

Sophos Endpoint Security and Control Ayuda

Versión: 10.0

Edición: diciembre de 2011



Contenido

- 1 Acerca de Sophos Endpoint Security and Control3
- 2 Acerca de la página de inicio.....4
- 3 Grupos de Sophos.....5
- 4 Sophos Anti-Virus.....8
- 5 Control de dispositivos de Sophos.....48
- 6 Control de datos de Sophos.....50
- 7 Sophos Client Firewall.....52
- 8 Sophos AutoUpdate.....82
- 9 Protección contra manipulaciones de Sophos.....85
- 10 Solución de problemas.....90
- 11 Glosario.....98
- 12 Soporte técnico.....104
- 13 Aviso legal.....105

1 Acerca de Sophos Endpoint Security and Control

Sophos Endpoint Security and Control versión 10.0 es una suite integrada de productos de seguridad.

Sophos Anti-Virus detecta y limpia virus, troyanos, gusanos y programas espía, además de otros programas publicitarios y aplicaciones no deseadas. El sistema de prevención contra intrusiones (HIPS) protege los equipos contra archivos sospechosos y rootkits, virus no identificados y comportamientos sospechosos.

El sistema de **control de comportamiento de Sophos** utiliza la tecnología HIPS para proteger equipos con Windows 2000 y posterior contra amenazas desconocidas y comportamiento sospechoso.

La **protección activa de Sophos** mejora de forma significativa la detección de nuevas amenazas sin el riesgo de falsos positivos. La comprobación se realiza con los datos de los programas maliciosos más recientes. Cuando se detecte una nueva amenaza, Sophos enviará la actualización de forma inmediata.

La **protección web de Sophos** ofrece una seguridad mejorada contra las amenazas de Internet, impidiendo el acceso a sitios que albergan programas maliciosos. Para ello, la protección web realiza una búsqueda en tiempo real basada en la base de datos online de Sophos de sitios web maliciosos.

La **restricción de aplicaciones de Sophos** bloquea aplicaciones no autorizadas de voz sobre IP, mensajería instantánea, intercambio de archivos y juegos.

El **control de dispositivos de Sophos** bloquea dispositivos de almacenamiento externo no autorizados y tecnologías de conexión inalámbrica.

El **control de datos de Sophos** impide la fuga accidental de información personal de equipos afectados.

Sophos Client Firewall impide que los gusanos, troyanos y programas espía roben y distribuyan información delicada, además de frenar las intrusiones de hackers.

Sophos AutoUpdate ofrece actualizaciones sin errores y regula el ancho de banda durante actualizaciones con conexiones de red lentas.

La **protección contra manipulaciones de Sophos** permite evitar que programas maliciosos o usuarios no autorizados puedan desinstalar el software de seguridad de Sophos o desactivarlo desde Sophos Endpoint Security and Control.

2 Acerca de la página de inicio

La página de **Inicio** aparece en el panel derecho al abrir la ventana de **Sophos Endpoint Security and Control**. Permite configurar y utilizar el software.

A medida que utilice Sophos Endpoint Security and Control, el contenido del panel derecho será diferente. Para volver a la página de **Inicio**, haga clic en el botón **Inicio** de la barra de herramientas.

3 Grupos de Sophos

3.1 Acerca de los grupos de Sophos

Sophos Endpoint Security and Control restringe el acceso a determinadas partes del software a los miembros de determinados grupos de Sophos.

Al instalar Sophos Endpoint Security and Control, todos los usuarios del equipo se asignan de forma inicial a un grupo de Sophos, según el grupo de Windows al que pertenecen.

Grupo de Windows	Grupo de Sophos
Administradores	SophosAdministrator
Usuarios avanzados	SophosPowerUser
Usuarios	SophosUser

Los usuarios que no están asignados a un grupo de Sophos, incluidos los usuarios invitados, sólo pueden realizar las tareas siguientes:

- Escaneado en acceso
- Escaneado de botón derecho

SophosUsers

Los SophosUsers pueden realizar las tareas anteriores, además de las siguientes:

- Abrir la ventana de Sophos Endpoint Security and Control
- Configurar y ejecutar escaneados en demanda
- Configurar escaneados de botón derecho
- Gestionar (con privilegios limitados) los elementos en cuarentena
- Crear y configurar reglas del cortafuegos

SophosPowerUsers

Los SophosPowerUsers tienen los mismos derechos que los SophosUsers, además de los siguientes:

- Mayores privilegios en el área de cuarentena
- Acceso al Gestor de autorización

SophosAdministrators

SophosAdministrators pueden utilizar y configurar cualquier parte de Sophos Endpoint Security and Control.

Nota: los usuarios del grupo SophosAdministrator deben conocer la contraseña de la protección contra manipulaciones, si está activada, para realizar las siguientes tareas:

- Configurar el escaneado en acceso.

- Configurar la detección de comportamiento sospechoso.
- Desactivar la protección contra manipulaciones.

Para más información, consulte [Protección contra manipulaciones](#) en la página 85.

3.2 Añadir usuarios a grupos de Sophos

Los administradores del dominio y los usuarios del grupo de administradores de Windows en el ordenador pueden cambiar el grupo de Sophos al que pertenecen los usuarios. De esta forma, se modifican los permisos de acceso que tienen a Sophos Endpoint Security and Control.

Para añadir usuarios a grupos de Sophos:

1. En Windows, abra Administración de equipos.
2. En el árbol de la consola, haga clic en **Usuarios**.
3. Haga clic con el botón derecho en la cuenta del usuario y seleccione **Propiedades**.
4. En la ficha **Miembro de**, haga clic en **Agregar**.
5. En **Escriba los nombres de objeto que desea seleccionar**, escriba el nombre de uno de los grupos de Sophos:
 - **SophosAdministrator**
 - **SophosPowerUser**
 - **SophosUser**
6. Si desea validar el nombre del grupo de Sophos, haga clic en **Comprobar nombres**.

La próxima vez que el usuario inicie sesión en el equipo, verá que los permisos de acceso a Sophos Endpoint Security and Control han cambiado.

Notas

- Para abrir la Administración de equipos, haga clic en **Inicio** y en **Panel de control**. Haga doble clic en **Herramientas administrativas** y doble clic en **Administración de equipos**.
- Para eliminar el usuario de un grupo de usuarios de Sophos, en la ficha **Miembro de**, seleccione el grupo en **Miembro de** y haga clic en **Quitar**.

3.3 Configurar los derechos sobre el área de cuarentena

Si pertenece al grupo SophosAdministrator, puede configurar los derechos del usuario en el área de cuarentena.

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Derechos sobre el área de cuarentena**.

2. Seleccione el tipo de usuario que puede realizar cada tipo de acción.

Nota: a excepción de la opción **Autorizar**, los derechos configurados aquí sólo afectan al **Área de cuarentena**.

Opción	Descripción
Limpiar sectores	Los usuarios pueden limpiar sectores de arranque de disquetes.
Limpiar archivos	Los usuarios pueden limpiar documentos y programas.
Borrar archivos	Los usuarios pueden eliminar archivos infectados.
Mover archivos	Los usuarios pueden mover archivos infectados a otra carpeta.
Autorizar	Los usuarios pueden autorizar elementos sospechosos y programas publicitarios o aplicaciones no deseadas, para permitir su ejecución en el equipo. Esta opción afecta tanto al Gestor de autorización como al Área de cuarentena .

4 Sophos Anti-Virus

4.1 Acerca del escaneado en acceso y en demanda

Escaneado en acceso

El escaneado en acceso es el principal método de protección contra virus y demás amenazas.

Al copiar, guardar, mover o abrir un archivo, Sophos Anti-Virus lo escanea y permite el acceso sólo si no supone una amenaza para el equipo o si su uso está autorizado.

Los administradores de Sophos pueden especificar el escaneado de archivos al guardarlos, crearlos o cambiarlos de nombre.

Para más información, consulte [Configurar el escaneado en acceso](#) en la página 8 .

Escaneado en demanda

Los escaneados en demanda ofrecen protección adicional. Estos escaneados se pueden utilizar cuando sea necesario. Es posible escanear desde un solo archivo hasta el equipo completo.

Para más información, consulte [Tipos de escaneado en demanda](#) en la página 15.

4.2 Escaneado en acceso

4.2.1 Acerca del escaneado en acceso

Se recomienda usar la configuración predeterminada del escaneado en acceso, ya que ofrece el mejor equilibrio entre protección y consumo de recursos.

Nota: el escaneado en acceso no puede escanear elementos cifrados. Modifique el proceso de inicio del sistema para que los archivos se puedan escanear cuando se active el escaneado en acceso. Para más información sobre cómo utilizar la política Antivirus y HIPS en sistemas con cifrado, consulte el artículo 12790 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/12790.html>).

4.2.2 Configurar el escaneado en acceso

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Por defecto, Sophos Anti-Virus detecta y limpia las siguientes amenazas durante el escaneado en acceso:

- virus
- troyanos
- gusanos
- programas espía

Para configurar el escaneado en acceso:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado en acceso** .
2. Para cambiar cuándo ocurre el escaneado en acceso, en la sección **Comprobar archivos al**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Leer	Se escanean los archivos que se copian, mueven o abren.
Cambiar nombre	Se escanean los archivos que se cambian de nombre.
Escribir	Se escanean los archivos que se crean o guardan.

3. En la sección **Detectar**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Adware y PUA	Los programas publicitarios muestran anuncios, por ejemplo, en ventanas emergentes, que afectan a la productividad del usuario y al rendimiento del sistema. Las aplicaciones no deseadas (PUA, Potentially Unwanted Applications) no son maliciosas, pero se consideran inapropiadas en redes corporativas..
Archivos sospechosos	Archivos con características habituales de virus, aunque no exclusivas.

4. En la sección **Otras opciones de escaneo**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Permitir el acceso a unidades con sectores de arranque infectados	Permite el acceso a unidades externas como CD-ROM, disquetes o unidades USB que tengan el sector de arranque infectado. Sólo debería utilizar esta opción bajo las indicaciones del soporte técnico de Sophos. Consulte la sección Permitir el acceso a unidades con sectores de arranque infectados en la página 94.
Escanear todos los archivos	Sólo se recomienda utilizar esta opción en un escaneo semanal, ya que puede afectar al rendimiento del sistema.
Escanear archivos comprimidos	Active esta opción para escanear el contenido de archivos comprimidos al descargarlos o enviarlos por email. Se recomienda desactivar esta opción ya que puede ralentizar el escaneo. El contenido de los archivos comprimidos se escanea: <ul style="list-style-type: none"> ■ Cuando se realiza la extracción. ■ Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.
Escanear memoria del sistema	Active esta opción para disponer de un escaneo en segundo plano cada hora que detecte amenazas en la memoria del sistema.

4.2.3 Desactivar el escaneo en acceso temporalmente

Si es miembro del grupo SophosAdministrator, podrá activar o desactivar el escaneo en acceso de forma temporal para tareas de mantenimiento o solución de problemas. Aún con el escaneo en acceso desactivado, podrá realizar escaneos en demanda.

Sophos Endpoint Security and Control mantendrá la configuración incluso tras reiniciar el equipo. Si desactiva el escaneo en acceso, su ordenador estará desprotegido.

- Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneo en acceso** .
- Desactive la opción **Activar el escaneo en acceso en este equipo**.

4.2.4 Configurar la limpieza del escaneo en acceso

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para configurar la limpieza del escaneado en acceso:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado en acceso**.
2. Abra la ficha **Limpieza**.
3. En la sección **Viruses/spyware**, active la opción **Limpiar automáticamente elementos con virus/spyware**.

Nota: si activa esta opción, la limpieza de ciertos virus y programa espía puede requerir un escaneado completo del sistema para intentar limpiar *todos* los elementos detectados. Esto puede tardar bastante.

4. En la sección **Virus/spyware**, seleccione la acción que desea llevar a cabo si Sophos Anti-Virus no puede llevar a cabo la limpieza automática:

Opción	Descripción
Sólo denegar acceso	Sophos Anti-Virus pedirá confirmación antes de continuar. Esta es la opción predeterminada.
Borrar Denegar acceso y mover a	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar virus y programas espía que encuentre Sophos Anti-Virus. Consulte Deal with viruses/spyware in quarantine en la página 36.

5. En la sección **Archivos sospechosos**, seleccione la acción que desea llevar a cabo si Sophos Anti-Virus detecta código que puede ser malicioso:

Opción	Descripción
Denegar acceso	Sophos Anti-Virus pedirá confirmación antes de continuar. Esta es la opción predeterminada.
Borrar Denegar acceso y mover a	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar los archivos sospechosos que Sophos Anti-Virus encuentre en el equipo. Consulte Deal with suspicious files in quarantine en la página 38.

4.2.5 Eliminar sumas de verificación de archivos escaneados

La lista de sumas de verificación de archivos escaneados se elimina cada vez que Sophos Anti-Virus se actualiza y cuando se reinicia el sistema. La lista se crea de nuevo con los archivos escaneados por Sophos Anti-Virus.

Si lo desea, puede eliminar la lista existente de sumas de verificación desde Sophos Endpoint Security and Control.

Para eliminar las sumas de verificación de archivos escaneados:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado en acceso** .
2. En la ficha **Escaneado**, haga clic en **Purgar caché**.

4.2.6 Especificar extensiones de archivo del escaneado en acceso

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si lo desea, puede especificar las extensiones de archivo que se escanean durante el escaneado en acceso.

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado en acceso** .
2. Abra la ficha **Extensiones** y configure las opciones según se describe a continuación.

Escanear todos los archivos

Seleccione esta opción para escanear todos los archivos, independientemente de la extensión.

Permitir el control de lo que se escanea

Seleccione esta opción para restringir el escaneado a los archivos con cierta extensión (especificadas en la lista de extensiones).



Advertencia: la lista de extensiones incluye los tipos de archivo que se recomienda escanear. Si va a modificar la lista, hágalo con cautela.

Para agregar extensiones a la lista, haga clic en **Añadir**. Puede utilizar el carácter comodín ? para indicar cualquier carácter posible.

Para borrar una extensión de la lista, selecciónela y haga clic en el botón **Eliminar**.

Para modificar una extensión de la lista, selecciónela y haga clic en el botón **Editar**.

Al seleccionar **Permitir el control de lo que se escanea**, estará activada por defecto la opción **Escanear archivos sin extensión**. Desactive la opción **Escanear archivos sin extensión** para no escanear archivos con la extensión omitida.

4.2.7 Añadir, modificar y borrar exclusiones del escaneado en acceso

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para modificar la lista de archivos, carpetas o unidades excluidas del escaneado en acceso:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado en acceso** .
2. Abra la ficha **Exclusiones** y realice la acción necesaria.
 - Haga clic en **Añadir** para especificar un archivo, carpeta o unidad a excluir del escaneado en acceso.

- Para borrar una exclusión, selecciónela y haga clic en **Eliminar**.
 - Para modificar una exclusión, selecciónela y haga clic en **Editar**.
3. Para añadir o modificar una exclusión, en el cuadro de diálogo **Exclusión de elementos**, seleccione el tipo de **Elemento**.
 4. Indique el **Nombre** mediante el botón **Examinar** o introduciendo el nombre en el cuadro de texto.

Nota: si utiliza un sistema de 64 bits, el botón **Examinar** no estará visible en el cuadro de diálogo **Exclusión de elementos**.

Para más información, consulte [Especificar archivos y rutas para la exclusión de elementos](#) en la página 17.

4.2.8 Especificar archivos y rutas para la exclusión de elementos

Nomenclatura estándar

Sophos Anti-Virus utiliza la nomenclatura estándar de Windows a la hora de establecer las exclusiones de elementos. Por ejemplo, el nombre de una carpeta puede contener espacios pero no **sólo** espacios.

Excluir un archivo

Para excluir un archivo, debe especificar el nombre y la ruta de acceso. La ruta de acceso puede incluir una unidad local o compartida:

C:\Documentos\CV.doc

\\servidor\Usuarios\Documentos\CV.doc

Nota: para asegurar que la exclusión se aplica siempre correctamente, añada tanto el nombre largo como en formato 8.3:

C:\Archivos de programa\Sophos\Sophos Anti-Virus

C:\Archiv~1\Sophos\Sophos~1

Para más información, consulte <http://esp.sophos.com/support/knowledgebase/article/13045.html>.

Excluir todos los archivos con el mismo nombre

Para excluir todos los archivos con el mismo nombre, indique el nombre de archivo sin la ruta de acceso:

spacer.gif

Excluir una unidad local o compartida

Para excluir una unidad local o compartida, indique la letra de la unidad local o el nombre de la unidad compartida:

C:

\\servidor

Excluir una carpeta

Para excluir una carpeta y todo su contenido, indique la ruta de acceso a la carpeta en una unidad local o compartida:

D:\Herramientas\registros

Excluir todas las carpetas con el mismo nombre

Para excluir todas las carpetas con el mismo nombre en **cualquier** unidad local o compartida, indique el nombre de la carpeta sin la unidad. Por ejemplo, \Herramientas\registros excluye las siguientes carpetas:

C:\Herramientas\registros

\\servidor\Herramientas\registros

Nota: debe especificar la ruta de acceso sin la unidad, local o compartida. En el ejemplo anterior, si sólo escribe \registros\ no se excluirá ningún archivo.

Los caracteres comodín ? y *

Utilice el carácter comodín ? en el nombre o extensión de un archivo para sustituir a cualquier carácter.

Al final del nombre o extensión, el carácter comodín ? puede sustituir a un o ningún carácter. Por ejemplo, archivo?.txt incluiría archivo.txt, archivo1.txt y archivo12.txt, pero no file123.txt.

Utilice el carácter comodín * en el nombre o extensión de un archivo de la forma [nombre].* o *.[extensión]:

Uso correcto

archivo.*

*.txt

Uso incorrecto

archivo*.txt

archivo.txt*

archivo.*txt

Archivos con múltiples extensiones

Los archivos con múltiples extensiones serán tratados como si la última extensión es la extensión y el resto es el nombre del archivo.

ejemplo.txt.doc = nombre ejemplo.txt + extensión .doc.

4.2.9 Activar el control de comportamiento

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Sólo miembros del grupo SophosAdministrator pueden activar el control de comportamiento.

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Control de comportamiento** .
2. En el cuadro de diálogo **Configuración del control de comportamiento**, seleccione la opción **Activar el control de comportamiento**.

4.3 Escaneado en demanda

4.3.1 Tipos de escaneado en demanda

Escaneado del botón derecho

Para escanear archivos, carpetas o unidades del Explorador de Windows en cualquier momento.

- [Run a right-click scan](#) en la página 20

Escaneado personalizado

Para grupos específicos de archivos o carpetas. Los escaneados personalizados se pueden ejecutar de forma manual o programarse para que se ejecuten automáticamente.

- [Run a custom scan](#) en la página 25
- [Schedule a custom scan](#) en la página 24

Escaneado exhaustivo

Para escanear el sistema, incluido el sector de arranque y la memoria del sistema, en cualquier momento.

- [Run a full computer scan](#) en la página 26

4.3.2 Especificar extensiones de archivo del escaneado en demanda

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si lo desea, puede especificar las extensiones de archivo que se escanean durante el escaneado en demanda.

1. En el menú **Configurar**, seleccione **Extensiones y exclusiones en demanda**.

2. Abra la ficha **Extensiones** y configure las opciones según se describe a continuación.

Escanear todos los archivos

Seleccione esta opción para escanear todos los archivos, independientemente de la extensión.

Permitir el control de lo que se escanea

Seleccione esta opción para restringir el escaneo a los archivos con cierta extensión (especificadas en la lista de extensiones).



Advertencia: la lista de extensiones incluye los tipos de archivo que se recomienda escanear. Si va a modificar la lista, hágalo con cautela.

Para agregar extensiones a la lista, haga clic en **Añadir**. Puede utilizar el carácter comodín ? para indicar cualquier carácter posible.

Para borrar una extensión de la lista, selecciónela y haga clic en el botón **Eliminar**.

Para modificar una extensión de la lista, selecciónela y haga clic en el botón **Editar**.

Al seleccionar **Permitir el control de lo que se escanea**, estará activada por defecto la opción **Escanear archivos sin extensión**. Desactive la opción **Escanear archivos sin extensión** para no escanear archivos con la extensión omitida.

4.3.3 Añadir, modificar y borrar exclusiones del escaneo en demanda

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

El procedimiento descrito a continuación se aplica a **todos** los escaneados en demanda. Para más información sobre cómo excluir elementos del escaneo personalizado, consulte [Crear un escaneo personalizado](#) en la página 21.

Para modificar la lista de archivos, carpetas o unidades excluidas del escaneo en demanda:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Configuración > Extensiones y exclusiones en demanda**.
2. Abra la ficha **Exclusiones** y realice la acción necesaria.
 - Haga clic en **Añadir** para especificar un archivo, carpeta o unidad a excluir del escaneo en demanda.
 - Para borrar una exclusión, selecciónela y haga clic en **Eliminar**.
 - Para modificar una exclusión, selecciónela y haga clic en **Editar**.
3. Para añadir o modificar una exclusión, en el cuadro de diálogo **Exclusión de elementos**, seleccione el tipo de **Elemento**.
4. Indique el **Nombre** mediante el botón **Examinar** o introduciendo el nombre en el cuadro de texto.

Nota: si utiliza un sistema de 64 bits, el botón **Examinar** no estará visible en el cuadro de diálogo **Exclusión de elementos**.

Para más información, consulte [Especificar archivos y rutas para la exclusión de elementos](#) en la página 17.

4.3.4 Especificar archivos y rutas para la exclusión de elementos

Nomenclatura estándar

Sophos Anti-Virus utiliza la nomenclatura estándar de Windows a la hora de establecer las exclusiones de elementos. Por ejemplo, el nombre de una carpeta puede contener espacios pero no **sólo** espacios.

Excluir un archivo

Para excluir un archivo, debe especificar el nombre y la ruta de acceso. La ruta de acceso puede incluir una unidad local o compartida:

C:\Documentos\CV.doc

\\servidor\Usuarios\Documentos\CV.doc

Nota: para asegurar que la exclusión se aplica siempre correctamente, añada tanto el nombre largo como en formato 8.3:

C:\Archivos de programa\Sophos\Sophos Anti-Virus

C:\Archiv~1\Sophos\Sophos~1

Para más información, consulte <http://esp.sophos.com/support/knowledgebase/article/13045.html>.

Excluir todos los archivos con el mismo nombre

Para excluir todos los archivos con el mismo nombre, indique el nombre de archivo sin la ruta de acceso:

spacer.gif

Excluir una unidad local o compartida

Para excluir una unidad local o compartida, indique la letra de la unidad local o el nombre de la unidad compartida:

C:

\\servidor

Excluir una carpeta

Para excluir una carpeta y todo su contenido, indique la ruta de acceso a la carpeta en una unidad local o compartida:

D:\Herramientas\registros

Excluir todas las carpetas con el mismo nombre

Para excluir todas las carpetas con el mismo nombre en **cualquier** unidad local o compartida, indique el nombre de la carpeta sin la unidad. Por ejemplo, \Herramientas\registros excluye las siguientes carpetas:

C:\Herramientas\registros

\\servidor\Herramientas\registros

Nota: debe especificar la ruta de acceso sin la unidad, local o compartida. En el ejemplo anterior, si sólo escribe \registros\ no se excluirá ningún archivo.

Los caracteres comodín ? y *

Utilice el carácter comodín ? en el nombre o extensión de un archivo para sustituir a cualquier carácter.

Al final del nombre o extensión, el carácter comodín ? puede sustituir a un o ningún carácter. Por ejemplo, archivo?.txt incluiría archivo.txt, archivo1.txt y archivo12.txt, pero no file123.txt.

Utilice el carácter comodín * en el nombre o extensión de un archivo de la forma [nombre].* o *.*[extensión]:

Uso correcto

archivo.*

*.txt

Uso incorrecto

archivo*.txt

archivo.txt*

archivo.*txt

Archivos con múltiples extensiones

Los archivos con múltiples extensiones serán tratados como si la última extensión es la extensión y el resto es el nombre del archivo.

ejemplo.txt.doc = nombre ejemplo.txt + extensión .doc.

4.3.5 Escaneo de botón derecho

4.3.5.1 Configurar escaneados de botón derecho

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, *no* sobrescribirá los cambios que realice desde aquí.

Por defecto, Sophos Anti-Virus detecta y limpia las siguientes amenazas durante el escaneo del botón derecho:

- virus
- troyanos
- gusanos
- programas espía
- programas publicitarios y otras aplicaciones no deseadas

Para configurar el escaneo de botón derecho:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneo de botón derecho** .

2. En la sección **Detectar**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Adware y PUA	Los programas publicitarios muestran anuncios, por ejemplo, en ventanas emergentes, que afectan a la productividad del usuario y al rendimiento del sistema. Las aplicaciones no deseadas (PUA, Potentially Unwanted Applications) no son maliciosas, pero se consideran inapropiadas en redes corporativas..
Archivos sospechosos	Archivos con características habituales de virus, aunque no exclusivas.

3. En la sección **Otras opciones de escaneado**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Escanear todos los archivos	Sólo se recomienda utilizar esta opción en un escaneado semanal, ya que puede afectar al rendimiento del sistema.
Escanear archivos comprimidos	Active esta opción para escanear el contenido de archivos comprimidos al descargarlos o enviarlos por email. Se recomienda desactivar esta opción ya que puede ralentizar el escaneado. El contenido de los archivos comprimidos se escanea: <ul style="list-style-type: none"> ■ Cuando se realiza la extracción. ■ Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.

4.3.5.2 Configurar la limpieza del escaneado de botón derecho

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para configurar la limpieza del escaneado de botón derecho:

- Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado de botón derecho** .
- Abra la ficha **Limpieza**.
- En la sección **Viruses/spyware**, active la opción **Limpiar automáticamente elementos con virus/spyware**.

4. Seleccione la acción que desea llevar a cabo si Sophos Anti-Virus no puede llevar a cabo la limpieza automática:

Opción	Descripción
Sólo registrar	Sophos Anti-Virus sólo registra los archivos afectados sin realizar ninguna otra acción. Consulte View the scanning log en la página 47. Esta es la opción predeterminada.
Borrar Mover a	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar virus y programas espía que encuentre Sophos Anti-Virus. Consulte Deal with viruses/spyware in quarantine en la página 36.

5. En la sección **Archivos sospechosos**, seleccione la acción que desea llevar a cabo si Sophos Anti-Virus detecta código que puede ser malicioso:

Opción	Descripción
Sólo registrar	Sophos Anti-Virus sólo registra los archivos afectados sin realizar ninguna otra acción. Esta es la opción predeterminada.
Borrar Mover a	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar virus y programas espía que encuentre Sophos Anti-Virus. Consulte Deal with suspicious files in quarantine en la página 38.

6. Para eliminar programas publicitarios y aplicaciones no deseadas, en la sección **Adware/PUA**, active la opción **Limpiar automáticamente elementos con adware/PUA**. La limpieza no repara los cambios que el programa publicitario o la aplicación no deseada haya podido realizar.
- Para obtener más información desde la web de Sophos, consulte [Get cleanup information](#) en la página 42.
 - Para más información sobre cómo limpiar programas publicitarios y aplicaciones no deseadas desde el Área de cuarentena, consulte [Deal with adware and PUAs in quarantine](#) en la página 37.

4.3.5.3 Realizar un escaneado de botón derecho

Desde el Explorador de Windows y en el escritorio es posible escanear archivos, carpetas y unidades mediante el escaneado de botón derecho.

1. En el Explorador de Windows o en el escritorio, seleccione los archivos, carpetas y/o unidades a escanear.
Puede seleccionar más de un elemento.

- Haga clic con el botón derecho del ratón y seleccione **Escanear con Sophos Anti-Virus**.

Si se detecta alguna amenaza o aplicación restringida, haga clic en **Más** y consulte la sección *Gestionar elementos en cuarentena*.

4.3.6 Escaneados personalizados


4.3.6.1 Crear un escaneado personalizado

- En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
- Haga clic en **Crear un nuevo escaneado**.
- En el cuadro de texto **Nombre del escaneado**, indique un nombre descriptivo para el nuevo escaneado.
- En el panel **Elementos a escanear**, seleccione las unidades y carpetas que desee escanear. Para ello, active la casilla situada a la izquierda de cada unidad o carpeta. Para entender el significado de los iconos que aparecen junto a las casillas de activación, consulte [Representación de los elementos a escanear](#) en la página 21.
Nota: las unidades o carpetas que no están disponibles (porque no están conectadas o han sido borradas) se mostrarán tachadas. Serán eliminadas del panel **Elementos a escanear** si se desactivan o si se produce algún cambio en la selección de su unidad o carpeta padre.
- Haga clic en **Configurar el escaneado** para ver más opciones (consulte [Configurar escaneados personalizados](#) en la página 22 para más información).
- Para disponer de escaneado programado, haga clic en **Programar el escaneado** (consulte [Programar un escaneado personalizado](#) en la página 24 para más información).
- Haga clic en el botón **Guardar** para guardar el escaneado, o en **Guardar e iniciar** para guardar y ejecutar el escaneado.

4.3.6.2 Representación de los elementos a escanear

En el panel **Elementos a escanear** se mostrarán diferentes iconos en las casillas de activación, según los elementos a escanear. A continuación se explica cada uno de ellos.

Icono	Significado
<input type="checkbox"/>	El elemento y subelementos <i>no están</i> seleccionados para el escaneado.
<input checked="" type="checkbox"/>	El elemento y subelementos <i>están</i> seleccionados para el escaneado.
<input checked="" type="checkbox"/>	El elemento está seleccionado parcialmente, es decir, algunos subelementos están seleccionados para el escaneado.
<input checked="" type="checkbox"/>	El elemento y subelementos están excluidos en este escaneado.
<input checked="" type="checkbox"/>	El elemento está excluido parcialmente, es decir, algunos subelementos están excluidos en este escaneado.

Icono	Significado
	El elemento y subelementos están excluidos en todos los escaneados en demanda al existir una exclusión general en demanda. Para más información, consulte Añadir, modificar y borrar exclusiones del escaneado en acceso en la página 12.

4.3.6.3 Configurar escaneados personalizados

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Por defecto, Sophos Anti-Virus detecta y limpia las siguientes amenazas durante un escaneado personalizado:

- virus
- troyanos
- gusanos
- programas espía
- programas publicitarios y otras aplicaciones no deseadas
- rootkits

Para configurar un escaneado personalizado:

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, seleccione el escaneado que desee editar y haga clic en **Editar**.
3. Haga clic en **Configurar el escaneado**.
4. En la sección **Detectar**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Adware y PUA	Los programas publicitarios muestran anuncios, por ejemplo, en ventanas emergentes, que afectan a la productividad del usuario y al rendimiento del sistema. Las aplicaciones no deseadas (PUA, Potentially Unwanted Applications) no son maliciosas, pero se consideran inapropiadas en redes corporativas..
Archivos sospechosos	Archivos con características habituales de virus, aunque no exclusivas.
Rootkits	Si pertenece al grupo SophosAdministrator, al realizar un escaneado completo también se detectarán rootkits. También se pueden detectar rootkits en escaneados personalizados.

5. En la sección **Otras opciones de escaneo**, seleccione las opciones necesarias según se describe a continuación.

Opción	Descripción
Escanear todos los archivos	Sólo se recomienda utilizar esta opción en un escaneo semanal, ya que puede afectar al rendimiento del sistema.
Escanear archivos comprimidos	<p>Active esta opción para escanear el contenido de archivos comprimidos al descargarlos o enviarlos por email.</p> <p>Se recomienda desactivar esta opción ya que puede ralentizar el escaneo.</p> <p>El contenido de los archivos comprimidos se escanea:</p> <ul style="list-style-type: none"> ■ Cuando se realiza la extracción. ■ Los archivos comprimidos con herramientas de compresión dinámica (PKLite, LZEXE o Diet) se escanean siempre.
Escanear memoria del sistema	Active esta opción para disponer de un escaneo en segundo plano cada hora que detecte amenazas en la memoria del sistema.
Ejecutar escaneo con baja prioridad	En Windows Vista y posterior, realiza los escaneos personalizados en baja prioridad para minimizar el impacto en los recursos del sistema.

4.3.6.4 Configurar la limpieza del escaneo personalizado

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para configurar la limpieza del escaneo personalizado:

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, seleccione el escaneo que desee editar y haga clic en **Editar**.
3. Haga clic en **Configurar el escaneo**.
4. Abra la ficha **Limpieza**.
5. En la sección **Viruses/spyware**, active la opción **Limpiar automáticamente elementos con virus/spyware**.

6. Seleccione la acción que desea llevar a cabo si Sophos Anti-Virus no puede llevar a cabo la limpieza automática:

Opción	Descripción
Sólo registrar	Sophos Anti-Virus sólo registra los archivos afectados sin realizar ninguna otra acción. Consulte View the log for a custom scan en la página 26. Esta es la opción predeterminada.
Borrar Mover a	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar virus y programas espía que encuentre Sophos Anti-Virus. Consulte Deal with viruses/spyware in quarantine en la página 36.

7. En la sección **Archivos sospechosos**, seleccione la acción que desea llevar a cabo si Sophos Anti-Virus detecta código que puede ser malicioso:

Opción	Descripción
Sólo registrar	Sophos Anti-Virus sólo registra los archivos afectados sin realizar ninguna otra acción. Esta es la opción predeterminada.
Borrar Mover a	Sólo debería utilizar estas opciones bajo las indicaciones del soporte técnico de Sophos. Utilice el Área de cuarentena para limpiar virus y programas espía que encuentre Sophos Anti-Virus. Consulte Deal with suspicious files in quarantine en la página 38.

8. Para eliminar programas publicitarios y aplicaciones no deseadas, en la sección **Adware/PUA**, active la opción **Limpiar automáticamente elementos con adware/PUA**. La limpieza no repara los cambios que el programa publicitario o la aplicación no deseada haya podido realizar.
- Para obtener más información desde la web de Sophos, consulte [Get cleanup information](#) en la página 42.
 - Para más información sobre cómo limpiar programas publicitarios y aplicaciones no deseadas desde el Área de cuarentena, consulte [Deal with adware and PUAs in quarantine](#) en la página 37.

4.3.6.5 Programar un escaneo personalizado

Si pertenece al grupo SophosAdministrator, puede programar los escaneados personalizados, además de poder ver y editar escaneados creados por otros usuarios.

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

2. En la lista de **Escaneados disponibles**, seleccione el escaneado que desee editar y haga clic en **Editar**.
3. Haga clic en **Programar el escaneado**.
4. En el cuadro de diálogo **Programar el escaneado**, seleccione **Activar escaneado programado**.
Seleccione el día o días en los que desea que se lleve a cabo el escaneado.
Haga clic en el botón **Añadir** para indicar las horas a las que se ejecutará el escaneado.
Utilice los botones **Eliminar** y **Editar** para modificar la lista de horas del escaneado.
5. Escriba el *nombre de usuario y contraseña*. La contraseña no puede estar en blanco.
El escaneado programado se ejecutará con los derechos de este usuario.

Nota: si se detecta alguna amenaza en la memoria, y no tiene activada la limpieza automática, el escaneado se detiene. Esto se debe a que si se continúa con el escaneado, la amenaza se podría extender. Debe limpiar la amenaza antes de continuar con el escaneado.

4.3.6.6 Ejecutar un escaneado personalizado

Nota: los escaneados programados no se pueden ejecutar de forma manual. Los escaneados programados aparecerán en la lista de **Escaneados disponibles** con un reloj.

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acercas de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, seleccione el escaneado que desee ejecutar y haga clic en **Iniciar**.
Se abrirá un cuadro de diálogo con una barra de evolución y, en la ventana de , se mostrará el panel **Resumen de actividad**.

Nota: si se detecta alguna amenaza en la memoria, y no tiene activada la limpieza automática, el escaneado se detiene. Esto se debe a que si se continúa con el escaneado, la amenaza se podría extender. Debe limpiar la amenaza antes de continuar con el escaneado.

Si aparecen aplicaciones restringidas o amenazas, haga clic en **Más** y consulte la sección *Gestionar elementos en cuarentena*.

4.3.6.7 Cambiar el nombre de un escaneado personalizado

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acercas de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, seleccione el escaneado que desee editar y haga clic en **Editar**.
3. En el cuadro de texto **Nombre del escaneado** escriba el nuevo nombre.

4.3.6.8 Ver el registro de un escaneado personalizado

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, haga clic en **Resumen**.
3. En el cuadro de diálogo de **Resumen**, haga clic en el enlace de la parte inferior.

Desde la página del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

Para buscar un texto concreto en el registro, haga clic en **Buscar** e introduzca el texto que desea encontrar.

4.3.6.9 Ver resúmenes de escaneados personalizados

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, haga clic en **Resumen**.

4.3.6.10 Borrar un escaneado personalizado

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escaneados**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista de **Escaneados disponibles**, seleccione el escaneado que desee eliminar y haga clic en **Borrar**.

4.3.7 Realizar un escaneado exhaustivo

Para realizar un escaneado exhaustivo del ordenador, incluido el sector de arranque y la memoria del sistema:

- ❖ En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Escanear el ordenador**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

Se abrirá un cuadro de diálogo con una barra de evolución y, en la ventana de **Sophos Endpoint Security and Control**, se mostrará el panel **Resumen de actividad**.

Nota: si se detecta alguna amenaza en la memoria, el escaneado se detiene. Esto se debe a que si se continua con el escaneado, la amenaza se podría extender. Debe limpiar la amenaza antes de continuar con el escaneado.

Si aparecen aplicaciones restringidas o amenazas, haga clic en **Más** y consulte la sección *Gestionar elementos en cuarentena*.

4.4 Control de comportamiento de Sophos

4.4.1 Acerca de la monitorización de comportamiento

Integrado en el escaneo en acceso, el sistema de control de comportamiento de Sophos protege equipos con Windows 2000 y posterior contra amenazas desconocidas y comportamiento sospechoso.

La detección en tiempo de ejecución permite interceptar amenazas que no se pueden detectar con anterioridad. El sistema de control de comportamiento utiliza dos métodos para interceptar amenazas:

- Detección de comportamiento malicioso o sospechoso
- Detección de desbordamiento del búfer.

Detección de comportamiento malicioso o sospechoso

La detección de comportamientos sospechosos utiliza el sistema de prevención contra intrusiones en el host HIPS de Sophos para analizar de forma dinámica el comportamiento de todos los programas en ejecución, y detectar y bloquear toda actividad que parezca maliciosa. Los cambios en el registro que puedan permitir que un virus se ejecute de forma automática al reiniciar el equipo pueden considerarse como comportamientos sospechosos.

El sistema de detección de comportamiento sospechoso comprueba los procesos activos en busca de indicios que denoten la presencia de programas maliciosos. Se puede configurar para alertar y detener los procesos sospechosos.

La detección de comportamiento malicioso consiste en el análisis dinámico de todos los programas en ejecución para detectar y bloquear actividades que parezcan maliciosas.

Detección de desbordamiento del búfer

Esta función es imprescindible para detener amenazas de "día cero".

El sistema de análisis dinámico del comportamiento de los programas en ejecución permite evitar el desbordamiento del búfer como forma de ataque. Esto permite detener ataques relacionados con agujeros de seguridad en el sistema operativo y aplicaciones.

4.4.2 Activar el control de comportamiento

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Sólo miembros del grupo SophosAdministrator pueden activar el control de comportamiento.

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Control de comportamiento** .
2. En el cuadro de diálogo **Configuración del control de comportamiento**, seleccione la opción **Activar el control de comportamiento**.

4.4.3 Bloquear comportamiento malicioso

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

La detección de comportamiento malicioso consiste en el análisis dinámico de todos los programas en ejecución para detectar y bloquear actividades que parezcan maliciosas.

Si pertenece al grupo SophosAdministrator, puede cambiar la configuración de la detección comportamiento malicioso:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Control de comportamiento** .
2. En el cuadro de diálogo **Configuración del control de comportamiento**, seleccione la opción **Activar el control de comportamiento**.
3. Para detectar y alertar ante comportamiento malicioso, seleccione la opción **Detectar comportamiento malicioso**.

4.4.4 Evitar comportamiento sospechoso

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

El sistema de detección de comportamiento sospechoso comprueba los procesos activos en busca de indicios que denoten la presencia de programas maliciosos. Se puede configurar para alertar y detener los procesos sospechosos.

Si pertenece al grupo SophosAdministrator, puede cambiar la configuración de la detección comportamiento sospechoso:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Control de comportamiento** .
2. En el cuadro de diálogo **Configuración del control de comportamiento**, seleccione la opción **Activar el control de comportamiento**.
3. Seleccione la opción **Detectar comportamiento malicioso**.
4. Para detectar y alertar ante comportamiento sospechoso, seleccione la opción **Detectar comportamiento sospechoso**.
5. Para alertar ante comportamiento sospechoso, seleccione la opción **Sólo alertar ante comportamiento sospechoso**.

Para una protección más completa, se recomienda detectar comportamiento sospechoso. Para más información, consulte:

- [Configurar el escaneado en acceso](#) en la página 8
- [Configurar escaneados de botón derecho](#) en la página 18
- [Configurar escaneados personalizados](#) en la página 22

4.4.5 Evitar desbordamiento del búfer

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

El sistema de análisis dinámico del comportamiento de los programas en ejecución permite evitar el desbordamiento del búfer como forma de ataque.

Si pertenece al grupo SophosAdministrator, puede cambiar la configuración de la detección de desbordamiento del búfer:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Control de comportamiento** .
2. En el cuadro de diálogo **Configuración del control de comportamiento**, seleccione la opción **Activar el control de comportamiento**.
3. Para detectar y alertar ante el desbordamiento del búfer, seleccione la opción **Detectar desbordamiento del búfer**.
4. Para alerta ante el desbordamiento del búfer, seleccione la opción **Sólo alertar**.

4.5 Protección activa de Sophos

4.5.1 Acerca de la protección activa de Sophos

La protección activa de Sophos determina si los archivos sospechosos suponen una amenaza y, en caso afirmativo, se llevan a cabo de inmediato las acciones especificadas en la configuración para la limpieza de virus de Sophos Anti-Virus.

La protección activa de Sophos mejora de forma significativa la detección de nuevas amenazas sin el riesgo de falsos positivos. La comprobación se realiza con los datos de los programas maliciosos más recientes. Cuando se detecte una nueva amenaza, Sophos enviará la actualización de forma inmediata.

La protección activa de Sophos utiliza las opciones siguientes:

■ **Activar la protección activa**

Si en un escaneo se detecta algún archivo sospechoso pero no se consigue su identificación con los datos de detección en dicho ordenador, se enviarán a Sophos ciertos datos del archivo (como la suma de verificación y otros atributos) para su verificación.

Para la comprobación se utilizan las bases de datos de SophosLabs. La respuesta se envía al ordenador, donde se actualiza de forma automática el estado del archivo afectado.

■ **Enviar archivos de muestra de forma automática a Sophos**

Si un archivo se considera sospechoso, pero los datos del archivo no son suficientes para identificarlo como malicioso, puede enviar una muestra del mismo a Sophos. Si activa esta opción y Sophos no dispone todavía de la muestra necesaria, se enviará de forma automática una copia del archivo.

El envío de archivos de muestra permite que Sophos mejore la detección de programas maliciosos de forma continua y se elimine el riesgo de falsos positivos.

4.5.2 Activar o desactivar las opciones de la protección activa de Sophos

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Los miembros del grupo SophosAdministrator pueden activar o desactivar las opciones para la protección activa de Sophos:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Configuración > Protección activa de Sophos**.
2. En el cuadro de diálogo **Protección activa de Sophos**:
 - Para activar o desactivar el envío de datos de archivos a Sophos, active o desactive la opción **Activar la protección activa**.
 - Para activar o desactivar el envío de muestras de archivos a Sophos, active o desactive la opción **Enviar automáticamente muestras de archivos**.

Esta opción sólo está disponible si seleccionó **Activar la protección activa**.

Nota

Cuando se envía una muestra a Sophos también se incluyen los datos del archivo.

4.5.3 Ver el registro de la protección activa de Sophos

La información enviada a Sophos para el escaneado en línea y el estado del archivo se indica en el registro del escaneado.

Si está activada la protección activa de Sophos, el registro muestra:

- La ruta de acceso al archivo sospechoso.
- La fecha y hora en que se enviaron los datos.
- Los motivos de los posibles errores que se puedan producir al enviar los datos.
- El estado del archivo como resultado del escaneado (por ejemplo, “virus/spyware” si se ha identificado como malicioso).

Para ver el registro del escaneado:

- En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Ver el registro del antivirus y HIPS**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

Desde la página del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

Para buscar un texto concreto en el registro, haga clic en **Buscar** e introduzca el texto que desea encontrar.

4.6 Protección web de Sophos

4.6.1 Acerca de la protección web de Sophos

La protección web de Sophos ofrece una protección mejorada contra las amenazas de Internet. Para su funcionamiento utiliza la base de datos online de Sophos con direcciones web y bloquea el acceso a aquellos sitios web que albergan programas maliciosos.

La protección web es compatible con los siguientes navegadores:

- Internet Explorer
- Firefox
- Google Chrome
- Safari
- Opera

Cuando se bloquea el acceso a un sitio web, se crea un evento en el registro de escaneado. Para más información sobre el registro de escaneado, consulte [Ver el registro del escaneado](#) en la página 47.

4.6.2 Desbloquear el acceso a sitios web maliciosos

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para desbloquear el acceso a sitios web maliciosos:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Configuración > Protección web**.
2. En **Bloquear acceso a sitios web maliciosos**, seleccione **No**.
Para más información sobre cómo autorizar sitios web clasificados como maliciosos, consulte [Autorizar sitios web](#) en la página 33.
3. En **Escanear descargas**, seleccione **No**, **Sí** o **Según el escaneado en acceso**.
La opción **Según el escaneado en acceso** utilizará la configuración del *escaneado en acceso*.

4.7 Restricción de aplicaciones de Sophos

4.7.1 Acerca del escaneado de aplicaciones restringidas

Las *aplicaciones restringidas* son aplicaciones que la política de seguridad empresarial impide ejecutar en los equipos.

La detección de aplicaciones restringidas se activa y desactiva desde la consola de administración como parte de la política interna de cada empresa y se incluye como parte del escaneado en acceso.

Para más información sobre el escaneado en acceso, consulte [Acerca del escaneado en acceso y en demanda](#) en la página 8.

4.7.2 Desactivar el escaneado de aplicaciones restringidas

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si activa la detección de aplicaciones restringidas, es posible que se bloquee la instalación de ciertos programas. Si pertenece al grupo SophosAdministrator, puede desactivar de forma temporal el escaneado de aplicaciones restringidas en el equipo:

Para desactivar el escaneado de aplicaciones restringidas:

1. En el menú **Configurar**, seleccione **Restricción de aplicaciones**.
2. Desactive la opción **Activar escaneado en acceso**.

4.8 Autorizar el uso de elementos

4.8.1 Autorizar el uso de programas publicitarios y aplicaciones no deseadas

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si desea ejecutar programas publicitarios o aplicaciones que Sophos Anti-Virus ha clasificado como no deseadas, autorícelas.

Para autorizar el uso de programas publicitarios y aplicaciones no deseadas:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Configurar autorización**.
2. En la ficha **Adware/PUA**, en la lista **Adware/PUA conocidos**, seleccione el programa publicitario o aplicación no deseada.
3. Haga clic en **Añadir**.

El programa publicitario o la aplicación no deseada aparecerá en el cuadro de la lista **Adware/PUA autorizados**.

Nota: también es posible autorizar programas publicitarios y aplicaciones no deseadas desde el Área de cuarentena. Para más información sobre cómo hacerlo, consulte [Revisar programas publicitarios y aplicaciones no deseadas en cuarentena](#) en la página 37.

4.8.2 Bloquear aplicaciones no deseadas y programas publicitarios autorizados

Para impedir la ejecución de programas publicitarios (adware) y aplicaciones no deseadas (PUA) actualmente autorizados:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Configurar autorización**.

2. En la ficha **Adware/PUA**, en la lista **Adware/PUA autorizados**, seleccione el programa publicitario o aplicación no deseada que desea bloquear.
3. Haga clic en **Quitar**.

4.8.3 Autorizar el uso de elementos sospechosos

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si desea autorizar un elemento que Sophos Anti-Virus ha clasificado como sospechoso, autorícelo como se explica a continuación.

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Configurar autorización**.
2. Abra la ficha del tipo de elemento detectado, por ejemplo, **Desbordamiento del búfer**.
3. En la lista **Conocidos**, seleccione el elemento sospechoso.
4. Haga clic en **Añadir**.

El elemento sospechoso aparece en la lista **Autorizados**.

Nota: también es posible autorizar elementos sospechosos desde el Área de cuarentena. Para más información, consulte los temas siguientes:

- [Revisar archivos sospechosos en cuarentena](#) en la página 38
- [Revisar comportamientos sospechosos en cuarentena](#) en la página 40

4.8.4 Preautorizar elementos sospechosos

Si desea autorizar un elemento que Sophos Endpoint Security and Control no ha clasificado aún como sospechoso, preautorícelo según se explica a continuación.

Para preautorizar un elemento:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Configurar autorización**.
2. Abra la ficha del tipo de elemento detectado, por ejemplo, **Desbordamiento del búfer**.
3. Haga clic en **Nuevo**.
4. Haga doble clic en el elemento.

El elemento sospechoso aparece en la lista **Autorizados**.

4.8.5 Autorizar sitios web

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si desea desbloquear un sitio web que Sophos ha clasificado como malicioso, añádalo a la lista de sitios autorizados. Al autorizar un sitio web, Sophos deja de verificar las direcciones web del sitio con el servicio de filtrado web online.



Advertencia: al autorizar sitios web clasificados como maliciosos, puede correr el peligro de exponerse a amenazas. Asegúrese de que el sitio web es seguro antes de autorizarlo.

Para autorizar sitios web:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Configurar autorización** .
2. Abra la ficha **Sitios web**.
3. Haga clic en **Añadir**.
4. Indique el nombre de dominio o la dirección IP.

El sitio web se mostrará en la lista **Sitios web autorizados**.

4.9 Gestionar elementos en cuarentena

4.9.1 Acerca del área de cuarentena

El área de cuarentena permite gestionar los elementos encontrados durante el escaneo que no se hayan eliminado de forma automática. Los elementos en el área de cuarentena llegan ahí por los siguientes motivos:

- No se seleccionaron opciones de limpieza (limpiar, eliminar, mover) para el tipo de escaneo que encontró el elemento.
- No se pudo llevar a cabo la acción indicada para el escaneo.
- El elemento tiene múltiples infecciones y todavía contiene amenazas.
- La amenaza ha sido detectada sólo de forma parcial y se requiere un escaneo exhaustivo del ordenador. Para saber cómo hacerlo, consulte [Realizar un escaneo exhaustivo](#) en la página 26.
- El elemento muestra un comportamiento sospechoso.
- El elemento es una aplicación restringida.

Nota: los programas publicitarios, aplicaciones no deseadas e infecciones de varios componentes detectados durante el escaneo en acceso se enumeran siempre en el Área de cuarentena. Desde el escaneo en acceso no es posible realizar la limpieza automática de aplicaciones no deseadas, programas publicitarios o infecciones múltiples.

La limpieza puede fallar si no dispone del permiso de acceso apropiado. Si dispone de los derechos suficientes, podrá utilizar el área de cuarentena para gestionar los elementos.

Las amenazas detectadas en el escaneo de páginas web no se muestran en la cuarentena ya que no se encuentran en su ordenador. En este caso no se requiere ninguna acción.

4.9.2 Ventana principal del Área de cuarentena

En el Área de cuarentena se muestran los elementos detectados durante el escaneo. Los elementos del **Área de cuarentena** se describen a continuación.



1	En el cuadro de lista Ver , seleccione el tipo de elemento que desea mostrar.
2	Identidad del elemento, con un enlace al análisis correspondiente en la web de Sophos.
3	Nombre del archivo y ubicación del elemento. Si el elemento está asociado con un rootkit, aparece como Oculto . Si el elemento está afectado por una infección múltiple, aparecerá un enlace con más información junto al nombre del archivo. Haga clic en el enlace para ver el resto de componentes que forman parte de la infección. Si alguno de los componentes está asociados con un rootkit, se mostrará como oculto.
4	Las acciones disponibles. Si el elemento no está oculto, se ofrece: Limpiar, Eliminar o Mover . Haga clic en la acción que desee llevar a cabo. Los archivos ocultos sólo se pueden limpiar.
5	La lista de elementos detectados. Para ordenar la lista, haga clic en el encabezado de la columna adecuada.
6	Utilice el botón Seleccionar todo para realizar la misma acción en todos los elementos de la lista. Para deseleccionar un elemento, desactive la casilla correspondiente en la columna Tipo .
7	Para deseleccionar todos los elementos seleccionados, haga clic en el botón Deseleccionar todo . Para seleccionar un elemento, active la casilla correspondiente en la columna Tipo .
8	Haga clic en Quitar de la lista para quitar los elementos seleccionados de la lista sin realizar ninguna acción. Esta acción no borra los archivos del disco duro.



Haga clic en **Realizar acción** para mostrar la lista de acciones disponibles para los elementos seleccionados.

4.9.3 Revisar virus y programas espía en cuarentena

Nota: la palabra *virus* se utilizará aquí para referirse a cualquier virus, gusano, troyano o cualquier otro tipo de código malintencionado.

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Revisar la cuarentena**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista **Ver**, seleccione **Virus/spyware**.

Las columnas contienen información sobre cada elemento.

La columna **Nombre** muestra la identidad que ha detectado Sophos Anti-Virus. Para obtener más información sobre el virus o sobre el programa espía, haga clic en la identidad para que Sophos Anti-Virus le conecte con el análisis correspondiente en el sitio web de Sophos.

La columna **Detalles** muestra el nombre y la ubicación del elemento. Si el elemento está asociado con un rootkit, aparece como "Oculto". Si el elemento está afectado por una infección múltiple, aparecerá un enlace con **más información** junto al nombre del archivo. Haga clic en el enlace para ver el resto de componentes que forman parte de la infección. Si alguno de los componentes están asociados con un rootkit, el cuadro de diálogo indica que algunos componentes están ocultos.

La columna **Acciones disponibles** muestra las acciones que puede realizar con el elemento. Si el elemento no está oculto, puede limpiarlo, eliminarlo o moverlo, según se describe a continuación. Para ejecutar cualquiera de las acciones, selecciónela. Los archivos ocultos sólo se pueden limpiar.

Tratar elementos infectados

Para tratar los virus y programas espía, utilice los botones que se describen a continuación.

Seleccionar todo, Deseleccionar todo

Utilice estos botones para seleccionar o deseleccionar todos los elementos de la lista. De esta forma podrá realizar una acción en toda la selección. Para seleccionar o deseleccionar un elemento en particular, haga clic en la casilla situada a la izquierda del tipo de elemento.

Quitar de la lista

Haga clic aquí para eliminar elementos seleccionados de la lista, si está seguro de que no contienen virus o programas espía. Este botón no borra los archivos del disco duro.

Realizar acción

Haga clic aquí para mostrar una lista de acciones que puede realizar con los elementos seleccionados.

- Haga clic en **Limpiar** para eliminar un virus o programa espía de los elementos seleccionados. La limpieza de documentos no puede deshacer los efectos secundarios que el virus haya podido causar.

Nota: para limpiar completamente los virus o programas espía formados por varios componentes, o para limpiar archivos ocultos, tendrá que reiniciar el ordenador. En este caso, tendrá la opción de reiniciar el sistema de forma inmediata o más tarde. El proceso de limpieza continuará cuando reinicie el sistema.

Nota: la limpieza de ciertos virus requiere un escaneado completo del sistema, durante el que se intentarán limpiar *todos* los virus. Esto puede tardar bastante. La acción disponible cambia a **Limpiando** durante el escaneado.

- Haga clic en **Borrar** para borrar los elementos seleccionados. Tenga precaución al utilizar este botón.
- Haga clic en **Mover** para mover los elementos seleccionados a otra carpeta. Los elementos se moverán a la carpeta indicada en la configuración de limpieza. Mover un archivo ejecutable reduce la probabilidad de activarlo. Tenga precaución al utilizar este botón.



Advertencia: a veces, al eliminar o mover un archivo infectado, el equipo puede dejar de funcionar correctamente porque no puede encontrar el archivo. Además, un archivo infectado puede ser sólo parte de una infección múltiple, en cuyo caso la eliminación de dicho archivo no limpiará el sistema. En ese caso, póngase en contacto con el servicio técnico de Sophos para obtener ayuda.

Para ver la información de contacto, consulte [Soporte técnico](#) en la página 104.

Para configurar las acciones disponibles, consulte [Configurar los derechos sobre el área de cuarentena](#) en la página 6.

4.9.4 Revisar programas publicitarios y aplicaciones no deseadas en cuarentena

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Revisar la cuarentena**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista **Ver**, seleccione **Adware/PUA**.

Las columnas contienen información sobre cada elemento.

La columna **Nombre** muestra la identidad que ha detectado Sophos Anti-Virus. Para obtener más información sobre los programas publicitarios o aplicaciones no deseadas, haga clic en la identidad para que Sophos Anti-Virus le conecte con el análisis correspondiente en el sitio web de Sophos.

La columna **Detalles** muestra el subtipo de programa publicitario o aplicación no deseada. Si el elemento está asociado con un rootkit, aparece como "Oculto". Si el elemento está afectado por una infección múltiple, aparecerá un enlace con **más** información junto al nombre del archivo. Haga clic en el enlace para ver el resto de componentes que forman parte del programa publicitario o aplicación no deseada. Si alguno de los componentes están asociados con un rootkit, el cuadro de diálogo indica que algunos componentes están ocultos.

La columna **Acciones disponibles** muestra las acciones que puede realizar con el elemento. Existen dos: Autorizar y Limpiar, que se describen a continuación. Para ejecutar cualquiera de las acciones, selecciónela.

Gestionar los programas publicitarios o aplicaciones no deseadas

Para gestionar los programas publicitarios o aplicaciones no deseadas, utilice los botones que se describen a continuación.

Seleccionar todo, Deseleccionar todo

Utilice estos botones para seleccionar o deseleccionar todos los elementos de la lista. De esta forma podrá realizar una acción en toda la selección. Para seleccionar o deseleccionar un elemento en particular, haga clic en la casilla situada a la izquierda del tipo de elemento.

Quitar de la lista

Utilice este botón para borrar de la lista elementos que no suponen una amenaza. Este botón no borra los archivos del disco duro.

Realizar acción

Haga clic aquí para mostrar una lista de acciones que puede realizar con los elementos seleccionados.

- Haga clic en **Autorizar** para autorizar los elementos seleccionados, si son de confianza. De esta forma los elementos pasan a la lista de programas publicitarios y aplicaciones no deseadas autorizados y Sophos Anti-Virus no los bloqueará.
- Haga clic en **Limpiar** para eliminar todos los componentes conocidos de los elementos seleccionados para todos los usuarios. Para limpiar programas publicitarios y aplicaciones no deseadas, debe pertenecer a los grupos de administradores de Windows y administradores de Sophos.

Nota: para limpiar completamente los programas maliciosos o aplicaciones no deseadas formados por varios componentes, o para limpiar archivos ocultos, tendrá que reiniciar el ordenador. En este caso, tendrá la opción de reiniciar el sistema de forma inmediata o más tarde. El proceso de limpieza continuará cuando reinicie el sistema.

Para configurar las acciones disponibles, consulte [Configurar los derechos sobre el área de cuarentena](#) en la página 6.

Para ver la lista de programas publicitarios y aplicaciones no deseadas autorizados, haga clic en **Configurar autorización**.

4.9.5 Revisar archivos sospechosos en cuarentena

Los *archivos sospechosos* son archivos con características habituales de virus, aunque no exclusivas.

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Revisar la cuarentena**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista **Ver**, seleccione **Archivos sospechosos**.

Las columnas contienen información sobre cada elemento.

La columna **Nombre** muestra la identidad que ha detectado Sophos Anti-Virus. Para obtener más información sobre el archivo sospechoso, haga clic en la identidad para que Sophos Anti-Virus le conecte con el análisis correspondiente en el sitio web de Sophos.

La columna **Detalles** muestra el nombre y la ubicación del elemento. Si el elemento está asociado con un rootkit, aparece como "Oculto".

La columna **Acciones disponibles** muestra las acciones que puede realizar con el elemento. Si el elemento no está oculto, puede autorizarlo, eliminarlo o moverlo, según se describe a continuación. Para ejecutar cualquiera de las acciones, selecciónela. Los archivos ocultos sólo se pueden autorizar.

Tratar archivos sospechosos

Las opciones disponibles se describen a continuación.

Seleccionar todo, Deseleccionar todo

Utilice estos botones para seleccionar o deseleccionar todos los elementos de la lista. De esta forma podrá realizar una acción en toda la selección. Para seleccionar o deseleccionar un elemento en particular, haga clic en la casilla situada a la izquierda del tipo de elemento.

Quitar de la lista

Utilice este botón para borrar de la lista elementos que no suponen una amenaza. Este botón no borra los archivos del disco duro.

Realizar acción

Haga clic aquí para mostrar una lista de acciones que puede realizar con los elementos seleccionados.

- Haga clic en **Autorizar** para autorizar los elementos seleccionados, si son de confianza. De esta forma los elementos pasan a la lista de archivos sospechosos autorizados y Sophos Anti-Virus no los bloqueará.
- Haga clic en **Borrar** para borrar los elementos seleccionados. Tenga precaución al utilizar este botón.
- Haga clic en **Mover** para mover los elementos seleccionados a otra carpeta. Los elementos se moverán a la carpeta indicada en la configuración de limpieza. Mover un archivo ejecutable reduce la probabilidad de activarlo. Tenga precaución al utilizar este botón.



Advertencia: a veces, al eliminar o mover un archivo infectado, el equipo puede dejar de funcionar correctamente porque no puede encontrar el archivo.

Para configurar las acciones disponibles, consulte [Configurar los derechos sobre el área de cuarentena](#) en la página 6.

Para ver la lista de archivos sospechosos autorizados, haga clic en **Configurar autorización**.

4.9.6 Revisar comportamientos sospechosos en cuarentena

El *comportamiento sospechoso* es toda actividad con apariencia maliciosa.

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Revisar la cuarentena**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista **Ver**, seleccione **Comportamiento sospechoso**.

Las columnas contienen información sobre cada elemento.

La columna **Nombre** muestra la identidad que ha detectado Sophos Anti-Virus. Para obtener más información sobre el comportamiento, haga clic en la identidad para que Sophos Anti-Virus le conecte con el análisis correspondiente en el sitio web de Sophos.

La columna **Detalles** muestra el nombre y la ubicación del elemento.

La columna **Acciones disponibles** muestra las acciones que puede realizar con el elemento. Si ha activado el bloqueo de comportamientos sospechosos, hay una acción: Autorizar, que se describe a continuación. Para ejecutar cualquiera de las acciones, selecciónela.

Tratar comportamientos sospechosos

Las opciones disponibles se describen a continuación.

Seleccionar todo, Deseleccionar todo

Utilice estos botones para seleccionar o deseleccionar todos los elementos de la lista. De esta forma podrá realizar una acción en toda la selección. Para seleccionar o deseleccionar un elemento en particular, haga clic en la casilla situada a la izquierda del tipo de elemento.

Quitar de la lista

Utilice este botón para borrar de la lista elementos que no suponen una amenaza. Este botón no borra los archivos del disco duro.

Realizar acción

Haga clic aquí para mostrar una lista de acciones que puede realizar con los elementos seleccionados.

- Haga clic en **Autorizar** para autorizar los elementos seleccionados, si son de confianza. De esta forma los elementos pasan a la lista de archivos sospechosos autorizados y Sophos Anti-Virus no impide el comportamiento.

Para configurar las acciones disponibles, consulte [Configurar los derechos sobre el área de cuarentena](#) en la página 6.

Para ver la lista de comportamientos sospechosos autorizados, haga clic en **Configurar autorización**.

4.9.7 Revisar las aplicaciones restringidas en cuarentena

Las *aplicaciones restringidas* son aplicaciones que la política de seguridad empresarial impide ejecutar en los equipos.

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Revisar la cuarentena**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la lista **Ver**, seleccione **Aplicaciones restringidas**.

Las columnas contienen información sobre cada elemento.

La columna **Nombre** muestra la identidad que ha detectado Sophos Anti-Virus. Para obtener más información sobre la aplicación restringida, haga clic en la identidad para que Sophos Anti-Virus le conecte con el análisis correspondiente en el sitio web de Sophos.

La columna **Detalles** muestra el subtipo de aplicación restringida. Si desea ver la lista del resto de componentes que forman parte de la aplicación restringida, haga clic en el enlace **más** que aparece junto al subtipo.

La columna **Acciones disponibles** muestra las acciones que puede realizar con el elemento. Sin embargo, la única acción disponible para las aplicaciones restringidas es limpiar el elemento de la lista, que se describe a continuación.

Gestionar las aplicaciones restringidas

Las opciones disponibles se describen a continuación.

Seleccionar todo, Deseleccionar todo

Utilice estos botones para seleccionar o deseleccionar todos los elementos de la lista. De esta forma podrá realizar una acción en toda la selección. Para seleccionar o deseleccionar un elemento en particular, haga clic en la casilla situada a la izquierda del tipo de elemento.

Quitar de la lista

Haga clic aquí para eliminar los elementos seleccionados de la lista. Este botón no borra los archivos del disco duro. Las aplicaciones restringidas deben autorizarse en la consola central para poder utilizarlas.

4.10 Limpieza

4.10.1 Acerca de la limpieza

La limpieza elimina amenazas de los equipos:

- Borrando virus o programas espía en sectores de arranque, documentos, programas y archivos
- Moviendo o borrando archivos sospechosos
- Borrando programas maliciosos o aplicaciones no deseadas

Cuando Sophos Anti-Virus limpia de forma automática virus o programas espía, borrará los archivos maliciosos e intentará desinfectar los elementos infectados. La limpieza no será capaz de reparar el daño que la infección haya podido causar en estos archivos.

Limpieza de documentos

La limpieza de documentos no puede deshacer los efectos secundarios que el virus o programa espía haya podido causar. Consulte [Get cleanup information](#) en la página 42 para más información.

Limpieza de programas

La limpieza de programas es sólo una medida temporal. Debería sustituir los programas afectados desde los discos originales o copias de seguridad.

Limpieza de amenazas en páginas web

Esta función no está disponible para el escaneo de páginas web ya que las amenazas no se encuentran en su ordenador.

Notas

- No es posible deshacer el daño que la amenaza haya podido causar.
- Las acciones que Sophos Anti-Virus realice quedarán anotadas en el Sophos Anti-Virus o en el registro del escaneo personalizado. Consulte [View the scanning log](#) en la página 47 o [View the log for a custom scan](#) en la página 26.
- Para limpiar completamente algunas infecciones múltiples, será necesario que reinicie el equipo. En este caso, tendrá la opción de reiniciar el sistema de forma inmediata o más tarde. El proceso de limpieza continuará cuando reinicie el sistema.

4.10.2 Información de limpieza

Cuando se detecte algún tipo de amenaza en su ordenador, es muy importante que lea la descripción correspondiente en la web de Sophos para entender los posibles daños al sistema y para obtener instrucciones de recuperación y limpieza. Puede hacerlo:

- Desde el propio mensaje de alerta (escaneo en acceso)
- Desde el cuadro de diálogo del escaneo (escaneados personalizados y de botón derecho)
- Desde el área de cuarentena (todos los tipos de escaneo)

Obtener información desde el mensaje de alerta

Si tiene activado el escaneo en acceso, Sophos Anti-Virus mostrará un mensaje de alerta cuando se detecte una amenaza.

En el cuadro del mensaje, haga clic en el nombre de la amenaza sobre la que desea informarse. Sophos Anti-Virus conectará con la web de Sophos para ofrecer una descripción de la amenaza.

Obtener información desde el cuadro de diálogo del escaneo

Para los escaneados personalizados y de botón derecho, en el cuadro de diálogo del escaneo, haga clic en el nombre de la amenaza sobre la que desee obtener información.

Sophos Anti-Virus conectará con la web de Sophos para ofrecer una descripción de la amenaza.

Obtener información desde el área de cuarentena

1. En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Revisar la cuarentena**. Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la columna **Nombre**, haga clic en el nombre de la amenaza sobre la que desee obtener información.

Sophos Anti-Virus conectará con la web de Sophos para ofrecer una descripción de la amenaza.

4.11 Configurar alertas

4.11.1 Configurar la mensajería de escritorio del antivirus

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para que Sophos Anti-Virus muestre un mensaje de escritorio cada vez que se detecte una amenaza, haga lo siguiente. Sólo aplicable al escaneado en acceso.

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Notificación > Mensajes**.
2. En el cuadro de diálogo **Notificación**, abra la ficha **Mensaje de escritorio**. Las opciones disponibles se describen a continuación.

Activar mensaje de escritorio

Active esta opción para que Sophos Anti-Virus muestre un mensaje de escritorio cada vez que se detecte una amenaza.

Notificar

Seleccione los eventos que desea que Sophos Anti-Virus notifique.

Mensaje

Este mensaje se mostrará con cada alerta; indique aquí instrucciones para el usuario.

4.11.2 Configurar las alertas antivirus por email

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para que Sophos Anti-Virus envíe un email de alerta cada vez que se detecte una amenaza o se produzca algún error, haga lo siguiente. (aplicable a los escaneados en acceso, en demanda y de botón derecho).

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Notificación > Mensajes**.

2. En el cuadro de diálogo **Notificación**, abra la ficha **Alerta por email**. Las opciones disponibles se describen a continuación.

Activar alerta por email

Active esta opción para que Sophos Anti-Virus envíe email de alerta.

Notificar

Seleccione los eventos que desea que Sophos Anti-Virus notifique. **Errores de escaneado** incluye ocasiones en que Sophos Anti-Virus no tiene acceso a algún elemento que intenta escanear.

Sophos Anti-Virus no enviará alertas por email ante amenazas detectadas en el escaneado de páginas web ya que dichas amenazas no se encuentran en el ordenador. En este caso no se requiere ninguna acción.

Destinatarios

Haga clic en **Añadir** o **Eliminar** para modificar la lista de direcciones de email a las que se enviarán las alertas. Haga clic en **Editar** para cambiar una dirección ya introducida.

Configurar correo SMTP

Haga clic en este botón para indicar la dirección de su servidor de correo SMTP, la dirección remitente, la dirección de respuesta y el idioma de las alertas (consulte la tabla que aparece a continuación).

Configurar correo SMTP	
Servidor SMTP	Indique el nombre o dirección IP de su servidor SMTP. Haga clic en Probar para verificar el acceso al servidor SMTP (no se enviará <i>ningún</i> mensaje de prueba).
Dirección remitente	Indique la dirección de email a la que llegarán mensajes devueltos o rechazados.
Dirección de respuesta	Indique la dirección a la que se enviarán las respuestas que el mensaje de alerta pueda generar.
Language	Seleccione en la lista desplegable el idioma en el que desea enviar las alertas.

4.11.3 Configurar la mensajería SNMP del antivirus

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Para que Sophos Anti-Virus envíe un mensaje SNMP cada vez que se detecte una amenaza o se produzca algún error, haga lo siguiente (aplicable a los escaneados en acceso, en demanda y de botón derecho).

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Notificación > Mensajes** .
2. En el cuadro de diálogo **Notificación**, abra la ficha **Mensaje SNMP**. Las opciones disponibles se describen a continuación.

Activar mensaje SNMP

Active esta opción para que Sophos Anti-Virus envíe mensajes SNMP de alerta.

Notificar

Seleccione los eventos que desea que Sophos Anti-Virus notifique mediante mensajes SNMP. **Errores de escaneo** incluye ocasiones en que Sophos Anti-Virus no tiene acceso a algún elemento que intenta escanear.

Sophos Anti-Virus no enviará mensajes SNMP ante amenazas detectadas en el escaneo de páginas web ya que dichas amenazas no se encuentran en el ordenador. En este caso no se requiere ninguna acción.

Destino SNMP

Indique la dirección IP del equipo que recibirá las alertas.

Nombre de la comunidad SNMP

Indique el nombre de su comunidad SNMP.

Probar

Haga clic en este botón para enviar un mensaje de prueba a la dirección SNMP indicada.

4.11.4 Configurar el registro de eventos del antivirus

Para que Sophos Anti-Virus añada alertas al registro de eventos de Windows 2000 o posterior cada vez que encuentre una amenaza o se produzca un error, haga lo siguiente (aplicable a los escaneados en acceso, en demanda y de botón derecho).

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar el antivirus y HIPS > Notificación > Mensajes** .

2. En el cuadro de diálogo **Notificación**, abra la ficha **Registro de eventos**. Las opciones disponibles se describen a continuación.

Activar registro de eventos

Active esta opción para que Sophos Anti-Virus envíe un mensaje en el registro de eventos de Windows.

Notificar

Seleccione los eventos que desea que Sophos Anti-Virus notifique. **Errores de escaneado** incluye ocasiones en que Sophos Anti-Virus no tiene acceso a algún elemento que intenta escanear.

Sophos Anti-Virus no enviará mensajes ante amenazas detectadas en el escaneado de páginas web ya que dichas amenazas no se encuentran en el ordenador. En este caso no se requiere ninguna acción.

4.12 Registro del escaneado

4.12.1 Configurar el registro del escaneado

El registro del escaneado se almacena en:

Windows Vista, Windows 7	C:\ProgramData\Sophos\Sophos Anti-Virus\logs\SAV.txt
Otros sistemas Windows	C:\Documents and Settings\All Users\Datos de programa\Sophos\Sophos Anti-Virus\logs\SAV.txt

1. Haga clic en **Inicio > Antivirus y HIPS > Ver el registro del antivirus y HIPS > Configurar registro**.
2. En el cuadro de diálogo **Configurar registro del equipo**, configure las opciones según se describe a continuación.

Nivel del registro

Seleccione la opción **Omitir** para no disponer de registro. Seleccione la opción **Normal** para registrar el resumen de los escaneados, mensajes de error, etc. Seleccione la opción **Detallado** para incluir información como nombre de archivos escaneados, etapas del escaneado, etc.

Archivar registros

Seleccione la opción **Activar archivado** para que se cree un archivo de registro nuevo cada mes. Los archivos comprimidos se almacenan en la misma carpeta que el archivo del registro. Indique el **Número de archivos** máximo que se guardarán. Active la opción **Comprimir registro** para reducir el tamaño de los archivos de registro.

4.12.2 Ver el registro del escaneado

- ❖ En la página de **Inicio**, en **Antivirus y HIPS**, haga clic en **Ver el registro del antivirus y HIPS**.

Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

Desde la página del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

Para buscar un texto concreto en el registro, haga clic en **Buscar** e introduzca el texto que desea encontrar.

5 Control de dispositivos de Sophos

5.1 Acerca del control de dispositivos

Si no se utiliza una consola para administrar Sophos Endpoint Security and Control en el equipo, la función de control de dispositivos *no* está incluida.

El control de dispositivos se activa o desactiva desde una consola de administración. Si el control de dispositivos está activado, puede impedir que se conecte un dispositivo al equipo para tareas de mantenimiento o solución de problemas. Si lo desea, puede desactivar el control de dispositivos de forma temporal en el equipo. Para más información, consulte [Desactivar temporalmente el control de dispositivos](#) en la página 48.

5.2 Tipos de dispositivos controlados

El control de dispositivos bloquea o permite tres tipos de dispositivos: *almacenamiento*, *red* y *corto alcance*.

Almacenamiento

- Dispositivos extraíbles de almacenamiento (como memoria USB, dispositivos PC Card o discos duros externos)
- Unidades ópticas (CD-ROM, DVD o Blu-ray)
- Disqueteras
- Dispositivos seguros de almacenamiento extraíbles (como memoria USB con encriptación por hardware)

Red

- Módems
- Inalámbricos (Wi-Fi, 802.11 estándar)

La política de control de dispositivos puede tener activada la opción **Bloquear puente**, que bloquea otras conexiones de red cuando el ordenador está conectado por cable a la red de la empresa (conexión Ethernet). Cuando el ordenador se desconecta de la red de la empresa, podrá volver a utilizar los dispositivos inalámbricos o módem.

Corto alcance

- Bluetooth
- Infrarrojos (IrDA)

5.3 Desactivar temporalmente el control de dispositivos

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si pertenece al grupo SophosAdministrator y desea conectar algún dispositivo en un ordenador (por ejemplo, para instalar software), desactive el control de dispositivos de forma temporal.

Para desactivar el control de dispositivos en un equipo:

1. En el menú **Configurar**, seleccione **Control de dispositivos**.
2. Desactive la opción **Activar el control de dispositivos**.

5.4 Configurar el registro del control de dispositivos

1. En el menú **Configurar**, seleccione **Control de dispositivos**.
2. En la sección **Nivel del registro**, seleccione una de las opciones:
 - Haga clic en **Omitir** para no disponer de registro.
 - Seleccione la opción **Normal** para registrar el resumen de los escaneados, mensajes de error, etc.
 - Seleccione la opción **Detallado** para proporcionar mucha más información de lo normal. Utilice esta configuración sólo cuando necesite un registro detallado para la solución de problemas, ya que el tamaño del registro puede aumentar muy rápido.
3. En **Archivar registros**, siga las instrucciones en pantalla.

5.5 Ver el registro del control de dispositivos

- ❖ En la página de **Inicio**, en **Control de dispositivos**, haga clic en **Ver el registro del control de dispositivos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

Desde la página del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

Para buscar un texto concreto en el registro, haga clic en **Buscar** e introduzca el texto que desea encontrar.

6 Control de datos de Sophos

6.1 Acerca del control de datos

Si no se utiliza una consola para administrar Sophos Endpoint Security and Control en el equipo, la función de control de datos *no* está incluida.

El control de datos se gestiona mediante la política correspondiente desde la consola de administración. Si pertenece al grupo SophosAdministrator, puede desactivar de forma temporal el control de datos en los equipos para labores de mantenimiento o solución de problemas. Para más información, consulte [Desactivar temporalmente el control de datos](#) en la página 50.

6.2 Desactivar temporalmente el control de datos

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Si pertenece al grupo SophosAdministrator, puede desactivar de forma temporal el control de datos en los equipos para labores de mantenimiento o solución de problemas:

1. En el menú **Configurar**, seleccione **Control de datos**.
2. Desactive la opción **Activar el control de datos**.

6.3 Copiar archivos a un dispositivo de almacenamiento

Si tiene activado el control de datos con una política que bloquea la copia de archivos a dispositivos de almacenamiento controlados, no podrá:

- Guardar datos desde un programa
- Usar el comando de copia de DOS
- Crear un archivo nuevo en el dispositivo con el Explorador de Windows

En este caso, se mostrará un mensaje de aviso. Para copiar el archivo deberá guardarlo primero en el ordenador o en la red y utilizar el Explorador de Windows para realizar la transferencia al dispositivo de almacenamiento.

6.4 Configurar el registro del control de datos

1. En el menú **Configurar**, seleccione **Control de datos**.
2. En la sección **Nivel del registro**, seleccione una de las opciones:
 - Haga clic en **Omitir** para no disponer de registro.
 - Seleccione la opción **Normal** para registrar el resumen de los escaneados, mensajes de error, etc.
 - Seleccione la opción **Detallado** para proporcionar mucha más información de lo normal. Utilice esta configuración sólo cuando necesite probar reglas nuevas del control de datos, ya que el tamaño del registro puede aumentar muy rápido.

3. En **Archivar registros**, siga las instrucciones en pantalla.

6.5 Ver el registro del control de datos

- ❖ En la página de **Inicio**, en **Control de datos**, haga clic en **Ver el registro del control de datos**.

Para más información sobre la página de **Inicio**, consulte [Acercas de la página de inicio](#) en la página 4.

Desde la página del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

Para buscar un texto concreto en el registro, haga clic en **Buscar** e introduzca el texto que desea encontrar.

7 Sophos Client Firewall

7.1 Empezar a usar el cortafuegos

Al instalar el cortafuegos por primera vez, es posible que tenga que configurarlo. Esto depende de cómo se haya instalado. Existen dos tipos de instalación:

- Instalación en un equipo de red administrado desde una consola de administración
- Instalación desde un equipo independiente y administrado desde el equipo

Cortafuegos administrado desde una consola de administración

Si el cortafuegos está instalado y administrado desde una consola de administración, permite o bloquea las aplicaciones y el tráfico según las reglas establecidas por la política.

A menos que la política ponga el cortafuegos en modo interactivo (que se explica a continuación), no recibirá ningún mensaje y no necesita configurar el cortafuegos.

Cortafuegos administrado desde el equipo

Si el cortafuegos se administra desde el equipo, es aconsejable empezar por crear reglas para permitir el acceso a la red para las aplicaciones y servicios habituales, como navegadores de Internet y programas de correo electrónico.

Para más información sobre la creación de reglas, consulte [Acerca de la configuración del cortafuegos](#) en la página 52.

El cortafuegos estará inicialmente en modo interactivo (que se describe a continuación). Deje el cortafuegos en modo interactivo por un tiempo para poder permitir y bloquear otras aplicaciones y servicios que utilice.

Una vez que esté configurado el cortafuegos para que reconozca las aplicaciones que utiliza habitualmente, es aconsejable que cambie el modo por uno de los modos no interactivos.

Para más información, consulte [Cambiar a modo no interactivo](#) en la página 60.

¿Qué es el modo interactivo?

En modo interactivo, el cortafuegos pide al usuario que permita o bloquee las aplicaciones y el tráfico para los que no cuenta con una regla.

Para más información sobre qué hacer con los mensajes del cortafuegos, consulte [Acerca del modo interactivo](#) en la página 60.

7.2 Configurar el cortafuegos

7.2.1 Acerca de la configuración del cortafuegos

El cortafuegos se puede configurar de muchas formas distintas antes de activarlo. Pero, si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Estas son algunas de las funciones comunes:

- [Activar el modo interactivo](#) en la página 60
- [Filtrar mensajes ICMP](#) en la página 58
- [Permitir todo el tráfico en la red local](#) en la página 55
- [Permitir descargas de FTP](#) en la página 54
- [Crear reglas globales](#) en la página 67
- [Permitir una aplicación](#) en la página 57
- [Permitir que las aplicaciones inicien procesos ocultos](#) en la página 71
- [Permitir que las aplicaciones utilicen conexiones de bajo nivel](#) en la página 71
- [Utilizar sumas de verificación para autenticar aplicaciones](#) en la página 72

7.2.2 Desactivar el cortafuegos temporalmente

Si es miembro del grupo SophosAdministrator, podrá activar o desactivar el cortafuegos de forma temporal para tareas de mantenimiento o solución de problemas.

Sophos Endpoint Security and Control mantendrá la configuración incluso tras reiniciar el equipo. Si desactiva el cortafuegos, su ordenador estará desprotegido.

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la sección **Configuración**, active la opción **Permitir todo el tráfico** junto a la ubicación primaria o secundaria.

7.2.3 Permitir aplicaciones de correo electrónico

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Haga clic en **Añadir** y haga doble clic en la aplicación de correo electrónico.

La aplicación de correo electrónico se permite como aplicación de confianza.

Las aplicaciones de confianza tienen permiso completo e incondicional de acceso a la red, incluido acceso a Internet. Para mayor seguridad, puede aplicar las reglas predefinidas proporcionadas por Sophos:

1. En la lista de aplicaciones permitidas, haga clic en la aplicación de correo electrónico.

2. Haga clic en **Personalizar > Predefinidas > Cliente de email** .

7.2.4 Permitir el uso de navegadores de Internet

Nota: al permitir el uso de navegadores de Internet, también se permite el acceso FTP.

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Haga clic en **Añadir** y haga doble clic en el navegador de Internet.

El navegador de Internet se permite como aplicación de confianza.

Las aplicaciones de confianza tienen permiso completo e incondicional de acceso a la red, incluido acceso a Internet. Para mayor seguridad, puede aplicar las reglas predefinidas proporcionadas por Sophos:

1. En la lista de aplicaciones permitidas, haga clic en el navegador de Internet.
2. Haga clic en **Personalizar > Predefinidas > Navegador web** .

7.2.5 Permitir descargas de FTP

Nota: si ha permitido el uso de navegadores de Internet que pueden acceder a servidores FTP, no es necesario permitir también las descargas de FTP.

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Haga clic en **Añadir** y haga doble clic en la aplicación FTP.

La aplicación FTP se permite como aplicación de confianza.

Las aplicaciones de confianza tienen permiso completo e incondicional de acceso a la red, incluido acceso a Internet. Para mayor seguridad, puede aplicar las reglas predefinidas proporcionadas por Sophos:

1. En la lista de aplicaciones permitidas, haga clic en la aplicación FTP.
2. Haga clic en **Personalizar > Predefinidas > Cliente FTP** .

7.2.6 Permitir todo el tráfico en la red local

Para permitir todo el tráfico entre los equipos de una red local:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **Red local**, siga uno de estos procedimientos:
 - Haga clic en **Detectar** para detectar la red local en la que se encuentra el equipo y añádala a la lista de direcciones de red.
 - Haga clic en **Añadir**. En el cuadro de diálogo **Seleccionar dirección**, seleccione el **Formato de dirección**, escriba el nombre del dominio o la dirección IP y haga clic en **Añadir**.
Nota: si selecciona **Red local (detección automática)**, no son necesarios más datos. Para más información sobre la detección de la red local, consulte [Acerca de la detección de red local](#) en la página 65.
4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Seleccionar dirección**.
5. En la ficha **Red local**, active la opción **De confianza** en la red deseada.

Nota

- Al permitir todo el tráfico entre equipos de una red local, también se permite el uso compartido de archivos e impresoras.

7.2.7 Permitir el uso compartido de archivos e impresoras en la red local

Nota: si tiene autorizado todo el tráfico entre ordenadores de una red, no es necesario que autorice también el uso compartido de archivos e impresoras.

Para permitir el uso compartido de archivos e impresoras en la red local:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **Red local**, siga uno de estos procedimientos:
 - Haga clic en **Detectar** para detectar la red local en la que se encuentra el equipo y añádala a la lista de direcciones de red.

- Haga clic en **Añadir**. En el cuadro de diálogo **Seleccionar dirección**, seleccione el **Formato de dirección**, escriba el nombre del dominio o la dirección IP y haga clic en **Añadir**.

Nota: si selecciona **Red local (detección automática)**, no son necesarios más datos. Para más información sobre la detección de la red local, consulte [Acerca de la detección de red local](#) en la página 65.

4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Seleccionar dirección**.
5. En la lista de **Configuración de red**, active la opción **NetBIOS** para permitir el uso compartido de archivos e impresoras en la red local.

Para más información sobre cómo permitir el uso compartido de archivos e impresoras en otras redes aparte de las indicadas en **Red local**, consulte los siguientes apartados:

- [Bloquear el uso compartido de archivos e impresoras](#) en la página 57
- [Control flexible del uso compartido de archivos e impresoras](#) en la página 56

Para más información sobre cómo permitir todo el tráfico en la red, consulte [Permitir todo el tráfico en la red local](#) en la página 55.

7.2.8 Control flexible del uso compartido de archivos e impresoras

Si desea disponer de un control más flexible del uso compartido de archivos e impresoras en su red (por ejemplo, tráfico NetBIOS unidireccional), puede hacer lo siguiente:

1. Permita el uso compartido de archivos e impresoras en otras redes aparte de las indicadas en **Red local**. De esta manera el tráfico NetBIOS en dichas redes será procesado mediante las reglas del cortafuegos.
2. Cree reglas globales de alta prioridad que permitan la comunicación entrante y saliente mediante puertos y protocolos NetBIOS. Se recomienda crear reglas globales que bloqueen de forma explícita el tráfico no deseado del uso compartido de archivos e impresoras en vez de dejarlo en manos de la regla predeterminada.

Para permitir el uso compartido de archivos e impresoras en otras redes aparte de las indicadas en **Red local**:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **Red local**, desactive la opción **Bloquear el uso compartido de archivos e impresoras en otras redes**.

7.2.9 Bloquear el uso compartido de archivos e impresoras

Para bloquear el uso compartido de archivos e impresoras en otras redes aparte de las indicadas en **Red local**:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **Red local**, seleccione la opción **Bloquear el uso compartido de archivos e impresoras en otras redes**.

7.2.10 Permitir una aplicación

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Haga clic en **Añadir** y haga doble clic en la aplicación.

La aplicación se considera de confianza.

Las aplicaciones de confianza tienen permiso completo e incondicional de acceso a la red, incluido acceso a Internet. Para mayor seguridad, puede aplicar una o más *reglas de aplicaciones* para especificar las condiciones bajo las cuales se puede ejecutar la aplicación.

- [Crear una regla de aplicaciones](#) en la página 69
- [Aplicar reglas de aplicaciones predefinidas](#) en la página 69

7.2.11 Bloquear una aplicación

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Si la aplicación no está en la lista, haga clic en **Añadir** y haga doble clic en la aplicación.
5. Seleccione la aplicación en la lista y haga clic en **Bloquear**.

7.2.12 Activar o desactivar el bloqueo de procesos modificados

Los programas maliciosos pueden intentar esquivar el cortafuegos modificando un proceso en memoria iniciado por un programa de confianza, para luego utilizar el proceso modificado para acceder a la red en su lugar.

Si lo desea, puede configurar el cortafuegos para que detecte y bloquee los procesos modificados en memoria.

Para activar o desactivar el bloqueo de procesos modificados:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en la sección **Bloqueo**, desactive la opción **Bloquear procesos si otro programa modifica la memoria** para desactivar el bloqueo de procesos modificados.
Para activar el bloqueo de procesos modificados, active la opción.

Si detecta un proceso que se ha modificado en memoria, el cortafuegos añade reglas para impedir que el proceso modificado acceda a la red.

Notas

- No es aconsejable desactivar el bloqueo de procesos modificados de forma permanente. Sólo debe desactivarlo cuando sea estrictamente necesario.
- El bloqueo de procesos modificados no es compatible con versiones de 64 bits de Windows.
- Sólo se bloquea el proceso modificado. No se impide el acceso a la red al programa que lo ha bloqueado.

7.2.13 Filtrar mensajes ICMP

El protocolo ICMP (protocolo de mensajes de control de Internet) permite el intercambio de información de estado y errores entre los equipos de una red. Si lo desea, puede bloquear o permitir determinados tipos de mensajes ICMP entrantes y salientes.

No se recomienda filtrar los mensajes ICMP a menos que conozca bien los protocolos de red. Para más información sobre los tipos de mensajes ICMP, consulte [Explicación de los tipos de mensajes ICMP](#) en la página 58.

Para filtrar mensajes ICMP:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **ICMP**, active las casillas **Entrada** o **Salida** para permitir los mensajes entrantes o salientes de cada tipo.

7.2.14 Explicación de los tipos de mensajes ICMP

Petición eco, Respuesta eco

Se utilizan para probar la accesibilidad y el estado de los destinos. El host envía una **Petición eco** y espera la **Respuesta**

	eco correspondiente. La operación suele llevarse a cabo con el comando ping .
Destino no alcanzado, Respuesta eco	Enviado por un router cuando no puede entregar un datagrama IP. Los datagramas son las unidades de datos o paquetes transmitidos en una red TCP/IP.
Acallar fuente	Enviado por un host o router si recibe datos demasiado rápido. El mensaje solicita a la fuente que reduzca la velocidad de transmisión de datagramas.
Redireccionar	Enviado por un router si recibe un datagrama que se debería haber enviado a otro router. El mensaje contiene la dirección a la que la fuente debería enviar datagramas en el futuro. Se utiliza para optimizar el enrutado del tráfico de red.
Anuncio de router, Solicitud de router	Permite al host descubrir la existencia de routers. Los routers retransmiten de forma periódica las direcciones IP mediante mensajes Anuncio de router . Los hosts también pueden solicitar la dirección de un router retransmitiendo un mensaje Solicitud de router al que responderá el router con un Anuncio de router .
Tiempo agotado para un datagrama	Enviado por un router cuando el datagrama alcanza el número máximo de routers por los que puede pasar.
Problema de parámetros en un datagrama	Enviado por un router si se produce un problema durante la transmisión de un datagrama que impide finalizar el proceso. Los encabezados incorrectos de los datagramas suelen provocar este problema.
Petición de sincronización, Respuesta timestamp	Se utiliza para sincronizar los relojes entre los hosts para calcular el tiempo de tránsito.
Solicitar información, Respuesta de información	Obsoletos. Los hosts utilizaban estos mensajes para determinar las direcciones entre redes, pero ya no deberían utilizarse.
Petición de máscara de red, Respuesta de máscara de red	Se utiliza para encontrar la máscara de la subred (es decir, las partes de la dirección que definen la red). Un host envía una Petición de máscara de red a un router y recibe una Respuesta de máscara de red .

7.2.15 Restaurar la configuración predeterminada del cortafuegos

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En la sección **Opciones de configuración**, haga clic en **Predeterminado**.

7.3 Modo interactivo

7.3.1 Acerca del modo interactivo

En modo interactivo, el cortafuegos muestra un *cuadro de diálogo de aprendizaje* cada vez que una aplicación desconocida o servicio solicita acceso a la red. El cuadro de diálogo de aprendizaje pide información para permitir el tráfico, bloquearlo una vez o crear una regla para ese tipo de tráfico.

En modo interactivo, existen estos tipos de diálogos de aprendizaje:

- *Cuadros de diálogo de aprendizaje de procesos ocultos* en la página 61
- *Cuadros de diálogo de aprendizaje de protocolo* en la página 61
- *Cuadros de diálogo de aprendizaje de aplicaciones* en la página 61
- *Cuadros de aprendizaje de conexiones de bajo nivel* en la página 61
- *Cuadros de diálogo de aprendizaje de sumas de verificación* en la página 62

7.3.2 Activar el modo interactivo

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en **Modo de funcionamiento**, haga clic en **Interactivo**.

7.3.3 Cambiar a modo no interactivo

Existen dos opciones para el modo no interactivo:

- Permitir por defecto
- Bloquear por defecto

En el modo no interactivo, el cortafuegos aplica las reglas existentes al tráfico de red. El tráfico que no disponga de regla puede permitirse (si es de salida) o bloquearse.

Para cambiar el tipo de modo no interactivo:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en **Modo de funcionamiento**, seleccione **Permitir por defecto** o **Bloquear por defecto**.

7.3.4 Cuadros de diálogo de aprendizaje de procesos ocultos

Los procesos ocultos son las aplicaciones iniciadas por otras para acceder a la red. Las aplicaciones maliciosas pueden usar esta técnica para esquivar los cortafuegos: inician una aplicación de confianza para acceder a la red en lugar de hacerlo directamente.

Los cuadros de diálogo de aprendizaje de procesos ocultos muestran información sobre los procesos ocultos y las aplicaciones que los han iniciado.

■ [Activar cuadros de diálogo de aprendizaje de procesos ocultos](#) en la página 61

7.3.5 Activar cuadros de diálogo de aprendizaje de procesos ocultos

Al utilizar el modo interactivo, el cortafuegos puede mostrar un cuadro de diálogo de aprendizaje si detecta un iniciador de programas nuevo.

Al utilizar el modo interactivo sin activar esta opción, los iniciadores de programas nuevos no tienen permitido el inicio de procesos ocultos.

Para activar diálogos de aprendizaje de procesos ocultos:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Procesos**.
4. Active la casilla **Avisar ante nuevos iniciadores**.

7.3.6 Cuadros de diálogo de aprendizaje de protocolo

Si el cortafuegos detecta actividades en la red que no puede relacionar con ninguna aplicación determinada, solicita la creación de una regla de protocolo.

El cuadro de diálogo de aprendizaje de protocolo muestra información sobre la actividad en la red no reconocida, es decir, el protocolo y la dirección remota.

7.3.7 Cuadros de diálogo de aprendizaje de aplicaciones

Si el cortafuegos detecta una aplicación que intenta acceder a la red de un modo no expresado en ninguna regla, solicita la creación de una regla de aplicaciones.

Los cuadros de diálogo de aprendizaje de aplicaciones muestran información sobre las actividades en la red no reconocidas, es decir, el servicio y la dirección remota.

7.3.8 Cuadros de aprendizaje de conexiones de bajo nivel

Las conexiones de bajo nivel permiten el control de todos los aspectos de los datos enviados por los procesos en la red y pueden utilizarse con fines maliciosos.

Cuando el cortafuegos detecta una conexión de bajo nivel que intenta acceder a la red de un modo no expresado en ninguna regla, solicita la creación de una regla de conexiones de bajo nivel.

Los cuadros de diálogo de aprendizaje de conexiones de bajo nivel muestran información sobre las conexiones de bajo nivel.

- [Activar los cuadros de diálogo de aprendizaje de conexiones de bajo nivel](#) en la página 62

7.3.9 Activar los cuadros de diálogo de aprendizaje de conexiones de bajo nivel

Al utilizar el modo interactivo, el cortafuegos puede mostrar un cuadro de diálogo de aprendizaje al detectar conexiones de bajo nivel que intenten acceder a la red de un modo no especificado en ninguna regla existente.

Al utilizar el modo interactivo sin activar esta opción, las conexiones de bajo nivel no tienen permitido el acceso a la red.

Para activar cuadros de diálogo de aprendizaje de conexiones de bajo nivel:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Procesos**.
4. Active la casilla **Avisar ante conexiones de bajo nivel**.

7.3.10 Cuadros de diálogo de aprendizaje de sumas de verificación

Si el cortafuegos detecta una aplicación nueva o modificada, muestra un cuadro de diálogo de aprendizaje de sumas de verificación.

Si desea permitir que la aplicación acceda a la red, deberá añadir la suma de verificación correspondiente (un identificador exclusivo) a la lista de sumas de verificación reconocidas.

Seleccione una de estas opciones:

- **Añadir suma de verificación a las existentes para esta aplicación** permite diferentes versiones de la aplicación.
- **Sustituir sumas de verificación existentes para esta aplicación** sustituye todas las sumas de verificación existentes de la aplicación con la que solicita el acceso, permitiendo sólo la versión más reciente de la aplicación.
- **Bloquear esta aplicación hasta que se reinicie** bloquea la aplicación en esta ocasión.

7.3.11 Activar cuadros de diálogo de aprendizaje de sumas de verificación

Al utilizar el modo interactivo, el cortafuegos puede mostrar un cuadro de diálogo de aprendizaje si detecta una aplicación nueva o modificada.

Al utilizar el modo interactivo sin activar esta opción, las aplicaciones no tienen permitido el acceso a la red.

Para activar cuadros de diálogo de aprendizaje de sumas de verificación:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la sección **Bloqueo**, active la opción **Autenticar aplicaciones mediante sumas de verificación**.

7.4 Archivos de configuración del cortafuegos

7.4.1 Acerca de los archivos de configuración del cortafuegos

Sophos Client Firewall permite exportar las reglas y la configuración general del cortafuegos como archivos de configuración. Utilice esta función para:

- Crear una copia de seguridad y restaurar la configuración completa del cortafuegos.
- Guardar las opciones de configuración para instalarlas en varios equipos.
- Crear reglas para aplicaciones en un equipo y exportarlas para usarlas en otros equipos con las mismas aplicaciones.
- Usar la consola de administración para unir configuraciones creadas en varios equipos diferentes y crear una política válida para todos los equipos de la red.

7.4.2 Exportar archivos de configuración del cortafuegos

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Haga clic en **Exportar**.
3. Escriba un nombre para el archivo de configuración, seleccione la ubicación y haga clic en **Guardar**.

7.4.3 Importar archivos de configuración del cortafuegos

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Haga clic en **Importar**.
3. Seleccione un archivo de configuración y haga clic en **Abrir**.
4. Siga las instrucciones en pantalla.

7.5 Reglas del cortafuegos

7.5.1 Acerca de las reglas del cortafuegos

Reglas globales

Las reglas globales afectan a todas las comunicaciones de red y a las aplicaciones, incluso si cuentan con reglas de aplicaciones.

Reglas de aplicaciones

Cada aplicación puede tener una o más reglas. Utilice las reglas preconfiguradas por Sophos o cree reglas personalizadas para un control más ajustado del acceso a la aplicación permitido.

7.5.2 Orden de aplicación de las reglas

Para las conexiones de bajo nivel, sólo se comprueban las reglas globales.

Para las conexiones que *no* son de bajo nivel, se comprueban varias reglas, dependiendo de si la conexión es a una dirección en la ficha **Red local**.

Si la dirección aparece en la ficha **Red local**, se comprueban las siguientes reglas:

- Si la dirección es de **Confianza**, se permite todo el tráfico.
- Si la dirección es de **NetBIOS**, se permiten las conexiones de uso compartido de archivos e impresoras según el siguiente criterio:

Conexión	Puerto	Rango
TCP	Remoto	137-139 ó 445
TCP	Local	137-139 ó 445
UDP	Remoto	137 ó 138
UDP	Local	137 ó 138

Si la dirección *no* aparece en la ficha **Red local**, se comprueban otras reglas en el orden siguiente:

1. Para el tráfico **NetBIOS** no autorizado en la ficha **Red local** se aplica la opción **Bloquear el uso compartido de archivos e impresoras en otras redes**:
 - Si activa esta opción, se bloqueará el tráfico.
 - Si desactiva esta opción, se aplicarán las reglas restantes.
2. Se comprueban las reglas globales de alta prioridad en el orden especificado.
3. Si aún no se ha aplicado ninguna regla a la conexión, se comprueban las reglas de aplicaciones.

4. Si la conexión no dispone de reglas, se comprueban las reglas globales de prioridad normal en el orden en que aparecen en la lista.
 5. Si la conexión no dispone de reglas:
 - En el modo **Permitir por defecto**, el tráfico está permitido (si es de salida).
 - En el modo **Bloquear por defecto**, el tráfico está bloqueado.
 - En el modo **Interactivo**, se pide confirmación al usuario.
- Nota:** inicialmente, el cortafuegos se encuentra en el modo **Bloquear por defecto**.

7.5.3 Acerca de la detección de red local

Si lo desea, puede asignar la red local del equipo a las reglas del cortafuegos.

El cortafuegos determina la red local del equipo al iniciarse y vigila cualquier cambio que se produzca mientras está en funcionamiento. Si se detecta algún cambio, el cortafuegos actualiza las reglas correspondientes con el rango de dirección de red nuevo.



Advertencia: Sophos recomienda precaución a la hora de utilizar reglas de red local como parte de las configuraciones que se puedan usar en ubicaciones "fuera de la oficina". Para más información, consulte [Crear una configuración secundaria](#) en la página 74.

7.5.4 Reglas globales

7.5.4.1 Configuración predeterminada de las reglas globales

En esta sección se describen las condiciones y las acciones de las reglas globales predeterminadas. Utilice estas opciones si desea crear una regla global predeterminada nueva.

Permitir traducción DNS (TCP)

- Protocolo: TCP
- Dirección: Saliente
- Puerto remoto: DOMINIO
- Acción: Permitir

Permitir traducción DNS (UDP)

- Protocolo: UDP
- Dirección: Saliente
- Puerto remoto: DNS
- Acción: Permitir filtrado dinámico

Permitir DHCP saliente

- Protocolo: UDP
- Puerto local: BOOTPS, BOOTPC, 546, 547
- Acción: Permitir

Permitir identificación entrante

- Protocolo: TCP
- Dirección: Entrante
- Puerto local: AUTH
- Acción: Permitir

Permitir conexión de retorno

- Protocolo: TCP
- Dirección: Entrante
- Puerto local: 127.0.0.0 (255.255.255.0)
- Acción: Permitir

Permitir protocolo GRE

- Protocolo: TCP
- Tipo de protocolo: Saliente
- Acción: Permitir

Permitir control de conexión PPTP

- Protocolo: TCP
- Dirección: Saliente
- Puerto remoto: PPTP
- Puerto local: 1024-65535
- Acción: Permitir

Bloquear llamada RPC (TCP)

- Protocolo: TCP
- Dirección: Entrante
- Puerto local: DCOM
- Acción: Bloquear

Bloquear llamada RPC (UDP)

- Protocolo: UDP
- Puerto local: 135
- Acción: Bloquear

Bloquear protocolo de bloqueo de mensajes del servidor (TCP)

- Protocolo: TCP
- Dirección: Entrante
- Puerto local: MICROSOFT_DS

- Acción: Bloquear

Bloquear protocolo de mensajes del servidor (UDP)

- Protocolo: TCP
- Puerto local: 445
- Acción: Bloquear

Permitir conexión UDP de host local

- Protocolo: UDP
- Host remoto: 255.255.255.255 (0.0.0.0)
- Host local: 255.255.255.255 (0.0.0.0)
- Puerto local igual al puerto remoto
- Acción: Permitir

7.5.4.2 Crear reglas globales

Importante: se recomienda crear reglas globales sólo si conoce bien los protocolos de red.

Las reglas globales afectan a todas las comunicaciones de red y a las aplicaciones que no disponen de ninguna regla.

Para crear una regla global:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Reglas globales**.
4. Haga clic en **Añadir**.
5. En **Nombre de la regla**, escriba un nombre para la regla.
El nombre debe ser exclusivo en la lista de reglas. No pueden existir dos reglas globales con el mismo nombre.
6. Para aplicar la regla antes que otras reglas de aplicaciones o reglas globales de prioridad normal, active la opción **Alta prioridad**.
Para más información sobre el orden de aplicación de las reglas, consulte [Orden de aplicación de las reglas](#) en la página 64.
7. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
8. En **Seleccione las acciones que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
9. Escoja una de las siguientes opciones:
 - Para permitir otras conexiones con la misma dirección mientras la conexión inicial se encuentra activa, seleccione **Conexiones concurrentes**.
Nota: esta opción sólo está disponible para reglas TCP, por defecto con filtrado dinámico.

- Para permitir las respuestas del equipo remoto según la conexión inicial, seleccione **Filtrado dinámico**.

10. En **Descripción de la regla**, haga clic en un valor subrayado. Por ejemplo, al hacer clic en el enlace **TCP**, se abre el cuadro de diálogo **Select Protocol**.

7.5.4.3 Editar reglas globales

Importante: se recomienda cambiar las reglas globales sólo si conoce bien los protocolos de red.

Para editar una regla global:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Reglas globales**.
4. En la lista **Regla**, seleccione la regla que desea cambiar.
5. Haga clic en el botón **Editar**.
Para más información sobre la configuración de reglas globales, consulte [Crear reglas globales](#) en la página 67.

7.5.4.4 Copiar una regla global

Para copiar una regla global y añadirla a la lista de reglas:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Reglas globales**.
4. En la lista **Regla**, seleccione la regla que desea copiar.
5. Haga clic en **Copiar**.

7.5.4.5 Eliminar una regla global

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Reglas globales**.
4. En la lista **Regla**, seleccione la regla que desea eliminar.
5. Haga clic en **Quitar**.

7.5.4.6 Cambiar el orden de aplicación de las reglas globales

Las reglas globales se aplican en el orden descendente en que aparecen en la lista de reglas.

Para cambiar el orden de aplicación de las reglas globales:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Reglas globales**.
4. En la lista **Regla**, seleccione la regla que desea subir o bajar en la lista.
5. Haga clic en **Arriba** o **Abajo**.

7.5.5 Reglas de aplicaciones

7.5.5.1 Aplicar reglas de aplicaciones predefinidas

Las reglas de aplicaciones predefinidas las crea Sophos. Para añadir reglas predefinidas a la lista de reglas de una aplicación:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Seleccione la aplicación en la lista y haga clic en la flecha situada junto a **Custom**.
5. Señale **Predefinidas** y haga clic en una regla predefinida.

7.5.5.2 Crear una regla de aplicaciones

Para crear una regla personalizada que permita el control ajustado del acceso a una aplicación:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
También puede hacer doble clic en la aplicación de la lista.
5. En el cuadro de diálogo **Reglas de aplicaciones**, haga clic en **Añadir**.
6. En **Nombre de la regla**, escriba un nombre para la regla.
El nombre debe ser exclusivo en la lista de reglas. No puede haber dos reglas con el mismo nombre, pero dos aplicaciones distintas pueden tener una regla que se llame igual.
7. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
8. En **Seleccione las acciones que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
9. Para permitir las respuestas del equipo remoto según la conexión inicial, seleccione **Filtrado dinámico**.

10. En **Descripción de la regla**, haga clic en un valor subrayado. Por ejemplo, al hacer clic en el enlace **TCP**, se abre el cuadro de diálogo **Select Protocol**.

7.5.5.3 Editar reglas de aplicaciones

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
También puede hacer doble clic en la aplicación de la lista.
5. En el cuadro de diálogo **Reglas de aplicaciones**, haga clic en **Editar**.
6. En **Nombre de la regla**, escriba un nombre para la regla.
El nombre debe ser exclusivo en la lista de reglas. No puede haber dos reglas con el mismo nombre, pero dos aplicaciones distintas pueden tener una regla que se llame igual.
7. En **Seleccione los eventos que la regla verificará**, seleccione las condiciones que debe cumplir la conexión para que se aplique la regla.
8. En **Seleccione las acciones que la regla ejecutará**, seleccione **Autorizar** o **Bloquear**.
9. Para permitir las respuestas del equipo remoto según la conexión inicial, seleccione **Filtrado dinámico**.
10. En **Descripción de la regla**, haga clic en un valor subrayado. Por ejemplo, al hacer clic en el enlace **TCP**, se abre el cuadro de diálogo **Select Protocol**.

7.5.5.4 Copiar reglas de aplicaciones

Para copiar una regla de aplicaciones y añadirla a la lista de reglas:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
También puede hacer doble clic en la aplicación de la lista.
5. En el cuadro de diálogo **Reglas de aplicaciones**, haga clic en **Copiar**.

7.5.5.5 Eliminar reglas de aplicaciones

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Seleccione la aplicación en la lista y haga clic en **Personalizar**.

5. En el cuadro de diálogo **Reglas de aplicaciones**, haga clic en **Eliminar**.

7.5.5.6 Cambiar el orden de aplicación de las reglas de aplicaciones

Las reglas de aplicaciones se aplican en el orden descendente en que aparecen en la lista de reglas.

Para cambiar el orden de aplicación de las reglas de aplicaciones:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Aplicaciones**.
4. Seleccione la aplicación en la lista y haga clic en **Personalizar**.
También puede hacer doble clic en la aplicación de la lista.
5. En la lista **Regla**, seleccione la regla que desea subir o bajar en la lista.
6. Haga clic en **Arriba** o **Abajo**.

7.5.5.7 Permitir que las aplicaciones inicien procesos ocultos

A veces, las aplicaciones inician otros procesos ocultos para acceder a la red.

Las aplicaciones maliciosas pueden usar esta técnica para esquivar los cortafuegos: inician una aplicación de confianza para acceder a la red en lugar de hacerlo directamente.

El cortafuegos envía una alerta a la consola de gestión, si se dispone de una, la primera vez que se detecta un proceso oculto.

Para permitir que las aplicaciones inicien procesos ocultos:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Procesos**.
4. En la parte superior, haga clic en el botón **Añadir**.
5. Haga doble clic en la aplicación.

Al utilizar el modo interactivo, el cortafuegos puede mostrar un cuadro de diálogo de aprendizaje si detecta un iniciador de programas nuevo.

■ [Activar el modo interactivo](#) en la página 60

■ [Activar cuadros de diálogo de aprendizaje de procesos ocultos](#) en la página 61

7.5.5.8 Permitir que las aplicaciones utilicen conexiones de bajo nivel

Algunas aplicaciones pueden acceder a la red mediante conexiones de bajo nivel, lo que les proporciona control sobre todos los aspectos de los datos enviados.

Las aplicaciones maliciosas pueden aprovechar las conexiones de bajo nivel suplantando las direcciones IP o enviando mensajes corruptos de forma deliberada.

El cortafuegos envía una alerta a la consola de gestión, si se dispone de una, la primera vez que se detecta una conexión de bajo nivel.

Para permitir que las aplicaciones accedan a la red mediante conexiones de bajo nivel:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Procesos**.
4. En la parte inferior, haga clic en el botón **Añadir**.
5. Haga doble clic en la aplicación.

Al utilizar el modo interactivo, el cortafuegos puede mostrar un cuadro de diálogo de aprendizaje al detectar una conexión de bajo nivel.

- [Activar el modo interactivo](#) en la página 60
- [Activar los cuadros de diálogo de aprendizaje de conexiones de bajo nivel](#) en la página 62

7.5.5.9 Utilizar sumas de verificación para autenticar aplicaciones

Una suma de verificación es un número único que identifica a cada versión de una aplicación. El cortafuegos utiliza estos números para verificar la autenticidad de las aplicaciones autorizadas.

Por defecto, el cortafuegos comprueba todas las sumas de verificación de las aplicaciones que se ejecutan. Si no reconoce la suma de verificación o se ha cambiado, el cortafuegos la bloquea o (en modo interactivo) solicita la intervención del usuario.

El cortafuegos envía una alerta a la consola de gestión, si se dispone de una, la primera vez que se detecta una aplicación nueva o modificada.

Para añadir sumas de verificación a la lista de sumas de verificación permitidas:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. Abra la ficha **Sumas de verificación**.
4. Haga clic en **Añadir**.
5. Haga doble clic en la aplicación.

Al utilizar el modo interactivo, el cortafuegos puede mostrar un cuadro de diálogo de aprendizaje si detecta una aplicación nueva o modificada.

- [Activar el modo interactivo](#) en la página 60
- [Activar cuadros de diálogo de aprendizaje de procesos ocultos](#) en la página 61

7.6 Detección de la ubicación

7.6.1 Sistema de detección de la ubicación

El sistema de detección de la ubicación es una función que se incluye con Sophos Client Firewall y que permite aplicar una configuración del cortafuegos diferente a cada adaptador de red según la ubicación.

Un escenario habitual sería el de un portátil que se utiliza desde la oficina y desde casa. En este caso se están utilizando dos conexiones de red de forma simultánea:

- La conexión a la oficina se realiza a través de VPN mediante un **adaptador de red virtual**.
- La conexión física en casa se realiza a través del proveedor de acceso a Internet mediante un **adaptador de red físico**.

En este escenario, las reglas de configuración del cortafuegos son diferentes para la conexión general a Internet y para el acceso a la red de la empresa.

Nota: la configuración de acceso a Internet debe permitir el acceso "virtual" a la oficina.

7.6.2 Configurar la detección de la ubicación

1. Defina una lista con las direcciones MAC del gateway o con los nombres de dominio de las ubicaciones primarias. Normalmente, las redes de la empresa.
2. Establezca la configuración del cortafuegos que se aplica a las ubicaciones primarias. Normalmente, menos restrictiva.
3. Establezca una configuración secundaria del cortafuegos. Normalmente, más restrictiva.
4. Seleccione la configuración que se aplica en cada caso.

Según el modo de detección que utilice, el cortafuegos obtiene la dirección del DNS o gateway para cada adaptador de red y la compara con la lista establecida.

- Si alguna dirección coincide, se asigna al adaptador de red la configuración de la **ubicación primaria**.
- Si no coincide ninguna dirección, se asigna al adaptador de red la configuración de la **ubicación secundaria**.

La ubicación activa se muestra en el panel **Estado** en la ventana de **Sophos Endpoint Security and Control**. Si aplican las dos configuraciones, la **Ubicación activa** aparece como **Ambas**.

Importante: la configuración secundaria cambia de modo **interactivo** a **bloquear por defecto** cuando se cumplen estas condiciones:

- Las dos ubicaciones se encuentran activas.
- La configuración primaria *no* se encuentra en modo interactivo.

7.6.3 Definir las ubicaciones primarias

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Abra la ficha **Detección de ubicación**.
3. En la sección **Método de detección**, haga clic en **Configurar** junto al método que desea utilizar para definir las ubicaciones primarias:

Opción	Descripción
Identificación DNS	Es necesario crear una lista con los nombres de dominio y direcciones IP que corresponden a las ubicaciones primarias.
Identificación de la dirección MAC del gateway	Es necesario crear una lista de las direcciones MAC del gateway que corresponden a las ubicaciones primarias.

4. Siga las instrucciones en pantalla.

7.6.4 Crear una configuración secundaria

El cortafuegos utiliza la configuración secundaria al detectar que no está conectado a la ubicación primaria.

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Active la opción **Configurar una ubicación secundaria**.

Configure la ubicación secundaria. Para más información sobre cómo hacerlo, consulte [Acerca de la configuración del cortafuegos](#) en la página 52 o la sección *Configurar el cortafuegos*.



Advertencia: un portátil que se utiliza fuera de la oficina podría conectarse a una red desconocida. Si esto ocurre, las reglas de la configuración secundaria que incluyan la dirección de red local podrían permitir tráfico desconocido. Por ello, se recomienda cautela a la hora de utilizar reglas de red local como parte de la configuración secundaria.

7.6.5 Seleccionar la configuración que se aplica

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

2. En la ficha **General**, en la sección **Ubicación actual**, seleccione una de las siguientes opciones:

Opción	Descripción
Ubicación detectada	El cortafuegos aplica la configuración primaria o secundaria según la conexión detectada (establecida en Configurar la detección de la ubicación en la página 73).
Ubicación primaria	El cortafuegos aplica la configuración primaria.
Ubicación secundaria	El cortafuegos aplica la configuración secundaria.

7.7 Informes del cortafuegos

7.7.1 Acerca de los informes del cortafuegos

Por defecto, el cortafuegos informa a la consola de administración sobre cambios en el estado, eventos y errores.

Cambios en el estado del cortafuegos

El cortafuegos considera como tales los cambios de estado siguientes:

- Cambios en el modo de funcionamiento
- Cambios en la versión del software
- Cambios en la configuración del cortafuegos que permite todo el tráfico
- Cambios en el cumplimiento de la política por parte del cortafuegos

Al utilizar el cortafuegos en modo interactivo, puede que necesite que la configuración sea diferente de la establecida desde la consola de administración. En este caso, puede **desactivar** el envío de alertas a la consola sobre las diferencias con la política al hacer cambios en determinadas partes de la configuración del cortafuegos.

Para más información, consulte [Activar o desactivar notificación de cambios locales](#) en la página 76.

Eventos del cortafuegos

Los *eventos* se producen cuando una aplicación del equipo o del sistema operativo del equipo intenta comunicarse con otro equipo mediante una conexión de red.

Si lo desea, puede impedir que el cortafuegos envíe informes sobre los eventos a la consola de administración.

Para más información, consulte [Desactivar la notificación de tráfico desconocido](#) en la página 76.

7.7.2 Activar o desactivar notificación de cambios locales

Si la configuración del cortafuegos varía de la política central, puede **desactivar la notificación de cambios locales**.

De esta forma la consola de administración dejará de recibir alertas de cambios en reglas, aplicaciones, procesos o sumas de verificación. Esto puede convenir, por ejemplo, si utiliza el cortafuegos en modo interactivo.

Si desea controlar que los ordenadores cumplen con la política central del cortafuegos, **active la notificación de cambios locales**.

Para desactivar la notificación de cambios locales:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en la sección **Notificación**, desactive la opción **Enviar una alerta a la consola de administración si se modifica alguna regla global, aplicación, proceso o suma de verificación**.

Para activar la notificación de cambios locales, seleccione dicha opción.

7.7.3 Desactivar la notificación de tráfico desconocido

Si lo desea, puede impedir que el cortafuegos envíe notificación a la consola de administración en relación con tráfico de red desconocido. El tráfico desconocido es el que no dispone de una regla.

Para impedir que el cortafuegos envíe notificación en relación con tráfico de red desconocido:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en la sección **Bloqueo**, seleccione la opción **Autenticar aplicaciones mediante sumas de verificación**.
4. En la sección **Notificación**, desactive la opción **Notificar aplicaciones y tráfico desconocidos a la consola de administración**.

7.7.4 Desactivar la notificación de errores del cortafuegos

Importante: no se recomienda tener desactivada esta opción de forma permanente. Sólo debe desactivarla cuando sea estrictamente necesario.

Para impedir que el cortafuegos envíe notificación de errores a la consola de administración:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en la sección **Notificación**, desactive la opción **Notificar errores a la consola de administración**.

7.7.5 Configurar los mensajes de escritorio

Los mensajes que muestra el cortafuegos en el escritorio mediante sugerencias en pantalla se pueden configurar.

Las sugerencias en pantalla sobre el tráfico y las aplicaciones desconocidas no se muestran en modo interactivo porque la información aparece en los diálogos de aprendizaje.

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En **Configuración**, haga clic en **Configurar** junto a la ubicación que desea configurar.
3. En la ficha **General**, en **Mensaje de escritorio**:
 - Para mostrar las sugerencias sobre errores y advertencias del cortafuegos, active la opción **Mostrar avisos y errores**.
 - Para mostrar sugerencias en pantalla sobre el tráfico y aplicaciones desconocidos, active la casilla **Mostrar aplicaciones y tráfico desconocidos**.

7.8 Registro del cortafuegos

7.8.1 Acerca del visualizador del registro del cortafuegos

El visualizador del registro de Sophos Client Firewall permite ver, filtrar y guardar datos sobre:

- Todas las conexiones
- Conexiones que se han permitido o bloqueado
- Eventos del cortafuegos
- El registro del sistema

7.8.2 Abrir el visualizador del registro del cortafuegos

- ❖ En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

7.8.3 Configurar el registro del cortafuegos

Para administrar el tamaño y el contenido de la base de datos del registro de eventos del cortafuegos:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Configurar el cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Abra la ficha **Registro**.
3. Para administrar el tamaño de la base de datos del registro de eventos del cortafuegos, seleccione una de estas opciones:
 - Para permitir que el tamaño de la base de datos aumente sin límites, haga clic en **Mantener todas las entradas**.
 - Para borrar entradas antiguas, haga clic en **Borrar entradas obsoletas** y configure las opciones de la **Configuración de mantenimiento del registro**.
4. En la sección **Configuración de mantenimiento del registro**, seleccione, al menos, una de las siguientes opciones:
 - Active la opción **Borrar entradas tras** y escriba o seleccione una cantidad en el cuadro **Días**.
 - Active la opción **No guardar más de** y escriba o seleccione una cantidad en el cuadro **Entradas**.
 - Active la opción **No pasar de** y escriba o seleccione una cantidad en el cuadro **MB**.

7.8.4 Cambiar el aspecto del visualizador del registro del cortafuegos

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el menú **Ver**, haga clic en **Diseño**.
3. En el cuadro de diálogo **Personalizar vista**, seleccione los elementos que desea ocultar o mostrar:
 - El **árbol de la consola** aparece en el panel izquierdo.
 - La **barra de herramientas** aparece en la parte superior del visualizador del registro del cortafuegos.
 - La **barra de descripción** aparece sobre los datos en el panel derecho.
 - La **barra de estado** aparece en la parte inferior del visualizador del registro del cortafuegos.

7.8.5 Personalizar el formato de los datos

Si lo desea, puede cambiar el formato utilizado para mostrar los elementos siguientes en los registros del cortafuegos:

- Mostrar los puertos en forma de número o por nombre, por ejemplo, **HTTP** o **80**.
- Mostrar aplicaciones en forma de iconos, rutas de archivo, o ambos.
- Especificar la unidad utilizada para mostrar la velocidad de transferencia, por ejemplo, **KBytes** o **MBytes**.
- Ocultar o mostrar las cuadrículas.

Para personalizar el formato de los datos:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el menú **Ver**, haga clic en **Personalizar**.
3. Seleccione las opciones correspondientes.

7.8.6 Ocultar o mostrar columnas del visualizador del registro del cortafuegos

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Haga clic en un elemento del árbol de la consola para ver las columnas en el panel de información.
3. En el menú **Ver**, seleccione **Añadir/quitar columnas**.
También puede hacer clic con el botón derecho en los encabezados de las columnas.
4. En el cuadro de diálogo **Columnas**, siga uno de estos pasos:
 - Para ocultar las columnas, desactive las casillas correspondientes.
 - Para mostrar las columnas, active las casillas correspondientes.

7.8.7 Reordenar las columnas del visualizador del registro del cortafuegos

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. Haga clic en un elemento del árbol de la consola para ver las columnas en el panel de información.
3. En el menú **Ver**, seleccione **Añadir/quitar columnas**.
También puede hacer clic con el botón derecho en los encabezados de las columnas.

4. En el cuadro de diálogo **Columnas**, haga clic en el nombre de la columna y, a continuación, haga clic en **Arriba** o **Abajo** para cambiar la posición de la columna.

Notas

- También puede reordenar las columnas del panel informativo arrastrando el encabezado de la columna hacia la derecha o hacia la izquierda. Al arrastrar una columna, el espacio resaltado entre los encabezados de las columnas indica la posición nueva de la columna.
- Arrastre los bordes de los encabezados de las columnas para hacerlas más anchas o más estrechas.

7.8.8 Filtrar entradas de registros del cortafuegos

Si lo desea, puede ordenar las entradas del registro del cortafuegos creando un filtro.

Para filtrar las entradas del registro del cortafuegos:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el árbol de la consola, seleccione un registro.
3. En el menú **Acción**, haga clic en **Añadir filtro**.
4. Siga las instrucciones del asistente de **filtrado**.

El filtro aparece en el árbol de la consola justo debajo del nodo del registro para el que creó el filtro.

7.8.9 Exportar todas las entradas del registro del cortafuegos

Para exportar todas las entradas de un registro del cortafuegos a un archivo de texto o CSV:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el árbol de la consola, seleccione un registro.
3. Haga clic con el botón derecho en la lista de entradas y seleccione **Exportar todas las entradas**.
4. En el cuadro de texto **Nombre**, escriba un nombre para el archivo.
5. En la lista **Tipo**, haga clic en el tipo de archivo que desee.

7.8.10 Exportar entradas específicas del registro del cortafuegos

Para exportar entradas específicas de un registro del cortafuegos a un archivo de texto o CSV:

1. En la página de **Inicio**, en **Cortafuegos**, haga clic en **Ver registro del cortafuegos**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

2. En el árbol de la consola, seleccione un registro.
3. Seleccione las entradas que desea exportar.
Si las entradas se actualizan rápidamente, en el menú **Ver**, desactive la opción **Actualizar vista**.
4. En el menú **Acción**, haga clic en **Exportar las entradas seleccionadas**.
5. En el cuadro de texto **Nombre**, escriba un nombre para el archivo.
6. En la lista **Tipo**, haga clic en el tipo de archivo que desee.

8 Sophos AutoUpdate

8.1 Actualización inmediata

Por defecto, Sophos AutoUpdate se actualiza cada 10 minutos si está conectado a la red de la empresa o cada 60 para ordenadores fuera de la red pero con conexión a Internet.

Si utiliza una conexión telefónica a redes, Sophos AutoUpdate se actualizará cuando se conecte a Internet o a la red, y después, cada 60 minutos.

Para realizar una actualización inmediata:

- ❖ Haga clic con el botón derecho en el icono de Sophos Endpoint Security and Control en la bandeja del sistema y seleccione **Actualizar ahora**.

8.2 Programar las actualizaciones

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Puede especificar la frecuencia de actualización de Sophos AutoUpdate.

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Programado**.
3. Seleccione la opción **Activar actualización automática** e indique la frecuencia de actualización (en minutos) de Sophos AutoUpdate.
La actualización en la red se realiza por defecto cada 10 minutos.
Si selecciona Sophos como fuente de actualización, la frecuencia máxima será de 60 minutos.

8.3 Configurar la fuente de actualización

Si desea que Sophos AutoUpdate se actualice de forma automática, deberá especificar la fuente de las actualizaciones.

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Ubicación primaria**.
3. Indique la **Dirección** en forma de ruta UNC o dirección web del servidor de actualización.
Para descargar las actualizaciones directamente desde Sophos por Internet, seleccione **Sophos** en la **Dirección**.
4. Indique el **Nombre de usuario** de acceso al servidor de actualización.
Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma *dominio\usuario*.
5. Indique la **Contraseña** de acceso al servidor de actualización.

8.4 Establecer una fuente alternativa de actualización

Es posible configurar una fuente alternativa de actualización. Si Sophos AutoUpdate no puede actualizarse desde la fuente habitual, lo intentará desde la fuente alternativa.

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Ubicación secundaria**.
3. Indique la **Dirección** en forma de ruta UNC o dirección web del servidor de actualización.

Para descargar las actualizaciones directamente desde Sophos por Internet, seleccione **Sophos** en la **Dirección**.

4. Indique el **Nombre de usuario** de acceso al servidor de actualización.
Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma *dominio\usuario*.
5. Indique la **Contraseña** de acceso al servidor de actualización.

8.5 Realizar la actualización vía proxy

Si su acceso a Internet se realiza a través de un servidor proxy, debe indicar los detalles a Sophos AutoUpdate para poder realizar las descargas.

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Servidor primario** o **Servidor secundario**.
3. Haga clic en el botón **Detalles del proxy**.
4. Active la opción **Usar servidor proxy**.
5. Especifique la **Dirección** y **Puerto** a utilizar.
6. Debe también indicar los datos de la cuenta de acceso al servidor proxy, **Nombre de usuario** y **Contraseña**.

Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma *dominio\usuario*.

8.6 Actualización a través de conexión telefónica a redes

Para actualizarse a través de una conexión telefónica a redes:

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Programado**.
3. Active la opción **Utilizar conexión telefónica**.

Sophos AutoUpdate se actualizará cada vez que se conecte a Internet.

8.7 Limitar el ancho de banda empleado en las actualizaciones

Para impedir que Sophos AutoUpdate utilice todo el ancho de banda necesario para otras tareas (como descargar el correo electrónico), puede limitar el ancho de banda utilizado.

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Servidor primario** o **Servidor secundario**.
3. Haga clic en **Avanzadas**.
4. Active la opción **Limitar el ancho de banda** y mueva el selector para especificar el ancho de banda que Sophos AutoUpdate puede utilizar.

Nota: si especifica un ancho de banda mayor del disponible, Sophos AutoUpdate utilizará todo el ancho de banda.

8.8 Registrar las actividades de actualización

Puede configurar Sophos AutoUpdate para registrar la actividad de actualización en un archivo de registro.

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Registro**.
3. Active la opción **Registrar la actividad de Sophos AutoUpdate**.
4. En el cuadro **Tamaño máximo**, escriba o seleccione el tamaño máximo en MB para el registro.
5. En la lista **Nivel del informe**, seleccione **Normal** o **Detallado**.

El registro detallado ofrece más información por lo que el tamaño del archivo de registro se incrementará más rápidamente. Utilice esta opción sólo cuando necesite un registro detallado para la solución de problemas.

8.9 Ver el registro de actualización

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Registro**.
3. Haga clic en **Ver registro**.

9 Protección contra manipulaciones de Sophos

9.1 Protección contra manipulaciones

La protección contra manipulaciones permite evitar que programas maliciosos o usuarios no autorizados puedan desinstalar el software de seguridad de Sophos o desactivarlo desde Sophos Endpoint Security and Control.

Nota: esta protección puede no ser efectiva ante usuarios con amplios conocimientos técnicos. También podría ser ineficaz ante programas maliciosos diseñados específicamente para realizar ciertos cambios en el funcionamiento del sistema operativo. Este tipo de programas maliciosos se detecta mediante el escaneado de amenazas y comportamientos sospechosos. (Para más información, consulte la sección "Utilizar Sophos Anti-Virus".)

Cómo afecta la protección contra manipulaciones a los diferentes usuarios

SophosUsers y SophosPowerUsers

La protección contra manipulaciones no afecta a los usuarios que pertenecen a los grupos SophosUser y SophosPowerUser. Cuando active la protección contra manipulaciones, los usuarios de estos grupos podrán seguir realizando las tareas habituales sin necesidad de introducir la contraseña de la protección contra manipulaciones.

Los usuarios de los grupos SophosUsers y SophosPowerUsers no pueden activar ni desactivar la protección contra manipulaciones.

Para más información sobre las tareas asignadas a los diferentes grupos de Sophos, consulte [Acerca de los grupos de Sophos](#) en la página 5.

SophosAdministrators

Los usuarios del grupo SophosAdministrator pueden activar o desactivar la protección contra manipulaciones.

Si utiliza la consola de administración para gestionar Sophos Endpoint Security and Control en las estaciones, la política de protección contra manipulaciones determina la contraseña y la configuración de dicha protección. El administrador debe dar a conocer la contraseña a los usuarios autorizados.

Los usuarios del grupo SophosAdministrator deben conocer la contraseña de la protección contra manipulaciones, si está activada, para realizar las siguientes tareas:

- Cambiar la configuración del escaneado en acceso o de la detección de comportamiento sospechoso. Para más información, consulte [Introducir la contraseña para configurar el software](#) en la página 87.
- Desactivar la protección contra manipulaciones. Para más información, consulte [Desactivar la protección contra manipulaciones](#) en la página 86.
- Desinstalar los componentes de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System) desde el Panel de control.
- Desinstalar Sophos SafeGuard Disk Encryption desde el Panel de control.

Los usuarios del grupo SophosAdministrator que no conozcan la contraseña podrán realizar el resto de tareas, aparte de las mencionadas anteriormente.

Si desactiva la protección contra manipulaciones, para volver a activarla deberá utilizar la opción **Autenticar usuario**. Cuando desactiva la protección contra manipulaciones, se restablecen las funciones asociadas al grupo SophosAdministrators. Para más información sobre cómo volver a activar la protección contra manipulaciones, vea [Reactivar la protección contra manipulaciones](#) en la página 87.

9.2 Activar la protección contra manipulaciones

Importante: si se utiliza la consola de administración para gestionar Sophos Endpoint Security and Control en el equipo, se podrían perder los cambios que se realicen de forma local.

Por defecto, la protección contra manipulaciones en Sophos Endpoint Security and Control se encuentra desactivada. Los miembros del grupo SophosAdministrator pueden activarla.

Para activar la protección contra manipulaciones:

1. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Configurar la protección contra manipulaciones**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el cuadro de diálogo **Configuración de la protección contra manipulaciones**, active la opción **Activar la protección contra manipulaciones**.
3. Haga clic en **Establecer** debajo del cuadro de texto **Contraseña**. En el cuadro de diálogo **Contraseña de la protección contra manipulaciones**, introduzca y confirme una contraseña.

Consejo: la contraseña debe contener al menos ocho caracteres, incluyendo mayúsculas, minúsculas y números.

9.3 Desactivar la protección contra manipulaciones

Importante: si se utiliza la consola de administración para gestionar Sophos Endpoint Security and Control en el equipo, se podrían perder los cambios que se realicen de forma local.

Sólo miembros del grupo SophosAdministrator pueden desactivar la protección contra manipulaciones.

Para desactivar la protección contra manipulaciones:

1. Si todavía no se ha autenticado como usuario y la opción **Configurar la protección contra manipulaciones** en la página de **Inicio** no está disponible, siga las instrucciones en [Introducir la contraseña para configurar el software](#) en la página 87 antes de continuar.
2. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Configurar la protección contra manipulaciones**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
3. En el cuadro de diálogo **Configuración de la protección contra manipulaciones**, desactive la opción **Activar la protección contra manipulaciones** y haga clic en **Aceptar**.

9.4 Reactivar la protección contra manipulaciones

Importante: si se utiliza la consola de administración para gestionar Sophos Endpoint Security and Control en el equipo, se podrían perder los cambios que se realicen de forma local.

Los miembros del grupo SophosAdministrator pueden reactivarla.

Para reactivar la protección contra manipulaciones:

1. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Autenticar usuario**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el cuadro de diálogo **Autenticación de la protección contra manipulaciones**, introduzca la contraseña correspondiente y haga clic en **Aceptar**.
3. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Configurar la protección contra manipulaciones**.
4. En el cuadro de diálogo **Configuración de la protección contra manipulaciones**, active la opción **Activar la protección contra manipulaciones**.

9.5 Contraseña de la protección contra manipulaciones

Si tiene activada la protección contra manipulaciones, deberá introducir la contraseña correspondiente para configurar el escaneo en acceso, la detección de comportamiento sospechoso o desactivar la protección contra manipulaciones. Debe pertenecer al grupo SophosAdministrator para poder realizar estas acciones.

Sólo es necesario introducir la contraseña de la protección contra manipulaciones una vez al abrir Sophos Endpoint Security and Control. Si cierra Sophos Endpoint Security and Control y lo vuelve a abrir, tendrá que introducir la contraseña de nuevo.

Si desea desinstalar cualquier componente de Sophos Endpoint Security and Control, deberá conocer la contraseña de la protección contra manipulaciones.

Si desactiva la protección contra manipulaciones, para volver a activarla, deberá introducir la contraseña.

Deberá introducir la contraseña de la protección contra manipulaciones para volver a activarla si:

- Ya había activado la protección contra manipulaciones anteriormente, pero después la había desactivado.
- Ya había establecido una contraseña para la protección contra manipulaciones, aunque no hubiera activado dicha protección.

9.6 Introducir la contraseña para configurar el software

Los usuarios que pertenecen al grupo SophosAdministrator pueden autenticarse utilizando la contraseña para la protección contra manipulaciones.

Para autenticarse:

1. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Autenticar usuario**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el cuadro de diálogo **Autenticación de la protección contra manipulaciones**, introduzca la contraseña correspondiente y haga clic en **Aceptar**.

9.7 Cambiar la contraseña de la protección contra manipulaciones

Importante: si se utiliza la consola de administración para gestionar Sophos Endpoint Security and Control en el equipo, se podrían perder los cambios que se realicen de forma local.

Debe pertenecer al grupo SophosAdministrator para poder cambiar la contraseña de la protección contra manipulaciones.

Para cambiar la contraseña de la protección contra manipulaciones:

1. Si todavía no se ha autenticado como usuario y la opción **Configurar la protección contra manipulaciones** en la página de **Inicio** no está disponible, siga las instrucciones en [Introducir la contraseña para configurar el software](#) en la página 87 antes de continuar.
2. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Configurar la protección contra manipulaciones**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
3. En el cuadro de diálogo **Configuración de la protección contra manipulaciones**, haga clic en **Cambiar** debajo del cuadro de texto **Contraseña**.
4. En el cuadro de diálogo **Contraseña de la protección contra manipulaciones**, introduzca y confirme la nueva contraseña.

Consejo: la contraseña debería contener al menos ocho caracteres, incluyendo mayúsculas, minúsculas y números.

9.8 Desinstalar el software de seguridad de Sophos

Si pertenece al grupo SophosAdministrator, puede desinstalar el software de seguridad de Sophos desde el Panel de control:

- Los componentes de Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System)
- Sophos SafeGuard Disk Encryption

Para desinstalar el software de seguridad de Sophos con la protección contra manipulaciones activada:

1. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Autenticar usuario**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.
2. En el cuadro de diálogo **Autenticación de la protección contra manipulaciones**, introduzca la contraseña correspondiente y haga clic en **Aceptar**.
3. En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Configurar la protección contra manipulaciones**.
4. En el cuadro de diálogo **Configuración de la protección contra manipulaciones**, desactive la opción **Activar la protección contra manipulaciones** y haga clic en **Aceptar**.
Se desactivará la protección contra manipulaciones.
5. En el **Panel de control**, seleccione **Agregar o quitar programas**, seleccione el software que desea desinstalar y haga clic en **Cambiar/Quitar** o **Eliminar**. Siga las instrucciones en pantalla para desinstalar el software.

9.9 Ver el registro de la protección contra manipulaciones

El registro de la protección contra manipulaciones muestra dos tipos de eventos:

- Autenticación satisfactoria, donde se muestra el nombre de usuario y la hora.
- Intento de manipulación, donde se muestra el nombre del componente de Sophos que se intentaba manipular, el nombre de usuario y la hora.

Debe pertenecer al grupo SophosAdministrator para poder ver el registro de la protección contra manipulaciones.

Para ver el registro de la protección contra manipulaciones:

- ❖ En la página de **Inicio**, en la sección **Protección contra manipulaciones**, haga clic en **Ver el registro de la protección contra manipulaciones**.
Para más información sobre la página de **Inicio**, consulte [Acerca de la página de inicio](#) en la página 4.

Desde la página del registro podrá copiar el contenido, enviarlo por email o imprimirlo.

Para buscar un texto concreto en el registro, haga clic en **Buscar** e introduzca el texto que desea encontrar.

10 Solución de problemas

10.1 La última actualización no se completó debido a algún error

10.1.1 Acerca de los errores en las actualizaciones

Encontrará información sobre el problema en el registro de actualización; para más información, consulte [Ver el registro de actualización](#) en la página 84.

A continuación se explican posibles causas del problema y la solución.

- [Sophos Endpoint Security and Control tiene una dirección incorrecta del servidor](#) en la página 90
- [Sophos Endpoint Security and Control tiene una configuración incorrecta del proxy](#) en la página 90
- [La actualización automática no está configurada correctamente](#) en la página 90
- [No se ha mantenido la fuente de actualización](#) en la página 91

10.1.2 Sophos Endpoint Security and Control tiene una dirección incorrecta del servidor

1. En el menú **Configurar**, seleccione **Actualización**.
2. En la ficha **Ubicación primaria** compruebe la dirección del servidor.
Para más información sobre la ficha **Ubicación primaria**, consulte [Configurar la fuente de actualización](#) en la página 82.

10.1.3 Sophos Endpoint Security and Control tiene una configuración incorrecta del proxy

Si Sophos Endpoint Security and Control se actualiza a través de Internet y utiliza un servidor proxy para la conexión, debe configurarlo correctamente.

1. En el menú **Configurar**, seleccione **Actualización**.
2. En la ficha **Ubicación primaria**, haga clic en **Detalles del proxy**.
3. Compruebe que la dirección, el puerto y la cuenta de acceso son correctas.
Para más información sobre los detalles del proxy, consulte [Realizar la actualización vía proxy](#) en la página 83.

10.1.4 La actualización automática no está configurada correctamente

1. En el menú **Configurar**, seleccione **Actualización**.
2. Abra la ficha **Programado**. (Para más información sobre la ficha **Programado**, consulte [Programar las actualizaciones](#) en la página 82.)

3. Si su equipo se encuentra en red, o si se conecta a Internet a través de banda ancha, seleccione la opción **Activar actualización automática** e indique la frecuencia de actualización. Si utiliza conexión telefónica a redes, active la opción **Utilizar conexión telefónica**.

10.1.5 No se ha mantenido la fuente de actualización

Es posible que se haya movido el directorio (de la red o del servidor web) desde el que deberían realizarse las actualizaciones. También es posible que se haya borrado dicho directorio.

Póngase en contacto con el administrador de la red.

10.2 No se pudo limpiar la amenaza

Si Sophos Anti-Virus no ha limpiado una amenaza en su equipo, puede ser por varias razones.

La limpieza automática está desactivada

Si Sophos Anti-Virus no ha intentado la limpieza, compruebe que tiene activada la limpieza automática. Para más información, consulte:

- [Configurar la limpieza del escaneado en acceso](#) en la página 10
- [Configurar la limpieza del escaneado de botón derecho](#) en la página 19
- [Configurar la limpieza del escaneado personalizado](#) en la página 23

La limpieza automática de programas publicitarios y aplicaciones no deseadas no está disponible para el escaneado en acceso.

Falló la limpieza

Si Sophos Anti-Virus no pudo limpiar una amenaza ("Falló la limpieza"), puede que no pueda limpiar ese tipo de amenaza o que no disponga de los derechos de acceso suficientes.

Es necesario un escaneado exhaustivo del ordenador

Puede que necesite ejecutar un escaneado completo para determinar todos los componentes de una amenaza múltiple o para detectar una amenaza en archivos que estaban ocultos y que Sophos Anti-Virus puede limpiar el equipo.

1. Para escanear los discos duros del equipo, incluyendo sectores de arranque, ejecute el escaneado **Escanear el ordenador**. Para más información, consulte [Realizar un escaneado exhaustivo](#) en la página 26.
2. Si la amenaza ha sido detectada sólo de forma parcial, es posible que no disponga de los derechos de acceso suficientes o que algunas unidades o carpetas del ordenador, donde se hallan los componentes de la amenaza, estén excluidos del escaneado. Para más información, consulte [Añadir, modificar y borrar exclusiones del escaneado en acceso](#) en la página 12. Compruebe la lista de elementos excluidos del escaneado. Si la lista contiene varios elementos, bórrelos de la lista y vuelva a escanear el ordenador.

La unidad extraíble está protegida contra escritura

Debe comprobar que el disco no está protegido contra escritura.

La unidad NTFS está protegido contra escritura

Debe comprobar que la unidad NTFS (Windows 2000 o posterior) no está protegida contra escritura.

Detección de fragmentos de virus o programas espía

Sophos Anti-Virus no limpiará un fragmento de virus o programa espía ya que no ha encontrado una correspondencia exacta del virus o programa espía. Consulte [Fragmento de virus/spyware detectado](#) en la página 92.

10.3 Fragmento de virus/spyware detectado

Si se informa de la presencia de un fragmento de virus/spyware:

1. Actualice la protección de forma inmediata, para que Sophos Anti-Virus cuente con los archivos de identidades de virus más recientes.
2. Ejecute un escaneado exhaustivo.

■ [Actualización inmediata](#) en la página 82

■ [Realizar un escaneado exhaustivo](#) en la página 26

Si se siguen detectando fragmentos de virus, póngase en contacto con el soporte técnico de Sophos.

■ [Soporte técnico](#) en la página 104

La detección de un fragmento de virus o programa espía indica que parte de un archivo coincide con parte de un virus o programa espía. Puede deberse a las siguientes causas:

Variedad de un virus o programa espía conocido

Muchos de los virus o programas espía nuevos están basados en otros existentes por lo que es posible que aparezcan fragmentos de código típicos de un virus o programa espía conocido en virus o programas espía nuevos. Si Sophos Anti-Virus encuentra un fragmento de virus o programa espía, podría tratarse en realidad de un virus o programa espía nuevo.

Virus corrupto

A menudo, los virus contienen errores por lo que su rutina de replicado podría fallar, creando archivos corruptos. Sophos Anti-Virus podría detectar el archivo que el virus intentaba crear o infectar. Un virus corrupto no puede extenderse.

Bases de datos con virus o programas espía

Al realizar escaneados exhaustivos, Sophos Anti-Virus podría notificar la existencia de un fragmento de virus o programa espía en una base de datos. Si se da este caso, no borre la base de datos. Póngase en contacto con el soporte técnico de Sophos si necesita ayuda.

Para ver la información de contacto, consulte [Soporte técnico](#) en la página 104.

10.4 Amenaza detectada parcialmente

Para escanear todas las unidades de disco, incluidos los sectores de arranque, ejecute un escaneo completo del equipo.

- [Realizar un escaneo exhaustivo](#) en la página 26

Si la amenaza ha sido detectada sólo de forma parcial, es posible que algunas unidades o carpetas del ordenador, donde se hallan los componentes de la amenaza, estén excluidos del escaneo. Si algunos de los elementos están en la lista de exclusión, elimínelos y vuelva a realizar el escaneo.

- [Añadir, modificar y borrar exclusiones del escaneo en demanda](#) en la página 16

Si la amenaza no se detecta por completo, puede que no tenga derechos suficientes.

Sophos Anti-Virus podría no detectar o eliminar de forma completa amenazas con componentes instalados en unidades de red.

10.5 Programas publicitarios o aplicaciones no deseadas eliminados de la cuarentena

Si un programa espía o aplicación no deseada detectada por Sophos Anti-Virus desaparece del Área de cuarentena, es posible que se haya autorizado desde la consola de administración o por parte de otro usuario. Revise la lista de programas publicitarios y aplicaciones no deseadas autorizados para ver si se ha añadido. Para saber cómo hacerlo, consulte [Autorizar el uso de programas publicitarios y aplicaciones no deseadas](#) en la página 32.

10.6 El sistema va muy lento

Si el sistema se vuelve lento, puede que se esté ejecutando una aplicación no deseada para vigilar el equipo. Si tiene el escaneo en acceso activado, puede que reciba también muchas alertas de escritorio sobre una aplicación no deseada. Para resolver este problema, haga lo siguiente.

1. Ejecute **Escanear el ordenador** para detectar todos los componentes de la aplicación no deseada. Para más información, consulte [Realizar un escaneo exhaustivo](#) en la página 26.

Nota: si se detecta una aplicación no deseada después del escaneo, consulte el paso 2 de la sección [Amenaza detectada parcialmente](#) en la página 93.

2. Limpie el programa publicitario o la aplicación no deseada. Para saber cómo hacerlo, consulte [Revisar programas publicitarios y aplicaciones no deseadas en cuarentena](#) en la página 37.

10.7 Permitir el acceso a unidades con sectores de arranque infectados

Importante: si se utiliza una consola de administración para administrar Sophos Endpoint Security and Control en el equipo, puede sobrescribir los cambios que realice.

Por defecto, Sophos Anti-Virus bloqueará el acceso a unidades extraíbles con sectores de arranque infectados.

Si necesita acceso a la unidad (por ejemplo, para copiar los archivos), haga lo siguiente:

1. Haga clic en **Inicio > Antivirus y HIPS > Configurar antivirus y HIPS > Configurar > Escaneado en acceso**.
2. En la ficha **Escaneado**, active la opción **Permitir el acceso a unidades con sectores de arranque infectados**.

Importante: cuando haya terminado con el disco, extráigalo para evitar posibles infecciones y desactive la opción de acceso.

10.8 No se puede acceder a ciertas áreas de Sophos Endpoint Security and Control

Si no puede utilizar o configurar determinadas áreas de Sophos Endpoint Security and Control, es posible que el acceso a las mismas esté restringido a los usuarios que pertenecen a determinados grupos de Sophos.

Para más información sobre los grupos de usuarios de Sophos, consulte [Acerca de los grupos de Sophos](#) en la página 5.

10.9 Recuperación tras una infección

La recuperación tras el ataque de un virus depende del tipo de infección.

Efectos secundarios de los virus

Algunos virus no provocan efectos secundarios, mientras que otros pueden destruir todos los datos del disco duro.

Algunos virus realizan pequeños cambios de forma gradual en documentos. Este tipo de daño es difícil de detectar y corregir.

Qué hacer

Es importante que lea la descripción ofrecida sobre cada amenaza en la web de Sophos y que compruebe sus documentos detenidamente tras la limpieza. Vea [Información de limpieza](#) en la página 42 para obtener desde la web de Sophos información sobre cada virus.

Siempre debe disponer de copias de seguridad. Si no dispone de copias de seguridad, comience a crearlas para minimizar el impacto de una posible infección.

A veces es posible recuperar datos en discos dañados por un virus. Sophos proporciona herramientas para reparar el daño creado por ciertos virus.

Póngase en contacto con el soporte técnico de Sophos si necesita ayuda.

Para ver la información de contacto, consulte [Soporte técnico](#) en la página 104.

10.10 Recuperación tras una infección de programas publicitarios o aplicaciones no deseadas

Es posible eliminar programas publicitarios o aplicaciones no deseadas, pero no el daño o los cambios que la aplicación haya podido realizar.

Modificación del sistema operativo

Ciertos programas publicitarios y aplicaciones no deseadas introducen cambios en Windows, por ejemplo, para utilizar una conexión diferente a Internet. Sophos Anti-Virus no siempre será capaz de restaurar la configuración utilizada antes de que la aplicación se instalara. Si, por ejemplo, una aplicación no deseada o programa publicitario modifica la página de inicio de su navegador web, Sophos Anti-Virus no podrá averiguar cuál era su página de inicio anterior.

Herramientas sin limpiar

Ciertos programas publicitarios y aplicaciones no deseadas pueden instalar herramientas en forma de archivos .dll o .ocx. Sophos Anti-Virus podría no detectar las herramientas inofensivas (es decir, las que no suponen ninguna amenaza para el sistema), por ejemplo bibliotecas del programa, que no pertenecen a la aplicación en sí. En este caso, dichos archivos no serán eliminados del sistema.

Programas publicitarios o aplicaciones no deseadas como parte de otro programa

Ciertos programas publicitarios o aplicaciones no deseadas forman parte de programas instalados de forma voluntaria y son necesarios para ejecutarlos. Si elimina dicho programa publicitario o aplicación no deseada, su programa podría dejar de funcionar.

Qué hacer

Es importante que lea la descripción ofrecida sobre cada amenaza en la web de Sophos. Vea [Información de limpieza](#) en la página 42 para obtener información sobre cada programa publicitario o aplicación no deseada desde la web de Sophos.

Para poder restaurar su sistema, es aconsejable realizar copias de seguridad frecuentes. Las copias de seguridad deberían incluir programas de uso habitual.

Para más información sobre los efectos secundarios de programas publicitarios y aplicaciones no deseadas, póngase en contacto con el soporte técnico de Sophos.

Para ver la información de contacto, consulte [Soporte técnico](#) en la página 104.

10.11 Error de contraseña

Si está intentando programar un escaneado personalizado y aparece un error sobre la contraseña, compruebe que:

- Utiliza la contraseña correcta para la cuenta

- El campo de contraseña no está vacío

Para asegurarse de que la contraseña es correcta, revise las propiedades de la cuenta de usuario en **Cuentas de usuario** del **Panel de control**.

10.12 Mensaje de error "fallo del servicio"

Síntomas

Aparece uno de los mensajes de error siguientes en el área de notificaciones:

- Antivirus y HIPS: fallo del servicio
- Cortafuegos: fallo del servicio

Causa

Se ha producido un error en uno de los servicios de Sophos Endpoint Security and Control y es necesario reiniciarlo.

Solución

1. Usando Windows, abra Servicios.
2. Escoja una de las siguientes opciones:
 - Si aparece un mensaje de error **Antivirus y HIPS: fallo del servicio**, haga clic con el botón derecho en **Sophos Anti-Virus** y seleccione **Reiniciar**.
 - Si aparece un mensaje de error **Cortafuegos: fallo del servicio**, haga clic con el botón derecho en **Sophos Client Firewall** y seleccione **Reiniciar**.

Notas

- Para abrir los Servicios, haga clic en **Inicio**, **Panel de control**, haga doble clic en **Herramientas administrativas** y haga doble clic en **Servicios**.

10.13 La base de datos del registro del cortafuegos está corrupta

Síntomas

Al utilizar el visor del registro, aparece el mensaje de error "La base de datos del registro de Sophos Client Firewall está corrupta".

Causa

La base de datos del registro del cortafuegos se ha dañado y es necesario volver a crearla.

Solución

Es necesario pertenecer al grupo de administradores de Windows.

1. Usando Windows, abra Servicios.
2. Haga clic con el botón derecho en **Sophos Client Firewall Manager** y, a continuación, haga clic en **Detener**.

3. Desde el Explorador de Windows, vaya a C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Client Firewall\logs.

Puede que necesite mostrar las carpetas y archivos ocultos desde el explorador para ver esta carpeta.

4. Elimine op_data.mdb.
5. En Servicios, haga clic con el botón derecho en **Sophos Client Firewall** Manager y, a continuación, haga clic en **Reiniciar**.

Notas

- Para abrir los Servicios, haga clic en **Inicio, Panel de control**, haga doble clic en **Herramientas administrativas** y haga doble clic en **Servicios**.

11 Glosario

adware y PUA	Los programas publicitarios (adware) muestran anuncios, por ejemplo, en ventanas emergentes, que afectan a la productividad del usuario y al rendimiento del sistema. Las aplicaciones no deseadas (PUA) son programas no maliciosos pero considerados inadecuados para la mayoría de redes empresariales.
análisis de comportamiento de ejecución	Análisis dinámico para detectar comportamiento sospechoso y desbordamiento del búfer.
aplicación de confianza	Aplicación a la que se da acceso incondicional a la red.
aplicación restringida	Aplicación cuya ejecución no está permitida en el equipo por la política de seguridad de la empresa.
archivo de detección (IDE)	Archivo que permite a Sophos Anti-Virus detectar y desinfectar un virus, gusano o troyano.
archivo sospechoso	Archivo con características habituales de virus, aunque no exclusivas.
barra de descripción	Barra en el visor del registro, sobre la vista de datos, que muestra el elemento seleccionado.
bloqueada	Estado que indica que se ha denegado el acceso a la red a una aplicación (incluyendo procesos oculto), conexiones, protocolos, mensajes ICMP, etc.
coincidencia	Se corresponde con el contenido definido en la lista de control de contenido.
conexión de bajo nivel	Las conexiones de bajo nivel permiten el control de todos los aspectos de los datos enviados por los procesos en la red y pueden utilizarse con fines maliciosos.
configuración de procesos	Configuración que especifica si los procesos modificados u ocultos tienen permiso de acceso a la red.
configuración de purgado del registro	Opciones que especifican cuando se borran las entradas del registro.
configuración ICMP	Configuración que especifica los tipos de comunicaciones de administración de la red permitidos.

configuración primaria	Configuración del cortafuegos utilizada para la red empresarial, a la que se conectan los usuarios a diario.
configuración secundaria	Configuración del cortafuegos que se utiliza cuando los usuarios no están conectados a la red empresarial principal, sino a otras redes inalámbricas de hoteles o aeropuertos u otras redes de la empresa.
control de datos	Sistema para prevenir la fuga accidental de datos en las estaciones. Se ejecuta cuando el usuario de una estación intenta transferir un archivo que cumple los criterios definidos en las reglas y políticas de control de datos. Por ejemplo, cuando un usuario intenta copiar una hoja de cálculo que contiene una lista de datos de clientes en un dispositivo de almacenamiento extraíble o cargar un documento marcado como confidencial en una cuenta de correo web, el control de datos bloquea la transferencia si está así configurado.
control de dispositivos	Sistema para prevenir la fuga accidental de datos en las estaciones y la entrada de software externo. Funciona limitando el uso de dispositivos de almacenamiento o red no autorizados.
cuadro de diálogo de aprendizaje	Cuadro de diálogo que solicita la confirmación del usuario para permitir o bloquear la actividad en la red cuando una aplicación desconocida solicita acceso a la red.
detección de comportamiento sospechoso	Análisis dinámico del comportamiento de todos los programas para detectar y bloquear aquellos cuya actividad parezca maliciosa.
detección de desbordamiento del búfer	Detección de ataques de desbordamiento del búfer.
dispositivo de almacenamiento	Dispositivos de almacenamiento extraíbles (unidades de memoria USB, lectores de tarjetas y unidades de disco externas), unidades de CD y DVD, unidades de disquete y dispositivos de almacenamiento extraíbles seguros (por ejemplo, las unidades USB de memoria flash SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise y IronKey Basic con cifrado de hardware).
error de escaneado	Error que se produce durante el escaneado de algún archivo, por ejemplo, acceso denegado.
escaneado del botón derecho	Escaneado de archivos desde Windows Explorer o en el escritorio mediante el menú contextual.

escaneado en acceso	Es la principal forma de protección contra virus. Al acceder (copiar, guardar, mover o abrir) un archivo, Sophos Anti-Virus lo escanea y permite el acceso sólo si no supone una amenaza para el equipo.
escaneado en demanda	Escaneado iniciado por el usuario. Puede escanear desde un solo archivo a todo el contenido del equipo con permiso de lectura.
escaneado exhaustivo	Escaneado íntegro de cada archivo.
escaneado normal	Escaneado de las partes de cada archivo que pueden contener virus.
escaneado programado	Escaneado del ordenador, o parte, que se ejecuta a las horas establecidas.
evento de amenaza	Detección o desinfección de alguna amenaza.
evento del cortafuegos	Situación que se produce cuando una aplicación desconocida o sistema operativo de un equipo intentan comunicarse con otro equipo mediante una conexión de red de un modo no solicitado por las aplicaciones en ejecución en el otro equipo.
filtrado dinámico	Tecnología del cortafuegos que mantiene una tabla de las sesiones activas TCP y UDP. Sólo se permite el paso de paquetes pertenecientes a conexiones activas.
gestor de autorización	Módulo que permite autorizar programas publicitarios y aplicaciones no deseadas, archivos sospechosos, aplicaciones que presentan comportamientos sospechosos y desbordamientos del búfer.
HIPS (sistema de prevención contra intrusiones)	Término general para el análisis de comportamiento previo y durante la ejecución.
ICMP	Del inglés "Internet Control Message Protocol". Una capa de red para el protocolo de Internet que proporciona corrección de errores e información relevante a el procesamiento de paquetes IP.
limpieza	La limpieza elimina amenazas de los equipos: quitando virus en archivos y sectores de arranque, moviendo o borrando archivos sospechosos, o borrando elementos de programas publicitarios u otras aplicaciones no deseadas. Esta función no está disponible para el escaneado de páginas web ya que las amenazas no se encuentran en su ordenador. En este caso no se requiere ninguna acción.

limpieza automática	Limpieza que se realiza sin la intervención del usuario o tras la confirmación del usuario.
limpieza manual	Limpieza que se realiza mediante herramientas específicas o borrando archivos de forma manual.
lista de control de contenido (LCC)	Conjunto de condiciones que especifican el contenido de archivos, por ejemplo, números de tarjetas de crédito o datos bancarios, junto a otra información personal. Existen dos tipos de listas de control de contenido: las listas de control de contenido de SophosLabs y las personalizadas.
memoria del sistema	Memoria que funciona como puente entre las aplicaciones y los datos procesados a nivel de hardware. La utiliza el sistema operativo.
mensajería instantánea	Categoría de aplicaciones restringidas donde se incluyen programas de chat (como MSN).
modo de funcionamiento	Configuración que determina si el cortafuegos lleva a cabo acciones con la interacción del usuario (modo interactivo) o de forma automática (modos no interactivos).
modo interactivo	Modo en el que el cortafuegos muestra cuadros de diálogo de aprendizaje al detectar tráfico de red para el que no dispone de reglas.
modo no interactivo	Modo en el que el cortafuegos bloquea o permite todo el tráfico de red para el que no dispone de reglas.
NetBIOS	Del inglés "Network Basic Input/Output System". Software que proporciona una interfaz entre el sistema operativo, el bus E/S y la red. Casi todas las redes locales de Windows están basadas en NetBIOS.
política del cortafuegos	Configuración proporcionada por la consola de administración que utiliza el cortafuegos para controlar la conexión del equipo a Internet y a otras redes.
proceso oculto	A veces, ciertas aplicaciones inician procesos ocultos para acceder a la red. Las aplicaciones maliciosas pueden usar esta técnica para esquivar los cortafuegos: inician una aplicación de confianza para acceder a la red en lugar de hacerlo directamente.
programas espía	Programa que se instala en un equipo de forma inadvertida y envía información sin conocimiento ni autorización del usuario.

Protección activa de Sophos	Función que utiliza la conexión a Internet para comprobar archivos sospechosos.
protección contra manipulaciones	Función que evita que programas maliciosos o usuarios no autorizados puedan desinstalar el software de seguridad de Sophos o desactivarlo desde Sophos Endpoint Security and Control.
protocolo de red	Conjunto de reglas y estándares diseñados para permitir las conexiones entre equipos en la red y el intercambio de información con el mínimo error posible.
regla de aplicación	Regla que afecta sólo a los paquetes de datos transferidos en la red entrantes o salientes de una aplicación.
regla de contenido	Regla que contiene una o más listas de control de contenido y especifica la acción que se lleva a cabo si el usuario intenta transferir datos que coinciden con las listas de control de contenido de la regla al destino especificado.
regla del sistema	Regla que se asigna a todas las aplicaciones y que permite o bloquea comunicaciones de bajo nivel.
regla global de alta prioridad	Regla global que se aplica antes que otras reglas globales o reglas de aplicaciones.
regla personalizada	Regla creada por el usuario para especificar las circunstancias bajo las cuales una aplicación se puede ejecutar.
reglas globales	Reglas aplicadas a todas las aplicaciones y conexiones de red que no disponen de ninguna otra regla. Tienen una prioridad más baja que las reglas configuradas en la página de la red local. También tienen menor prioridad que las reglas de aplicaciones (a menos que el usuario indique lo contrario).
rootkit	Troyano o tecnología que se utiliza para ocultar la presencia de un objeto malicioso (proceso, archivo, clave del registro o puerto de red) ante el usuario o el administrador.
suma de verificación	Una suma de verificación es un número único que identifica a cada versión de una aplicación. El cortafuegos utiliza estos números para verificar la autenticidad de las aplicaciones autorizadas.
tipo de archivo verdadero	Tipo de archivo establecido mediante el análisis de la estructura del archivo, en contraposición a la extensión del mismo. Este método es más fiable.

tráfico desconocido	Forma de acceso de una aplicación o servicio a la red para la que el cortafuegos no dispone de una regla.
virus no identificado	Virus para el que todavía no existe un archivo de detección específico.
visor del registro	Componente del cortafuegos donde se puede consultar la base de datos de eventos, como las conexiones permitidas o bloqueadas, el registro del sistema y alertas.
vista de datos	Vista que muestra los datos según el elemento seleccionado.
vista de árbol	Vista que lista los elementos que se pueden seleccionar en el visor del registro.
voz sobre IP	Categoría de aplicaciones restringidas donde se incluyen programas de llamadas por Internet.
área de cuarentena	Módulo que permite revisar los elementos que se han puesto en cuarentena.

12 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar el fórum SophosTalk en <http://community.sophos.com/> para consultar casos similares.
- Visitar la base de conocimiento de Sophos en <http://esp.sophos.com/support/>.
- Descargar la documentación correspondiente desde <http://esp.sophos.com/support/docs/>.
- Enviar un email a support@sophos.com indicando la versión del producto de Sophos, el sistema operativo y parches aplicados, y el texto exacto de cualquier mensaje de error.

13 Aviso legal

Copyright © 2011 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos y Sophos Anti-Virus son marcas registradas de Sophos Limited. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

Common Public License

El software de Sophos descrito en este documento incluye o puede incluir software con licencia (o sublicencia) de público común (CPL) que, entre otros derechos, permiten al usuario tener acceso al código fuente. Las licencias de dichos programas, que se distribuyen al usuario en formato de código de objeto, exigen que el código fuente esté disponible. Para cualquiera de tales programas que se distribuya junto con el producto de Sophos, el código fuente se ofrece a petición por correo; envíe su solicitud a Sophos por email a support@sophos.com o por Internet desde <http://www.sophos.com/support/queries/enterprise.html>. Para ver los términos de la licencia CPL, visite <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2011 The OpenSSL Project. Todos los derechos reservados.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (ey@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Índice

A

- acceso a discos 8, 94
- activar el cuadro de diálogo de aprendizaje de sumas de verificación 62
- activar el escaneo en acceso 10
- actualización 82, 84, 90
- actualización inmediata 82
- actualización mediante conexión telefónica 82
- adware 93, 95
 - autorización 32
 - detectar 8, 18, 22
 - limpieza automática 19, 23
- adware autorizado, bloquear 32
- amenaza detectada parcialmente 93
- análisis de amenazas 42
- análisis de comportamiento de ejecución 14, 27
- ancho de banda de actualización, limitar 84
- antivirus
 - configurar el registro de eventos 45
 - configurar la mensajería SNMP 44
 - configurar las alertas por email 43
 - configurar, mensajería de escritorio 43
- añadir usuarios a grupos de Sophos 6
- aplicaciones
 - bloquear 57
 - permitir 57
 - sumas de verificación para autenticar aplicaciones 72
- aplicaciones no deseadas en cuarentena, revisar 37
- aplicaciones restringidas
 - autorización 41
 - detectar 31
 - gestionar 41
- archivos comprimidos, escaneo 8, 18, 22
- archivos de configuración del cortafuegos
 - exportar 63
 - importar 63
- archivos sospechosos
 - autorización 33
 - detectar 8, 18, 22
 - limpieza automática 10, 19, 23
- archivos sospechosos en cuarentena, revisar 38
- área de cuarentena 34
- autenticación de aplicaciones, sumas de verificación 72

- autorización
 - adware 32
 - aplicaciones restringidas 41
 - archivos sospechosos 33
 - comportamiento sospechoso 33, 40
 - desbordamientos del búfer 33, 40
 - PUA (aplicaciones no deseadas) 32
 - sitios web 33

B

- bloquear
 - adware autorizado 32
 - aplicaciones 57
 - PUA autorizadas 32
 - sitios web maliciosos 31
 - uso compartido de archivos e impresoras 57
- borrar escaneados personalizados 26

C

- cambiar el nombre de un escaneo programado 25
- comportamiento malicioso
 - detectar 28
- comportamiento sospechoso
 - autorización 33, 40
 - detectar 28
- comportamientos sospechosos en cuarentena, revisar 40
- conexiones de bajo nivel, permitir 71
- configuración secundaria
 - crear 74
- configurar
 - informes centrales 75
 - alertas antivirus por email 43
 - derechos sobre el área de cuarentena 6
 - escaneo de botón derecho 18
 - escaneo en acceso 8
 - escaneados personalizados 22
 - mensajería de escritorio del antivirus 43
 - mensajería SNMP del antivirus 44
 - registro de eventos del antivirus 45
 - registro del cortafuegos 78
 - registro del escaneo 46
- configurar reglas globales 67–68, 71
- configurar una regla 68
- control de comportamiento 27
 - activar 14, 27
- control de datos, desactivar temporalmente 50

control de dispositivos 48
 bloqueo de puentes de red 48
 dispositivos controlados 48
 correo electrónico, permitir 53
 cortafuegos
 desactivar 53
 crear escaneados personalizados 21
 cuadro de diálogo de aprendizaje de sumas de
 verificación
 activar 62
 modo interactivo 62

D

derechos de acceso 5, 94
 derechos de usuario 5, 94
 derechos sobre el área de cuarentena, configurar 6
 desactivar el cortafuegos 53
 desactivar el escaneado en acceso 10
 desactivar escaneado 48
 desactivar la detección de aplicaciones restringidas
 32
 desbordamientos del búfer
 autorización 33, 40
 detectar 29
 descargas de FTP, permitir 54
 desinfección 91
 desinstalar el software de seguridad de Sophos 88
 detección de la ubicación
 acerca de 73
 crear configuración secundaria 74
 definir las ubicaciones primarias 74
 usar dos adaptadores de red 73
 detección parcial 93
 detectar aplicaciones restringidas 31
 detectar archivos sospechosos 8, 18, 22
 detectar comportamiento malicioso 28
 detectar comportamiento sospechoso 28
 detectar desbordamientos del búfer 29
 detectar programas publicitarios y aplicaciones no
 deseadas 8, 18, 22
 detectar rootkits 22
 detectar virus de Mac 8
 dos adaptadores de red
 usar 73

E

efectos secundarios 95
 ejecutar escaneado con baja prioridad 22

ejecutar escaneados personalizados 25
 elementos sospechosos, preautorizar 33
 eliminar sumas de verificación de archivos
 escaneados 11
 entradas de registro
 filtrar 80
 error de contraseña 95
 escaneado de aplicaciones restringidas, desactivar
 32
 escaneado de botón derecho 20
 escaneado de botón derecho, configurar 18
 escaneado de botón derecho, ejecutar 20
 escaneado de la memoria del sistema 8, 22
 escaneado de un elemento 20
 escaneado en acceso
 activar 10
 configurar 8
 desactivar 10
 especificar extensiones de archivo 12
 excluir elementos 12
 escaneado en acceso y en demanda, diferencias 8
 escaneado en demanda
 especificar extensiones de archivo 15
 excluir elementos 16
 escaneado exhaustivo, realizar 26
 escaneados en demanda, tipos de 15
 escaneados personalizados
 cambiar el nombre 25
 configurar 22
 crear 21
 ejecutar 25
 eliminar 26
 programación 24
 escanear archivos comprimidos 8, 18, 22
 escanear memoria del sistema 8, 22
 escanear todos los archivos 8, 18, 22
 escanear un elemento 20
 especificar extensiones de archivo del escaneado en
 acceso 12
 excluir elementos del escaneado en acceso 12
 excluir elementos del escaneado en demanda 16
 exportar archivos de configuración del cortafuegos
 63
 exportar entradas del visualizador del registro del
 cortafuegos 80

F

filtrar entradas de registro 80
 filtrar mensajes ICMP 58

fragmento 91
fragmento detectado, solución de problemas 92

G

gestionar las aplicaciones restringidas 41
Grupos de Sophos 5
 añadir usuarios 6
grupos de usuario 5, 94

H

HIPS 27

I

icono de la bandeja del sistema. 90
iconos
 elementos a escanear 21
importar archivos de configuración del cortafuegos 63
información de limpieza 42
información de seguridad 42
informes centrales, configuración 75

L

limitar el ancho de banda de actualización 84
limpieza
 acerca de 41
 solución de problemas 91
limpieza automática
 adware 19, 23
 archivos sospechosos 10, 19, 23
 programas espía 10, 19, 23
 PUA (aplicaciones no deseadas) 19, 23
 virus 10, 19, 23

M

mensajes ICMP
 filtrar 58
 información sobre 58
modo de funcionamiento, activar modo interactivo 60
modo interactivo
 cuadro de diálogo de aprendizaje de sumas de verificación 62
 mensajes de aplicaciones 61
 mensajes de conexiones de bajo nivel 61

modo interactivo (*continuación*)
 mensajes de procesos ocultos 61
 mensajes de protocolo 61
modo interactivo, acerca de 60
modo interactivo, activar 60
modo no interactivo, cambiar a 60

N

navegadores de Internet, permitir 54

O

obtener instrucciones de limpieza 42

P

página de inicio 4
para empezar
 por dónde empezar 52
permitir
 aplicaciones 57
 conexiones de bajo nivel 71
 correo electrónico 53
 descargas de FTP 54
 navegadores de Internet 54
 procesos ocultos 71
 tráfico de red local 55
 uso compartido de archivos e impresoras 55–56
preautorizar elementos sospechosos 33
prioridad de reglas 64
prioridad, escaneado 22
procesos ocultos, permitir 71
programar escaneados programados 24
programar la actualización 82
programar un escaneado 95
programas espía
 limpieza automática 10, 19, 23
programas espía en cuarentena, revisar 36
programas publicitarios en cuarentena, revisar 37
Protección activa de Sophos
 activar 30
 apagar 30
 desactivar 30
 descripción 29
 encender 30
 registro 30
 tecnología en la nube 29

protección contra manipulaciones
 activar 86
 apagar 86
 autenticación de usuario 87
 cambiar contraseña 88
 configurar el software 87
 desactivar 86
 descripción 85
 desinstalar el software de seguridad de Sophos 88
 desinstalar Sophos Endpoint Security and Control 88
 encender 86
 introducir contraseña 87
 reactivar 87
 registro 89

protección web
 descripción 31

PUA (aplicaciones no deseadas) 93, 95
 autorización 32
 detectar 8, 18, 22
 limpieza automática 19, 23

PUA autorizadas, bloquear 32

R

realizar un escaneado de botón derecho 20
 realizar un escaneado exhaustivo 26
 recuperación 95
 registro de actualización 84
 registro de un escaneado personalizado
 visualizar 26

registro del cortafuegos
 configurar 78

registro del escaneado
 configurar 46
 visualizar 47

regla
 configurar 68

reglas globales
 configurar 67–68, 71

reglas globales predeterminadas
 más información 65

revisar aplicaciones no deseadas en cuarentena 37
 revisar archivos sospechosos en cuarentena 38
 revisar comportamientos sospechosos en cuarentena 40
 revisar programas espía en cuarentena 36
 revisar programas publicitarios en cuarentena 37
 revisar virus en cuarentena 36

rootkits, detectar 22

S

sector de arranque infectado 8, 94
 servidor primario 82
 servidor proxy 83
 servidor secundario 83
 sistema de prevención contra intrusiones 27
 sistema lento, solución de problemas 93
 sitios web
 autorización 33
 sitios web maliciosos
 protección 31

Sophos Endpoint Security and Control 3
 sumas de verificación de archivos escaneados, eliminar 11
 sumas de verificación, autenticación de aplicaciones 72
 suspender escaneado 48

T

tecnología en la nube 29
 tipos de escaneado en demanda 15
 todos los archivos, escaneado 8, 18, 22
 tráfico de red local, permitir 55

U

ubicaciones primarias
 definir 74

uso compartido de archivos e impresoras, permitir 55–57
 uso compartido de archivos, bloquear 57
 uso compartido de archivos, permitir 55–56
 uso compartido de impresoras, bloquear 57
 uso compartido de impresoras, permitir 55–56

V

virus
 limpieza automática 10, 19, 23
 recuperación 94

virus de Mac, detectar 8
 virus en cuarentena, revisar 36

visor del registro
 acerca de 77

visualizador del registro del cortafuegos
 exportar entradas 80

visualizar
registro de un escaneado personalizado 26

visualizar (*continuación*)
registro del escaneado 47