleccionar una Política
    - Temporizador de inactividad
    - Filtro de nivel de aplicación
    - Control de componentes
    - Procesos ocultos
    - Control de procesos en memoria

- [Guía del usuario III](#)

- **Complementos**

- Introducción
- Bloqueo de anuncios publicitarios
- Bloqueo de contenido activo
- Detección de ataques
- Cuarentena de archivos adjuntos
- Caché DNS
- Filtro de contenido
- Protección contra software espía
- Ajuste rápido del navegador

## Para usuarios avanzados

- [Guía del usuario IV](#)

- **Configuraciones avanzadas**

- Introducción
- Creación de reglas para aplicaciones
- Configuraciones para redes domésticas y de oficina

- **Sistema de registro de Outpost**

- Introducción
- Ventana principal del Visor de registros de Outpost
- Cómo mostrar los registros
- Cómo trabajar con registros y filtros
- Cómo trabajar con los registros Favoritos

## Información adicional

- [Guía del usuario V](#)

- **Apéndice A**

Cómo personalizar la ventana principal de Outpost

- Diseño
- Filtro por hora
- Columnas
- Agrupar

- **Apéndice B**

- Tipos de mensajes ICMP

- **Apéndice C**

- Soporte técnico

## Para todos los usuarios

### Cómo empezar

#### Cómo iniciar Outpost Network Security Client

Una vez instalado, Outpost Network Security Client se ejecuta automáticamente al iniciar Windows, comenzando a proteger el ordenador desde antes que se active cualquier otro programa que pueda comprometer el sistema.

Para iniciar manualmente Outpost Network Security Client:

1. Pulse en el botón **Inicio** de Windows, **Programas**.
2. Seleccione **Agnitum**.
3. Pulse en **Outpost Network Security**.
4. Ejecute **Outpost Network Security Client**.

Cuando se está ejecutando Outpost Network Security Client, su icono se ubica en la bandeja de sistema, cerca del extremo inferior derecho de la barra de tareas de Windows.

Si el icono no aparece en la bandeja de sistema, implica que Outpost Network Security Client no está protegiendo el ordenador, o se está ejecutando en segundo plano en modo **De fondo**. Para obtener más información sobre esta característica, por favor consulte la sección [Configuraciones iniciales](#).

#### Cómo detener Outpost Network Security Client

Outpost Network Security Client no se detiene cuando se cierra su ventana principal. Su icono permanece en la bandeja de sistema.

Existen dos formas de detener Outpost Network Security Client:

- Pulse con el botón secundario del ratón en el icono de la bandeja de sistema, para desplegar el menú contextual.
- Seleccione **Salir**.
- Deberá aceptar el mensaje de advertencia.

También se puede cerrar desde la ventana principal:

- Pulse en el menú **Archivo**.
- Seleccione **Salir**.
- Deberá aceptar el mensaje de advertencia.

Usando cualquiera de estos procedimientos, se cierran conjuntamente la interfaz y se interrumpe el servicio del cortafuegos.

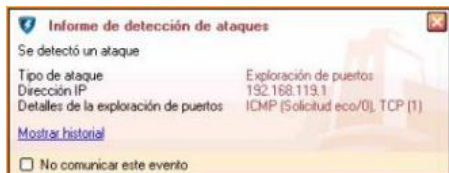
#### Las alertas de Outpost Network Security Client

Outpost Network Security Client muestra distintas alertas para notificar al usuario sobre ciertos sucesos específicos, y para mantenerlo informado de las actividades que realiza.

Las alertas se muestran en cuadros emergentes que automáticamente se cierran a los diez segundos. Si desea mantener visible un cuadro de alerta durante más tiempo, para leer detalladamente la información que muestra, simplemente pulse en cualquier lugar dentro del cuadro.

Pueden aparecer las siguientes alertas:

### Detección de ataques



El mensaje de alerta muestra los detalles del ataque bloqueado por Outpost Network Security Client.

Pulse en [Mostrar historial](#) para visualizar la lista completa de los informes de ataques de características similares.

Esta alerta se muestra solamente si ha sido habilitada su visualización en el complemento **Detección de ataques**, Alertas.

### Informe de Outpost Network Security Client



Una de las reglas de aplicación ha sido procesada por Outpost Network Security Client.

Pulse en el vínculo para modificar la regla que ha sido creada.

Esta alerta será mostrada según la configuración establecida para la creación automática de reglas.

### Noticias sobre complementos



Algunos complementos nuevos, o actualizaciones de los ya instalados, están disponibles para su descarga desde el sitio de Agnitum en Internet.

Pulse en el vínculo para obtener información más detallada.

La recepción de noticias se habilita desde la ventana principal de Outpost, en el menú Herramientas, **Descargar información sobre complementos**.

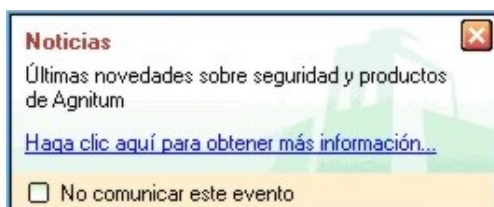
## Informe sobre archivos adjuntos en mensajes de correo electrónico puestos en cuarentena



Esta alerta sólo se exhibe cuando la opción **Informar** está seleccionada para algún tipo en particular de archivo adjunto.

Podrá acceder a la configuración de este complemento, pulsando en el menú Opciones, Configuración de complementos, **Cuarentena de archivo adjunto**.

## Noticias de Outpost



La ventana principal de Outpost Network Security Client ha recibido información actualizada.

Pulse en el vínculo para conocer las tendencias actuales de seguridad, las actualizaciones y las novedades de Outpost Network Security Client.

La recepción de noticias se habilita desde la ventana principal de Outpost, en el menú Herramientas, **Descargar noticias de Agnitum**.

## Limpieza de registros



El Limpiador del registro de Outpost está efectuando el mantenimiento de la base de datos según la configuración establecida por el usuario y eliminando registros para disminuir el tamaño de la misma.

Este mensaje sólo se muestra cuando la opción **Mostrar alertas** está seleccionada en la configuración de **Limpieza de registros**. del Visor de registros de Outpost.

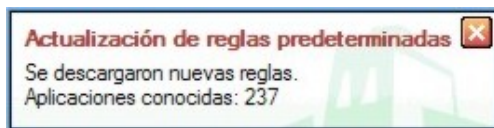
## Caché DNS



Ha sido detectada una petición DNS incorrecta y la misma ha sido bloqueada.

Este mensaje sólo se muestra cuando la opción **Alertar sobre solicitudes DNS bloqueadas** está seleccionada en la configuración del complemento Caché DNS, en la pestaña **General**.

## Actualización del cortafuegos



Cada vez que concluye el proceso de actualización del cortafuegos, en todos sus niveles, se generará un informe sobre el resultado de los diversos elementos actualizados.

Outpost Network Security Client descarga automáticamente las últimas novedades y los anuncios más recientes sobre complementos desde el sitio de Agnitum o su distribuidor autorizado, para la versión instalada y en su propio idioma, mostrándolos cuando el usuario pulsa en **Mi Internet** o en **Complementos**, en el directorio del panel izquierdo de la ventana principal de Outpost.

☑ Para activar esta característica, pulse con el botón secundario del ratón en **Mi Internet** o en **Complementos**, y seleccione **Descargar noticias y/o Descarga información sobre complementos**, respectivamente.

## Una orientación

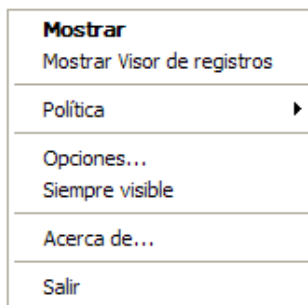
### El icono de Outpost en la bandeja de sistema

La bandeja de sistema se encuentra en el extremo derecho de la barra de tareas de Windows, y generalmente se ve de esta manera, pudiendo variar en color y presentación según sea el sistema operativo del usuario.



El círculo azul con un signo de interrogación, es el icono de Outpost Network Security Client, que en este caso en particular, se encuentra operando en modo Asistente para la creación de reglas. Este icono es la forma más práctica para acceder a los controles, configuraciones y registros de Outpost Network Security Client. Este icono varía de acuerdo a la configuración, para que el usuario visualice permanentemente el modo en que Outpost Network Security Client está protegiendo su ordenador. La descripción de estos modos se encuentra en la sección [Cómo seleccionar una Política](#).

Al pulsar con el botón secundario del ratón sobre el icono de Outpost Network Security Client, aparecerá un menú contextual:



- **Mostrar**  
Abre la ventana principal de Outpost Network Security Client.
- **Mostrar Visor de registros**  
Abre el Visor de registros.
- **Política**  
Despliega un menú secundario, donde el usuario puede seleccionar uno de los modos de funcionamiento del cortafuegos:
  - **Desactivar**
  - **Permitir casi todo**
  - **Asistente para la creación de reglas**
  - **Bloquear casi todo**
  - **Detener todo**
- **Opciones**  
Muestra la ventana de diálogo llamada Opciones a través de la cual se accede a los parámetros de Outpost.
- **Siempre visible**  
Mantiene visible la ventana actual de Outpost Network Security Client, por sobre todas las otras ventanas que estén abiertas en el sistema.
- **Acerca de**  
Informa acerca de la versión actual de Outpost Network Security Client y datos de la licencia.
- **Salir**  
Cierra la interfaz gráfica del usuario y detiene el cortafuegos. Si se ejecuta este comando, Outpost Network Security Client dejará de proteger el sistema.

**⚠ Importante:** Como se ha mencionado anteriormente, no se mostrará el icono de Outpost Network Security Client si el programa está configurado para ejecutarse en modo **De fondo**. En este caso, el usuario no podrá acceder a la configuración de Outpost Network Security Client hasta que el administrador del sistema cambie el modo en que funciona el cortafuegos.

## La ventana principal de Outpost Network Security Client

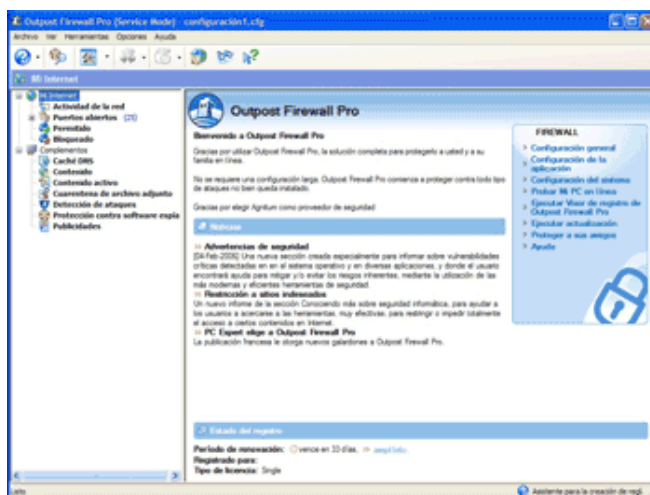
La ventana principal de Outpost Network Security Client es una aplicación centralizada de administración.

Se utiliza para controlar las operaciones de red del ordenador, y para modificar los parámetros de configuración del cortafuegos.

Para visualizar la ventana principal de Outpost Network Security Client:

1. Pulse con el botón secundario del ratón en el icono de Outpost Network Security Client en la bandeja de sistema.
2. Seleccione **Mostrar** en el menú contextual.

La ventana principal de Outpost Network Security Client, inmediatamente después de haber sido instalado, se muestra así:



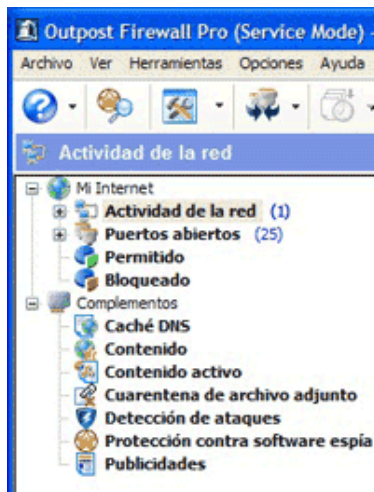
La ventana principal está compuesta por diversas secciones:

- El **menú principal** de Outpost Network Security Client
- La **Barra de herramientas**
- La **Barra de carpetas**
- El **Panel izquierdo**
- El **Panel de información**
- La **Barra de estado**.

## Los paneles

El panel izquierdo y el de información son similares a los paneles izquierdo y derecho del Explorador de Windows. El panel izquierdo contiene una lista de los componentes protegidos por Outpost Network Security Client en el ordenador. El panel de información (panel derecho) brinda datos específicos sobre cualquier componente seleccionado en el panel izquierdo.

La siguiente es una imagen del panel izquierdo:



Debajo de **Mi Internet** se encuentran los siguientes temas:

- **Actividad de la red**  
Muestra todas las aplicaciones y protocolos que actualmente tengan conexión activa a Internet o a una red de área local (*Local Area Network, LAN*), entre otras actividades de red.
- **Puertos abiertos**  
Muestra los puertos abiertos en el sistema.
- **Permitido**  
Muestra la estadística de los sucesos registrados en todas las aplicaciones y conexiones que Outpost Network Security Client haya permitido. Se puede visualizar una estadística más restringida, aplicando filtros para mostrar únicamente el registro de la sesión actual o del día en curso.
- **Bloqueado**  
Muestra la estadística de los sucesos registrados en todas las aplicaciones y conexiones que Outpost Network Security Client haya bloqueado. Se puede visualizar una estadística más restringida, aplicando filtros que permitan ver solamente el registro de la sesión en curso o de la fecha actual.
- **Informado**  
Es el registro de los sucesos que incluyen la opción **informar** en sus reglas establecidas, mostrando todos los intentos de acceso a Internet o a una *LAN* por parte de las aplicaciones o conexiones especificadas de antemano por el usuario.

Aunque la información detallada de los registros está destinada a los usuarios avanzados, los puntos anteriores cobran importancia cuando sea necesario ver las estadísticas de las conexiones establecidas, o la cantidad de unidades de información (*bytes*) enviadas y recibidas. Para poder ver los registros en más detalle, es necesario pulsar el botón **Mostrar registro detallado**, ubicado en el panel **Información de Permitido, Bloqueado e Informado**.

🔗 Consulte la sección [Sistema de registro de Outpost](#) para ampliar esta información.

Las estadísticas también ayudan a comprobar que Outpost Network Security Client esté configurado correctamente y que su funcionamiento sea el apropiado.

El paquete de instalación de Outpost Network Security Client, que el usuario ha descargado desde el sitio de Agnitum en Internet, contiene algunos complementos adicionales. Los complementos son independientes del motor principal de Outpost. El usuario puede instalar o desinstalar cualquiera de ellos, o todos. También se pueden hallar otros complementos de terceras partes, creados por desarrolladores independientes y disponibles desde otros sitios de Internet.

La segunda parte de la lista del panel izquierdo muestra los complementos instalados.

Cada complemento tiene su propio icono en el panel izquierdo y el registro de sus actividades se muestra en el panel de información.

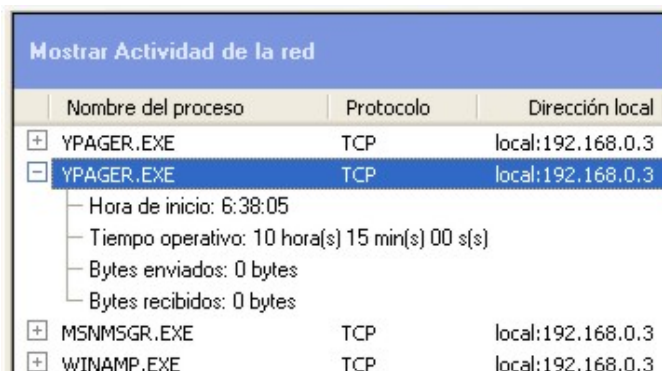
Cuando se instala Outpost Network Security Client por primera vez, la lista de **Complementos** contiene los siguientes módulos:

- **Caché DNS**  
Muestra el registro de las direcciones de Internet almacenadas por Outpost Network Security Client en su base de datos, permitiendo acelerar la conexión de Internet a esos sitios.
- **Contenido**  
Muestra el registro de todos los sitios o páginas de Internet que hayan sido bloqueadas por este complemento, y el motivo del bloqueo.
- **Contenido activo**  
Muestra el registro de los sitios que tuvieron algunos de sus contenidos activos bloqueados, basándose en la configuración para las aplicaciones Java, VBScript, ActiveX y otros elementos con esta característica.
- **Cuarentena de archivos adjuntos**  
Muestra el registro de todos los archivos adjuntos en mensajes de correo electrónico que hayan sido neutralizados y puestos en cuarentena.
- **Detección de ataques**  
Muestra el registro de cualquier ataque al ordenador, desde Internet, su procedencia y los puertos involucrados.
- **Protección contra software espía**  
Muestra el registro de los programas espía detectados, la cantidad de firmas en la base de datos, la última actualización de las mismas y otros datos referidos a la protección de información privada.
- **Publicidades**  
Muestra el registro de todos los anuncios publicitarios que hayan sido bloqueados.

Al igual que en el Explorador de Windows, cualquier línea que comience con un signo **más (+)** puede expandirse para mostrar cada uno de los elementos o datos que incluye.

Un signo **menos (-)** al principio de cualquier categoría denota que la misma ya ha sido expandida. Al pulsar en el mismo todos los datos incluidos quedarán ocultos, para reducir el espacio que ocupa dicha categoría.

Aquí se ve un ejemplo del Panel de información, mostrando los elementos constitutivos, expandidos y también aquellos comprimidos.

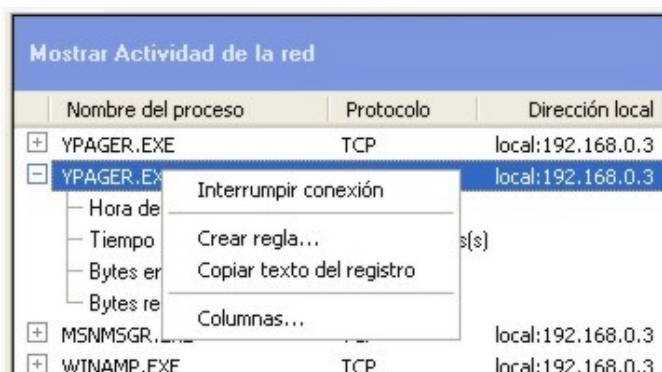


Mostrar Actividad de la red		
Nombre del proceso	Protocolo	Dirección local
+ YPAGER.EXE	TCP	local:192.168.0.3
- YPAGER.EXE	TCP	local:192.168.0.3
- Hora de inicio: 6:38:05		
- Tiempo operativo: 10 hora(s) 15 min(s) 00 s(s)		
- Bytes enviados: 0 bytes		
- Bytes recibidos: 0 bytes		
+ MSNMSGR.EXE	TCP	local:192.168.0.3
+ WINAMP.EXE	TCP	local:192.168.0.3

El título que no esté precedido por ningún signo no contiene información adicional.

Para obtener información avanzada sobre cómo personalizar el panel de información, consulte la sección [columnas](#) en el Apéndice A.

Al igual que en la mayoría de los elementos de Outpost Network Security Client, al pulsar con el botón secundario en el Panel de información se desplegará un menú contextual, que pertenece siempre a la categoría seleccionada.



Mostrar Actividad de la red		
Nombre del proceso	Protocolo	Dirección local
+ YPAGER.EXE	TCP	local:192.168.0.3
- YPAGER.EXE	TCP	local:192.168.0.3
- Hora de inicio: 6:38:05		
- Tiempo operativo: 10 hora(s) 15 min(s) 00 s(s)		
- Bytes enviados: 0 bytes		
- Bytes recibidos: 0 bytes		
+ MSNMSGR.EXE	TCP	local:192.168.0.3
+ WINAMP.EXE	TCP	local:192.168.0.3

- Interrumpir conexión
- Crear regla...
- Copiar texto del registro
- Columnas...

El menú del Panel de información, que se muestra en la imagen superior, es la manera de simple de acceder a funciones de suma utilidad, que serán apreciadas tanto por usuarios comunes como administradores de sistema.

Para todos sus elementos, categorías, paneles e iconos, Outpost Network Security Client hace un uso extenso de los menús contextuales. Un poco de experiencia ayudará al usuario a descubrir la función de cada uno, lo cual resultará más instructivo que leer varias descripciones detalladas de sus elementos. Las opciones de los menús que se han mencionado anteriormente son claras y fáciles de entender por cualquier nivel de usuario.

## La Barra de herramientas

La barra de herramientas está inmediatamente debajo de la barra de menús, y presenta esta imagen, inmediatamente de instalado Outpost.



Se puede ver cuál es la función que cumple cada botón con sólo mantener el cursor sobre el mismo durante unos segundos.

El icono que se halla en el extremo izquierdo de la Barra de herramientas muestra la política actual de Outpost Network Security Client. Al pulsar en este icono, se despliega un menú que puede ser utilizado para cambiar rápidamente entre los modos de funcionamiento del cortafuegos.



Sólo algunos de los botones están activos y visibles en cada momento, dependiendo de la categoría marcada en el Panel izquierdo o en el Panel de información.

Cada botón de la Barra de herramientas es un acceso directo a un objeto de menú, excepto el botón **Ayuda**. Los botones son simplemente una ruta directa y sencilla hacia las diversas funciones, y evitan la búsqueda entre diferentes menús o ventanas para acceder a ellas.

### Los botones en la barra de herramientas

Botón	Función	Ruta al menú
	Cambia la política de Outpost Network Security Client.	Opciones, Política
	Acceso directo a la ventana de diálogo de Opciones	Opciones
	Cambia el agrupamiento de los elementos en la lista	Ver, Agrupar por
	Reduce la lista de sucesos para mostrar sólo los de un horario específico.	Ver, Filtrar por tiempo
	Abre el Visor de registros de Outpost, que muestra los sucesos.	Herramientas, Visor de Registros
	Muestra la ayuda contextual de Outpost Network Security Client.	Ayuda, Ayuda contextual.

## Configuración de Outpost Network Security Client

### Información básica

Un cortafuegos en un ordenador cumple la misma función que una cerradura en la puerta de un hogar. En la mayoría de las ciudades, cerramos la puerta principal de nuestras casas cuando salimos.

Esto no quiere decir que la mayoría de nuestros vecinos sean criminales o que no confiemos en ellos.

Generalmente, cerramos las puertas con llave para evitar que algún delincuente pueda violentar nuestra privacidad, robar nuestras pertenencias o causarnos otros daños.

Internet es muy similar: la mayoría de los sitios son benignos y discretos. Sólo un pequeño porcentaje representa algún tipo de amenaza.

Sin embargo, como existe una enorme cantidad de usuarios de Internet, esta fracción con intenciones destructivas, relativamente pequeña, equivale sin embargo a un gran número de personas. Por esta razón, no es prudente que el ordenador funcione sin protección alguna.

Outpost Network Security Client ha sido desarrollado para detectar las conexiones sospechosas. Se recomienda mantener el cortafuegos en el modo **Asistente para la creación de reglas**, durante varios días de uso.

Para el usuario que no esté familiarizado con el funcionamiento de un cortafuegos, el Asistente para la creación de reglas es el modo más sencillo de utilizar.

✍ Si tiene alguna duda sobre el funcionamiento de la configuración predeterminada, se recomienda que **no realice cambios** si no está absolutamente seguro de lo que está haciendo.

Aún cuando entienda cómo y para qué hacer las modificaciones, se aconseja que guarde o grabe las configuraciones antes de editarlas.

Cuando Outpost alerta al usuario sobre un pedido sospechoso de conexión, por parte de una aplicación instalada en el ordenador o que inicia su ejecución desde Internet, el cortafuegos brinda ciertos datos sobre dicho pedido.

Entre la información que entrega al respecto, se hallan los datos del servidor de nombres de dominio (*Domain Name Server; DNS*), la dirección del protocolo de Internet (*Internet Protocol, IP*) de un ordenador remoto, la aplicación que realiza el pedido, y otros detalles que ayudan al usuario a resolver si desea permitir o prohibir la conexión.

En caso de duda, simplemente impida la conexión **Sólo por esta vez**, y observe el resultado. Si esta acción no le permite realizar lo que deseaba, inténtelo de nuevo, pero esta vez permita la conexión cuando se le pregunte.

De esta forma podrá aprender cuáles son las acciones que efectúan las aplicaciones, con cuáles de ellas debe ser cauteloso, e incluso cuáles debería desinstalar del sistema. Outpost también lo alertará contra la presencia de algún programa malicioso, como los denominados troyanos.

✍ Se aconseja mantener la configuración sugeridas por Outpost si el usuario no tiene una razón en particular, o los conocimientos necesarios para modificarlas.

En Outpost Network Security Client, la configuración de acceso es básicamente una regla que el usuario establece, teniendo en cuenta la información en su ordenador que desea habilitar para el acceso de otros ordenadores, y cuánta información quiere permitir que otros ordenadores le envíen.

Outpost Network Security Client utiliza varias configuraciones de seguridad para mantener protegido el sistema de los accesos indeseados, por parte de otros ordenadores conectados a Internet o a cualquier otro tipo de red.

Asimismo, restringe el flujo de información que ingresa al ordenador, del modo que el usuario juzgue conveniente.


Permite también que el usuario establezca una regla sobre los archivos compartidos, para que el ordenador sólo comparta los archivos con los ordenadores que se consideran confiables, por ejemplo, en una red de área local.

Otro uso común del cortafuegos es restringir la cantidad de información que el ordenador entrega mientras está conectado a Internet.

## Configuraciones iniciales

Outpost Network Security Client está listo para operar una vez instalado. Las configuraciones predeterminadas son más que suficientes para la mayoría de los usuarios. Se recomienda mantenerlas hasta que el usuario entienda por completo el funcionamiento del cortafuegos.

Una vez que el usuario esté familiarizado con las características de Outpost Network Security Client, podrá personalizar el cortafuegos de muchas maneras, para hallar las que mejor satisfagan sus necesidades particulares.

 Las configuraciones de Outpost Network Security Client son asignadas por el administrador a los ordenadores cliente de una red.

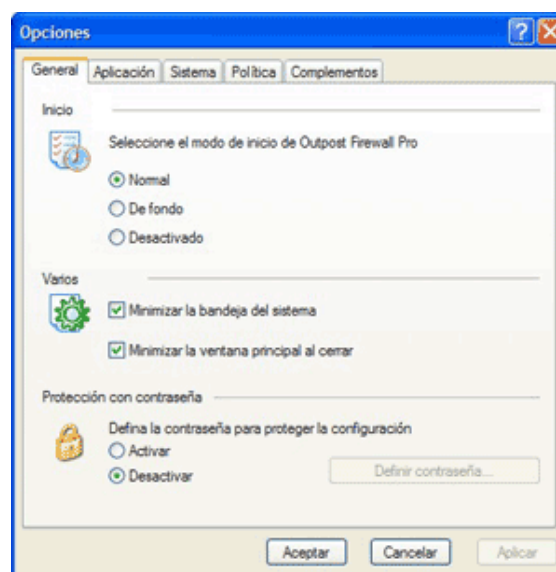
Outpost Network Security Client descarga los parámetros de la configuración del ordenador principal, cada vez que se inicia y a cada hora. Para actualizar la configuración actual, seleccione **Archivo**, y después **Actualizar configuración cliente**.

Tenga en cuenta que el administrador puede prohibir el cambio de las configuraciones específicas. En este caso, todos los cambios que se hayan realizado a la configuración serán reemplazados, al descargar la configuración del administrador.

Esta sección ofrece un breve panorama general, acerca de las maneras de personalizar el sistema. Se pueden modificar estas configuraciones en cualquier momento.

Para ver la ventana de diálogo de las configuraciones de Outpost Network Security Client:

1. Pulse con el botón secundario del ratón sobre el icono de Outpost Network Security Client, en la bandeja del sistema
2. Seleccione **Opciones** en el menú contextual.



En el cuadro **Varios**, de la ventana de diálogo, el usuario puede seleccionar **Minimizar en la bandeja de sistema**, provocando que al minimizar la ventana de principal de Outpost, no se vea un botón en la barra de tareas sino sólo en la barra de sistema.

Para visualizar Outpost nuevamente, es suficiente con pulsar dos veces sobre el icono de la barra de sistema o abrir el menú contextual con el botón secundario del ratón y seleccionar **Mostrar**.

Si selecciona **Minimizar la ventana principal al cerrar**, cuando pulse en el botón **Cerrar** se cerrará la ventana principal de Outpost Network Security Client, pero el cortafuegos continuará en ejecución.

En este caso, para cerrar Outpost Network Security Client:

1. Pulse con el botón secundario del ratón en el icono de Outpost de la bandeja de sistema
2. Seleccione **Salir**.
3. Acepte el mensaje de advertencia.

✎ Si no ha seleccionado la opción precedente, al pulsar en el botón **Cerrar**, un mensaje de advertencia le solicitará que confirme la finalización del servicio Outpost.






### Cómo seleccionar una política

Los **Modos de funcionamiento** se encuentran entre las características más importantes y útiles de Outpost Network Security Client.

Un Modo de funcionamiento define básicamente las posturas que Outpost debe adoptar cuando regula el acceso del ordenador a Internet, o a cualquier otra red a la que esté conectado.

El modo **Bloquear todo**, por ejemplo, determina una actividad sumamente restrictiva, en tanto que el modo **Permitir todo** resulta, en ocasiones, demasiado abierto.

Aquí se detallan los diferentes modos de uso:

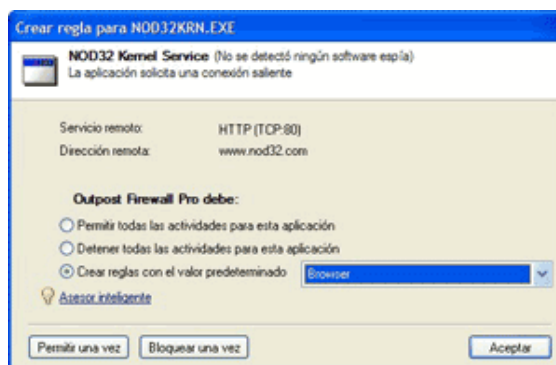
Icono	Modo	Descripción
	Detener todo	Bloquea todas las conexiones de la red.
	Bloquear casi todo	Bloquea todas las conexiones de la red, excepto aquellas que el usuario permita de forma explícita.
	Asistente para la creación de reglas	Determina cómo va a interactuar una aplicación con la red la primera vez que aquella se ejecute.
	Permitir casi todo.	Todas las conexiones de la red están permitidas, excepto las que el usuario bloquee de forma explícita.
	Desactivar	Permite todas las conexiones de la red, y equivale a desactivar el cortafuegos.

En la barra de sistema se visualiza el icono de Outpost que corresponde a la política en ejecución.

El modo **Asistente para la creación de reglas** ayuda al usuario a decidir si habilita o inhibe la conexión a las distintas aplicaciones. Asimismo, simplifica el trabajo de especificar los parámetros aplicables de red para cada programa.

Aunque Outpost Network Security Client crea reglas para aplicaciones ya instaladas en el sistema, pudiera no reconocer algún programa poco común. En este punto, el modo **Asistente para la creación de reglas** puede facilitar la tarea del usuario. En lugar de tener que crear una regla nueva, y a menudo compleja, para cada aplicación nueva que se ejecute, el Asistente para la creación de reglas basará sus parámetros en las configuraciones para los programas ya conocidos.

El Asistente para la creación de reglas también recomienda distintas configuraciones para cada situación específica, desplegando una ventana al detectar un intento de conexión. A menos que el usuario esté seguro de elegir otra opción mejor, se aconseja aceptar dichas recomendaciones.



Outpost Network Security Client tiene una base de datos de las aplicaciones utilizadas con más frecuencia. Nuestros ingenieros han desarrollado las configuraciones ideales para cada tipo de aplicación. De este modo, el usuario sólo tiene que tomar unas pocas decisiones.

El sistema de Outpost Network Security Client agrupa las aplicaciones en tres grupos:

- **Bloqueadas**  
Aplicaciones para las cuales todas las conexiones serán bloqueadas.
- **Parcialmente permitidas**  
Aplicaciones con acceso limitado a la red por medio de reglas especificadas sobre sus puertos, protocolos y direcciones.
- **Confiables**  
Aplicaciones para las cuales serán admitidas todas las solicitudes de conexión .

En la imagen de la ventana de diálogo que se ha presentado como ejemplo, el usuario puede observar:

- Cuál es la aplicación que está solicitando una conexión saliente (Internet Explorer, en este caso).
- Cuál es la forma de acceso que intenta
- Los parámetros básicos de la conexión
- Las decisiones que puede tomar el usuario con respecto al pedido.

El usuario podría, por ejemplo, elegir entre las siguientes posibilidades:

- **Permitir**

Permite todas las actividades del programa.

Se aconseja para aplicaciones completamente confiables.

Se admiten todas las solicitudes de red enviadas por esta aplicación, y se la incluye en la lista de **aplicaciones de confianza**.

- **Bloquear**

Bloquea todas las actividades de esta aplicación.

Se aconseja pPara aplicaciones identificadas como maliciosas, a las que no se les desea permitir el acceso a la red.

Se rechazan todos los pedidos de conexión de este programa, y se lo incluye en la lista de **aplicaciones bloqueadas**.

- **Aplicar reglas predeterminadas**

Establece las reglas para esta aplicación, utilizando configuraciones predeterminadas.

Se aconseja para restringir el acceso de las aplicaciones que pudieran interferir con la red bajo protocolos específicos, o por puertos específicos, entre otros casos.

Crea una regla para la aplicación, que limita el acceso a ciertos puertos y protocolos específicos. Para establecer dichas reglas se usan las configuraciones predeterminadas, desarrolladas por nuestros ingenieros, que resultan óptimas para la mayoría de los propósitos. Se incluye este programa en la lista de **aplicaciones parcialmente permitidas**.

- **Permitir una vez**

Admite sólo la presente solicitud del programa, sin autorizar la conexión para el futuro.

Se aconseja para probar qué resultados tiene la conexión de ciertas aplicaciones que despiertan dudas al usuario.

Esta conexión de red se permite una sola vez. En la siguiente ocasión en que este programa intente establecer una conexión de red, aparecerá esta misma ventana de diálogo. No se establece ninguna regla para esta aplicación.

- **Bloquear una vez**

Rechaza una solicitud de conexión actual, sin ordenar su bloqueo para el futuro.

Se aconseja para aplicaciones que suscitan desconfianza, pero cuya función no se conoce con seguridad.

Esta conexión de red será bloqueada sólo en el caso presente.  
La próxima vez que este programa intente establecer una conexión de red, aparecerá esta misma ventana de diálogo.  
No se establece ninguna regla para la aplicación.

Es probable que Outpost Network Security Client detecte la mayoría de las aplicaciones que acceden regularmente a la red, y que establezca las reglas más convenientes, aproximadamente durante el primer día a partir de su instalación. Una vez que Outpost Network Security Client haya registrado la mayoría de las aplicaciones, el usuario podrá activar el modo **Bloquear casi todo**.

También es posible crear reglas totalmente nuevas, en lugar de aplicar las predeterminadas.

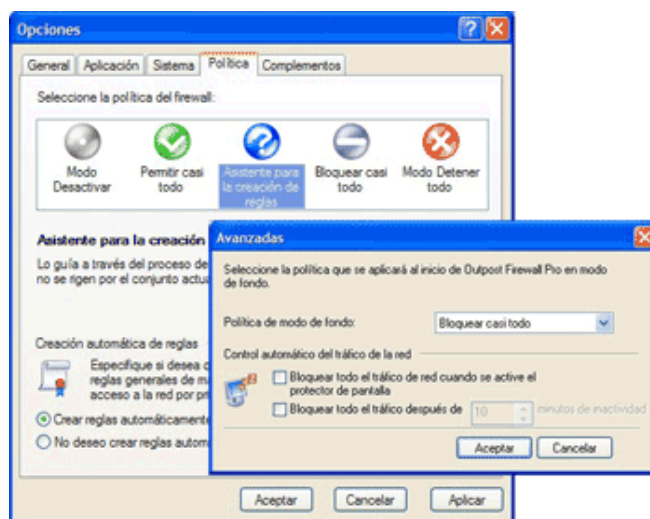
## Para crear una regla

1. Al desplegarse la ventana del Asistente para la creación de reglas, pulse en el menú desplegable de la derecha (Crear reglas con valores predeterminados) y seleccione el valor **Otro**.
2. Pulse en el botón **Aceptar**.
3. Aparecerá la ventana de diálogo **Reglas**, donde podrá establecer las normas que desee para cualquier aplicación.

Cuando Outpost Network Security Client se ejecuta en el modo **Fondo**, no podrá utilizar el Asistente para la creación de reglas, ya que dicho modo está diseñado para que funcione sin requerir la intervención del usuario.

Por lo tanto, en este caso tendrá que modificar la **Política de uso** de Outpost Network Security Client, seleccionando otra opción en lugar del Asistente para la creación de reglas.

1. Acceda al cuadro de diálogo **Opciones**
2. Pulse en la pestaña **Política**
3. Pulse en el botón Avanzadas.
4. Aparecerá el cuadro de diálogo **Política del modo de fondo**.
5. Escoja el tipo de política que desee aplicar.



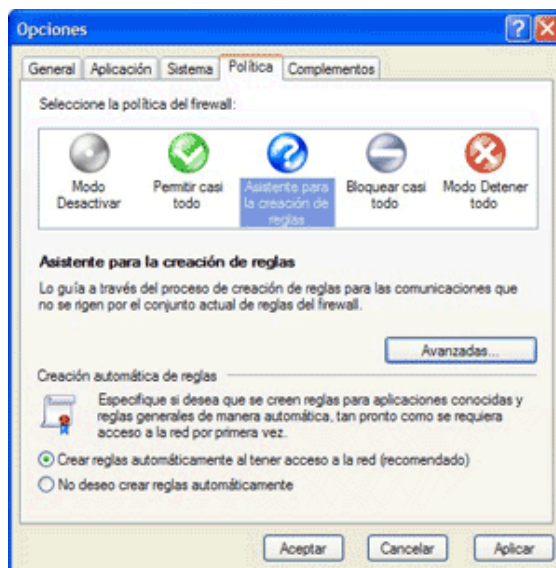
## Control automático del tráfico de red

Outpost Network Security Client puede bloquear todas las comunicaciones y tráfico de red mientras el sistema esté inactivo por un tiempo determinado. Esta función actúa de modo similar a un protector de pantalla e incluso, como veremos, puede sincronizarse con ese tipo de programas.

Esta función ayuda a proteger el sistema contra los accesos no autorizados, en momentos en que el usuario no esté presente. También puede prevenir que algunas aplicaciones legítimas consuman el ancho de banda de la red, mientras el usuario no utiliza el ordenador.

Para configurar el temporizador de inactividad:

1. En la Barra de herramientas pulse en **Opciones**.
2. Seleccione la pestaña **Política**.



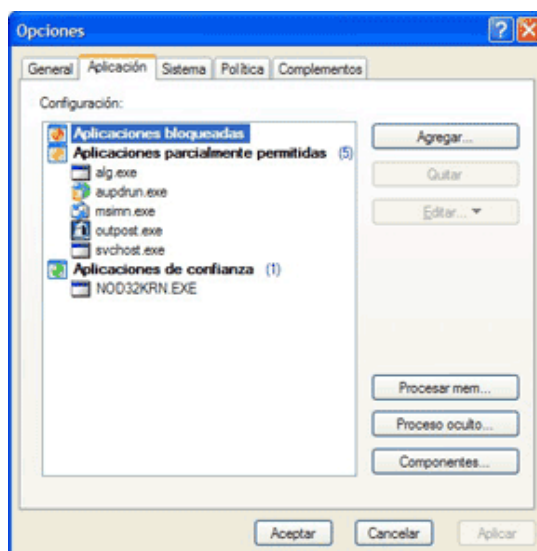
Pulse en el botón avanzada y establezca la configuración según sus preferencias.

### Filtro del nivel aplicación

Una de las funciones más importantes de Outpost es el filtro de nivel de aplicación. Dicho filtro ayuda al usuario a decidir la aceptación o denegación de acceso para cada programa.

Para acceder a la ventana de diálogo **Aplicaciones**, correspondiente a esta función:

1. Pulse en el icono de Outpost que se encuentra en la bandeja del sistema, con el botón secundario del ratón.
2. Seleccione **Opciones**.
3. Acceda a la pestaña **Aplicaciones**.



Outpost Network Security Client divide las aplicaciones en tres categorías:

- **Bloqueadas**

Toda actividad de red quedará bloqueada para este grupo. Se recomienda incluir aquí todas las aplicaciones que no necesiten acceso a Internet, tales como procesadores de texto, calculadoras, entre muchas otras.

- **Parcialmente permitidas**

Outpost Network Security Client permitirá o denegará las solicitudes de acceso a Internet de estas aplicaciones, basándose en las reglas establecidas según los métodos ya explicados. Se aconseja agregar la mayoría de las aplicaciones a este grupo.

- **De confianza**


Se permitirán todas las actividades de esta aplicación. No se recomienda incluir una aplicación en este grupo, a menos que el usuario confíe absolutamente en ella.

No es necesario agregar manualmente las aplicaciones a estos grupos. El Asistente para la creación de reglas lo hace de forma automática.

Se puede cambiar en cualquier momento la categoría de una aplicación, trasladándola de un grupo a otro. Sólo hay que pulsar en su nombre y moverla hacia el lugar deseado, manteniendo oprimido el botón principal del ratón.

También se puede agregar una aplicación desde el Explorador de Windows o desde el Escritorio:

1. Abra la ventana principal de Outpost.
2. Pulse en el menú **Opciones** y después en la pestaña **Aplicación**.
3. Abra el Explorador de Windows.
4. Con el botón principal de ratón, tome y arrastre un archivo ejecutable desde el Explorador hasta la pestaña Aplicación, pasando (y sin soltar) por el botón de Outpost en la barra de tareas, para depositarlo en la categoría deseada.

 Para efectuar este procedimiento, a veces es necesario detener el ratón unos segundos sobre el botón de Outpost en la barra de tareas, hasta que la ventana principal pase a estar activa.

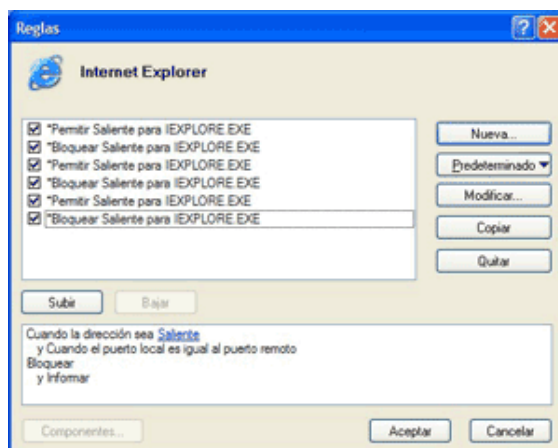
Otro método para lograr el mismo objetivo:

1. Pulse en el botón **Agregar** de la pestaña **Aplicación**.
2. Localice el archivo **ejecutable** de la aplicación correspondiente.
3. Pulse en el botón **Abrir**.

Si esta aplicación ya está en la lista, bajo otra categoría, será eliminada de esta última e incluida en la que haya seleccionado el usuario.

El botón **Editar** le permite al usuario cambiar cualquier configuración detallada, para cualquier aplicación que seleccione.

Cuando una aplicación sea movida o agregada a la categoría **Parcialmente permitida**, aparecerá el siguiente cuadro de diálogo con la lista de reglas:



Por medio de este cuadro de diálogo, los usuarios expertos pueden editar cada una de las diferentes configuraciones de cada componente interviniente. Sólo es necesario marcar cualquiera de ellas y presionar el botón **Modificar**. Este tema se explica detalladamente en la sección [Creación de reglas para las aplicaciones](#).

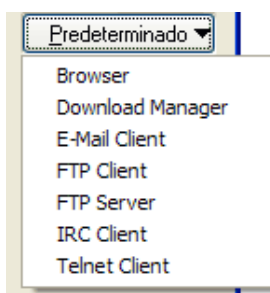
Una forma aún más simple es utilizar el botón **Predefinido**, para seleccionar el tipo general de aplicación que mejor se aplica. Las configuraciones para este grupo fueron diseñadas por nuestros ingenieros y son óptimas para la mayoría de los usuarios. Se recomienda el uso de estos parámetros predefinidos incluso a los usuarios avanzados, quienes si lo desean, podrán editar las configuraciones una vez que estén completamente familiarizados con el producto de acuerdo a sus necesidades.

No se aplicará ninguna regla a los programas cuyos casilleros estén desmarcados en esta ventana con el detalle de reglas establecidas.

**⚠ Importante:** Es posible crear diferentes reglas para una misma aplicación. Hay que tener en cuenta que Outpost Network Security Client actúa de acuerdo a la primera instancia de una regla que coincide con la actividad actual de la aplicación, e ignora todas las restantes. Las reglas del cortafuegos son procesadas según el orden en que figuran en la lista, de arriba hacia abajo. Tan pronto como se encuentra una regla correspondiente, se detiene la búsqueda. Cualquier otra regla que coincida con este tipo de comunicación es ignorada, si está por debajo de la primera regla que coincide.

Los botones **Mover hacia arriba** y **Mover hacia abajo** se utilizan para cambiar la secuencia de reglas, para que el usuario determine sus respectivas prioridades. En caso de no hallar ninguna regla, Outpost Network Security Client mostrará la ventana de diálogo del Asistente para la creación de reglas, o simplemente bloquea la conexión. Esto depende de si está funcionando en el modo **Asistente para la creación de reglas** o en el modo **Bloquear casi todo**.

Si presiona el botón **Predeterminado**, en el cuadro de diálogo mencionado, aparecerán las siguientes opciones:



Es muy probable que las opciones en la lista de **Predeterminado** se agreguen a medida que avanza el tiempo o que se modifiquen.

Esto se incluirá en cualquier actualización de Outpost Network Security Client. Para obtener información avanzada sobre la creación de reglas, consulte [Creación de reglas para aplicaciones](#).

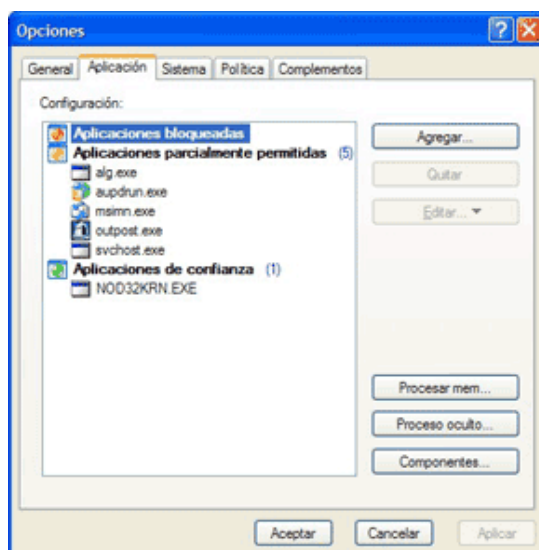
## Control de componentes

Además del comportamiento de las aplicaciones, Outpost Network Security Client controla el de los componentes de cada una. Por lo tanto, cuando se haya modificado un módulo de programa y este desee establecer conexión, Outpost Network Security Client le preguntará al usuario si se debe permitir dicha conexión.

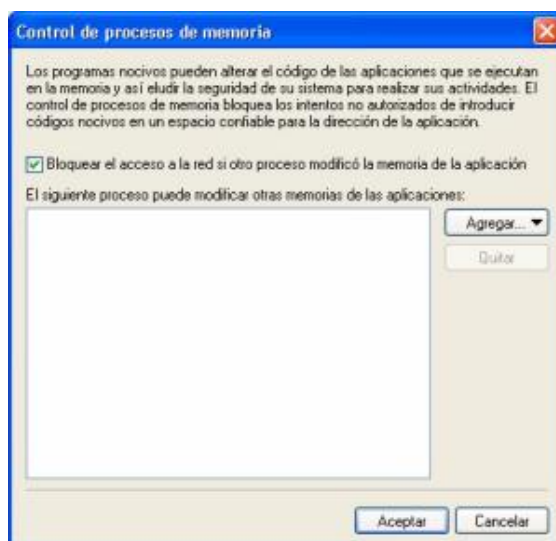
El propósito de esta función es comprobar que los componentes no sean falsos o maliciosos. Algunos troyanos, por ejemplo, pueden ser insertados como módulos de aplicaciones legítimas, para obtener así todos los permisos de conexión.

Outpost Network Security Client permite que el usuario establezca el nivel deseado de Control de componentes.

1. Pulse en el menú Opciones, **Aplicación**.
2. Presione el botón **Componentes**:



3. Se visualizará el siguiente cuadro de diálogo:



4. Seleccione, entre las siguientes opciones; el nivel de control de componentes deseado:

- o **Normal**

Una vez identificados los componentes que contiene cada aplicación en el momento de la instalación de Outpost Network Security Client, el cortafuegos controlará todos los nuevos componentes que se vayan agregando a las mismas. Esta opción es la apropiada para la mayoría de los casos y brinda un balance óptimo entre seguridad y rendimiento.

- o **Máximo**

Outpost Network Security Client controlará todos los componentes que se registren como parte de una aplicación confiable. Ya que esta opción puede impactar seriamente en el rendimiento del sistema, se recomienda utilizarla sólo cuando se sospeche de la existencia de un programa malicioso que aún no haya sido catalogado.

- o **Desactivado**

Esta opción detiene el control de componentes de Outpost Network Security Client. Sólo se recomienda esta configuración cuando el usuario experimenta una reducción importante en el rendimiento, colapsos u otros errores que deriven en la inestabilidad del sistema. Al detener el Control de componente, el nivel de seguridad del sistema se reducirá peligrosamente.

Existe una cantidad de componentes de cada sistema que siempre son utilizados por más de una aplicación. Dos ejemplos, son las bibliotecas de vínculos digitales (*Digital Link Libraries; DLL*) de Windows y los lenguajes comunes en tiempo de ejecución.

Dichos componentes son siempre considerados confiables, ya que no implican ninguna amenaza, y a menudo son compartidos por muchas aplicaciones. Por lo tanto, verificar cada uno de los componentes de este tipo insumiría demasiados recursos del sistema, afectando negativamente su rendimiento.

Para optimizar el rendimiento del Control de componentes, Outpost Network Security Client ofrece la lista **Componentes compartidos**, a la que se pueden añadir elementos confiables, utilizados por más de una aplicación.

Por defecto, todos los componentes ubicados en la carpeta de instalación de Windows y sus subordinadas, se agregan automáticamente a esta lista, una vez instalado Outpost Network Security Client.

Pulse en el botón **Editar lista** para agregar o quitar componentes.



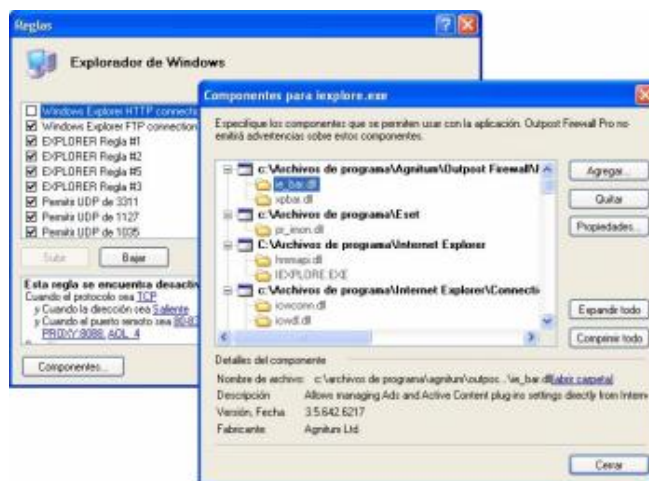
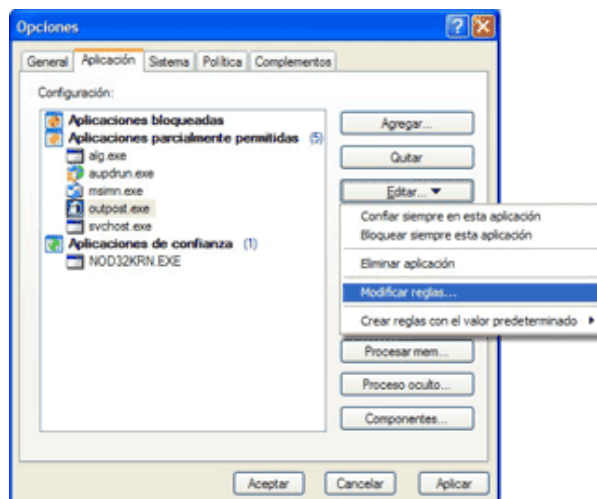
Después de instalar, por ejemplo, un paquete de servicio (*Service Pack*) o algún programa de actualización masiva, que afecte un gran número de componentes comunes, se recomienda seleccionar **Volver a crear base de datos**.

De este modo, Outpost Network Security Client podrá familiarizarse con los cambios realizados en la configuración del sistema.

☑ Después de pulsar en **Volver a crear base de datos**, se perderá toda la información de los componentes que haya sido añadida o modificada manualmente.

Para visualizar los componentes que Outpost Network Security Client controla para cada aplicación:

1. Pulse en el menú Opciones, **Aplicación**.
2. Pulse dos veces sobre una aplicación de la lista o seleccione la misma y posteriormente presione en el botón Editar, **Modificar reglas**.
3. Presione en el botón **Componentes**.



## Procesos ocultos

Muchas aplicaciones habilitadas no acceden directamente a la red, sino que envían procesos derivados para que actúen en su nombre.

Esto permite que algunos procesos eludan el control de los cortafuegos tradicionales, ya que no son tratados como parte de la aplicación respectiva. De tal manera, las restricciones de seguridad del cortafuegos no se aplican a tales procesos.

Además, como el proceso está oculto al usuario, no es posible rastrear las acciones que realiza.

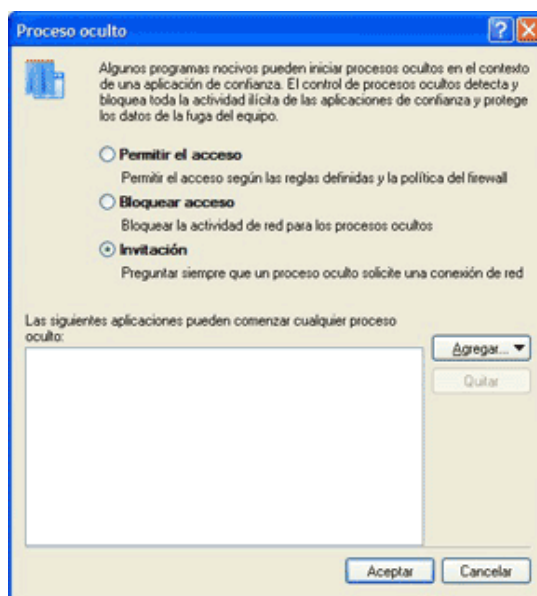
Esta tecnología es utilizada por algunas aplicaciones muy comunes, como Internet Explorer y otras, para realizar el control de las actualizaciones y otras rutinas de mantenimiento de una forma cómoda para el usuario.

Pero, por otro lado, un programa malicioso puede aprovecharse de este tipo de procesos para obtener información confidencial.

Outpost Network Security Client permite al usuario controlar los procesos ocultos, incluyendo los que se ejecuten en nombre de las aplicaciones de confianza, para que no realicen ninguna actividad inapropiada.

Para configurar la gestión de estos procesos:

1. Pulse en el menú **Opciones**, Aplicación.
2. Presione el botón **Procesos ocultos**.



3. Seleccione la política deseada para los procesos ocultos según su particular entorno de trabajo:

- **Permitir el acceso**

Permite a estos procesos acceder a la red, según las reglas y restricciones de la aplicación correspondiente. No se recomienda seleccionar esta opción, a menos que esté completamente seguro que se está ejecutando un programa confiable. De otra forma, esta opción puede permitir el acceso de programas maliciosos a la red y la salida de información confidencial del usuario.

- **Bloquear el acceso**

Se restringirá el uso de la red a todos los procesos de este tipo. Seleccione esta opción sólo en circunstancias de emergencia, o cuando considere que su ordenador está siendo atacado por un programa malicioso.

- **Invitación**

Outpost Network Security Client le solicitará autorización, cada vez que un proceso de esta índole trate de conectarse a la red. Se recomienda esta opción para la mayoría de los casos, ya que el usuario tendrá que decidir si permite o bloquea la comunicación cada vez que Outpost Network Security Client se lo pregunte. De este modo, podrá identificar la actividad realizada en el sistema.

## Control de procesos en memoria

Varios troyanos y virus utilizan técnicas sofisticadas, que les permiten alterar el código de las aplicaciones de confianza que se ejecutan en la memoria. De esta manera logran transgredir el perímetro de seguridad del sistema, para realizar sus actividades maliciosas.

Este método es conocido como inyección de código, o vulnerabilidad a la copia (*Copycat*).

Outpost Network Security Client controla las funciones que pueden ser utilizadas para inyectar códigos maliciosos dentro de la dirección de una aplicación de confianza. De este modo evita que los procesos corruptos implementen sus maniobras.

Para habilitar el control de proceso de memoria:

1. Pulse en el menú **Opciones**, Aplicación.
2. Presione el botón **Procesos en memoria**.
3. Active **Bloquear el acceso a la red si otro proceso modificó la memoria de la aplicación**.



## Complementos

### Introducción

El uso de complementos (*Plug-Ins*) es una estrategia de diseño sumamente efectiva y útil de Outpost Network Security Client.

Estos módulos pueden ser creados por desarrolladores independientes y fácilmente agregados para incrementar las aptitudes y características del cortafuegos.

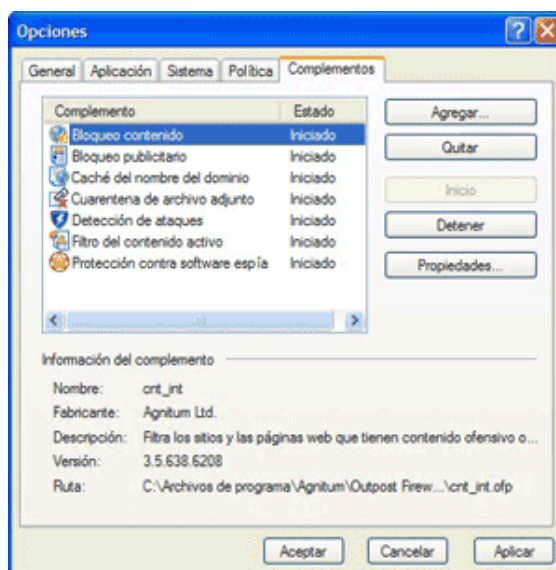
Si está interesado en desarrollar complementos para Outpost Network Security Client, por favor visite: [http://www.outpost-es.com/products\\_features\\_plugins/plugins.html](http://www.outpost-es.com/products_features_plugins/plugins.html)

Vale destacar que los complementos son absolutamente independientes entre sí, y también del módulo principal de Outpost Network Security Client.

Para acceder a la ventana de diálogo que controla estos complementos:

1. Pulse con el botón secundario del ratón en el icono de la bandeja de sistema
2. Seleccione **Opciones** y después, en la pestaña **Complementos**.

✍ También se puede acceder a la misma desde la ventana principal de Outpost, por medio del menú **Opciones, Configuración de los complementos**.



Los botones del lado derecho son:

- **Agregar**  
Se utiliza para agregar un nuevo complemento a Outpost Network Security Client.
- **Quitar**  
Borra, de la lista, un complemento seleccionado.
- **Inicio**  
Activa un complemento seleccionado que estuviera detenido.
- **Detener**  
Detiene la ejecución de un complemento seleccionado, sin eliminarlo de la lista de Outpost.
- **Propiedades**  
Modifica cualquier parámetro de un complemento seleccionado. Los tipos de configuraciones varían según los diferentes complementos.

⚠ **Importante:** Sólo se pueden modificar los parámetros de aquellos complementos que se hayan iniciado.

También puede acceder a la configuración de un complemento desde la ventana principal de Outpost:

1. Pulse con el botón secundario del ratón sobre el icono del complemento.
2. Seleccione **Propiedades**.

Otro modo de acceder:

1. Pulse con el botón secundario del ratón sobre el icono de Outpost en la barra de sistema.
2. Seleccione **Opciones**.

3. Pulse sobre la pestaña **Complementos**.
4. Seleccione el complemento cuyos parámetros desea modificar y presione el botón **Propiedades**.

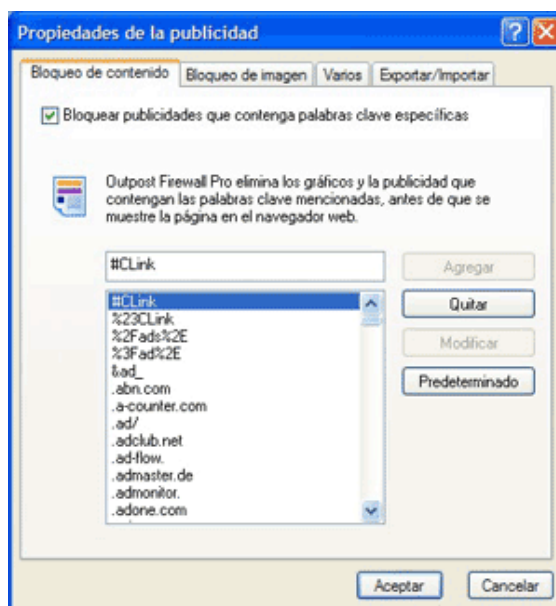
La sección **Información del complemento**, en la mitad inferior del cuadro de diálogo, muestra las propiedades más importantes del elemento seleccionado y, la ubicación en el sistema, del archivo **.ofp** del mismo.

### Bloqueo de anuncios publicitarios

Cada día, más sitios de Internet se llenan de publicidad. Esto no suele ser un problema si se dispone de una conexión rápida, pero sería preferible navegar sin la distracción de tantos anuncios publicitarios móviles.

Para cambiar la configuración del bloqueo de publicidad de Outpost Network Security Client:

1. Pulse con el botón secundario del ratón en el icono en la bandeja de sistema, para visualizar el menú contextual.
2. Seleccione **Opciones**.
3. Pulse en la pestaña **Complementos**.
4. Pulse en **Bloqueo publicitario** y después, sobre el botón **Propiedades**.



Outpost Network Security Client puede bloquear la visualización de publicidad de ciertos anunciantes.

Al instalarse, Outpost Network Security Client ya tiene incorporada una larga lista de las palabras más comunes utilizadas en la publicidad de Internet, que suelen ser direcciones ubicadas dentro de las etiquetas HTML denominadas **IMG SRC** y **A HREF**, que vinculan las páginas con archivos de imagen o con otras páginas, respectivamente.

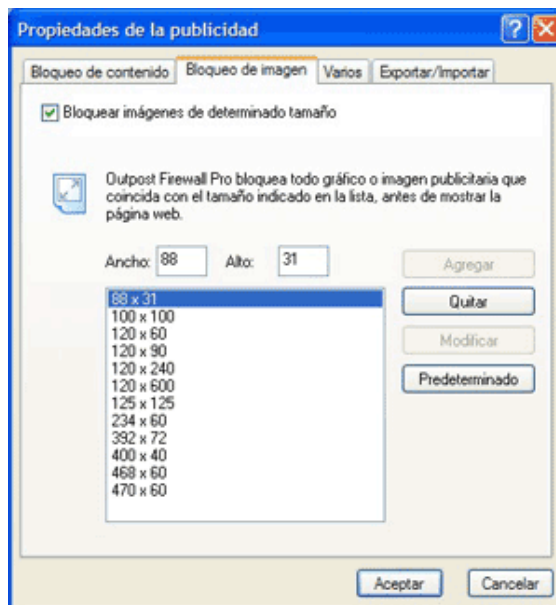
Para agregar otra palabra a la lista, simplemente ingrésela en el campo arriba de la lista y pulse en el botón **Agregar**.

Outpost Network Security Client reemplaza cualquier publicidad que contenga una de esas palabras con el texto **[AD-IMG]**.

Compruebe que la opción **Bloquear publicidades que contengan palabras claves específicas** esté seleccionada.

Pulse en **Agregar** para agregar una nueva anotación a la lista, o **Modificar** para cambiar una ya existente.

También, Outpost Network Security Client puede bloquear todos los anuncios publicitarios de tamaño estándar y se accede a la configuración de esta característica pulsando sobre la pestaña **Bloqueo de imagen**.



Outpost Network Security Client permite bloquear todas las imágenes gráficas de tamaño específico que contengan algún vínculo, tal como ha sido explicado anteriormente.

Asegúrese de haber seleccionado **Bloquear imágenes de determinado tamaño**.

Inmediatamente después de la instalación, Outpost Network Security Client está configurado para bloquear todas las imágenes que contengan vínculos, de los siguientes tamaños:

- 100 x 100 píxeles.
- 125 x 125 píxeles.
- 468 x 60 píxeles.
- 470 x 60 píxeles.
- 234 x 60 píxeles.
- 120 x 80 píxeles.
- 88 x 31 píxeles.

Por defecto, Outpost Network Security Client reemplaza las publicidades gráficas con el texto [AD] en la página Web.

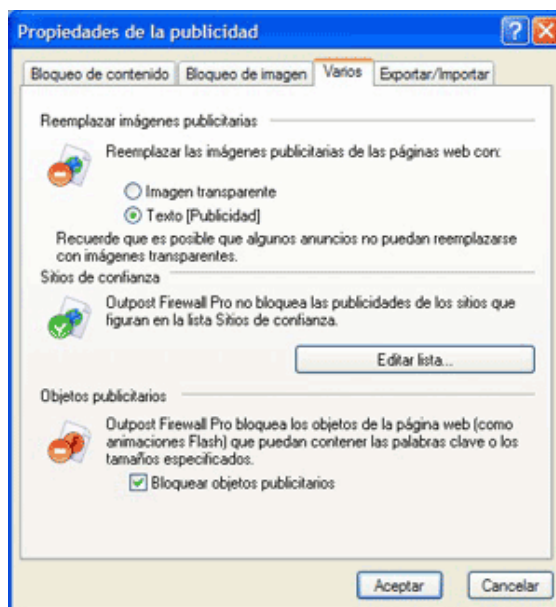
Para agregar a la lista de imágenes otros tamaños que se desean bloquear, escriba el tamaño y pulse en el botón **Agregar**. Hay que tener en cuenta que Outpost Network Security Client bloquea imágenes publicitarias de acuerdo con los parámetros especificados.

Algunas imágenes legítimas pudieran ser bloqueadas si los parámetros son muy estrictos, como resultaría de agregar la palabra "imagen" a la lista de palabras bloqueadas. Además, es probable que algunas publicidades no serán bloqueadas con esta configuración predeterminada del complemento.

Para permitir que todos los gráficos se muestren en la pantalla, desmarque el casillero **Bloquear imágenes de determinado tamaño**.

Outpost Network Security Client también le permite al usuario especificar si desea reemplazar las imágenes publicitarias con un mensaje de texto **[AD]**, o con imágenes transparentes del mismo tamaño que la publicidad.

También posee una lista de **Sitios de confianza** a la que se le pueden agregar los sitios de Internet cuyos anuncios no se desean bloquear. Pulse en la pestaña **Varios** para cambiar estos parámetros.



✍ Algunos gráficos publicitarios no pueden ser reemplazados con imágenes transparentes, por lo que serán sustituidas con mensajes de texto sin importar la opción especificada.

La publicidad moderna de Internet no sólo incluye publicidad gráfica, sino que también utiliza varios objetos ActiveX para mostrar sus anuncios.

El ejemplo más simple consiste en las películas de Macromedia Flash, programa que se utiliza ampliamente en los sitios de Internet.

Tales anuncios consumen mucho más recursos de sistema y ancho de banda de la red, que las publicidades tradicionales. Además, no pueden ser filtradas por las herramientas más comúnmente utilizadas para el bloqueo.

Outpost Network Security Client puede bloquear los anuncios de páginas de Internet que presenten diversos objetos ActiveX.

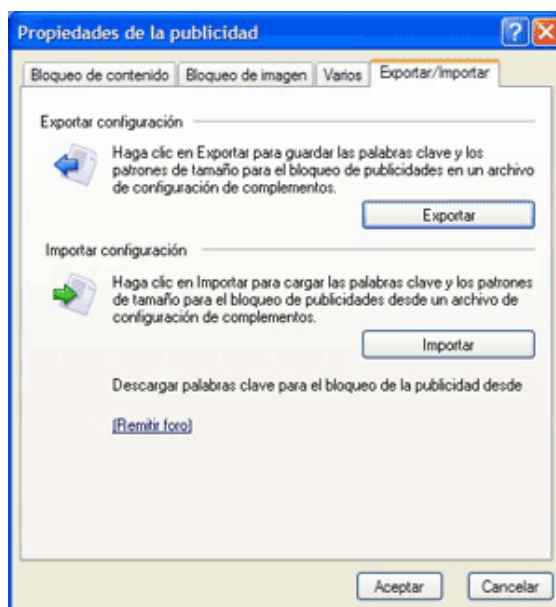
De esta forma, disminuye el uso de recursos de sistema y mejora el ancho de banda para el tráfico deseado. Seleccione **Bloquear objetos publicitarios** para activar este filtro.

Así, Outpost Network Security Client bloqueará dichos objetos, ya sea cuando encuentre una etiqueta **<OBJECT>**, utilizada para insertar estos objetos en las páginas de Internet, que contenga cualquier palabra clave incluida en la lista del filtro de publicidad, o bien cuando el tamaño del área de visualización del objeto coincida con alguno de los tamaños especificados.

Todos los parámetros de la configuración de estos complementos puede guardarse en un archivo especial, para poder utilizarlas nuevamente si el usuario considera poco satisfactorias algunas de las modificaciones, o si desea transferir esos parámetros a otro ordenador.

Para administrar los archivos de configuración de complementos:

1. Pulse en la pestaña **Exportar/Importar** en la ventana de propiedades.
2. Presione en el botón Exportar, para guardar los parámetros o en el botón Importar, para recuperar los mismos.



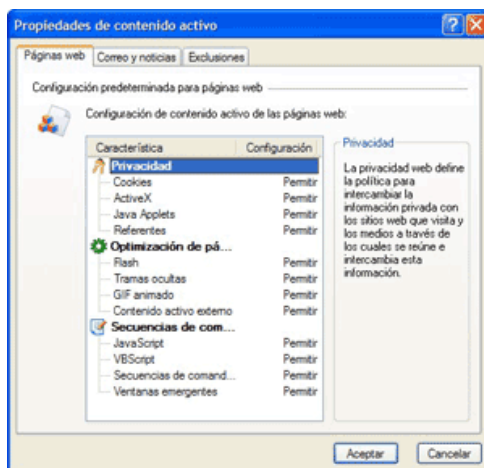
También puede descargar palabras claves para bloquear publicidad, e incrementar la lista predeterminada, accediendo al Foro de Outpost (lista AGNIS), utilizando el vínculo provisto en la ventana.

### **Bloqueo de contenido activo**

El complemento **Filtro del contenido activo** controla la ejecución de los siguientes elementos activos:

- Active X
- Aplicaciones Java
- Programas basados en JavaScript y VBScript
- Cookies
- Ventanas emergentes
- Referentes
- Marcos ocultos
- Animaciones Flash
- Imágenes animadas GIF
- Elementos guionados ActiveX
- Guiones para la navegación de páginas

Estos complementos permiten al usuario habilitar o bloquear independientemente cualquiera de estos elementos, que pueden estar incluidos en las páginas de Internet que visita.



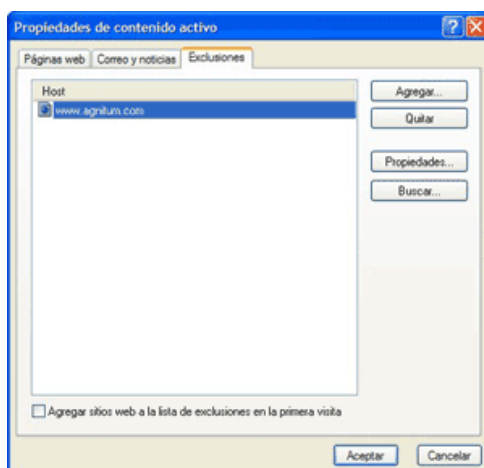
El tratamiento de los elementos interactivos puede ser configurado independientemente para correo electrónico, noticias y páginas de Internet:

1. Pulse en la pestaña **Correo y noticias** o en **Páginas de Internet**, y seleccione la clase de elemento que desee bloquear.
2. El sector derecho de la ventana le mostrará la descripción del elemento y los parámetros para cada selección.
3. Encontrará disponibles las siguientes configuraciones:
  - o **Bloquear**  
Bloquea la acción del contenido activo seleccionado.
  - o **Invitación**  
Solicita autorización para activar el contenido activo seleccionado.
  - o **Permitir**  
Permite la ejecución del elemento activo seleccionado.

De forma predeterminada, el uso de todos los elementos activos está permitido para todas las páginas de Internet.

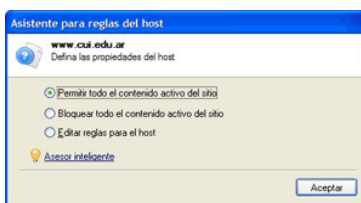
Para configurar los parámetros individuales para sitios de Internet específicos:

1. Seleccione la pestaña **Exclusiones**:

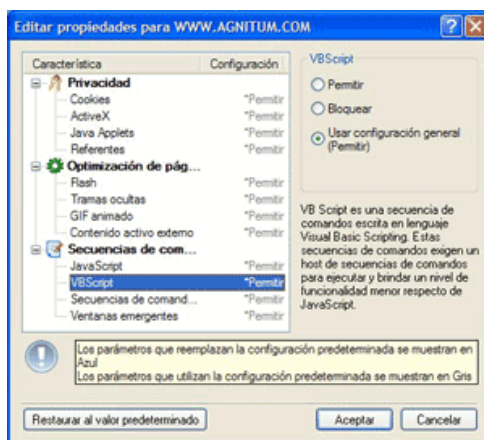


2. Pulse en **Agregar** y escriba la dirección del sitio, con la configuración de contenido activo que desea establecer en particular para dicho sitio.
3. Pulse en el botón **Aceptar**.
4. El sitio recién agregado recibirá todos los parámetros predeterminados para la actividad de contenido activo.
5. Pulse en **Propiedades** para cambiar la configuración específica que se aplicará a este sitio solamente y a cada elemento en particular.

🔗 Si desea configurar, de forma personalizada, cada sitio que visita, seleccione **Agregar sitios de Internet a la lista de Exclusiones en la primera visita**, para que Outpost Network Security Client muestre la ventana del Asistente para reglas del servidor (*host*) cuando una página es accedida por primera vez.



1. Seleccione **Permitir** o **Bloquear todo el contenido activo del sitio**, y este se agregará a la lista de exclusiones.
2. Posteriormente, seleccione **Editar reglas para el servidor**, para visualizar el cuadro de diálogo **Editar propiedades**, en el cual podrá personalizar los parámetros de tratamiento de contenido activo para un sitio específico y para cada elemento.



El sitio puede heredar las configuraciones de la política global o se le puede asignar un valor individual.

🔗 Las configuraciones que heredan valores predeterminados se ven en color gris mientras que las configuraciones a las que se le asignan valores únicos, se verán en color azul.

**Consejo:** este cuadro de diálogo también puede abrirse seleccionando un sitio en la pestaña **Exclusiones**, y pulsando posteriormente en el botón **Propiedades**.

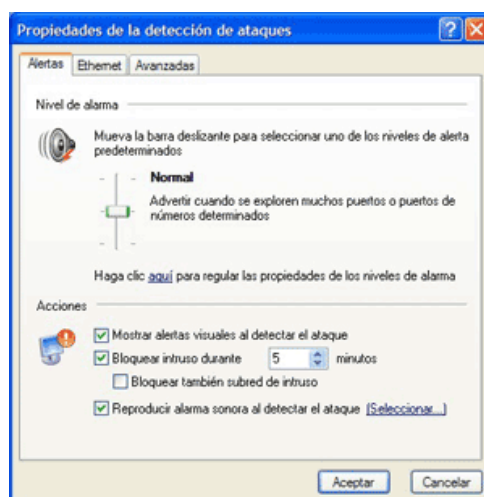
Algunos sitios requieren que todos o algunos de los elementos de contenido activo estén habilitados para poder mostrar sus páginas o funcionar correctamente. Si se restringe demasiado la configuración para todos los sitios, pueden aparecer algunos problemas: imágenes que no se ven, páginas que no aparecen o que se ven mal, o algunos servicios útiles insertados en aplicaciones, que no funcionen.

Si esto sucede con unos pocos sitios, sólo hay que cambiar los parámetros de los complementos para los mismos, como se ha indicado anteriormente, agregándolos a la lista de exclusiones. De lo contrario, se deberá suavizar la política predeterminada para el tratamiento de contenido activo.

## Detección de ataques

El complemento **Detección de ataques** informa al usuario sobre cualquier posible intento de intrusión al ordenador, desde Internet o desde un ordenador en la misma red. También aconseja los pasos a seguir para evitar posibles daños a su sistema.

Este complemento le permite especificar las condiciones en que se mostrará una advertencia. También tiene parámetros de respuesta que se utilizarán si se excede el nivel especificado de seguridad.



En la sección con el nombre **Nivel de alerta**, deslice el botón hacia arriba o hacia abajo, para definir el grado de seguridad deseado.

- **Máximo**  
Se muestra una alerta de detección de ataque aún cuando sólo se verifique un simple vistazo ajeno al puerto.
- **Normal**  
Se muestra una alerta de detección de ataque si varios puertos están siendo explorados, o si un puerto es explorado y Outpost Network Security Client reconoce que es uno comúnmente utilizado por atacantes.
- **Mínima**  
Se muestra una alerta de detección de ataque, sólo si se observan ataques múltiples.

El usuario puede restringir la entrada de los paquetes sospechosos para cada uno de los niveles, con sólo pulsar en el vínculo apropiado. El mismo le mostrará una ventana de diálogo donde podrá especificar el número exacto de paquetes sospechosos que se debe recibir para ser considerados como parte de un ataque.

Especifique los pasos que debe seguir Outpost Network Security Client si se detecta un intento de intrusión en su ordenador:

- **Mostrar alertas visuales al detectar el ataque**  
Outpost Network Security Client mostrará un mensaje de alerta cada vez que se detecte un ataque.
- **Reproducir alarma sonora al detectar el ataque**  
Outpost Network Security Client emitirá un sonido especificado cada vez que se detecte un ataque.

- **Bloquear IP de intruso durante...**

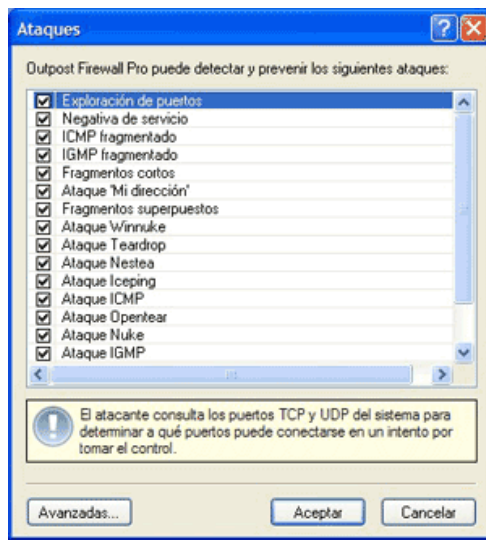
Se bloqueará todo intercambio en la red desde el sistema del agresor durante la cantidad de minutos establecido por el usuario. Por defecto, está fijado en 60 minutos.

- **Bloquear también subred de intruso**

Bloquea todo intercambio con todo el rango de la red de donde proviene la agresión.

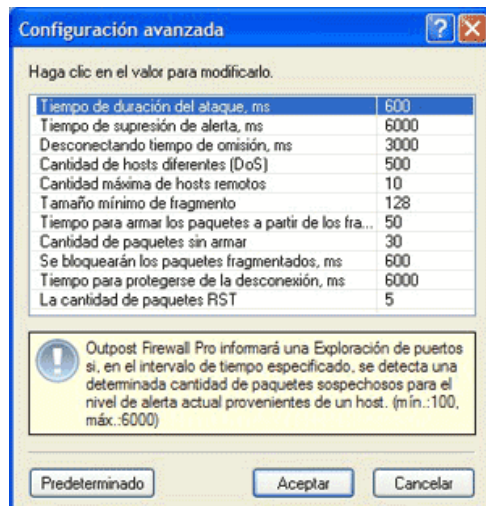
También se pueden seleccionar los ataques que Outpost Network Security Client debe detectar y advertir. Por defecto, Outpost Network Security Client es capaz de reconocer, por lo menos, diez y ocho tipos de ataques y de aprovechamiento malicioso de las vulnerabilidades del sistema (*exploits*).

Sin embargo, el usuario puede preferir que no se detecten ciertos tipos de ataques para eliminar mensajes de alerta, frecuentemente infundados, que pueden aparecer si un servicio de la red, por ejemplo, actúa como si fuera una fuente de ataque.



Para visualizar el cuadro de diálogo **Ataques**:

1. Acceda al cuadro de **Configuración de complementos**, tal como se ha explicado anteriormente.
2. Seleccione **Detección de ataques** y presione el botón **Propiedades**.
3. Pulse en la pestaña **Avanzadas**.
4. Presione el botón **Editar lista**.



Aquí se pueden seleccionar los ataques que el usuario desea que Outpost Network Security Client detecte y advierta.

El botón **Avanzadas** muestra un diálogo que permite cambiar los parámetros que se aplican a todos los ataques de la lista.

Para cambiar los valores de configuración, seleccione el parámetro en la lista y pulse dos veces sobre el valor en la columna derecha.

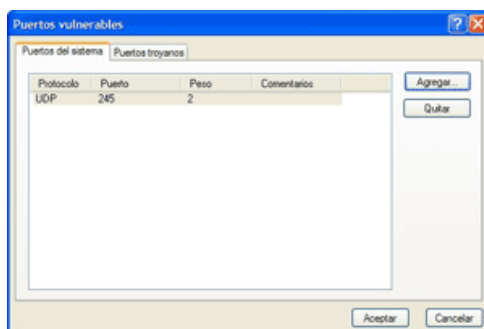
**⚠ Importante:** Hay que tener especial cuidado al cambiar estos parámetros, ya que una configuración inapropiada en la detección de ataques puede acarrear serios problemas con el sistema de conectividad de la red.

Desde el punto de vista de la seguridad, los puertos **TCP y UDP** en el sistema están divididos en varios grupos, de acuerdo a la probabilidad que exista un atacante que los utilice para acceder. Los intentos de acceso a los puertos asignados para servicios vulnerables como **DCOM o RCP**, que tienen mayores probabilidades de éxito, indican que el sistema está siendo explorado, lo cual podría generar, posteriormente, que el sistema sea invadido por un puerto común.

Sin embargo, existen servicios personalizados, que se asignan a determinados puertos que también son tentadores para los atacantes. Outpost Network Security Client permite crear una lista de dichos puertos, que tendrán un control prioritario cuando se analice el tráfico de la red.

Para crear una lista de puertos vulnerables:

1. Acceda al cuadro de **Configuración de complementos**, tal como se ha explicado anteriormente.
2. Seleccione **Detección de ataques** y presione el botón **Propiedades**.
3. Pulse en la pestaña **Avanzadas**.
4. Seleccione **Puertos vulnerables**
5. Pulse en el botón **Especificar**.



Los puertos vulnerables se clasifican en dos grandes grupos:

- **Puertos del sistema**
- **Puertos troyanos**

La lista correspondiente al sistema contiene puertos que son utilizados por los servicios vulnerables del mismo.

La lista llamada Troyanos contiene puertos que son aprovechados por los códigos maliciosos conocidos como troyanos.

Para modificar estas listas:

1. Pulse en la pestaña de acuerdo a la lista que desee cambiar.
2. Pulse en **Agregar** y especifique el Protocolo, Número de puerto y Peso.

✍ El **Peso** es un valor decimal que indica la importancia del puerto. Un número mayor indica un puerto más vulnerable. También se pueden añadir comentarios que describan el propósito del puerto, o cualquier otra cosa que se desee destacar.

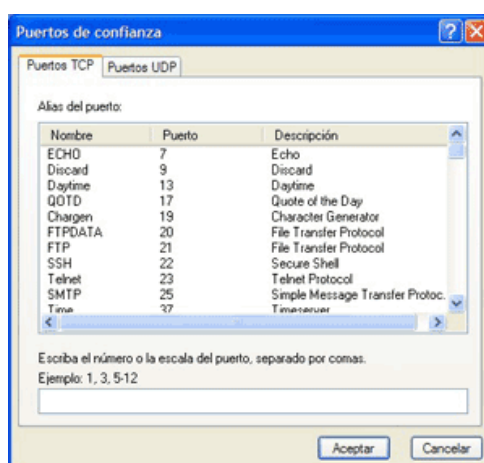
Puede haber ordenadores en una red que no representen ningún tipo de riesgo para la misma, como también puertos en el sistema que no cumplan la función de puerta trasera para los intrusos.

En otras palabras, el análisis de estos puertos y ordenadores puede considerarse de relativa utilidad según el entorno de trabajo y condiciones operativas, por lo que el usuario debe establecer el grado de importancia que tiene esta característica, en función también, de los recursos de sistema disponibles.

El complemento Detección de ataque de Outpost Network Security Client ofrece listas de exclusiones a la que se pueden agregar los servidores remotos (*hosts*) y los puertos que no desea controlar.

Para administrar estas listas:

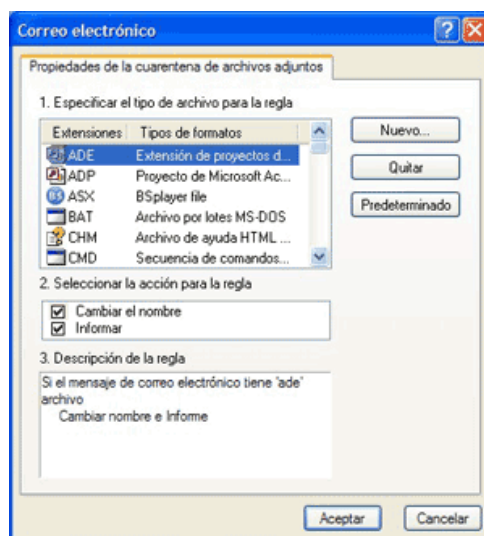
1. Acceda al cuadro de **Configuración de complementos**, tal como se ha explicado anteriormente.
2. Seleccione **Detección de ataques** y presione el botón **Propiedades**.
3. Pulse en la pestaña **Avanzadas**.
4. Bajo el apartado **Exclusiones**, pulse en **Ordenadores (Hosts)** o en **Puertos**.
5. Aquí podrá realizar todas las modificaciones necesarias.
6. Una vez finalizada la edición, pulse en el botón **Aceptar**.



### Cuarentena de archivos adjuntos

Este complemento analiza los archivos adjuntos en mensajes de correo electrónico que recibe el ordenador. Permite especificar cuáles tipos de archivos adjuntos serán puestos en cuarentena para que no dañen el ordenador, como también la manera en que el usuario será informado de su arribo. Se pueden establecer diferentes modos de análisis en este complemento, de acuerdo al tipo de archivo de cada adjunto.

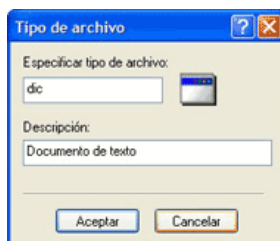
1. Acceda al cuadro de **Configuración de complementos**, tal como se ha explicado anteriormente.
2. Seleccione **Cuarentena de archivo adjunto** y presione el botón **Propiedades**.



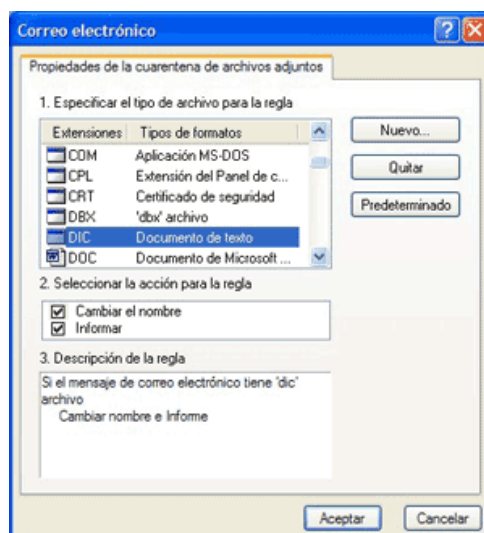
Este complemento tiene en su lista, los tipos de archivos más conocidos.

Si en la lista no se encuentra el tipo de archivo para el cual se desean crear ciertas reglas, se puede crear una nueva para un tipo de fichero en particular.

1. Pulse en el botón **Nuevo...**  
Aparecerá un cuadro de diálogo en el cual se puede especificar la extensión del tipo de archivo. La descripción del mismo es provista automáticamente por Outpost Network Security Client:



2. Pulse en **Aceptar** y se agregará el nuevo tipo de archivo a la lista que Outpost Network Security Client controlará.



3. Establezca las acciones que Outpost deberá realizar al detectarse un archivo con la extensión especificada.
4. Outpost mostrará un mensaje de alerta sobre los mensajes entrantes que adjunten archivos de los tipos que se agregaron.

### Caché DNS

Internet funciona asignándole una serie de números a cada ordenador conectado a ella.

A este número asignado se lo denomina dirección IP y es unívoco para cada ordenador conectado. Un ejemplo de dirección IP podría ser: 64.176.127.178.

Se puede simplemente escribir esta serie de números en el campo de dirección en el navegador (en el cuadro superior de la ventana principal del mismo) y presionando la tecla **Entrar**, el explorador se dirigirá a las páginas de ese ordenador en Internet.

Aunque estas direcciones numéricas IP son fáciles de utilizar para un ordenador, resultarían engorrosas para los humanos. Por tal motivo, se inventó un sistema de direcciones que utiliza palabras o letras llamado **Sistema de nombres de dominio** (*Domain Name System; DNS*). Probablemente se esté más familiarizado con un nombre DNS que con la dirección IP. Un ejemplo de nombre DNS es: www.protegerse.com.

Los nombres DNS son mucho más fáciles de recordar, pero los buscadores necesitan las direcciones IP para encontrar y transferir archivos en Internet.

Por lo tanto, existen bases de datos en Internet que mantienen una correspondencia entre direcciones IP y nombres DNS.

Para encontrar la dirección IP que corresponda a un nombre DNS, habitualmente el explorador tiene que consultar varias bases de datos diferentes, ubicadas en distintos lugares del mundo y esto a veces lleva mucho tiempo.

Para acelerar un poco las cosas, Outpost Network Security Client ofrece una tabla de búsqueda personalizada de direcciones DNS en el ordenador. Se lo denomina **Caché del nombre de dominio** o **Caché DNS**, y se puede personalizar según las preferencias del usuario.

Outpost Network Security Client mantiene el caché DNS automáticamente dentro de las especificaciones del usuario, para incluir aquellas direcciones que el usuario utiliza con más frecuencia.

La cantidad de tiempo que una dirección IP se guardará dependerá del tiempo especificado como uno de los parámetros para este complemento.

También depende de la cantidad de nombres DNS que deba verificar Outpost Network Security Client.

Sólo los nombres más utilizados recientemente se mantienen, hasta una cantidad máxima especificada.

1. Abra la ventana principal de Outpost.
2. Pulse con el botón secundario del ratón sobre el complemento Caché DNS.
3. Verifique que **Activar caché DNS** tenga una marca de verificación para que el mismo esté operativo.

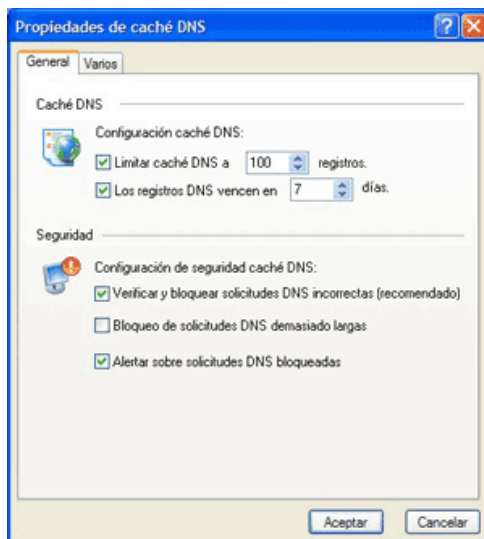
Para modificar los parámetros del complemento Caché DNS, seleccione **Propiedades** en el mismo menú. Se puede limitar la base de datos a un número específico de entradas y que se borren automáticamente si no se utilizan después de cierta cantidad de días.

Para no establecer un límite por tiempo, desmarque el casillero **Los registros DNS vencen en...**

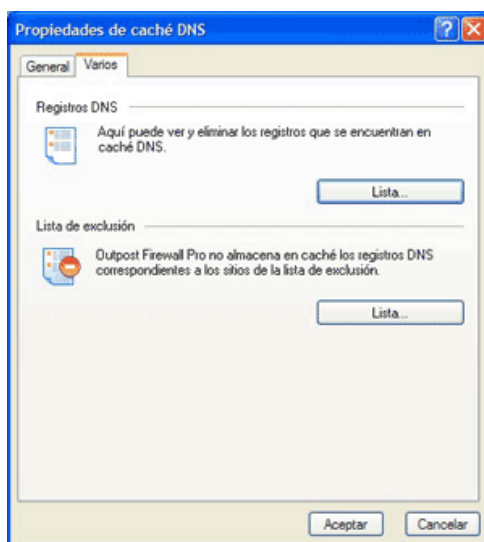
Para mejorar el sistema de seguridad, este complemento bloquea pedidos de DNS inválidos o fraguados que puedan causar un colapso del sistema o servir para el aprovechamiento de una vulnerabilidad en el sistema DNS.

Seleccione la opción **Verificar y bloquear solicitudes DNS incorrectas** para que este complemento bloquee estos pedidos, de modo que un agresor o un programa malicioso no tenga la posibilidad de aprovecharse de un DNS defectuoso del sistema. Además, puede recibir alertas emergentes sobre estos pedidos, para estar informado sobre los ataques DNS contra el sistema.

Para recibir mensajes de advertencia, seleccione el recuadro **Alertar sobre solicitudes DNS bloqueadas**.



La lista de nombres de sitios y sus direcciones IP, guardadas en la memoria caché, puede ser administrada en el cuadro de diálogo de registros DNS. El mismo se puede abrir seleccionando la pestaña **Varios** y pulsando en el botón **Lista** dentro del cuadro Registro DNS.



El complemento Caché DNS también ofrece una **Lista de exclusión** a la que se le pueden agregar los nombres de sitios que no se quieren guardar dentro de la lista específica de correlatividad.

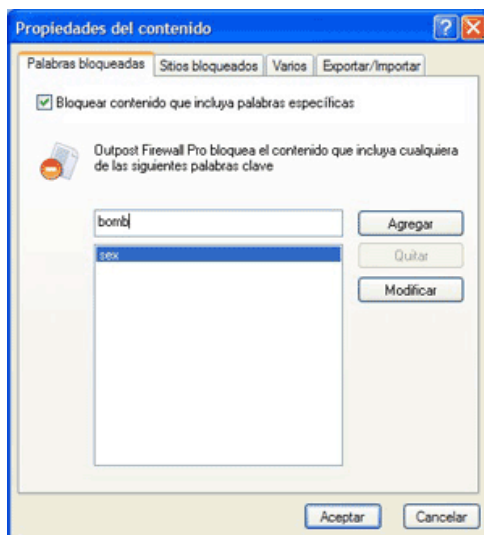
Esta lista es especialmente útil cuando se accede con frecuencia a sitios que tienen una dirección IP que a menudo cambia o cuando se experimentan otros problemas al acceder a sitios específicos desde el ordenador.

Para administrar esta lista, pulse el botón **Lista** debajo de Lista de Exclusión.

## Filtro de Contenido

Con el complemento **Contenido** se puede bloquear la visualización de ciertas páginas o sitios de Internet con material objetable:

1. Acceda al cuadro de **Configuración de complementos**, tal como se ha explicado anteriormente.
2. Seleccione **Contenido** y presione el botón **Propiedades**.

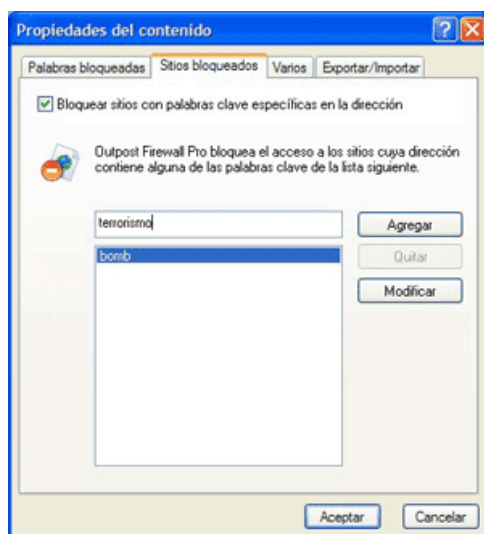


3. Seleccione **Bloquear contenido que incluya palabras específicas**.
4. En el campo de texto escriba cada palabra que desee que Outpost utilice para bloquear aquellas páginas que las contenga.
5. Pulse en **Agregar** para cada palabra o frase que quiera añadir a la lista.

No se mostrará ninguna página de Internet que contenga cualquiera de las palabras de la lista.

Para hacer una lista de sitios específicos en Internet que no desea que se abran en el ordenador:

1. Seleccione la pestaña **Sitios bloqueados**:

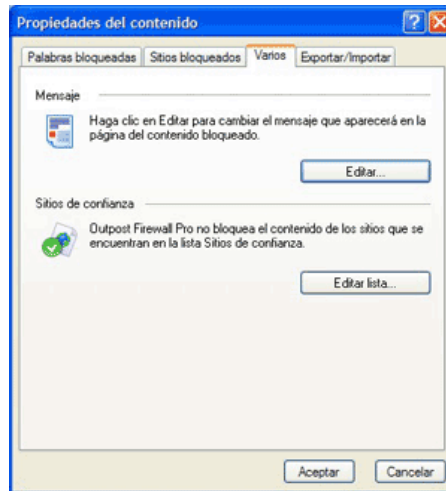


2. Seleccione **Bloquear sitios con palabras claves específicas en la dirección**.

3. Escriba la dirección del sitio de Internet (URL), o parte del mismo que no quiere que se muestre en su ordenador.
4. Pulse en el botón **Agregar** para incorporar cada sitio que desea bloquear.
5. Pulse en el botón **Aceptar**.

Para cambiar el mensaje que aparecerá en lugar de las páginas con material objetable:

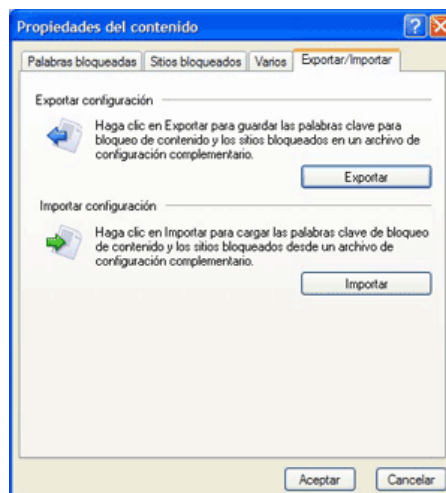
1. Pulse en la pestaña **Varios**.
2. Presione el botón **Editar** del cuadro **Mensaje**.



Outpost Network Security Client también tiene disponible la lista **Sitios de confianza**, que permite la exclusión de sitios de Internet cuyo contenido no se desea bloquear.

Para administrar los archivos de configuración:

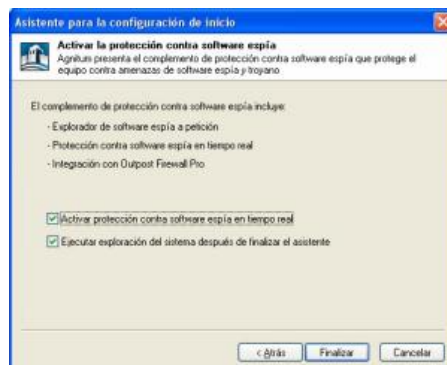
1. Acceda al cuadro de **Configuración de complementos**, tal como se ha explicado anteriormente.
2. Seleccione **Bloqueo contenido** y presione el botón **Propiedades**.
3. Pulse en la pestaña **Exportar/Importar**.
4. Presione el botón correspondiente a la acción a efectuar.
  - ✍ Sólo podrá importar una configuración previamente guardada.



## Protección contra software espía

Dado que el desafío de los programas espía es cada vez más personal y más real, es el momento adecuado para una solución integrada que no solo brinde una solución reactiva al limpiar un ordenador infectado, sino que, en primer lugar, también evite de manera proactiva que los programas espía ingresen en el ordenador.


Inmediatamente de instalado Outpost Network Security Client y tras el primer reinicio, será consultado sobre la activación de este módulo y la búsqueda de programas espía que pudieran estar instalados en su ordenador.

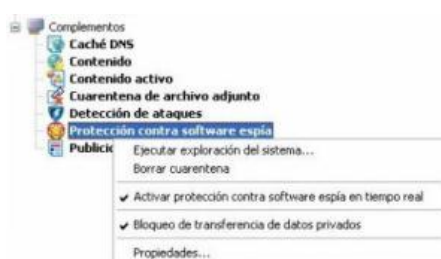


Este complemento permite la detección y eliminación de programas espía, admitiendo procedimientos automatizados o respuestas individuales por parte del usuario, así como establecer una lista de exclusión, asegurar el bloqueo de datos privados especificados correspondientes a contraseñas o números de tarjetas de crédito y definir una lista de acciones que el usuario permitirá para determinados programas.

Este complemento es activado o desactivado desde la ventana principal de Outpost Firewall.

1. Abra la ventana principal de Outpost Network Security Client.
2. Pulse con el botón secundario del ratón sobre el complemento Protección contra software espía.
3. Pulse sobre cada una de las protecciones que desee activar y verifique que posean un tilde a la izquierda del texto.

 Desde esta misma posición podrá iniciar acciones adicionales o acceder a la configuración del complemento.



Para modificar los parámetros de este complemento, también puede acceder siguiendo este camino:

1. Pulse en el menú **Opciones**.
2. Presione **Configuración de complementos**.

3. Seleccione **Protección contra software espía**.

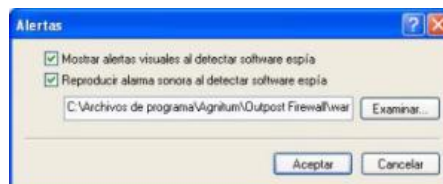
4. Pulse en el botón **Propiedades**.

En la pestaña **General** podrá activar la protección contra software espía, así como establecer que el objeto sea puesto en Cuarentena antes de eliminarlo de su sistema.

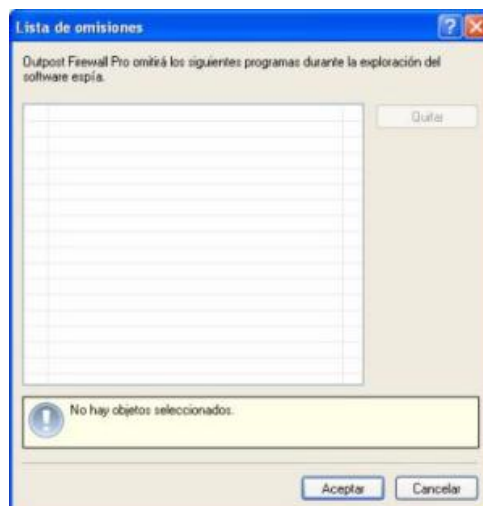
Al detectar la presencia de software espía, Outpost Firewall Pro podrá solicitar una respuesta de parte del usuario o proceder automáticamente.



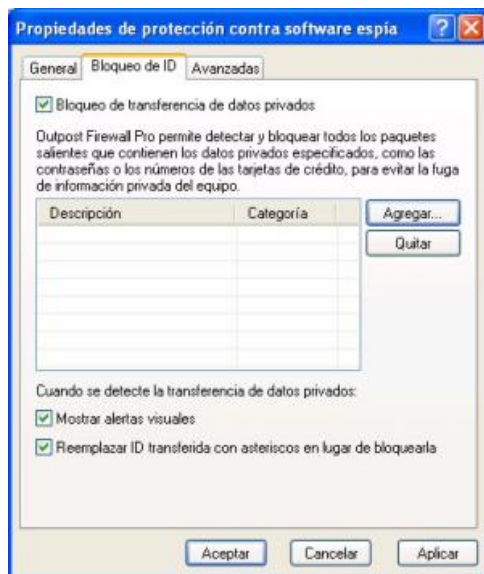
También podrá emitir distintos tipos de alerta informándole del objeto detectado.



Pulsando en el botón **Editar** de la lista de omisiones podrá determinar aquellos programas que no serán analizados por el complemento contra el software espía.



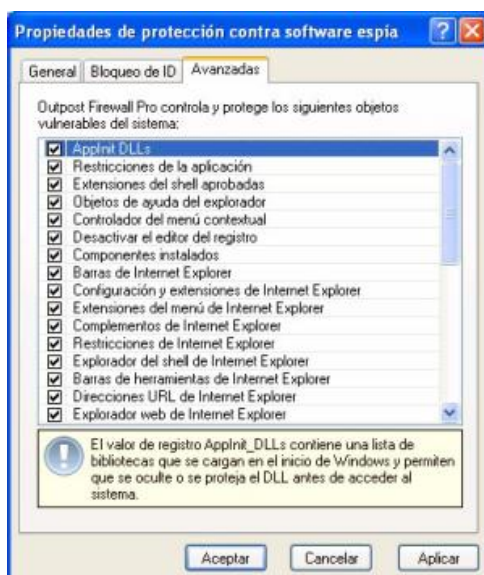
El bloqueo de identificadores ID, le permitirá impedir que sus datos personales especificados puedan fugar de su ordenador, produciendo un bloqueo específico y selectivo de los mismos.



La lista de datos protegidos es completada por el usuario permitiéndole un total control de su privacidad.

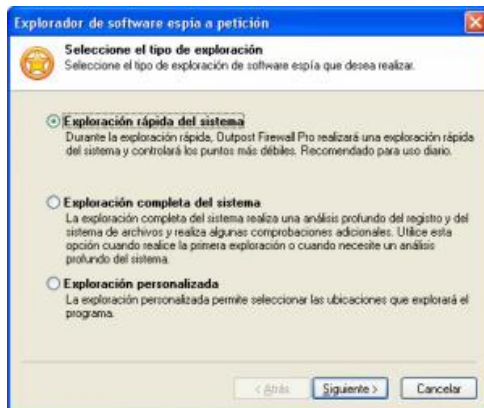


Especifique los elementos sensibles de su sistema sobre los cuales usted desee tener un control y protección más exhaustivo.

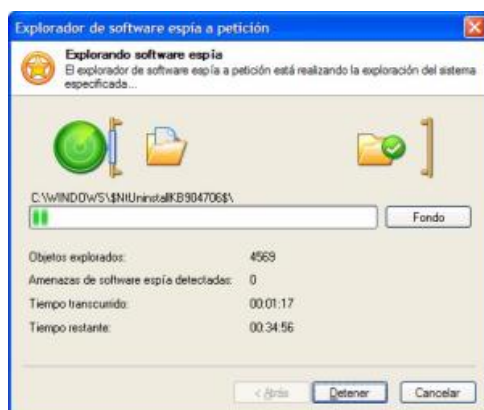


La exploración de su sistema a petición, en busca de software espía le otorgará una segunda línea de defensa y protección adicional.

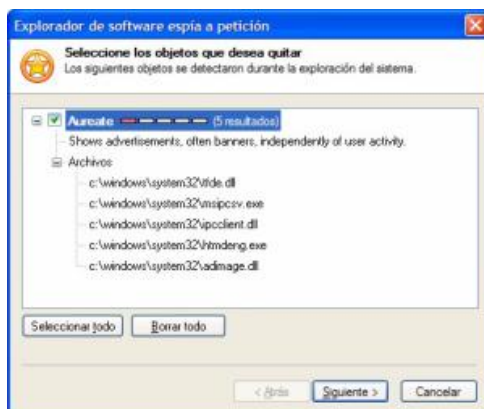
1. Pulse en el menú **Herramientas**.
2. Seleccione **Ejecutar exploración de software espía en el sistema**, pudiendo optar por distintas configuraciones.



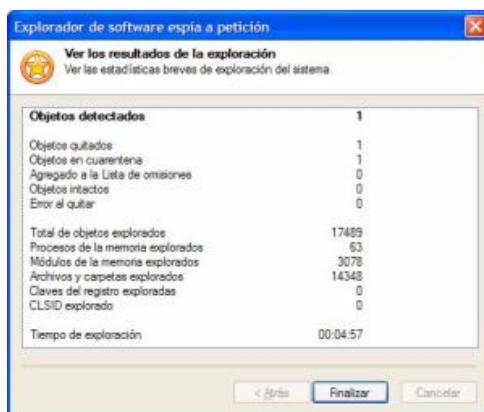
3. Durante la exploración de su sistema, podrá visualizar información adicional sobre el proceso y efectuar el mismo en segundo plano.



4. Si se hubiera encontrado software espía, se le ofrecerán acciones adicionales.



5. Al finalizar, se emitirá un resumen del análisis practicado.



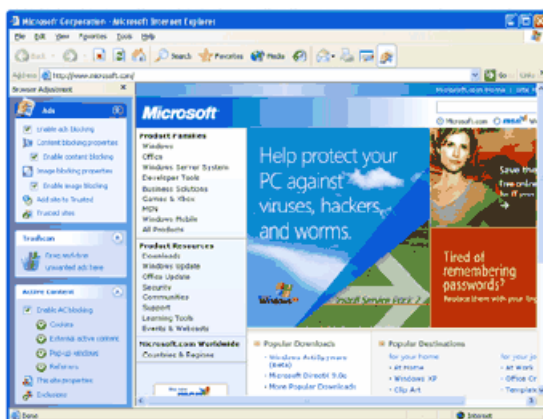
Para visualizar los registros de las conexiones controladas por este complemento, consulte la sección Protección contra software espía del [Visor de registros de Outpost](#).

### Ajuste rápido de Internet Explorer

Outpost Network Security Client proporciona una forma de controlar el contenido de las páginas descargadas, directamente desde el navegador Internet Explorer.

El complemento **Ajuste rápido del navegador**, también denominada **Barra de Outpost**, permite definir ciertos comportamientos y acciones al visualizarse en el navegador Internet Explorer, pudiendo administrarse la configuración de los complementos **Publicidad** y **Contenido activo**.

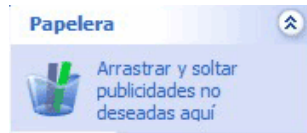
1. Visualice la ventana principal de Outpost.
2. Pulse en el menú **Herramientas** y asegúrese que esté marcado **Activar ajuste rápido en Internet Explorer**.
3. Ejecute una ventana nueva de Internet Explorer.
4. Si no se visualiza este complemento, pulse en el menú **Ver**, Barra del explorador, **Barra de Outpost**.



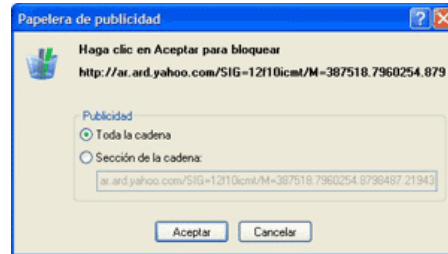
El panel contiene secciones con las configuraciones de los complementos **Publicidades** y **Contenido activo** que son muy similares a las que muestra Outpost Network Security Client en su interfaz.

En la ventana de la barra de Outpost podrá activar o desactivar el bloqueo de publicidad y contenido activo, así como modificar las propiedades de los mismos y especificar distintos parámetros para cada uno de ellos.

También, en esta barra, podrá utilizar la **Papelera de publicidad**, que le permitirá hacer bloqueos selectivos de imágenes publicitarias, directamente arrastrándolas desde una página visitada y depositándola en dicha papelera.



Al hacer esto, aparecerá el siguiente cuadro de diálogo, donde podrá proceder según sus preferencias.



## Para usuarios avanzados

### Configuraciones avanzadas

#### Introducción

Nuestros ingenieros configuraron los parámetros predeterminados de Outpost Network Security Client, de modo que brinde una protección óptima para la mayoría de los sistemas de los ordenadores y las redes.

Outpost Network Security Client fue diseñado desde un principio para ser utilizado de manera efectiva, en su configuración original, aún por los usuarios que no fueran expertos en informática. Ellos necesitan que su ordenador esté protegido contra los programas y los sitios de Internet maliciosos, sin tener que investigar al respecto de protocolos de redes u otros temas específicos para los profesionales.

Sin embargo, también deseábamos que Outpost Network Security Client fuese totalmente configurable por los usuarios avanzados, quienes entienden la tecnología de redes. Y para ellos está dedicado este capítulo, brindándoles información adicional para que puedan editar la configuración de Outpost Network Security Client, y descubrir sus características más poderosas.

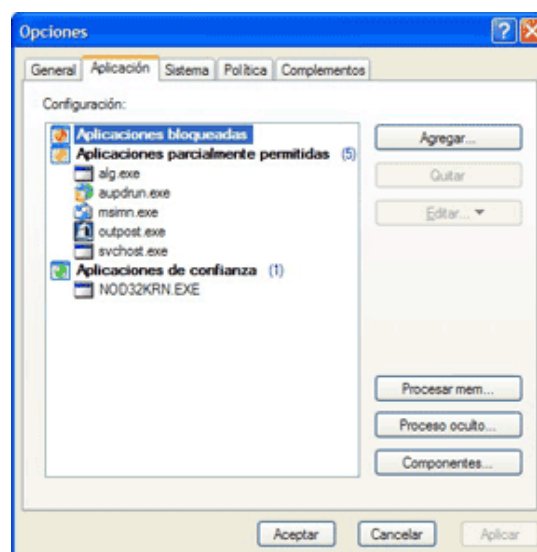
✍ Se aconseja mantener las configuraciones sugeridas para Outpost Network Security Client, si no existe una razón en especial o no se tiene el conocimiento necesario para modificarlas con seguridad.

#### Creación de reglas para aplicaciones

Esta sección es una extensión de lo que anteriormente fue tratado en la sección [Filtro del nivel aplicación](#).

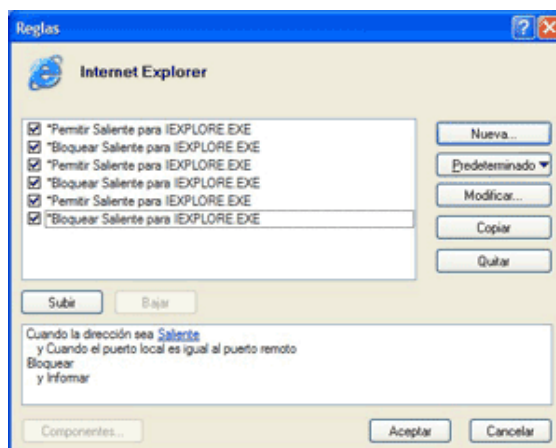
Las reglas para las aplicaciones pueden establecerse utilizando el cuadro de diálogo Reglas.

1. Pulse con el botón secundario del ratón sobre el icono de Outpost en la barra de sistema.
2. Seleccione **Opciones**.
3. Presione la pestaña **Aplicación**.

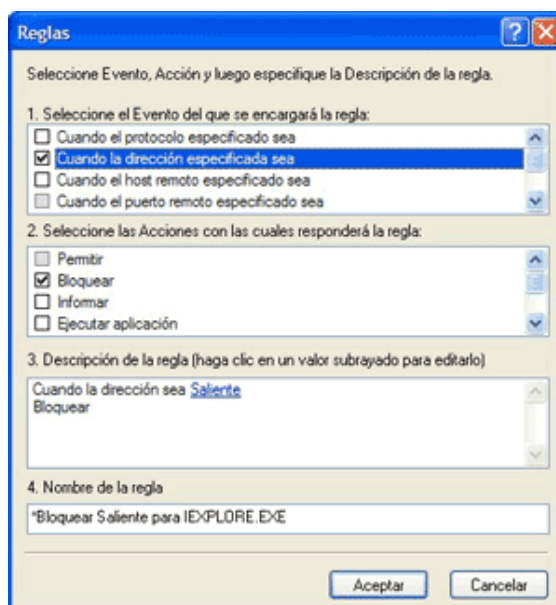


4. Pulse con el botón secundario del ratón sobre una aplicación y posteriormente en Crear reglas...

✎ Según el grupo al que pertenezca la aplicación seleccionada, pudiera ser necesario modificar ligeramente este procedimiento, pero en todos los casos será necesario Crear o modificar una regla para acceder al siguiente cuadro de diálogo.



5. Presione el botón **Nueva** para establecer parámetros ajustados para el control de la actividad de una aplicación.



⚠ **Advertencia:** Este cuadro de diálogo sólo debería ser usado por usuarios avanzados con conocimiento sobre protocolos de red.

En primer cuadro, denominado **Evento**, se definen las condiciones que deberán cumplirse para que la regla sea ejecutada.

- Cuando el protocolo especificado sea
- Cuando la dirección especificada sea
- Cuando el servidor remoto especificado sea
- Cuando el puerto remoto especificado sea
- Cuando el puerto local especificado sea
- Cuando el intervalo de tiempo especificado sea
- Cuando el puerto local sea el mismo que el puerto remoto.

Al seleccionar una condición, se visualiza la descripción de la misma, en el tercer cuadro de esta ventana.

Pulse en el valor subrayado para modificarlo.

Antes de finalizar, deberá definir las acciones que ejecutará Outpost cuando se cumple la condición especificada.

Las siguientes acciones son admitidas:

- **Permitir**  
Permite la comunicación especificada.
- **Bloquear**  
Bloquea la comunicación. Dado que no se notifica al remitente, el resultado es como si el bloque enviado no hubiese llegado nunca a destino.
- **Informar**  
Muestra un cuadro de mensaje cuando la regla sea implementada.
- **Ejecutar aplicación**  
Al cumplirse la condición que lanza la activación de la regla, se ejecutará la aplicación especificada según los parámetros establecidos.
- **Inspección dinámica**  
Habilita la **Inspección dinámica de paquetes en tránsito** para la aplicación correspondiente. Si se activa después de conectarse una aplicación a un servidor remoto, serán permitidas todas las comunicaciones entrantes desde este servidor, al puerto abierto por esta aplicación.
- **Omitir control de componentes**  
Si se satisfacen todas las condiciones especificadas, Outpost ignorará el **Control de componentes** durante esta comunicación.

El paso final es asignarle un nombre a la regla.

Se recomienda que este sea sencillo de reconocer, para que el usuario que la estableció u otros, puedan recordarlo o entenderlo fácilmente en el futuro.

La regla creada se visualizará en el Visor de registros, en la sección **Permitidos** o **Bloqueados**, y se mostrará también los motivos para esto.

☑ Cuando una aplicación intenta conectarse, Outpost Network Security Client verifica si existe alguna regla que cumpla las condiciones establecidas, en la lista de las llamadas **Reglas de aplicación**.

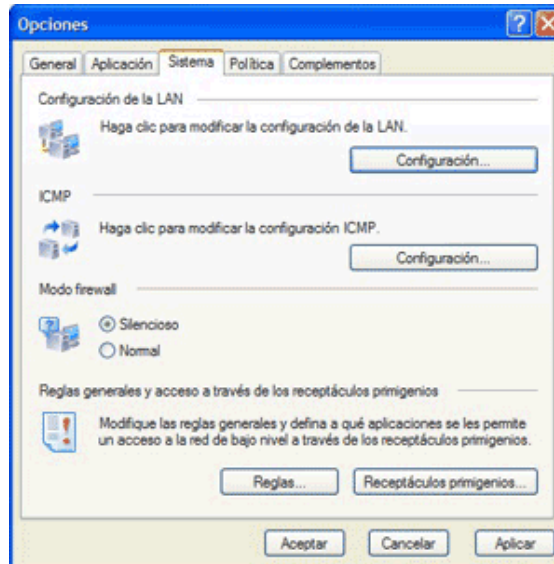
De ser así, Outpost utiliza esas reglas e ignora las **Reglas generales del sistema**.

De lo contrario, Outpost Network Security Client verifica las reglas que coinciden con la actividad del programa en la lista **Reglas generales del sistema**, y utiliza cualquiera que pueda aplicarse, siguiendo el orden de presentación de las mismas.

## Filtro del nivel sistema

Para acceder a la configuración de este filtro:

1. Pulse con el botón secundario del ratón sobre el icono de Outpost en la barra de sistema.
2. Seleccione **Opciones**.
3. Presione la pestaña **Sistema**.



**⚠ Advertencia:** la modificación inadecuada de estos parámetros puede producir serios inconvenientes en el funcionamiento del cortafuegos y disminuir drásticamente el nivel de seguridad del ordenador.

En esta pestaña es posible establecer los parámetros de funcionamiento para:

- **Configuración de la red de área local (LAN)**

Permite cambiar las configuraciones para la red local (*Local Area Network; LAN*) y las opciones de NetBIOS, como también agregar o quitar rangos IP que resulten confiables.

NetBIOS es un protocolo utilizado por Windows para la transferencia de archivos compartidos entre ordenadores y/o impresoras en una red. NetBIOS también es útil en una red local cuyos ordenadores sean confiables, pero puede dejar al ordenador abierto para un ataque, si se lo habilita para las conexiones de Internet en general.

Para aprender más sobre la configuración de los parámetros de la red local, consulte la sección [Configuración de redes domésticas o de oficina](#).

- **ICMP**

Permite especificar los tipos y las direcciones de los mensajes ICMP permitidos.

📖 Amplíe la información sobre los diferentes tipos de mensajes ICMP consultando el apéndice B: [Tipos de mensajes ICMP](#).

**⚠ Advertencia:** Se recomienda no cambiar las configuraciones ICMP a menos que esté totalmente seguro los cambios a ejecutar. El botón **Predeterminado** reinicia todos los parámetros ICMP al estado en que se encontraban cuando Outpost Network Security Client fue instalado por primera vez.

- **Modo del cortafuegos**

Normalmente, cuando el ordenador recibe un pedido de conexión de otro ordenador, le hace saber a este último que determinado puerto está cerrado. En **Modo silencioso**, el ordenador no responderá, simulando estar apagado o desconectado de Internet. Se recomienda mantener Outpost Network Security Client en **Modo silencioso**, como forma de incrementar la seguridad de su ordenador.

- **Reglas generales del sistema acceso a través de RAW-Sockets**

Permite especificar las reglas generales para todas las aplicaciones.

- Permitir resolución DNS (TCP y UDP)
- Permitir DHCP saliente
- Permitir identificación entrante (Desactivada por defecto)
- Permitir bucle local (Entrante)
- Permitir protocolo GRE
- Permitir conexión de control PPTP
- Bloquear llamada a procedimiento remoto (TCP y UDP)
- Bloquear protocolo SMB  
Bloquear Mensaje del servidor (TCP y UDP)
- Permitir conexión UDP servidor local

Pulse en el botón **Reglas** para editar las existentes o para crear otras nuevas. La forma en que se crean las reglas es muy similar a cómo se crean las basadas en aplicaciones. Por más detalles, consulte [Creación de reglas para aplicaciones](#).

Las únicas diferencias son las siguientes:

Se puede especificar el tipo de paquete para las conexiones entrantes. Por ejemplo, en caso que la condición **Cuando la dirección especificada sea**, tenga el atributo **Saliente**:

- Paquetes de datos locales desde o hacia la interfaz de la red local.
- Paquetes de tránsito que atraviesan la interfaz del sistema de red o que son reenviados a otras interfaces. Por ejemplo, los paquetes de información que se reciben y que después se reenvían.
- Paquetes NAT, con direcciones IP trasladadas. Aquellos que son enviados o recibidos por un proxy NAT.

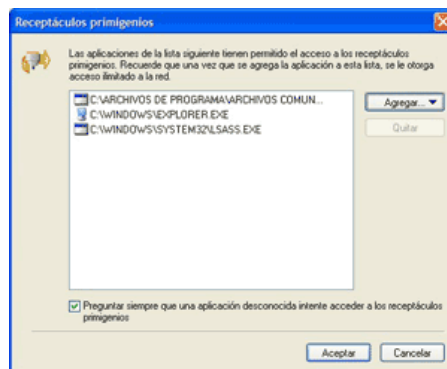
Además, se puede marcar la regla como de **Prioridad alta** si se desea que prevalezca sobre otras reglas de aplicación que, a falta de especificación, tienen precedencia.

Algunas aplicaciones pueden también acceder a la red por medio de los **Receptáculos primigenios** (RAW-Sockets).

Estas llamadas no pueden ser gobernadas por protocolos comunes o reglas de aplicación, y por lo tanto pueden servir como puertas traseras para aplicaciones o procesos corruptos que pretendan acceder a la red sin ningún límite o regulación.

Para mejorar la protección del sistema, Outpost Network Security Client le permite al usuario controlar el acceso a los receptáculos primigenios. Se puede definir a qué aplicaciones se permitirá realizar llamadas a nivel de RAW-Sockets y a cuáles no.

Pulse en el botón **Receptáculos primigenios** para acceder a la configuración.



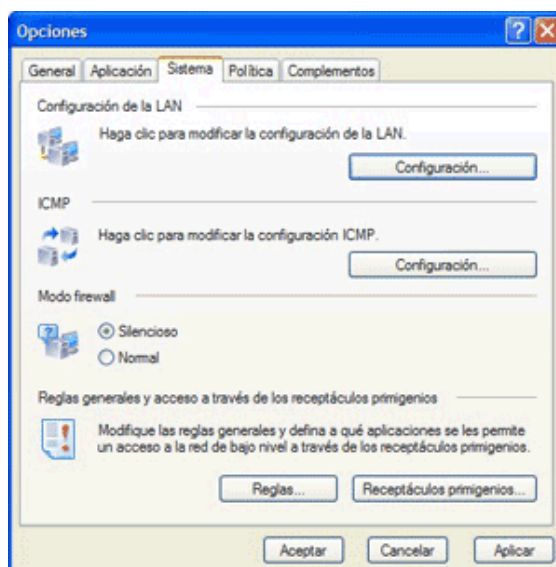
Pulse en el botón **Agregar** y seleccione la aplicación a la que desee garantizarle el acceso a nivel de RAW-Sockets. Si desea recibir una alerta visual cada vez que una aplicación que no figure en la lista de **permitidas**, intente acceder a los **receptáculos primigenios**, active la opción correspondiente.

### Configuración para redes domésticas y de oficina

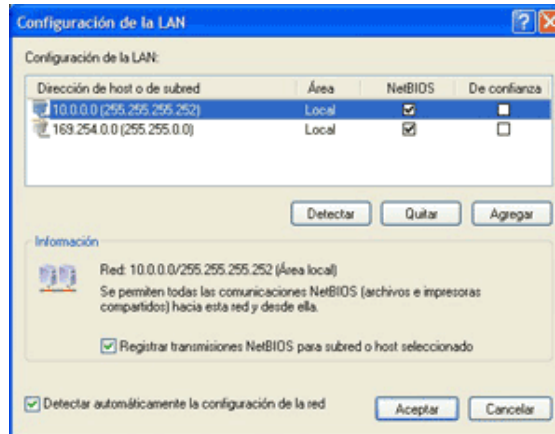
Una diferencia fundamental entre una red de área local (*Local Area Network, LAN*) e Internet, es el nivel de confianza que se les concede. Una red área local, utilizada en el hogar o en la oficina, está generalmente compuesta por ordenadores que son utilizados por otros miembros de la familia o compañeros de trabajo. A los ordenadores de una red de área local, puede incluirse en una **zona de confianza**.

Para verificar o modificar los parámetros de la red:

1. Pulse con el botón secundario del ratón sobre el icono de Outpost en la barra de sistema.
2. Seleccione **Opciones**.
3. Presione la pestaña **Sistema**.



4. En el cuadro **Configuración de la LAN**, pulse en el botón **Configuración** visualizar la ventana **Configuración de la LAN**.



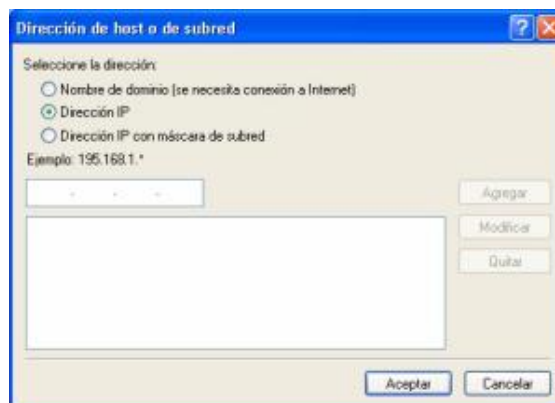
Pulse en el botón **Detectar** para que Outpost descubra automáticamente los componentes de la red.

También es conveniente mantener seleccionada la opción **Detectar automáticamente la configuración de la red** para que Outpost Network Security Client detecte automáticamente cualquier red nueva, de modo que no sea necesario agregarlas manualmente.

Si se desea permitir todas las conexiones para una red en particular, marque el cuadro correspondiente en la columna **De confianza**. En caso contrario, sólo desmarque el casillero.

Si se desean permitir todas las comunicaciones NetBIOS —hacia y desde una dirección de red —habilite el casillero correspondiente. Para desactivar todas las comunicaciones entre su ordenador y la red, desmarque los recuadros **NetBIOS** y **De confianza**.

También se puede agregar una dirección remota específica a la Zona de confianza pulsando en el botón **Agregar** del cuadro anterior.



Especifique el nombre de dominio, la dirección IP, o el rango IP.

✍ Deberá contar con una conexión activa a Internet para introducir un nombre de dominio.

Las entradas en la configuración de la LAN podrán ser modificadas posteriormente por el usuario, tanto en el nivel de confianza como en sus parámetros de localización.

Hay que tener en cuenta que los complementos son independientes de la configuración de la **Zona de confianza**.

Los complementos de Outpost Network Security Client bloquean publicidad, contenido activo y otros elementos, aún de los sitios incluidos en la zona de confianza.

Además, es muy importante recordar que las reglas de la zona de confianza tienen prioridad sobre todas las otras. Aún las aplicaciones restringidas pueden comunicarse con los servidores de la zona de confianza.

En esta zona se recomienda colocar **únicamente** el ordenador que mayor confianza le merezca. Si sólo necesita compartir algunos archivos, o una impresora, será mejor utilizar NetBIOS.

## Sistema de registros de Outpost

### Introducción

Outpost Network Security Client realiza muchas funciones diferentes mientras protege al ordenador contra los ataques. Cada acción que realiza es conocida como suceso, y crea una entrada en la base de datos de registro que Outpost mantiene.

Para hacer más fácil la visualización de estos registros de sucesos, nuestros ingenieros crearon el **Visor de registros de Outpost**. Este muestra el historial de cada operación que realice Outpost Network Security Client incluyendo:

- Cada aplicación y conexión que haya sido permitida o bloqueada por Outpost Network Security Client.
- Las actividades específicas de cada complemento de Outpost Network Security Client.
- El inicio de cada programa y todos los cambios hechos en las políticas, parámetros de configuración y contraseña.

Las características principales del sistema de registros de Outpost son:

- **Acceso con una sola pulsación del ratón**

Con sólo pulsar una vez el botón del ratón se podrá ver el registro entero o la selección de eventos específicos.

 Consulte la sección [Cómo visualizar los registros](#) para obtener más detalles.

- **Visualización personalizada de los registros**

El usuario puede filtrar y visualizar sólo la información que necesite con sólo seleccionar las columnas, limitando sus parámetros y clasificándolos por cualquiera de ellos.

- **Acceso rápido a los distintos grupos de registro**

Se pueden mostrar selecciones de sucesos preestablecidos.

El usuario puede cambiar fácilmente entre las conexiones bloqueadas durante los últimos diez minutos, por ejemplo, o entre todas las conexiones permitidas hoy. También puede crear, editar y quitar selecciones de sucesos.

 Consulte la sección [Cómo trabajar con registros y filtros](#), para obtener más detalles.

- **Filtros de visualización**

Las entradas de sucesos pueden ser clasificadas y mostradas según configuraciones específicas.

- **Análisis estadísticos**

Los registros pueden ser copiados y/o exportados para su posterior tratamiento en planillas de cálculo y procesadores de texto.

- **Mantenimiento de registros**

Los archivos de registro pueden administrarse bajo reglas automáticas de mantenimiento para ahorrar espacio en el disco duro.

- **Tratamiento avanzado de la información**

Se pueden crear consultas SQL personalizadas, para satisfacer propósitos específicos de control.

- **Administración avanzada de registros**

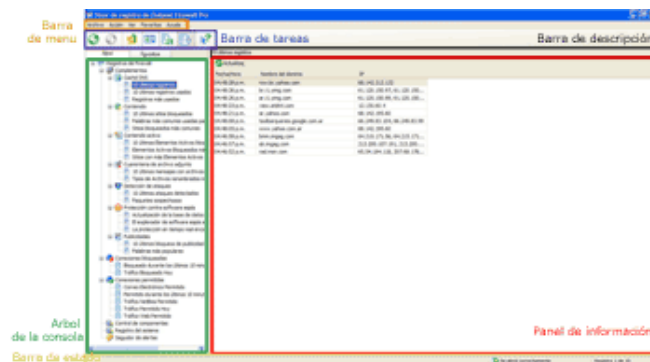
Los registros pueden explorarse a través del complemento de Administración de consola provisto por Microsoft (*Microsoft Console Management, MMC*).

### Ventana principal del Visor de registros de Outpost

La ventana principal del Visor de registros de Outpost permite ver y trabajar con los registros.

1. Pulse con el botón secundario del ratón sobre el icono de Outpost en la barra de sistema.
2. Seleccione **Mostrar Visor de registros**.

✍ También puede acceder desde la ventana principal de Outpost y pulsando en el icono correspondiente de la barra de herramientas.



Los principales elementos del Visor de registros son:

- Barra de menú
- Estructura de carpetas o panel izquierdo
- Panel de información o panel derecho
- Barra de tareas
- Barra de descripción
- Barra de estado.

La estructura de carpetas y el panel de información son similares a los paneles izquierdo y derecho del Explorador de Windows, respectivamente.

La estructura de carpetas contiene una lista de los filtros aplicables.

El panel de información brinda datos detallados al respecto de cualquiera de los filtros seleccionados en el árbol del panel izquierdo.


Como en el Explorador de Windows, cualquier línea precedida por un signo más (+) puede ser expandida para mostrar cada una de las categorías que contiene.

Si al principio de la categoría se ve un signo menos (-), significa que ya ha sido expandida dicha rama. Al pulsar en el signo menos, todos los componentes incluidos quedarán ocultos, para reducir el espacio que el directorio ocupa en la pantalla y sólo se exhibirá el nombre del componente.

Para expandir o plegar todos los objetos de un registro o complemento:

1. En la estructura de carpetas, pulse con el botón secundario del ratón en un registro o complemento.
2. Seleccione **Expandir todo** o **Comprimir todo** en el menú contextual.

El panel izquierdo consta de dos pestañas: **Arbol** y **Favoritos**.

 Para obtener más información sobre Favoritos, consulte la sección [Cómo trabajar con favoritos](#).

En la pestaña **Arbol**, existen los siguientes grupos de registros:

- **Complementos**

Cada complemento tiene su propio registro:

- **Caché DNS**  
Muestra las direcciones de Internet guardadas por Outpost Network Security Client para resolver y acelerar la conexión a esos sitios.
- **Contenido**  
Lista todos los sitios o páginas de Internet que fueron bloqueadas debido a su contenido.
- **Contenido activo**  
Muestra los sitios que hayan tenido alguno de sus contenidos activos bloqueados, basándose en las configuraciones para las aplicaciones Java, JavaScript, VBScript, objetos ActiveX y otros elementos de contenido activo.
- **Cuarentena de archivos adjuntos**  
Muestra todos los archivos adjuntos en mensajes de correo electrónico que fueron analizados y/o neutralizados, poniéndolos en cuarentena, en el ordenador.
- **Detección de ataques**  
Muestra cada uno de los ataques o actividades sospechosas desde Internet que se han detectado, su origen y los puertos del ordenador involucrados.
- **Protección contra software espía**  
Muestra información sobre el estado de la base de firmas de software espía y elementos potencialmente peligrosos encontrados.
- **Publicidad**  
Muestra una lista de todos los anuncios publicitarios que han sido bloqueados.

- **Conexiones bloqueadas**

Una lista de cada aplicación y conexión bloqueadas por Outpost Network Security Client.

- **Conexiones permitidas**

Una lista de cada aplicación y conexión que Outpost Network Security Client ha permitido.

- **Control de componentes**

Muestra todos los sucesos de actividad del Control de componentes.

- **Registro del sistema**

Registra cada uno de los inicios de todos los programas, y cada modificación realizada a la política del cortafuegos, las opciones de programa y los parámetros de configuración.

- **Seguidor de alertas**

Una lista de todas las notificaciones mostradas.

La información correspondiente a cada filtro es mostrada en el panel derecho, agrupándola según distintos parámetros. configurables por el usuario.

Cada filtro tiene su propio grupo de parámetros.

✍ Consulte la sección [Cómo mostrar los Registros](#) para obtener más detalles.

La barra de herramientas del Visor de registros de Outpost está en la ventana principal, cerca de su extremo superior.



Cuando trabaje con el Visor de registros de Outpost podrá ver una explicación de la utilidad de cada comando de la barra de herramientas, con sólo mantener el cursor sobre el mismo durante algunos segundos.

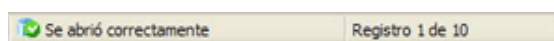
Botón	Función
	Retrocede hacia el objeto anteriormente visto
	Vuelve a adelantarse, después de haber retrocedido
	Sube un nivel
	Muestra u oculta el árbol de la estructura de carpetas
	Exporta el registro seleccionado
	Habilita la actualización automática de los registros
	Muestra la ayuda contextual

La **Barra de descripción** se halla inmediatamente sobre el **Panel de información**, en la ventana del **Visor de registros de Outpost**.



Muestra una descripción del filtro seleccionado en el árbol del panel izquierdo.

La **Barra de estado** se ubica en la parte inferior de la ventana del **Visor de registros de Outpost**.

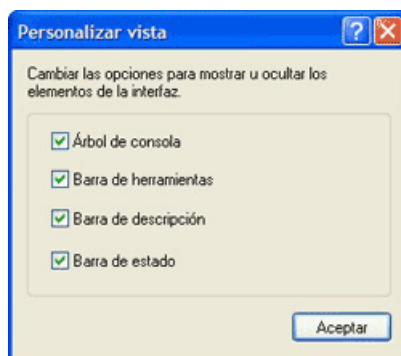


Está dividida en dos secciones que muestran la siguiente información:

- El resultado de los intentos de abrir el registro seleccionado.
- La cantidad de entradas que están siendo vistas y la cantidad total de entradas en ese registro.

La información se puede localizar más cómodamente si se muestran o se ocultan algunas partes específicas de la ventana del Visor de registros de Outpost.

Para personalizar la disposición del Visor de registro, pulse en el menú **Ver, Diseño**.



Seleccione los elementos que quiera mostrar y desmarque los casilleros de aquellos que desee ocultar.

Para mostrar u ocultar la estructura de carpetas, también se puede utilizar el botón **Mostrar/ocultar** en la barra de herramientas del Visor de registros de Outpost.

### Cómo mostrar los registros

Para poder ver los registros de Outpost Network Security Client:

1. Pulse en el menú **Herramientas** de la ventana principal de Outpost Network Security Client.
2. Seleccione **Visor de registros de Outpost**.
3. Seleccione los objetos de interés en árbol del panel izquierdo o cambie a la pestaña **Favoritos**.

📖 Consulte [Cómo trabajar con Favoritos](#) para obtener más detalles.

También puede abrir la entrada específica del Visor de registros que le interesa visualizar directamente desde la ventana principal de Outpost.

1. En el panel izquierdo de la ventana principal, seleccione el elemento del cual desea ver las estadísticas.
2. Pulse en el botón **Mostrar** registro detallado en el panel de información, si desea ver el registro entero, o seleccione un registro preestablecido o filtro específico, desde el menú desplegable utilizando el botón **Mostrar registro preestablecido**.

El Visor de registros de Outpost se abrirá mostrando los detalles del registro.

El contenido en el Visor de registro de Outpost cambia muy rápidamente.

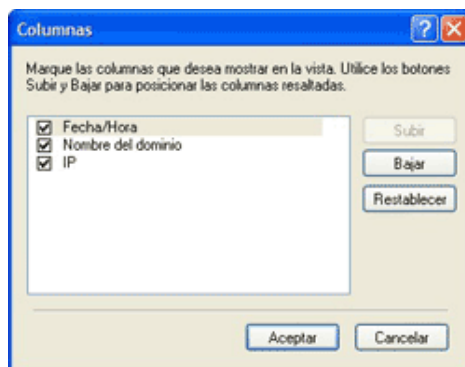
Se puede ver el historial de las actividades de Outpost Network Security Client en el Panel de información del Visor de registros, en forma de cuadro. Cada registro tiene su propio grupo de columnas.

El Visor de registros se puede configurar para que sólo muestre las columnas que interesan al usuario, en cualquier secuencia especificada.

Para seleccionar las columnas que desea visualizar en un registro dado:

1. Pulse con el botón secundario del ratón en cualquier parte del panel de información.
2. Seleccione **Columnas** en el menú contextual y establezca sus preferencias.

O bien, puede seleccionar **Agregar/quitar columnas**, en el menú **Ver**.



Seleccione las columnas que desea que se muestren en el Panel de información.


Para cambiar la secuencia de las columnas en el registro, utilice los botones **Subir** o **Bajar**.

Esto también puede hacerse desde la ventana principal del Visor de registros, seleccionando las columnas que desee mover con el botón principal del ratón y manteniéndolo pulsado mientras las arrastra hacia la ubicación deseada.

Para volver al orden predeterminado, pulse en el botón **Restablecer**.

Para cambiar el tamaño de una columna:

1. Pose el botón principal del ratón sobre uno de los bordes verticales de una columna.
2. El puntero pasa a mostrarse como una flecha doble con sentido a derecha e izquierda.
3. Pulse con el botón principal del ratón y manténgalo presionado mientras mueve el puntero hacia derecha o izquierda..
4. Suelte el botón tan pronto como la columna haya alcanzado el tamaño deseado.

 Puede dimensionar la columna al ancho máximo necesario si pulsa dos veces sobre un borde lateral vertical.

El Visor de Registros de Outpost permite ordenar las entradas de un registro por los valores de cualquier columna, en orden descendente o ascendente.

Pulse en el encabezado de la columna que desea utilizar para organizar las entradas.

Si el encabezado muestra una flecha dirigida hacia arriba, las entradas se organizarán en orden ascendente (1, 2, 3...). Para revertir el orden, sólo tiene que pulsar otra vez en el mismo lugar y el encabezado de la columna mostrará una flecha dirigida hacia abajo, y las entradas estarán dispuestas en orden descendente (3, 2, 1).

## Filtrado selectivo de visualización de determinadas entradas

Para facilitar la ubicación de datos específicos en un registro, se pueden mostrar u ocultar entradas que contengan idéntica información en cualquiera de las columnas que se exhiben:

1. Seleccione la entrada deseada en el Panel de información.
2. Con el botón secundario del ratón, pulse en la celda que contiene la información de interés.
3. Presione **Incluir selección** en el menú contextual, para ver aquellos datos similares, o **Excluir selección** para ocultarlas.

Para poder ver nuevamente todos los registros, seleccione **Mostrar todo**, en el menú contextual.

**Ejemplo:** Para visualizar datos sobre la conexión establecida por una cierta aplicación en un momento particular:

1. Seleccione **Conexiones permitidas** en el panel izquierdo.
2. En la columna **Aplicación**, pulse con el botón secundario del ratón en la celda que contenga la información pertinente.
3. Pulse en **Incluir selección**.
4. En la columna **Hora de inicio**, seleccione, con el botón secundario del ratón, la fecha y hora requerida.
5. Pulse nuevamente en **Incluir selección**.

El panel de información ahora mostrará todos los registros de la aplicación elegida, en la fecha y la hora especificadas. Esta operación puede hacerse tan rápidamente que no hay razón para guardar la configuración. Para crear una selección permanente de registros en condiciones más complejas, conviene crear un filtro.

🚩 Los comandos **Incluir selección** y **Excluir selección** no están disponibles para algunos registros.

## Cómo trabajar con registros y filtros

Existen varias operaciones útiles que se pueden realizar con los registros:

- Crear filtros.
- Agregar a **Favoritos** algunos registros, filtros o configuraciones.
- Copiar registros, filtros, configuraciones o datos particulares al portapapeles de Windows.
- Convertir registros, filtros, configuraciones o apuntes en archivos de texto.
- Limpiar registros.

Una prestación importante y flexible de Outpost consiste en que permite que el usuario decida cuáles datos del registro necesita conocer en cada circunstancia, excluyendo automáticamente la presentación de los demás.

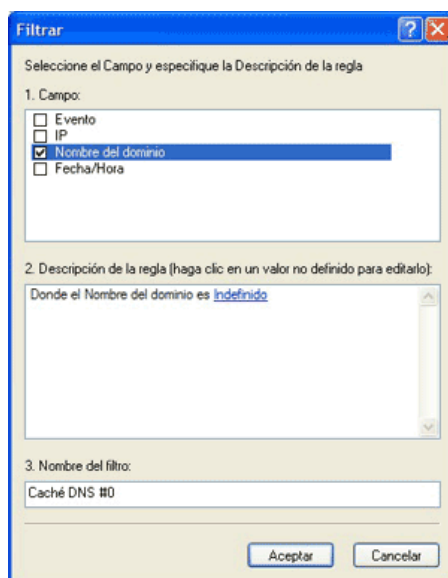
Un **Filtro** es una manera de seleccionar algunos sucesos específicos, según ciertas **Reglas** establecidas por el usuario.

Cada tipo de filtro aparece como un objeto separado en el árbol del panel izquierdo, y su nombre se utiliza para identificar fácilmente los datos que debe presentar o excluir.

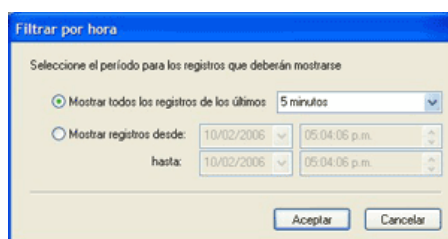
Las Reglas se basan en los distintos tipos de información registrada y ordenada en **Columnas**. Dichas reglas sirven para orientar una búsqueda únicamente hacia los sucesos ocurridos, por ejemplo, en un intervalo de tiempo dado, o sólo a los datos sobre una aplicación en particular, o sobre un puerto determinado, o una combinación de estas u otras opciones.

#### Para crear un nuevo filtro:

1. Seleccione un categoría del panel izquierdo (Caché DNS, Conexiones bloqueadas, u otra).
  - ✍ Deben existir registros en esa categoría para poder continuar.
2. Pulse en el menú Acción, **Agregar filtro** o con el botón secundario del ratón.
3. Seleccione las condiciones que deberá cumplir el filtro y las columnas a visualizar.



4. Al marcar un casillero, se visualiza en el cuadro descripción las posibilidades de configuración. Pulse sobre la palabra subrayada para modificar los parámetros.
5. Un cuadro de diálogo le permitirá definir los valores a utilizar para el nuevo filtro.



6. Modifique esta ventana según sus necesidades y pulse en **Aceptar**.
7. Una vez determinadas las reglas necesarias, escriba un nombre para el filtro y pulse en **Aceptar**. El mismo se visualizará en el árbol del panel izquierdo.
  - ✍ Se pueden especificar tantas reglas como se desee.

#### Para modificar las reglas de un filtro ya existente

1. Pulse con el botón secundario del ratón sobre un filtro del panel izquierdo.

2. Presione en **Editar filtro**.
3. Efectúe las modificaciones que considere necesarias.
4. Pulse en el botón **Aceptar**.

#### Para eliminar los filtros innecesarios

1. Pulse con el botón secundario del ratón sobre un filtro del panel izquierdo.
2. Presione en **Quitar filtro**.

Los filtros se pueden ver rápidamente desde la ventana principal de Outpost Network Security Client.

✍ Consulte la sección [Cómo mostrar registros](#) para obtener más detalles.

Otra opción es agregarlos a la lista de **Favoritos**.

✍ Consulte la sección [Cómo trabajar con Favoritos](#) para obtener más información.

Para guardar la información específica registrada, en un texto o en un archivo de valores separados por comas, o copiarla en el portapapeles para pegarla en otras aplicaciones, realice las siguientes acciones:

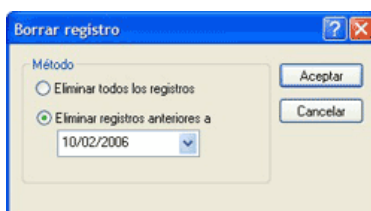
1. En el árbol del panel izquierdo seleccione un filtro.
2. En el panel de información, seleccione una o más entradas de registro.
3. Si lo considera necesario puede limitar la visualización utilizando las opciones de [incluir](#) o [excluir selección](#), explicadas anteriormente.
4. Pulse con el botón secundario del ratón sobre una de las entradas seleccionadas y posteriormente utilice alguna de las opciones disponibles para **copiar** o **exportar**, según sus intereses.

✍ Para completar la operación deberá **pegar** los datos en un documento abierto o **exportar** los mismos a un archivo determinado.

Estos registros se almacenan en una base de datos que se comprime automáticamente para reducir el espacio que ocupan en el disco, y por eso no hay necesidad de un excesivo mantenimiento.

Sin embargo, quizás quiera eliminarlos del disco duro.

1. En el panel izquierdo seleccione el registro que desee eliminar.
2. Pulse con el botón secundario del ratón en el panel de información, para que aparezca el menú contextual.
3. Seleccione **Borrar registro**.
4. Seleccione **Eliminar todas las entradas**, o bien especifique la fecha de la última entrada que desea sea descartada.



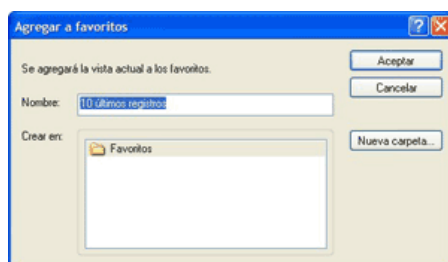
## Cómo trabajar con Favoritos

El panel izquierdo consta de dos pestañas: **Arbol** y **Favoritos**.


La lista de Favoritos sirve para guardar los elementos que se usan a menudo.

A la pestaña **Favoritos** se pueden agregar registros, configuraciones o filtros de uso frecuente, para tener un acceso rápido y conveniente.

1. En el árbol del panel izquierdo pulse con el botón secundario del ratón en el objeto requerido.
2. Seleccione **Agregar a favoritos**.



3. Se puede cambiar el nombre del objeto en el campo de edición **Nombre** y seleccionar una carpeta para almacenarlo.

 Puede crear una carpeta para ayudarlo en la organización de los favoritos.

4. Pulse en el botón **Aceptar** para finalizar.

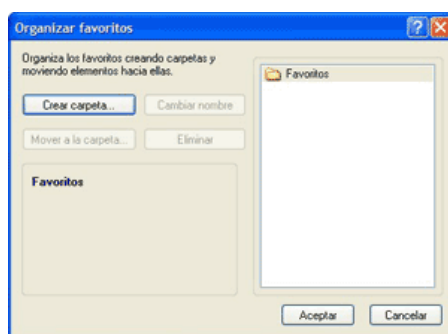
Para visualizar los objetos que guardó en esta estructura, pulse en la pestaña **Favoritos** y seleccione el objeto buscado.

## Para eliminar los objetos de la pestaña Favoritos

1. Pulse en la pestaña **Favoritos**.
2. Pulse con el botón secundario del ratón sobre un objeto.
3. Seleccione **Quitar**.

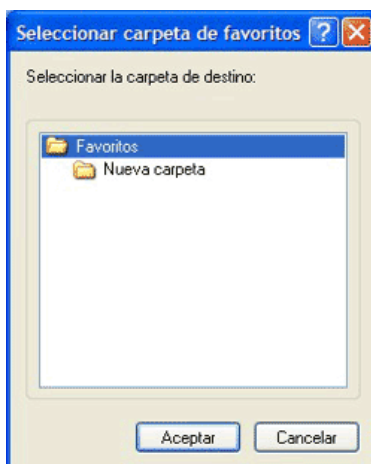
## Para administrar el orden de los objetos clasificados en Favorito

1. Seleccione **Favoritos** en el menú del Visor de registros.
2. Seleccione **Organizar favoritos**.



Desde aquí podrá crear una carpeta, cambiar el nombre, eliminar o mover un favorito a otra ubicación.

Al pulsar en **Mover a la carpeta** un cuadro de diálogo le permitirá seleccionar la nueva ubicación.

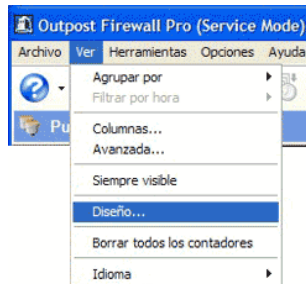


Marque la carpeta adonde desee mover el objeto y pulse en el botón **Aceptar**.

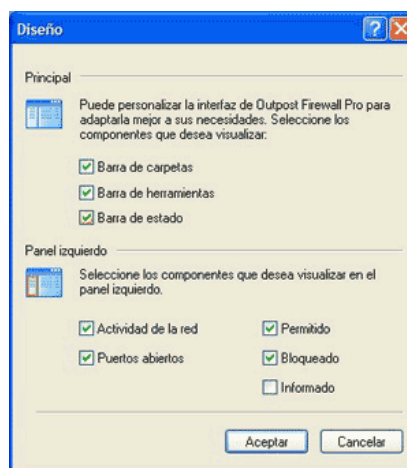
## Diseño

Para aumentar el espacio de visualización del Panel de información, el usuario pudiera preferir ocultar ciertos elementos, como el árbol de la estructura, la barra de herramientas o la barra de estado:

1. Pulse en el menú **Ver**
2. Seleccione **Diseño**.



3. Active o desactive los elementos a mostrar u ocultar.



En la sección Panel izquierdo se encuentran las categorías que pueden mostrarse u ocultarse en la vista del panel izquierdo. Marque o vacíe los recuadros correspondientes en este cuadro de diálogo según sus preferencias.

- **Actividad de la red**  
Son mostradas todas las conexiones de red.
- **Puertos abiertos**  
Se muestran todas las conexiones de red que tengan algún puerto abierto.
- **Permitido**  
Se visualiza un resumen de todas las conexiones de red permitidas.
- **Bloqueado**  
Se visualiza un resumen de todas las conexiones de red que han sido bloqueadas.
- **Informado**  
Se visualiza un resumen de todas las conexiones de red cuya configuración emite algún tipo de informe de actividad.

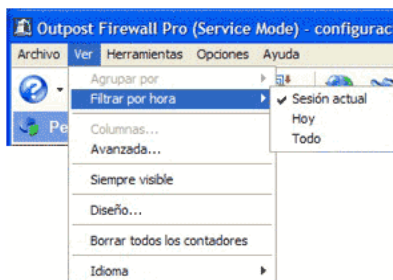
 El mismo objeto puede estar seleccionado en varias listas.

## Filtrar por hora

Este comando permite establecer limitaciones a la información visualizada, operando sobre las secciones:

- Informado
- Permitido
- Bloqueado

**⚠ Importante:** El **Filtro por hora** sólo estará disponible en el menú **Ver** cuando uno de los objetos permitidos, bloqueados o informados del panel izquierdo esté seleccionado.



También se puede acceder a esta herramienta a través de la barra de herramientas de Outpost Network Security Client.



Al pulsarlo, podrá limitar la visualización:

- **Sesión actual**  
Muestra el registro de sucesos de la sesión actual de Outpost Network Security Client, desde el momento en que se inició la actividad por primera vez al iniciar el ordenador.
- **Hoy**  
Muestra el registro de sucesos de la fecha actual.
- **Todos**  
Muestra el registro de sucesos entero, desde el momento en que se empezó a utilizar Outpost Network Security Client por primera vez.

📖 Consulte la sección [Sistema de registros](#) para mayor información.

## Columnas

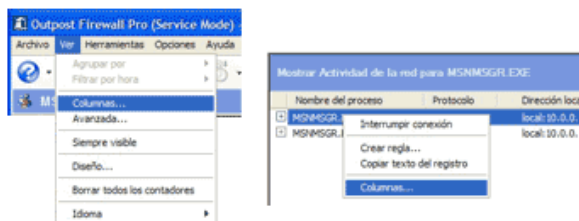
También se puede configurar Outpost Network Security Client para limitar la visualización de las columnas en el panel derecho.

1. Pulse en el menú **Ver**.
2. Seleccione **Columnas**.

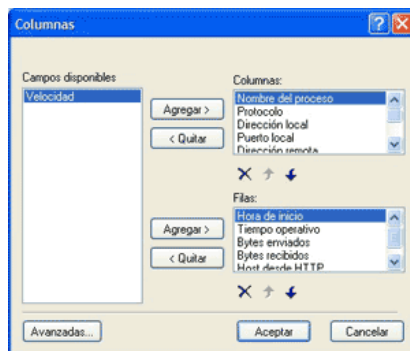
Esta configuración sólo está disponible para las secciones:

- Actividad de la red
- Puertos abiertos

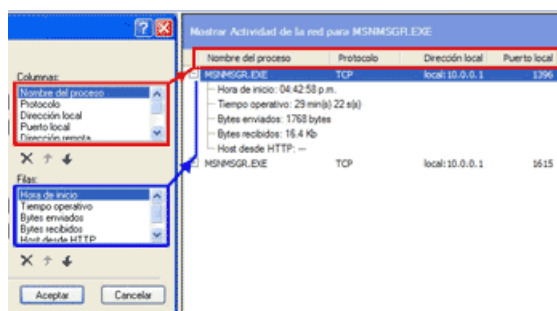
Asimismo, puede acceder pulsando con el botón secundario del ratón sobre cualquier elemento de las secciones habilitadas.




Defina sus preferencias de visualización:



Los encabezados de columna y lista de campos, en el cuadro de diálogo, corresponden a aquellos visualizados en el panel de información.



Se puede personalizar la lista con sólo quitar un objeto de la lista utilizando el botón **Quitar** o  o agregando un objeto previamente eliminado, utilizando el botón **Agregar**. También se puede reorganizar la secuencia de los objetos para cada lista.

Para mover un objeto, utilice el botón que muestra una flecha apuntando hacia arriba para mover un objeto una posición hacia arriba, o el botón flecha hacia abajo para descender el objeto. Estos botones se encuentran ubicados debajo de la lista que afectan.

El comando **Avanzadas**, también en el menú **Ver**, permite personalizar la visualización de la información que será mostrada en las columnas:



## Resolver

La sección **Resolver** le brinda al usuario la posibilidad de elegir la forma de visualización de las direcciones de Internet o de red local, ya sea, mostrándolas como dirección IP o como nombre de dominio.

- **Nunca**  
Siempre muestra estas direcciones por su numeración IP.  
Ejemplo: 64.176.127.178
- **Si se almacenó en caché**  
Si la dirección IP ya fue resuelta (interpretada) como nombre de dominio, y la misma se encuentra almacenada en el caché DNS, entonces se mostrará la misma por su nombre DNS.

🔗 Consulte el [Glosario](#) para ampliar la información sobre este tema.

- **Siempre**  
Siempre convierte y muestra las direcciones IP como nombres DNS. Sin embargo, esto no se recomienda ya que puede derivar en una gran cantidad de solicitudes DNS.

## Mostrar puerto como

La sección **Mostrar puerto** permite visualizar el puerto local (en el ordenador del usuario) y los valores del puerto remoto, como:

- **Número**  
Los puertos se identifican por su número.  
Ejemplo: 21
- **Nombre**  
Los puertos se identifican como nombres descriptivos de las tareas, si la información está disponible en el sistema.  
Ejemplo: FTP

## Mostrar tráfico como

La sección **Mostrar tráfico** permite especificar la medida base de la cantidad de información transferida:

- **Auto**  
Outpost decide la forma de visualización.
- **Bytes**  
El tráfico de red es mostrado en Bytes.
- **KB**  
El tráfico de red es mostrado en kilobytes.  
🔗 Un KB es igual a 1024 Bytes.
- **MB**  
El tráfico de red es mostrado en megabytes.  
🔗 Un MB es igual a 1024 KB y también a 1.048.576 Bytes.

## Agrupar por...

Este comando permite establecer limitaciones a la información visualizada, mostrando elementos por su similitud en su ejecución o estructura.

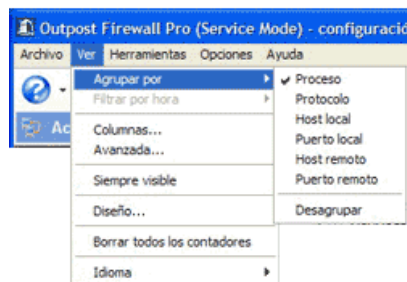
1. Seleccione una de las secciones principales del panel izquierdo:

- Actividad de la red
- Puertos abiertos

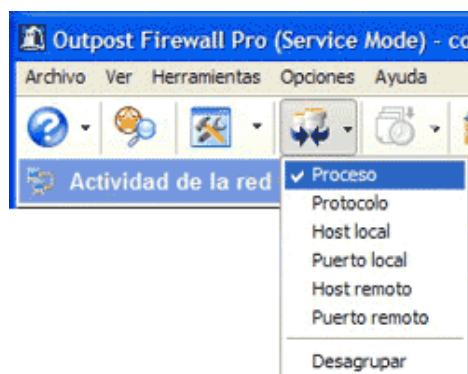
2. Pulse en el menú Ver.

3. Establezca el criterio de visualización y clasificación:

- Proceso
- Protocolo
- Dirección local
- Puerto local
- Dirección remota
- Puerto remoto
- Desagrupar



También puede lograr el mismo efecto utilizando el botón correspondiente de la barra de herramientas.



## Apéndice B

### Tipos de mensajes ICMP

Se sugiere la consulta al [glosario](#) de Outpost para mayor información.

0	Respuesta del eco
3	Destino inaccesible
4	Disminución del tráfico desde el origen
5	Redireccionar (cambio de ruta)
8	Solicitud de eco
10	Solicitud de enrutador
11	Tiempo excedido para un datagrama
12	Problema de parámetros en datagrama
13	Solicitud de marca de tiempo
14	Respuesta de marca de tiempo
16	Respuesta de información
17	Solicitud de máscara de dirección
18	Respuesta de máscara de dirección

Un mensaje ICMP **Solicitud de eco** es uno de los métodos más simples para verificar las condiciones operativas de un código de red.

Una vez que se recibe una señal de eco, cualquier nodo de la red genera una **Respuesta de eco** y la devuelve a la fuente.

Si la fuente recibe una respuesta a dicha solicitud, esto indica que los componentes más importantes del sistema de tráfico están en buenas condiciones.

Un mensaje ICMP **Destino inaccesible** es generado por una puerta de enlace, cuando no puede entregar un datagrama IP.

El datagrama, es la unidad de datos, o paquete, transmitida en una red TCP/IP. Cada datagrama contiene direcciones de fuente y de destino y datos.

Un mensaje ICMP **Disminución del tráfico desde el origen** se transmite desde el nodo a la fuente de datagrama en el suceso en que la cola entrante está superpoblada. En este caso, se quita el datagrama de la cola.

Un mensaje ICMP **Redireccionar** es un mensaje que se transmite cuando una puerta de enlace detecta que una ruta no satisfactoria es utilizada, entonces la puerta de enlace envía un pedido de cambio de ruta en la tabla de enrutamiento.

Un mensaje ICMP **Anuncio de IP** transmite un aviso de su dirección IP.

El mensaje ICMP **Tiempo excedido para datagrama** es enviado cuando un datagrama es transferido de una puerta de enlace a otra más veces de lo que se le está permitido (normalmente esto indica una ruta cíclica).

Un mensaje ICMP **Problema de parámetro en datagrama** es enviado por una puerta de enlace si ocurre un problema durante la transmisión de un datagrama específico que no está dentro de la diversidad de los mensajes antes mencionados. El datagrama debe abandonarse debido a este error.

Los mensajes ICMP **Solicitud de marca de tiempo** y **Respuesta de marca de tiempo** son utilizados para sincronizar los relojes en un nodo de la red.

Los mensajes ICMP **Solicitud de información** y **Respuesta de información** han quedado obsoletos.

Se utilizaban antes por los nodos de la red para determinar las direcciones internas en la red, pero hoy se consideran antiguas y no deberían usarse.

Los mensajes ICMP **Solicitud de máscara de dirección** y **Respuesta de máscara de dirección** son utilizados para encontrar la máscara de una red secundaria.

Por ejemplo, cuáles bits definen la dirección en la red.

Un nodo local envía una solicitud de máscara de dirección a una puerta de enlace, y recibe una respuesta de máscara de dirección como réplica.

## Apéndice C

### Soporte técnico

Para cualquier consulta adicional sobre Outpost Network Security visite la [página principal de soporte](#), donde encontrará una variedad de recursos y formas de contacto, a su disposición.